INTERNATIONAL STANDARD

ISO 15118-20

First edition
2022-04

Road vehicles — Vehicle to grid communication interface —

Part 20: 2nd generation network layer and application layer requirements

Véhicules routiers — Interface de communication entre véhicule et réseau électrique —

Partie 20: Exigences des couches réseau et application de 2ème génération

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Reference number
ISO 15118-20:2022(E)

© ISO 2022

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022



COPYRIGHT PROTECTED DOCUMENT

© ISO 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO 2022 – All rights reserved

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 4

4 Abbreviated terms 12

5 Conventions 15
5.1 Definition of OSI based services 15
5.2 Requirement structure 15
5.3 Usage of references 16
5.4 Notation used for XML schema diagrams 16

6 Document overview 16

7 Basic requirements for V2G communication 17
7.1 General information 17
7.2 Service primitive concept of OSI layered architecture 18
7.2.1 Overview 18
7.2.2 Syntax of service primitives 18
7.3 Security concept 19
7.3.1 General 19
7.3.2 Certificate and key management 21
7.3.3 Number of root certificates and root validity 35
7.3.4 Support and application of TLS 37
7.3.5 Firewall 38
7.3.6 Protection of the cryptographic keys 38
7.3.7 Random number generation 40
7.4 V2G communication states and data link handling 42
7.5 Data link layer 46
7.5.1 Data link layer security for WLAN 46
7.6 Network link layer 51
7.6.1 General 51
7.6.2 Applicable RFCs, limitations and protocol parameter settings 51
7.6.3 IP addressing 53
7.7 Transport layer 54
7.7.1 Transmission control protocol (TCP) 54
7.7.2 User datagram protocol (UDP) 55
7.7.3 Transport layer security (TLS) 56
7.8 V2G transfer protocol 82
7.8.1 General information 82
7.8.2 Supported ports 83
7.8.3 Protocol data unit 84
7.9 Presentation layer 87
7.9.1 XML and efficient XML interchange (EXI) 87
7.9.2 Message security 90
7.10 Application layer 115
7.10.1 SECC discovery protocol 115

8 Application layer messages 128
8.1 General information and definitions 128
8.2 Protocol handshake definition 129

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

8.2.1 Handshake sequence 129
8.2.2 Message definition supportedAppProtocolReq and supportedAppProtocolRes 131
8.2.3 Semantics description supportedAppProtocol messages 132
8.2.4 Message examples 133
8.3 V2G message definition 134
8.3.1 Overview 134
8.3.2 General 135
8.3.3 Header definition 135
8.3.4 Request and response definitions 138
8.3.5 Complex data types 240
8.4 Service selection 361
8.4.1 General 361
8.4.2 General description of configuration parameters 362
8.4.3 Selection of service and service parameters 363
8.5 V2G communication timing 373
8.5.1 Overview 373
8.5.2 Common 373
8.5.3 DC service 374
8.5.4 Message sequence and communication session 374
8.5.5 Session setup and ready to charge 381
8.5.6 V2G message synchronization for AC and DC with IEC 61851-1 signalling 387
8.5.7 V2G message synchronization with IEC 61980-2 signalling for WPT 394
8.6 Message sequencing and error handling 394
8.6.1 Overview 394
8.6.2 Basic definitions for error handling 395
8.6.3 ResponseCode handling 395
8.6.4 Request-response message sequence requirements 406
8.6.5 Multiplexed communication 434
8.6.6 Message sequence diagrams 437
Annex A (normative) Schema definition 442
Annex B (normative) Certificate profiles 444
Annex C (normative) Specification of identifiers 498
Annex D (informative) ACDP 504
Annex E (informative) Basic PPD for interoperability 506
Annex F (informative) Message sequencing for renegotiation 509
Annex G (informative) Association of VAS client to V2G session 511
Annex H (informative) Application of certificates 512
Annex I (informative) Precision of measurements and tolerances 547
Annex J (informative) Absolute pricing examples 549

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared jointly by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 31, *Data communication*, Technical Committee IEC/TC 69, *Electrical power/energy transfer systems for electrically propelled road vehicles and industrial trucks*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 301, *Electrically propelled road vehicles,* in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

A list of all parts in the ISO 15118 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Introduction

The pending energy crisis and necessity to reduce greenhouse gas emissions started in the former century has led the vehicle manufacturers to a very significant effort to reduce the energy consumption of their vehicles up to the present. As countermeasures to this continuous problem, they developed vehicles partly or completely propelled by electric power and launched them into the market. Those vehicles will reduce the dependency on oil, improve the global energy efficiency and reduce the total CO_2 emissions for road transportation if the electricity is produced from renewable sources. To charge electricity to the batteries of such vehicles, a specific charging infrastructure is required.

Much of the standardization work on dimensional and electrical specifications of the charging infrastructure for electric vehicles and the vehicle interface were treated in the relevant ISO or IEC groups. However, the standardization work about direct information transfer between the electric vehicle and the charging infrastructure was not enough, and it was assigned to the ISO 15118 series to treat the subject sufficiently.

Such communication is necessary for the optimization of energy resources and energy production systems. With it electric vehicles can be connected to the supply network and communicate the most economic or most energy efficient way for charging/discharging. It is also required to develop efficient and convenient billing systems in order to cover the resulting payments. The necessary communication channel can serve in the future to contribute to the stabilization of the supply network as well as to support additional information services required to operate electric vehicles efficiently and economically.

After the standardization work of the first basic smart charging was completed, more standardization work for further evolved functions and high energy efficiency was continuously requested again.

It includes:

— improved charge methods that reduces efforts and agonies of the charging operation;

— extended functions for the electric vehicles to be utilized as distributed energy resources, which enable smoothing of the electricity load of the supply network for higher energy efficiency and also provide power back to the grid;

— information services for the user with higher added value and new convenience.

As for the communication system, the next evolution will be expected to realize these new applications.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Road vehicles — Vehicle to grid communication interface —

Part 20: Network and application protocol requirements

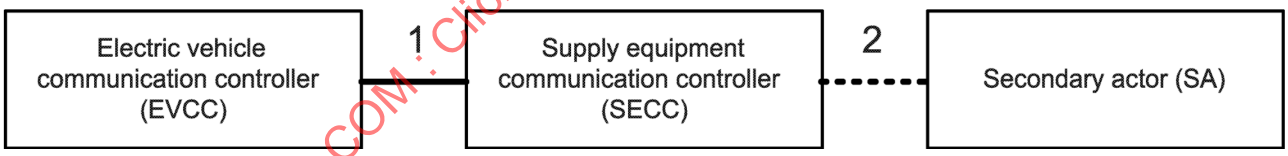
1 Scope

This document specifies the communication between the electric vehicle (EV), including battery electric vehicle (BEV) and plug-in hybrid electric vehicle (PHEV), and the electric vehicle supply equipment (EVSE). The application layer messages defined in this document are designed to support the electricity power transfer between an EV and an EVSE.

This document defines the communication messages and sequence requirements for bidirectional power transfer.

This document furthermore defines requirements of wireless communication for both conductive charging and wireless charging as well as communication requirements for automatic connection device and information services about charging and control status.

The purpose of this document is to detail the communication between an electric vehicle communication controller (EVCC) and a supply equipment communication controller (SECC). Aspects are specified to detect a vehicle in a communication network and enable an Internet Protocol (IP) based communication between the EVCC and the SECC (see Figure 1).



Key

1 scope of this document
2 message definition considers use cases defined for communication between SECC to SA

Figure 1 — Communication relationship among the EVCC, SECC and SA

This document defines messages, data model, XML/EXI-based data representation format, usage of V2GTP, TLS, TCP and IPv6. These requirements belong to the 3rd until the 7th OSI layer model. In addition, the document describes main service sequences of conductive charging, wireless power transfer and bidirectional power transfer, and how data link layer services can be accessed from an OSI layer 3 perspective.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 3780, *Road vehicles – World Manufacturer Indentifier (WMI) code*

ISO 4217, *Codes for the representation of currencies*

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

ISO 15118-2:2014, *Road vehicles — Vehicle to grid communication interface — Part 2: Network and application protocol requirements*

ISO 15118-3:2015, *Road Vehicles — Vehicle to grid communication interface — Part 3: Physical and data link layer requirements*

ISO 15118-8, *Road Vehicles — Vehicle to grid communication interface — Part 8: Physical and data link layer requirements for wireless communication*

ISO 19363:2020, *Electrically propelled vehicles—Magnetic field wireless power transfer—Safety and interoperability requirements*

ISO/IEC 11889-1:2015, *Information technology — Trusted platform module library — Part 1: Architecture*

IEC 61851-1:2017, *Electric vehicle conductive charging system — Part 1: General requirements*

IEC 61851-23-1:2014, *Electric vehicle conductive charging system - Part 23-1: DC Charging with an automatic connection system*

IEC 61980-2, *Electric vehicle wireless power transfer (WPT) systems - Part 2: Specific requirements for communication between electric road vehicle (EV) and infrastructure*

IEC 63119-2[1], *Information exchange for Electric Vehicle charging roaming service — Part 2: Use cases*

EN 50696:2021, *Contact interface for automated connection devices (ACD)*

IETF RFC 768, *User Datagram Protocol* (August 1980)

IETF RFC 793, *Transmission Control Protocol - DARPA Internet Program - Protocol Specification (September 1981)*

IETF RFC 2865, *Remote Authentication Dial In User Service (RADIUS)* (June 2000)

IETF RFC 2866, *RADIUS Accounting* (June 2000)

IETF RFC 3122, *Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification* (June 2001)

IETF RFC 3579, *RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)* (September 2003)

IETF RFC 3748, *Extensible Authentication Protocol (EAP)* (June 2004)

IETF RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax* (January 2005)

IETF RFC 4291, *IP Version 6 Addressing Architecture* (February 2006)

IETF RFC 4429, *Optimistic Duplicate Address Detection (DAD) for IPv6* (April 2006)

IETF RFC 4443, *Internet Control Message Protocol (ICMP v6) for the Internet Protocol version 6 (IPv6) specification* (March 2006)

[1] Under preparation. Stage at the time of publication: IEC/CCDV 63119-2:2022.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

IETF RFC 4514, *Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names* (June 2006)

IETF RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)* (September 2007)

IETF RFC 4862, *IPv6 Stateless Address Autoconfiguration* (September 2007)

IETF RFC 5116, *An Interface and Algorithms for Authenticated Encryption* (January 2008)

IETF RFC 5216, *The EAP-TLS Authentication Protocol* (March 2008)

IETF RFC 5234, *Augmented BNF for Syntax Specifications: ABNF* (January 2008)

IETF RFC 5480, *Elliptic Curve Cryptography Subject Public Key Information* (March 2009)

IETF RFC 5722, *Handling of Overlapping IPv6 Fragments* (December 2009)

IETF RFC 6066, *Transport Layer Security (TLS) Extensions: Extension Definitions* (January 2011)

IETF RFC 6724, *Default Address Selection for Internet Protocol version 6 (IPv6)* (September 2012)

IETF RFC 6818, *Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* (January 2013)

IETF RFC 6874, *Representing IPv6 Zone Identifiers in Address Literals and Uniform Resource Identifiers* (February 2013)

IETF RFC 6960, X.*509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP* (June 2013)

IETF RFC 7405, *Case-Sensitive String Support in ABNF* (December 2014)

IETF RFC 7748, *Elliptic Curves for Security* (January 2016)

IETF RFC 8032, *Edwards-Curve Digital Signature Algorithm (EdDSA)* (January 2017)

IETF RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification* (July 2017)

IETF RFC 8201, *Path MTU Discovery for IP version 6* (July 2017)

IETF RFC 8398, *Internationalized Email Addresses in X.509 Certificates* (May 2018)

IETF RFC 8399, *Internationalization Updates to RFC 5280* (May 2018)

IETF RFC 8415, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)* (November 2018)

IETF RFC 8439, *ChaCha20 and Poly1305 for IETF Protocols* (June 2018)

IETF RFC 8446, *The Transport Layer Security (TLS) Protocol Version 1.3* (August 2018)

IETF RFC 8504, *IPv6 Node Requirements* (January 2019)

IETF RFC 8335, *PROBE: A Utility for Probing Interfaces* (February 2018)

ANSI X9.62, *Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)* (2005)

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

W3C EXI 1.0, *Efficient XML Interchange (EXI) Format 1.0, W3C Recommendation* (March 2011)

IANA Service & Port Registry, *Service Name and Transport Protocol Port Number Registry [viewed 2011-01-16],* Available from: http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml

NIST FIPS PUB 180-4, *Secure Hash Standard (SHS)* (March 2012)

NIST FIPS PUB 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions* (August 2015)

ITU-T X.509, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks* (October 2019)

IEEE 802.1X-2020, *IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control (January, 2020)*

WPA3, *WPA3 Specification Version 3.0* (December 2020)

NIST Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC* (November 2007)

NIST Special Publication 800-56A, Revision 3, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography* (April 2018)

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
access point
AP
wireless communication device that allows the user to connect to other wireless or wired communication devices

3.2
authorization mode
authenticate and authorize the user account

Note 1 to entry: Authorization mode refers to *EIM* (3.17) and *PnC* (3.41).

3.3
automatic connection device pantograph
ACDP
components supporting the automatic connection and disconnection process for conductive energy transfer between an EV and EVSE via pantograph

3.4
basic charging

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

BC
charging based on PWM

Note 1 to entry: According to ISO/IEC 11889-1:2015, Annex A.

3.5
certificate
electronic document which uses a digital signature to bind a public key with an identity

Note 1 to entry: The ISO 15118 series describe several certificates covering different purposes [e.g. contract certificate including the *EMAID* (3.19) and *OEM* (3.36) provisioning certificates].

3.6
charging limit
set of physical constraints that is negotiated during a *service session* (3.50)

EXAMPLE Voltage, current, energy, power, etc.

3.7
charging session
collection of charging transactions at a charge point related only to the charging of an electric vehicle assigned to a specific customer in a specific timeframe with a unique identifier

Note 1 to entry: The charging session is a subset of the *service session* (3.50).

3.8
charging station operator
CSO
secondary actor responsible for the installation and operation of a charging infrastructure (including charging sites), and the management of electricity to provide the requested energy transfer services

Note 1 to entry: The term CSO for charge point operator is also used in other ISO 15118 documents. This term is not recommended for trademark reasons.

3.9
communication session
sequence of time where *EVCC* (3.21) and *SECC* (3.47) interactively exchange digital information in order to manage charging or discharging the EV battery

Note 1 to entry: A communication session can be paused and resumed later several times. The communication session encapsulates zero or more energy transfer periods.

3.10
communication setup timer
timer (3.61) monitoring the time between establishment of TLS connection and reception of SessionSetupRes by *EVCC* (3.21)

3.11
contract certificate
certificate (3.5) issued for the *EVCC* (3.21) by an *eMSP* (3.20) *sub-CA* (3.57), which is used in XML signatures on application layer so that the *SECC* (3.47) or secondary actor can verify the signature created by the EVCC with the contract certificate issued for that EV

Note1 to entry: The secondary actor uses the *EMAID* (3.19), which is part of the contract certificate's subject field, to authorize the EV for charging based on the eMSP's associated e-mobility contract.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

3.12
CP state
control pilot state
state according to control pilot function defined in IEC 61851-1

3.13
credential
piece of information attesting an entity's identity

3.14
cross certificate
certificate (3.5) containing the public key of an existing certificate of a CA in one organization (called cross-certified CA) but signed by a root CA of another organization (called cross-certifying CA)

Note 1 to entry: With cross-certification, an end-entity, who only trusts a cross-certifying root CA, can validate a certificate chain issued by the root CA of another organization through a cross certificate appended to the chain.

3.15
distinguished encoding rules
DER
method for encoding a data object, such as an ITU-T X.509 *certificate* (3.5), to be digitally signed or to have its signature verified

3.16
dynamic control mode
control mode for the communication

Note 1 to entry: Further Information can be found in ISO 15118-1.

Note 2 to entry: The *SECC* (3.47) controls the power flow and gives the *EVCC* (3.21) set points it should follow.

3.17
external identification means
EIM
authorization means that are handled outside of this document

3.18
elliptic curve cryptography
ECC
mechanism for implementing public-key cryptography based on the discrete logarithms by algebraic structure of elliptic curves

3.19
eMobility account identifier
EMAID
contract identification for the contract that is issued by the *eMSP* (3.20) and used by the *SECC* (3.47) or secondary actor to enable energy transfer and related services (including billing)

Note 1 to entry: The term contract ID is not used anymore in this document. It has been replaced by the term EMAID. The definition is still present for compatibility with ISO 15118-1.

3.20
eMobility service provider
eMSP
entity with which the customer has a contract for all services related to the EV energy transfer

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

Note 1 to entry: Typically, the eMSP will include some of the other actors, like spot operator or EP, and has a close relationship with the distribution system operator and *meter* (3.33) operator. An *OEM* (3.36) or utility could also fulfil such a role.

Note 2 to entry: eMSPs validate *EMAIDs* (3.19) from their customers, which were received either from the EMOCH, other eMSPs or spot operators the customer is in relation with.

Note 3 to entry: eMSPs issue EMAIDs to their customers.

3.21
electric vehicle communication controller
EVCC
embedded system, within the vehicle, that implements the communication between the vehicle and the *SECC* (3.47) in order to support specific functions

Note 1 to entry: Such specific functions could be, e.g. controlling input and output channels, encryption, or data transfer between vehicle and SECC.

3.22
EVPowerProfile
scheme which contains the power limits for charging or discharging the battery during an energy transfer period

Note 1 to entry: Refer to definition of "energy transfer schedule" in ISO 15118-1.

Note 2 to entry: In *dynamic control mode* (3.16) it describes a simulation from the EVs perspective on the fastest charging profile in order to reach the EVMaximumEnergyRequest under the constraint of the minimum of the EVSEMaximumChargePower and EVMaximumChargePower.

EXAMPLE The schedule is calculated based on target setting, sales tariff table and grid schedule information, respecting the corresponding current limitations, i.e. using the lowest current value.

3.23
electric vehicle supply equipment ID
EVSEID
unique identification of the EVSE

3.24
electric vehicle supply equipment
EVSE
<conductive power transfer> conductors, including the phase(s), neutral and protective earth conductors, the EV couplers, attached plugs, and all other accessories, devices, power outlets or apparatuses installed specifically for the purpose of delivering energy from the premises wiring to the EV and allowing communication between them as necessary

3.25
electric vehicle supply equipment
EVSE
<wireless power transfer> off-board equipment comprising the *SECC* (3.47) and one or multiple supply devices working under the control of the same SECC

3.26
global address
IP address (3.28) with unlimited scope

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

3.27
high level communication charging
HLC-C
energy transfer phase during a *service session* (3.50)

3.28
IP address
address
IP-layer identifier for an interface or a set of interfaces

3.29
link-local address
IP address (3.28) with link-only scope that can be used to reach neighboring interfaces attached to the same link

3.30
maximum transfer unit
MTU
maximum size (in bytes) of the largest protocol data unit that the data link layer can pass onwards

3.31
message set
set of *V2G messages* (3.66) and parameters for the *EVCC* (3.21) or *SECC* (3.47) covering one or multiple use case elements

3.32
message timer
timer (3.61) monitoring the exchange of a request-response-pair

3.33
meter
analogic device able to measure the amount of energy used and to monitor it

3.34
multiplexed communication
MC
exchange of multiple messages with different payload types over the *V2GTP* (3.68) connection between the *EVCC* (3.21) and *SECC* (3.47)

3.35
node
device that implements IPv6

3.36
original equipment manufacturer
OEM
producer who manufactures products or components that are purchased by a company and retailed under that purchasing company's brand name

Note 1 to entry: OEM refers to the company that originally manufactured the product.

Note 2 to entry: When referring to automotive parts, OEM designates a replacement part made by the manufacturer of the original part.

3.37

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

OEM provisioning certificate
certificate (3.5) issued to the *EVCC* (3.21) by the *OEM* (3.36) to enable the provisioning of a *contract certificate* (3.11)

Note 1 to entry: It is securely requested and received from a secondary actor to uniquely identify the EVCC.

3.38
PE certificate
leaf *certificate* (3.5) issued in *PE* (3.42) to a *private SECC* (3.43) by a PE private root CA or optionally by a PE sub CA, which is used in TLS so that the *EVCC* (3.21) can verify the authenticity of the private SECC

3.39
PE EVSE
EVSE that is operating in a *private environment* (3.42) and is containing or being controlled by a *private SECC* (3.43)

3.40
performance time
non-functional timing requirement defining the time a *V2G entity* (3.65) should not exceed when executing or processing certain functionality

Note 1 to entry: This is a fixed time value.

3.41
park and charge
PnC
authorization mechanism using *certificates* (3.5) stored in the EV which does not require any user interaction

3.42
private environment
PE
area of private responsibility with physical access limited to a small number of vehicles

3.43
private SECC
SECC (3.47) operating in a *private environment* (3.42) that uses a *PE certificate* (3.38)

Note 1 to entry: *PE* (3.42) usually implies lower security. In most cases SECC requirements will also apply to a private SECC. In some specific cases, the SECC and private SECC requirements can be distinct. Those cases and requirements will be called out as such.

3.44
public SECC
SECC (3.47) operating in a public environment that uses a *PE certificate* (3.38)

3.45
request-response message pair
request message and the corresponding response message

3.46
request-response message sequence
predefined sequence of *request-response message pairs* (3.45)

3.47

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

supply equipment communication controller
SECC
entity which implements the communication to one or multiple *EVCCs* (3.21) and which may be able to interact with secondary actors

Note 1 to entry: Functions of a supply equipment communication controller may control input and output channels, data encryption, or data transfer between vehicle and SECC.

3.48
SECC certificate
leaf *certificate* (3.5) issued to an *SECC* (3.47) by a *CSO* (3.8) sub-CA2, which is used in TLS so that the *EVCC* (3.21) can verify the authenticity of the SECC

3.49
sequence timer
timer (3.61) monitoring a *request-response message sequence* (3.46)

3.50
service session
collection of services around a charge point mainly related to the charging of an EV assigned to a specific customer in a specific timeframe with a unique identifier

Note 1 to entry: *Charging session* (3.7) and WPT session are some kinds of service sessions.

3.51
scheduled control mode
control mode for the communication

Note 1 to entry: Further Information can be found in ISO 15118-1.

Note 2 to entry: The *EVCC* (3.21) and *SECC* (3.47) negotiate a power profile for charging or discharging purposes.

3.52
schedule renegotiation
messaging for updating the agreement on the energy transfer schedule between the *EVCC* (3.21) and *SECC* (3.47) during a *V2G communication session* (3.64) by retransmitting the parameters schedule and *EVPowerProfile* (3.22)

3.53
station
STA
logical entity that is a singly addressable instance of a medium access control and physical layer interface to the wireless medium which does not act as an *access point* (3.1)

3.54
SDP client
V2G entity (3.65) that uses the *SDP server* (3.55) to get configuration information about the *SECC* (3.47) to be able to access the SECC

3.55
SDP server
V2G entity (3.65) providing configuration information for accessing the *SECC* (3.47)

3.56
smart meter
device that is able to measure and monitor the energy used or generated

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

Note 1 to entry: In this case during EV *charging session* (3.7).

Note 2 to entry: The values for active/reactive energy, active/reactive power, current, power factor, based on timing slot can be recorded. The values are monitored remotely, so they can be programmed to manage the power (for example, reducing or modulating it). Furthermore, the values can share the information with DSO and other devices based on PLC communication.

3.57
sub-CA
subordinate certificate authority which issues, e.g. *SECC certificates* (3.48) and/or *contract certificates* (3.11) on behalf of a root CA such as *V2G root CA* (3.70) or e-mobility service provider root CA (the latter only for contract certificates)

Note 1 to entry: The ability of issuing the certificates are delegated from a root CA and a root CA can revoke the sub-CA at any time.

3.58
sub-CA certificate
certificate (3.5) issued to *sub-CA* (3.57)

3.59
TCP_DATA
socket interface for data transfer based on TCP connection

3.60
timeout
timing requirement defining the time a *V2G entity* (3.65) monitors the communication system for a certain event to occur

Note 1 to entry: If the specified time is exceeded, the respective *V2G entity* (3.65) initiates the related error handling. This is a fixed-time value.

3.61
timer
device or piece of software used in an implementation for measuring time

Note 1 to entry: Depending on the specific use case a timer is used to trigger certain system events.

3.62
vehicle certificate
leaf *certificate* (3.5) issued to an *EVCC* (3.21) by an *OEM* (3.36) or *V2G* (3.63), which is used in TLS so that the *SECC* (3.47) can verify the authenticity of the EVCC

Note 1 to entry: This certificate is also used for binding between different TLS sessions that belong to the same V2G session by SECC.

3.63
vehicle to grid
V2G
plug-in electric vehicle interaction with the electric grid, including charging as well as discharging and bi-directional communication interface

Note 1 to entry: The first part of this definition is excerpted from the scope of the V2G domain expert working group, SGIP, NIST.

3.64

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

V2G communication session
association of two specific V2G entities for exchanging *V2G messages* (3.66)

3.65
V2G entity
primary actor participating in the V2G communication

Note 1 to entry: Primary actors can be the *EVCC* (3.21) or *SECC* (3.47).

3.66
V2G message
message exchanged on application layer

Note 1 to entry: Refer to Clause 8.

3.67
V2G setup
setup phase for V2G messaging

3.68
V2G transfer protocol
V2GTP
communication protocol to transfer *V2G messages* (3.66) between two V2GTP entities

3.69
V2GTP entity
V2G entity (3.65) supporting the *V2G transfer protocol* (3.68)

3.70
V2G root CA
certificate authority (CA) which issues *sub-CA* (3.57) certificates to sub-CAs

Note 1 to entry: Those sub-CAs are then delegated to issue either certificates to a second sub-CA (sub-CA2) or to directly issue leaf certificates, such as *contract certificate* (3.11) or *SECC certificates* (3.48).

3.71
V2G root CA certificate
certificate issued to *V2G root CA* (3.70)

4 Abbreviated terms

The abbreviations given in ISO 15118-1 and the following apply.

AC	alternating current
ACDP	automatic connection device pantograph
CPDA	DC_ChargeParameterDiscovery
AKI	authority key identifier
AP	access point
APOS	ACDP_VehiclePositioning
ASUP	AuthorizationSetup

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

AUTH	authorization
BEV	battery electric vehicle
BPT	bidirectional power transfer
CA	certificate authority
CC	CableCheck
CINS	CertificateInstallation
CONA	ACDP_Connect
CPM4PE	certificate provisioning mode for private environment
CPS	certificate provisioning service
CRL	certificate revocation list
CSO	charging station operator
DC	direct current
DCCL	DC_ChargeLoop
DH	Diffie Hellman
DER	distinguished encoding rules
DISA	DisconnetACDP
EAP	extensible authentication protocol
ECDSA	elliptic curve digital signature algorithm
EdDSA	Edwards-curve digital signature algorithm
EMA	e-mobility account
EMAID	e-mobility account identifier
EMOCH	e-mobility operator clearing house
eMSP	eMobility service provider
ESDW	emergency shut down
EV	electric vehicle
EVCC	electric vehicle communication controller
EVRESS	electric vehicle rechargeable energy storage system
EVSE	electric vehicle supply equipment

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

EVSEID	electric vehicle supply equipment identification
EXI	efficient XML interchange
HLC-C	high level communication charging
IV	initialization vector
MCON	MeteringConfirmation
NACK	negative acknowledgement
OCSP	online certificate status protocol
OEM	original equipment manufacturer
OID	object identifier
PC	PreCharge
PD(Start)	PowerDelivery(Start)
PD(Stop)	PowerDelivery(Stop)
PDU	protocol data unit
PE	private environment
PHEV	plug-in hybrid electric vehicle
PKI	public key infrastructure
PLC	power line communication
PMF	protected management frames
PnC	park and charge
PPD	pairing and positioning device
RFC	request for comments(IETF)
SA	secondary actor
SAID	secondary actor ID
SAP	SupportedAppProtocol
SDE	ServiceDetails
SDI	ServiceDiscovery
SDP	SECC discovery protocol
SDU	service data unit

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

SE	ScheduleExchange
SECC	supply equipment communication controller
SKI	subject key identifier
SOC	state of charge
SSEL	ServiceSelection
SSU	SessionSetup
SSP	SessionStop
SYSS	ACDP_SystemStatus
TCP	transmission control protocol
UDP	user datagram protocol
VAS	value added service
V2G	vehicle to grid

NOTE V2G as is used in this document only means the communication between EVCC and SECC.

V2G CI	vehicle-to-grid communication interface
V2GTP	V2G transfer protocol
WMI	world manufacturer identifier
WPT	wireless power transfer
XML	extensible markup language

5 Conventions

5.1 Definition of OSI based services

This document is based on the conventions defined in the OSI service conventions (refer to ISO/IEC 10731) as they apply for the individual layers specified in this document.

This document describes requirements applicable to layer 3 – 7 according to the OSI layered architecture.

5.2 Requirement structure

This document uses the requirement structure defined here. A unique number identifies each individual requirement defined in this document. Systematic and ordered requirement structure enables readers to find the target requirement number easily.

The following format is applied for new defined and updated requirements:

[V2G20-xxxx] requirement text, where:

– "V2G20" represents this document;

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

- "xxxx" represents the unique requirement number consisting of four digits starting from 1 000;
- "requirement text" defines the actual text of the requirement.

EXAMPLE **[V2G20-1000]** This is an example requirement introduced in this document.

The format below is applied to the handed over requirements from ISO 15118-2:

[V2G20-yyy] requirement text, where:

- "V2G20" represents this document;
- "yyy" represents the unique requirement number same as already defined in ISO 15118-2;
- "requirement text" is the same text as defined in first edition.

EXAMPLE **[V2G20-000]** This is an example requirement originally defined in ISO 15118-2.

5.3 Usage of references

[V2G20-1230] All published updates and error corrections (errata) shall be applied to the referred documents.

NOTE This does not include updated RFC or other requirement numbers not referenced in Clause 2 or Bibliography. This additionally does not include requirements published after publication of this document.

EXAMPLE If an errata to IETF RFC 8446 for TLS 1.3 is published 2 months after publication of this document and simply provides correction to an existing spec without which TLS 1.3 could not be implemented, that errata can be considered during implementation of this document. But if an IETF RFC is published 2 months after publication of this document and updates TLS 1.3 to TLS 1.4 due to some major issues in the protocol, this IETF RFC cannot be considered for implementation of this document as it can result in unforeseen issues.

5.4 Notation used for XML schema diagrams

This document makes use of XML as a description format for V2G messages. For details with regards to the XML schema diagram notation used in this document refer to Reference [96].

Allowing for an easy way to distinguish the types used for the XML schema definitions in this document, the following naming conventions apply:

- complex type use capitalized first letters,
- simple types use non capitalized first letters.

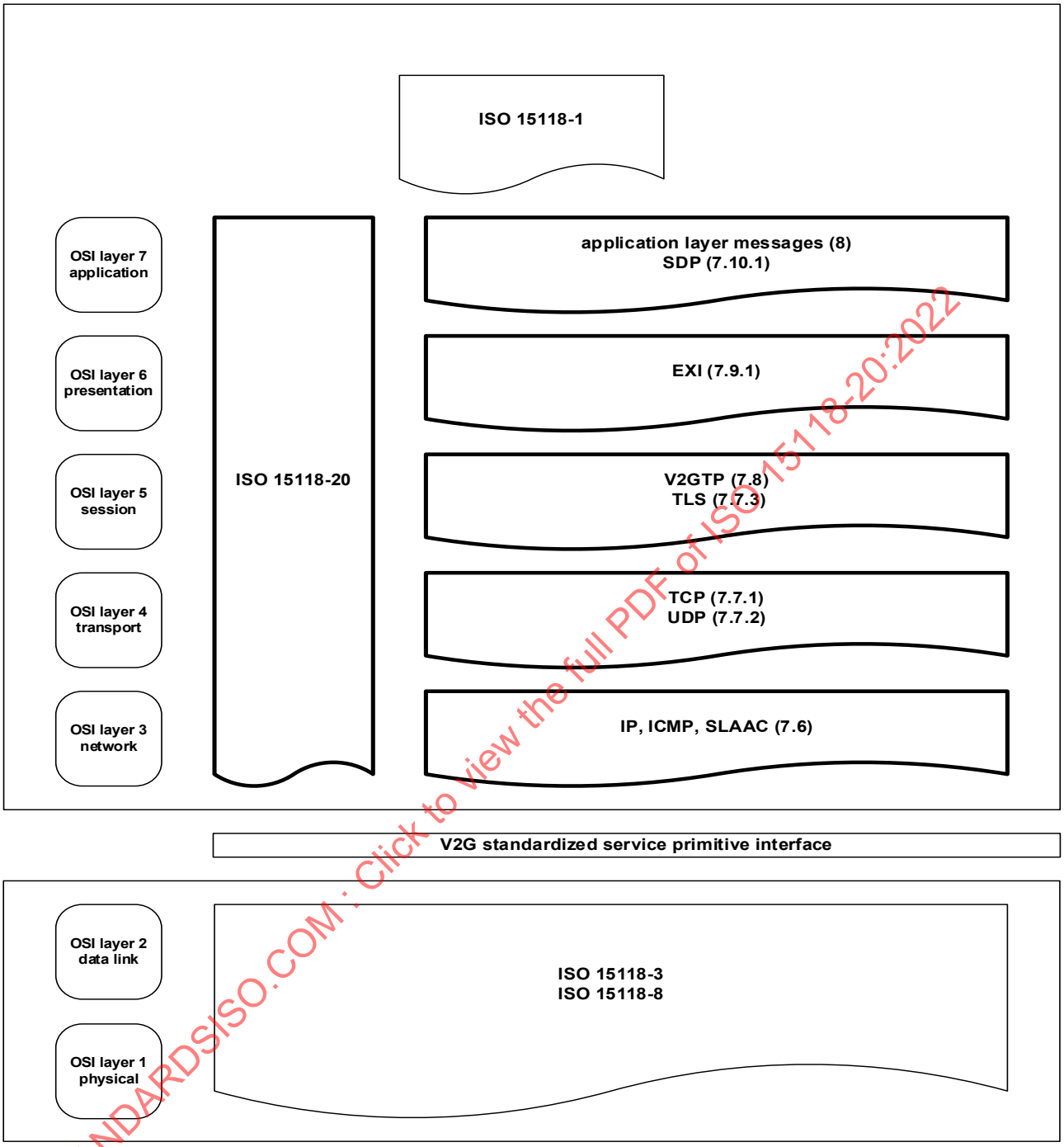
6 Document overview

Figure 2 describes the organization of the different documents in the ISO 15118 series and the usage of the subclauses, according to the OSI layered architecture.

As indicated by the bold framed shapes, this document defines requirements applicable to layers 3 – 7 according to the OSI layered architecture. Layer 1 and layer 2 requirements including the V2G standardized service primitive interface are specified in ISO 15118-3 and ISO 15118-8.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Figure 2 — Vehicle to grid communication document overview

7 Basic requirements for V2G communication

7.1 General information

This document describes the realization of the V2G use case elements defined in ISO 15118-1.

© ISO 2022 – All rights reserved

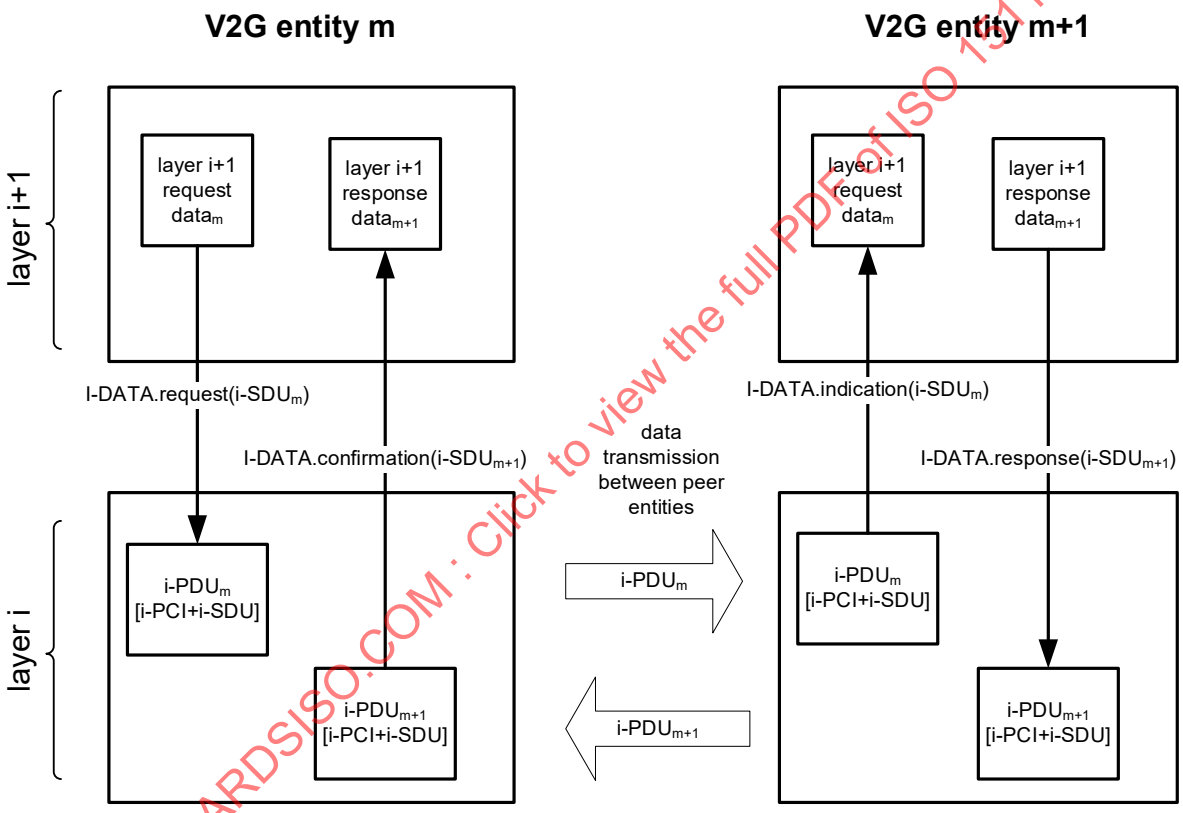
7.2 Service primitive concept of OSI layered architecture

7.2.1 Overview

This subclause explains how the OSI layered architecture is applied for the purpose of this document. It is intended to provide simple means for describing the interfaces between the individual communication protocol layers required by this document and furthermore allows for defining timing requirements more precisely.

Services are specified by describing the service primitives and parameters that characterize a service. This is an abstract definition of services and does not force a particular implementation.

Figure 3 depicts a simplified view of OSI layer interaction sufficient to understand the OSI layered architecture principles for the context of this document.



Key

PDUx: protocol data unit of network entity x
PCI: protocol control information
SDUx: service data unit of network entity x

Figure 3 — OSI layered architecture principles

When a layer i+1 instance of V2G entity m exchanges data with a layer i+1 instance of V2G entity m+1 each instance uses services of an instance of layer i. A service is defined as a set of service primitives.

7.2.2 Syntax of service primitives

Service primitives are described with the following syntax:

– [Initial of layer]-[NAME].[primitive type](parameter list);

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

a) whereas [initial of layer] is one out of the following seven:

   – physical, data link, network, transport, session, presentation, application;

b) whereas [NAME] is the name of the primitive;

EXAMPLE Typical examples for [Name] are CONNECT, DISCONNECT, DATA; other names are used in this document and ISO 15118-3.

c) whereas [primitive type] is one out of the following four:

   – request, indication, response, confirmation;

d) whereas (parameter list) includes a list of parameters separated by comma the user of the service is supposed to provide when using the respective service primitive; optional parameters are marked with brackets "[..]".

NOTE In this document, the primitive type ".indication" always indicates an event asynchronously to the upper layer.

7.3 Security concept

7.3.1 General

This subclauses provide specific and separate requirements for the private SECC and the SECC. Thus, unless otherwise specified, private SECC and SECC are not considered interchangeable.

In ISO 15118-2, transport layer security (TLS) was only required for PnC or VAS. In this document, TLS is always mandatory. For backward compatibility, connection setup processes will accept both ISO 15118-2 handling and the handling defined in this document. This means the connection setup processes will not change.

If an application still requires optional TLS, ISO 15118-2 shall be used. Refer to 7.7.3.10 for further details.

Figure 4 depicts the principal approach for various cases from a security point of view, showing the necessary security services applied as well as an abstract view on the different data flows necessary for the operation.

The data flow/sequence diagrams can be found in 8.6.6. In Figure 4, only the security relevant information is highlighted.

The security concept provides a basic transport based protection mechanism. For all scenarios described in this document, the usage of TLS for the transport communication between the EVCC and SECC is mandatory. In case data should be protected to or from a secondary actor or if the protection should last longer than the existence of the TLS channel, specific messages could be protected on application layer (XML-based signatures).

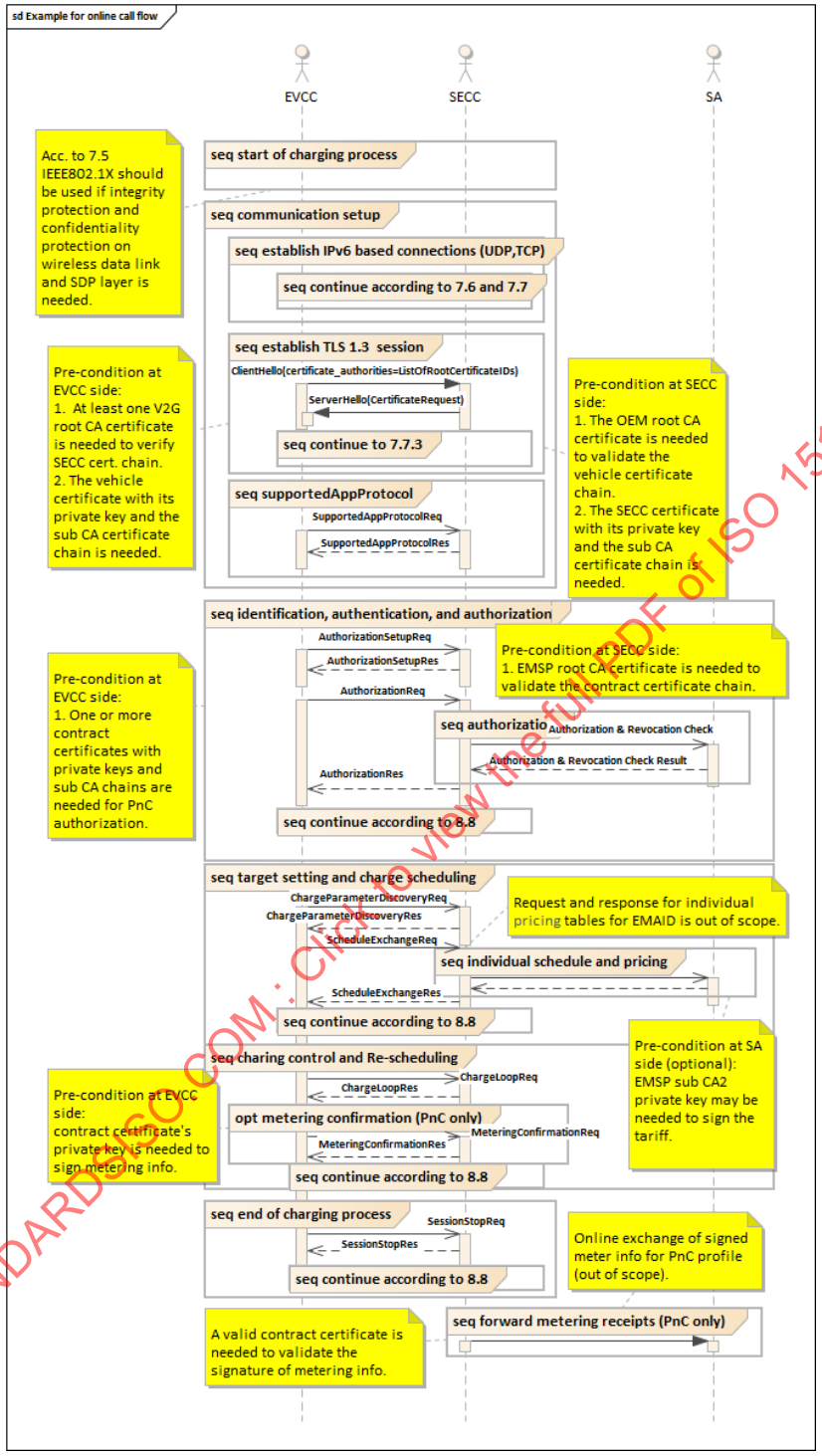
Figure 4 shows an example sequence for a PnC scenario. As described in Figure 4, all TCP/IP based communication is protected using a mutually authenticated TLS channel between the two peers.

Some of the information provided by the EVCC may need to be sent to the SA for further processing. The EVCC calculates a power profile (refer to 8.3.4.3.8.2) and sends it to the SECC. The SECC may send it to SA systems like energy management system or demand clearing house. Further process is similar to the semi-online case with the exception that the final charging data can be directly submitted to the SA. It is assumed that the SECC will also use a secure transport connection to the SA.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE The communication between SECC and SA in Figure 4 is shown for informational purpose only and not intended to specify a particular message sequence.



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Figure 4 — Example for call flows

There are further use cases where security mechanisms are needed on application layer. These are the initial enrollment/installation of contract certificates and keys as well as the update of the contract certificates and keys. In this case vehicle specific OEM keys are used. Those mechanisms are described in 7.9.2.5. An overview on all needed certificates can be found in Annex B.

© ISO 2022 – All rights reserved

While storing any data related to certificates/messages provided by the EVCC, the EVSE and the SAs (including CSO/eMSP/OEM/etc.) should be cognizant of the local/state/national/international privacy rules, regulations and requirements. These rules/regulations/requirements are not in the scope of this document but should be taken into account when designing and implementing the solution.

7.3.2 Certificate and key management

The call flows shown in 7.3.1 require the existence of multiple certificates to be applied for the different security layers. There are SECC certificates used in the TLS layer for the EVCC to authenticate SECC. There are contract certificates used at the application layer to authenticate against an SECC and/or SA. There are V2G root CA certificates and possibly sub-CA certificates which certify SECC certificates and contract certificates.

Separate from above certificates, there are OEM root CA certificates and vehicle certificates used in the TLS layer for the SECC to authenticate the EVCC. OEM provisioning certificates that stem from OEM root CA certificates may be used for installing and updating contract certificates.

Requirements for various certificates can be found in 7.3.2.1. For an overview of all possible certificate profiles, see Annex B. For examples of the certificate structures, see Annex H.

[V2G20-1231] Each V2G entity shall use X.509v3 certificates.

Table 1 shows what fields an X.509v3-certificate consists of:

Table 1 — Basic certificate fields

Certificate field	Description
Version	Version of certificate (for 15118 it shall be v3 = 0x2)
Serial number	Unique number of certificate (within the domain of the issuer)
Signature algorithm	Used signature algorithm
Issuer	Entity, who has issued and signed the certificate
Validity period	Time period, in which the certificate is valid
Subject	Entity, to which the certificate is issued
Public key	Public key corresponding to a private key
Issuer UID	Optional issuer unique identifier
Subject UID	Optional subject unique identifier
Extensions	Additional attributes associated with entities or public keys or used to manage relationships between CAs
Signature	Signature of the certificate generated by the issuer

NOTE 1 For those not familiar with the various fields, refer to IETF RFC 5280 and ITU-T X.509.

NOTE 2 IETF RFC 5280 has been updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399. These updates are considered to be included in this document.

Depending on the use case, additional information may be included using so called certificate extensions. Table 2 summarizes common certificate extensions.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 2 — Certificate extension examples

Certificate extensions	Description
Key usage	Usage of the corresponding private key (e.g. Digital Signature, non-repudiation, key encipherment, ...)
Extended Key Usage	Further specification of key usage using OIDs, e.g.: – server authentication (1.3.6.1.5.5.7.3.1); – client authentication (1.3.6.1.5.5.7.3.2). NOTE Sometimes the following values are encoded here: – Microsoft SGC (1.3.6.1.4.1.311.10.3.3) – Netscape SGC (2.16.840.1.113730.4.1) SGC stands for server gated crypto and indicates that the server can also use strong cryptography for the connection with the client's browser. This extension was used at the time of strong crypto export control to enable financial web site to provide appropriate protection of the data transfer.
CRL distribution point	Location to retrieve certificate revocation lists
OCSP	Location to retrieve OCSP. Refer to IETF RFC 6960 as updated by IETF RFC 8954 for details.
Authority information	Additional authorization information
Subject alternative name	Alternative names of the entity
Basic constraint = CA	True if the certificate is a root certificate or a sub-CA certificate.
subjectAltPublicKeyInfo	Alternative/secondary certificate key data. This contains the alternative key algorithm and the alternative key generated using the said algorithm. Refer to ITU-T X.509 for further details.

NOTE 3 For those not familiar with OIDs, e.g. 1.3.6.1.5.5.7.3.1, refer to the Object Identifier (OID) Repository.

[V2G20-2673] Each V2G entity shall support Hash-operation SHA-512 (signature process) according to NIST FIPS PUB 180-4 (for ISO 15118-1, use case element ID: F1).

[V2G20-2318] Each V2G entity shall support SHAKE256 according to NIST FIPS PUB 202 (for ISO 15118-1, use case element ID: F1).

[V2G20-2674] Each V2G entity shall support signature operations using ECC based elliptic curve (secp521r1[SECG notation]) with signature algorithm ECDSA (for ISO 15118-1, use case element ID: F1).

[V2G20-2319] Each V2G entity shall additionally support signature operations with ECC algorithm Ed448 (for ISO 15118-1, use case element ID: F1), i.e. signature algorithm EdDSA using elliptic curve Curve448 (or Curve448-Goldilocks) in Edwards form, see IETF RFC 7748 and IETF RFC 8032.

NOTE 4 In case V2G entity chooses to use Curve448-based signature algorithm, it also uses ECC-based DH algorithm X448 defined for this curve (see IETF RFC 7405), in addition to the algorithms specified by NIST Special Publication 800-56A. See also [V2G20-2710] and [V2G20-2711].

[V2G20-2320] Multiple algorithms are integrated to allow for cryptographic agility. Each V2G entity shall implement a secure configurable mechanism to securely switch usage of (elliptic curve) EC from that defined in [V2G20-2674] to the one defined by [V2G20-2319] and prevent the usage of a particular algorithm, e.g. in case a security flaw was found in the preferred ECC algorithm.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 5 The design and implementation of this configuration mechanism is not in the scope of this document.

NOTE 6 secp521r1 is a very common ECC algorithm supported by NIST. Curve Ed448 is not as widely used at the time of the publication of this document. Although there are quite a few implementations supporting curve Ed448, secp521r1 is used as the main curve due to its ubiquity. In case flaw(s) are found in the secp521r1, availability of the alternative curves allows implementers to quickly switch to a parallel algorithm without the need for implementation and validation of a new cryptographic algorithm. This ensures that the implementers/operators can quickly respond to any reported vulnerabilities in secp521r1.

[V2G20-2321] As long as no issues or flaws are identified in the (elliptic curve) EC as specified by [V2G20-2674], the (elliptic curve) EC as specified by [V2G20-2674] shall be considered the preferred ECC algorithm. The mechanism defined by [V2G20-2320] shall only be updated to usage of (elliptic curve) EC as defined by [V2G20-2319] when there are issues/flaws identified with the (elliptic curve) EC as specified by [V2G20-2674].

NOTE 7 By default the mechanism defined by [V2G20-2320] can be set to use (elliptic curve) EC as specified by [V2G20-2674].

[V2G20-2675] Each V2G entity shall support a key length of 521 bits for ECC based asymmetric cryptography.

NOTE 8 Additionally, key length of 448 bits is used with certain curves in the application of this document. If a V2G entity can manage and utilize 521 bit keys, it can be capable of managing and utilizing 448 bit keys as well.

[V2G20-2322] Each certificate shall meet all requirements as specified for that certificate in this subclause (and any of its subclauses), 7.3.3 (and any of its subclauses) and in Annex B.

NOTE 9 Annex B provides the certificate profiles.

[V2G20-926] The certificate extensions mentioned in Annex B shall be supported.

NOTE 10 Where necessary, deviations have been specified.

[V2G20-2323] Certificates used in this document shall not contain any extensions other than those specified in Annex B.

NOTE 11 If an extension is mentioned as allowed for a certificate profile in Annex B, regardless whether it is marked as mandatory or optional, a certificate generated to meet that certificate profile is permitted to utilize that extension. If the extension is not mentioned as allowed in the corresponding certificate profile, that extension cannot be present in the corresponding certificate. For example, "CertificatePolicies" extension is marked as optional in most profiles. That means whether the "CertificatePolicies" extension is included is up to the certificate issuer's and certificate requester's discretion. On the other hand, since the "subjectDirectoryAttributes" extension is not specified as a mandatory or optional extension by Annex B, the "subjectDirectoryAttributes" extension cannot be included in any certificate used in this document.

NOTE 12 This ensures that incompatible extensions do not result in unforeseen issues or result in interoperability concerns.

[V2G20-1234] Each certificate in a certificate chain shall be DER encoded and the size of each certificate in DER encoded form shall be limited to a maximum of 1 600 bytes. Refer to ITU-T X.509 for details of DER encoding.

NOTE 13 A certificate chain is made up of multiple certificates. [V2G20-1234] applies to each certificate in the certificate chain, not the entire certificate chain itself. If a certificate chain is made up of four certificates, that chain will be a maximum of 6 400 bytes in DER format.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 14 As mentioned in Annex B, there are many mandatory and optional parameters in a certificate. Some parameters have well defined fixed lengths while others are variable length parameters. The certificate issuer can experiment with different optional parameters, different parameter data for variable length parameters, etc. to stay within the bounds of [V2G20-1234]. For example, if the OCSP responder address is too long, the certificate issuer can use methodologies to shorten the address to keep the certificate length within the bounds of [V2G20-1234].

[V2G20-1004] Certificates shall be issued and signed by the CA within the validity of its own certificate.

[V2G20-911] If only one sub-CA layer is used, i.e. a sub-CA signed by a root CA directly signs leaf certificates, the profile of sub-CA2 shall apply for that sub-CA.

[V2G20-1003] All certificate chains (except where a cross certificate is used) shall have a maximum length of 3.

NOTE 15 The certificate chain includes the leaf certificate. The certificate chain does not include the root certificate.

NOTE 16 This means, at most two sub-CA levels can be used.

[V2G20-1005] All certificate chains, including a cross certificate, shall have a maximum length of 4.

NOTE 17 The certificate chain includes the leaf certificate and the cross certificate. The certificate chain does not include the root certificate.

NOTE 18 A cross certificate adds one more level.

[V2G20-1002] When cross-certification is used, the certificate chain sent shall include the cross-certificate.

NOTE 19 The profile of a cross certificate differs from that of other CA certificates by the validity period and the use of Subject Information Access extension. See Annex B for further details.

[V2G20-1853] A cross-certificate shall not be valid beyond the validity period of the cross-certified CA's certificate and cross-certifying CA's certificate.

[V2G20-1001] All certificate validations shall be carried out in conformance with IETF RFC 5280 and ITU-T X.509. During certificate validation, each certificate shall be checked for conformance with the appropriate profile in Annex B. All requirements from Annex B shall be met for the appropriate certificate profile. The EVCC and the SECC shall cache certificate validation results during one service session.

NOTE 20 The certificate validation includes checking the following.

a) The content of a leaf certificate has not been altered after issue. This means it is possible to check and confirm the signature up to the trust anchor level and thus the integrity of the signed content.
b) The signature up to the trust anchor level is not compromised (none of the certificates have been revoked). Certificate revocation is checked via the OCSP response (or CRL, if allowed for that particular certificate) as detailed in 7.7.3.1 and 7.7.3.3.
c) The validity period of each certificate in the chain up to the trust anchor has not yet elapsed.
d) Each certificate in the certificate chain matches the appropriate certificate profile as defined in Annex B. This includes checking the following:
   – the key length of each certificate in the certificate chain matches the key length specified by that certificate's profile in Annex B;
   – every critical KeyUsage attribute is set to the appropriate value (i.e. 0 or 1) as defined for that certificate's profile in Annex B;

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

- every mandatory parameter, as defined for that certificate's profile in Annex B, exists;
- all BasicConstraints attributes are set as defined for that certificate's profile in Annex B;
- DomainComponent value matches the definition of that certificate's profile in Annex B;
- the subjectID of the leaf certificate is acceptable [e.g. if the CN (common name) of the certificate is accepted by the V2G entity];
- the subjectID of the leaf certificate is acceptable [e.g. if the CN (common name) of the certificate is accepted by the V2G entity].

e) All critical parameters are processed.
f) All non-critical parameters that are recognized by the relying party are processed.

NOTE 21 A V2G entity can use the services of a secondary actor to carry out one or more of these validation steps. For example, the SECC can use the service of a secondary actor to receive revocation information for each certificate in the certificate chain the EVCC provided.

NOTE 22 IETF RFC 5280 has been updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399. These updates are considered to be included in this document.

[V2G20-2324] When the configurable mechanism as defined by [V2G20-2320] indicates that the curve as defined by [V2G20-2319] needs to be used, certificates and certificate profiles as defined in Table B.4, Table B.6, Table B.8, Table B.10, Table B.12, Table B.14, Table B.16 and Table B.18 for that particular certificate type shall be used during certificate validation (as defined by [V2G20-1001]).

[V2G20-2325] When the configurable mechanism as defined by [V2G20-2320] indicates that the curve as defined by [V2G20-2674] needs to be used, certificates and certificate profiles as defined in Table B.3, Table B.5, Table B.7, Table B.9, Table B.11, Table B.13, Table B.15 and Table B.17 for that particular certificate type shall be used during certificate validation (as defined by [V2G20-1001]).

7.3.2.1 Certificate structure

This document does not provide any mandatory PKI for implementations. It, however, defines a minimum required certificate structure that shoud be followed ensuring that the system as a whole is functioning. The details of the PKI, though, are left to the industry and implementers to define. For examples of the possible certificate structures/PKI, see H.1.6.

[V2G20-2581] When using the curve as defined by [V2G20-2674], each certificate used in this document shall comply to the appropriate profile as specified in Annex B, Table B.3, Table B.5, Table B.7, Table B.9, Table B.11, Table B.13, Table B.15 and Table B.17. When using the curve as defined by [V2G20-2319], each certificate used in this document shall comply to the appropriate profile as specified in Annex B, Table B.4Table B.6, Table B.8, Table B.10, Table B.12, Table B.14, Table B.16 and Table B.18.

NOTE 1 Although Annex B defines certificate profiles with the two different curves, as defined by [V2G20-2674] and [V2G20-2319], it is not mandatory for a V2G entity to have certificates with both curves available at the same time. It is up to the V2G entity's discretion whether to store certificate chains with both curves at the same time or just the ones as required to be used per the configurable mechanism as defined by [V2G20-2320]. If the V2G entity chooses to store certificate chains based on just one curve, the V2G entity will need a capability to replace those certificate chains with different ones when the configurable mechanism as defined by [V2G20-2320] is updated to use the secondary curve.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2326] An SECC certificate shall be generated using a certificate chain that uses a V2G root CA certificate as the trust anchor. Refer to Figure 5 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of a certificate structure. Refer to Annex B for details of the certificate profile.

NOTE 2 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the CSO's discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use as the trust anchor for the SECC certificate in their SECCs.

[V2G20-2327] An OCSP signer certificate used to sign the OCSP response for SECC certificate status shall be generated using a certificate chain that uses a V2G root CA certificate as the trust anchor. Refer to Figure 5 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of a certificate structure. Refer to Annex B for details of the certificate profile.

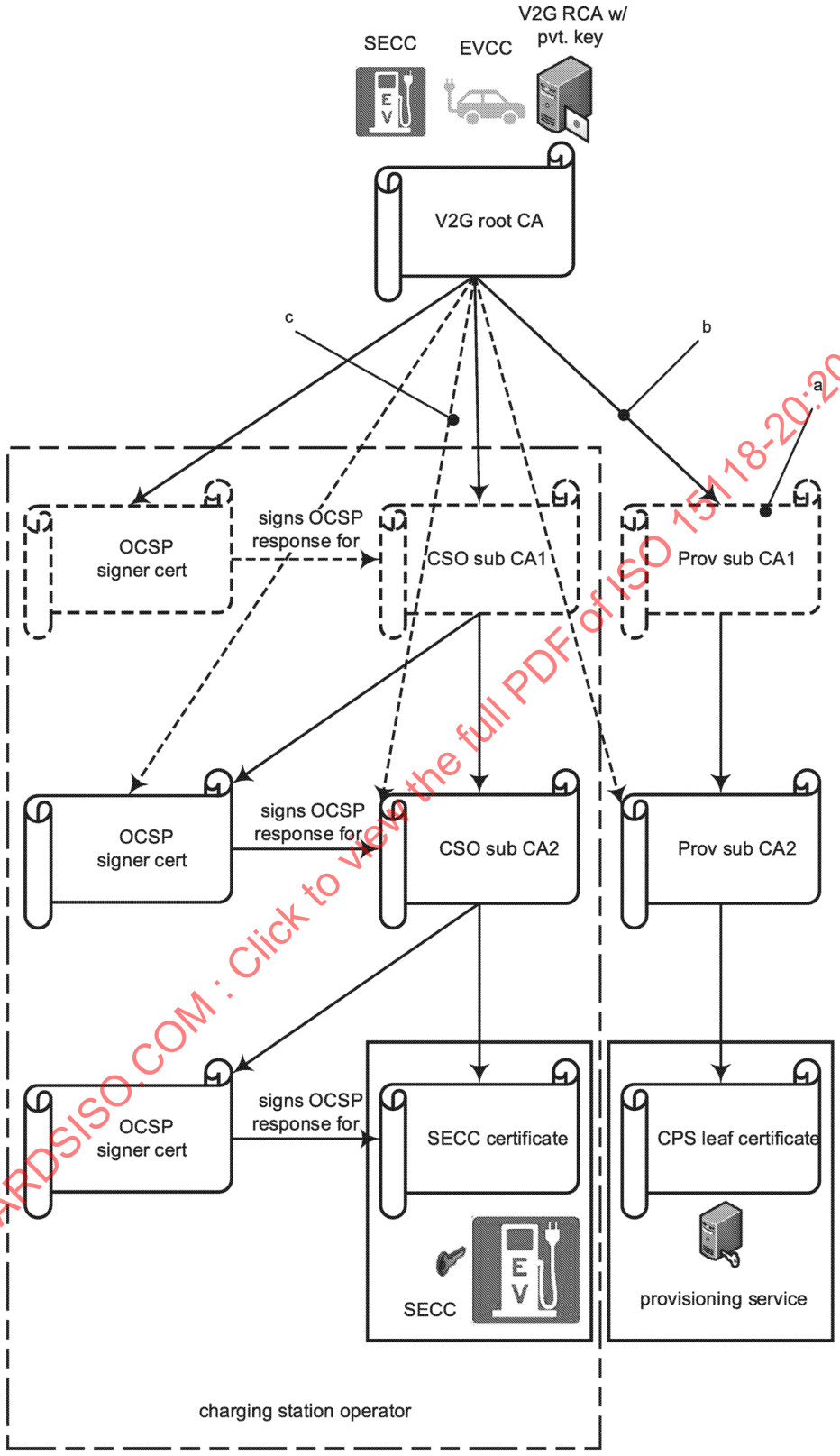
NOTE 3 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the CSO's discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use as the trust anchor for the OCSP signer certificate that signs the OCSP response for their SECC certificates.

[V2G20-2328] A CPS leaf certificate shall be generated using a certificate chain that uses a V2G root CA certificate as the trust anchor. Refer to Figure 5 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of a certificate structure. Refer to Annex B for details of the certificate profile.

NOTE 4 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the CPS' discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use as the trust anchor for their CPS leaf certificate.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Key

a Optional certificate – If the sub-CA1 is not present, the sub-CA2 is signed by the V2G root CA.

b Direct certification – The use of sub-CA1 is optional.

c Optional direct certification – If the sub-CA1 is present, it signs the sub-CA2 certificates.

Figure 5 — Mandatory certificate structure originating from V2G root CA certificate

© ISO 2022 – All rights reserved

[V2G20-2329] A contract certificate shall be generated using a certificate chain that uses either an eMSP root CA certificate or a V2G root CA certificate as the trust anchor. Refer to Figure 6 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of a certificate structure. Refer to Annex B for details of the certificate profile.

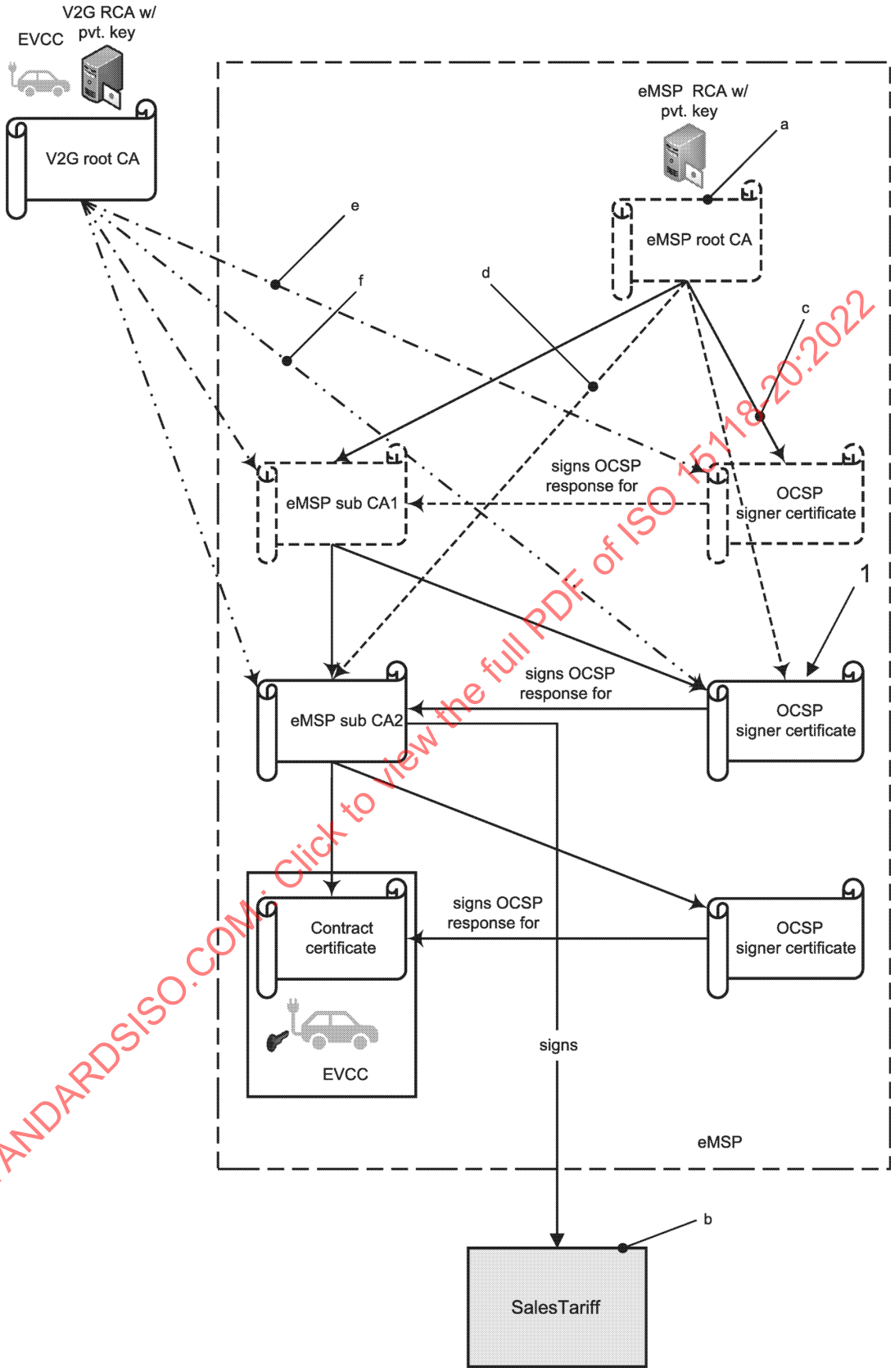
NOTE 5 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the eMSP's discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use (if any) as the trust anchor for their contract certificates.

[V2G20-2330] The OCSP signer certificate used to sign the OCSP response for contract certificate status shall be generated using a certificate chain that uses either an eMSP root CA certificate or a V2G root CA certificate as the trust anchor. Refer to Figure 6 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of a certificate structure. Refer to Annex B for details of the certificate profile.

NOTE 6 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the eMSP's discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use (if any) as the trust anchor for the OCSP signer certificate that signs the OCSP response for their contract certificates.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Key

1 certificate

[a] Optional certificate — If the sub-CA1 is not present, the sub-CA2 is signed by the V2G root CA.

© ISO 2022 – All rights reserved

[b] SalesTariff is not a certificate. The black arrow does not depict a certificate signing or certificate derivation/origination. SalesTariff is data that is signed by the eMSP using the private key of the eMSP sub-CA2. Since, in a PnC use case, the EVCC always contains the eMSP sub-CA2 as part of its contract certificate chain, the EVCC always has the associated public key for eMSP sub-CA2 that it can use to verify the signatures on SalesTariff.

[c] Direct certification — The use of sub-CA1 is optional.

[d] Optional direct certification — If the sub-CA1 is present, it signs the sub-CA2 certificates.

[e] Upon eMSP's discretion the contract certificate chain may originate from V2G root CA certificate. This type of arrow shows when the sub-CA1 is signed by the V2G root CA.

[f] Upon eMSP's discretion the contract certificate chain may originate from V2G root CA certificate. This type of arrow shows when the sub-CA1 is not used and sub-CA2 is signed by the V2G root CA.

Figure 6 — Contract certificate structure

[V2G20-2331] A vehicle certificate shall be generated using a certificate chain that uses either an OEM root CA certificate or a V2G root CA certificate as the trust anchor. Refer to Figure 7 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of certificate structure. Refer to Annex B for details of the certificate profile.

NOTE 7 In case the vehicle certificate is generated using a certificate chain that uses an OEM root CA certificate as the trust anchor, the issuer can consider to cross-sign the vehicle certificate chain (one of the sub-CAs in the vehicle certificate chain or the OEM root CA) by a V2G root CA certificate. This will improve availability of communications as specified in this document and allow the EV to utilize communications as specified in this document on any EVSE that supports the said V2G root CA regardless if the EVSE trusts the specific OEM root CA (i.e. has access to the specific OEM root CA certificate) or not.

NOTE 8 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the OEM's discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use (if any) as the trust anchor for their vehicle certificates.

[V2G20-2332] The OCSP signer certificate used to sign the OCSP response for vehicle certificate status shall be generated using a certificate chain that uses either an OEM root CA certificate or a V2G root CA certificate as the trust anchor. Refer to Figure 7 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of certificate structure. Refer to Annex B for details of the certificate profile.

NOTE 9 As in case of vehicle certificate, if the OCSP signer certificate that signs the OCSP response for the vehicle certificates is generated using a certificate chain that uses an OEM root CA as the trust anchor, the issuer can consider to cross-sign the OCSP signer certificate chain (one of the sub-CAs in the OCSP signer certificate chain or the OEM root CA) by a V2G root CA certificate. This will improve availability of communications as specified in this document and allow the EV to utilize communications as specified in this document on any EVSE that supports the said V2G root CA regardless if the EVSE trusts the specific OEM root CA (i.e. has access to the specific OEM root CA certificate) or not.

NOTE 10 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the OEM's discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use (if any) as the trust anchor for the OCSP signer certificate that signs the OCSP response for their vehicle certificates.

[V2G20-2333] An OEM provisioning certificate shall be generated using a certificate chain that uses either an OEM root CA certificate or a V2G root CA certificate as the trust anchor. Refer to Figure 7 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of certificate structure. Refer to Annex B for details of the certificate profile.

NOTE 11 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the OEM's discretion (while being aware of the applicable

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

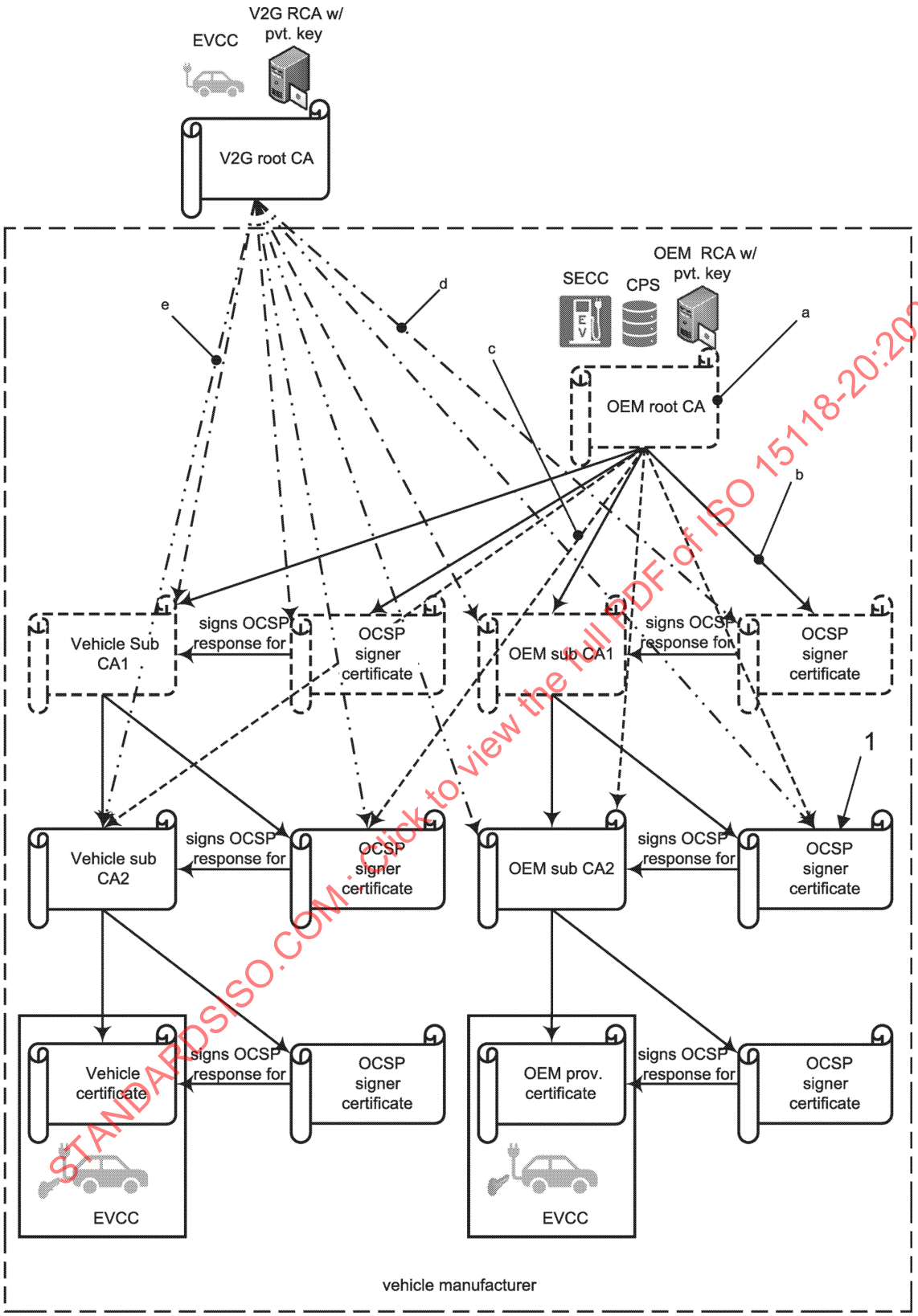
local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use (if any) as the trust anchor for their OEM provisioning certificates.

[V2G20-2334] The OCSP signer certificate used to sign the OCSP response for OEM provisioning certificate status shall be generated using a certificate chain that uses either an OEM root CA certificate or a V2G root CA certificate as the trust anchor. Refer to Figure 7 for a pictorial representation. Refer to Annex H for further details. Refer to H.1.6 for examples of certificate structure. Refer to Annex B for details of the certificate profile.

NOTE 12 This document does not mandate usage of a particular V2G root CA. In case multiple V2G root CAs are available in a region, it is up to the OEM's discretion (while being aware of the applicable local/regional/state/federal/international rules/regulations/laws) to decide which V2G root CA they use (if any) as the trust anchor for the OCSP signer certificate that signs the OCSP response for their OEM provisioning certificates.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Key

1 certificate

[a] Optional certificate — If the sub-CA1 is not present, the sub-CA2 is signed by the V2G root CA.

[b] Direct certification — The use of sub-CA1 is optional.

[c] Optional direct certification — If the sub-CA1 is present, it signs the sub-CA2 certificates.

© ISO 2022 – All rights reserved

[d] Upon OEM's discretion the vehicle certificate and OEM provisioning certificate chain may originate from V2G root CA certificate. This type of arrow shows when the sub-CA1 is signed by the V2G root CA.

[e] Upon OEM's discretion the vehicle certificate and OEM provisioning certificate chain may originate from V2G root CA certificate. This type of arrow shows when the sub-CA1 is not used and sub-CA2 is signed by the V2G root CA.

Figure 7 — Certificate structure originating from OEM root CA certificate

[V2G20-2335] A PE certificate shall be generated using a certificate chain that uses a PE private root CA certificate as the trust anchor. Refer to Annex H for further details. Refer to H.1.6 for examples of certificate structure. Refer to Annex B for details of the certificate profile.

[V2G20-2336] A PE certificate chain shall not be signed or cross-signed by any CA under a V2G root CA or an eMSP root CA or an OEM root CA. Similarly, PE certificate chain shall not be signed or cross-signed by any V2G root CA or eMSP root CA or OEM root CA.

NOTE 13 A PE certificate chain can, however, be cross-signed by a CA in another PE certificate chain.

7.3.2.1.1 Minimum required/mandatory certificates

Some certificates are needed for the functioning of this document. This subclause defines the minimum certificates required both in the SECC and the EVCC that allows basic communication to function. The basic function is defined as being able to setup the communication and utilize EIM for authorization of services. This subclause does not cover requirements for the private SECC.

[V2G20-2337] The SECC shall contain an SECC certificate. This certificate is necessary to establish a TLS session. Refer to 7.3.2.1 for SECC certificate requirements.

NOTE 1 In case of cross-signing the SECC certificate chain, the SECC can actually contain multiple sub-CA certificates and cross certificates.

[V2G20-2338] Each SECC shall possess at least one of either of the following root certificates:

- V2G root CA certificate;

OR

- OEM root CA certificate.

NOTE 2 This means that at any given time, the SECC can have at least one of the above valid root certificates. Since the vehicle certificate used during TLS session setup is based on at least one, if not both, of the root certificates mentioned here, an SECC cannot support communication without at least one of these roots.

NOTE 3 The SECC can possess more than one V2G root CA certificates.

NOTE 4 The SECC can possess more than one OEM root CA certificates.

NOTE 5 The SECC can possess both V2G root CA certificates and OEM root CA certificates.

[V2G20-2339] The EVCC shall contain a vehicle certificate. This certificate is necessary to establish a TLS session. Refer to 7.3.2.1 for vehicle certificate requirements.

NOTE 6 In case of cross-signing the vehicle certificate chain in the EVCC can actually contain multiple sub-CA certificates and cross certificates.

[V2G20-2340] The EVCC shall possess at least one V2G root CA certificate. This certificate is necessary to verify SECC certificates to establish TLS session. Refer to 7.3.2.1 for V2G root CA certificate requirements.

NOTE 7 The EVCC can possess more than one V2G root CA certificates.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

7.3.2.1.2 Certificates required for PnC

Support for PnC is not mandatory for EVCC/SECC. It is up to the OEM/CSO to decide whether to support PnC or not. If the EVCC wants to support PnC, requirements defined in this subclause are mandatory.

[V2G20-2341] The EVCC shall contain at least one contract certificate or, in case the EVCC supports contract certificate installation via EVSE, storage space for at least one contract certificate. This certificate is necessary for PnC authorization. Refer to 7.3.2.1 for contract certificate requirements.

NOTE 1 EVCC can contain more than one contract certificate.

NOTE 2 This requirement does not provide details of how the contract certificate was installed. This document provides a methodology to install these certificates via EVSE but the OEM can choose to install contract certificates in another manner as suitable for their design.

7.3.2.1.3 Certificates required for installation of contract certificates via EVSE

Support for contract certificate installation via EVSE is not mandatory. It is up to the OEM to decide whether to support contract certificate installation via EVSE or not. If the EVCC wants to support contract certificate installation via EVSE, requirements defined in this subclause are mandatory.

[V2G20-2342] The EVCC shall contain one OEM provisioning certificate. This certificate is necessary for contract certificate installation via EVSE. Refer to 7.3.2.1 for OEM provisioning certificate requirements.

NOTE If the EVCC does not want to install contract certificates via EVSE, this requirement can be skipped.

[V2G20-2343] If the EVCC does not contain an OEM provisioning certificate, it shall not send CertificateInstallationReq message. Refer to 8.3.4.3.9.2 for details of CertificateInstallationReq message. Refer to 7.9.2.5 and its subclauses for details of contract certificate installation via the EVSE.

7.3.2.1.4 Minimum certificates required for PE

This subclause covers both the SECC and the private SECC.

[V2G20-2344] The SECC shall not contain any PE private root CA certificates.

NOTE 1 The SECC is assumed to always operate in public environment.

[V2G20-2345] The SECC operating in public environment shall not contain any PE certificate.

NOTE 2 The SECC is assumed to always operate in public environment.

[V2G20-2346] The private SECC shall not contain any SECC certificate.

[V2G20-2347] The private SECC shall possess a PE private root CA certificate. This certificate is necessary to establish a TLS session. Refer to 7.3.2.1 for PE private root CA certificate requirements.

[V2G20-2348] The private SECC shall contain a PE certificate. This certificate is necessary to establish a TLS session. Refer to 7.3.2.1 for PE certificate requirements.

7.3.2.2 Certificate governance

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Certificate governance and lifecycle management is a major aspect of any PKI system to secure the PKI, build trust and provide the necessary assurance. However, these aspects of the PKI system are outside the scope of this document.

A certificate, in and of itself, does not provide assurance on how the certificate holder ensures that the private key associated with the certificate is not compromised, what is the guarantee that the holder of the certificate is actually who they say they are, steps the CA will take when a private key is compromised, etc. That assurance and trust in the certificates comes through a certificate policy, certification practice statement, etc. certificate policy (CP) and certification practice statement (CPS) contain the topics as defined IETF RFC 3647.

X.509 defines a CP as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements".

Per IETF RFC 3647, "When a certification authority (CA) issues a certificate, it is providing a statement to a certificate user (i.e. relying party) that a particular public key is bound to a particular entity (i.e. certificate subject). The extent to which the certificate user should rely on that statement needs to be assessed by the certificate user." The certificate policy provides the information that can be used by a certificate user to decide whether or not to trust a certificate.

Certificate policies are also used to establish trust relationships between CAs (i.e. cross certification). When CAs issue cross certificates, one CA assesses and recognizes one or more certificate polices of the other CA.

Mostly the CAs post the CP, CPS, audit results, etc. publicly so that the certificate users can see how the CA ensures the security of the keys, identity of the certificate holders, manages the certificate lifecycle, etc. and develop trust in the CA.

[V2G20-2349] Any certificates originating from, or cross-signed by, a V2G root CA certificate chain or eMSP root CA certificate chain or OEM root CA certificate chain shall follow a well-established certificate governance structure, including but not limited to CP, CPS, etc.

[V2G20-2350] Any certificates originating from a PE private root CA certificate chain are not required to follow [V2G20-2349] if the private SECC using them is not scheduled to support PnC.

NOTE This does not mean that a governance structure cannot be used in PE. This just says it is not mandated.

[V2G20-2351] Any certificates originating from a PE private root CA certificate chain are required to follow [V2G20-2349] if the private SECC using them is scheduled to support PnC utilizing contract certificates.

This document does not provide any certificate governance structure. With many industry participants, this document leaves it to those participants, the CAs, PKI implementers, etc. to define the certificate governance structure that best suits their use cases. It is envisioned that the industry will automatically gravitate towards robust and secure CAs who have strong CP/CPS and provide periodic audit results along with verifiable data proving that they actually adhere to their CP/CPS.

7.3.3 Number of root certificates and root validity

This subclause defines requirements for storage space for number of various types of root CA certificates for the SECC and EVCC. This subclause does not mandate actual installation of these various root CA certificates in the SECC or EVCC. It is up to the discretion of the CSOs to decide which root CA certificates they want to install in their SECCs and to the OEMs to decide which root CA certificates they want to install in their EVCCs. For example, an OEM may want to support a specific PE for a certain fleet of vehicles

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

and as such may install the PE private root CA certificate for that particular PE in the EVCC of the EVs in that fleet but may choose not to install any PE private root CA certificate in EVCC in any other EVs it manufactures.

If the communication should work, some root CA certificates are installed in each SECC and EVCC. Depending on the use case of the EV and/or EVSE, the OEMs/CSOs will need to figure out which root CA certificates they should install in their EVCC/SECC so as to enable that particular use case.

[V2G20-1806] Each EVCC shall provide storage space for at least two V2G root CA certificates.

Storing two V2G root CA certificates is required by [V2G20-1806] to be able to store the currently valid V2G root CA certificate of a specific V2G root CA and additionally the new V2G root CA certificate of that V2G root CA that will be valid after the previous V2G root CA certificate has expired.

[V2G20-2352] Each SECC shall provide storage space for at least two V2G root CA certificates.

NOTE 1 It is not mandatory for SECC to support any V2G root CA certificates. A CSO can decide to only offer ISO 15118-20 communications to those EVs whose vehicle certificate is signed (or cross-signed) by an OEM root CA certificate supported by the CSO's SECC.

Storing two V2G root CA certificates is required by [V2G20-2352] to be able to store the currently valid V2G root CA certificate of a specific V2G root CA and additionally the new V2G root CA certificate of that V2G root CA that will be valid after the previous V2G root CA certificate has expired.

NOTE 2 This requirement does not apply to a private SECC.

There can be multiple V2G root CAs in a given market. [V2G20-1806] and [V2G20-2352] define the minimum number of V2G root CA certificates that need to be supported by EVCC and SECC respectively. Regulatory and market conditions may require EVCC and/or SECC to support more than the minimum number of V2G root CA certificates. For example, it is strongly advised, but not mandated, that the EVCC and SECC support all local/regional V2G root CA certificates. This will improve availability of ISO 15118-20 communications and allow the EV to utilize ISO 15118-20 based communications on any local/regional EVSE.

It is not in the scope of this document to define the maximum number of V2G root CA certificates to be supported by the EVCC and/or SECC. It is left up to the OEM to decide on the maximum number of V2G root CA certificates to be supported by the EVCC. Similarly, it is left up to the CSO to decide on the maximum number of V2G root CA certificates to be supported by the SECC.

Additionally, if the EV drives to a different region, it would need V2G root CA certificates for that region. It is not in the scope of this document to define how the OEM manages that situation. But the OEM is advised to take that into account when designing the EVs.

[V2G20-2353] Each public SECC shall provide storage space for at least two OEM root CA certificates.

NOTE 3 It is not mandatory for a public SECC to support any OEM root CA certificates. A CSO can decide to only offer ISO 15118-20 communications to those EVs whose vehicle certificate is signed (or cross-signed) by a V2G root CA certificate supported by the CSO's SECC.

Storing two OEM root CA certificates is required by [V2G20-2353] to be able to store the currently valid OEM root CA certificate of a specific OEM and additionally the new OEM root CA certificate of that OEM that will be valid after the previous V2G root CA certificate has expired.

[V2G20-2354] Each private SECC shall provide storage space for at least one OEM root CA certificate or V2G root CA certificate.

NOTE 4 A private SECC can contain more than one OEM root CA certificates and/or V2G root CA certificates.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

There can be multiple OEMs in a given market. [V2G20-2353] defines the minimum number of OEM root CA certificates that need to be supported by the public SECC. [V2G20-2354] defines the minimum number of OEM root CA certificates that need to be supported by the private SECC. Regulatory and market conditions may require the SECC to support more than the minimum number of OEM root CA certificates. For example, it is strongly advised, but not mandated, that the SECC support all local/regional OEM root CA certificates. This will improve availability of ISO 15118-20 communications and allow the EV to utilize ISO 15118-20 based communications on any local/regional EVSE.

It is not in the scope of this document to define the maximum number of OEM root CA certificates to be supported by the SECC. It is left up to the CSO to decide on the maximum number of OEM root CA certificates to be supported by the SECC.

Additionally, as new EV OEMs startup, there would be a need to add OEM root CA certificates for those new OEMs to the SECCs. It is not in the scope of this document to define how the CSO/PE operator manages that. But the CSO/PE operator is advised to take that into account when designing their systems.

[V2G20-2355] Each EVCC should provide storage space for at least one PE private root CA certificate.

NOTE 5 It is not mandatory for the EV to support private environment.

[V2G20-867] Except in private environment (PE), a root CA shall not issue a leaf certificate.

NOTE 6 Leaf certificates can only be issued by a sub-CA.

NOTE 7 This applies to all root CAs including V2G root CA, OEM root CA, eMSP root CA, etc. except PE private root CA. A PE private root CA can issue a leaf certificate. Refer to 7.3.4 for further details of PE security.

7.3.4 Support and application of TLS

According to 7.3.2 and 7.3.3, this document requires the following TLS:

1) the certificate management defined in 7.3.2;
2) the key management defined in 7.3.2;
3) the certificate chain structure defined in 7.3.2 and 7.3.3;
4) the certificate validity period defined in 7.3.2 and 7.3.3.

[V2G20-1238] In the SDP handshake, when the SECC intends to offer ISO 15118-20 communication, it shall respond to a TLS request by the EVCC with TLS.

[V2G20-1235] V2G-CI-TLS shall always be applied for both the EVCC and SECC, if the chosen ProtocolNamespace is equal to "urn:iso:std:iso:15118:-20".

[V2G20-2646] After the message exchange of supportedAppProtocolReq/Res, usage of V2G-CI-TLS shall be confirmed.

[V2G20-1237] If the established connection between EVCC and SECC is TLS 1.2 (or lower) or TCP without TLS the EVCC shall not offer ISO 15118-20 communication in SupportedAppProtocolReq message (see Table 5).

[V2G20-2356] If the established connection between EVCC and SECC is TLS 1.2 (or lower) or TCP without TLS the SECC shall not select ISO 15118-20 communication from SupportedAppProtocolReq message (see Table 5).

Private environment is considered to be a power transfer service for a closed user group. This user group is defined and managed by the eMSP of the power transfer service itself. The security of the field is

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

managed according to the security policy of the eMSP, so the authentication of private SECC by EVCC through TLS connection might be negligible. Refer to H.2 for further details of PE security.

7.3.5 Firewall

This subclause defines firewall functionality, where the term firewall refers to the definition made in ISO/IEC 27033-1. The firewall specified here separates the trusted from the untrusted network, where trusted and untrusted are defined as follows.

Trusted network — SECCs and SDP servers are part of the trusted network. Access to this network is controlled by the EVSE operator. Only authorized nodes of the operator have access to this network.

Untrusted network — EVCCs are part of the untrusted network. Access to this network is not controlled by the EVSE operator.

[V2G20-1013] There shall be at least one firewall between the EVCC, which is connected to an untrusted network, and the SECC, which is connected to a trusted network.

[V2G20-1014] For security reasons the rules mentioned in Table 3 shall apply for the firewall mentioned in [V2G20-1013].

Table 3 — Firewall action for wireless communication

Source		Destination		Protocol	Interface		Action
IP address	Port	IP address	Port		Inbound	Outbound	
all	EVCC Port (dynamic range)	ff02:01	15118	UDP	untrusted	trusted	allow
all	EVCC Port (dynamic range)	SECC IP address	SECC Port (V2G_DST_TCP_DATA)	TCP	untrusted	trusted	allow
all	EVCC Port (dynamic range)	SECC IP address	1080	TCP	untrusted	trusted	allow
SDP server IP address	15118	EVCC IP address	EVCC port	UDP	trusted	untrusted	allow
SECC IP address	SECC Port (V2G_DST_TCP_DATA)	EVCC IP address	EVCC port	TCP	trusted	untrusted	allow
SECC IP address	1080	EVCC IP address	EVCC port	TCP	trusted	untrusted	allow
SECC IP address	SECC Port [SECC_VAS_Port]	EVCC IP address	EVCC port	TCP	trusted	untrusted	allow
all	all	all	all	all	trusted	trusted	allow
all	all	all	all	all	all	all	deny
NOTE "Allow" means to establish a connection and "deny" means port-unreachable for the source.							

7.3.6 Protection of the cryptographic keys

The private keys of certificates are sensitive data. Once a private key gets compromised, it cannot be trusted anymore and therefore not supposed to be used anymore. If one of these private keys could be

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

read by an attacker, the attacker could impersonate the original equipment. It is considered good security practice that each V2G entity and any PKI operator additionally protects all private keys and symmetric keys. This can range from simple security measures such as setting readout protection fuse bits in the microcontroller to more advanced protection via secure boot facilities, debug access protection, and embedded hardware security modules (HSM). The HSMs offer a high level of security including protection against physical attacks. A suitable HSM provides a secure environment for private key and symmetric key operations. It offers interfaces to use the private key and the symmetric keys but ensures that the keys cannot be read out or manipulated.

The V2G entity or the PKI operator can use a trusted platform module (TPM) 2.0 to implement the HSM.

The TPM 2.0 is representative of a HSM that is qualified for the automotive use cases according to AEC-Q100, has Common Criteria (CC) EAL4+ certification and can implement the desired security features. A TPM 2.0 can securely store sensitive data such as private keys, provides a secure execution environment for symmetric and asymmetric cryptographic operations (including secure random number generation) and enables additional security mechanisms such as the direct import of encrypted keys, credential protection, secured (measured) boot and a policy-based enhanced authorization mechanism. The TPM 2.0 library specification developed by the Trusted Computing Group (TCG) is adopted as open international standards ISO/IEC 11889-1:2015, ISO/IEC 11889-2:2015, ISO/IEC 11889-3:2015 and ISO/IEC 11889-4:2015.

7.3.6.1 Protection of the EVCC keys

In an EVCC environment, the private keys of the contract certificate, vehicle certificate and the OEM provisioning certificate are considered to be sensitive data. The EVCC can protect the private keys and symmetric keys (including session keys) by employing secure environments like HSM that offer interfaces to use the keys but ensures that the keys cannot be read out or manipulated, even from a program running on the EVCC. A customized HSM may even accept input of an encrypted contract certificate private key, so that the private key is never accessible outside of the HSM in plain, unencrypted form. Such a HSM can be integrated into the EVCC as a separate physical package or as an on-chip microcontroller extension.

It is advised that the EVCC keeps the keys secure under all conditions, including while they are in use. An easy way to achieve this is to utilize the HSM to store and use the keys including any cryptographic operations that use those keys.

In addition, the EVCC can also utilize the HSM to perform other cryptographic functions in a secure manner (e.g. encryption/decryption, signature calculation and verification, asymmetric key-pair generation, etc.).

The EVCC can opt to use TPM to perform all (or some) of the functions mentioned above for the HSM. Refer to 7.3.6 for details of TPM.

7.3.6.2 Protection of the keys in public SECC

This subclause does not cover requirements for the private SECC. It only covers requirements for a public SECC. In some cases, though, a private SECC may be required to meet these requirements as well. Such cases will be specifically called out. In a public SECC environment, the private key of the SECC certificate is considered to be sensitive data. It is advised that the public SECC protects the private key and symmetric keys (including session keys) by employing secure environments like HSM that offer interfaces to use the keys but ensure that the keys cannot be read out or manipulated, even from a program running on the public SECC. Such a HSM can be integrated into the public SECC as a separate physical package or as an on-chip microcontroller extension.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

It is recommended that the public SECC keeps the keys secure under all conditions, including while they are in use. An easy way to achieve this is to utilize HSM to store and use the keys including any cryptographic operations that use those keys.

In addition, the public SECC can also utilize the HSM to perform other cryptographic functions in a secure manner (e.g. encryption/decryption, signature calculation and verification, asymmetric key-pair generation, etc.).

The public SECC can opt to use TPM to perform all (or some) of the functions mentioned above for the HSM. Refer to 7.3.6 for details of TPM.

7.3.6.3 Protection of the keys in private SECC

This subclause does not cover requirements for the SECC operating in public environment. It only covers requirements for a private SECC. Since the private SECC operates in a private environment, it is not required to follow the same security requirements as an SECC operating in a public environment.

However, to improve security of the solution, private SECC is encouraged to meet the similar security standards as an SECC operating in a public environment. Refer to 7.3.6.2 for further details.

[V2G20-2357] Any private SECC that supports PnC (using contract certificate(s)) shall meet the same security standards as an SECC operating in a public environment. Refer to 7.3.6.2 for further details.

7.3.7 Random number generation

Asymmetric cryptographic algorithms like ECDSA, EdDSA, etc. strongly rely on the fact that an attacker does not have information about the random nonce. Otherwise, signatures would leak information about the secret key. Depending on the type of defect in the random generator implementation, this may enable an attacker to derive the secret key after a certain number of signatures. In the worst case, simple reuse of the random nonce will enable an attacker to calculate the secret key after only two signatures. Therefore, it is vital to have a suitable random number generator (RNG), a so-called cryptographically secure RNG. In addition, for generating the initialization vector in AES-GCM, for generating a challenge for PnC and for generating a nonce for TLS session negotiation a cryptographically secure RNG is needed.

[V2G20-835] Whenever a V2G entity requires random numbers within this document, a state-of-the-art cryptographically secure random number generator shall be used.

NOTE 1 There could already be a suitable, cryptographically secure random number generator available in the implementation. As the actual implementation of the RNG does not affect interoperability, this document does not prescribe a specific way in order to be future-proof and to avoid duplication. Some examples of established RNG standards are NIST SP 800-90 A, German BSI AIS 20/AIS 31, etc.

NOTE 2 Additionally, IETF RFC 8937 provides a few methodologies for improvement of randomness for some use cases.

In general, there are two different kinds of RNGs, a deterministic random bit generator (DRBG) that utilizes an algorithm to produce random numbers based on a seed input. These kinds of RNGs are quite fast in producing a random number but suffer from the consequences of using a seed as an input. These kinds of RNGs have a few advantages like speed, no loss of entropy over time or usage, etc. As such, DRBGs are usually the preferred class of RNGs. These RNGs are also called pseudo-random number generator (PRNG).

Not all DRBGs are cryptographically secure. The random number generated by a DRBG is only as random as the input seed. If the input seed is known, the output random number could be predicted. As such, DRBGs are usually seeded every so often by another kind of RNG called non-deterministic random bit

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

generator (NRBG) that utilizes unpredictable physical processes/phenomenon to generate the random numbers. These kinds of RNGs do not require a seed as an input, but are much slower at generating the random number as they first gathers enough physical entropy before they can generate a random number. Additionally, these kinds of RNGs tend to loose entropy over time or with usage. Hence, NRBGs are usually not used for direct generation of a random number. In cryptographic applications, they are mostly used to seed a DRBG. These RNGs are also called true-random number generator (TRNG).

[V2G20-2607] The V2G entity shall ensure that the random number used to re-seed/re-initialize a DRBG has the minimum amount of entropy required for the particular application/feature/function as defined by this specification document. The entropy input and the seed shall be kept secret.

NOTE 3 Some applications could accept a low amount of entropy in the random number while others could require a very high amount of entropy. It is left up to the different applications/features/functions to define the amount of entropy needed for those particular applications/features/functions.

NOTE 4 As mentioned earlier, NRBGs can take some time to build entropy. If the seed for the DRBG is generated by a NRBG, there can be a need to either wait for the NRBG to build enough entropy before requesting the NRBG to generate the random number (seed) or the random number could be generated and securely stored at a time when the NRBG is known to have a good entropy and using that random number to re-seed/re-initialize the DRBG when the need to re-seed/re-initialize the DRBG arrives/occurs.

[V2G20-2608] The V2G entity shall keep a random number generated according to [V2G20-835] secret and shall use this random number only once.

7.3.7.1 Random number generator best practices

Cryptographic algorithms are highly dependent on random numbers. An implementation of the security architecture defined by this document is only as secure as the RNG implemented by the V2G entity and secure usage of the random numbers generated by that RNG.

Random number produced by a RNG should be used/processed securely.

If the V2G entity stores the random number generated by NRBG before using it, it should ensure security of that stored random number, such that no processes other than the process that actually needs to use the random number, have access to that random number. Similarly, the V2G entity should ensure that the seed (number generated by NRBG used to re-seed DRBG) is erased from memory after it has been used to re-seed the DRBG.

If the V2G entity uses a DRBG to generate the random number and the DRBG is seeded using a NRBG, the DRBG should be re-seeded/re-initialized from the NRBG at least once every 24 h or at power-up, whichever occurs earlier.

Most cryptographic RBGs are advertised as being able to produce 0,93 bits (or so) of entropy for every 1 bit generated by the RBG. In such cases a 128-bit random number generated by the RBG will have 120 bits of entropy. Requirements below take that into account when defining the minimum entropy requirements.

Higher the entropy, better the RBG is. Most applications/features/functions in this document require minimum 0,90 bits of entropy for every 1 bit generated. That means, they require 116 bits of entropy in a 128-bit random number.

If an application/feature/function in this document does not specify a minimum entropy requirement, it should be assumed to require minimum of 116 bits of entropy for any random number used by that application/feature/function.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 116 bits of entropy is based on 0,9 bits of entropy/bit generated by the RBG for a 128 bit number.

7.4 V2G communication states and data link handling

V2G messaging on application layer requires the establishment of the lower layer protocols to enable V2G message exchange between the EVCC and SECC. This document focuses on protocols above the data link layer. The data link layer is described in ISO 15118-3 and ISO 15118-8.

This subclause defines the basic requirements for establishing communication above the data link layer. This document does not imply any implementation. The figures in this subclause only show the basic sequencing for managing the protocol stack.

The timer, timeout and performance time values used in this subclause are described in 8.6 and its subclauses. Figure 8 depicts the general communication states of the V2G communication from an EVCC perspective. The following applies for the EVCC:

[V2G20-014] After the data link layer connection is established (D-LINK_READY.indication(DLINKSTATUS=Link established)), the EVCC shall initiate the IP address assignment mechanism as defined in 7.6.3.2 and 7.6.3.3.

[V2G20-016] The EVCC shall process the IP address assignment mechanism as defined in 7.6.3.2 and 7.6.3.3.

[V2G20-018] After a link-local IP address is assigned, the EVCC shall start the process for discovering the SECC address as defined in 7.10.1.

[V2G20-019] The EVCC shall start the SDP client according to 7.10.1.

[V2G20-1804] After receiving an SDP response with transport protocol set to TCP and security option set to TLS, the EVCC shall establish the TLS connection to the SECC as described in 7.7.3.

[V2G20-1805] If [V2G20-1804] is not fulfilled, then ISO 15118-20 (this document) shall not be offered by the EVCC during SupportedAppProtocolReq or selected by the SECC in SupportedAppProtocolRes. Refer to Table 5 for further details of services/standards that can be supported in such a condition.

[V2G20-024] After the TLS connection is established, the EVCC shall initiate the V2G communication session as defined in Clause 8.

[V2G20-025] The EVCC shall terminate the TLS connection after stopping the V2G communication session.

[V2G20-717] If the EVCC sent the message SessionStopReq with parameter ChargingSession equal to "Terminate" it shall terminate the Data-Link (D-LINK_TERMINATE.request()) after receiving the message SessionStopRes.

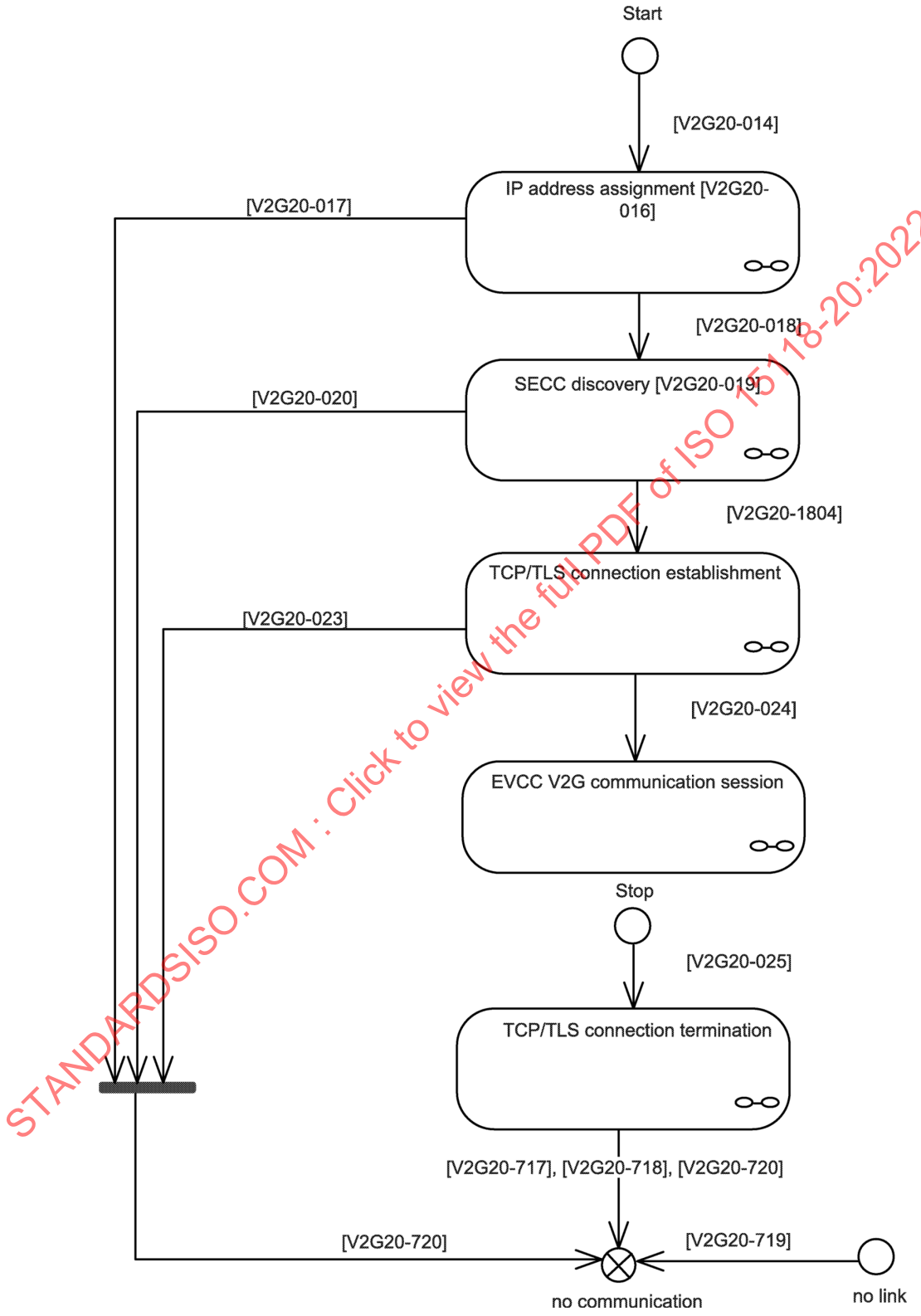
[V2G20-1227] If the EVCC sent the message SessionStopReq with parameter ChargingSession equal to "Pause" it shall pause the Data-Link (D-LINK_PAUSE.request()) after receiving the message SessionStopRes with ResponseCode set to "OK" and follow the sleep and wake-up requirements defined in ISO 15118-3:2015, 7.6.

[V2G20-719] Whenever the EVCC receives the indication for a missing Data-Link (D-LINK_READY.indication(DLINKSTATUS=No link)), the EVCC shall continue with [V2G20-014].

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-720] If the EVCC identifies any error it shall indicate a Data-Link error (D-LINK_ERROR.request()) and continue with [V2G20-014].



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Figure 8 — Overview V2G communication states EVCC

Figure 9 depicts the general communication states of the V2G communication from an SECC perspective. The following applies for the SECC:

© ISO 2022 – All rights reserved

[V2G20-721] After indication of a successful Data-Link establishment (D-LINK_READY.indication(DLINKSTATUS=Link established)), the SECC shall initiate the address assignment mechanism.

[V2G20-026] The SECC shall configure an IP address (static or dynamic) by any appropriate mechanism.

NOTE 1 To enable the integration of an SECC in different communication infrastructures, the definition of the address assignment for the SECC is not in the scope of this document. This enables the operator to assign an appropriate mechanism. For example, the operator can choose any existing mechanism providing a valid IP address like, for example, a static IP or the mechanism described in 7.6.3.2 and 7.6.3.3.

[V2G20-027] After the IP address is assigned, the SECC shall start the SDP server as defined in 7.10.1.

NOTE 2 It is not required that the SECC discovery service is implemented in the SECC directly. It is also possible to have a separate unit providing the SECC discovery service.

[V2G20-723] The SECC may stop the SDP server when SECC_CommunicationSetup_Timer is equal or larger than V2G_SECC _CommunicationSetup_Performance_Time.

[V2G20-029] The SECC may stop the IP address assignment mechanism when V2G_SECC_CommunicationSetup_Timer is equal or larger than V2G_SECC_CommunicationSetup_Performance_Time.

[V2G20-030] After the SDP server is started successfully, the SECC shall wait for a TLS connection initialization depending on the SDP response message as defined in 7.10.1.6.

[V2G20-031] The SECC shall wait until the TLS connection is established.

[V2G20-032] The SECC shall stop waiting for establishing the TLS connection when V2G_SECC_CommunicationSetup_Timer is equal or larger than V2G_SECC_CommunicationSetup_Performance_Time.

[V2G20-033] After the TLS connection is established, the SECC shall wait for the initialization of the V2G communication session as defined in Clause 8.

[V2G20-722] If [V2G20-033] applies the SECC may stop the SDP server after successful establishment of a TLS connection.

[V2G20-034] The SECC shall terminate the TLS connection after stopping the V2G communication session.

[V2G20-1776] If the SECC received the message SessionStopReq with parameter ChargingSession equal to "Terminate" it shall terminate the Data-Link (D-LINK_TERMINATE.request()) 2 s after sending the message SessionStopRes.

[V2G20-1777] If the SECC received the message SessionStopReq with parameter ChargingSession equal to "Pause" it shall pause the Data-Link (D-LINK_PAUSE.request()) after sending the message SessionStopRes with ResponseCode set to "OK" and follow the sleep and wake-up requirements defined in ISO 15118-3:2015, 7.6.

[V2G20-726] Whenever the SECC receives the indication for a missing Data-Link (D-LINK_READY.indication(DLINKSTATUS=No link)), the SECC shall continue with [V2G20-721].

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-727] If the SECC identifies any error it shall indicate a data link error (D-LINK_ERROR.request()) and continue with [V2G20-721].

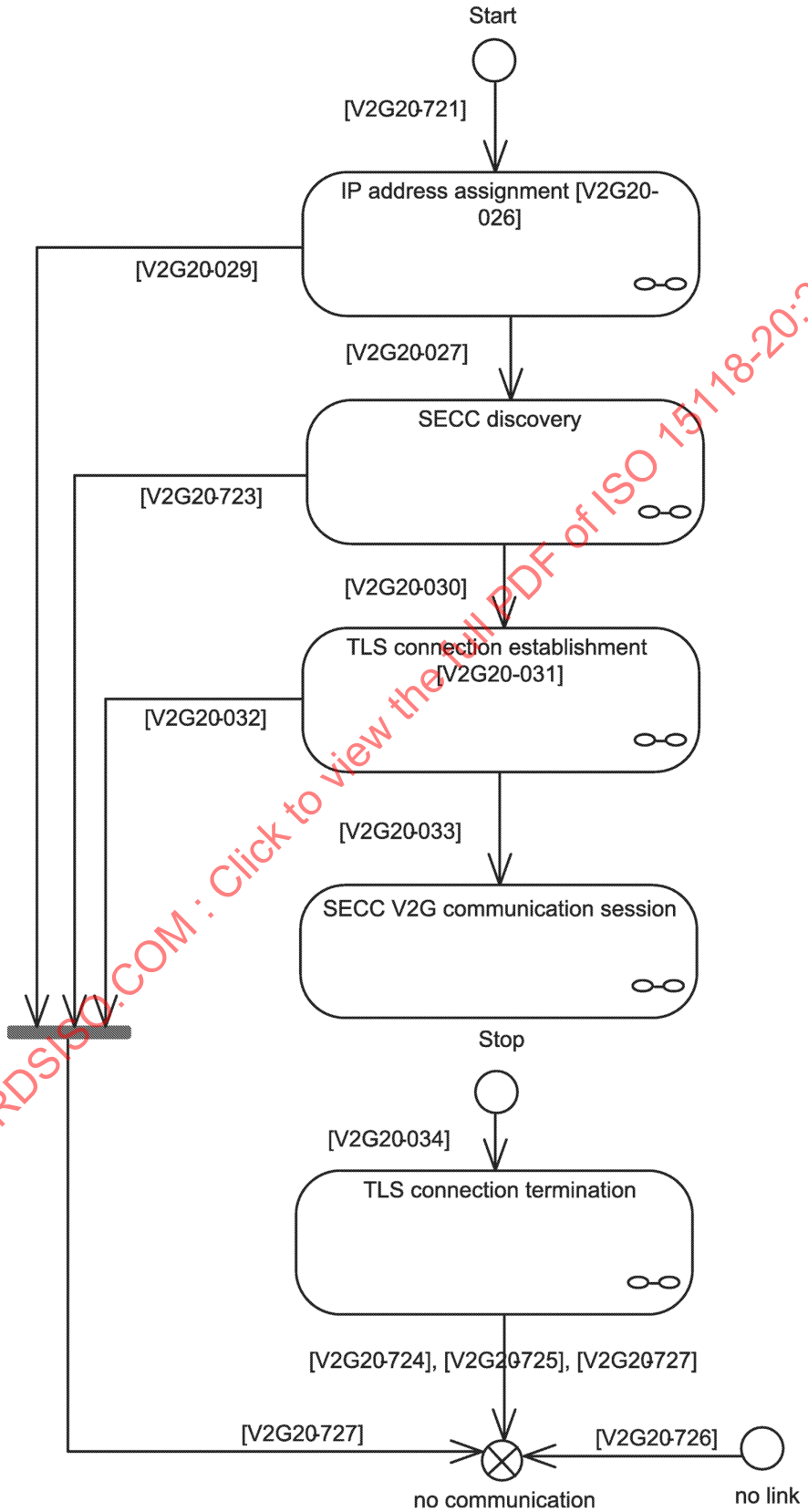


Figure 9 — Overview V2G communication session states SECC

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

7.5 Data link layer

The definitions in this document assume the data link layer to support the transport of IP packets as defined in the requirements. ISO 15118-3 and ISO 15118-8 define additional details on data link layer to be covered.

[V2G20-035] If a V2G entity communicates by PLC, the V2G entity shall comply with ISO 15118-3.

[V2G20-1015] If a V2G entity communicates by WLAN, the V2G entity shall comply with ISO 15118-8.

7.5.1 Data link layer security for WLAN

All wireless communication between the EVSE and the EV is inherently insecure unless specific security protocols are implemented. The reason is that the underlying physical layer protocol does not require authentication between the two parties trying to communicate with each other using WLAN. Additionally, all data sent over the WLAN is in plain text unless specific encryption protocols are implemented. This allows an adversary to not only access the WLAN network, but also to sniff and spoof the data being sent on the unprotected WLAN channel.

Although this document mandates TLS for most communications, SDP is sent before TLS is established. As such SDP is vulnerable to sniffing, spoofing, etc. In addition, since WLAN connection is established before TLS tunnel is setup, current specifications do not offer any way to authenticate the clients (EVs) trying to join a WLAN or the wireless access points offering ISO 15118 communication. For example, for an EV driving down the road, there is no way to identify whether the wireless access point that offers ISO 15118 communication is a legitimate EVSE or an attacker trying to establish a connection to the EV to try and compromise it.

Even if EV were to reject all messages/requests unless a TLS session is established, there are vulnerabilities that can be leveraged to scan the EV for other open vulnerabilities, etc. The same can be said for the EVSEs as well.

Currently the ISO 15118 series does not mandate any particular security or encryption methods on WLAN channels. Although security of wireless networks is optional in this document, it is highly recommended to use it. Unprotected wireless connections expose particularly high risks.

This subclause (and its subclauses) offers security on WLAN data link layer by allowing optional use of IEEE 802.1X. Usage of IEEE 802.1X allows establishment of an authenticated channel between the EV's WLAN STA device and the CSO's WLAN AP. Refer to ISO 15118-8 for details of WLAN, AP and STA.

It should be noted that EV's WLAN STA can be same as or different than EVCC. Similarly, CSO's WLAN AP could be same as or different than the SECC.

In addition to authentication, IEEE 802.1X allows optional encryption as well. This document takes advantage of this optional feature of IEEE 802.1X to provide integrity protection and ensure confidentiality of the data exchange between the WLAN access point(s) and the client(s) (EVs) trying to join the network. It also protects the EV by ensuring that the EV is joining a legitimate and secure WLAN network associated with charging infrastructure.

[V2G20-2237] If the CSO desires to secure access to their WLAN for EV-EVSE charging communications, the WLAN AP (see ISO 15118-8 for details) operated by that CSO shall implement all specifications in this subclause and the subclauses within.

NOTE 1 It is not mandatory for CSO to support these security mechanisms.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

[V2G20-2238] If the OEM wants their EVs to access CSO's secure WLAN for EV-EVSE charging communications, the WLAN STA (see ISO 15118-8 for details) in the OEM's EV shall implement all specifications in this subclause and the subclauses within.

NOTE 2 It is not mandatory for the OEM to support these security mechanisms.

[V2G20-2239] It is up to the CSOs discretion whether to allow an EV that does not support the required security for WLAN to access the CSO's secure WLAN for EV-EVSE charging communications.

NOTE 3 The CSO is free to decline access to such EVs to access the CSO's WLAN.

NOTE 4 If the CSO goes through the effort of securing their WLAN for EV-EVSE charging communications, the CSO will likely not accept insecure connections to its WLAN.

[V2G20-2240] It is up to the OEM's discretion whether to allow an EV that supports security for WLAN to access a CSO's unsecured WLAN for EV-EVSE charging communications.

NOTE 5 The OEM (EV) is free to decline connections to insecure WLAN.

7.5.1.1 Applicable RFCs

The security on the data link layer is ensured through the use of IEEE 802.1X. It is part of the IEEE 802.11-2020 group of network protocols. IEEE 802.1X defines the encapsulation of the extensible authentication protocol (EAP) via IEEE 802.11-2020. EAP is an authentication framework that supports multiple authentication methods. EAP works directly over data link layers (IEEE 802) without the need for IP. EAP encapsulation can be used for both wired and wireless media. This document strongly recommends the use of IEEE 802.1X for connections utilizing wireless media.

[V2G20-2241] A V2G entity shall implement IEEE 802.1X.

NOTE 1 These requirements are normally not implemented in the SECC or EVCC. The OEM would normally implement these requirements in the WLAN STA. The CSO/PE operator would normally implement these requirements in the WLAN AP.

[V2G20-2242] IETF RFC 3748 shall be used as the encapsulation of IEEE 802.1X.

NOTE 2 IETF RFC 3748 has been updated by IETF RFC 5247 and IETF RFC 7057. IETF RFC 5247 has been updated by IETF RFC 8940. All these updates are considered to be included in this document.

[V2G20-2243] Remote authentication dial-in user service (RADIUS) as specified by IETF RFC 3579 shall be used as "pass-through peer" implementation of IETF RFC 3748 by the CSO/PE operator.

NOTE 3 IETF RFC 3579 has been updated by IETF RFC 5080. These updates are considered to be included in this document.

[V2G20-2244] The V2G entity shall use EAP extension EAP-TLS, as specified by IETF RFC 5216. TLS 1.3 shall be used for EAP-TLS.

NOTE 4 At the time of writing, an update of RFC 5216 for EAP-TLS with TLS 1.3 was still in progress. Once it has been released, this update will become applicable according to [V2G20-2244].

7.5.1.1.1 Applicable RFCs for RADIUS

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

If it is desired to use remote authentication dial-in user service (RADIUS) as the authentication, authorization, and accounting (AAA or Triple A) management solution, RFCs mentioned in this subclause shall be followed.

[V2G20-2245] Remote authentication dial in user service (RADIUS) as defined in IETF RFC 2865 shall be implemented.

NOTE 5 IETF RFC 2865 has been updated by IETF RFC 2868, IETF RFC 3575, IETF RFC 5080, IETF RFC 6929 and IETF RFC 8044. IETF RFC 2868 has been updated by IETF RFC 3575. IETF RFC 3575 has been updated by IETF RFC 6929. All these updates are considered to be included in this document.

[V2G20-2246] RADIUS accounting requirements specified in IETF RFC 2866 shall be implemented.

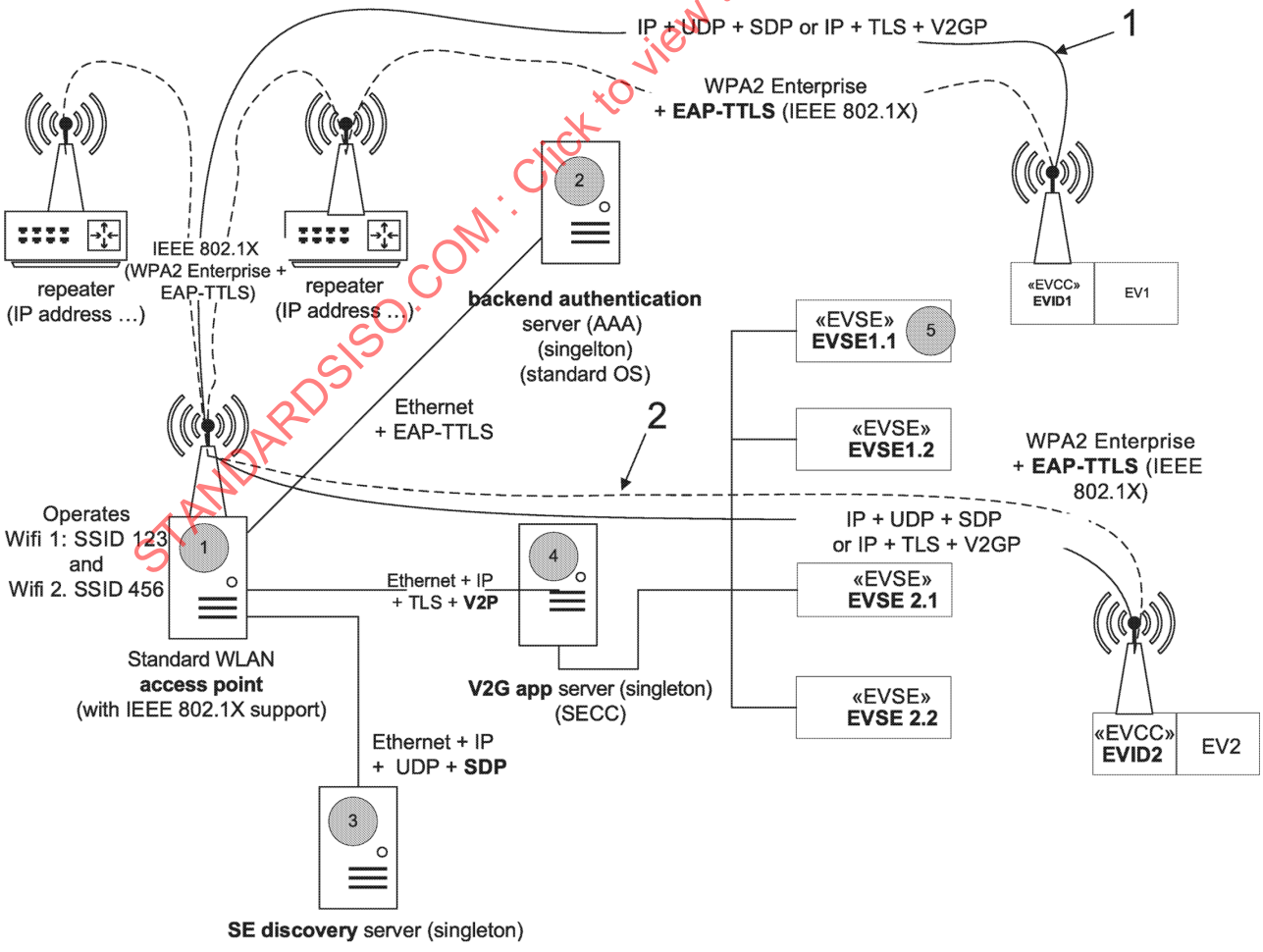
NOTE 6 IETF RFC 2866 has been updated by IETF RFC 2867, IETF RFC 5080 and IETF RFC 5997. All these updates are considered to be included in this document.

There are multiple other IETF RFCs that are necessary to implement RADIUS. This document does not list all of them. RFCs related to RADIUS and dated before the publication of this document should be considered for RADIUS implementation.

7.5.1.2 Example of secure WLAN connection setup

This subclause uses RADIUS as a synonym for this type of security architecture.

Figure 10 shows an example of the steps (circled numbers) involved in establishing a connection for wireless power transfer (WPT) using RADIUS.



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Key

1 App layer communication protocol

2 IEEE 802.1X communication protocol

Figure 10 — IEEE 802.1X example with backend authentication for WPT

RADIUS is not just limited to WPT, it can be used in other wireless communication use cases like ACDP or AC / DC wireless charging.

1. EV's WLAN STA (see ISO 15118-8 for details) uses WPA3-Enterprise or WPA2-Enterprise to build up a physical connection to a central access point (AP) (see ISO 15118-8 for details) of the infrastructure.

2. The AP forwards the connection request to the authorization server (AS) of the infrastructure via EAP (IEEE 802.1X with EAP pass-through-authentication).

3. After successful mutual authentication via RADIUS, the AP forwards the further establishment of the IP and service discovery protocol (SDP) connection of the EVCC to the central service discovery service. In the SDP request, the EVCC specifies the desired parameters of the electrical system. The central identification service sends back the transport address of the corresponding V2G application via SDP.

4. EVCC and SECC authenticate each other via transport layer security (TLS). The following assignment activity on the V2G application layer checks whether the EVSE can actually operate the EV with its electrical parameters or not.

5. EV now positions itself on the EVSE, uses the pairing and positioning device (PPD) to align itself with the energy transmission device and couples to the EVSE via SECC. After pairing, the EVCC causes the SECC to charge its EV battery.

In summary, it can be stated that RADIUS enables the establishment of an authenticated and encrypted channel on the data link layer, which guarantees the integrity and confidentiality between the EV and the infrastructure. This means that all protocols that use such a protected data connection are equally protected.

7.5.1.3 Secure WLAN connection setup

[V2G20-2247] When the EVCC uses a wireless medium to establish a physical connection to an AP (see ISO 15118-8 for details), the EV's WLAN STA (see ISO 15118-8 for details) shall use WPA3-Enterprise or WPA2-Enterprise according to IEEE 802.1X.

[V2G20-2248] When the CSO offers a wireless medium to establish a physical connection to an AP (see ISO 15118-8 for details), the CSO shall use WPA3-Enterprise or WPA2-Enterprise according to IEEE802.1X.

NOTE 1 The AP is not required to support both WPA3-Enterprise and WPA2-Enterprise.

[V2G20-2249] If the EVCC uses WPA3-Enterprise, its STA device shall set protected management frames (PMF) to required. Refer to WPA3 specifications for details.

[V2G20-2250] If the CSO uses WPA3-Enterprise, its AP shall set protected management frames (PMF) to required. Refer to WPA3 specifications for details.

[V2G20-2251] If the EVCC uses WPA3-Enterprise, its WLAN STA shall not support WPA3-Enterprise transition mode. Refer to WPA3 specifications for details.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2252] If the CSO uses WPA3-Enterprise, its AP shall not support WPA3-Enterprise transition mode. Refer to WPA3 specifications for details.

[V2G20-2253] Regardless if WPA3-Enterprise is used or WPA2-Enterprise is used, the EV's WLAN STA (see ISO 15118-8 for details) shall implement MAC address randomization. Refer to WPA3 specifications for details.

[V2G20-2254] Regardless if WPA3-Enterprise is used or WPA2-Enterprise is used, the EV's WLAN STA (see ISO 15118-8 for details) shall implement "server certificate validation" to ensure that the AP that the EVCC connects to is a valid and trustworthy WLAN AP.

[V2G20-2256] The EVCC shall disable user override of server certificate (UOSC). Refer to WPA3 specifications for further details.

NOTE 2 This means TOD-STRICT (trust override disable strict) applies. This requirement applies to both WPA3-Enterprise and WPA2-Enterprise.

[V2G20-2255] The CSO shall provide an SECC certificate, as defined in Annex B, to the EVCC so that the EVCC can authenticate the CSO's authentication server.

[V2G20-2257] The EVCC shall authenticate CSO's authentication server with the certificate provided by the CSO's authentication server.

[V2G20-2258] The EVCC shall validate the provided certificate per [V2G20-1001] (with the SECC certificate profile as defined in Annex B).

NOTE 3 The EV can use its STA or the EVCC or another entity to perform this certificate validation.

[V2G20-2259] If the EVCC is unable to successfully authenticate the CSO's authentication server, it shall decline to establish a wireless connection with the CSO's access point.

[V2G20-2260] When the CSO's authentication server requests EVCC to present its certificate to authenticate itself, the EVCC shall provide its vehicle certificate.

[V2G20-2261] The CSO's authentication server shall authenticate the EVCC using the certificate provided by the EVCC.

[V2G20-2262] The CSO's authentication server shall validate the provided certificate per [V2G20-1001] (with the vehicle certificate profile as defined in Annex B).

[V2G20-2263] If the CSO's authentication server is unable to successfully authenticate the EV, it shall decline establishing a wireless connection with the EV. The CSO's access point forwards the data traffic to the SECC only after CSO's authentication server indicates successful mutual authentication via IEEE 802.1X.

[V2G20-2264] The CSO shall utilize the cipher suites as specified by Table 6 for EAP-TLS.

NOTE 4 Table 6 lists multiple cipher suites in the order of preference. Based on the configuration of the CSO's AP, only one of these cipher suites will be used for EAP-TLS. In general, the preferred cipher suite will be used for EAP-TLS. In case a security flaw was found in the preferred cipher suite, the AP can be configured to switch to the backup cipher suite as listed in Table 6.

[V2G20-2265] The EVCC shall utilize the cipher suite as specified by Table 6 for EAP-TLS.

NOTE 5 Table 6 lists multiple cipher suites in the order of preference. Based on the configuration of the EV's WLAN STA, only one of these cipher suites will be used for EAP-TLS. In general, the preferred cipher suite will be

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

used for EAP-TLS. In case a security flaw was found in the preferred cipher suite, the WLAN STA can be configured to switch to the backup cipher suite as listed in Table 6.

[V2G20-2266] The CSO shall utilize the (elliptic curve) ECs as specified by Table 7 for EAP.

NOTE 6 Table 7 lists multiple curves in the order of preference. Based on the configuration of the CSO's AP, only one of these curves will be used for EAP-TLS. In general, the preferred curve will be used for EAP-TLS. In case a security flaw was found in the preferred curve, the AP can be configured to switch to the backup curve as listed in Table 7.

[V2G20-2267] The EVCC shall utilize the (elliptic curve) ECs as specified by Table 7 for EAP-TLS.

NOTE 7 Table 7 lists multiple curves in the order of preference. Based on the configuration of the EV's WLAN STA, only one of these curves will be used for EAP. In general, the preferred curve will be used for EAP. In case a security flaw was found in the preferred curve, the WLAN STA can be configured to switch to the backup curve as listed in Table 7.

[V2G20-2268] The CSO shall utilize ECDHE for EAP.

[V2G20-2269] The EVCC shall utilize ECDHE for EAP.

[V2G20-2270] The CSO shall utilize the signature algorithm as specified by Table 8 for EAP.

NOTE 8 Table 8 lists multiple signature algorithms in the order of preference. Based on the configuration of the CSO's AP, only one of these signature algorithms will be used for EAP. In general, the preferred signature algorithm will be used for EAP. In case a security flaw was found in the preferred signature algorithm, the AP can be configured to switch to the backup signature algorithm as listed in Table 8.

[V2G20-2271] The EVCC shall utilize the signature algorithm as specified by Table 8 for EAP.

NOTE 9 Table 8 lists multiple signature algorithms in the order of preference. Based on the configuration of the EV's WLAN STA, only one of these signature algorithms will be used for EAP. In general, the preferred signature algorithm will be used for EAP. In case a security flaw was found in the preferred signature algorithm, the WLAN STA can be configured to switch to the backup signature algorithm as listed in Table 8.

Since the SECC and the CSO's authentication server are two separate entities, the SECC certificate provided by the CSO's authentication server during IEEE 802.1X will likely not be the same as the SECC certificate provided by the SECC to setup the TLS session between the EVCC and the SECC. Similarly, the EVCC and the EV WLAN STA may be two separate entities, resulting in a different vehicle certificate for IEEE 802.1X communication compared to the certificate used during TLS session setup between the EVCC and the SECC. This should not result in any issues though as the WPA3-Enterprise (or WPA2-Enterprise) protected wireless communication is only between the EV's WLAN STA and the CSO's wireless AP while the TLS session protects the communication between the EVCC and the SECC involved in the energy transfer process.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

7.6 Network link layer

7.6.1 General

The protocol specified in this document is based on the internet protocol standard known as IPv6 (see IETF RFC 8200).

7.6.2 Applicable RFCs, limitations and protocol parameter settings

7.6.2.1 IPv6

[V2G20-1244] A V2G entity shall support IPv6 as defined in IETF RFC 8200.

© ISO 2022 – All rights reserved

[V2G20-1017] A V2G entity shall fulfil the IPv6 node requirements specified in IETF RFC 8504.

[V2G20-1245] A V2G entity shall not use IPsec as defined by IETF RFC 8200 for the V2G communication.

NOTE 1 In case of ISO 15118-20 communication, TLS 1.3 is used to secure the communication between EVCC and SECC. To secure VAS, TLS 1.3 can also be used.

The IANA allocation guidelines for the routing type field in the IPv6 routing header are described in IETF RFC 5871. It is recommended to adhere to these guidelines.

[V2G20-1241] A V2G entity shall implement path MTU discovery according to IETF RFC 8201.

[V2G20-041] A V2G entity shall support handling of overlapping IP fragments according to IETF RFC 5722.

NOTE 2 IETF RFC 5722 has been updated by IETF RFC 6946. These updates are considered to be included in this document.

A V2G entity should comply with the specification in IETF RFC 5220, which extends IETF RFC 8200.

[V2G20-042] When sending an IPv6 packet from EVCC to SECC or from SECC to EVCC, no IP fragmentation shall be used.

It is recommended to use TCP segmentation to transmit a V2G message larger than the MTU.

The communication between EVCC and secondary actors as well as SECC and secondary actors is not in the scope of this document and may or may not use IP fragmentation.

[V2G20-1518] When sending an IPv6 packet containing energy transfer related communication from EVCC to SECC or from SECC to EVCC, the Traffic Class field in the IPv6 header shall be set to a value between 192 and 255.

[V2G20-1519] When sending an IPv6 packet containing non-energy transfer related value added service communication from EVCC to SECC or from SECC to EVCC, the Traffic Class field in the IPv6 header shall be set to a value between 0 and 127.

7.6.2.2 Dynamic host control protocol (DHCPV6)

Data link requirements are described in ISO 15118-3 and ISO 15118-8. The EVCC starts the address assignment triggered by the Data-Link when a Data-Link connection is established. This is done according to 7.6.3.2 using SLAAC (Stateless auto address configuration), which is mandatory according to this document. DHCPv6 might be implemented as an optional IP configuration method.

[V2G20-1242] If an EVCC chooses to implement a DHCPv6 client, it shall implement it according to IETF RFC 8415.

[V2G20-1239] If the infrastructure chooses to implement a DHCPv6 server on an EVSE, it shall implement it according to IETF RFC 8415.

7.6.2.3 Neighbor discovery (ND)

The EVCC uses IPv6 SLAAC for generating addresses for its interface. All interfaces have a link-local address. To ensure unique addresses and to support global addresses, the neighbour discovery protocol (NDP) is used.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

[V2G20-045] The EVCC shall implement NDP as defined in IETF RFC 4861.

NOTE 1 IETF RFC 4861 has been updated by IETF RFC 5942, IETF RFC 6980, IETF RFC 7048, IETF RFC 7527, IETF RFC 7559, IETF RFC 8028, IETF RFC 8319 and IETF RFC 8425. These updates are considered to be included in this document.

[V2G20-046] The EVCC shall comply with IETF RFC 4429 allowing assignment of IP addresses before duplicate address detection is finished.

NOTE 2 IETF RFC 4429 has been by IETF RFC 7527. These updates are considered to be included in this document.

7.6.2.4 Internet control message protocol (ICMP)

The internet control message protocol (ICMP) is used to send error messages (e.g. a requested service is not available, a host could not be reached).

[V2G20-047] Each V2G entity shall implement ICMPv6 as specified in IETF RFC 4443.

NOTE 3 IETF RFC 4443 has been updated by IETF RFC 4884 which has been updated by IETF RFC 8335. These updates are considered to be included in this document.

[V2G20-049] Each V2G entity shall implement the RFCs referred to in column "Reference" of Table 4 describing the implementation details for the respective ICMP message type.

Table 4 — Mandatory ICMP message set

ICMP message type	ICMP message name	Reference
1	Destination unreachable	IETF RFC 4443
2	Packet too big	IETF RFC 8335
3	Time exceeded	IETF RFC 4443
4	Parameter problem	IETF RFC 8335
128	Echo request	IETF RFC 4443
129	Echo reply	IETF RFC 8335
133	Router solicitation	IETF RFC 4861
134	Router advertisement	IETF RFC 4861
135	Neighbor solicitation	IETF RFC 4861
136	Neighbor advertisement	IETF RFC 4861
137	Redirect message	IETF RFC 4861
141	Inverse neighbor discovery solicitation message	IETF RFC 3122
142	Inverse neighbor discovery advertisement message	IETF RFC 3122

NOTE 4 IETF RFC 4443 has been updated by IETF RFC 4884 which has been updated by IETF RFC 8335. These updates are considered to be included in this document.

NOTE 5 IETF RFC 4861 has been updated by IETF RFC 5942, IETF RFC 6980, IETF RFC 7048, IETF RFC 7527, IETF RFC 7559, IETF RFC 8028, IETF RFC 8319 and IETF RFC 8425. These updates are considered to be included in this document.

7.6.3 IP addressing

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

7.6.3.1 General

This subclause specifies how an EVCC retrieves valid IP addresses to communicate over an IP-based network. The following addresses are considered for the purpose of this document:

- link local IP address of EVCC;
- global IP address of EVCC, if router is present in local link;
- IP address of SECC.

NOTE An IPv6 host can have multiple IP addresses assigned to one physical network interface, e.g. link-local and global address.

7.6.3.2 Stateless auto address configuration (SLAAC)

[V2G20-050] Each V2G entity shall support the configuration of a link-local IPv6 unicast address as specified in IETF RFC 4291.

NOTE 1 IETF RFC 4291 has been updated by IETF RFC 5952, IETF RFC 6052, IETF RFC 7136, IETF RFC 7346, IETF RFC 7371 and IETF RFC 8064. These updates are considered to be included in this document.

[V2G20-051] The interface ID of the link-local address of a V2G entity shall be generated from its IEEE 48 bit MAC identifier according to the definition in IETF RFC 4291.

[V2G20-052] The EVCC shall support auto configuration of IPv6 addresses as described in IETF RFC 4862.

NOTE 2 IETF RFC 4862 has been updated by IETF RFC 7527. These updates are considered to be included in this document.

7.6.3.3 Address selection

[V2G20-1263] If multiple IPv6 addresses are supported, the IPv6 default address selection shall be performed according to IETF RFC 6724.

7.7 Transport layer

This subclause, and all subclauses provide specific and separate requirements for the private SECC and the SECC. Thus, unless otherwise specified for this subclause or any subclause within it, private SECC and SECC are not considered interchangeable.

7.7.1 Transmission control protocol (TCP)

7.7.1.1 Overview

The transmission control protocol (TCP) allows applications of V2G entities to establish a reliable data connection to other entities in order to exchange data in a reliable way and in-order. Additionally TCP provides flow control and congestion control and also provides for various algorithms to handle congestion and influence flow control.

7.7.1.2 Applicable RFCs, limitations and protocol parameter settings

[V2G20-055] Each V2G entity shall implement TCP as specified in IETF RFC 793.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

NOTE IETF RFC 793 has been updated by IETF RFC 1122, IETF RFC 3168, IETF RFC 6093 and IETF RFC 6528. Additionally:

- IETF RFC 1122 has been updated by IETF RFC 2474, IETF RFC 5884, IETF RFC 6093, IETF RFC 6298, IETF RFC 6633, IETF RFC 6864 and IETF RFC 6;
- IETF RFC 3168 has been updated by IETF RFC 4301, IETF RFC 6040 and IETF RFC 8311;
- IETF RFC 2474 has been updated by IETF RFC 3186, IETF RFC 3260 and IETF RFC 8436;
- IETF RFC 8029 has been updated by IETF RFC 8611;
- IETF RFC 8584 has been updated by IETF RFC 7726;
- IETF RFC 4301 has been updated by IETF RFC 6040 and IETF RFC 7619.

All these updates are considered to be included in this document.

7.7.1.3 TCP performance and checksum requirements

The following requirements define TCP implementation details relative to congestion control, retransmission, timing, initial window size and Selective Acknowledgement for the purpose of improving the overall performance of TCP.

It is recommended to use the following congestion control and retransmission algorithms in addition to the standard TCP methods:

[V2G20-057] Each V2G entity should implement TCP congestion control according to IETF RFC 5681.

[V2G20-059] Each V2G entity should compute TCP's retransmission timer according to IETF RFC 6298.

[V2G20-2134] Whenever a TCP retransmission timeout (RTO) is computed in a V2G entity, the RTO shall be lower than 400 ms.

[V2G20-2135] Whenever a TCP retransmission timeout (RTO) is computed in a V2G entity, the RTO should be in the range of 50 ms (lower bound) and 110 ms (upper bound).

NOTE While [V2G20-2134] defines the maximum upper bound allowed in this document, [V2G20-2135] provides a recommendation.

[V2G20-060] To increase TCP's performance each V2G entity should implement TCP extensions for high performance according to IETF RFC 7323.

[V2G20-062] Each V2G entity should implement the user timeout option according to IETF RFC 5482.

[V2G20-063] The urgent pointer for TCP should not be used by any V2G entity.

It is recommended to use the following checksum algorithm:

[V2G20-064] The checksum fields required in TCP headers should be implemented according to IETF RFC 1624.

[V2G20-2358] To improve packet loss handling, each V2G entity should implement selective acknowledgment (SACK) and selective repeat retransmission according to IETF RFC 2018.

7.7.2 User datagram protocol (UDP)

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

7.7.2.1 Overview

The user datagram protocol (UDP) is a connectionless protocol. UDP does not provide the reliability and ordering guarantees that TCP provides. Packets may arrive out of order or may be lost without notification to the sender or receiver. However, UDP is faster and more efficient for many lightweight or time-sensitive purposes. UDP is located on the transport layer of the OSI layered architecture model.

Optional security mechanisms are provided in 7.5.1 to secure UDP over WLAN. Currently there is no PLC based use case utilizing UDP, for which security mechanisms on UDP would be required (refer to ISO 15118-1 for details on security use cases).

7.7.2.2 Applicable RFC, limitations and protocol parameter settings

[V2G20-065] Each V2G entity shall implement user datagram protocol according to IETF RFC 768.

7.7.3 Transport layer security (TLS)

7.7.3.1 Overview

Security on transport layer is being provided by using TLS. This allows establishment of an authenticated and encrypted channel between the EVCC and the SECC. TLS allows for unilateral or mutual authentication (ensures integrity protection and confidentiality protection). For security in the ISO 15118 series mutual authentication is used (the EVCC authenticates the SECC and the SECC authenticates the EVCC).

For transport layer security, the EVCC authenticates a public SECC using SECC certificate. This is being achieved by a public SECC having a private key corresponding to the SECC certificate and the EVCC verifying the certificate chain from the V2G root CA certificate to the SECC certificate. The revocation status check of sub-CA certificates and the SECC leaf certificate in the certificate chain is performed via the OCSP response received during TLS handshake (for details refer to IETF RFC 6066 as updated by IETF RFC 8446 and IETF RFC 8449).

The public SECC provides a certificate chain comprising its own SECC certificate and CPO sub-CA certificate(s) whose corresponding root certificate is possessed by the EVCC. Together with this certificate chain, the public SECC also sends the OCSP response for each certificate in the SECC certificate chain it sends to the EVCC.

Similarly, the EVCC authenticates private SECC using PE certificate. This is achieved by private SECC having a private key corresponding to the PE certificate and the EVCC verifying the certificate chain from the PE private root CA certificate to the PE certificate. The revocation status is usually not checked.

In this case, the private SECC provides a certificate chain comprising its own PE certificate and PE sub-CA certificate(s) whose corresponding root certificate is possessed by the EVCC.

In instances where the private SECC wants to provide PnC services (via usage of contract certificate(s)), the private SECC additionally provides OCSP responses for all certificates in its PE certificate chain, except for the PE private root CA certificate. EVCC performs the revocation status check of sub-CA certificates and the PE certificate in the certificate chain by utilizing the OCSP responses it received during the TLS handshake (for details refer to IETF RFC 6066 as updated by IETF RFC 8446 and IETF RFC 8449).

Likewise, the SECC authenticates EVCC using vehicle certificate. This is achieved by EVCC having a private key corresponding to the vehicle certificate and SECC verifying the certificate chain from the root certificate to the vehicle certificate. The public SECC checks the revocation status of the vehicle certificate chain while the private SECC typically does not check the revocation status of the vehicle certificate chain. The revocation status check of sub-CA certificates and the vehicle certificate in the certificate chain is performed via the OCSP responses (for details refer to IETF RFC 6066 as updated by IETF RFC 8446 and

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

IETF RFC 8449) or via CRLs (for details refer to IETF RFC 5280 as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399).

The EVCC provides a certificate chain comprising its own vehicle certificate and corresponding sub-CA certificate(s). The EVCC does not provide revocation status with the certificate chain it sends. The public SECC contacts the OCSP responder or CRL provider for revocation status of each certificate it received in the vehicle certificate chain from the EVCC. Similarly, if the private SECC offers PnC, the private SECC will contact the OCSP responder or CRL provider for revocation status of each certificate it received in the vehicle certificate chain from the EVCC.

7.7.3.2 Applicable RFCs

[V2G20-1264] For the considered use cases mutual authentication with TLS version 1.3 according to IETF RFC 8446 shall be supported by each V2G entity.

[V2G20-1521] TLS versions higher than 1.3 may also be supported.

[V2G20-2359] The EVCC or SECC may support TLS version 1.2 as specified in ISO 15118-2 for backwards compatibility.

NOTE 1 [V2G20-2356] applies if TLS 1.2 is negotiated.

NOTE 2 Refer to 7.7.3.10 for TLS 1.2 support.

NOTE 3 Table 5 describes which version of ISO spec is supported by what TLS mechanisms.

Table 5 — Supported communication protocols

TLS version	Communication protocols supported
1.3	– This document – ISO 15118-2
1.2	– ISO 15118-2
1.1 or earlier	– ISO 15118-2 EIM only
No TLS	– ISO 15118-2 EIM only – Communication specified in DIN SPEC 70121

[V2G20-2360] Random numbers used during TLS session setup shall follow requirements as specified by 7.3.7 and its subclauses.

[V2G20-2361] Session key(s) generated and used during TLS session shall be protected per the requirements as specified by 7.3.6 and its subclauses.

7.7.3.3 Transport layer security usage

[V2G20-2362] The EVCC shall always act as the TLS client component.

NOTE 1 Per IETF RFC 8446, since EVCC acts as the client, the EVCC will initiate the TLS session by sending the "ClientHello" message.

[V2G20-2363] The EVCC shall not request any application data until the TLS handshake is complete.

NOTE 2 Refer to IETF RFC 8446 for the definition of TLS handshake and when it is considered to be complete.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2609] The "nonce" sent by the EVCC in the "ClientHello" message shall have a minimum of 231 bits of entropy. Refer to 7.3.7 for details. Additional details can be found in IETF RFC 8446:2018, Annex C.1.

[V2G20-2364] The EVCC shall include the supported_versions extension described in IETF RFC 8446 as an extension in the "ClientHello" message.

[V2G20-2365] The EVCC shall include the version "0x0304" for TLS 1.3 in the supported_versions extension.

IETF RFC 8446 requires the "legacy_version" field to be mandatorily included in the "ClientHello" message. It also requires the "legacy_version" field to be mandatorily set to "0x0303".

[V2G20-2366] If an EVCC supports CPM4PE, the EV shall provide a methodology for authorized users to securely place the EVCC in CPM4PE. Refer to H.2.2.3 for details of CPM4PE.

NOTE 3 It is not in the scope of this document to define who the authorized user(s) of the EV are or how to recognize them.

NOTE 4 Similarly, it is not in the scope of this document to define the methodology for securely placing the EVCC in CPM4PE. In some cases it could be as simple as a button press while in others more sophisticated authorization methods could be required. Regardless of the methodology used, CPM4PE on EVCC can only be activated by explicit user interaction.

[V2G20-2367] The CPM4PE shall expire on the EVCC at least 120 s after the user activates the mode. Refer to H.2.2.3 for details of CPM4PE.

NOTE 5 Longer times are allowed but can result in user experience issues. For example, if the user does not actually want to perform the pairing between the particular EV and the particular private SECC, the user could still need to wait for the timeout period defined here before CPM4PE mode expires on the vehicle. Increasing the time the EV and the private SECC can pair, will also result in increased wait time in this example.

[V2G20-1006] While the EVCC is not in CPM4PE, it shall send a list of all the V2G root CA certificate(s) and PE private root CA certificate(s) it possesses via an extension of type "certificate_authorities" in the "ClientHello" message as defined in IETF RFC 8446. Refer to H.2.2.3 for details of CPM4PE.

NOTE 6 If the EVCC has V2G root CA certificate(s) and/or PE private root CA certificate(s) based on curves as defined by [V2G20-2674] and [V2G20-2319], it will include both in the "certificate_authorities" extension in the "ClientHello" message.

NOTE 7 The "authorities" element contains "DistinguishedName" of the V2G root CA certificate(s) and PE private root CA certificate(s) supported by the EVCC.

[V2G20-2368] The "DistinguishedName" (DN) of the V2G root CA certificate(s) and PE private root CA certificate(s) provided by the EVCC in "authorities" element of "certificate_authorities" extension in the "ClientHello" message shall include the following relative distinguished name (RDN) fields in the order specified below for each V2G root CA certificate and PE private root CA certificate supported by the EVCC and shall follow X501 and X509 for distinguished names:

- "Country" sub-sub-field from "Issuer" sub-field from "TBSCertificate" field of the V2G root CA certificate or PE private root CA certificate;
- "Organization" sub-sub-field from "Issuer" sub-field from "TBSCertificate" field of the V2G root CA certificate or PE private root CA certificate;

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

- "Organization Unit" sub-sub-field from "Issuer" sub-field from "TBSCertificate" field of the V2G root CA certificate or PE private root CA certificate;
- "Common Name" sub-sub-field from "Issuer" sub-field from "TBSCertificate" field of the V2G root CA certificate or PE private root CA certificate;
- "CertificateSerialNumber" sub-field from "TBSCertificate" field of the V2G root CA certificate or PE private root CA certificate.

NOTE 8 As specified by IETF RFC 8446, if a particular field/sub-field/sub-sub-field is not available in a particular V2G root CA certificate or PE private root CA certificate that RDN can be included, but left empty in the DistinguishedName (DN).

[V2G20-2369] If no V2G root CA certificate(s) and PE private root CA certificate(s) are available in the EVCC, "authorities" element of "certificate_authorities" extension in the "ClientHello" message shall be left empty.

[V2G20-2370] While the EVCC is in CPM4PE, it shall send an empty "authorities" element of "certificate_authorities" extension in the "ClientHello" message as defined in IETF RFC 8446 regardless if the EVCC has any V2G root CA certificate(s) and PE private root CA certificate(s) or not. Refer to H.2.2.3 for details of CPM4PE.

[V2G20-2371] The EVCC shall not include "oid_filters" extension in the "CertificateRequest" message it sends to the SECC.

[V2G20-2372] The EVCC shall include the extension "status_request" in the "ClientHello" message as defined in IETF RFC 8446.

[V2G20-2373] The EVCC shall include a zero-length "responder_id_list" sequence in the "ResponderID" field of "OCSPStatusRequest".

NOTE 9 "OCSPStatusRequest" is a field in "CertificateStatusRequest". "CertificateStatusRequest" makes up the "extension_data" field of "status_request" extension.

[V2G20-2374] The SECC shall always act as the TLS server component.

NOTE 10 Per IETF RFC 8446, since SECC acts as the server, the SECC will respond to the TLS session requests ("ClientHello") by sending the "ServerHello" message.

[V2G20-2375] The SECC shall not transmit any application data until the TLS handshake is complete.

NOTE 11 Refer to IETF RFC 8446 for the definition of TLS handshake and when it is considered to be complete.

[V2G20-2610] The "nonce" sent by the SECC in the "ServerHello" message shall have a minimum of 231 bits of entropy. Refer to 7.3.7 for details. Additional details can be found in IETF RFC 8446:2018, Annex C.1.

[V2G20-2376] If a private SECC supports CPM4PE, the private SECC shall provide a methodology for authorized users to securely place the private SECC in CPM4PE. Refer to H.2.2.3 for details of CPM4PE.

NOTE 12 It is not in the scope of this document to define who the authorized user(s) of the private SECC are or how to recognize them.

NOTE 13 Similarly, it is not in the scope of this document to define the methodology for securely placing the private SECC in CPM4PE. In some cases it could be as simple as a button press while in others more sophisticated

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

authorization methods could be required. Regardless of the methodology used, CPM4PE on private SECC can only be activated by explicit user interaction.

[V2G20-2377] The CPM4PE shall expire on the private SECC at least 120 s after the user activates the mode. Refer to H.2.2.3 for details of CPM4PE.

NOTE 14 Longer times can result in user experience issues.

[V2G20-1007] A public SECC shall send in the "ServerHello" message its own certificate chain (SECC certificate chain) including any necessary cross-certificates up to a root (excluding the root certificate itself), which shall be one of those roots previously indicated by the EVCC as being present in the EVCC.

[V2G20-2378] If the EVCC did not provide any indication of the available roots (i.e. the "authorities" element of "certificate_authorities" extension in the "ClientHello" message is empty), a public SECC shall send in the "ServerHello" message its own certificate chain (SECC certificate chain) including any necessary cross certificates up to a root (excluding the root certificate itself) of its own choosing.

[V2G20-2379] If the EVCC provides a list of the available roots (i.e. the "authorities" element of "certificate_authorities" extension in the "ClientHello" message is not empty), the public SECC shall follow IETF RFC 5280:2008, 7.1, as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399, to utilize the received "DistinguishedNames" (see [V2G20-1006]) to choose an SECC certificate chain originating from one of the received "DistinguishedNames" and provide it to the EVCC in "ServerHello" message as defined in IETF RFC 8446.

[V2G20-2380] If the EVCC offers and the public SECC chooses a named group and signature algorithm based on curves as defined by [V2G20-2674] (as per the configurable mechanism as defined by [V2G20-2320]), the SECC certificate chain provided by the public SECC in the "ServerHello" message shall be based on profiles as defined in B.4.1.

[V2G20-2381] If the EVCC offers and the public SECC chooses a named group and signature algorithm based on curves as defined by [V2G20-2319] (as per the configurable mechanism as defined by [V2G20-2320]), the SECC certificate chain provided by the public SECC in the "ServerHello" message shall be based on profiles as defined in B.4.2.

[V2G20-2382] A private SECC not in CPM4PE shall send the "ServerHello" message containing its own certificate chain (PE certificate chain) including any necessary cross-certificates up to a root (excluding the root certificate itself), which shall be one of those roots previously indicated by the EVCC as being present in the EVCC. Refer to H.2.2.3 for details of CPM4PE.

[V2G20-2383] If the EVCC provides a list of the available roots (i.e. the "authorities" element of "certificate_authorities" extension in the "ClientHello" message is not empty), the private SECC shall follow IETF RFC 5280:2008, 7.1 as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399, to utilize the received "DistinguishedNames" (see [V2G20-1006]) to choose a PE certificate chain originating from one of the received "DistinguishedNames" and provide it to the EVCC in "ServerHello" message as defined in IETF RFC 8446.

[V2G20-2384] If the EVCC did not provide any indication of the available roots (i.e. the EVCC the "authorities" element of "certificate_authorities" extension in the "ClientHello"

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

message is empty), a private SECC not in CPM4PE shall send in the "ServerHello" message its own certificate chain (PE certificate chain) including any necessary cross-certificates up to a root (excluding the root certificate itself) of its own choosing.

[V2G20-2385] A private SECC in CPM4PE shall disregard [V2G20-2383] and send the "ServerHello" message containing its own certificate chain (PE certificate chain) including any necessary cross-certificates and its PE private root CA certificate. Refer to H.2.2.3 for details of CPM4PE.

[V2G20-2386] If the EVCC offers and private SECC chooses a named group and signature algorithm based on curves as defined by [V2G20-2674] (as per the configurable mechanism as defined by [V2G20-2320]), the PE certificate chain provided by the private SECC in the "ServerHello" message shall be based on profiles as defined in B.10.1.

[V2G20-2387] If the EVCC offers and private SECC chooses a named group and signature algorithm based on curves as defined by [V2G20-2319] (as per the configurable mechanism as defined by [V2G20-2320]), the PE certificate chain provided by the private SECC in the "ServerHello" message shall be based on profiles as defined in B.10.2.

[V2G20-2388] Since the EVCC used the "status_request" extension to request OCSP response for the certificate chain sent by the public SECC, it shall include an OCSP response for each certificate in the certificate chain sent by the public SECC in the "ServerHello" message. Refer to IETF RFC 6960 (as updated by IETF RFC 8954) and IETF RFC 8446 for further details.

NOTE 15 If the public SECC is deployed in a stand-alone application without internet connection or is operating in a semi-online manner without internet connection, the public SECC will not be able to provide the OCSP response.

[V2G20-2389] If the EVCC offers and the public SECC chooses a named group and signature algorithm based on curves as defined by [V2G20-2674] (as per the configurable mechanism as defined by [V2G20-2320]), the OCSP certificate chain(s) provided by the public SECC in the "ServerHello" message shall be based on profiles as defined in B.9.1.

NOTE 16 In these cases, the OCSP responses are signed using signature algorithm based on curves as defined by [V2G20-2674].

[V2G20-2390] If the EVCC offers and the public SECC chooses a named group and signature algorithm based on curves as defined by [V2G20-2319] (as per the configurable mechanism as defined by [V2G20-2320]), the OCSP certificate chain(s) provided by the public SECC in the "ServerHello" message shall be based on profiles as defined in B.9.2.

NOTE 17 In these cases, the OCSP responses are signed using signature algorithm based on curves as defined by [V2G20-2319].

[V2G20-2391] Since the EVCC used the "status_request" extension to request OCSP response for the certificate chain sent by private SECC, if the private SECC supports PnC, it shall include an OCSP response for each certificate in the certificate chain sent by the private SECC in the "ServerHello" message. Refer to IETF RFC 6960 (as updated by IETF RFC 8954) and IETF RFC 8446 for further adetails.

[V2G20-2392] If the EVCC offers and the private SECC chooses a named group and signature algorithm based on curves as defined by [V2G20-2674] (as per the configurable mechanism as defined by [V2G20-2320]), the OCSP certificate chain(s) provided by

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

the private SECC in the "ServerHello" message shall be based on profiles as defined in B.9.1.

NOTE 18 In these cases, the OCSP responses are signed using signature algorithm based on curves as defined by [V2G20-2674].

[V2G20-2393] If the EVCC offers and the private SECC chooses a named group and signature algorithm based on curves as defined by [V2G20-2319] (as per the configurable mechanism as defined by [V2G20-2320]), the OCSP certificate chain(s) provided by the private SECC in the "ServerHello" message shall be based on profiles as defined in B.9.2.

NOTE 19 In these cases, the OCSP responses are signed using signature algorithm based on curves as defined by [V2G20-2319].

[V2G20-1021] The validity period of the OCSP response provided by the SECC shall be limited to one week.

NOTE 20 If cached, each OCSP response can be updated at least once a week.

The validity period is left to the discretion of the OCSP responder. The OCSP response validity cannot be longer than as specified by [V2G20-1021], but it can be shorter than specified by [V2G20-1021].

[V2G20-1008] In the case where the OCSP response for a certificate was not signed by the issuing CA of the certificate (V2G root CA, CSO sub-CA1, CSO sub-CA2 or any cross-certified CA), each OCSP response shall contain the associated OCSP responder's certificate chain including any necessary cross-certificates and each certificate in the chain (except the OCSP signer certificate) shall include the AuthorityInfoAccess extension field.

NOTE 21 As defined in IETF RFC (as updated by IETF RFC 8954), an OCSP responder might either be the sub-CA itself, or it might be an entity which is directly signed by the corresponding sub-CA/root CA using a key pair with a special extended key usage flag in the certificate.

[V2G20-2394] Each of the OCSP responses provided by the public SECC in the "ServerHello" message shall be signed by a certificate derived from one of the V2G root CA certificates supported by the EVCC (EVCC provided a list of the V2G certificates via [V2G20-1006]).

[V2G20-2395] Each of the OCSP responses provided by the private SECC in the "ServerHello" message shall be signed by a certificate derived from one of the PE private root CA certificates supported by the EVCC (EVCC provided a list of the V2G certificates via [V2G20-1006] or it received from the private SECC via [V2G20-2385]).

[V2G20-2396] If the OCSP response for a particular certificate is not available from an OCSP responder that has a certificate derived from one of the V2G root CA certificates supported by the EVCC (EVCC provided a list of the V2G certificates via [V2G20-1006]), the public SECC shall omit providing OCSP response for that certificate in the "ServerHello" message.

[V2G20-2397] If the OCSP response for a particular certificate is not available from an OCSP responder that has a certificate derived from one of the PE private root CA certificates supported by the EVCC (EVCC provided a list of the V2G certificates via [V2G20-1006] or it received from the private SECC via [V2G20-2385]), private SECC shall omit providing OCSP response for that certificate in the "ServerHello" message.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2398] A private SECC not supporting PnC can ignore the "status_request" extension, and continue as if the EVCC never sent that request. Refer IETF RFC 8446 for further details.

NOTE 22 A private SECC not supporting PnC is allowed to function in an offline mode where it cannot provide OCSP response for its PE certificate chain.

A private SECC supporting PnC is required to provide OCSP response for its PE certificate chain.

[V2G20-2399] If the public SECC cannot provide a certificate with a chain up to one of the roots, which the EVCC signaled as being present in the EVCC, the public SECC shall provide within the TLS handshake a valid certificate including a chain to a root certificate (the root certificate itself shall not be transmitted).

[V2G20-2400] The SECC shall request EVCC to send the EVCC's certificate via "CertificateRequest" message.

NOTE 23 This allows setting up a mutually authenticated TLS session where both the EVCC and SECC verify the authenticity of each other.

[V2G20-2401] A public SECC shall send a list of all V2G root CA certificate(s) and/or OEM root CA certificate(s) it possesses via the "certificate_authorities" extension in the "CertificateRequest" message it sends to the EVCC.

NOTE 24 Refer to IETF RFC 8446.

NOTE 25 The "authorities" element contains "DistinguishedName" of the V2G root CA certificate(s) and/or OEM root CA certificate(s) supported by the SECC.

[V2G20-2402] A private SECC not in CPM4PE shall send a list of all V2G root CA certificate(s) and/or OEM root CA certificate(s) it possesses via the "certificate_authorities" extension in the "CertificateRequest" message it sends to the EVCC.

NOTE 26 Refer to IETF RFC 8446.

NOTE 27 The "authorities" element contains "DistinguishedName" of the V2G root CA certificate(s) and/or OEM root CA certificate(s) supported by the private SECC.

[V2G20-2403] The "DistinguishedName" (DN) of the V2G root CA certificate(s) and/or OEM root CA certificate(s) provided by the public SECC or private SECC not in CPM4PE in the "authorities" element of "certificate_authorities" extension in the "CertificateRequest" message shall include the following relative distinguished name (RDN) fields in the order specified below for each V2G root CA certificate and OEM root CA certificate supported by the public SECC or private SECC not in CPM4PE and shall follow X501 and X509 for distinguished names:

- "Country" sub-sub-field from "Issuer" sub-field from "TBSCertificate" field of the V2G root CA certificate or OEM root CA certificate;
- "Organization" sub-sub-field from "Issuer" sub-field from "TBSCertificate" field of the V2G root CA certificate or OEM root CA certificate;
- "Organization Unit" sub-sub-field from "Issuer" sub-field from "TBSCertificate" field of the V2G root CA certificate or OEM root CA certificate;
- "Common Name" sub-sub-field from "Issuer" sub-field from "TBSCertificate" field of the V2G root CA certificate or OEM root CA certificate;
- "CertificateSerialNumber" sub-field from "TBSCertificate" field of the V2G root CA certificate or OEM root CA certificate.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 28 As specified by IETF RFC 8446, if a particular field/sub-field/sub-sub-field is not available in a particular V2G root CA certificate or OEM root CA certificate that RDN can be included but left empty in the DistinguishedName (DN).

[V2G20-2404] If no V2G root CA certificate and OEM root CA certificate is/are available in the public SECC or private SECC not in CPM4PE, the "authorities" element of "certificate_authorities" extension in the "CertificateRequest" message shall be left empty.

[V2G20-2405] A private SECC in CPM4PE shall send an empty "authorities" element of "certificate_authorities" extension in the "CertificateRequest" message as defined in IETF RFC 8446. Refer to H.2.2.3 for details of CPM4PE.

[V2G20-2406] SECC shall not include "oid_filters" extension in the "CertificateRequest" message it sends to the EVCC.

[V2G20-2407] SECC shall not include "status_request" extension in the "CertificateRequest" message it sends to the EVCC.

NOTE 29 "status_request" extension requires EVCC to provide OCSP response for its certificate.

[V2G20-2408] Although a valid time in the EVCC is not mandatory, the EVCC should implement a mechanism to discard outdated certificates from the SECC.

NOTE 30 It is not in the scope of this document how errors with EVCC time are handled. It is up to the OEM how these errors are handled.

[V2G20-2409] The EVCC shall validate, according to [V2G20-1001], [V2G20-2324] and [V2G20-2325], the certificate chain that was provided by the SECC during the TLS handshake.

[V2G20-1240] When the EVCC receives the certificate chain in TLS handshake, it validates it per [V2G20-2409]. During this certificate validation, the EVCC shall check the revocation status of the certificates it received in the certificate chain from the public SECC. This revocation check shall be performed via an OCSP response according to IETF RFC 6960 (as updated by IETF RFC 8446).

NOTE 31 In most cases the EVCC will receive the OCSP response from the SECC in the "ServerHello" message.

NOTE 32 The EVCC can determine that the received certificate chain is linked to a V2G root CA certificate. In that case, the received certificate is an SECC certificate and the EVCC is connected to a public SECC.

[V2G20-2410] When the EVCC receives the certificate chain in TLS handshake, it validates it per [V2G20-2409]. During this certificate validation, if the EVCC received OCSP response for any of the certificates in the certificate chain it received from the private SECC, the EVCC shall check the revocation status of the certificates it received in the certificate chain from the private SECC. This revocation check shall be performed via an OCSP response according to IETF RFC 6960 (as updated by IETF RFC 8954) and IETF RFC 8446.

NOTE 33 The EVCC can determine that the received certificate chain is linked to a PE private root CA certificate. In that case, the received certificate is a PE certificate and the EVCC is connected to a private SECC in a private environment.

NOTE 34 A private SECC can provide OCSP responses or choose not to. If the private SECC did provide OCSP response for any one of the certificates in the PE certificate chain, then the revocation status can be checked for each certificate in the PE certificate chain.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2411] If the OCSP status of any certificate in SECC certificate chain is not provided by the public SECC in the "ServerHello", the EVCC may contact the OCSP server listed in the said certificate for the OCSP status of that certificate.

NOTE 35 The EVCC can determine that the received certificate chain is linked to a V2G root CA certificate. In that case, the received certificate is a SECC certificate and the EVCC is connected to a public SECC.

NOTE 36 It is not in the scope of this document to specify the methodology for the EVCC to contact the OCSP server directly.

[V2G20-2412] If the private SECC provided OCSP status of at least one but not all of the certificates in the PE certificate chain in the "ServerHello", the EVCC may contact the OCSP server listed in the said certificate for the OCSP status of that certificate.

NOTE 37 The EVCC can determine that the received certificate chain is linked to a PE private root CA certificate. In that case, the received certificate is a PE certificate and the EVCC is connected to a private SECC in a private environment.

NOTE 38 It is not in the scope of this document to specify the methodology for the EVCC to contact the OCSP server directly.

[V2G20-2413] Per IETF RFC 6960 (as updated by IETF RFC 8954), the EVCC will verify the OCSP responder certificate before accepting the OCSP response. If the EVCC is unable to successfully verify the OCSP responder certificate (e.g. when the OCSP responder's certificate is derived from a root not trusted by the EVCC) for any of the OCSP responses, the EVCC shall consider the entire SECC/PE certificate chain to have failed validation.

[V2G20-2414] Per IETF RFC 6960 (as updated by IETF RFC 8954), the EVCC will verify the signature on the received OCSP response. If the EVCC is unable to successfully verify the signature on the OCSP response (e.g. when the signature on the response does not match the signature calculated by the EVCC using the OCSP responder's certificate) for any of the OCSP responses, the EVCC shall consider the entire SECC/PE certificate chain to have failed validation.

[V2G20-2415] If the certificate status of any certificate in the received SECC/PE certificate chain is not "good", the EVCC shall consider the entire SECC/PE certificate chain to have failed validation.

NOTE 39 Refer to IETF RFC 6960 (as updated by IETF RFC 8954) for further details of the certificate status as provided by OCSP server.

[V2G20-2416] If the revocation status of any certificate in the received SECC certificate chain from the SECC is not available or cannot be determined, the EVCC shall consider the entire SECC certificate chain to have failed validation.

NOTE 40 The EVCC can determine that the received certificate chain is linked to a V2G root CA certificate. In that case, the received certificate is an SECC certificate and the EVCC is connected to a public SECC.

[V2G20-2417] If the revocation status of at least one certificate of the received PE certificate chain from the private SECC is available, but the revocation status of all other certificates of the received PE certificate chain from the private SECC is not available or cannot be determined, the EVCC shall consider the entire PE certificate chain to have failed validation.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 41 The EVCC can determine that the received certificate chain is linked to a PE private root CA certificate. In that case, the received certificate is a PE certificate and the EVCC is connected to a private SECC in a private environment.

[V2G20-2418] If the EVCC determines that the certificate chain it received during TLS session setup process is a PE certificate chain and the private SECC did not provide OCSP response for any of the certificates in the PE certificate chain, the EVCC shall ignore the fact that the private SECC has not sent OCSP responses. The EVCC shall continue with the PE certificate chain validation without the certificate revocation check as specified by [V2G20-1001].

NOTE 42 The EVCC can determine that the received certificate chain is linked to a PE private root CA certificate. In that case, the received certificate is a PE certificate and the EVCC is connected to a private SECC in a private environment.

[V2G20-2419] If the EVCC is in CPM4PE and it successfully validated the received certificate chain and the received chain contains a root CA certificate, the EV shall assume that the certificate it received during TLS session setup process is a PE certificate chain from the private SECC and the EVCC shall store the received root CA certificate as a PE private root CA certificate that it trusts for TLS session setup only. Refer to H.2.2.3 for details of CPM4PE.

NOTE 43 Refer to H.2 and its subclauses for details of PE and risks with PE certificate chains. Also refer to 7.3.2.2 for further details of risks with PE certificate chains.

[V2G20-2420] The CPM4PE shall expire on the EVCC after the PE private root CA certificate has been installed per [V2G20-2419].

[V2G20-2421] If the SECC has provided a certificate chain that does not trace up to a V2G root CA certificate or a PE private root CA certificate that the EVCC contains/possesses, the EVCC shall only accept such a certificate, if it successfully validated the certificate chain using an out of band validation mechanism (e.g. server based certificate validation protocol, SCVP, according to IETF RFC 5055). If the validation using such a service is not done, gives a negative result or fails (e.g. due to missing connectivity), the EVCC shall treat the SECC/PE certificate chain as failed validation.

NOTE 44 It is not in the scope of this document to specify the methodology for an out of band certificate validation mechanism.

[V2G20-2422] If the EVCC is unable to validate SECC/PE certificate chain successfully, the EVCC shall abort the TLS session setup process and apply [V2G20-1805].

NOTE 45 This requirement applies regardless of why the SECC/PE certificate chain validation failed. For example, the validation could have failed due to missing OCSP response or because one of the certificates in the SECC certificate chain was revoked, etc.

[V2G20-2423] When the EVCC receives a "CertificateRequest" message, the EVCC shall check that extension "status_request" is not present in the "CertificateRequest" message. If extension "status_request" is present in the "CertificateRequest" message, the EVCC shall disregard this extension and continue with the TLS handshake as if the "CertificateRequest" message did not contain those extension(s).

[V2G20-2424] In response to a "CertificateRequest" message, the EVCC shall send a "Certificate" message containing its own certificate chain (vehicle certificate chain) including any necessary cross-certificates up to the corresponding root (excluding the root

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

certificate itself), which shall be one of those roots previously indicated by the SECC as being present in the SECC.

[V2G20-2426] If the SECC provides a list of the available roots (i.e. the "authorities" element of "certificate_authorities" extension in the "CertificateRequest" message is not empty), the EVCC shall follow IETF RFC 5280, 7.1, as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399, to utilize the received "DistinguishedNames" (see [V2G20-2401]) to choose a vehicle certificate chain originating from one of the received "DistinguishedNames" and provide it to the SECC in "CertificateRequest" message as defined in IETF RFC 8446.

[V2G20-2427] If the public SECC did not provide any indication of the available roots (i.e. the "authorities" element of "certificate_authorities" extension in the "CertificateRequest" message is empty), the EVCC shall send a "Certificate" message containing its own certificate chain (vehicle certificate chain) including any necessary cross-certificates up to the corresponding root (excluding the root certificate itself) of its own choosing.

NOTE 46 The EVCC can determine that the received certificate chain is linked to a V2G root CA certificate. In that case, the received certificate is an SECC certificate and the EVCC is connected to a public SECC.

[V2G20-2428] If the private SECC did not provide any indication of the available roots (i.e. the "authorities" element of "certificate_authorities" extension in the "CertificateRequest" message is empty), an EVCC not in CPM4PE shall send a "Certificate" message containing its own certificate chain (vehicle certificate chain) including any necessary cross-certificates up to the corresponding root (excluding the root certificate itself) of its own choosing.

NOTE 47 The EVCC can determine that the received certificate chain is linked to a PE private root CA certificate. In that case, the received certificate is a PE certificate and the EVCC is connected to a private SECC in a private environment.

[V2G20-2429] If the EVCC cannot provide a certificate with a chain up to one of the roots, which the SECC signaled as being present in the SECC, the EVCC shall provide within the TLS handshake a valid certificate including a chain to a root certificate (the root certificate itself shall not be transmitted).

NOTE 48 It is assumed that the EVCC is not in CPM4PE.

[V2G20-2430] If the named group and signature algorithm selected for the TLS session are based on curves as defined by [V2G20-2674] (as per the configurable mechanism as defined by [V2G20-2320]), the vehicle certificate chain provided by the EVCC in the "Certificate" message shall be based on profiles as defined in B.8.1.

[V2G20-2431] If the named group and signature algorithm selected for the TLS session are based on curves as defined by [V2G20-2319] (as per the configurable mechanism as defined by [V2G20-2320]), the vehicle certificate chain provided by the EVCC in the "Certificate" message shall be based on profiles as defined in B.8.2.

[V2G20-2432] The public SECC shall validate, according to according to [V2G20-1001], [V2G20-2324] and [V2G20-2325], the certificate chain that was provided by the EVCC during the TLS handshake. During the EVCC certificate chain validation the public SECC shall check revocation status of the certificates in the EVCC's certificate chain.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2433] The private SECC shall validate, according to [V2G20-1001], [V2G20-2324] and [V2G20-2325], the certificate chain that was provided by the EVCC during the TLS handshake. During the vehicle certificate chain validation, a private SECC not supporting PnC is not mandated to check revocation status of the certificates in the EVCC's certificate chain.

[V2G20-2434] The private SECC shall validate, according to [V2G20-1001], [V2G20-2324] and [V2G20-2325], the certificate chain that was provided by the EVCC during the TLS handshake. During the vehicle certificate chain validation, a private SECC supporting PnC shall check revocation status of the certificates in the EVCC's certificate chain.

[V2G20-2437] Depending on whether the OEM supports OCSP services or CRL or both for the certificates in vehicle certificate chain, the SECC is free to utilize either OCSP or CRL or both for vehicle certificate revocation check.

NOTE 49 If the vehicle certificate chain contains AuthorityInfoAccess, the SECC can check the revocation status of the certificates in the EVCC's certificate chain via an OCSP response according to IETF RFC 8446. Refer to 7.7.3.3.1 for further details.

NOTE 50 If the vehicle certificate chain contains CRLDistributionPoints, the SECC can check the revocation status of the certificates in the EVCC's certificate chain via a CRL according to IETF RFC 5280, as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399. Refer to 7.7.3.3.2 for further details.

NOTE 51 The SECC can receive the revocation status of the vehicle certificate chain from SA or can contact the referenced CRL distribution point/OCSP responder for this status. It is not in the scope of this document to specify the methodology for the SECC to contact the CRL distribution point/OCSP server directly or the SA.

NOTE 52 It is not in the scope of this document to specify the methodology for the SECC to indicate to CRL distribution point/OCSP server/another SA of the named group and signature algorithm that the SECC would like to use. The named group and signature algorithm used for this purpose can be same as those selected for the TLS session (as per the configurable mechanism as defined by [V2G20-2320]).

NOTE 53 It is not advisable to check both OCSP response and CRL for certificate revocation check. If the SECC does want to check both then the response of both can be "good" to consider the said certificate valid. If either of the responses does not indicate "good" then the said certificate can be considered invalid.

[V2G20-2438] If the certificate status of any certificate in vehicle certificate chain is not "good", the SECC shall consider that the received vehicle certificate chain has failed validation.

NOTE 54 Refer to IETF RFC 6960 (as updated by IETF RFC 8954) for further details of the certificate status as provided by OCSP server.

[V2G20-2439] If the revocation status of any certificate in vehicle certificate chain is not available or cannot be determined, the public SECC shall consider that the received vehicle vertificate chain has failed validation.

[V2G20-2440] If the revocation status of any certificate in vehicle certificate chain is not available or cannot be determined, the private SECC supporting PnC shall consider that the received vehicle certificate chain has failed validation.

NOTE 55 This requirement does not apply to a private SECC that does not support PnC.

[V2G20-2441] If the revocation status of any certificate in vehicle certificate chain is not available or cannot be determined, per [V2G20-2433], the private SECC not supporting PnC can continue validation of the received vehicle certificate chain.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 56 It is up to the discretion of the PE operator whether a private SECC that does not support PnC can check the revocation status of any certificate in vehicle certificate chain or not. This document does not mandate this check.

[V2G20-2442] If the EVCC has provided a certificate chain that does not trace up to a root certificate that is trusted by the SECC, the SECC shall only accept such a certificate, if it successfully validated the certificate chain using an out of band validation mechanism (e.g. server based certificate validation protocol, SCVP, according to IETF RFC 5055). If the validation using such a service is not done, gives a negative result or fails (e.g. due to missing connectivity), the SECC shall consider that the received vehicle certificate chain has failed validation.

NOTE 57 It is not in the scope of this document to specify the methodology for an out of band certificate validation mechanism.

[V2G20-2443] If the SECC is unable to validate received vehicle certificate chain successfully, the SECC shall abort the TLS session setup process and apply [V2G20-1805].

NOTE 58 This requirement applies regardless of why the vehicle certificate chain validation failed. For example, the validation could have failed due to missing OCSP response or because one of the certificates in the vehicle certificate chain was revoked, etc.

[V2G20-2444] If the private SECC is in CPM4PE and it successfully validated the received certificate chain and the received chain contains a root CA certificate, the private SECC shall store the received root CA certificate as an OEM/V2G root CA certificate that it trusts for TLS session setup only. Refer to H.2.2.3 for details of CPM4PE.

[V2G20-2445] The CPM4PE shall expire on the private SECC after the OEM/V2G root CA certificate has been installed per [V2G20-2444].

[V2G20-2446] The SECC shall support maximum fragment length negotiation according to IETF RFC 6066.

[V2G20-2447] The SECC shall be able to support, but not be limited to, a maximum fragment length of 2^9 bytes according to IETF RFC 6066.

7.7.3.3.1 Vehicle certificate revocation check via OCSP

[V2G20-2448] The validity period of the OCSP response provided for a vehicle certificate shall not be longer than one week.

NOTE 1 Each OCSP response can be updated at least once every one week.

The validity period is left to the discretion of the OCSP responder. The OCSP response validity cannot be longer than specified by [V2G20-2448], but it can be shorter than specified by [V2G20-2448].

[V2G20-2449] In the case where the OCSP response for a certificate was not signed by the issuing CA of the certificate (V2G root CA, OEM root CA, OEM sub-CA1, OEM sub-CA2 or any corresponding cross-certified CA), each OCSP response shall contain the associated OCSP responder's certificate chain up to, but not including, the corresponding root. If a cross-certificate is used, the OCSP responder's certificate chain shall including any necessary cross-certificates. Each certificate in the OCSP signer certificate chain (except the OCSP signer certificate itself and the root certificate) shall include the AuthorityInfoAccess extension.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 2 As defined in IETF RFC 6960 (as updated by IETF RFC 8954), an OCSP responder can either be the sub-CA itself, or it can be an entity which is directly signed by the corresponding sub-CA/root CA using a key pair with a special extended key usage flag in the certificate.

[V2G20-2450] Each of the OCSP responses received by the SECC should be signed by a certificate derived from one of the root certificates supported by the SECC.

NOTE 3 It is not in the scope of this document to define the methodology used by the SECC to indicate to the OCSP responder the roots that are trusted by the SECC. Refer to IETF RFC 6960 (as updated by IETF RFC 8954) for further details.

[V2G20-2451] Per IETF RFC 6960 (as updated by IETF RFC 8954), the SECC will verify the OCSP responder certificate before accepting the OCSP response. If the SECC is unable to successfully authenticate the OCSP responder certificate (e.g. when the OCSP responder's certificate is derived from a root not trusted by the SECC), the SECC shall consider the received vehicle certificate chain to have failed validation.

[V2G20-2452] Per IETF RFC 6960 (as updated by IETF RFC 8954), the SECC will verify the signature on the received OCSP response. If the SECC is unable to successfully verify the signature on the OCSP response (e.g. when the signature on the response does not match the signature calculated by the SECC using the OCSP responder's certificate), the SECC shall consider the received vehicle certificate chain to have failed validation.

7.7.3.3.2 Vehicle certificate revocation check via CRL

[V2G20-2453] The validity period of the CRL provided for a vehicle certificate shall not be longer than 1 week.

NOTE 1 Each CRL can be updated at least once every one week. The validity period is left to the discretion of the CRL issuer. The CRL validity cannot be longer than as specified by [V2G20-2453], but it can be shorter than specified by [V2G20-2453].

[V2G20-2454] In the case where the CRL for a certificate was not signed by the issuing CA of the certificate (V2G root CA, OEM root CA, OEM sub-CA1, OEM sub-CA1, OEM sub-CA2 or any corresponding cross-certified CA), each CRL shall contain the associated CRL issuer's certificate chain up to, but not including, the corresponding root. If a cross-certificate is used, the CRL issuer's certificate chain shall including any necessary cross-certificates. Each certificate in the CRL certificate chain (except the CRL certificate itself and the root certificate) shall include the CRLDistributionPoints extension.

NOTE 2 As defined in IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399), a CRL issuer can either be the sub-CA itself, or it can be an entity which is directly signed by the corresponding sub-CA/root CA using a key pair with a special extended key usage flag in the certificate.

[V2G20-2455] Each of the CRL received by the SECC should be signed by a certificate derived from one of the root certificates supported by the SECC.

NOTE 3 It is not in the scope of this document to define the methodology used by the SECC to indicate to the CRL issuer the roots that are trusted by the SECC. Refer to IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399) for further details.

[V2G20-2456] Per IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399), the SECC will verify the CRL issuer certificate before accepting the CRL. If the SECC is unable to successfully authenticate the CRL issuer certificate (e.g. when the CRL issuer's certificate is derived from a root not trusted by the SECC), the SECC shall consider the received vehicle certificate chain to have failed validation.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2457] Per IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399), the SECC will verify the signature on the received CRL. If the SECC is unable to successfully verify the signature on the CRL (e.g. when the signature on the response does not match the signature calculated by the SECC using the CRL issuer's certificate), the SECC shall consider the received vehicle certificate chain to have failed validation.

7.7.3.4 Transport layer security credentials and cipher suites

[V2G20-2458] The SECC shall support all cipher suites defined in Table 6.

[V2G20-1856] The SECC shall include the cipher suites in the order as they appear in Table 6.

NOTE 1 Cipher suites listed in Table 6 are cataloged in the order of preference with the most preferred cipher suite first.

[V2G20-1857] When selecting the cipher suite from the list of cipher suites received in the "cipher_suites" field of the received "ClientHello" message, the SECC shall give preference to the most preferred cipher suite that the SECC supports.

NOTE 2 Cipher suites are listed in the "cipher_suites" field in the order of preference with the most preferred cipher suite first.

[V2G20-2459] The EVCC shall support all cipher suites defined in Table 6.

[V2G20-1858] The EVCC shall include the cipher suites in the order as they appear in Table 6.

NOTE 3 Cipher suites listed in Table 6 are cataloged in the order of preference with the most preferred cipher suite first.

[V2G20-1860] When transmitting the list of supported cipher suites in the "cipher_suites" field of the "ClientHello" message, the EVCC shall list the cipher suites that the EVCC supports in the order of preference of the EVCC.

NOTE 4 Cipher suites are listed in the "cipher_suites" field in the order of preference with the most preferred cipher suite first.

Table 6 — Supported cipher suites

Cipher suite	RFC
TLS_AES_256_GCM_SHA384	IETF RFC 5116
TLS_CHACHA20_POLY1305_SHA256	IETF RFC 8439

NOTE 5 Multiple algorithms are integrated to allow for cryptographic agility. Implementers can provide a configuration mechanism to securely prevent the usage of a particular algorithm, e.g. in case a security flaw was found in the preferred cipher suite. The design and implementation of that configuration mechanism is not in the scope of this document.

[V2G20-1634] The SECC shall support all named groups defined in Table 7.

[V2G20-2460] When selecting the named group from the list of named groups received in the "supported_groups" extension field of the received "ClientHello" message, the SECC shall give preference to the most preferred named group that the SECC supports. The SECC's/private SECC's preference shall be determined by Table 7 and the configurable mechanism as defined by [V2G20-2320].

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 6 Named groups are listed in the "supported_groups" extension field in the order of preference of the EVCC with the most preferred named group first.

NOTE 7 Named groups listed in Table 7 are cataloged in the order of preference with the most preferred named group first.

NOTE 8 When the configurable mechanism as defined by [V2G20-2320] indicates that the curve as defined by [V2G20-2674] needs to be used, named group "secp521r1" is given preference. When the configurable mechanism as defined by [V2G20-2320] indicates that the curve as defined by [V2G20-2319] needs to be used, named group "x448" is given preference.

[V2G20-1637] The EVCC shall support all named groups defined in Table 7.

[V2G20-1638] The EVCC shall include the named groups in the order as they appear in Table 7 or as per the configurable mechanism as defined by [V2G20-2320].

NOTE 9 Named groups listed in Table 7 are cataloged in the order of preference with the most preferred named group first.

NOTE 10 When the configurable mechanism as defined by [V2G20-2320] indicates that the curve as defined by [V2G20-2674] needs to be used, named group "secp521r1" is given preference. When the configurable mechanism as defined by [V2G20-2320] indicates that the curve as defined by [V2G20-2319] needs to be used, named group "x448" is given preference.

[V2G20-1639] When transmitting the list of supported named groups in the "supported_groups" extension field of the "ClientHello" message, the EVCC shall list the named groups that the EVCC supports in the order of preference of the EVCC.

NOTE 11 Named groups are listed in the "supported_groups" extension field in the order of preference with the most preferred named group first.

NOTE 12 The configurable mechanism as defined by [V2G20-2320] indicates EVCC's preference.

Table 7 — Supported named groups

Named group	Standards
secp521r1	IETF RFC 8446
x448	IETF RFC 8446

NOTE 13 Multiple named groups are integrated to allow for cryptographic agility. Implementers can provide a configuration mechanism to securely prevent the usage of a particular named group, e.g. in case a security flaw was found in the preferred named group. The design and implementation of that configuration mechanism is beyond the scope of this document. It is important that the implementers are careful that this mechanism cannot be used nefariously to downgrade to an insecure named group.

NOTE 14 The configurable mechanism as defined by [V2G20-2320] can be used for this purpose.

[V2G20-1663] The EVCC shall also include the list of supported named groups in the "client_shares" field of the "KeyShareClientHello" value of the "key_share" extension in the "ClientHello" message.

[V2G20-1664] The supported named groups included in the "client_shares" field of the "KeyShareClientHello" value of the "key_share" extension in the "ClientHello" message shall be in the order of preference of the EVCC.

NOTE 15 The configurable mechanism as defined by [V2G20-2320] indicates EVCC's preference.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

[V2G20-1665] The SECC shall include the selected named group in the "server_share" field of the "KeyShareServerHello" value of the "key_share" extension in the "ServerHello" message.

NOTE 16 The configurable mechanism as defined by [V2G20-2320] indicates SECC's preference.

[V2G20-1666] The SECC shall support all signature algorithms defined in Table 8.

[V2G20-1667] The SECC shall include the signature algorithms in the order as they appear in Table 8.

[V2G20-1668] When selecting the signature algorithm from the list of signature algorithms received in the "signature_algorithms" and/or "signature_algorithms_cert" extension field(s) of the received "ClientHello" message (per IETF RFC 8446, extension "signature_algorithms_cert" is optional), the SECC shall give preference to the most preferred signature algorithm that the SECC supports. The SECC's/private SECC's preference shall be determined by Table 8 and the configurable mechanism as defined by [V2G20-2320].

NOTE 17 Signature algorithms are listed in the "signature_algorithms" and/or "signature_algorithms_cert" extension field(s) in the order of preference of the EVCC with the most preferred signature algorithm first.

NOTE 18 Signature algorithms listed in Table 8 are cataloged in the order of preference with the most preferred signature algorithm first.

NOTE 19 When the configurable mechanism as defined by [V2G20-2320] indicates that the curve as defined by [V2G20-2674] needs to be used, signature algorithm "ecdsa_secp521r1_sha512" is given preference. When the configurable mechanism as defined by [V2G20-2320] indicates that the curve as defined by [V2G20-2319] needs to be used, signature algorithm "ed448" is given preference.

[V2G20-2461] The signature algorithm selected by the SECC shall be compatible with the selected named group.

NOTE 20 For example, the SECC can decide not select signature algorithm based on curve as defined by [V2G20-2674] while selecting named group based on curve as defined by [V2G20-2319].

[V2G20-1669] The EVCC shall support all signature algorithms defined in Table 8.

[V2G20-1670] The EVCC shall include the signature algorithms in the order as they appear in Table 8.

NOTE 21 Signature algorithms listed in Table 8 are catalogued in the order of preference with the most preferred signature algorithm first.

NOTE 22 When the configurable mechanism as defined by [V2G20-2320] indicates that the curve as defined by [V2G20-2674] needs to be used, signature algorithm "ecdsa_secp521r1_sha512" is given preference. When the configurable mechanism as defined by [V2G20-2320] indicates that the curve as defined by [V2G20-2319] needs to be used, signature algorithm "ed448" is given preference.

[V2G20-1671] When transmitting the list of supported signature algorithms in the "signature_algorithms" and/or "signature_algorithms_cert" extension field(s) of the "ClientHello" message (per IETF RFC 8446, extension signature_algorithms_cert is optional), the EVCC shall list the signature algorithms that the EVCC supports in the order of preference of the EVCC.

NOTE 23 Signature algorithms are listed in the "signature_algorithms" and/or "signature_algorithms_cert" extension field(s) in the order of preference with the most preferred signature algorithm first.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 24 The configurable mechanism as defined by [V2G20-2320] indicates EVCC preference.

Table 8 — Supported signature algorithms

Signature algorithms	Standards
ecdsa_secp521r1_sha512	ANSI X9.62
ed448	IETF RFC 8032

NOTE 25 Multiple signature algorithms are integrated to allow for cryptographic agility. Implementers can provide a configuration mechanism to securely prevent the usage of a particular signature algorithm, e.g. in case a security flaw was found in the preferred signature algorithm. The design and implementation of that configuration mechanism is beyond the scope of this document. It is important that the implementers are careful that this mechanism cannot be used nefariously to downgrade to an insecure signature algorithm.

NOTE 26 The configurable mechanism as defined by [V2G20-2320] can be used for this purpose.

V2G communication sessions can be paused and resumed with no need for re-authentication and/or re-authorization by using the same V2G session credentials used in the previously paused V2G session. 8.3.1 provides further details on pausing and resuming V2G sessions. To ensure a seamless resumption of the V2G communication session, the TLS session should be handled in a similar fashion. A renewal of TLS authentication should not be required, and the credentials (session ticket, pre-shared key, etc.) of the previously established session should be used. Refer to 7.7.3.7 forfurther details of TLS session resumption.

[V2G20-1672] The SECC shall support all pre-shared key exchange modes defined in Table 9.

[V2G20-1673] The SECC shall include pre-shared key exchange modes in the order as they appear in Table 9.

NOTE 27 Pre-shared key exchange modes listed in Table 9 are cataloged in the order of preference with the most preferred pre-shared key exchange mode first.

NOTE 28 The configurable mechanism as defined by [V2G20-2320] indicates SECC's preference.

[V2G20-1674] When selecting the pre-shared key exchange mode from the list of pre-shared key exchange modes received in the "psk_key_exchange_modes" extension field of the received "ClientHello" message, the SECC shall give preference to the most preferred pre-shared key exchange mode that the SECC supports.

NOTE 29 Pre-shared key exchange modes are listed in the "psk_key_exchange_modes" extension field in the order of preference with the most preferred pre-shared key exchange mode first.

NOTE 30 The configurable mechanism as defined by [V2G20-2320] indicates SECC's preference.

[V2G20-1675] The EVCC shall support all pre-shared key exchange modes defined in Table 9.

[V2G20-1676] The EVCC shall include pre-shared key exchange modes in the order as they appear in Table 9.

NOTE 31 Pre-shared key exchange modes listed in Table 9 are cataloged in the order of preference with the most preferred pre-shared key exchange mode first.

[V2G20-1677] When transmitting the list of supported pre-shared key exchange modes in the "psk_key_exchange_modes" extension field of the "ClientHello" message, the EVCC shall list the pre-shared key exchange modes that the EVCC supports in the order of preference of the EVCC.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 32 Pre-shared key exchange modes are listed in the "psk_key_exchange_modes" extension field in the order of preference with the most preferred pre-shared key exchange mode first.

Table 9 — Supported pre-shared key exchange modes

Pre-shared key exchange modes	Standards
psk_dhe_ke	IETF RFC 8446

[V2G20-1678] The SECC shall accept a PSK handshake only to resume a TLS session.

[V2G20-1679] The EVCC shall utilize a PSK handshake only to resume a TLS session.

[V2G20-1680] Regardless if a previous TLS session is being resumed or a new TLS session is being initiated, the SECC shall not accept the "early_data" extension in the received "ClientHello" message as described in IETF RFC 8446.

[V2G20-1612] Regardless if a previous TLS session is being resumed or a new TLS session is being initiated, the EVCC shall not send the "early_data" extension in the transmitted "ClientHello" message as described in IETF RFC 8446.

7.7.3.5 TLS session setup

There can be multiple TLS handshakes between the EVCC and SECC during the same V2G session. For the purposes of this document, "Initial Handshake" is defined as the first successful TLS handshake between the EVCC and SECC during the given V2G session.

Similarly, for the purposes of this document, "Full Handshake" is defined as the TLS handshake where client (EVCC)/server (SECC) authentication is performed via client (vehicle)/server (SECC) certificate validation. This is same as "Full Handshake" as defined in IETF RFC 8446. "Full Handshake" does not include "pre_shared_key" in the "ClientHello" and "ServerHello" messages. Refer to IETF RFC 8446 for further details. An "Initial Handshake" is always a "Full Handshake".

[V2G20-2677] Only full-handshake TLS shall be used for V2G communication between EVCC and SECC, whether initial or resumed, except for VAS communication.

[V2G20-2462] The SECC shall follow the requirements defined in 7.7.3.3 and IETF RFC 8446 to setup the TLS 1.3 session.

[V2G20-2465] The EVCC shall follow the requirements defined in 7.7.3.3 and IETF RFC 8446 to setup the TLS 1.3 session.

[V2G20-2468] The CPM4PE, if active, shall expire on the EVCC after the TLS session has been established and PE private root CA certificate was not received in the PE certificate chain.

[V2G20-2469] The CPM4PE, if active, shall expire on the private SECC after the TLS session has been established and OEM root CA certificate was not received in the vehicle certificate chain.

7.7.3.6 Enabling of VAS communication

[V2G20-1523] Each VAS shall be offered via a dedicated port at SECC.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1524] The firewall running on the SECC shall be configured to allow access to this (these) dedicated VAS port(s).

[V2G20-1525] Either full-handshake TLS or resumed TLS can be used to open an additional communication channel for a VAS. The resumption shall be based on the TLS context (i.e. ticket) exchanged in the V2G session. TLS session resumption shall be performed using the mechanism described in 7.7.3.7.

[V2G20-1527] If the SECC allows TLS resumption for VAS, the SECC shall issue the EVCC a separate TLS session ticket for each offered VAS.

The SECC can provide TCP-level forwarding. This forwarding can be mapped to a fixed external URI or a Proxy server or localhost for local VAS. For an end-to-end secured communication via the proxy server, the proxy server should offer the HTTP CONNECT method as specified in IETF RFC 2817. If UDP based VAS are desired, the approach using session resumption can also be used in conjunction with OpenVPN. For end-to-end secured communication over fixed external URI, the EVCC and the target VAS server should negotiate a separate security association, e.g. a separate TLS session. The specific security for VAS is not in the scope of this document.

NOTE 1 For detailed information on the realization, please refer to Annex G.

NOTE 2 IETF RFC 2817 has been updated by IETF RFC 7230 (which is updated by IETF RFC 8615) and IETF RFC 7231. These updates are considered to be included in this document.

[V2G20-2470] If the SECC does not support TLS session resumption, the EVCC shall setup a distinct TLS session for each value added service supported/provided by the SECC.

NOTE 3 For methods of associating a VAS session with a V2G session, see Annex G.

7.7.3.7 TLS session resumption

TLS session cannot be paused, but it can be closed (terminated). Refer to 7.7.3.8 for details of TLS session termination.

A closed TLS session can be restarted/resumed if the server (SECC) provided the client (EVCC) with the necessary information to resume the TLS session. The resumed TLS session, as described by IETF RFC 8446 is cryptographically bound to the initial TLS session without the need for re-authentication of the server/client certificates saving valuable time in time-critical applications.

A TLS session resumption requires usage of "Session Tickets". The session ticket, in IETF RFC 8446, ensures that the client has access to the session credentials negotiated in the TLS handshake.

In the application of ISO 15118-20, TLS session resumption can be used to ensure that the value added service can be securely related to an already established V2G session. TLS session resumption cannot be used for V2G session resumption. Only full-handshake TLS can be used for V2G session resumption. Both TLS resumption and TLS full-handshake can be used for opening a VAS communication.

[V2G20-2021] 0-RTT shall not be used for TLS session resumption.

NOTE 1 0-RTT can lead to replay attacks.

TLS session resumption in this document is performed via the "PSK Handshake" as defined in IETF RFC 8446 using "pre_shared_key" in the "ClientHello" and "ServerHello" messages. Refer to IETF RFC 8446 for further details.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

The "NewSessionTicket" message is also (and interchangeably/commonly) referred to as "TLS session ticket" in this document.

[V2G20-2023] If the SECC supports VAS services and it allows EVCC to use TLS resumption for VAS, it may send up to the same number of separate/unique "NewSessionTicket" messages (as described in IETF RFC 8446) as the number of VAS supported by the SECC.

NOTE 2 "NewSessionTicket" message sets up the PSK for TLS session resumption.

NOTE 3 Each value added service uses a separate TLS session which are all tied to the same V2G session. Each "NewSessionTicket" message provides a unique PSK that can be used to set up a separate, though parallel, resumed TLS session.

NOTE 4 8.3.4.3.4.3 limits the number of value added services supported by SECC to be eight (8). Hence, at most, additional eight (8) "NewSessionTicket" messages are sent out by the SECC to support each separate value added service.

[V2G20-2611] The SECC shall follow [V2G20-2023] for every "Full Handshake".

NOTE 5 "Full Handshake" can occur multiple times during the same V2G session whenever the V2G session is resumed after a pause.

[V2G20-2612] The "ticket_nonce" sent by the SECC in the "NewSessionTicket" message shall have minimum 7 bits of entropy. Refer to 7.3.7 for details. Additional details can be found in IETF RFC 8446:2018, Annex C.1.

[V2G20-2024] The SECC shall set "ticket_lifetime" in "NewSessionTicket" message to be greater than or equal to Minimum_TLS_SessionTicket_Lifetime and less than or equal to Maximum_TLS_SessionTicket_Lifetime. Refer to IETF RFC 8446 for further details of "ticket_lifetime".

[V2G20-2025] Minimum_TLS_SessionTicket_Lifetime shall be 20 s.

NOTE 6 This can give both the SECC and the EVCC enough time to transmit/receive and process all the "NewSessionTicket" messages. For example, including one for the V2G session, there could be a maximum of 8 "NewSessionTicket" messages exchanged between the SECC and the EVCC. This is to ensure that the SECC does not keep sending new tickets per [V2G20-2027]. The ticket lifetime can also be long enough for the EVCC to initiate a VAS communication when needed during the V2G session.

[V2G20-2026] Maximum_TLS_SessionTicket_Lifetime shall be 86 400 s (24 h).

NOTE 7 Although IETF RFC 8446 supports ticket lifetimes up to 7 days, longer session ticket lifetimes can lead to security issues. Most nominal use cases of TLS session resumption in the context of this document would not need tickets valid longer than a few hours. As such, ticket lifetimes longer than 24 h are not allowed for implementations defined in this document.

[V2G20-2029] It is up to the discretion of the CSO/PE operator whether to support TLS resumption for VAS. If the SECC does not support TLS resumption, the SECC shall not send "NewSessionTicket" messages to EVCC.

NOTE 8 Lack of support for TLS session resumption eliminates security concerns related to TLS session resumption (refer to [V2G20-2024] for examples of the security concerns).

[V2G20-2705] The "ticket_lifetime" according to IETF RFC 8446 shall be less than Minimum_TLS_SessionTicket_Lifetime and greater than Maximum_TLS_SessionTicket_Lifetime.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2027] If TLS resumption is supported, the SECC shall send a new TLS session ticket(s) with updated information Minimum_TLS_SessionTicket_Lifetime before the TLS session ticket(s) are set to expire while the TLS session is still active, i.e. it has not been terminated yet.

NOTE 9 This helps ensure that EVCC has valid session tickets at any given time while the TLS session is still active. It also enables the SECC to set "ticket_lifetime" to short values reducing some of the security risks inherent with TLS session resumption.

NOTE 10 This requires SECC to maintain the knowledge of how long the session tickets it sent are still valid for.

[V2G20-2028] The SECC shall stop sending new TLS session tickets (per [V2G20-2027]) as soon as it has been 604 800 s (7 days) since the last "Full Handshake" during the currently active V2G session.

NOTE 11 This ensures that the existing TLS session is not extended indefinitely. Indefinite TLS session extension can lead to security risks like TLS session continuation long (604 800 s (7 days)) after certificate expiration or revocation, etc.

NOTE 12 This requires SECC to maintain the knowledge of how long it has been since the "Full Handshake".

[V2G20-2031] The SECC shall not send the "early_data" extension in the transmitted "NewSessionTicket" message (as described in IETF RFC 8446).

[V2G20-2032] The SECC shall securely cache/store the data transmitted in "NewSessionTicket" message(s).

NOTE 13 It is not in the scope of this document to define the requirements on how the data transmitted in "NewSessionTicket" message(s) is stored and how the data coherency is maintained.

[V2G20-2033] The SECC shall discard all data associated with TLS session tickets that have expired.

NOTE 14 This requires SECC to periodically check if any of the stored/cached TLS session tickets have expired or otherwise fail to meet the requirements in this document. This document leaves the periodicity of such checks to the discretion of the implementers.

[V2G20-2034] Upon reception of a "NewSessionTicket" message, the EVCC shall ensure that the "ticket_lifetime" in the received "NewSessionTicket" message is greater than or equal to Minimum_TLS_SessionTicket_Lifetime and less than or equal to Maximum_TLS_SessionTicket_Lifetime. Any "NewSessionTicket" messages not meeting this criterion shall be discarded. Refer to IETF RFC 8446 for further details of "ticket_lifetime".

[V2G20-2035] The EVCC shall reject any "NewSessionTicket" messages if they are received 604 800 s (7 days) or more after the "Full Handshake".

NOTE 15 This ensures that the existing TLS session is not extended indefinitely. Indefinite TLS session extension can lead to security risks like TLS session continuation long (604 800 s (7 days)) after certificate expiration or revocation, etc.

NOTE 16 This requires EVCC to maintain the knowledge of how long it has been since the "Full Handshake".

[V2G20-2036] The EVCC shall reject any "NewSessionTicket" message with "early_data" extension (as described in IETF RFC 8446.

[V2G20-2037] After verifying the "NewSessionTicket" message to be valid and contain a TLS session ticket that meets requirements [V2G20-2034], [V2G20-2035], and [V2G20-2036],

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

the EVCC shall securely cache/store the data in the received "NewSessionTicket" message.

NOTE 17 It is not in the scope of this document to define the requirements on how the data received in "NewSessionTicket" message(s) is stored and how the data coherency is maintained.

When the EVCC wants to resume a TLS session, it needs to check if there is (are) any valid TLS session ticket(s) stored in the EVCC. Each TLS session ticket comes with a "ticket_lifetime". According to IETF RFC 8446:2018, 4.2.11.1, the EVCC checks if the ticket age is less than the ticket lifetime before using the ticket to resume the TLS session. It is up to the OEM to define how TLS session ticket expiration/age is calculated using the "ticket_lifetime".

[V2G20-2039] The EVCC shall include only one (1) "PskIdentity" in the "OfferedPsks" field of "PreSharedKeyExtension" value of "pre_shared_key" extension field of the "ClientHello" message it sends to set up a resumed TLS session.

The EVCC will include the data from the "ticket" field from one of the securely stored/cached "NewSessionTicket" message in the "identity" field of "PskIdentity" field of the "OfferedPsks" field of "PreSharedKeyExtension" value of "pre_shared_key" extension field of the "ClientHello" message it sends to set up a resumed TLS session. Refer to IETF RFC 8446:2018, 4.2.11 for further details.

[V2G20-2040] Once a TLS session ticket has been used to try to resume a TLS session, that particular TLS session ticket shall be discarded by the EVCC.

NOTE 18 Each TLS session ticket is used only once. This is done regardless if the EVCC was actually able to successfully resume the TLS session using the said TLS session ticket. This prevents EVCC tracking. Refer to IETF RFC 8446:2018, Annex C.4 for further details of the security risks.

Upon receiving the "pre_shared_key" extension in the "ClientHello" message, the SECC will authenticate the EVCC via the credentials provided in "pre_shared_key" extension of the "ClientHello" message. Refer to IETF RFC 8446 for further details of this authentication process.

[V2G20-2042] During the authentication of the EVCC using the credentials provided in "pre_shared_key" extension of the "ClientHello" message, the SECC shall simply fail to set up a TLS session if it is unable to successfully validate the PSK identity provided by the EVCC in the "pre_shared_key" extension of the "ClientHello" message.

[V2G20-2043] During the authentication of the EVCC using the credentials provided in "pre_shared_key" extension of the "ClientHello" message, the SECC shall simply fail to set up a TLS session if it is unable to successfully validate the binder provided by the EVCC in the "pre_shared_key" extension of the "ClientHello" message.

[V2G20-2044] If a TLS session is already active between the SECC and the EVCC, after processing a "ClientHello" message with a "pre_shared_key" extension, the SECC shall send a "NewSessionTicket" message (as described in IETF RFC 8446) as long as [V2G20-2028] is not violated.

[V2G20-2045] If no TLS for V2G session is active between the EVCC and SECC, the "pre_shared_key" extension in a "ClientHello" message shall be ignored and a full-handshake TLS shall be established.

7.7.3.8 TLS session termination

A TLS session is terminated when the V2G session is paused or terminated due to any reason (charging process completed, cable disconnected, etc.), the VAS session is terminated, etc.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2046] When a TLS session is terminated due to a VAS session being terminated, the EVCC shall irretrievably erase/delete/destroy all cryptographic data calculated for that particular TLS session. This includes all keys calculated for TLS encryption, any data calculated for certificate validation, etc.

[V2G20-2047] When a TLS session is terminated due to a V2G session being paused, the EVCC shall irretrievably erase/delete/destroy all cryptographic data calculated for that particular TLS session. This includes all keys calculated for TLS encryption, any data calculated for certificate validation, etc.

[V2G20-2049] When a V2G session is terminated due to any reason (charging process completed, user cancelled charging, cable disconnected, etc.), the EVCC shall terminate all TLS sessions associated with that V2G session. This includes terminating any TLS sessions associated with any VAS associated with that V2G session. The EVCC shall irretrievably erase/delete/destroy all cryptographic data calculated for all TLS sessions being terminated. This includes all keys calculated for TLS encryption, any data calculated for certificate validation, any TLS session tickets that may have been stored, data stored for "Session Binding", etc.

[V2G20-2050] When a TLS session is terminated due to a VAS session being terminated, the SECC shall irretrievably erase/delete/destroy all cryptographic data calculated for that particular TLS session. This includes all keys calculated for TLS encryption, any data calculated for certificate validation, etc.

NOTE 1 All other active TLS session(s) tied to the same V2G session can be completely unaffected under these circumstances.

[V2G20-2051] When a TLS session is terminated due to a V2G session being paused, the SECC shall irretrievably erase/delete/destroy all cryptographic data calculated for that particular TLS session. This includes all keys calculated for TLS encryption, any data calculated for certificate validation, etc.

[V2G20-2053] When a V2G session is terminated due to any reason (charging process completed, user cancelled charging, cable disconnected, etc.), the SECC shall terminate all TLS sessions associated with that V2G session. This includes terminating any TLS sessions associated with any VAS associated with that V2G session. SECC shall irretrievably erase/delete/destroy all cryptographic data calculated for all TLS sessions being terminated. This includes all keys calculated for TLS encryption, any data calculated for certificate validation, any TLS session tickets that may have been stored, data stored for "Session Binding", etc.

NOTE 2 This is different than pausing of the V2G session.

7.7.3.9 General TLS security comments

IETF RFC 8446:2018, Annex E provides some security risks associated with TLS 1.3 and suggests a few mitigation techniques. The implementers should be cognizant of these and should carefully consider pros and cons of each mitigation technique before incorporating it in the solution.

At the discretion of CSO, the SECC may cache OCSP responses for vehicle certificate for later use. The next time the SECC receives the vehicle certificates for the same EVCC, it may use the cached OCSP responses, if still valid, for revocation status thereby saving time. The methodology to achieve this is not in the scope of this document. It should be noted, though, that relying on the cached OCSP response here will mean that latest updates to that certificate's status could be missed. Refer to 7.3.1 when implementing OCSP response caching.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

7.7.3.10 TLS backwards compatibility

Implementations of this document may be interoperable with earlier versions of th ISO 15118 series (i.e. various editions of ISO 15118-2). To enable an EVCC implementing this document to connect to an SECC implementing a previous revision of 15118 (i.e. various editions of ISO 15118-2), the ClientHello message needs to comply with a specific set of requirements.

Similarly, to enable an SECC implementing this document to accept a connection from an EVCC implementing a previous revision of the ISO 15118 series (i.e. various editions of ISO 15118-2), the interpretation of a received ClientHello message needs to comply with a specific set of requirements.

Therefore, the following requirements should only be implemented, if an implementation of this document should be backwards compatible. Otherwise the following requirements should be ignored.

[V2G20-2054] If the EVCC is required to be backwards compatible to ISO 15118-2, the requirements in 7.7.3.10 shall be implemented.

[V2G20-2055] If the SECC is required to be backwards compatible to ISO 15118-2, the requirements in 7.7.3.10 shall be implemented.

[V2G20-2056] If the EVCC is required to be backwards compatible to ISO 15118-2, it shall additionally support the certificate profiles defined in ISO 15118-2.

[V2G20-2057] If the SECC is required to be backwards compatible to ISO 15118-2, it shall additionally support the certificate profiles defined in ISO 15118-2.

[V2G20-2058] If the EVCC is required to be backwards compatible to ISO 15118-2, it shall include the cipher suites of the ISO 15118-2 in the cipher_suites field of the ClientHello message after the TLS 1.3 cipher suites in the same order as they appear in ISO 15118-2.

NOTE 1 Cipher suites are listed in the cipher_suites field in the order of preference with the most preferred cipher suite first.

[V2G20-2059] If the SECC is required to be backwards compatible to ISO 15118-2, it shall additionally support the cipher suites of the ISO 15118-2 in the cipher_suites field of the ClientHello message.

[V2G20-2060] If the EVCC is required to be backwards compatible to ISO 15118-2, it shall include the necessary extensions, as required by the ISO 15118-2, in the ClientHello message.

NOTE 2 All extensions, as specified in 7.7.3.10 can be included/supported to perform a TLS 1.2 handshake in case an implementation of this document encounters a legacy V2G entity.

[V2G20-2061] If the SECC is required to be backwards compatible to ISO 15118-2, it shall additionally support the necessary extensions, as required by the ISO 15118-2, in the ClientHello message.

NOTE 3 All extensions, as specified in 7.7.3.10 can be included/supported to perform a TLS 1.2 handshake in case an implementation of this document encounters a legacy V2G entity.

[V2G20-2062] If the EVCC is required to be backwards compatible to ISO 15118-2, it shall include the version 0x0303 for TLS 1.2 in the supported_versions extension.

NOTE 4 This allows the SECC to setup a TLS 1.3 or TLS 1.2 session with the EVCC.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2063] If the EVCC wants/prefers to setup and utilize ISO 15118-2 communications, it shall omit sending supported_versions extension.

NOTE 5 This either forces the SECC to setup a TLS 1.2 session with EVCC or fails to setup any TLS session at all.

[V2G20-2064] The EVCC shall continue a TLS 1.2 handshake, as described in ISO 15118-2, if the SECC selected TLS 1.2 and EVCC supports TLS 1.2.

[V2G20-2065] The SECC shall perform a TLS 1.2 handshake, as specified in ISO 15118-2, if supported_versions extension is not present in (i.e. missing from) the received ClientHello and the SECC supports TLS 1.2.

[V2G20-2066] The SECC shall perform a TLS 1.2 handshake, as specified in ISO 15118-2, if supported_versions extension in the received ClientHello is set to 0x0303 (i.e. no other versions are listed in the supported_versions extension) and the SECC supports TLS 1.2.

NOTE 6 [V2G20-2356] applies, if a TLS 1.2 handshake is negotiated.

NOTE 7 A SECC that does not support TLS 1.3 sends a ServerHello without the supported_versions extension, since implementations are required to ignore unknown extensions. In contrast, a server that does support TLS 1.3 sends a supported_version extension containing the selected version (see IETF RFC 8446).

NOTE 8 The TLS 1.2 and TLS 1.3 ClientHello messages are compatible on the network binary level; i.e. all mandatory fields are present and have the same size in both revisions. TLS 1.3 is specified using extensions to the ClientHello message. Since both TLS 1.2 and TLS 1.3 implementations are required to ignore unknown extensions, a TLS 1.2 implementation can safely ignore any TLS 1.3 mandatory extension. If a TLS 1.3 peer is willing to negotiate TLS 1.2, it can accept the legacy ClientHello and respond with a legacy ServerHello or respectively accept a legacy ServerHello. Refer to IETF RFC 8446:2018, Annex D for further details.

[V2G20-2067] An SECC trying to establish legacy ISO 15118-2 communication shall not request EVCC to send the EVCC's certificate via "CertificateRequest" message.

NOTE 9 This ensures backwards compatibility with ISO 15118-2 utilizing unilateral authentication.

[V2G20-2068] The EVCC shall abort the handshake, if a downgrade is detected in the server's random value according to IETF RFC 8446.

[V2G20-2069] If the EVCC and SECC do not support the same TLS versions, TLS session setup will fail. For example, if the EVCC only supports TLS 1.3 while SECC only supports TLS 1.2, a TLS session setup request will fail. If TLS session setup process fails due to incompatible TLS versions, the EVCC shall abort the TLS setup process and apply [V2G20-1805].

[V2G20-2070] If the EVCC and SECC do not support the same TLS versions, TLS session setup will fail. For example, if the EVCC only supports TLS 1.3 while SECC only supports TLS 1.2, a TLS session setup request will fail. If TLS session setup process fails due to incompatible TLS versions, the SECC shall abort the TLS setup process and apply [V2G20-035].

7.8 V2G transfer protocol

7.8.1 General information

The V2G transfer protocol (V2GTP) is a compact communication protocol to transfer V2G messages between two V2GTP entities. It mainly consists of a header and payload definition that allow to be

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

separated and process V2G messages efficiently. V2GTP is the standard transfer protocol between the EVCC and SECC but may also be used for communication with other V2G entities that support the V2GTP protocol.

7.8.2 Supported ports

V2GTP is based on TLS+TCP. TLS+TCP uses a pair of IP addresses (source address and destination address) and a pair of port numbers (source port and destination port) to establish and identify a connection for bidirectional exchange of byte streams. The connection is established from the source address and source port to the destination address and destination port. The ports listed in Table 10 are used by V2GTP entities.

Table 10 — Supported TCP ports for V2GTP

Name	Protocol	Port number	Description
V2G_SRC_TCP_DATA	TCP(unicast)	Port number in the range of Dynamic Ports (49152-65535) as defined in IETF RFC 6335.	V2GTP source port at a Primary Actor (e.g. EVCC) that implements the V2GTP protocol.
V2G_DST_TCP_DATA	TCP (unicast)	Port number at V2GTP entity providing a V2GTP destination port number in the range of Dynamic Ports (49152-65535) as defined in IETF RFC 6335. For an SECC it will be dynamically assigned by the SDP mechanism (see 7.10.1)	V2GTP destination port at a Primary Actor (e.g. SECC)

For V2GTP entities implementing the V2GTP the following general requirements apply.

[V2G20-073] A V2GTP entity providing a destination port shall support at least one connection on the local port V2G_DST_TCP_DATA as defined in Table 10.

NOTE 1 A V2GTP entity providing a destination port can support multiple simultaneous connections on the local port V2G_DST_TCP_DATA as defined by Table 10.

[V2G20-075] A V2GTP entity using a source port shall support at least one connection on the local port V2G_SRC_TCP_DATA as defined in Table 10.

NOTE 2 A V2GTP entity using a source port can support multiple connections on the local port V2G_SRC_TCP_DATA as defined in Table 10.

Especially, for an EVCC and an SECC the following applies.

[V2G20-077] The EVCC shall use a source port V2G_SRC_TCP_DATA as defined in Table 10.

[V2G20-078] The SECC shall provide a destination port V2G_DST_TCP_DATA as defined in Table 10.

[V2G20-079] The EVCC shall support at least one connection for a V2G communication session on port V2G_SRC_TCP_DATA.

[V2G20-080] The SECC shall support at least one connection for a V2G communication session on port V2G_DST_TCP_DATA.

[V2G20-081] The EVCC shall use the port V2G_DST_TCP_DATA returned in the last SECC discovery response message (refer to 7.10.1.6) for connecting the SECC.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

7.8.3 Protocol data unit

7.8.3.1 Structure

The V2GTP PDU consists of a header and a body section as shown in Table 11.

Table 11 — V2GTP message structure

Header	Payload
8 Bytes	4294967295 Bytes

The payload contains the application data (e.g. a V2G message). The header separates the payloads (i.e. individual V2GTP messages) within a byte stream and gives information for the payload processing.

The V2GTP message header structure is shown in Table 12 and described in Table 13. The supported payload types are described in Table 14.

Table 12 — V2GTP message header structure

Byte No.	1	2	3	4	5	6	7	8
Header field	Protocol version	Inverse protocol version	Payload type		Payload length			

[V2G20-082] A V2GTP entity shall use the header structure as shown in Table 12.

[V2G20-083] A V2GTP entity shall send the 8 bytes of the V2GTP header in the order as shown in Table 12.

[V2G20-084] A byte with a lower number shall be sent before a byte with a higher number. The header starts with byte 1 and ends with byte 8.

[V2G20-085] A V2GTP entity shall send the fields "payload type" and "payload length" in big-endian format: The most significant byte is sent first, the least significant byte is sent last.

Table 13 — Generic V2GTP header structure

Header field	Header field description	Header field values
Protocol Version	Identifies the protocol version of V2GTP messages.	0x01: V2GTP version 1 0x00, 0x02-0xFF: reserved by document
Inverse Protocol Version	Contains the bit-wise inverse value of the protocol version which is used in conjunction with the V2GTP protocol version as a protocol verification pattern to ensure that a correctly formatted V2GTP message is received. Equals the <Protocol_Version> XOR 0xFF	0xFE: V2GTP Version 1 0xFF, 0xFD-0x00: reserved by document
Payload Type	Contains information about how to decode the payload following the V2GTP header.	Refer to Table 14 for a complete list of payload type values.
Payload Length	Contains the length of the V2GTP message payload in bytes (i.e. excluding the generic V2GTP header bytes).	0…4294967295

Table 14 — V2GTP payload types

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Payload type value	Payload type identifier	Explanation
0x0000 - 0x8000	Not applicable	Reserved for future use
0x8001	SAPPayloadID	EXI encoded V2G messages of ISO 15118-2. For backward compatibility the supportedAppProtocol messages of this document also use this payload type (see 8.2.1)
0x8002	Part20MainstreamPayloadID	EXI encoded V2G messages of this document which are exchanged as part of the main stream of the communication flow. This set of messages is using the XSD schema with the namespace "urn:iso:std:iso:15118:-20:CommonMessages".
0x8003	Part20ACMainstreamPayloadID	EXI encoded V2G messages of this document which are exchanged as part of the main stream of the communication flow and are specific to AC. This set of messages is using the XSD schema with the namespace "urn:iso:std:iso:15118:-20:AC".
0x8004	Part20DCMainstreamPayloadID	EXI encoded V2G messages of this document which are exchanged as part of the main stream of the communication flow and are specific to DC. This set of messages is using the XSD schema with the namespace "urn:iso:std:iso:15118:-20:DC".
0x8005	Part20ACDPMainstreamPayloadID	EXI encoded V2G messages of this document which are exchanged as part of the main stream of the communication flow and are specific to ACDP. This set of messages is using the XSD schema with the namespace "urn:iso:std:iso:15118:-20:ACDP".
0x8006	Part20WPTMainstreamPayloadID	EXI encoded V2G messages of this document which are exchanged as part of the main stream of the communication flow and are specific to WPT. This set of messages is using the XSD schema with the namespace "urn:iso:std:iso:15118:-20:WPT".
0x8007 - 0x8100	Not applicable	Reserved for future use
0x8101	ScheduleRenegotiationPayloadID	EXI encoded V2G message on a multiplexed side stream for the purpose of schedule renegotiation (see 8.6.5.1 and Annex F)
0x8102	MeteringConfirmationPayloadID	EXI encoded V2G message on a multiplexed side stream for the purpose of exchanging Metering information (see 8.3.4.3.11)
0x8103	ACDPSystemStatusPayloadID	EXI encoded V2G message on a multiplexed side stream for the purpose of exchanging ACDP system status information (see 8.3.4.7.8)

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Payload type value	Payload type identifier	Explanation
0x8104	ParkingStatusPayloadID	EXI encoded V2G message on a multiplexed side stream for the purpose of delivering Parking Status information (see 8.6.5.3 and 8.3.4.8.1)
0x8105 - 0x8FFF	Not applicable	Reserved for future use
0x9000	SDPRequestPayloadID	SDP request message (see 7.10.1.5)
0x9001	SDPResponsePayloadID	SDP response message (see 7.10.1.6)
0x9002	SDPRequestWirelessPayloadID	SDP request message for wireless communication (see 7.10.1.8)
0x9003	SDPResponseWirelessPayloadID	SDP response message for wireless communication (see 7.10.1.9)
0x9004 - 0x9FFF	Not applicable	Reserved for future use
0xA000 - 0xFFFF	Not applicable	Available for manufacturer specific use. Uniqueness of those identifiers is not guaranteed by this document.

NOTE 1 Only the payload type value numbers are technically used by the protocol. However, the requirements of this document reference those values by the associated identifier with the PayloadID suffix.

[V2G20-086] A V2GTP entity shall use the V2GTP message structure as shown in Figure 8 to send V2G messages as defined in Clause 8.

[V2G20-2307] A V2GTP entity shall use the definitions as defined in Table 13 and Table 14.

[V2G20-1229] For EXI encoded V2G messages (payload 0x8001 up to and including 0x8FFF) a V2GTP entity shall use a separate V2GTP message for each V2G message.

NOTE 2 Requirement [V2G20-1229] implies that the payload field can include neither a part of a message nor multiple messages.

7.8.3.2 Header processing

For the processing of the payload the V2GTP entity processes the header first. For this, a V2GTP entity that receives a V2GTP message checks the header field step by step. The header processing as defined below is illustrated in Figure 11.

[V2G20-089] A V2GTP entity shall process the V2GTP header as defined in Table 13 before processing the payload as defined in Table 14.

[V2G20-090] A V2GTP entity shall check the protocol version and inverse protocol version fields (synchronization pattern) before any other header fields.

[V2G20-092] A V2GTP entity shall check the payload type after the successful check of the version and inverse version field.

[V2G20-094] A V2GTP entity shall check the payload length after the successful check of the payload type.

[V2G20-096] If the header processing was successful the V2GTP entity shall process the payload.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-800] If the V2GTP header contains wrong data (e.g. not supported payload type, wrong payload length, or not supported V2GTP version) the V2GTP entity shall ignore this message.

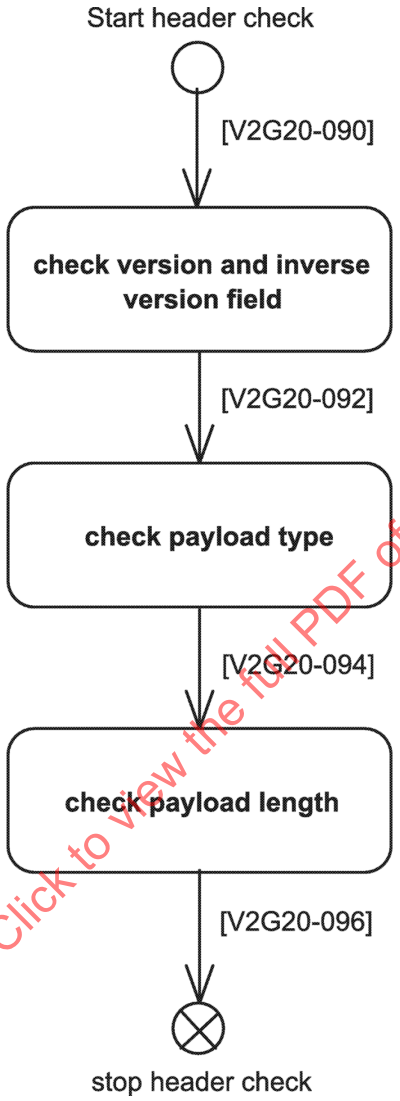


Figure 11 — V2GTP generic header handler

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

7.9 Presentation layer

7.9.1 XML and efficient XML interchange (EXI)

7.9.1.1 Overview

For the purpose of describing the V2G message set the presentation layer uses the widely adopted XML data representation. The document defines messages (i.e. data structures and data types) based on XML schema which allows the type aware use of XML and enables simplified validity evaluation of exchanged messages.

[V2G20-097] When transmitting V2G messages defined in this document by using XML all V2G entities shall use encoding format according to definitions of W3C EXI 1.0.

7.9.1.2 Efficient XML interchange

© ISO 2022 – All rights reserved

The efficient XML interchange (EXI) format allows to use and process XML-based messages on a binary level. Thus, the EXI format increases the processing speed of XML-based data as well as reduces the memory usage. Basically, EXI is a W3C recommendation. The EXI format uses a relatively simple grammar driven approach that achieves very efficient encodings for a broad range of use cases. It is not uncommon for EXI messages to be up to 100 times smaller than equivalent XML documents. The EXI specification describes in a predefined process how schema information should be transformed into EXI grammar. The reason for doing so is that EXI grammar is much simpler to process, compared to XML schema information. Nevertheless the parsing can be performed in the same accurate way as it is possible in XML.

There are different kinds of coding mechanism with EXI. To meet the demands of efficient processing, less resources usage, message size, and message extendibility schema-aware settings should be selected (see 7.9.1.3 for the requirement EXI settings for ISO 15118 communication).

In general, EXI streams can be created in a very efficient way if all encoded information (elements/attributes) are defined by an underlying XML Schema (Schema-informed Grammars). Deviant information based on XML Schema knowledge is encoded in a more generic way. The EXI coder encodes the qualified names (namespace and element/attribute name) of such unknown information in a string-based manner. However, simple types of the schema deviations may be still encoded type-aware.

EXI decoders are able to decode the efficient EXI streams by using the same underlying XML Schema which was used for the encoding process. Schema deviations are recognized in the EXI stream. These deviations (unknown elements or attributes) can be either processed or skipped.

Figure 12 summarizes the Efficient XML Interchange concept for the ISO 15118 communication. Due to the high limited resource restriction the EVCC may only be able to handle the XML-based data using a corresponding data structure representation. Such data structures can be used to serialize or deserialize ISO 15118 communication application messages. Meanwhile, the SECC may be able to handle the data as data structure and/or the more resource intensive document object model (DOM) or in a traditional plain-text XML variant.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

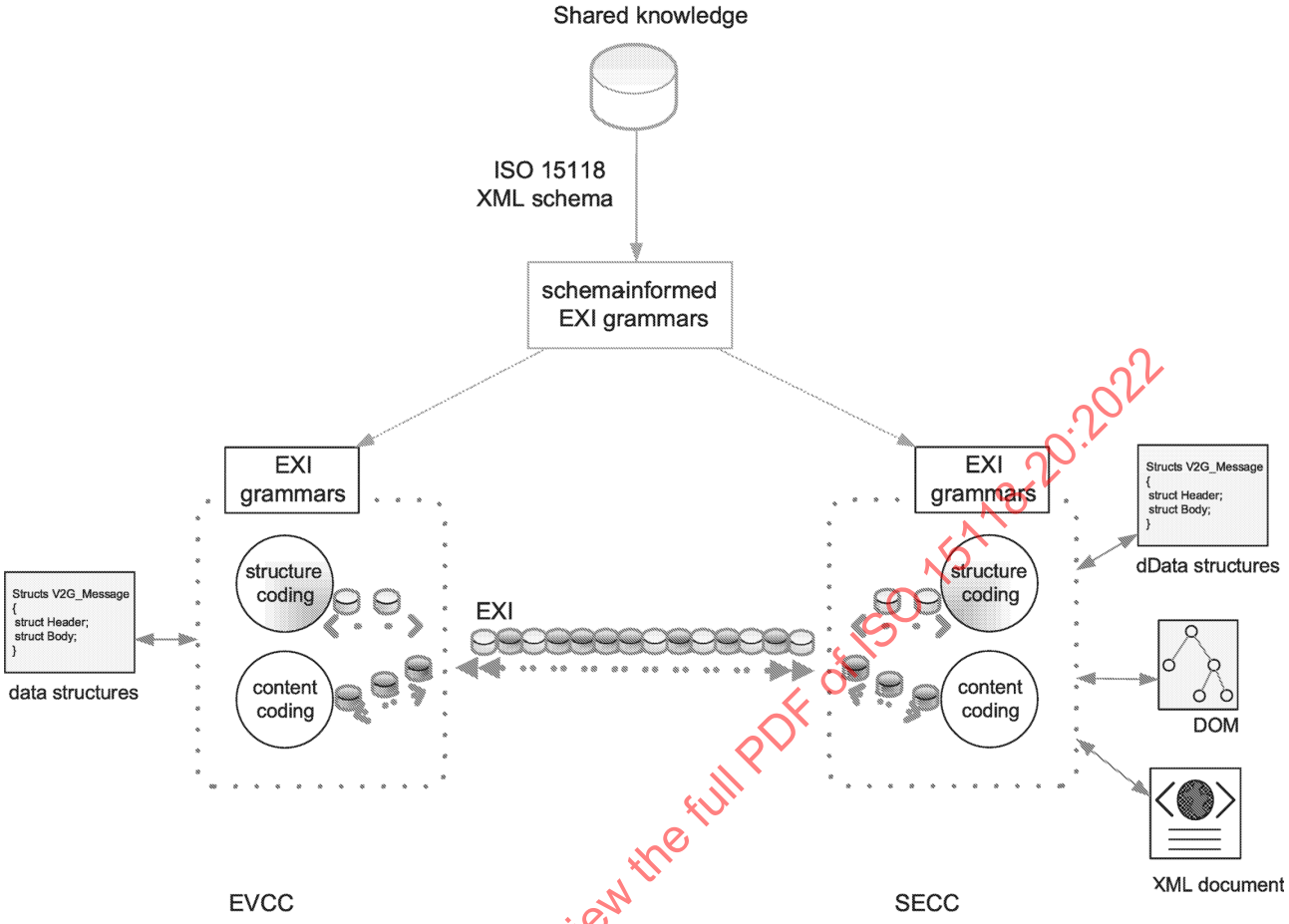


Figure 12 — Basic concept of EXI applied to V2G communication

7.9.1.3 EXI settings for application layer messages

The following EXI settings are used for the EXI-based V2G communication.

[V2G20-1020] The XML schema with the namespace "urn:iso:std:iso:15118:-20:CommonMessages" shall be used for encoding and decoding EXI streams sent or received with Part20MainstreamPayloadID and defined in 8.3.4.1. For the definition of the XML schema, refer to Annex A.

[V2G20-2308] The XML schema with the namespace "urn:iso:std:iso:15118:-20:AC" shall be used for encoding and decoding EXI streams sent or received with Part20ACMainstreamPayloadID and defined in 8.3.4.4.

[V2G20-2309] The XML schema with the namespace "urn:iso:std:iso:15118:-20:DC" shall be used for encoding and decoding EXI streams sent or received with Part20DCMainstreamPayloadID and defined in 8.3.4.5.

[V2G20-4106] The XML schema with the namespace "urn:iso:std:iso:15118:-20:ACDP" shall be used for encoding and decoding EXI streams sent or received with Part20ACDPMainstreamPayloadID and defined in 8.3.4.7.

[V2G20-5125] The XML schema with the namespace "urn:iso:std:iso:15118:-20:WPT" shall be used for encoding and decoding EXI streams sent or received with Part20WPTMainstreamPayloadID and defined in 8.3.4.6.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-099] The EXI coder for encoding and decoding of the ISO 15118 communication shall use the default EXI coding options according to W3C EXI 1.0, subclause "EXI options" with the exception of the options listed in Table 15.

Table 15 — EXI option settings

EXI Option	Description	Value defined by this document
valuePartitionCapacity	Specifies the total capacity of value partitions in a string table	0

[V2G20-100] The EXI header (refer to W3C EXI 1.0, clause "Header") shall be used in a way that fulfils the ISO 15118 needs. That means, the optional EXI cookie ($EXI) shall never be used and the presence bit for EXI options shall be always set to 0 (=false). As a consequence the optional EXI options shall never be part of an EXI message defined by this document. Each EXI implementation (on EVCC or SECC side) shall discard messages that do not respect the EXI header options defined by this document.

[V2G20-2310] An element/attribute which is not defined in Annex A shall be encoded and decoded as schema deviation case according to W3C EXI 1.0.

[V2G20-600] The EXI coder for encoding and decoding of the ISO 15118 communication shall use the EXI profile settings (Reference [105]) according to Table 16.

NOTE For details describing the EXI profile refer to Reference [105].

Table 16 — EXI profile settings

EXI profile parameter	Description	Value defined by this document
maximumNumberOfBuiltInElementGrammars	This option is the maximum number of built-in element grammars for which dynamically productions other than AT (xsi:type) productions have been added.	0
maximumNumberOfBuiltInProductions	This option is the maximum number of top-level productions that can be dynamically inserted in built-in element grammars excluding AT (xsi:type) productions.	0

[V2G20-2311] A simple type/value of an element/attribute which is not defined in Annex A shall be encoded and decoded type-aware.

7.9.2 Message security

7.9.2.1 Overview

XML signature is a W3C recommendation that addresses the authenticity requirements of some data fragments (e.g. metering information) of the XML-based V2G communications. XML signature defines a mechanism by which messages and message parts can be digitally signed to provide integrity, to ensure that the data is not tampered with and is authentic and to verify the identity of the message producer. For protecting confidentiality, a hybrid encryption scheme based on the Diffie-Hellman-Protocol is applied.

7.9.2.2 Application layer credentials and cipher suites

Credentials to be applied on application layer shall be suitable for the targeted XML security. Here, XML signature is chosen to protect billing relevant information between EVCC, SECC and/or SA. Moreover,

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

binary encryption provides a confidentiality protected way for private key provisioning to the EVCC without having intermediaries access to this private key. Both approaches require asymmetric key material. The credentials for EVCC signing are provided by the private key associated with the contract certificate and credentials for EVCC receiving encrypted data are provided by an ECDH key exchange as described in 7.9.2.5.4.

An OEM provisioning certificate enables an EVCC to request a valid contract certificate for PnC.

Refer to 7.3.6 and is subclauses for further details of securing the private keys in EVCC.

7.9.2.3 Contract certificates as XML signature credentials

Contract certificate is bound to an EMAID and used in XML signature to authorize the EV for charging. The contract certificate's attributes, like signature and validity period, can be verified even if the SECC is offline, given that the corresponding root CA certificate is stored locally on the SECC. For checking the revocation status via OCSP, the SECC needs to be online. The contract binding is handled as follows.

[V2G20-108] The EMAID shall be encoded in the subject of the certificate.

NOTE The EVCC is sending the sub-CA certificates within its authentication request so that the SECC can check the certificate chain up to the root certificate which it has stored itself.

7.9.2.4 XML security specifics for "PnC" message set(s)

7.9.2.4.1 XML data structures for application layer security

Security on application layer is provided using signature and encryption of messages. Information targeted for SA services is exchanged using XML data structures. Consequently, this information can be protected end-to-end using XML security.

7.9.2.4.2 XML signature mechanism

This subclause is intended as an introduction to XML signatures. For an overview on XML signatures see ISO 15118-2:2014.

NOTE 1 This document uses different ECC algorithms, signature algorithms, hash algorithms, etc. as compared to the examples in ISO 15118-2:2014. Hence the examples in ISO 15118-2:2014, do not directly apply to this document, but are very close.

XML signatures as defined in W3C XML can be applied to arbitrary digital content (data objects) in the same way as digital signatures are calculated. When applying a digital signature to data objects, the data objects are first digested (hashed) and the result is then signed using an asymmetric algorithm like ECDSA or EdDSA. In the case of XML, the digest is placed in an XML element, together with additional information. This element is then hashed and cryptographically signed. This document uses detached XML signatures according to W3C XML. That means the signature and data can be in separate (externally detached) or in the same XML document (internally detached) as sibling elements. The signature may comprise only a part of the XML document referenced by an ObjectID.

Figure 13 shows the schema diagram of the XML signature element included in the V2G message header.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

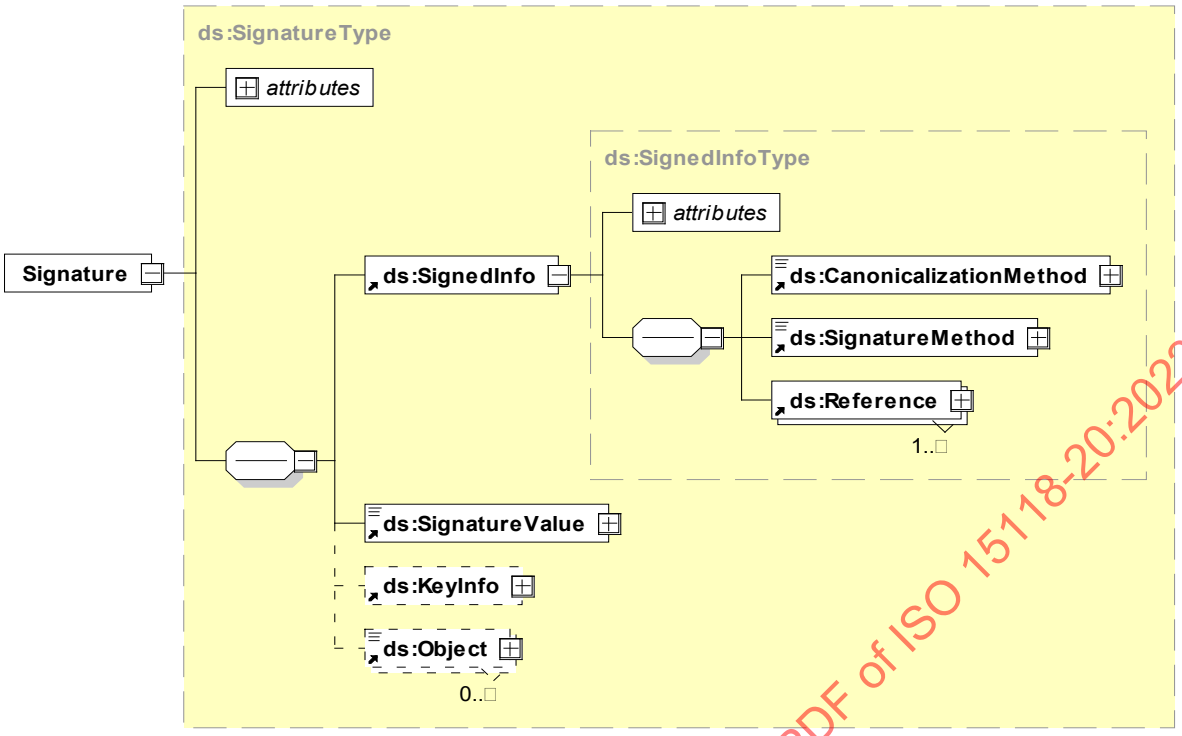


Figure 13 — Schema diagram – XML signature

Figure 14 shows the schema diagram of the element Reference included in the element SignedInfo which is part of the XML Signature depicted in Figure 13.

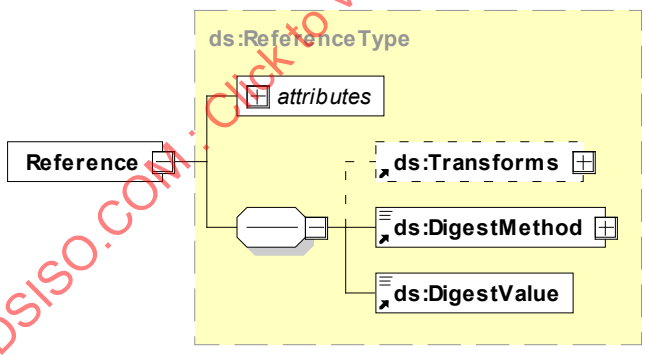


Figure 14 — Schema diagram – element Reference included in element SignedInfo

[V2G20-117] Each V2G entity shall support detached XML signatures.

[V2G20-119] For XML signature operations, the data which gets signed, shall be the EXI representation of this data.

[V2G20-764] As canonicalization method EXI with schema-informed fragment grammar shall be used.

[V2G20-765] Each message that needs the XML signature framework shall use the value "http://www.w3.org/TR/canonical-exi/" as algorithm attribute within the canonicalization method element.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-766] Each message that needs the XML signature framework shall use the value "http://www.w3.org/TR/canonical-exi/" as algorithm attribute within the transform element.

[V2G20-767] The maximum number of Transforms is limited to one (1) (i.e. per referenced element where a signature is to be transmitted for, just one single Transform algorithm can be indicated).

[V2G20-1449] The parts which are signed in the XML-based messages shall be encoded as EXI schema-informed fragment. To encode the signature header, the XML signature schema shall be used as entry point, instead of the schema defined by this document.

[V2G20-2473] Each message, that needs the XML signature framework shall use the value "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512" as algorithm attribute within the SignatureMethod element, if the algorithm defined in [V2G20-2674] shall be used according to the configuration in [V2G20-2320]. The certificate whose private key is used for signing the message shall be based on the algorithm defined in in [V2G20-2674].

[V2G20-2474] Each message, that needs the XML signature framework shall use the value "urn:iso:std:iso:15118:-20:Security:xmldsig#Ed448" as Algorithm attribute within the SignatureMethod element, if the algorithm defined in [V2G20-2319] shall be used according to the configuration in [V2G20-2320]. The certificate whose private key is used for signing the message shall be based on the algorithm defined in [V2G20-2319].

[V2G20-2475] Each message, that needs the XML signature framework shall use the value "http://www.w3.org/2001/04/xmlenc#sha512" as algorithm attribute within the DigestMethod element, if the algorithm defined in [V2G20-2674] shall be used according to the configuration in [V2G20-2320].

[V2G20-2476] Each message, that needs the XML signature framework shall use the value "urn:iso:std:iso:15118:-20:Security:xmlenc#SHAKE256" as algorithm attribute within the DigestMethod element, if the algorithm defined in [V2G20-2318] shall be used according to the configuration in [V2G20-2320].

[V2G20-771] The following message elements of the XML signature framework shall not be used when transmitting signatures in the header of the V2G message:

- Id (attribute in SignedInfo)
- ##any in SignedInfo – CanonicalizationMethod
- HMACOutputLength in SignedInfo – SignatureMethod
- ##other in SignedInfo – SignatureMethod
- Type (attribute in SignedInfo-Reference)
- ##other in SignedInfo – Reference – Transforms – Transform
- XPath in SignedInfo – Reference – Transforms – Transform
- ##other in SignedInfo – Reference – DigestMethod
- Id (attribute in SignatureValue)
- Object (in Signature)
- KeyInfo

NOTE 2 This allows to determine an upper bound for the size of the signature header.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

For the application of XMLDsig, any element which should be signed is addressable. In this document, this is achieved by a URI referencing the ID attribute of such an element. Therefore, any message element that is signed carries an ID attribute. If a specific element is to be signed in all use cases, the ID attribute is marked mandatory in the XSD. Otherwise, if it is signed in only some use cases, the ID attribute is marked optional and can be omitted when not needed.

NOTE 3 Presence of an ID attribute does not necessarily indicate that a signature is used, i.e. if no signature is used, an ID can be present nevertheless.

NOTE 4 Refer IETF RFC 3986 as updated by IETF RFC 6874 and IETF RFC 7320 for details of URI.

7.9.2.4.3 Application of security mechanisms to XML message

In general, two pairs of security mechanisms are supported.

- Authenticity and integrity: signature generation → signature verification; XML based signature is applied. The entity creates the XML message and signs certain or all fields of an XML message. The receiver verifies the signature.
- Confidentiality: encryption → secryption; encryption is applied. The entity creates the message and encrypts a single binary field of the XML message. The receiver decrypts that binary field.

Table 17 and Table 18 provide an overview of the applied security mechanisms.

The public/private key pair associated with the "subjectPublicKeyInfo" parameter of the appropriate certificate is used for the purposes of XML signatures.

Table 17 — Overview of applied XML based signatures

XML message	Protected fields	Signing entity (sender)	Verifying entity (receiver)
AuthorizationReq	PnC_AReqIdentificationMode	EVCC; signed with private key associated with the contract certificate provided within PnC_AReqIdentificationMode	SECC
CertificateInstallationReq	message body/all fields	EVCC; signed with private key associated with OEM provision certificate (transmitted in message body element)	secondary actor
CertificateInstallationRes	SignedInstallationData	secondary actor; signed with the private key associated with the leaf certificate of the certificate provisioning service	EVCC
MeteringConfirmationReq	message body / all fields	EVCC; signed with private key associated with the contract certificate (certificate is transmitted in AuthorizationReq message)	SECC
ChargeParameterDiscoveryRes	AbsolutePriceSchedule (if present, signature required for PnC)	secondary actor; signed with the private key associated with the eMSP sub-CA2 certificate	EVCC

Table 18 — Overview of applied encryption

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

XML message	Protected fields	Encrypting entity (sender)	Decrypting entity (receiver)
CertificateInstallationRes	SECP521_EncryptedPrivateKey	secondary actor	EVCC
CertificateInstallationRes	X448_EncryptedPrivateKey	secondary actor	EVCC
CertificateInstallationRes	TPM_EncryptedPrivateKey	secondary actor	EVCC

[V2G20-2312] Each V2G entity shall be able to generate XML signatures as specified in Table 17.

[V2G20-2313] Each V2G entity shall be able to verify XML signatures as specified in Table 17.

[V2G20-2477] Each V2G entity generating XML signatures shall utilize the private key associated with the "subjectPublicKeyInfo" parameter of the appropriate certificate, as specified in Table 17, to generate the XML signatures.

[V2G20-2478] Each V2G entity verifying XML signatures shall utilize the public key included in the "subjectPublicKeyInfo" parameter of the appropriate certificate, as specified in Table 17, to verify the XML signatures.

[V2G20-2479] The SA receiving a CertificateInstallationReq indicating the SignatureMethod as defined by [V2G20-2474] shall use the public key in "subjectPublicKeyInfo" of the OEM provisioning certificate contained in CertificateInstallationReq message to verify the signature.

NOTE 1 The key in the extension "subjectAltPublicKey" is encoded for use only in ECDH algorithm. It cannot be used to verify signatures using the Ed448 algorithm.

[V2G20-2699] When generating or verifying the XML signatures, each V2G entity shall utilize the public/private key associated with the appropriate certificate (as specified in Table 17) that uses the algorithm as indicated by the configuration in [V2G20-2320].

NOTE 2 This means that when the configuration in [V2G20-2320] indicates usage of algorithm defined in [V2G20-2674], the V2G entity can use keys from appropriate certificate (as specified in Table 17) based on algorithm defined in [V2G20-2674]. Similarly, when the configuration in [V2G20-2320] indicates usage of algorithm defined in [V2G20-2319], the V2G entity can use keys from appropriate certificate (as specified in Table 17) based on algorithm defined in [V2G20-2319].

[V2G20-2700] When generating the XML signatures, if the V2G entity does not possess appropriate certificate (as specified in Table 17) that uses the algorithm as indicated by the configuration in [V2G20-2320], it shall fail to generate the necessary XML signatures and take steps as defined for the particular message sequence.

NOTE 3 For example, if the contract certificates contained in the EVCC are based on algorithm defined in [V2G20-2674] but the EVCC's configuration in [V2G20-2320] indicates usage of algorithm defined in [V2G20-2319], the EVCC does not utilize those contract certificates in AuthorizationReq message(s) it sends.

NOTE 4 The example above is possible in cases where the EVCC was recently switched over from algorithm defined in [V2G20-2674] to algorithm defined in [V2G20-2319] (via changes to the configuration defined in [V2G20-2320]) while leaving the existing certificates intact in the EVCC.

[V2G20-2701] When verifying the XML signatures, if the V2G entity does not possess appropriate certificate (as specified in Table 17) that uses the algorithm as indicated by the configuration in [V2G20-2320], it shall fail to verify the necessary XML signatures and take steps as defined for the particular message sequence.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 5 For example, if the EVCC sends a CertificateInstallationReq containing OEM provisioning certificate based on algorithm defined in [V2G20-2674] but the SA's configuration in [V2G20-2320] indicates usage of algorithm defined in [V2G20-2319], the SA fails to verify the signatures received in CertificateInstallationReq message.

[V2G20-1000] Both, the r- and the s-values shall always be transferred with their maximum length. If any of these values is shorter, it shall be filled up with leading zeros. The receiver shall assign the first half of the bytes to r and the second half of the bytes to s. This encoding is described in IETF RFC 4050:2005, 3.3.

NOTE 6 The r- and s-values are the output of the ECDSA or EdDSA and consist of a pair of integers.

7.9.2.5 Certificate provisioning

In this document, the contract certificates are created and then distributed from an SA to the EVCC. In order to minimize roundtrips and communication processing time, and ease organizational processes, it was decided, that the SA (and not the EVCC) generates the key pair for the certificate, uses the key pair to then generate the corresponding certificate itself, and finally distributes the certificate and the corresponding private key to the EVCC. Since the private key is kept confidential, appropriate security mechanisms should be used for secure transmission of the contract certificate private key.

The eMSP creates credentials (SignedInstallationData) for the EVCC, consisting of a contract certificate including the encrypted contract certificate private key (the key is encrypted specifically for that EVCC). The contract certificate and the encrypted private key can then be distributed to the EVCC via an online installation service through the EVSE.

The contract certificate and the associated private key can also be distributed to the EVCC via offline/out-of-band installation. This document does not mandate offline or online contract certificate installation. Refer to H.5 for further details of offline contract certificate installation.

For online installation via the EVSE, the eMSP then forwards the credentials to the certificate provisioning service (CPS). The CPS asserts the correctness and authenticity of the credentials with a signature and relays the signed message fragment to the SECC, who compiles a CertificateInstallationRes message and transmits that to the EVCC. The certificate provisioning service is considered trustworthy. It is therefore not required that the EVCC is able to verify the contract certificate it has received via the CertificateInstallationRes.

The role "certificate provisioning service" can be assumed, for example, by the eMSP itself, the EVSE operator or a completely stand-alone service.

Figure 15, Figure 25 and Figure 26 illustrate operations performed by all involved actors to ensure a secure delivery of the contract certificate data to the intended EVCC without and with the usage of TPM 2.0, respectively. In order to inform a SA that an EVCC is equipped with a TPM and that the contract certificate private key should be encrypted for this TPM, the information about the EVCC's TPM is included by the OEM in a non-critical (optional) extension of the OEM provisioning certificate (see Figure 25). In case of a TPM-equipped EVCC, as signaled by the respective extension in the OEM provisioning certificate, the SA/eMSP should encrypt the private contract key for the EVCC's TPM according to 7.9.2.5.3 and its subclauses.

7.9.2.5.1 Common requirements for contract certificate installation in EVCC

[V2G20-2480] Unless specified otherwise, the SA (eMSP) shall use big-endian order for all bit strings and calculations specified by this subclause and the subclauses within.

[V2G20-2481] Unless specified otherwise, the EVCC shall use big-endian order for all bit strings and calculations specified by this subclause and the subclauses within.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

[V2G20-2698] The SA shall use the same (elliptic curve) EC to generate the contract certificate key pair and to encrypt the contract certificate private key as the one used in the EVCC's OEM provisioning certificate, except for the case when the SA's configuration parameter according to [V2G20-2320] does not allow to use this curve.

NOTE 1 In case the SA's configuration parameter according to [V2G20-2320] does not allow to use the (elliptic curve) EC as used in the EVCC's OEM provisioning certificate [V2G20-2709] will apply.

NOTE 2 At the time of CertificateInstallationReq, if the SA intends to provide multiple different contract certificates based on different curves as defined by [V2G20-2674] and [V2G20-2319], the SA will need to send multiple different SignedInstallationData containers to the SECC and the EVCC can, at its/user's discretion, utilize the looping mechanism for CertificateInstallationReq to get and install all different contract certificates.

[V2G20-2709] In case SA's configuration parameter as defined by [V2G20-2320] does not allow the SA to use the elliptic curve from the EVCC's OEM provisioning certificate, i.e. SA considers this curve insecure, the SA shall not provide a contract certificate.

NOTE 3 The CertificateInstallationReq message is signed using the OEM provisioning certificate that is contained within the CertificateInstallationReq message itself. The signatures on CertificateInstallationReq message are validated using the public key contained in the OEM provisioning certificate. Before the OEM provisioning certificates public key can be used to validate the signatures on CertificateInstallationReq message, the OEM provisioning certificate is validated. If this OEM provisioning certificate validation fails, the SECC sends the appropriate ResponseCode starting with "WARNING_" as defined in 8.6 and its subclauses.

NOTE 4 If this OEM provisioning certificate validation fails because the SECC/SA cannot process the curves in OEM provisioning certificate (due to changes to configuration parameter as defined by [V2G20-2320]), the SECC sends the ResponseCode "WARNING_CertificateValidationError" as defined in 8.6 and its subclauses.

NOTE 5 Communication between the SECC and the SA is not in the scope of this document. As such the exact error message sent by SA in cases described above is not defined by this document. This document simply provides the ResponseCode that the SECC is supposed to use in these circumstances.

[V2G20-2487] If the SA uses the elliptic curve corresponding to signature algorithm specified by [V2G20-2674] for contract certificate private key encryption key generation via ECDHE as specified in 7.9.2.5.4, it shall set ECDHCurve parameter in SignedInstallationDataType element of CertificateInstallationRes message to "SECP521".

[V2G20-2488] If the SA uses the elliptic curve corresponding to signature algorithm specified by [V2G20-2319] for contract certificate private key encryption key generation via ECDHE as specified in 7.9.2.5.4, it shall set ECDHCurve parameter in SignedInstallationDataType element of CertificateInstallationRes message to "X448".

[V2G20-2489] The ephemeral public key used in requirement [V2G20-2497] shall be contained in the XML element "DHPublicKey" encoded in its uncompressed form as "Subject Public Key" as defined in IETF RFC 5480.

NOTE 6 DHPublicKey is maximum 133 bytes long. The first byte has the fixed value 0x04 indicating the uncompressed form.

NOTE 7 When ECDHCurve is set to "SECP521", the DHPublicKey is 133 bytes long. When ECDHCurve is set to "X448", the DHPublicKey is 57 bytes long.

NOTE 8 IETF RFC 5480 has been updated by IETF RFC 8813. These updates are considered to be included in this document.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

It is encouraged, but not required/mandated, to encrypt the contract certificate private key with unique ECDHE keys for every single SignedInstallationData packet sent by the SA to the SECC. Changing the ECDHE keys for every single SignedInstallationData packet sent by the SA to the SECC means if the EVCC sends three consecutive CertificateInstallationReq messages for the same contract certificate, it will get the exact same contract certificate with the exact same private key in all three SignedInstallationData in CertificateInstallationRes messages, but the encrypted data package (SignedInstallationData) will be unique in every single CertificateInstallationRes message. This requires that the SA encrypts the contract certificate private key and generate SignedInstallationData on-the-fly (i.e. when it gets the request from the SECC to provide the SignedInstallationData for a particular PCID). This improves security, but may add some delay in responding to CertificateInstallationReq especially in those cases where eMSP already stores the OEM provisioning certificate public key(s) and as such may have the data packets ready to go. It is left to the eMSP's discretion to design their system as they deem fit. This document does not mandate changing the ECDHE keys for every single SignedInstallationData packet sent by the SA.

[V2G20-2490] The SA (eMSP) may indicate to the CPS the curves it wants the CPS to use for the CPS certificates that are used to sign the SignedInstallationData.

NOTE 9 This will ensure that the CPS uses the certificates associated with the curves that the SA (eMSP) wants it to use for that particular SignedInstallationData signature.

NOTE 10 This is not mandatory, but could help the SA (eMSP) ensure that the contract certificates are not rejected by the EVCC.

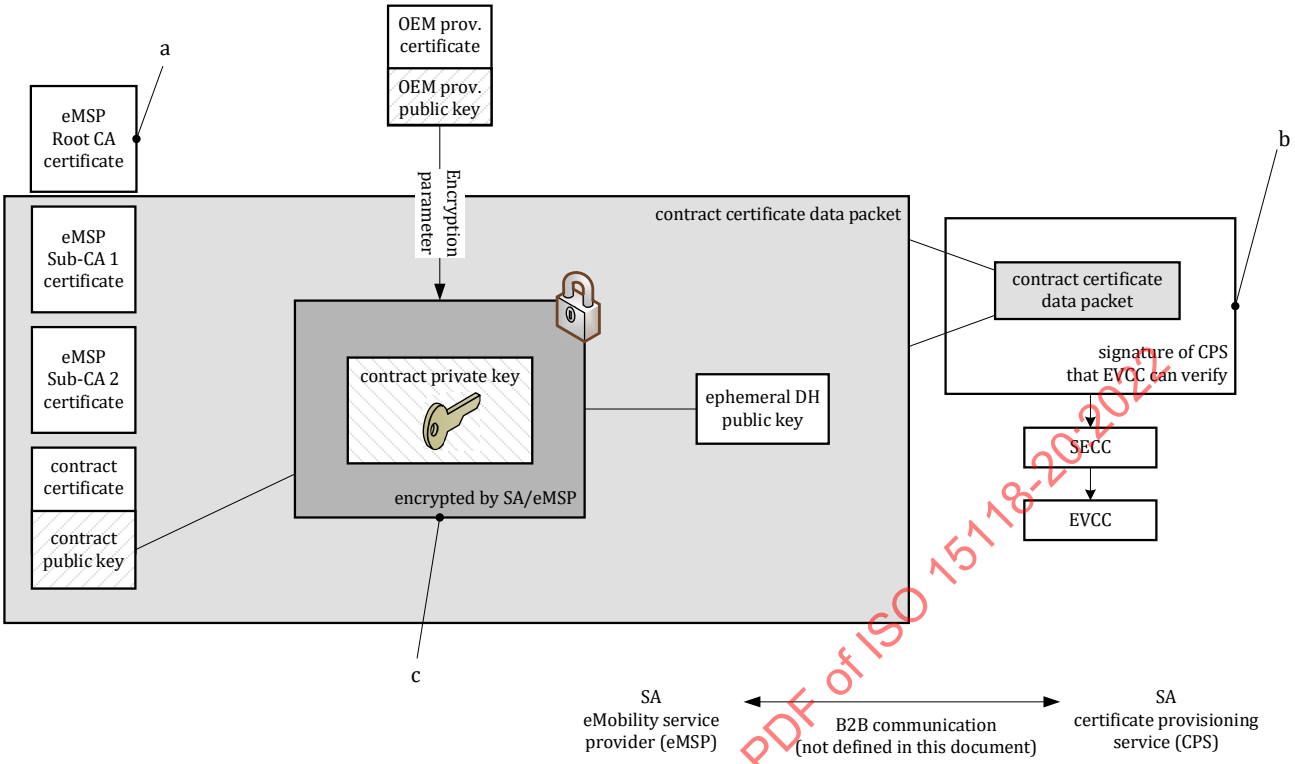
NOTE 11 In case CPS' certificates associated with the (elliptic curve) EC as specified by [V2G20-2674] have been revoked, but the SA (eMSP) requests it to sign the SignedInstallationData with the certificates based on (elliptic curve) EC as specified by [V2G20-2674], the CPS could not be able to oblige the SA (eMSP). It is not in the scope of this document to define the CPS behavior under these conditions. CPS can have certificates based on (elliptic curve) EC as specified by [V2G20-2319] that it can use for signing the SignedInstallationData.

NOTE 12 In case CPS does not have certificates based on (elliptic curve) EC as specified by [V2G20-2319], but the SA (eMSP) requests it to sign the SignedInstallationData with the certificates based on (elliptic curve) EC as specified by [V2G20-2319], the CPS could not be able to oblige the SA (eMSP). It is not in the scope of this document to define the CPS behavior under these conditions. CPS can have certificates based on (elliptic curve) EC as specified by [V2G20-2674] that it can use for signing the SignedInstallationData.

7.9.2.5.2 Contract certificate installation in EVCC without TPM 2.0

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved



Key

a This is the root certificate which the eMSP uses to derive the contract certificate. The root does not need to be present in the EVCC but the CPS needs to handle it according to well established guidelines.

b The signature of the CPS ensures that the data are authentic.

c Encrypted with AES in GCM mode (with authentication tag) based on ECDH shared secret with input coming from the public key of OEM provisioning certificate.

Figure 15 — Process for CertificateInstallationRes

Private keys belonging to contract certificates need to be protected (i.e. encrypted) when distributed from the SA (eMSP) to the EVCC. This subclause (and the subclauses within) describes how the contract certificate private key is encrypted and decrypted for installation in an EVCC that does not contain TPM 2.0.

If the EVCC contains a TPM 2.0, 7.9.2.5.3 (and its subclauses) applies instead.

7.9.2.5.2.1 Common requirements for contract certificate private key encryption/decryption mechanism for EVCC without TPM 2.0

[V2G20-2491] Each V2G entity shall have mechanisms to process ECDHE Key exchange. Public parameters are derived from the public ECDSA or EdDSA parameters.

[V2G20-2492] Additional authenticated data (AAD) shall be calculated by concatenating the PCID received/used in the CertificateInstallationReq message with capital letters and digits without separators (18 bytes), followed by the SKI value of the contract certificate included in the CertificateInstallationRes encoded as a hexa-decimal string with capital letters and digits according to IETF RFC 5234 (16 bytes).

NOTE 1 Refer to C.2 for further details of PCID.

NOTE 2 Refer to Table B.9 and Table B.10 further details of SKI value of the contract certificate.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 3 See Figure 16 for a pictorial reference.

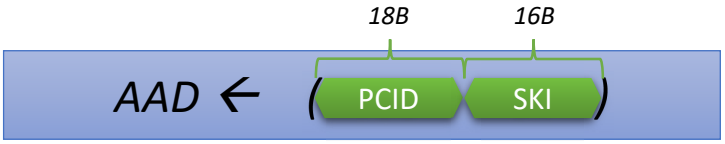


Figure 16 — AAD calculation

7.9.2.5.2.2 Contract certificate private key encryption mechanism for EVCC without TPM 2.0

7.9.2.5.2.2.1 Common requirements for encryption of 521-bit and 448-bit contract certificate private keys for EVCC without TPM 2.0

[V2G20-2493] The private key corresponding to the contract certificate shall be transmitted only in encrypted format within SECP521_EncryptedPrivateKey or X448_EncryptedPrivateKey element in the SignedInstallationData parameter of the CertificateInstallationRes message.

NOTE 1 SECP521_EncryptedPrivateKey is used when the contract certificate provided in SignedInstallationData is based on curve as defined by [V2G20-2674]. X448_EncryptedPrivateKey is used when the contract certificate provided in SignedInstallationData is based on curve as defined by [V2G20-2319].

NOTE 2 At the time of CertificateInstallationReq, if the SA intends to provide multiple different contract certificates based on different curves as defined by [V2G20-2674] and [V2G20-2319], the SA will need to send multiple different SignedInstallationData containers to the SECC and the EVCC can, at its/user's discretion, utilize the looping mechanism for CertificateInstallationReq to get and install all different contract certificates.

[V2G20-2494] The sender shall ensure that the authenticated encryption function used to encrypt data produces an authentication tag (also known as "tag" for short) of 128 bits. Refer to 5.2.1.2 of NIST Special Publication 800-38D for further details.

[V2G20-2495] When using 448-bit ephemeral public key in requirement [V2G20-2497], the sender shall not include any extra filler/padding bytes to reach DHPublicKey size of 133 bytes.

[V2G20-2496] Once the sender sends the data to the certificate provisioning service (CPS) for verification and signature generation, the sender shall irretrievably erase/delete/destroy the contract certificate private key, ECDHE private key and the session key as generated in 7.9.2.5.4, and the ciphertext.

NOTE 3 This ensures that the contract certificate private key cannot be compromised through a compromised SA. It also ensures that the ECDHE private key or session key are not reused. It further ensures that the same ciphertext is not sent out again to the receiver.

NOTE 4 This requirement is simply referring to unencrypted contract certificate private keys, ciphertext, session keys, etc. It does not refer to the SignedInstallationData that the eMSP gets back from the CPS which includes the CPS certificates and the CPS signature on the entire data. It also does not refer to the ECDH public key that the eMSP sends to the EVCC in DHPublicKey parameter.

7.9.2.5.2.2.2 Encryption of 521-bit contract certificate private key for EVCC without TPM 2.0

[V2G20-2497] The 521-bit private key corresponding to the contract certificate shall be encrypted by the sender (the SA (eMSP)) using the session key derived in the ECDHE protocol (see 7.9.2.5.4). The sender shall apply the algorithm AES-GCM-256 according to NIST

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

Special Publication 800-38D for this encryption. Per NIST Special Publication 800-38D, the private key shall be extended to 528 bits by padding 7 leading zero bits so that AES-GCM-256 can be applied. The Initialization Vector (IV) for this encryption shall be randomly generated before encryption and shall have a length of 96 bits with minimum entropy as defined by the implementer(s). The AAD for this encryption shall be calculated according to [V2G20-2492]. The encryption shall produce the 528-bit long ciphertext (encrypted private key) and 128 bit long authentication tag ("tag" for short).

NOTE 1 See Figure 17 for a pictorial reference.

NOTE 2 Explicit padding is required by [V2G20-2497] since the 521-bit private key is not byte-aligned.

NOTE 3 Refer to 7.3.7 for further details on random number generation.

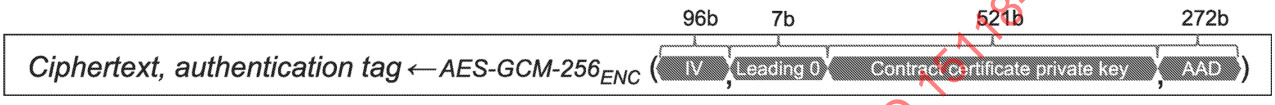


Figure 17 — 521 bit contract certificate private key encryption

[V2G20-2498] The byte order of all input data elements for AES-GCM-256 encryption, as specified by [V2G20-2497], shall be big-endian. This includes leading zeros needed in any data element to reach the length as prescribed by [V2G20-2497] or NIST Special Publication 800-38D.

NOTE 4 Padding of the plain text (private key) is not required when its length is a multiple of the block size of the encryption algorithm used.

The output of AES-GCM-256 encryption will be the ciphertext and the authentication tag. The 528 bit ciphertext contains the encrypted 521-bit contract certificate private key.

[V2G20-2499] The IV (as defined by [V2G20-2497]) shall be transmitted in the 12 most significant bytes of the SECP521_EncryptedPrivateKey field. The ciphertext (encrypted private key) of 66 bytes shall be written after the IV in the SECP521_EncryptedPrivateKey field. The tag (as defined by [V2G20-2494]) shall make up the 16 least significant bytes of the SECP521_EncryptedPrivateKey field.

Figure 18 provides this structure in pictorial format.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

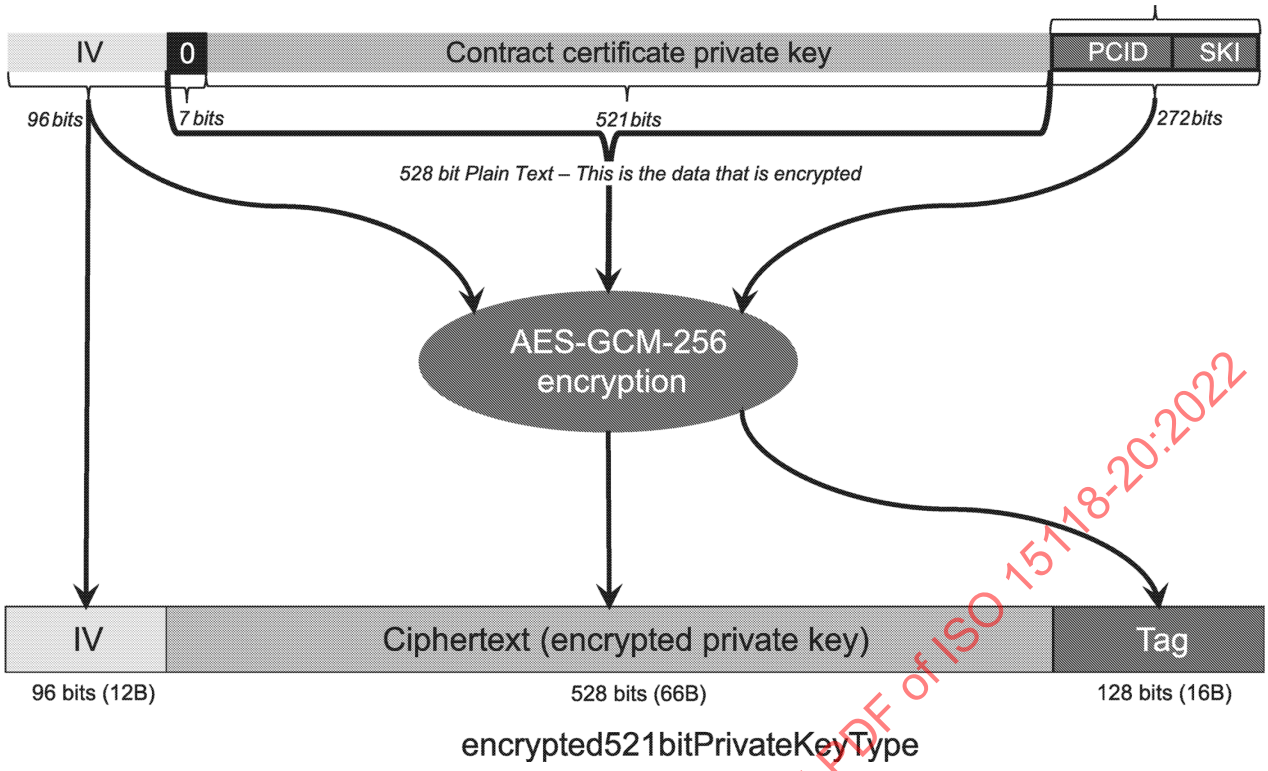


Figure 18 — encrypted521bitPrivateKeyType

7.9.2.5.2.2.3 Encryption of 448 bit contract certificate private key for EVCC without TPM 2.0

[V2G20-2500] The 448 bit private key corresponding to the contract certificate shall be encrypted by the sender (the SA (eMSP)) using the same session key used to encrypt the 521 bit private key in [V2G20-2497]. The sender shall apply the algorithm AES-GCM-256 according to NIST Special Publication 800-38D for this encryption. The initialization vector (IV) for this encryption shall be randomly generated before encryption and shall have a length of 96 bits with minimum entropy as defined by the implementer(s). The AAD for this encryption shall be calculated according to [V2G20-2492]. The encryption shall produce the 448 bit long ciphertext (encrypted private key) and 128 bit long authentication tag ("tag" for short).

NOTE 1 See Figure 19 for a pictorial reference.

NOTE 2 No explicit padding is required here since the 448-bit private key is byte aligned.

NOTE 3 Refer to 7.3.7 for further details on random number generation. Refer to 7.9.2.5.2.2.2 for further details of 521 bit contract certificate private key encryption.

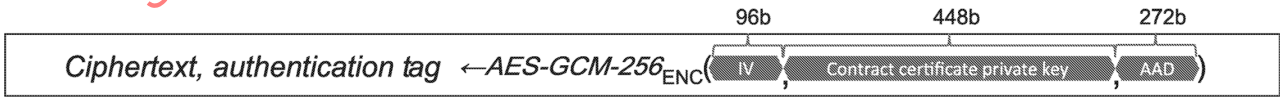


Figure 19 — 448 bit contract certificate private key encryption

[V2G20-2501] The byte order of all input data elements for AES-GCM-256 encryption, as specified by [V2G20-2500], shall be big-endian. This includes leading zeros needed in any data element to reach the length as prescribed by [V2G20-2500] or NIST Special Publication 800-38D.

NOTE 4 Padding of the plain text (private key) is not required when its length is a multiple of the block size of the encryption algorithm used.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

The output of AES-GCM-256 encryption will be the ciphertext and the authentication tag. The 448 bit ciphertext is the encrypted contract certificate private key.

[V2G20-2502] The IV (as defined by [V2G20-2497]) shall be transmitted in the 12 most significant bytes of the X448_EncryptedPrivateKey field. The ciphertext (encrypted private key) of 56 bytes shall be written after the IV in the X448_EncryptedPrivateKey field. The tag (as defined by [V2G20-2494]) shall make up the 16 least significant bytes of the X448_EncryptedPrivateKey field. Figure 20 provides this structure in pictorial format.

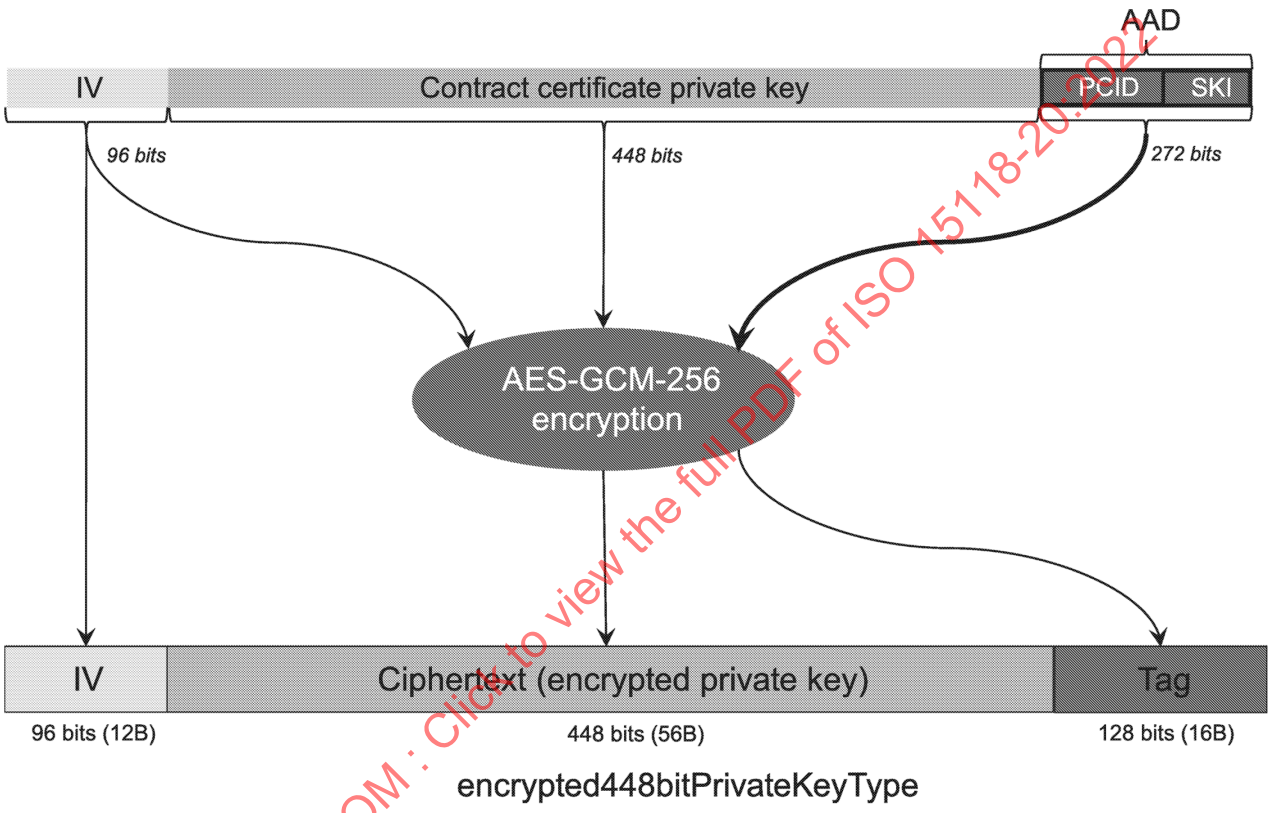


Figure 20 — encrypted448bitPrivateKeyType

7.9.2.5.2.3 Contract certificate private key decryption mechanism for EVCC without TPM 2.0

7.9.2.5.2.3.1 Common requirements for decryption of 521-bit and 448-bit contract certificate private keys for EVCC without TPM 2.0

[V2G20-2503] The receiver shall ensure that the authenticated decryption function used to decrypt data can take an authentication tag (also known as "tag" for short) of 128 bits as the second input. Refer to 5.2.2 of NIST Special Publication 800-38D for further details.

[V2G20-2504] If the decryption of either the 521-bit private key or 448-bit private key or both fails, the receiver shall reject the CertificateInstallationRes message as invalid.

NOTE NIST Special Publication 800-38D describes some of the decryption failures. The chosen AES-GCM-256 decryption implementation can describe further failure conditions and error codes.

7.9.2.5.2.3.2 Decryption of 521-bit contract certificate private key for EVCC without TPM 2.0

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2505] Upon reception of SECP521_EncryptedPrivateKey, the receiver (EVCC) shall decrypt the contract certificate private key using the session key derived in the ECDHE protocol (see 7.9.2.5.4) and applying the algorithm AES-GCM-256 according to NIST Special Publication 800-38D. The IV shall be read from the 12 most significant bytes of the SECP521_EncryptedPrivateKey field. The ciphertext (encrypted private key) shall be read from the 66 bytes after the IV in the SECP521_EncryptedPrivateKey field. The AAD for this decryption shall be calculated before decryption following [V2G20-2492] and [V2G20-2494]. The authentication tag shall be read from the 16 least significant bytes of the SECP521_EncryptedPrivateKey field.

NOTE 1 See Figure 21 for a pictorial reference of the decryption.

NOTE 2 Refer to Figure 18 further details of the SECP521_EncryptedPrivateKey structure.

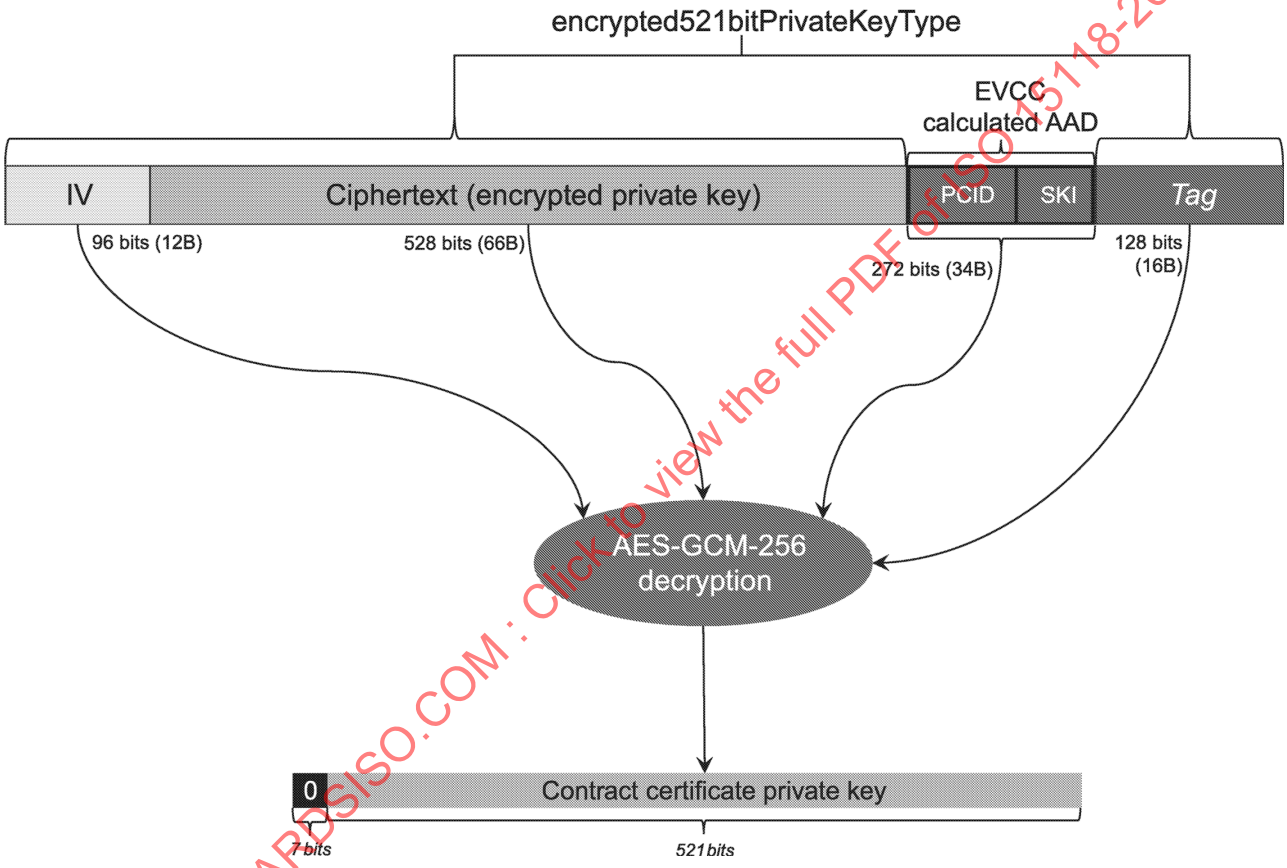


Figure 21 — 521 bit contract certificate private key decryption overview

When decrypting the data using AES-GCM-256, the order of data is important. The receiver should ensure that the input data to AES-GCM-256 decryption function/API follows NIST Special Publication 800-38D. Refer to Figure 22 for further details.

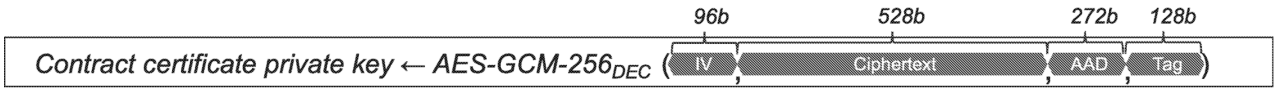


Figure 22 — 521 bit contract certificate private key decryption

[V2G20-2678] The EVCC shall consider the CertificateInstalaltionRes as invalid if the decrypted data does not contain 7 zeros in the most significant 7 bits.

[V2G20-2506] The EVCC shall use the 521 least significant bits of the decrypted data as the 521 bit contract certificate private key.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2507] Upon receipt of a contract certificate, the EVCC shall verify that the 521 bit private key received with the certificate is a valid 521 bit private key for that certificate:

- its value shall be strictly smaller than the order of the base point for secp521r1 curve;

AND

- multiplication of the base point with this value shall generate a key matching the 521 bit public key of the contract certificate.

7.9.2.5.2.3.3 Decryption of 448-bit contract certificate private key for EVCC without TPM 2.0

[V2G20-2508] Upon reception of X448_EncryptedPrivateKey, the receiver (EVCC) shall decrypt the contract certificate private key using the same session key used to decrypt the 521-bit private key in [V2G20-2505] and applying the algorithm AES-GCM-256 according to NIST Special Publication 800-38D. The IV shall be read from the 12 most significant bytes of the X448_EncryptedPrivateKey field. The ciphertext (encrypted private key) shall be read from the 56 bytes after the IV in the X448_EncryptedPrivateKey field. The AAD for this decryption shall be calculated before decryption following [V2G20-2492]. The authentication tag shall be read from the 16 least significant bytes of the X448_EncryptedPrivateKey field.

NOTE 1 See Figure 23 for a pictorial reference of the decryption.

NOTE 2 Refer to Figure 20 for further details of the X448_EncryptedPrivateKey structure.

NOTE 3 Refer to 7.9.2.5.2.3.2 for further details of 521 bit contract certificate private key decryption.

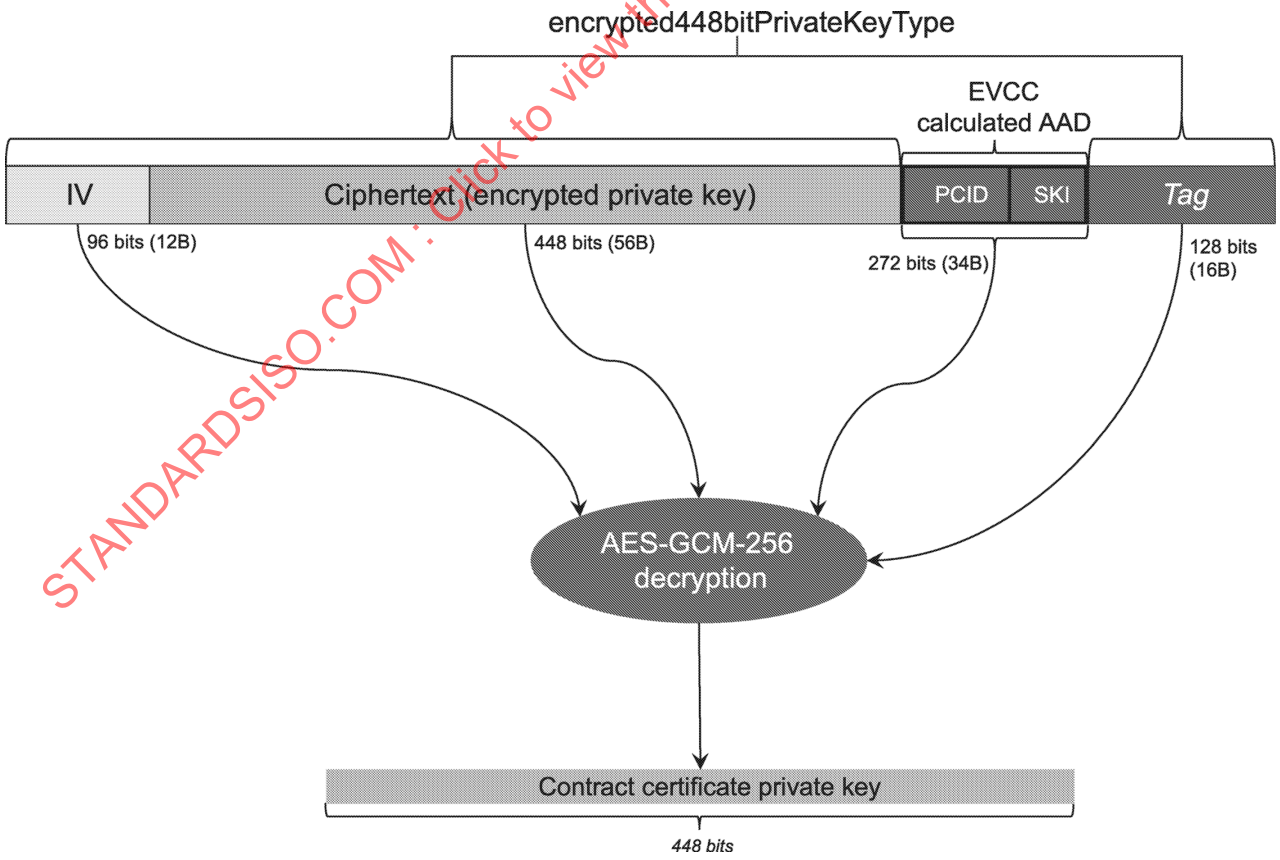


Figure 23 — 448 bit contract certificate private key decryption overview

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

When decrypting the data using AES-GCM-256, the order of data is important. The receiver should ensure that the input data to AES-GCM-256 decryption function/API follows NIST Special Publication 800-38D. Refer to Figure 24 for further details.



Figure 24 — 448 bit contract certificate private key decryption

[V2G20-2509] The EVCC shall use the 448 bit decrypted data as the 448 bit contract certificate private key.

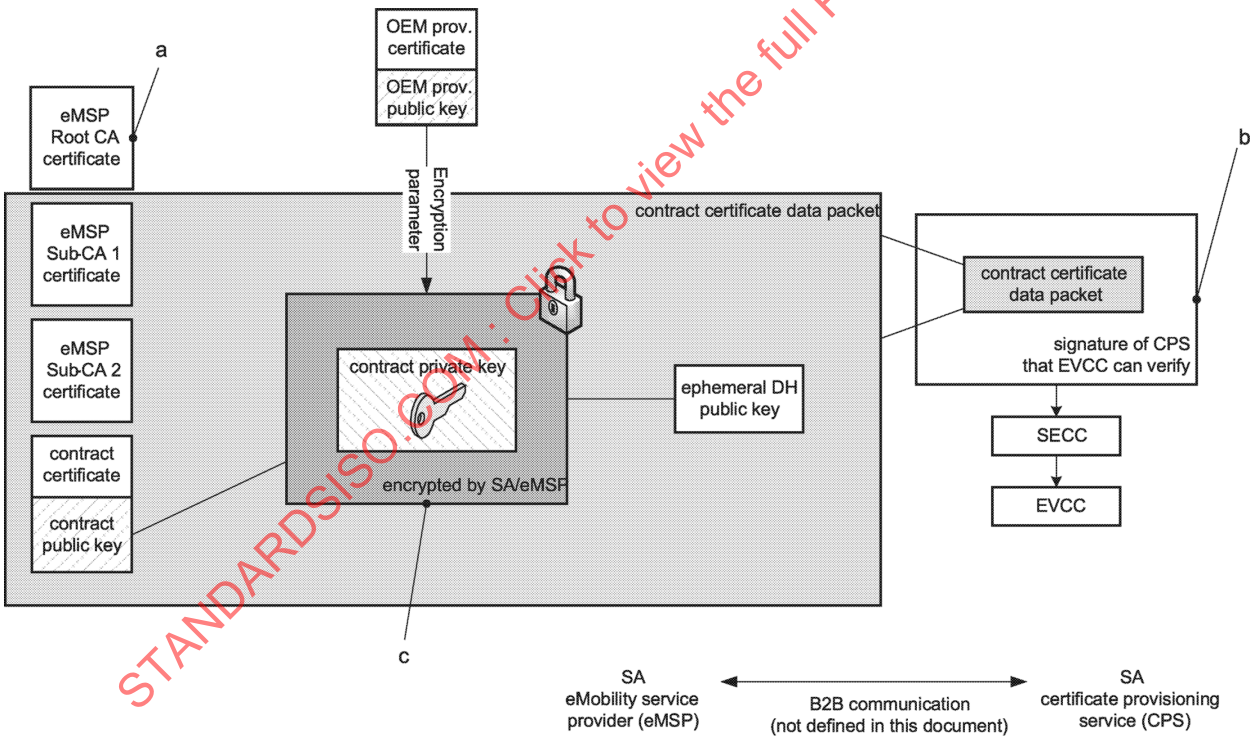
[V2G20-2510] Upon receipt of a contract certificate, the EVCC shall verify that the 448 bit private key received with the certificate is a valid 448 bit private key for that certificate:

- its value shall be strictly smaller than the order of the base point for x448 curve;

AND

- multiplication of the base point with this value shall generate a key matching the 448-bit public key of the contract certificate.

7.9.2.5.3 Contract certificate installation in EVCC with TPM 2.0



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Key

a This is the root certificate which the eMSP uses to derive the contract certificate. This root does not need to be present in the EVCC but the CPS needs to handle it according to well established guidelines.

b The signature of the CPS ensures that the data are authentic.

c Encrypted with AES in CFB mode based on ECDH shared secret with input from the TPM 2.0 TPM storage key (public key) coming from the OEM provisioning certificate and is additionally protected with an HMAC which binds the encrypted contract private key to the corresponding contract public key.

Figure 25 — Process for CertificateInstallationRes for EVCC equipped with TPM 2.0

© ISO 2022 – All rights reserved

Private keys belonging to contract certificates need to be protected (i.e. encrypted) when distributed from the SA (eMSP) to the EVCC. This subclause (and the subclauses within) describes how the contract certificate private key is encrypted and decrypted for installation in an EVCC that contains TPM 2.0. Use of TPM to protect the keys is optional. Refer to 7.3.6 (and its subclauses) for further details.

If the EVCC does not contain a TPM 2.0, 7.9.2.5.2 (and its subclauses) applies instead.

When an EVCC that contains TPM 2.0, a private key should be encrypted for a direct import into the EVCC's TPM 2.0 to exclude a situation when these critical keys are temporarily held unencrypted in the EVCC's memory and thus made vulnerable to compromise. A direct import of contract certificate private key into the EVCC's TPM guarantees the confidentiality of private key without having to trust the EVCC's software stack.

7.9.2.5.3.1 TPM 2.0 protected storage hierarchy for EVCC's keys

An asymmetric contract certificate key is a protected object in TPM 2.0, which consists of a public part and a private/sensitive part that follow a pre-defined format. The public part is described in the TPM key profile (see Table 19) and contains the contract certificate public key (in its "unique" field). The encrypted sensitive part contains the contract certificate private key. In this subclause, the term "contract certificate key" and "contract key" (or, similarly, OEM provisioning key) is used interchangeably to refer to the protected object representing the asymmetric contract certificate keys (or, similarly, OEM provisioning certificate keys). When a contract certificate public or private key is considered, it is named unambiguously. Similarly, when an OEM provisioning certificate public or private key is considered, it is named unambiguously.

TPM objects belong to a hierarchy. The import operation allows a protected object not created by a TPM such as an asymmetric contract key generated by an SA/eMSP to be incorporated into a protected storage hierarchy of the TPM. The parent for the contract key in this hierarchy is referred to as a "storage key". This subclause specifies the requirements that SAs should follow in order to provide certificates and keys in a fashion such that the EVCC can securely install asymmetric contract certificate keys under the protection of the TPM 2.0. Only TPM key profiles are specific to a particular (elliptic curve) EC, e.g. secp521r1 or Curve448. The rest of the requirements in this subclause and the subclauses within is valid for any ECC algorithm supported by EVCC.

The cryptographic protections for the contract key include encryption to prevent disclosure of the confidential contents, i.e. the private key and an integrity check to allow detection of modifications to either the confidential or the non-confidential portions of the asymmetric key object. The integrity value is computed in such a way that the confidential contract certificate private key will not be decrypted if it is not properly paired with the public area including its respective public key.

[V2G20-2511] The EVCC's TPM 2.0 shall contain a storage key pair. The storage key pair in the EVCC's TPM shall use the storage key profile from Table 19 for the default ECC algorithm (see [V2G20-2674]) or a separately defined TPM key profile for an alternative ECC algorithm (see [V2G20-2319]).

As the storage public key is used in ECDHE to encrypt the contract private key, the EVCC shall possess at least two storage keys to support the configuration mechanism defined in [V2G20-2320].

NOTE 1 OEM can generate and store a storage key pair into the EVCC's TPM in a secure environment.

NOTE 2 The storage key is a restricted decryption key, i.e. this key can only be used with specific commands and on strictly formatted objects, e.g. for direct import of specifically encrypted keys into the TPM. The storage key cannot be used for general-purpose decryption. This is one of the reasons why OEM provisioning key cannot be used as a storage key.

NOTE 3 This storage key can be a primary key of the TPM, i.e. a storage root key.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 19 — TPM key profiles for (elliptic curve) EC P-521/secp521r1 (public area)

Parameter	Content		
	Storage key	OEM provisioning key	Contract key
type	TPM2_ALG_ECC	TPM2_ALG_ECC	TPM2_ALG_ECC
nameAlg	TPM2_ALG_SHA512	TPM2_ALG_SHA512	TPM2_ALG_SHA512
objectAttributes	fixedTPM = 1 stClear = 0 fixedParent = 1 sensitiveDataOrigin = 1 userWithAuth = 1 adminWithPolicy = 0 noDA = 0 encryptedDuplication = 0 restricted = 1 decrypt = 1 sign = 0	fixedTPM = 1 stClear = 0 fixedParent = 1 sensitiveDataOrigin = 1 userWithAuth = 0 (1 if no policy) adminWithPolicy = 1 (0 if no policy) noDA = 0 encryptedDuplication = 0 restricted = 0 decrypt = 1 sign = 1	fixedTPM = 0 stClear = 0 fixedParent = 0 sensitiveDataOrigin = 1 userWithAuth = 0 (1 if no policy) adminWithPolicy = 1 (0 if no policy) noDA = 0 encryptedDuplication = 0 restricted = 0 decrypt = 0 sign = 1
authPolicy			
size	0	64 (0 if no policy)	64 (0 if no policy)
buffer	NULL	OEM chosen policy digest	OEM chosen policy digest
parameters			
symmetric.algorithm	TPM2_ALG_AES	TPM2_ALG_NULL	TPM2_ALG_NULL
symmetric.keyBits	256	NULL	NULL
symmetric.mode	TPM2_ALG_CFB	NULL	NULL
symmetric.details	NULL	NULL	NULL
scheme.scheme	TPM2_ALG_NULL	TPM2_ALG_NULL	TPM2_ALG_NULL
scheme.details	NULL	NULL	NULL
curveID	TPM2_ECC_NIST_P521	TPM2_ECC_NIST_P521	TPM2_ECC_NIST_P521
kdf.scheme	TPM2_ALG_NULL	TPM2_ALG_NULL	TPM2_ALG_NULL
kdf.details	NULL	NULL	NULL
Unique			
x.size	66	66	66
x.buffer	NULL	NULL	NULL
y.size	66	66	66
y.buffer	NULL	NULL	NULL

NOTE 4 Table 19 contains the TPM Key Profiles for the default ECC algorithm as defined by [V2G20-2321]. Further ECC algorithms supported by TPM 2.0 are specified in TCG algorithm registry. Once the specifications add support for Curve448, the implementers can follow the TPM 2.0 specifications to define the TPM key profiles for X448 (alternative ECC algorithm according to [V2G20-2319]) by adjusting the respective parameters in Table 19. The parameters specific to the curve type that need to be updated by the TPM key profiles include the fields "nameAlg", "authPolicy", "curveID" and "Unique".

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

7.9.2.5.3.2 OEM provisioning certificate for EVCC with TPM 2.0

[V2G20-2512] The OEM provisioning key pair shall be generated using the provisioning key profile from Table 19 for the default ECC algorithm (see [V2G20-2674]) or a separately defined TPM key profile for an alternative ECC algorithm (see [V2G20-2319]).

NOTE 1 The OEM can generate the OEM provisioning key pair in a secure environment. Key generation can be done in a secure fashion and can follow the necessary security guidelines. OEM can achieve this by generating the key pair in the EVCC's TPM using the protected functionality of the EVCC's TPM, which fulfils the respective security requirements (CC EAL4+).

NOTE 2 In case of a TPM-equipped EVCC, the OEM provisioning key pair can be generated in the EVCC's TPM and never leave this TPM. This ensures that only the intended EVCC has access to the OEM provisioning certificate private key and that this key cannot be copied to and used by any other system, e.g. to request contract certificates (identity theft). These guarantees are especially critical for this credential due to its long lifetime.

NOTE 3 After generating the OEM provisioning key pair in the EVCC's TPM, the OEM reads out the public portion of the OEM provisioning key pair in order to generate the OEM provisioning certificate.

[V2G20-2513] If the OEM provisioning key pair is generated outside the TPM, the parameters "fixedTPM" and "fixedParent" in the "objectAttributes" field of the public area shall be set to 0. If the OEM provisioning key pair is generated within the TPM, the parameters "fixedTPM" and "fixedParent" in the "objectAttributes" field shall be set to 1.

[V2G20-2514] The OEM provisioning key pair shall be stored in the EVCC's TPM underneath the storage key corresponding to the ECC algorithm used to generate this key (see [V2G20-2320]).

NOTE 4 The OEM can store the OEM provisioning key pair in the EVCC's TPM in a secure environment using secure mechanisms.

[V2G20-2515] If the OEM provisioning key pair in the EVCC's TPM is desired to be sealed to an OEM specific policy, this policy shall be provided in the "authPolicy" of the key (see Table 19).

NOTE 5 Policies are part of the TPM's enhanced authorization capability. A policy is a set of assertions that can be validated before authorizing key usage and can be used to, e.g. ensure that the EVCC booted into a trusted software state before authorizing the usage of the OEM provisioning key. Policies are calculated using the "nameAlg" of the key (see Table 19). The actual content of the sealing policy for the OEM provisioning key is up to the OEM.

[V2G20-2516] The OEM provisioning certificate for an OEM provisioning public key shall include the public key of its parent storage key pair in the EVCC's TPM to be used in ECDHE into the "TPMStorageKey" extension of the OEM provisioning certificate as defined in [V2G20-2594] and [V2G20-1226]. The uncompressed form is to be used exclusively.

NOTE 6 This allows the OEM to indicate that the EVCC is equipped with a TPM 2.0 and to provide the necessary information regarding the EVCC's TPM to the eMSP (or other SAs) in a cryptographically secure fashion.

NOTE 7 According to [V2G20-2595] this extension indicates that an SA/eMSP can use the method described in 7.9.2.5.3 (and its subclauses) to encrypt the private contract certificate key for this EVCC.

[V2G20-2517] If the contract certificate keys are supposed to be sealed to a policy, the digest of the EVCC's TPM policy shall be included in the "TPMPolicyDigest" extension of the OEM provisioning certificate as defined in [V2G20-2594] and [V2G20-1226]. The big-endian byte order rule shall be applied.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 8 The policy digest is part of the TPM key profile (see "authPolicy") and is created using the "nameAlg" algorithm of the key. In case of the default ECC algorithm as defined by [V2G20-2674], the EVCC's TPM policy digest uses SHA-512 and is 64 byte long (see Table 19).

NOTE 9 The actual content of the contract key sealing policy is up to the OEM.

7.9.2.5.3.3 Contract certificate private key encryption mechanism for EVCC with TPM 2.0

[V2G20-2518] In order to enable a direct import of the encrypted contract certificate private key into the EVCC's TPM, the contract certificate private key shall be encrypted with the TPM storage key of the EVCC's TPM from the OEM provisioning certificate extension (in contrast to [V2G20-2529] and [V2G20-2530]). This encryption shall comply with ISO/IEC 11889-1:2015, 23.3.2 and only use the outer duplication wrapper. This encryption shall use the values from Table 19 for the default ECC algorithm (see [V2G20-2674])or a separately defined TPM key profile for an alternative ECC algorithm (see [V2G20-2319]), whereby the contract certificate public key is inserted into the buffers of the contract key profile's "unique" field. If a policy digest is provided in the OEM provisioning certificate of this EVCC, the value of the policy digest shall be included in the encryption of the contract certificate private key via the "authPolicy" field of the contract key profile.

NOTE 1 The high-level overview of the contract certificate private key encryption for direct import into the EVCC's TPM is shown in Figure 26.

NOTE 2 The values from Table 19 are necessary to calculate the "Name" (see ISO/IEC 11889-1:2015, Clause 16) of the asymmetric contract key in TPM 2.0 or when parameter selection is based on the "new parent" (in this context the new parent would be the storage key). Table 19 also shows the values for the key profile in the case that the OEM chooses to not seal the contract key to a policy, i.e. for the case that the optional policyDigest field of the custom TPM certificate extension in the OEM provisioning certificate is omitted.

[V2G20-2519] The encryption, as specified by [V2G20-2518], requires the generation of a new seed (session key). The seed shall be generated using the method defined in 7.9.2.5.3., with the "TPM storage key" from the OEM provisioning certificate extension used as static public key for calculation of the session key as defined by [V2G20-2535]. Also refer to ISO/IEC 11889-3:2015, B.5.1 for further details with respect to TPM 2.0.

NOTE 3 The seed is used to derive HMAC and encryption keys (see Figure 26).

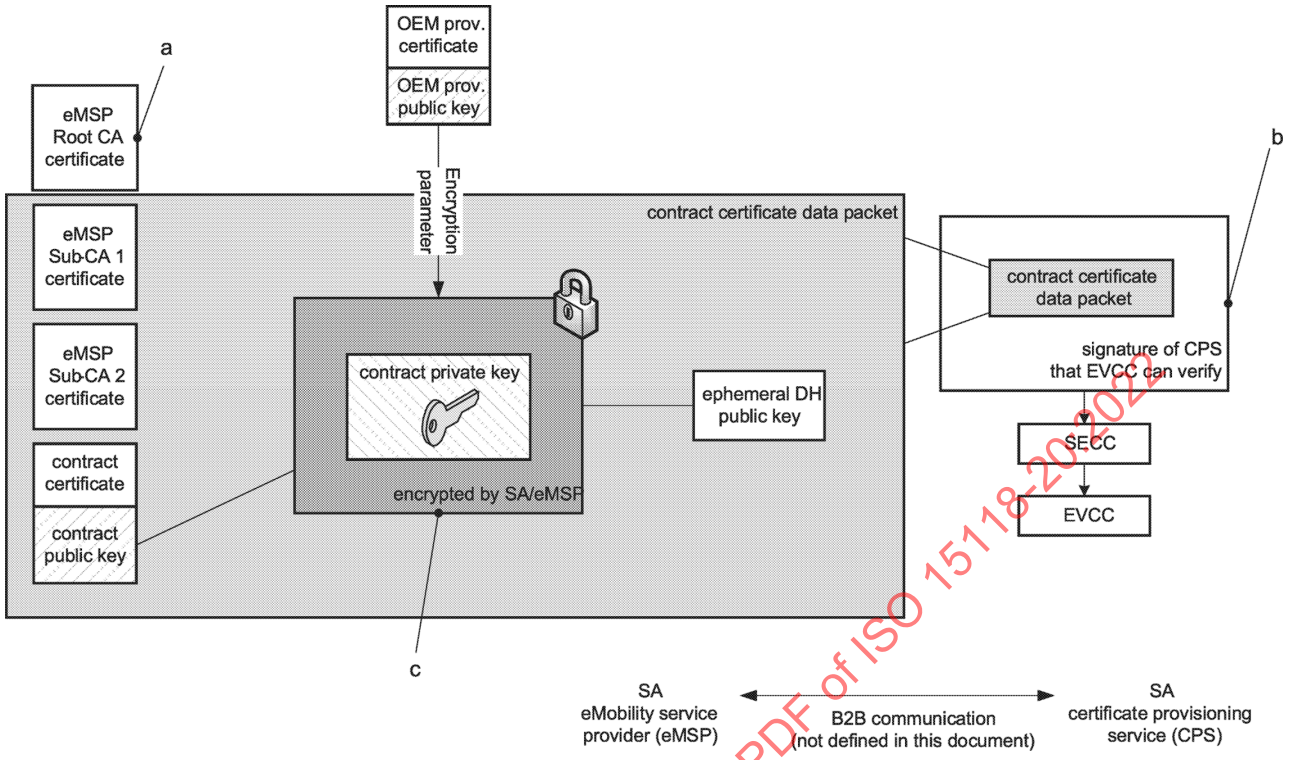
[V2G20-2520] The ephemeral public key of the eMSP (SA) shall be transmitted using the method defined in [V2G20-2489].

[V2G20-2521] The encrypted contract certificate private key shall be transmitted within TPM_EncryptedPrivateKey in the message CertificateInstallationRes if the private contract key was encrypted with the public storage key from the OEM provisioning certificate extension carrying TPM Information. The SA shall not add any padding to the encrypted key to increase its size to the maximum size of 206 bytes.

NOTE 4 At the time of CertificateInstallationReq, if the SA intends to provide multiple different contract certificates based on different curves as defined by [V2G20-2674] and [V2G20-2319], the SA will need to send multiple different SignedInstallationData containers to the SECC and the EVCC can, at its/user's discretion, utilize the looping mechanism for CertificateInstallationReq to get and install all different contract certificates.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved



Key

a This is the root certificate which the eMSP uses to derive the contract certificate. This root does not need to be present in the EVCC but the CPS needs to handle it according to well established guidelines.

b The signature of the CPS ensures that the data are authentic.

c Encrypted with AES in CFB mode based on ECDH shared secret with input from the TPM 2.0 TPM storage key (public key) coming from the OEM provisioning certificate and is additionally protected with an HMAC which binds the encrypted contract private key to the corresponding contract public key.

Figure 26 — Contract key encryption for direct import into EVCC's TPM 2.0 (for (elliptic curve) EC P-521/secp521r1)

NOTE 5 Key encryption process and structures illustrated in Figure 26 are valid for both currently specified (elliptic curve) ECs. In case of the Ed448 curve, the length of the contract private key, encrypted TPM 2.0 contract private key and HMAC should be adjusted.

NOTE 6 The SA can either send secp521 (see [V2G20-2674]) or Curve448 (see [V2G20-2319]) based encrypted contract private key using the TPM_EncryptedPrivateKey parameter.

[V2G20-2522] Once the sender sends the data to the certificate provisioning service (CPS) for verification and signature generation, the sender shall irretrievably erase/delete/destroy the contract certificate private keys (both the encrypted and unencrypted format), ECDHE private key and the session key as generated in 7.9.2.5.3.

NOTE 7 This ensures that the contract certificate private key cannot be compromised through a compromised SA. It also ensures that the ECDHE private key or session key are not reused. It further ensures that the same ciphertext is not sent out again to the receiver.

NOTE 8 This requirement is simply alluding to unencrypted contract certificate private keys, ciphertext, session keys, etc. It does not refer to the SignedInstallationData that the eMSP gets back from the CPS which includes the CPS certificates and the CPS signature on the entire data. It also does not refer to the ECDH public key that the eMSP sends to the EVCC in DHPublicKey parameter.

7.9.2.5.3.4 Direct import of contract certificate private key into EVCC with TPM 2.0

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2523] If the contract certificate private key was transmitted within the TPM_EncryptedPrivateKey field in the message CertificateInstallationRes and the EVCC with TPM 2.0 fully supports the respective curve, the EVCC shall directly import the encrypted contract key into its TPM underneath the storage key using the values from Table 19 for the curve P-521/secp521r1 or a separate TPM key profile for the curve Ed448.

NOTE 1 The direct import of encrypted contract keys into the TPM is done using the TPM2_Import() command with the storage key as new parent. Refer to ISO/IEC 11889-3:2015 for further details of TPM2_Import() command.

NOTE 2 The direct import of the encrypted contract certificate private key requires the EVCC to provide both the public and the encrypted private part of the contract key object as input to the TPM. The public part of the contract key object in TPM 2.0 consists of the contract key profile values from Table 19 (for the default ECC algorithm) with the contract certificate public key from the received contract certificate inserted into the "unique" field of this key profile.

NOTE 3 TPM_EncryptedPrivateKey can contain secp521 (see [V2G20-2674]) or Curve448 (see [V2G20-2319]) based encrypted contract private key. Assuming SA chooses the ECDHCurve parameter based on the ECC algorithm of the EVCC's OEM provisioning certificate, when the EVCC receives the parameter ECDHCurve set to "SECP521", TPM_EncryptedPrivateKey is expected to be 206 bytes long (see Figure 26). The respective value for an alternative ECC algorithm can be derived using TPM Key Profile for this algorithm.

7.9.2.5.4 Encryption/decryption (session) key generation for the distribution of secret keys

ISO 15118 communication uses an ephemeral-static Diffie-Hellman key exchange protocol to derive a session key where the receiver's keys are static. The SA (eMSP) uses this session key to transmit the private key in encrypted form to the EVCC.

In the ephemeral-static variant of the Diffie-Hellman protocol, the public key of the receiver (EVCC) does not change, i.e. is static, and is already known to the sender (eMSP). The sender, however, still uses an ephemeral public key that is transmitted to the receiver. In this manner, both sender and receiver can derive the same session key without a reply message from the receiver.

Since the SA uses ephemeral keys, the derived session keys will be different for each instance (distribution) of the secret keys (private key).

NOTE 1 The ephemeral-static Diffie-Hellman protocol does not provide perfect forward secrecy, i.e. if the static private key of the EVCC (OEM provisioning certificate) is leaked to an adversary, then this adversary can derive the respective session key(s) and decrypt any past and future communication between the eMSP and EVCC that relies on the private key of OEM provisioning certificate (or a key derived from the private key of OEM provisioning certificate) for secrecy. The same is true for the ephemeral private key of the eMSP (in case eMSP reuses this key, all transfers will be affected). In addition, the EVCC leaking the OEM provisioning private key allows an adversary to impersonate this EVCC and generate signatures as if the adversary is/was the EVCC, as the basic key used for signatures is the same as the basic key used for encryption, i.e. the private key of the OEM provisioning certificate.

[V2G20-2710] If SA uses the elliptic curve corresponding to signature algorithm specified by [V2G20-2319], the SA (eMSP) shall additionally support X448 as specified by IETF RFC 7748 for calculation of the ECDHE secret and key-derivation for the encryption of private keys.

[V2G20-2711] If EVCC uses the elliptic curve corresponding to signature algorithm specified by [V2G20-2319], the EVCC shall additionally support X448 as specified by IETF RFC 7748 for calculation of the ECDHE secret and key-derivation for the decryption of encrypted information like private keys.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2524] The SA (eMSP) shall support calculation of the ECDHE secret and the key derivation function, as specified by NIST Special Publication 800-56A, for the encryption of private keys.

[V2G20-2525] The EVCC shall support calculation of the ECDHE secret and the key derivation function, as specified by NIST Special Publication 800-56A, for the decryption of encrypted information like private keys.

[V2G20-2526] When the mechanism defined by [V2G20-2320] indicates usage of the (elliptic curve) EC as specified by [V2G20-2674], the SA (eMSP) shall generate a 521 bit ephemeral public/private key pair using elliptic curve secp521r1[SECG notation] as specified by NIST Special Publication 800-56A.

[V2G20-2527] When the mechanism defined by [V2G20-2320] indicates usage of the curve corresponding to the signature algorithm specified by [V2G20-2319], the SA (eMSP) shall generate a 448 bit ephemeral public/private key pair using ECC algorithm X448 as specified by IETF RFC 7748.

[V2G20-2528] The private key generated by [V2G20-2526] or [V2G20-2527] shall be used by the SA (eMSP) as ephemeral private key for calculation of the session key as defined by [V2G20-2535].

NOTE 2 It is assumed that the ephemeral private key is destroyed by the SA after the session key was derived.

[V2G20-2529] When the mechanism defined by [V2G20-2320] indicates usage of the (elliptic curve) EC as specified by [V2G20-2674], the "Subject Public Key" of the OEM provisioning certificate shall be used as static public key for calculation of the session key as defined by [V2G20-2535].

NOTE 3 Refer to the "subjectPublicKey" extension in B.7.1.

NOTE 4 If [V2G20-2595] applies, the TPM storage key from the respective OEM provisioning certificate extension is used by the SA as the public static key according to [V2G20-2518].

[V2G20-2530] When the mechanism defined by [V2G20-2320] indicates usage of the (elliptic curve) EC as specified by [V2G20-2319], the "Alternate Subject Public Key" of the OEM provisioning certificate shall be used as static public key for calculation of the session key as defined by [V2G20-2535].

NOTE 5 Refer to the "subjectAltPublicKey" extension in B.7.2.

NOTE 6 If [V2G20-2595] applies, the TPM storage key from the respective OEM provisioning certificate extension is used by the SA as the public static key according to [V2G20-2518].

[V2G20-2531] When the EVCC receives the parameter ECDHCurve set to "SECP521", it shall use the 1056 least significant bits of the DHPublicKey as the public key in calculation of the session key as defined by [V2G20-2535].

[V2G20-2532] When the EVCC receives the parameter ECDHCurve set to "X448", it shall use the 448 least significant bits of the DHPublicKey as the public key in calculation of the session key as defined by [V2G20-2535].

[V2G20-2533] If the EVCC receives the parameter ECDHCurve set to "SECP521", it shall use the OEM provisioning certificate private key along with the public key calculated from [V2G20-2531] for calculation of the session key as defined by [V2G20-2535].

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 7 Refer to B.7.1 for the OEM provisioning certificate profile associated with the algorithm specified by [V2G20-2674].

NOTE 8 If EVCC is equipped with TPM 2.0, the EVCC will perform the direct TPM import and apply requirement [V2G20-2523] instead.

[V2G20-2534] If the EVCC receives the parameter ECDHCurve set to "X448", it shall use the private key associated with the "Alternate Subject Public Key" of the OEM provisioning certificate along with the public key calculated from [V2G20-2532] for calculation of the session key as defined by [V2G20-2535].

NOTE 9 Refer to B.7.2 for the OEM provisioning certificate profile associated with the algorithm specified by [V2G20-2319] and [V2G20-2674].

NOTE 10 If EVCC is equipped with TPM 2.0, the EVCC will perform the direct TPM import and apply requirement [V2G20-2523] instead.

[V2G20-2535] For session key agreement, the ephemeral-static ECDHE protocol "6.2.2.2 One-Pass Diffie-Hellman, C(1, 1, ECC CDH)" as defined in NIST Special Publication 800-56A shall be used. The KDF shall be the "concatenation key derivation function", where the hash function shall be SHA512. In case the curve corresponding to ECC signature algorithm specified by [V2G20-2319] is chosen, the input parameters for KDF including the shared secret shall be derived according to IETF RFC 7748. The SA shall act as party U (as defined in said NIST document) and the EVCC shall act as party V. The protocol shall use elliptic curves as defined in Annex B. The algorithm ID shall be one character 0x01. The sender name ID U shall be one character "U" = 0x55, the receiver name ID V shall be one character "V" = 0x56. A symmetric encryption key of exactly 256 bits shall be derived.

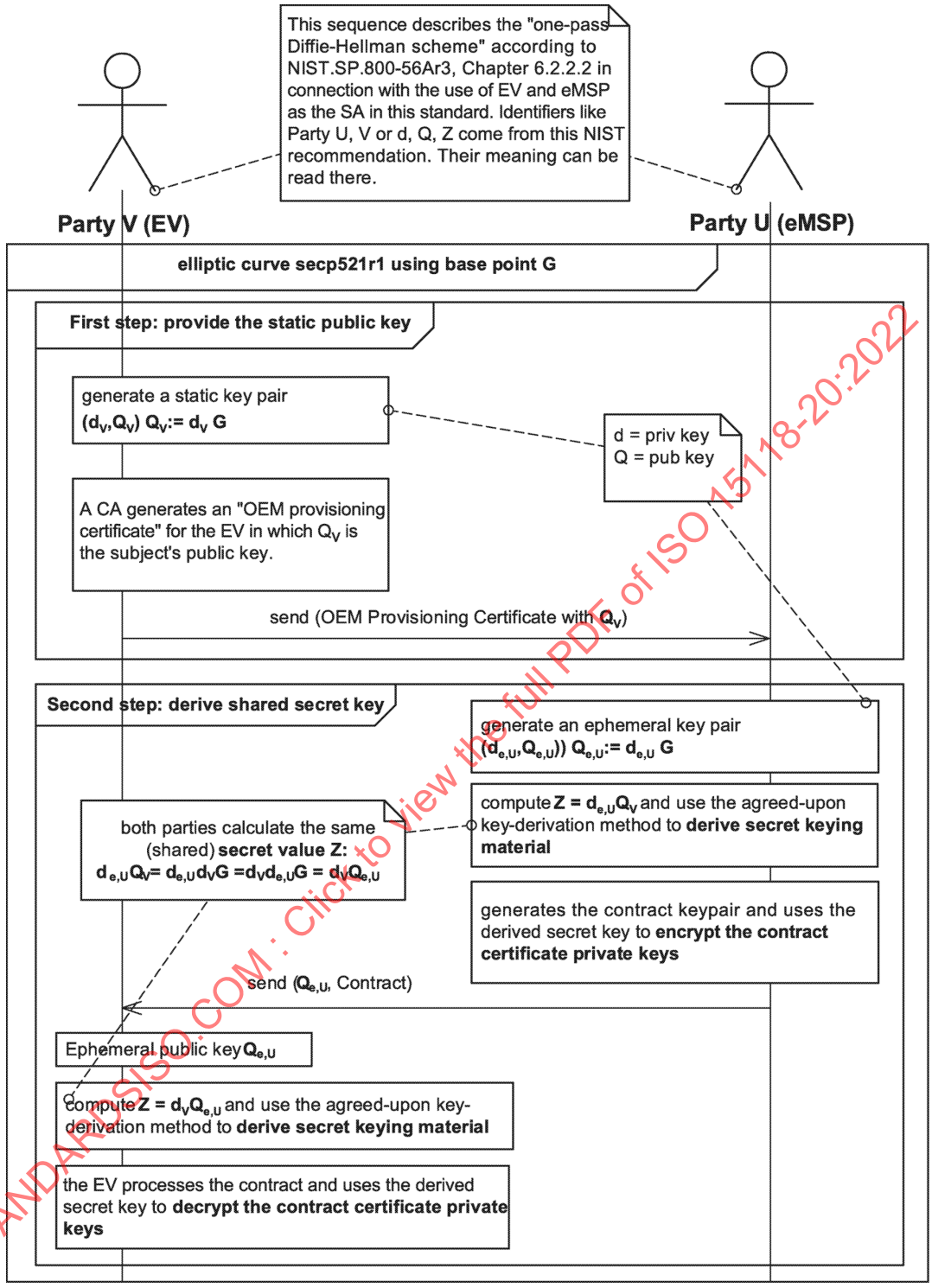
NOTE 11 The authenticity of the transmission is ensured by the surrounding signature. The authenticity check is vital for the security of the ECDHE protocol.

NOTE 12 For a more detailed explanation please refer to Figure 27.

[V2G20-822] A certificate whose key pair is used for ECDHE shall have its keyAgreement flag set. This applies to all OEM provisioning certificates and shall be enforced by all participating parties.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Figure 27 — Ephemeral-static Diffie-Hellman key agreement (informational depiction, do not use for implementation)

7.10 Application layer

7.10.1 SECC discovery protocol

7.10.1.1 General information

© ISO 2022 – All rights reserved

An EVCC uses the SECC discovery protocol (SDP) to get the IP address and port number of the SECC. The SDP client sends out SECC discovery request messages to the local link (multicast) expecting any SDP server to answer its request with an SECC discovery response message containing this information.

After the EVCC received the IP address and the port number of the SECC, it can establish a transport layer connection to the SECC (refer to 7.3.4).

Depending on the physical communication layer different messages are used for the SECC discovery.

[V2G20-2273] If PLC communication according to ISO 15118-3 is applied, the SDP client in the EVCC shall use SECC discovery message with the payload type SDPRequestPayloadID (see Table 14).

[V2G20-2274] If PLC communication according to ISO 15118-3 is applied, the SDP client in the EVCC shall only accept SDP response messages with the payload type SDPResponsePayloadID (see Table 14).

[V2G20-2275] If the SDP server shall handle charging services with PLC (according to ISO 15118-3), the SDP server shall accept SECC discovery request messages with payload type SDPRequestPayloadID (see Table 14).

[V2G20-2276] An SDP server which is used for PLC communication according to ISO 15118-3 shall use SECC discovery response message for PLC with payload type SDPResponsePayloadID (see Table 14).

[V2G20-2277] If wireless communication according to ISO 15118-8 is applied the SDP client in the EVCC shall use SECC discovery message for wireless communication with the payload type SDPRequestWirelessPayloadID (see Table 14).

[V2G20-2278] If wireless communication according to ISO 15118-8 is applied, the SDP client in the EVCC shall only accept SDP response messages with the payload type SDPResponseWirelessPayloadID (see Table 14).

[V2G20-2279] If the SDP server shall handle charging services with wireless communication (according to ISO 15118-8), the SDP server shall accept SECC discovery request messages with payload type SDPRequestWirelessPayloadID (see Table 14).

[V2G20-2280] An SDP server which is used for wireless communication according to ISO 15118-8 shall use SECC discovery response message for wireless communication with payload type SDPResponseWirelessPayloadID (see Table 14).

7.10.1.2 Communication architectures

7.10.1.2.1 Single SECC communication architecture

Within a single SECC communication architecture, multiple EVSEs share one common SECC. The SECC has a WLAN AP with an individual SSID. See Figure 28.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

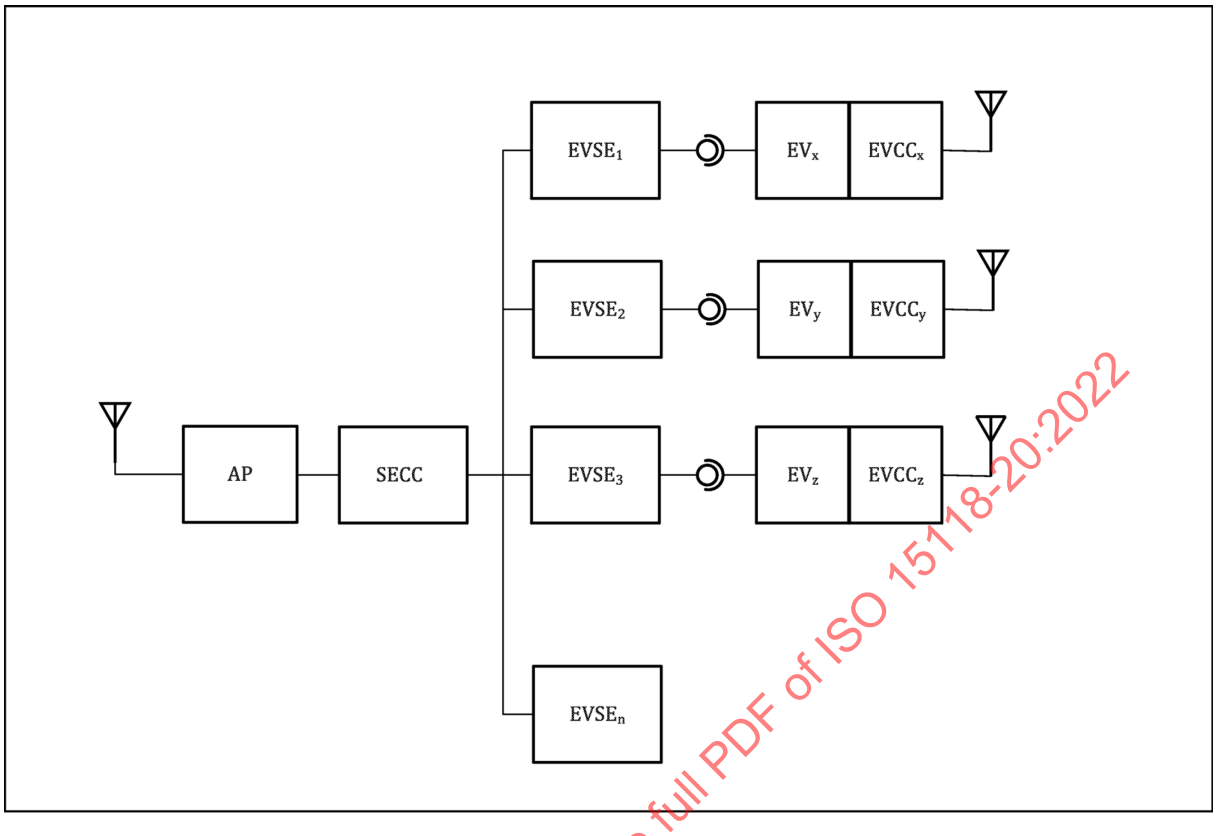


Figure 28 — Single SECC communication architecture

7.10.1.2.2 Multiple SECC communication architecture

Within a multiple SECC communication architecture, every EVSE has its own SECC. All the SECCs share a common WLAN AP with an individual SSID. See Figure 29.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

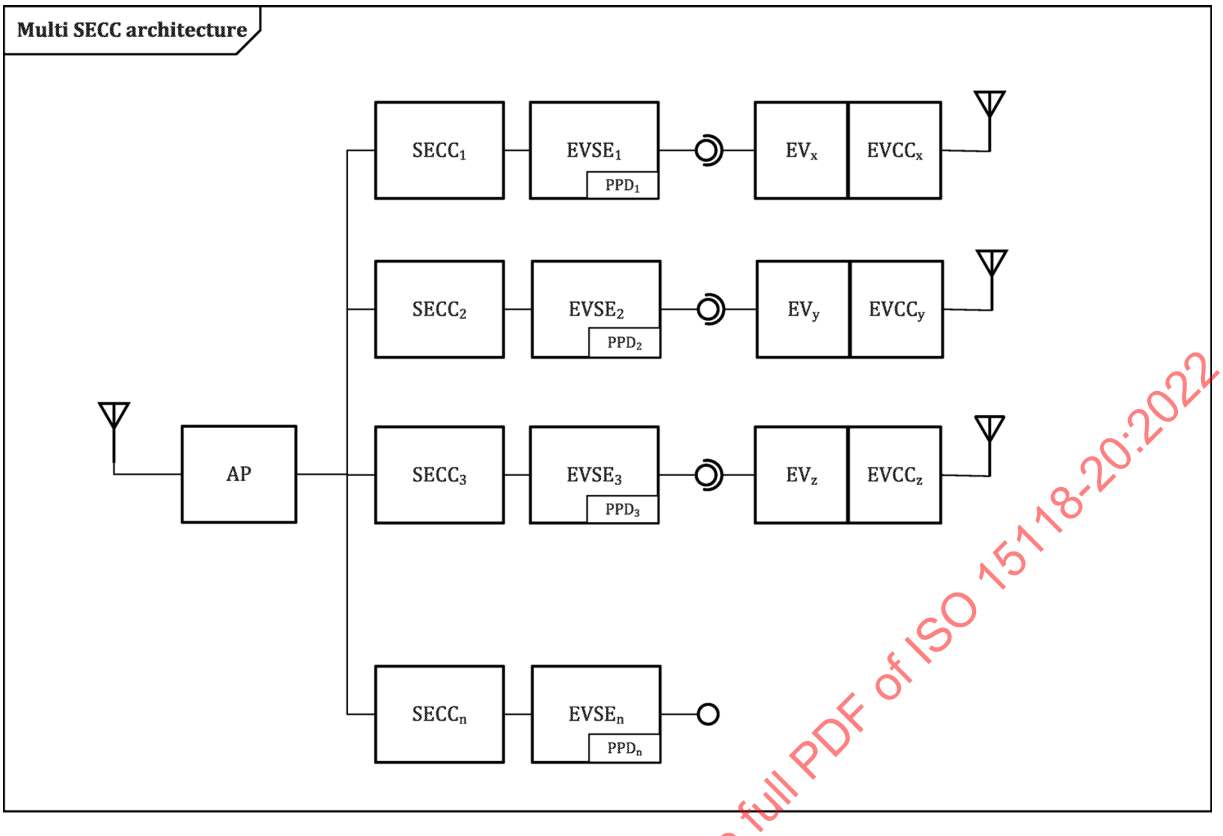


Figure 29 — Multiple SECC communication architecture

7.10.1.3 Supported ports

SDP is a UDP based protocol. The ports listed in Table 20 are used by SDP.

Table 20 — Supported UDP ports for SDP

Name	Protocol	Port number	Description
V2G_UDP_SDP_CLIENT	UDP (unicast)	Port number in the range of Dynamic Ports (49152-65535) as defined in IETF RFC 6335.	SDP client source port at the EVCC
V2G_UDP_SDP_SERVER	UDP (multicast)	15118	SDP server port which accepts UDP packets with a local-link IP multicast destination address.

[V2G20-123] An SDP server shall be accessible in the local link network.

NOTE 1 As common for internet technologies, SDP server can be implemented on the same physical device as the SECC and can also interface to the same IP address. If this is not the case, optimistic DAD as specified in IETF RFC 4429 will not lead to a benefit.

NOTE 2 IETF RFC 4429 has been updated IETF RFC 7527. These updates are considered to be included in this document.

[V2G20-124] An SDP client shall support the port V2G_UDP_SDP_CLIENT as defined in Table 20 for sending and receiving SDP messages.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-125] An SDP server shall support the port V2G_UDP_SDP_SERVER as defined in Table 20 for receiving and sending SDP messages.

NOTE 3 Depending on the implementation of the EVCC, the dynamically assigned V2G_UDP_SDP_CLIENT port is assigned once during or before the first transmission of a UDP packet to an SECC or can be dynamically re-assigned for each individual UDP request message and response. Also depending on whether messages are repeatedly sent, response messages can arrive asynchronously and cannot be associated to the exact corresponding request anymore.

[V2G20-126] The SDP client shall be able to handle asynchronously arriving SECC discovery response messages.

7.10.1.4 Protocol data unit

7.10.1.4.1 Structure

An SDP message is based on the V2GTP message format as defined in 7.8.3.1.

[V2G20-127] An SDP client shall support the definitions in 7.8.3.1.

[V2G20-128] An SDP client shall use a separate UDP packet for each request message.

[V2G20-129] An SDP client shall locate the first byte of the request message header as defined in Table 12 and Table 13 in the first byte of the UDP packet payload.

[V2G20-130] An SDP server shall support the definitions in 7.8.3.1.

[V2G20-131] An SDP Server shall use a separate UDP packet for each response.

[V2G20-132] An SDP server shall locate the first byte of the response message header as defined in Table 12 and Table 13 in the first byte of the UDP packet payload.

7.10.1.4.2 Header processing

An SDP header processing is based on the V2GTP message header processing as defined in 7.8.3.2.

[V2G20-133] An SDP client shall apply to the header processing as defined in 7.8.3.2.

[V2G20-134] An SDP server shall apply to the header processing as defined in 7.8.3.2.

7.10.1.5 SECC discovery request message for communication according to ISO 15118-3

The SDP client uses the SECC discovery request message to request the IP address and the port number of the SECC.

[V2G20-135] Only an SDP client shall send SECC discovery request messages.

[V2G20-136] An SDP client shall send SECC discovery request messages with the source IP address on which it expects the SECC discovery response message.

[V2G20-137] An SDP client shall send SDP request messages to destination port V2G_UDP_SDP_SERVER as defined in Table 20.

[V2G20-138] An SDP client shall send SDP request messages with source port V2G_UDP_SDP_CLIENT as defined in Table 20 on which it expects the SECC discovery response message.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-139] An SDP client shall send SECC discovery request message to the destination local-link multicast address (FF02:1) as defined in IETF RFC 4291.

[V2G20-1254] The SDP client shall send the SECC discovery request message with payload type SDPRequestPayloadID as defined in Table 14.

[V2G20-141] The SDP client shall send the SECC discovery request message with the payload length 2.

[V2G20-142] The SDP client shall send the SECC discovery request message with the payload as defined in Figure 30.

[V2G20-622] An SDP client shall send the payload in the order as shown in Figure 30. A byte with a lower number shall be sent before a byte with a higher number. The payload starts with byte 1 and ends with byte 2.

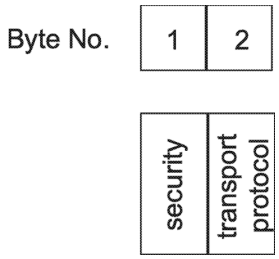


Figure 30 — SECC discovery request message payload

[V2G20-623] An SDP client shall use the encoding for the requested security option and the requested transport protocol as defined in Table 21.

Table 21 — SDP security and protocol option encoding

Description	Security	Transport protocol
Byte no. SDP request message	1	2
Byte no. SDP response message	19	20
Applicable values	0x00 = secured with TLS 0x01-0x0F = reserved 0x10 = No transport layer security 0x11-0xFF = reserved	0x00= TCP 0x01-0x0F = reserved 0x10 = reserved for UDP 0x11-0xFF = reserved

NOTE In this document, all communication after the SDP handshake uses TLS and TCP. Therefore, the parameter "Security" is typically set to "TLS" and the parameter "Transport Protocol" is typically set to "TCP". The value "No transport layer security" for the parameter "Security" is used to continue with unencrypted communication according to DIN SPEC 70121 or ISO 15118-2 with EIM.

7.10.1.6 SECC discovery response message for communication according to ISO 15118-3

The SDP server uses the SDP response message to respond to an SDP request message and provide the IP-address and the port of the SECC to the client.

[V2G20-143] The SDP server shall be able to extract the source IP address and source port of a received UDP packet (client IP address and port number) and send a UDP packet to the identified IP address and port number.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-144] An SDP server shall reply to any SECC discovery request messages with an SECC discovery response Message.

NOTE 1 This requirement ensures that an SDP server serving multiple clients can be reached at any time. This supports charging of multiple EVs at an EVSE with a single SECC.

[V2G20-145] An SDP client shall not reply to any SECC discovery request message.

[V2G20-146] An SDP server shall only send response messages after an SECC discovery request message has been received.

NOTE 2 For detailed timing requirements refer to requirements [V2G20-159] - [V2G20-162].

[V2G20-149] An SDP server shall send an SDP response with source port V2G_UDP_SDP_SERVER as defined in Table 20.

[V2G20-150] An SDP server shall send an SECC discovery response message to the SDP client which sent the SECC discovery request message.

[V2G20-151] An SDP server shall send an SECC discovery response message to the port of the SDP client which sent the SECC discovery request message.

[V2G20-1255] An SDP server shall send the SECC discovery response message with the payload type SDPResponsePayloadID as defined in Table 14.

[V2G20-153] An SDP server shall send the SECC discovery response message with payload length 20.

[V2G20-154] An SDP server shall send the SECC discovery response message with the payload as defined in Figure 31.

[V2G20-155] An SDP server shall send the payload in the order as shown in Figure 31. A byte with a lower number shall be sent before a byte with a higher number. The payload starts with byte 1 and ends with byte 20.

[V2G20-156] An SDP server shall send the fields "SECC IP address" and "SECC port" in big-endian format The most significant byte is sent first the least significant byte is sent last.

NOTE 3 The mechanism used by the SDP server to determine its own IP address is out of the scope of this document.

NOTE 4 The source IP address and the source port of a received UDP packet is usually provided by the TCP/IP stack.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

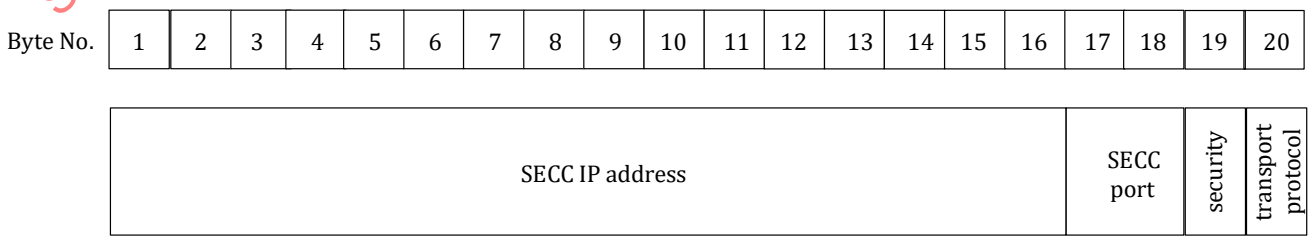


Figure 31 — SECC discovery response message payload

[V2G20-624] An SDP server shall use the encoding for the requested security option and the requested transport protocol as defined in Table 21 to define the supported

© ISO 2022 – All rights reserved

transmission security and transport protocol for the port provided in the same payload as the security and transport protocol bytes.

7.10.1.7 Timing and error handling

The process of SECC discovery is based on the application time out definitions as described in 7.10.1. This subclause describes additional timing and error handling for the SECC discovery protocol.

[V2G20-157] The SDP client shall count the number of SECC discovery request messages until a valid SECC discovery response message has been received.

[V2G20-158] The SDP client shall reset the counter for sent SECC discovery request messages after a valid SECC discovery response message has been received.

NOTE Valid means that a valid IP address was received and communication setup procedure can continue.

[V2G20-159] After sending an SECC discovery request message, the SDP client shall wait for an SECC discovery response message for at least 250 ms.

[V2G20-160] After unsuccessfully waiting for an SECC discovery response message the SDP client shall send a new SECC discovery request message and increment the counter for sent SECC discovery request messages.

[V2G20-161] If the SDP client has not received any valid SECC discovery response message after sending in maximum 50 consecutive SECC discovery request messages it shall stop the SECC discovery.

[V2G20-162] After unsuccessfully stopping the SECC discovery, the SDP client shall go to the same state as defined for a timeout (refer to Figure 8).

7.10.1.8 SECC discovery request message for communication according to ISO 15118-8

For the SDP clients for wireless communication, the requirements [V2G20-135], [V2G20-136], [V2G20-137], [V2G20-138], [V2G20-139] shall apply. Table 22 contains further information for the request message for wireless communication.

Information regarding P2PS/PPD and CouplingType value settings in the SDP request can be found below in Table 23.

Table 22 — SECC Discovery request message for wireless communication

Byte No.	Description
1	Security
2	Transport protocol
3 – 4	P2PS/PPD
5	CouplingType
6 – 25	EVID
26 – 62	EVSEID

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 23 — P2PS/PPD and CouplingType value setting in the SDP request

Description	P2PS/PPD	Coupling type
Byte no. SDP request message	3-4	5
Applicable values	Bit coding according to Table 24 Bit 7 of Byte 3 is reserved for future applications Byte 4 is reserved for future applications	0x00: Configuration according to IEC 61851-23-1 and EN 50696:2021, Annex A.2 (infrastructure mounted inverse pantograph, cross-rail contacts) 0x01: Configuration according to IEC 61851-23-1 and EN 50696:2021, Annex A.3 (infrastructure mounted inverse pantograph, in line contacts) 0x02: Configuration according to IEC 61851-23-1 and EN 50696:2021, Annex A.4 (infrastructure mounted pantograph, contact dome) 0x03: Configuration according to IEC 61851-23-1 and EN 50696:2021, Annex B EV mounted pantograph 0x04: Configuration according to IEC 61851-23-1 and EN 50696:2021, Annex C, ACD mounted underneath the EV 0x05: Configuration according to IEC 61851-23-1 and EN 50696:2021, Annex D, ACD mounted on infrastructure to the side or roof of EV 0x10 = WPT (IEC 61980) 0x20 = ACD-U (Manipulator on Infrastructure) 0x21 = ACD-U (Manipulator on EV) 0x30 = ACD-S 0x40 = Conductive manual 0xFF = n.a.

Table 24 below specifies the bit coding for Byte No.3 and No.4 for an SDP request.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 24 — Bit coding for Byte No.3 and 4 of SDP request

Byte No.	3								4							
Bit	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
PPD on Infrastructure								x								
PPD on EV							x									
WPT_LF on infrastructure						x										
WPT_LF on EV					x											
WPT_Cam on EV				x												
ACD_U_Infrared			x													
ACD_directed_WLAN		x														

An overview of the SDP request message for wireless communication option encoding can be found in Table 25.

Table 25 — SECC Discovery request message for wireless communication option encoding

Element	Type	Semantics
EVID	ASCII encoded string of max 20 Byte: ALPHA = %x41-5A / %x61-7A; according to IETF RFC 5234 (7-Bit ASCII), case-insensitive (IETF RFC 7405) DIGIT = %x30-39; according to IETF RFC 5234 (7-Bit ASCII)	Any (temporary) ID that uniquely identifies the EV.
EVSEID	ASCII encoded string of max 36 Byte: ALPHA = %x41-5A / %x61-7A; according to IETF RFC 5234 (7-Bit ASCII), case-insensitive (IETF RFC 7405) DIGIT = %x30-39; according to IETF RFC 5234 (7-Bit ASCII)	Any ID that uniquely identifies the EVSE and the power outlet the EV is intended to be connected to.

NOTE 1 The elements EVID and EVSEID as they are used in the SDP messages serve as identifiers of an EV and an EVSE. There is no relation to other identifiers which are applied during the exchange of the application layer messages.

[V2G20-2281] If an EVCC cannot provide data for the EVID, the EVID shall be set to "ZZ00000"

[V2G20-2284] For wireless communication the SDP client shall send the SECC discovery request message with the payload type SDPRequestWirelessPayloadID as defined in Figure 20.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2285] For wireless communication an SDP client shall send the payload in the order as shown in Figure 3. A byte with a lower number shall be sent before a byte with a higher number.

[V2G20-2286] For wireless communication the SDP client shall send the SECC discovery request message with the payload type value SDPRequestWirelessPayloadID as defined in Table 14, Figure 3 and Figure 4.

[V2G20-2287] The SDP client shall stop sending SECC discovery request messages after a valid SECC discovery response message has been received with "DiagStatus" = "finished with EVSEID" or "finished without EVSEID".

[V2G20-2288] For wireless communication the SDP client shall wait at least 250 ms before sending the next SECC discovery request message after an SECC discovery response message has been received with the payload parameter "DiagStatus" = "ongoing".

[V2G20-2289] For wireless communication the SDP client shall set the timeout V2G_EVCC_CommunicationSetup_Timeout to the value as defined in Table 221, reset the V2G_EVCC_CommunicationSetup_Timer and start monitoring the V2G_EVCC_CommunicationSetup_Timer when a successful TCP/TLS connection is established.

NOTE 2 Valid SECC discovery response message means that the EV was able to establish a functioning IP communication to the SECC using the IP address and port sent by the SECC discovery response message.

7.10.1.9 SECC discovery response message for communication according to ISO 15118-8

The SDP server uses the SDP response message to respond to an SDP request message and provide the IP-address and the port of the SECC to the client.

For an SDP server for wireless communication the requirements [V2G20-143], [V2G20-146], [V2G20-149], [V2G20-150] and [V2G20-151] shall apply.

[V2G20-2290] A SDP server for wireless communication in a single SECC architecture shall reply to any SECC discovery request message with an SECC discovery response message.

Table 26 contains further information for the response message for wireless communication.

Information regarding SECC discovery response message payload for wireless communication can be found below in Table 27.

Table 26 — SECC Discovery response message for wireless communication

Byte No.	1-16	17-18	19	20	21	22	23-59
	SECC IP address	SECC Port	Security	Transport protocol	DiagStatus	CouplingType	EVSEID

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 27 — SECC discovery response message payload for wireless communication

Description	DiagStatus	Coupling type	EVSEID
Byte no. SDP response message	21	22	23-59
Applicable values	0x00 = ongoing 0x01 = finished with EVSEID 0x02 = finished without EVSEID 0x10 = Error - no SECC	0x00: Configuration according to IEC 61851-23-1 and EN 50696:2021, Annex A.2 (infrastructure mounted inverse pantograph, cross rail contacts) 0x01: Configuration according to IEC 61851-23-1 and EN 50696:2021, Annex A.3 (infrastructure mounted inverse pantograph, in line contacts) 0x02: Configuration according to IEC 61851-23-1 and EN 50696:2021, Annex A.4 (infrastructure mounted pantograph, contact dome) 0x03: Configuration according to IEC 61851-23-1 and EN 50696:2021, Annex B EV mounted pantograph 0x04: Configuration according to IEC 61851-23-1 and EN 50696:2021, Annex C, ACD mounted underneath the EV 0x05: Configuration according to IEC 61851-23-1 and EN 50696:2021, Annex D, ACD mounted on infrastructure to the side or roof of EV 0x10 = WPT (IEC 61980) 0x20 = ACD-U (manipulator on Infrastructure) 0x21 = ACD-U (manipulator on EV) 0x30 = ACD-S 0xFF = n.a.	

[V2G20-2291] For wireless communication the SDP server shall send the SECC discovery response message with the payload type value SDPResponseWirelessPayloadID as defined in Table 14, when it has received a request with payload type SDPRequestWirelessPayloadID.

[V2G20-2292] For wireless communication the SDP server shall send the SECC discovery response message with the payload type value SDPResponseWirelessPayloadID as defined in

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 14 if the element "CouplingType" of the SDP request message matches with the "CouplingType" type of the EVSE. Otherwise the SDP server shall not respond.

[V2G20-2293] For wireless communication the SDP server shall send the SECC discovery response message with the payload as defined in Table 26 and Table 27.

[V2G20-2294] For wireless communication an SDP server shall send the payload in the order as shown in Table 26 and Table 27. A byte with a lower number shall be sent before a byte with a higher number. The payload starts with byte 1 and ends with byte 59.

7.10.1.10 SDP for wireless communication application for ACDP

WLAN communication according to ISO 15118-8 is deployed for, for example, ACDP with infrastructure mounted pantograph and uses the multiple SECC communication architecture. Each EVSE has its own pairing and positioning device (PPD) that provides information about the EVID when an EV is in close proximity to the ACDP. The EVCC uses the EVID information provided by the PPD within the SDP response message to initiate the correct associated communication between the EVCC and the related EVSE. For this the PPD will use the same EVID which is send in the SDP request message.

Furthermore, the PPD may provide relative position information between the EV and the ACDP. This position information can be used to guide the driver to the correct EV x and y charging position within the mechanical tolerances of the ACDP. Only within these tolerances the EVSE is allowed to initiate the activation of the ACDP and to start the charging procedure.

The pairing and positioning device (PPD) provides a spatial selective orthogonal communication channel to the WLAN communication when the EV is in close proximity to the ACDP in order to resolve the undetermined association of the EV communication to the ACDP's EVSE. The PPD consists of a marker located on the EV and a receiver located in the ACDP infrastructure. The pairing and positioning identification method is not in the scope of this document. A possible design of a PPD is presented in Annex D.

[V2G20-4100] For pairing and positioning device support the SDP client shall send SECC discovery request messages with the element EVID set the element PPD/P2PS to "PPD on infrastructure" according to Table 24 and leave the element EVSEID free.

NOTE 1 EVID can be set to a random number for privacy purposes. If no privacy is required, the EVID can be a readable string, e.g. as on an EV number plate.

[V2G20-4101] For pairing and positioning device support the SDP client shall reset the counter for sent SECC discovery request messages after a valid SECC discovery response message has been received with the payload parameter "DiagStatus = Ongoing".

[V2G20-4102] For wireless communication an SDP server shall send the SECC discovery response message with the payload parameter "DiagStatus = Ongoing" as long as no EVID is detected by the pairing and positioning device when the element PPD/P2PS of the SDP request was set to value "PPD on infrastructure" according to Table 24. The parameter EVSEID may be sent optionally.

NOTE 2 In case of "DiagStatus = Ongoing" the parameter EVSEID can be used in the EV to inform the driver about the available charging points.

[V2G20-4103] For wireless communication an SDP server shall send the payload parameters SECC IP address and port number and DiagStatus set to "Finished with EVSEID" or "Finished without EVSEID" as soon as the EVID has been detected by the pairing and positioning device.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

7.10.1.10.1 Option for large number of SECC

The following optional requirements may be optional implemented in order to avoid a message avalanche of SDP response messages, when there is a very large number of SECCs in a depot in the same network.

[V2G20-4104] For early association support an SDP server shall wait a random number of milliseconds that is smaller than 100 ms before sending the SECC discovery response message with the payload parameter "DiagStatus = Finished with EVSEID" or "DiagStatus = Finished without EVSEID" as long as no EVID has been received by the pairing and positioning device that matches with the EVID of the SDP request. The parameter EVSEID may be sent optionally.

[V2G20-4105] For early association support and when [V2G20-4104] applies an SDP server may abort a pending SDP response message related to an SDP request with EVID when recognizing an SDP response message of another SDP server containing the same EVID.

7.10.1.10.2 Loss of association PPD exception handling

After the SDP process has been completed successfully the EV and the EVSE are associated correctly and the high-level communication starts. The association status of EV and EVSE shall continuously be supervised by the consistency of the received EVID of the PPD until the ACDP is activated successfully. If the detected EVID changes or disappears the V2G process aborts.

A typical reason for losing the association status is when the driver was closely approaching an ACDP and decides to head for another ACDP afterwards. In such a case the association will first be established with the first ACDP. As soon as the EV leaves the PPD detection zone the existing association will quit. This is then a loss of association event. In case of a loss of association event the ACDP_VehiclePositioningRes will have the response code "FAILED_AssociationError".

7.10.1.11 SDP for wireless communication application for WPT

By setting the CouplingType in the SDP request message to "WPT" the EV indicates that in intends to use wireless power transfer. As a consequence the P2PS/PPD parameter of the SDP request should be coded according to the P2PS options of the EV, which are featured for WPT.

Setting no bit typically indicates that the EV has no additional P2PS means and thus would apply WPT defaults or proprietary means. Since PPD is not used in combination with WPT, an error response of the SDP server can be expected if the P2PS/PPD parameter is coded for PPD support. Refer to IEC 61980-2 for P2PS specification and usage.

8 Application layer messages

8.1 General information and definitions

The vehicle to grid (V2G) application layer message definition describes the client-server based message exchange between EVCC and SECC for the purpose of initializing and configuring the energy transfer process from or to an EV. The message set is designed to cover the use cases defined in ISO 15118-1. The messages and the required message flow (i.e. communication protocol) represent the application layer according to the OSI layered architecture model.

A V2G message uses the EXI-based Presentation Layer as described in 7.9.1. The communication between EVCC and SECC at application layer level is based on client/server architecture. The EVCC always acts as a client (service requester) during the entire charging process, whereas the SECC always acts as a server (service responder). Hence the EVCC always initiates communication by sending a request message to

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

the SECC, then the SECC returns the corresponding response message. All messages exchanged between EVCC and SECC are described with their syntax and their semantics in 8.2 and 8.3. The entire XML schema definition describing V2G message set is included in Annex A.

8.3.4 defines the V2G message and respective message elements required to be supported for a certain set of use case elements described in ISO 15118-1.

8.5 defines message timing and error handling for the V2G communication message exchange.

Message sequences are shown in 8.6.

V2G communication consists of two different message types:

- V2G application layer protocol handshake messages (refer to 8.2),
- V2G application layer messages (refer to 8.3).

[V2G20-809] When transmitting application layer messages the big-endian byte order rule shall be applied: the most significant byte is sent first, the least significant byte is sent last.

8.2 Protocol handshake definition

[V2G20-2129] If in the supportedAppProtocolReq, an energy transfer mode is offered based on ISO 15118-20, all features implemented for this energy transfer mode in older generations of the document still need to be supported for ISO 15118-20.

NOTE The impact of [V2G20-2129] is described by the following examples:

- An EVCC currently supports DIN SPEC 70121 and now wants to support ISO 15118-20 (this document) as well. Since DIN SPEC 70121 only offers the minimum feature set, implementing even the most minimal feature set of ISO 15118-20 for DC will suffice.
- An EVCC currently supports DIN SPEC 70121 DC & PnC according to ISO 15118-2. It now wants to support BPT/DC according to ISO 15118-20 (this document). Based on [V2G20-2129], the EVCC also supports PnC for this document, as otherwise a feature would only be supported with ISO 15118-2 and not with this document, potentially forcing the usage of ISO 15118-2 even when both sides support this document.
- An EVCC currently supports AC & PnC according to ISO 15118-2 and now wants to support BPT/DC according to ISO 15118-20 (this document). The EVCC will transmit a supportedAppProtocolReq with two entries. One entry uses the namespace "urn:iso:15118:2:2013:MsgDef" while the other one uses "urn:iso:std:iso:15118:-20:DC". Since it becomes clear to the SECC from the namespace "urn:iso:std:iso:15118:-20:DC" that the EVCC only supports DC according to (this document), an AC SECC will select ISO 15118-2, while a DC SECC will select this document.

8.2.1 Handshake sequence

[V2G20-165] Before starting the application layer message exchange, an appropriate application layer protocol including its version shall be negotiated between the EVCC and the SECC.

In order to negotiate the protocol between the EVCC and the SECC the following application layer protocol handshake is performed.

[V2G20-166] The EVCC shall initiate the handshake by sending a supportedAppProtocolReq message as depicted in Figure 32 to the SECC. This request message provides a list of charging protocols supported by the EVCC.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-167] Each entry in the list of supported EVCC protocols shall include the ProtocolNamespace, the VersionNumberMajor and VersionNumberMinor, the unique SchemaID dynamically assigned by the EVCC and the priority of the protocol entry. The priority in the EVCC request message enables the EVCC to announce the preferred application layer protocol where priority equal to "1" indicates the highest priority and priority equal to "20" indicates the lowest priority. The number of protocols included in the request message is limited to 20.

[V2G20-168] The SECC shall respond with the supportedAppProtocolRes message as depicted in Figure 33 indicating the protocol to be used for the subsequent message exchange by both, the EVCC and the SECC.

[V2G20-169] The response message shall include a ResponseCode and the SchemaID of the protocol/schema which is agreed as application protocol for the following V2G communication session. Thereby, the SECC shall select from its own list of supported protocols the protocol with highest priority indicated by the EVCC.

[V2G20-170] The SECC shall confirm (positively respond with ResponseCode "OK_SuccessfulNegotiation") an EVCC supported protocol even if the values of the VersionNumberMinor in EVCC request message does not match with the VersionNumberMinor of an SECC supported protocol where the VersionNumberMajor matches.

NOTE 1 A higher value in the VersionNumberMinor indicates that (in comparison to a lower value) additional data elements is transmitted from either the EVCC or SECC. Implementations only supporting the lower VersionNumberMinor value possibly are not be able to process the data and could ignore this data. A difference in the VersionNumberMinor value between EVCC and SECC does not lead to an incompatibility. Refer to 8.2.4 showing examples for successful protocol negotiation.

An EVCC supporting multiple energy transfer modes may therefore add multiple entries for ISO 15118-20 (this document) in the supportedAppProtocolReq. As an example, an EVCC that supports both AC and DC would have two entries for ISO 15118-20, one with the namespace "urn:iso:std:iso:15118:-20:AC" and one with the namespace "urn:iso:std:iso:15118:-20:DC". Another example may be found in 8.2.4.1.

[V2G20-1039] If an EVCC supports the service AC and intends to offer it for this V2G communication session, it shall add an AppProtocol element to the supportedAppProtocolReq with ProtocolNamespace set to "urn:iso:std:iso:15118:-20:AC", VersionNumberMajor set to "1" and VersionNumberMinor set to "0".

[V2G20-2132] If an EVCC supports the service DC and intends to offer it for this V2G communication session, it shall add an AppProtocol element to the supportedAppProtocolReq with ProtocolNamespace set to "urn:iso:std:iso:15118:-20:DC", VersionNumberMajor set to "1" and VersionNumberMinor set to "0".

[V2G20-4107] If an EVCC supports the service ACDP and intends to offer it for this V2G communication session, it shall add an AppProtocol element to the supportedAppProtocolReq with ProtocolNamespace set to "urn:iso:std:iso:15118:-20:ACDP", VersionNumberMajor set to "1" and VersionNumberMinor set to "0".

[V2G20-5126] If an EVCC supports the service WPT and intends to offer it for this V2G communication session, it shall add an AppProtocol element to the supportedAppProtocolReq with ProtocolNamespace set to "urn:iso:std:iso:15118:-20:WPT", VersionNumberMajor set to "1" and VersionNumberMinor set to "0".

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2133] The namespaces "urn:iso:std:iso:15118:-20:CommonMessages" and "urn:iso:std:iso:15118:-20:CommonTypes" shall never be used in the context of the supportedAppProtocolReq.

[V2G20-171] All additional data elements defined by the respective minor version shall be encoded as schema deviated case by the EXI coder (see also EXI option settings in 7.9.1.3).

[V2G20-172] Usually it is expected that the SECC is able to support the relevant application layer protocols indicated by the EVCC. However when none of the application layer protocols included in the list received from the EVCC is supported by the SECC, the ResponseCode in the response message shall be equal to Failed_NoNegotiation indicating that the protocol negotiation was not successful. In this error scenario the response message shall not include a SchemaID.

[V2G20-173] If no successful protocol negotiation can be achieved the EVCC shall not initialize a communication session.

[V2G20-1837] EVSE that supports basic charging as defined in IEC61851-1 shall revert to basic charging after sending a ResponseCode equal to "Failed_NoNegotiation" in the supportedAppProtocolRes message.

NOTE 2 In the "Failed_NoNegotiation" error case, the V2G session is terminated. It is the responsibility of the EVSE to ensure a clean transition to basic charging. In case the authorization was successfully completed before protocol negotiation was performed (e.g. using EIM), it is up to the EVSE to ensure that transition to basic charging does not require a repeated authorization procedure.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

8.2.2 Message definition supportedAppProtocolReq and supportedAppProtocolRes

[V2G20-175] The SECC and EVCC shall implement the message elements as defined in Figure 32.

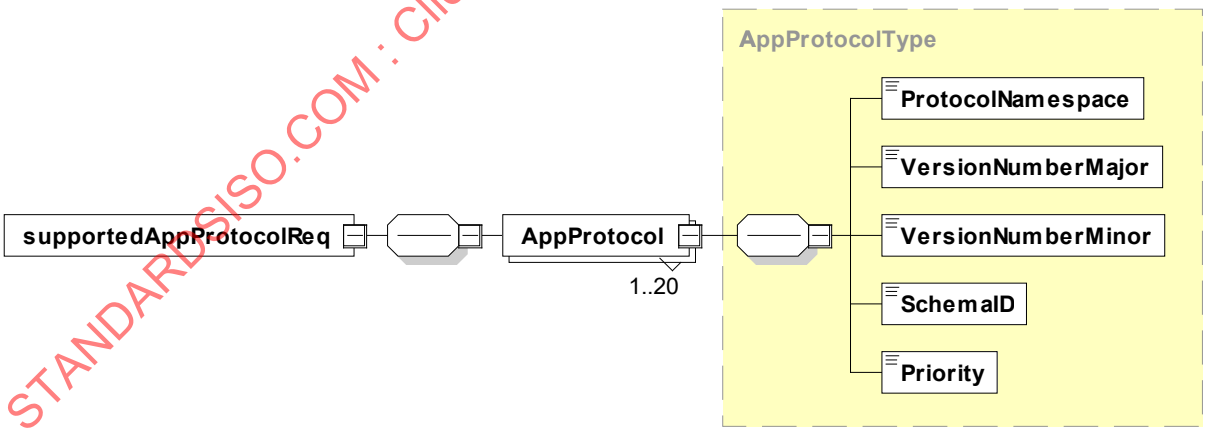


Figure 32 — Schema diagram – supportedAppProtocolReq

[V2G20-176] The SECC and EVCC shall implement the message elements as defined in Figure 33.

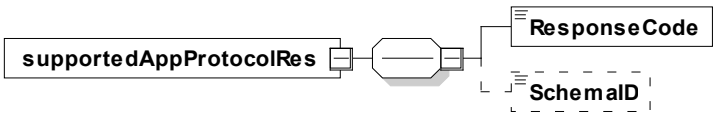


Figure 33 — Schema diagram – supportedAppProtocolRes

© ISO 2022 – All rights reserved

NOTE Refer to Annex A for the XML schema code for supportedAppProtocolReq and supportedAppProtocolRes messages.

8.2.3 Semantics description supportedAppProtocol messages

[V2G20-178] The message elements of the messages defined in Figure 32 and Figure 33 shall be used as defined in Table 28 and Table 30.

Table 28 — Semantics and type definition for supportedAppProtocolReq message elements

Element Name	Type	Semantics
AppProtocol	complexType: AppProtocolType refer to Table 29	This message element is used by the EVCC for transmitting the list of supported protocols. Each protocol with a particular version supported by the EVCC is represented by one AppProtocol entry in the request message (maximum number of entries: 20).

[V2G20-1019] The SECC and EVCC shall implement "AppProtocolType" as defined by Table 29.

Table 29 — Semantics and type definition for AppProtocolType

Element Name	Type	Semantics
ProtocolNamespace	simpleType: protocolNamespaceType refer to Annex A for the type definition	This message element is used by the EVCC to uniquely identify the Namespace URI of a specific protocol supported by the EVCC, i.e. this is the protocol name of the related protocol.
VersionNumberMajor	simpleType xs:unsignedInt	This message element is used by the EVCC to indicate the major version number of the protocol indicated in the message element ProtocolNamespace. The protocol version will be incremented after every new release of the document.
VersionNumberMinor	simpleType: xs:unsignedInt	This message element is used by the EVCC to indicate the minor version number of the protocol indicated in the message element ProtocolNamespace.
SchemaID	simpleType: idType refer to Annex A for the type definition	This message element is used by the EVCC to indicate the SchemaID assigned by the EVCC to the protocol indicated in the message element ProtocolNamespace, VersionNumberMajor and VersionNumberMinor.
Priority	simpleType: priorityType refer to Annex A for the type definition	This message element is used by the EVCC for indicating the protocol priority of a specific protocol allowing the SECC to select a protocol based on priorities. See also [V2G20-167].

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 30 — Semantics and type definition for supportedAppProtocolRes message elements

Element/Attribute Name	Type	Semantics
SchemaID	simpleType: idType refer to Annex A for the type definition	Optional: This message element is used by the SECC to reference one of the EVCC supported protocols received in the request message. Always mandatory, only not used in case ResponseCode is equal to FAILED_NoNegotiation
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	This message element is used by the SECC for indicating whether the list of protocols received from the EVCC includes at least one protocol matching with the protocols supported by the SECC.

8.2.4 Message examples

8.2.4.1 Protocol negotiation

Examples below illustrate the exchange of supportedAppProtocol messages between the EVCC and the SECC. In the request message, the EVCC sends a prioritized list of supported application layer protocols to the SECC. The Priority element indicates to the SECC which protocol is preferred by the EVCC. The SchemaID is simply a running counter, enabling the SECC to refer to a specific entry. In the response message the SECC confirms "urn:iso:std:iso:15118:-20:DC" by setting the SchemaID element to "2" and using a ResponseCode equal to "OK_SuccessfulNegotiation".

The following is V2G message example 1 – supportedAppProtocolReq: protocol negotiation.

```
<?xml version="1.0" encoding="UTF-8"?>
<n1:supportedAppProtocolReq xmlns:n1="urn:iso:15118:2:2010:AppProtocol"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:iso:15118:2:2010:AppProtocol V2G_CI_AppProtocol.xsd">
    <AppProtocol>
        <ProtocolNamespace>urn:iso:std:iso:15118:-20:AC</ProtocolNamespace>
        <VersionNumberMajor>1</VersionNumberMajor>
        <VersionNumberMinor>0</VersionNumberMinor>
        <SchemaID>1</SchemaID>
        <Priority>2</Priority>
    </AppProtocol>
    <AppProtocol>
        <ProtocolNamespace>urn:iso:std:iso:15118:-20:DC</ProtocolNamespace>
        <VersionNumberMajor>1</VersionNumberMajor>
        <VersionNumberMinor>0</VersionNumberMinor>
        <SchemaID>2</SchemaID>
        <Priority>1</Priority>
    </AppProtocol>
    <AppProtocol>
        <ProtocolNamespace>urn:iso:15118:2:2013:MsgDef</ProtocolNamespace>
        <VersionNumberMajor>2</VersionNumberMajor>
        <VersionNumberMinor>0</VersionNumberMinor>
        <SchemaID>3</SchemaID>
        <Priority>3</Priority>
    </AppProtocol>
</n1:supportedAppProtocolReq>
```

The following is V2G message example 2 – supportedAppProtocolRes: protocol negotiation.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

```
<?xml version="1.0" encoding="UTF-8"?>
<n1:supportedAppProtocolRes xmlns:n1="urn:iso:15118:2:2010:AppProtocol"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:iso:15118:2:2010:AppProtocol
..\V2G_CI_AppProtocol.xsd">
    <ResponseCode>OK_SuccessfulNegotiation</ResponseCode>
    <SchemaID>2</SchemaID>
</n1:supportedAppProtocolRes>
```

8.3 V2G message definition

8.3.1 Overview

A V2G communication session in this document is defined as the exchange of V2G messages between two V2G entities in a predefined sequence (see 8.6) for managing the energy transfer process. A V2G communication session always starts with the SessionSetup message pair and always ends with the SessionStop message pair.

All messages of a V2G communication session carry a SessionID that allows to manage the V2G communication sessions between V2G entities on application level. The SessionID is negotiated by the EVCC and the SECC in the SessionSetup message pair. All V2G messages of a V2G communication session except the SessionSetupReq message use the same SessionID.

The SessionID enables pausing and resuming communication by the EVCC during a single service session using multiple V2G communication sessions. For this, the EVCC and the SECC apply the same SessionID in all V2G communication sessions during a service session. Applying multiple V2G communication sessions enables the EVCC to initiate a stop and, when resuming, to restart all layers while keeping the same application context and energy transfer process management data. This for example allows the EV and the EVSE to switch off the ISO 15118 communication module completely during pause to save energy.

In this document a V2G communication session pause is controlled by the parameter ChargingSession in SessionStopReq with its value set to "Pause". For the scheduled control mode the parameter should be used in conjunction with the EVPowerProfile. This means that an EVCC can initiate a pause at any time after sending PowerDeliveryReq with ChargeProgress equal to "Stop", but it needs to be ensured that this pause period is also reflected as a zero power phase in the previously agreed EVPowerProfile.

Instead of "Pause", an EVCC can alternatively enter a "Standby" period during a V2G communication session when no power transfer is needed but the V2G communication needs to be maintained. For example, the EVCC may choose standby over pause when pause and resuming of communication for a short duration is more costly than beneficial. Also, an EVCC may want to receive value added services while no power is transferred, requiring an active V2G communication session. In contrast to pause, standby allows for performing a schedule renegotiation with multiplexed communication. standby is applicable to all energy transfer modes.

In this document a standby period starts by a PowerDeliveryReq with ChargeProgress set to "Standby" and ends by a PowerDeliveryReq with ChargeProgress set to "Start" or "Stop".

EVSE may choose not to allow a standby period by replying with a PowerDeliveryRes with response code set to "WARNING_StandbyNotAllowed". In this case, the EV is expected to follow the initially agreed power profile or to trigger a schedule renegotiation.

An EV may use pause at its discretion in scheduled control mode. For example, EV may enter a pause period when battery depletion is expected during a zero power period due to its battery consumption for the communication. In dynamic control mode the EV is not expected to initiate a pause as this can pose a conflict with the grid side charging/discharging plan. Instead, the SECC can request the EVCC to pause in dynamic control mode.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

During conductive charging applying communication via PLC, the conductive connection, e.g. of the charging cable, needs be maintained throughout a service session, including both pause and standby periods.

The example in Figure 34 shows two V2G communication sessions separated by a pause period and a standby period during the latter V2G communication session, illustrating their relation over time to the TCP/TLS connections, the data link establishment, the service session, and the power transfer between EV and EVSE.

For safety reasons to enter a standby period in DC or WPT, an EV will gradually decrease the current to 0A before sending a PowerDeliveryReq message with ChargeProgress set to "Standby".

An EV or EVSE may want to change the charging service or the prior agreed charging schedule in the same communication session, therefore the "renegotiation" concept is introduced. Two types of renegotiation are set. The first one is the "ServiceRenegotiation" as a means to change the charging service. The second one is the "ScheduleRenegotiation" as an option to change the prior agreed schedules. For further information see Annex F.

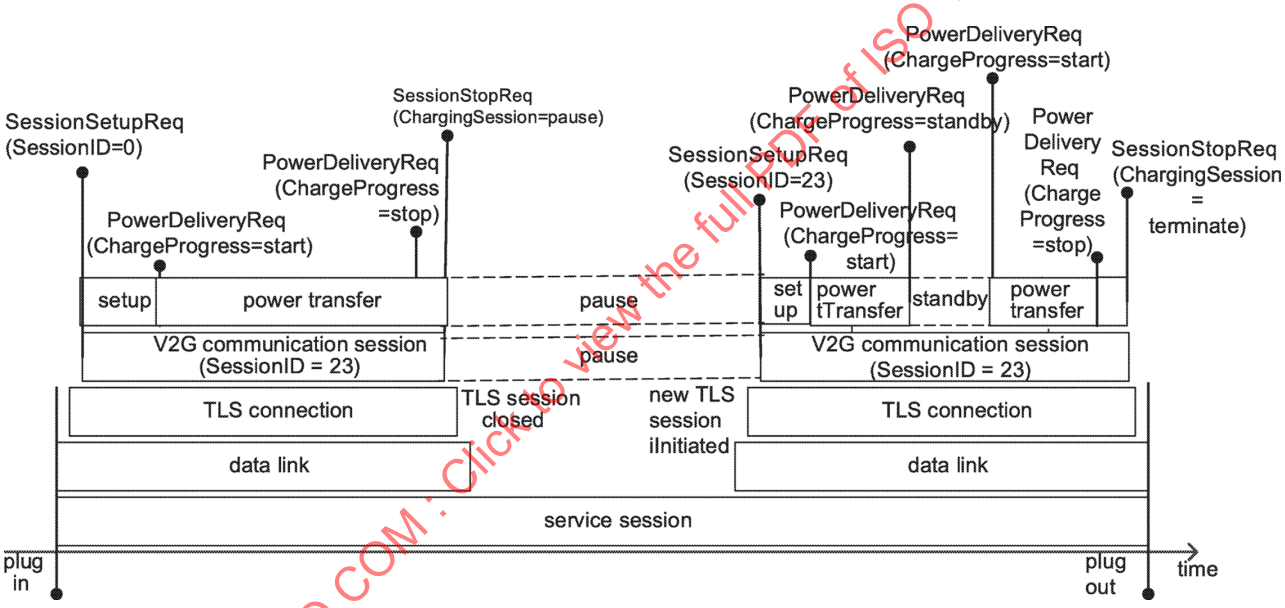


Figure 34 — Example of V2G communication session handling

8.3.2 General

This subclause and the subclauses within describe the messages of the V2G messages and their contents.

[V2G20-2314] Whenever a requirement only refers to ChargeParameterDiscoveryReq/Res, this requirement applies to all energy transfer mode specific extensions, e.g. DC_ChargeParameterDiscoveryReq/Res.

[V2G20-2315] Whenever a requirement only refers to ChargeLoopReq/Res, this requirement applies to all energy transfer mode specific extensions, e.g. DC_ChargeLoopReq/Res.

The application layer message set defined in this document is signalized by the XML schema namespace "urn:iso:std:iso:15118:-20". Refer to the XML schema definition in Annex A for details relative to sub-namespace definitions used for the message definition and for the XML schema code.

8.3.3 Header definition

8.3.3.1 General

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

The message header contains general information that is included in all messages. Figure 35 shows the schema definition of the V2G message header.

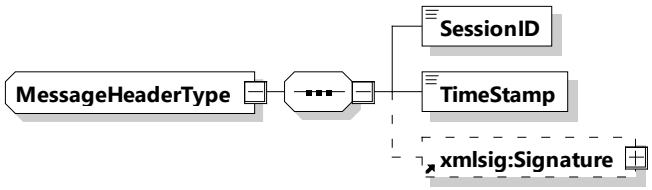


Figure 35 — Schema diagram – message header

[V2G20-2676] The message elements of the message header shall be used as defined in Table 31.

Table 31 — Semantics and type definition for a V2G message header

Element Name	Type	Semantics
SessionID	simpleType: sessionIDType refer to Annex A for the type definition	This message element is used by EVCC and SECC for uniquely identifying a V2G communication session. Refer to 8.3.4.1 for requirements relative to this message element.
TimeStamp	simpleType xs:unsignedLong	Timestamp that marks the time of message creation. The value is encoded at microseconds resolution in SECC time, a concept that is defined in 8.3.3.3
xmlsig:Signature	separate namespace: "http://www.w3.org/2000/09/xmldsig#"	Optional: This element is used if a certain V2G message requires to be signed.

[V2G20-182] Each V2G message containing signed elements shall include the xmlsig:Signature element in the header to be able to transmit the signature attached to signed body message elements of the respective message.

[V2G20-1022] After having received the SessionSetupRes, the EVCC shall check if the SessionID included in any following response messages is the same as the one received during SessionSetupRes.

8.3.3.2 Coordinated activities

One of the primary design goals within this document is to provide the means to coordinate activities on the two sides of the charging cable. For the scheduled control mode, where power schedules are negotiated which then define future behavior, this leads to the necessity of a concept of coordinated time.

In addition, it is necessary to ensure the validity of certificates or to coordinate activities based on power or price schedules which have been created by external secondary actors outside the local communication network. So a clear definition of a relationship to coordinated universal time (UTC) is required.

While time appears like a trivial issue there are a number of technical requirements that need to be satisfied within this context. Besides the regular questions of the handling of leap seconds, time zones

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

and common issues like hardware clock drift, this document needs to support use cases where the SECC and/or the EVCC do not have a buffered real time clock and the coordination of the entire energy transfer process should also work reliably when there is no internet connection or if the backend networks are temporarily unreachable.

The management of (scheduled) events with a time resolution shorter than 1 s is considered not in scope for ISO 15118 communication and they are typically handled by safety standards, power inverter hardware designs or similar solutions. However, for some purposes a very fine-grained time notation is necessary after all.

To address all those requirements this document is introducing the concept of "SECC time".

8.3.3.3 The definition of SECC time

[V2G20-1529] Unless noted otherwise, all time stamps and time anchors (e.g. as used in schedules) are values that shall be interpreted in the context of SECC time.

NOTE 1 SECC time is modeled after UNIX time (also known as POSIX time or epoch time) to simplify its implementation and it therefore shares many, but not all characteristics. This means that if an SECC is based on a system that works with UNIX time and uses some common form of clock synchronization (e.g. via NTP), then the system's time can be used directly to fulfill all possible SECC time requirements. On the EVCC side implementation requirements are slightly different, as is outlined further below.

NOTE 2 SECC time is a system for describing a point in time, defined as the number of seconds that have elapsed since the beginning of the local SECC epoch minus the number of leap seconds that have taken place since then.

NOTE 3 Leap seconds are intentionally omitted in SECC time, just like in UNIX time, so every day has precisely 86 400 s. This makes calculations into the future predictable but has the consequence that SECC time, in the context of UTC, is neither a truly linear measure of time nor a true representation of UTC.

[V2G20-1531] If coordination with external secondary actors is necessary, than SECC time shall use an SECC epoch starting at 00:00:00 (hh:mm:ss) Coordinated Universal Time (UTC), Thursday, 1 January 1970.

NOTE 4 The coordination with external secondary actors implies that some form of backend communication is possible, meaning that the SECC has some technical capability to synchronize with UTC. This automatically places SECC time into the UTC time zone.

[V2G20-1532] For situations where UTC synchronization is not necessary or no internet connection is possible any other SECC epoch start time shall be allowed.

NOTE 5 Typically this is the point in time where the system was powered on.

NOTE 6 The charging systems, for example, designed as PV-battery buffered power islands or vehicle-to-vehicle charging solutions, with EIM access control can properly work in scheduled or dynamic control modes even without SECC time being in sync with UTC. Refer to 8.4.2 for description of scheduled and dynamic control modes.

[V2G20-1533] SECC time shall never be used as the reference time for the purpose of certificate expiration validation.

NOTE 7 The SECC and EVCC can perform certificate expiration validation with the help of time sources which they individually consider as trustworthy. From the EVCCs perspective SECC time cannot be guaranteed to meet any well-defined security criteria.

8.3.3.4 TimeStamp within MessageHeaderType

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1534] The value of the TimeStamp element of the common MessageHeaderType shall always be in SECC time and encoded at microseconds resolution.

NOTE 1 The use of microseconds in a 64 bit unsigned long integer has the benefit of preventing the year 2038 problem, allowing for precise synchronization with other high resolution clocks (e.g. as used in smart meters) and allowing precise calculations of clock drift and data transmission or processing latencies in cases where this might be helpful to trace down technical problems.

NOTE 2 While even the EVCC is required to use TimeStamps in SECC time this does not require that it changes its internal hardware clock. The EVCC will only need to calculate its clock offset to SECC time and always apply this delta appropriately. Due to the nature of clock drift that delta can change over time and the EVCC monitors its delta and adjust it continuously.

[V2G20-1535] The value of the TimeStamp element of the common MessageHeaderType sent by the EVCC during the initial SessionSetupReq message shall be its best effort guess of the present SECC time stamp, assuming the SECC time is synchronized to UTC. If the EVCC has no knowledge of the present UTC time than it shall indicate this by sending "zero" as the initial TimeStamp.

NOTE 3 In cases where the SECC does not have any means to synchronize its clock to external sources (e.g. due to lack of internet connectivity, etc.), the above requirement allows the SECC to decide if it wants to join the EVCC's world view of time.

[V2G20-1536] The value of the TimeStamp element of the common MessageHeaderType sent by the SECC during the SessionSetupRes message shall define the initial SECC time stamp, which serves as the reference for all future message exchanges.

NOTE 4 The EVCC might not have any means to synchronize its clock to external sources. [V2G20-1533] discourages the use of SECC time for security related purposes. If the EVCC, in lack of better options, wants to utilize SECC time as a source for the synchronization of its internal real time clock, it can try to ensure that the conditions of [V2G20-1531] are met, where UTC time alignment is assured.

[V2G20-1537] The value of the TimeStamp element of the common MessageHeaderType sent by the SECC or the EVCC shall always increase with each message and according to the progress of time.

[V2G20-1538] The previous requirement [V2G20-1537] shall not apply to the first (SessionSetupReq) and the second (ServiceDiscoveryReq) message which is being sent by the EVCC within a newly established charging session.

NOTE 5 The always increasing time stamps allow "ordering" of messages (linearization) which can be helpful in situations where multiple multiplexed sequences are taking place and where internal processing queue prioritization can result in out of order processing that might need detection in some applications.

8.3.4 Request and response definitions

8.3.4.1 V2G session handling

Messages defined as common messages in the following clause and its subclauses can be applied to the message sequence in any charging mode.

Additionally, this subclause and the subclauses within it, will provide specific and separate requirements for the private SECC and the SECC. Thus, unless otherwise specified for this subclause or any subclause within it, private SECC and SECC are not considered interchangeable.

8.3.4.1.1 General

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

[V2G20-747] The header of any message sent by the EVCC during an active V2G communication session shall include the SessionID value returned by the SECC in the response to the SessionSetupReq initiating the currently active V2G communication session.

[V2G20-751] The SessionID value returned by the SECC in the SessionSetupRes message shall not change as long as the V2G communication session is not terminated (i.e. value of parameter ChargingSession of SessionStopReq has not been set to "Terminate" at any time).

[V2G20-752] The header of any message sent by the SECC during an active V2G communication session shall include the SessionID value returned by the SECC in the response to the SessionSetupReq initiating the currently active V2G communication session.

[V2G20-2541] If the EVCC detects that there has been no communication associated with a particular V2G session for 648 000 s (7,5 days), the EVCC shall immediately terminate/close that V2G session.

NOTE 1 If there is no communication for 7,5 days for a particular V2G session, it is assumed that the V2G session has been abandoned/orphaned and as such can be terminated/closed.

[V2G20-2620] If the SECC detects that there has been no communication associated with a particular V2G session for 648 000 s (7,5 days), the SECC shall immediately terminate/close that V2G session.

NOTE 2 If there is no communication for 7,5 days for a particular V2G session, it is assumed that the V2G session has been abandoned/orphaned and as such can be terminated/closed.

8.3.4.1.2 Initial V2G session setup

[V2G20-1243] When sending the first SessionSetupReq message for the initiated service session (i.e. when the EVCC is not trying to resume a previously paused V2G communication session), the EVCC shall only transmit zeroes in the parameter SessionID in the message header.

[V2G20-2106] When receiving the SessionSetupReq with the parameter SessionID equal to zero, the SECC shall generate a new (not stored) SessionID value different from zero and return this value in the SessionSetupRes message header.

NOTE 3 In this case the EVCC will follow [V2G20-1484] and [V2G20-1486].

[V2G20-2621] When generating a new SessionID, the SECC shall ensure that the generated SessionID is 64-bit long nonce with a minimum of 58 bits of entropy. Refer to 7.3.7 for further details.

[V2G20-2618] If the EVCC sent the SessionSetupReq message with a SessionID consisting only of zeroes and received the SessionSetupRes message with the ResponseCode set to "OK_NewSessionEstablished" as well as the SessionID set to a value other than zero, the EVCC shall consider this as a new V2G communication session.

[V2G20-2619] If [V2G20-2618] applies, the EVCC shall follow normal steps to setup a new V2G session with new authorizations.

NOTE 4 In this case the EVCC will follow [V2G20-1484] and [V2G20-1486].

[V2G20-1059] The EVCC and SECC shall cache the relevant authorization data for the duration of the V2G communication session.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 5 From first authorization until termination of the V2G communication session or physical plug out - CP state changes B to A for conductive charging

NOTE 6 For EIM the relevant authorization data of the SECC is the authorization status. For PnC the relevant authorization data of an EVCC includes the credentials of the TLS sessions including VAS, and the relevant authorization data of an SECC includes the credentials of the TLS sessions including VAS, the certificate chains received from the EV, validation and revocation check results of those certificates, and the authorization status.

8.3.4.1.3 V2G session pausing

[V2G20-1540] If an EVCC wants to pause an active V2G communication session, it shall do so by sending PowerDeliveryReq with ChargeProgress set to "Stop" followed by SessionStopReq message with the parameter ChargingSession set to value "Pause".

[V2G20-1839] In scheduled control mode, any pause period initiated by the EVCC shall be indicated as zero power period in the currently applied EVPowerProfile, sent in the latest PowerDeliveryReq with ChargeProgress set to "Start", "Standby", "Stop" or "Pause".

A "zero power" period in an EVPowerProfile does not require a standby to be initiated. Only if a standby is requested by the EVCC shall the applied EVPowerProfile indicate this accordingly.

[V2G20-1197] At the point in time when entering pause by SessionStopReq with ChargingSession=Pause in Scheduled control mode, the EVCC shall ensure that the applied EVPowerProfileEntry is equal to 0kW.

[V2G20-1061] In scheduled control mode, any pause period initiated by the SECC shall be indicated as zero power period in the currently applied EVPowerProfile, sent in the latest PowerDeliveryReq with Charge progress set to "Start", "Standby", "Stop" or "Pause".

A "zero power" period in an EVPowerProfile does not require a pause to be initiated. Only if a pause is requested by the SECC shall the applied EVPowerProfile indicate this accordingly.

It is not recommended for the SECC to request a pause for short time periods of zero power transfer. In case the SECC requests the EVCC to enter a pause, the EVCC can alternatively enter a StandbyPeriod according to [V2G20-1850].

[V2G20-1198] At the point in time when requesting pause by setting the parameter EVSENotification to Pause in scheduled control mode, the SECC shall ensure that the applied EVPowerProfileEntry is equal to 0kW.

[V2G20-1842] In dynamic control mode, the EVCC shall only request a pause period if triggered by the SECC according to [V2G20-1850].

NOTE 1 In dynamic control mode the SECC needs to dynamically adjust the power profile based on grid demands, etc. A pause initiated by the EVCC contradicts the intent of dynamic control mode where the SECC controls the power profile, not the EVCC.

[V2G20-4002] If SECC is using ServiceName = DC_ACDP, in the case the SECC wants to perform a pause period, it shall trigger the EVCC via EVSEStatus Parameter EVSENotification set to "Pause". The EVCC shall than initiate a pause period according to [V2G20-4001].

[V2G20-2071] After pausing the V2G session, the EVCC shall terminate the TLS connection associated with the V2G session.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

NOTE 2 When pausing a V2G communication session, the EVCC turns OFF its transport layer connection which induces a phase of no active communication and no power transfer, therefore no value added services are usable during a pause either.

[V2G20-2099] During a pause period with conductive charging and communication via PLC, the physical connection shall be maintained throughout the entire service session.

NOTE 3 Any physical disconnection, for example, removal of the connector, will result in abortion of the service session.

8.3.4.1.4 V2G session resumption

[V2G20-1199] In scheduled control mode, the EVCC shall ensure it is resuming the communication session according to [V2G20-1541], while the applied EVPowerProfileEntry is still equal to 0 kW.

During V2G communication session resumption, the SECC compares the SessionID (received in the current SessionSetupReq) and the vehicle certificate (received during the TLS handshake for the currently active TLS session in which the SessionSetupReq for V2G communication session resumption is received) with the SessionID and the vehicle certificate data that was stored when the corresponding V2G communication session was initially setup. If the data does not match, V2G communication session resumption will fail. For example, if the vehicle certificate provided during initial V2G communication session setup is different than the vehicle certificate provided during V2G communication session resumption because the vehicle certificate was updated as it was about to expire, the SECC will detect this as a request to initiate a new V2G communication session, not to resume the previously paused V2G communication session.

Similarly, during V2G communication session resumption, the EVCC compares the SessionID (received in the current SessionSetupRes) and the SECC certificate (received during the TLS handshake for the currently active TLS session in which the SessionSetupRes for V2G communication session resumption is received) with the SessionID and the SECC certificate data that was stored when the corresponding V2G communication session was initially setup. If the data does not match, V2G communication session resumption will fail. For example, if the SECC certificate provided during initial V2G communication session setup is different than the SECC certificate provided during V2G communication session resumption because the SECC certificate was updated as it was about to expire, the EVCC will detect this as an issue and terminate the V2G communication session. It will then setup a new V2G communication session.

Since setting up a new V2G communication session (i.e. a V2G communication session with new SessionID) means that the previous authorizations are no longer valid. This requires the EVCC requesting authorization of the session once again. This can become an issue, especially in cases where user interaction is required for authorization (e.g. in EIM). Hence, the EVCC should be careful about pausing the V2G session close to SECC certificate's expiration and its own vehicle certificate's expiration.

The EVCC receives the SECC certificate in the TLS handshake and can get the SECC certificate's expiration date/time stamp from the SECC certificate. The EVCC contains its own vehicle certificate and can get the vehicle certificate's expiration date/time stamp from the vehicle certificate.

Before EVCC can resume a paused V2G session, it needs to start a new TLS session.

[V2G20-2073] When the EVCC wants to resume the previously paused V2G communication session, the EVCC shall follow 7.7.3.3, 7.7.3.4 and 7.7.3.5 to set up a new TLS session that can be used for V2G session resumption.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-4000] If EVCC is using ServiceName = DC_ACDP, the following requirements are not applicable: [V2G20-1540], [V2G20-2301], [V2G20-2624] and [V2G20-1028].

NOTE 1 To enable pause when using ServiceName = DC_ACDP the common requirements [V2G20-1227], [V2G20-1541], [V2G20-1839], [V2G20-1840], [V2G20-1841], [V2G20-1842], [V2G20-1843] and [V2G20-1844] apply.

[V2G20-4001] If EVCC is using ServiceName = DC_ACDP, an EVCC shall pause a V2G communication session with the parameter ChargingSession set to value "Pause" in message SessionStopReq after receiving ACDP_DisconnectRes with parameter "EVSEProcessing" set to "Finished".

NOTE 2 To enable pause when using ServiceName = DC_ACDP the common requirements [V2G20-1058], [V2G20-1613], [V2G20-2545], [V2G20-1614], [V2G20-2623], [V2G20-1847], [V2G20-1061] and [V2G20-1032] apply.

[V2G20-1541] When the EVCC wants to resume the previously paused V2G communication session, the EVCC shall send the SessionID of the previously paused V2G communication session it is trying to resume.

NOTE 3 The EVCC received this SessionID in the SessionSetupRes message before the EVCC paused the V2G communication session. The EVCC will send this SessionID in the SessionSetupReq message to resume the previously paused V2G communication session.

[V2G20-1613] If an EVCC chooses to resume an energy transfer session by sending a SessionSetupReq with a message header including the SessionID value from the previously paused V2G communication session, the SECC shall compare this value to the value stored from the preceding V2G communication session.

[V2G20-2545] If the SessionID value received in the current SessionSetupReq is equal to a SessionID value stored from a preceding V2G communication session that has not been terminated yet, the SECC shall check that this V2G communication session resumption request came from the same EVCC with which the SECC had setup this particular V2G communication session. The exact methodology for this check is left up to the CSO and/or the manufacturer of the SECC.

NOTE 4 Since authorization from the preceding V2G communication session is reused in a resumed V2G communication session, it is important for the SECC to ensure that it does not resume a paused V2G session with a wrong EVCC. An example is provided in NOTE 2 below.

NOTE 5 For example, when two EVCCs are connected to the same SECC and both pause their respective V2G communication session, one EV can try to restart the V2G communication session using the SessionID of the other EV. If the SECC does not ensure that the EV trying to reuse someone else's V2G communication session is not denied that privilege, the EV trying to reuse the other EV's V2G communication session will not only be able to reuse other EV's V2G communication session, it will also be able to utilize other EV's charging/service authorization regardless if that authorization was based on PnC or EIM.

NOTE 6 An example of a methodology to check that this V2G communication session resumption request came from the same EVCC with which the SECC had setup this particular V2G communication session is provided in 8.3.4.1.1.

[V2G20-2622] If the check as described by [V2G20-2545] succeeds, i.e. this V2G communication session resumption request came from the same EVCC with which the SECC had setup this particular V2G communication session, the SECC shall continue with V2G session resumption.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 7 In this case the EVCC will follow [V2G20-2097], [V2G20-2098] or [V2G20-5046], depending on the energy transfer mode selected. Authorization from previous V2G communication session is used. As such the EVCC will bypass the authorization messages.

[V2G20-2623] If [V2G20-2622] applies, the SECC shall provide confirmation of continuation of the charging session by sending a SessionSetupRes message including the SessionID it received in the SessionSetupReq message (stored SessionID value) and indicating the resumed V2G communication session with the ResponseCode set to "OK_OldSessionJoined" (refer also to [V2G20-463] for selecting the appropriate response code).

[V2G20-2539] If the EVCC received SessionSetupRes message with the ResponseCode set to "OK_OldSessionJoined" and the SessionID set to the same value that it sent in SessionSetupReq message to resume the previously paused V2G communication session, the EVCC shall check that it is still connected to the same SECC with which it had initially setup this particular V2G communication session. The exact methodology for this check is left up to the OEM.

NOTE 8 An example of this methodology is provided in 8.3.4.1.1.

[V2G20-1032] After resuming a previously paused V2G communication session, following a SessionSetupReq, the SECC shall respond with a SessionSetupRes within V2G_SECC_Msg_Performance_Time according to Table 215. The allowed next request shall be ChargeParameterDiscoveryReq within the V2G_SECC_Sequence_Timeout according to Table 215.

NOTE 9 In case of a resumed session, the AuthorizationReq/Res messages are not required as authorization details of the previous communication session are valid for the whole service session, see [V2G20-1844].

[V2G20-2628] If a new SessionID was assigned per [V2G20-2627] or [V2G20-2547], the SECC shall consider this as a new V2G session. The SECC shall not apply any previously stored authorizations to this new V2G session. The SECC shall expect and require the EVCC to follow normal steps to setup a new V2G session with new authorizations.

NOTE 10 In this case the EVCC will follow [V2G20-1484] and [V2G20-1486].

8.3.4.1.4.1 V2G session resumed successfully

[V2G20-2540] If the check as described by [V2G20-2539] succeeds, i.e. the V2G communication session has been resumed with the same SECC with which the EVCC had initially setup this same communication session, the EVCC shall continue with V2G session resumption

NOTE 1 In this case the EVCC will follow [V2G20-2097], [V2G20-2098] or [V2G20-5046], depending on the energy transfer mode selected. Authorization from previous V2G communication session is used. As such the EVCC will bypass the authorization messages.

[V2G20-1844] When a previously paused V2G communication session is successfully resumed by the EVCC (i.e. [V2G20-2540] applies), the authorization from the previously paused V2G communication session shall be considered as valid.

NOTE 2 An EV can resume a previously paused session by applying the wake up procedure as specified in ISO 15118-3:2015, 7.6.2.1.

[V2G20-1847] When a previously paused V2G communication session is resumed by the SECC, the authorization from the previous session shall be considered valid.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 3 An EVSE can resume a previously paused session by applying the wake up procedure as specified in ISO 15118-3:2015, 7.6.2.2.

[V2G20-1843] In case EVCC successfully resumes a previously paused V2G communication session (i.e. [V2G20-2540] applies), the EVCC shall apply the message sequence according to [V2G20-2097], [V2G20-2098] and [V2G20-5046].

[V2G20-2301] If [V2G20-1540] applies and a connection based on ISO 15118-3 has been established, the EVCC shall take care that [V2G20-1541] is fulfilled as long as no CP state E or F was detected in the EVCC as defined in IEC 61851-1.

[V2G20-1027] If [V2G20-1540] applies and a connection based on ISO 15118-8 has been established, the EVCC shall take care that [V2G20-1541] is fulfilled as long as no alignment failure has been reported by the SECC.

[V2G20-1028] If [V2G20-2623] applies and a connection based on ISO 15118-8 has been established, the SECC shall take care that [V2G20-1058] is fulfilled as long as no alignment failure was detected in the SECC.

[V2G20-2624] If [V2G20-2623] applies and a connection based on ISO 15118-3 has been established, the SECC shall take care that [V2G20-1058] is fulfilled as long as no CP State A, E, or F was detected in the SECC as in IEC 61851-1.

[V2G20-1058] If the V2G communication session is resumed according to [V2G20-2623] the SECC shall ensure that if a ScheduleTuple is offered with the same ScheduleTupleID that was offered previously, this ScheduleTuple shall not differ from the previously offered ScheduleTuple.

NOTE 4 This allows the EVCC to continue/reuse an EVPowerProfile that was calculated before the pause based on a ScheduleTuple that is still offered by the SECC.

[V2G20-1840] If an EVCC successfully resumes a previously paused V2G communication session (i.e. [V2G20-2540] applies) it shall reduce the time elapsed during the pause period for the ScheduleTuple selected in the previous V2G communication session.

[V2G20-1841] If an EVCC successfully resumes a previously paused V2G communication session (i.e. [V2G20-2540] applies) and the time elapsed is greater than the time covered by the ScheduleTuple whose ID was selected in the previous V2G communication session the EVCC shall trigger an instant schedule renegotiation.

[V2G20-1765] If the EVCC wants to change the energy transfer parameters, it shall use the schedule renegotiation mechanism defined in this document.

[V2G20-2625] If the V2G communication session is resumed according to [V2G20-2623] and if the SECC wants to change the energy transfer parameters listed in [V2G20-1058] it shall use the schedule renegotiation mechanism defined in this document.

[V2G20-2546] If the V2G communication session is resumed according to [V2G20-2545] and if the SECC wants to change the energy transfer parameters listed in [V2G20-1058], it shall use the schedule renegotiation mechanism defined in this document.

[V2G20-1614] If the EVCC or SECC want to change the energy transfer parameters, the EVCC or SECC shall use the schedule renegotiation mechanism defined in this document.

8.3.4.1.4.2 V2G session resumption failed

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

[V2G20-2626] If the check as described by [V2G20-2545] fails, i.e. this V2G communication session resumption request came from a different EVCC than the one with which the SECC had setup this particular V2G communication session, the SECC shall consider this as an attempt to start a new V2G session.

[V2G20-2627] If [V2G20-2626] applies, the SECC shall send a SessionID value in the SessionSetupRes message that is unequal to zero and unequal to the SessionID value received in SessionSetupReq message. The new SessionID shall meet [V2G20-2621]. The SECC shall indicate the setup of new V2G communication session with the ResponseCode in the SessionSetupRes message set to "OK_NewSessionEstablished" (refer also to [V2G20-462] for applicability of this response code).

NOTE 1 Refer to 8.6.3 for additional requirements of response codes applicable to the SessionSetupRes message.

[V2G20-2547] If the SECC receives a SessionSetupReq including a SessionID value which is not equal to zero and not equal to the SessionID value stored from the preceding V2G communication session, it shall send a SessionID value in the SessionSetupRes message that is unequal to zero and unequal to the SessionID value stored from the preceding V2G communication session and indicate the new V2G communication session with the ResponseCode set to "OK_NewSessionEstablished" (refer also to [V2G20-462] for applicability of this response code).

NOTE 2 Refer to 8.6.3 for additional requirements of response codes applicable to the SessionSetupRes message.

[V2G20-2613] If the check as described by [V2G20-2539] fails, i.e. the V2G communication session has not been resumed with the same SECC with which the EVCC had initially setup this same V2G communication session, the EVCC shall consider this as a new V2G communication session.

[V2G20-2614] If [V2G20-2613] applies, the EVCC shall purge all data associated with the paused V2G communication session and terminate that V2G communication session.

NOTE 3 Something went wrong if the V2G communication session has not been resumed with the same SECC with which the EVCC had initially setup this same V2G communication session. As such the safest course of action is to terminate this V2G communication session.

[V2G20-2615] If the EVCC received SessionSetupRes message with the ResponseCode set to "OK_NewSessionEstablished" and the SessionID set to a value different than the value that it sent in SessionSetupReq message to resume the previously paused V2G communication session, the EVCC shall consider this as a new V2G communication session.

[V2G20-2616] If [V2G20-2615] applies, the EVCC shall purge all data (including any authorizations) associated with the paused V2G communication session that the EVCC was trying to resume.

[V2G20-2617] If [V2G20-2615] applies, the EVCC shall follow normal steps to setup a new V2G session with new authorizations.

NOTE 4 In this case the EVCC will follow [V2G20-1484] and [V2G20-1486].

8.3.4.1.4.3 Example of V2G session to vehicle/SECC certificate binding

This is just an example. It is not mandated to follow this methodology. The OEM, CSO, SECC manufacturer may decide to use another methodology.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2630] After a successful "Initial Handshake" (as described in 7.7.3.5) to setup a TLS session (as described in 7.7.3.3, 7.7.3.4 and 7.7.3.5), the SECC should calculate the SHA512 hash of the vehicle certificate (only the leaf certificate not the entire certificate chain).

NOTE 1 It is not in the scope of this document to define a methodology for the SECC to capture the vehicle certificate from the TLS handshake for the purposes of calculating the hash per this requirement.

[V2G20-2631] The SECC should securely store the hash generated by [V2G20-2630] until it is used per [V2G20-2550].

[V2G20-2550] Once a new SessionID has been assigned to the V2G session, the SECC should calculate the SHA512 hash of the SessionID of the V2G session concatenated with the hash generated by [V2G20-2630]. Refer to [V2G20-2106], [V2G20-2626] and [V2G20-2627] for details of SessionID assignment.

NOTE 2 SessionIDtoVehicleCertificateBinding = SHA512 (SessionID || SHA512 (vehicle certificate)).

[V2G20-2551] The SECC shall discard the hash generated by [V2G20-2630] after the hash has been utilized per [V2G20-2550].

[V2G20-2552] The SECC shall securely store the hash generated by [V2G20-2550] until the V2G session associated with the particular SessionID is terminated/closed.

[V2G20-2553] Whenever the SECC performs the "Full Handshake" (as described in 7.7.3.5) to setup a TLS session (as described in 7.7.3.3, 7.7.3.4 and 7.7.3.5), it shall calculate a new hash by following [V2G20-2630].

[V2G20-2632] The SECC should securely store the hash generated by [V2G20-2553] until it is used per [V2G20-2633].

[V2G20-2633] When the SECC receives a SessionID value in the SessionSetupReq that is equal to a SessionID value stored from a preceding V2G communication session that has not been terminated yet, the SECC should calculate the SHA512 hash of the SessionID received in SessionSetupReq message concatenated with the hash generated by [V2G20-2553].

NOTE 3 ReceivedSessionIDtoVehicleCertificateBinding = SHA512 (SessionID || SHA512 (Vehicle Certificate)).

[V2G20-2634] The SECC should discard the hash generated by [V2G20-2553] after the hash has been utilized per [V2G20-2633] or when the associated V2G communication session is terminated.

[V2G20-2554] The SECC should check that the hash value calculated by [V2G20-2633] is the same as the hash value calculated by [V2G20-2550].

[V2G20-2635] After a successful "Initial Handshake" (as described in 7.7.3.5) to setup a TLS session (as described in 7.7.3.3, 7.7.3.4 and 7.7.3.5), the EVCC should calculate SHA512 hash of the SECC certificate (only the leaf certificate not the entire certificate chain) or, in case of a private SECC, PE certificate (only the leaf certificate not the entire certificate chain).

NOTE 4 It is not in the scope of this document to define a methodology for the EVCC to capture the SECC/PE certificate from the TLS handshake for the purposes of calculating the hash per this requirement.

[V2G20-2636] The EVCC should securely store the hash generated by [V2G20-2635] until it is used per [V2G20-2555].

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2555] Once a new SessionID has been assigned to the V2G Session, the EVCC should calculate SHA512 hash of the SessionID of the V2G session concatenated with the hash generated by [V2G20-2635]. Refer to [V2G20-2106], [V2G20-2626] and [V2G20-2627] for details of SessionID assignment.

NOTE 5 SessionIDtoSECCCertificateBinding = SHA512 (SessionID || SHA512 (SECC/PE certificate)).

[V2G20-2556] The EVCC should discard the hash generated by [V2G20-2635] after the hash has been utilized per [V2G20-2555].

[V2G20-2557] The EVCC should securely store the hash generated by [V2G20-2555] until the V2G session associated with the particular SessionID is terminated/closed.

[V2G20-2558] Whenever the EVCC performs the "Full Handshake" (as described in 7.7.3.5) to setup a TLS session (as described in 7.7.3.3, 7.7.3.4 and 7.7.3.5), it shall calculate a new session binding by following [V2G20-2635].

[V2G20-2637] The EVCC should securely store the hash generated by [V2G20-2558] until it is used per [V2G20-2638].

[V2G20-2638] When the EVCC receives the SessionID value in the SessionSetupRes for the V2G communication session that it is trying to resume, the EVCC should calculate the SHA512 hash of the SessionID received in SessionSetupRes message concatenated with the hash generated by [V2G20-2558].

NOTE 6 ReceivedSessionIDtoSECCCertificateBinding = SHA512 (SessionID || SHA512 (SECC/PE certificate)).

[V2G20-2639] The EVCC should discard the hash generated by [V2G20-2558] after the hash has been utilized per [V2G20-2638] or when the associated V2G communication session is terminated.

[V2G20-2559] The EVCC should check that the hash value calculated by [V2G20-2638] is the same as the hash value calculated by [V2G20-2555].

8.3.4.2 V2G session standby

[V2G20-1194] To enter a standby period, the EVCC shall stop charging (no current drawn by EV) before sending a PowerDeliveryReq message with ChargeProgress set to "Standby".

[V2G20-2100] During a standby period with conductive charging and ACD, the physical connection shall be maintained throughout the entire service session.

NOTE Any physical disconnection, for example, removal of the connector, results in abortion of the service session.

8.3.4.3 Common messages

This subclause and the subclauses within only apply for main stream EXI encoded messages with V2GTP payload types in the range 0x8001 up to 0x80FF.

8.3.4.3.1 SessionSetupReq/Res

8.3.4.3.1.1 SessionSetupReq

By using the SessionSetupReq message the EVCC establishes a V2G communication session.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1246] The EVCC and the SECC shall implement the message elements as defined in Table 32 and Figure 36.

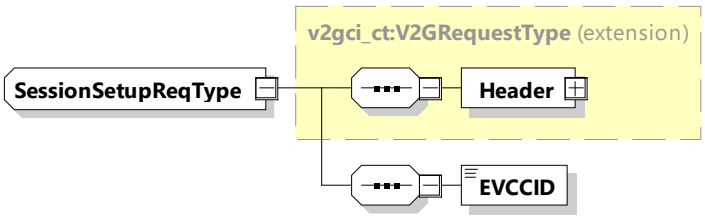


Figure 36 — Schema diagram – SessionSetupReq

The element of this message is used according to Table 32.

Table 32 — Semantics and type definition for SessionSetupReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
EVCCID	simpleType: identifierType refer to Annex A for the type definition	Specifies the EVCC's unique identifier.

[V2G20-1062] The EVCC shall transmit an EVCCID with the first 3 bytes containing the WMI as defined in ISO 3780:2009.

8.3.4.3.1.2 SessionSetupRes

By using the SessionSetupRes the SECC responds to a SessionSetupReq. With the SessionSetupRes the SECC notifies the EVCC with an enclosed ResponseCode, whether establishing a new session or joining a previous communication session was successful or not.

[V2G20-1247] The EVCC and the SECC shall implement the message elements as defined in Table 33 and Figure 37.

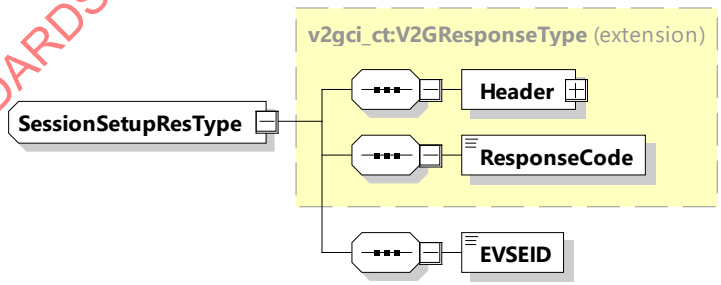


Figure 37 — Schema diagram – SessionSetupRes

The elements of this message are used according to Table 33.

Table 33 — Semantics and type definition for SessionSetupRes

Element Name	Type	Semantics

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
EVSEID	simpleType: identifierType refer to Annex A for the type definition	Any ID that uniquely identifies the EVSE and the power outlet the EV is connected to. The format of this message element is defined in Annex C. If an SECC cannot provide such ID data, the value of the EVSEID is set to zero ("ZZ00000").

[V2G20-192] The SECC and the EVCC shall use the format for EVSEID as defined in Annex C.

8.3.4.3.2 AuthorizationSetupReq/Res

This subclause, and all subclauses within it, will provide specific and separate requirements for the private SECC and the SECC. Thus, unless otherwise specified for this subclause or any subclause within it, private SECC and SECC are not considered interchangeable.

8.3.4.3.2.1 AuthorizationSetupReq

Message is empty, besides the header, and is only required to start the process of choosing the authorization method.

[V2G20-1066] The EVCC and the SECC shall implement the message elements as defined in Figure 38 and Table 34.

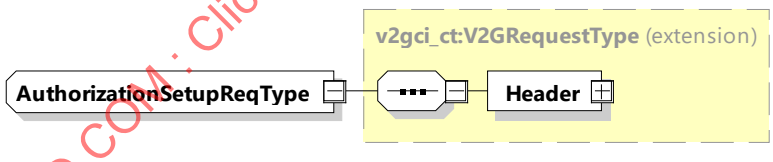


Figure 38 — Schema diagram – AuthorizationSetupReq

The elements of this message are used according to Table 34.

Table 34 — Semantics and type definition for AuthorizationSetupReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.

8.3.4.3.2.2 AuthorizationSetupRes

The SECC provides information about the available authorization modes and whether the certificate installation service is available.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1067] The EVCC and the SECC shall implement the message elements as defined in Figure 39 and Table 35.

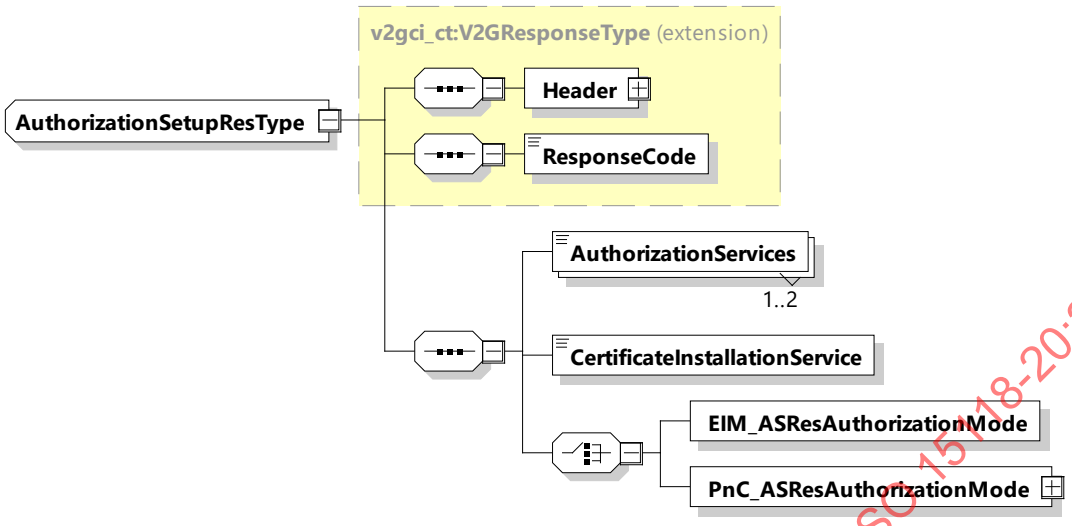


Figure 39 — Schema diagram – AuthorizationSetupRes

The elements of this message are used according to Table 35.

Table 35 — Semantics and type definition for AuthorizationSetupRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
AuthoritzationServices	simple Type: authorizationType enumeration refer to Annex A for the type definition	A parameter that indicates which Authorization Service the EVSE can provide.
CertificateInstallationService	simpleType: xs:boolean	If set to true, the EVSE provides the CertificateInstallation service.
EIM_ASResAuthorizationMode	complexType: EIM_ASResAuthorizationModeType refer to 8.3.5.3.33	Element to be sent when EIM is chosen as authorization method.
PnC_ASResAuthorizationMode	complexType: PnC_ASResAuthorizationModeType refer to 8.3.5.3.34	Includes the challenge by the SECC. This element contains the generated random number.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1219] If in message AuthorizationSetupRes, the SECC offers the service "PnC" in the parameter AuthorizationServices, the SECC shall use the element PnC_ASResAuthorizationMode.

[V2G20-1220] If in message AuthorizationSetupRes, the SECC does not offer the service "PnC" in the parameter AuthorizationServices, the SECC shall use the element EIM_ASResAuthorizationMode.

[V2G20-2096] In case authorization has already been completed by the time AuthorizationSetupReq is received by the SECC or authorization is not necessary, the SECC shall only offer EIM in AuthorizationSetupRes.

[V2G20-2566] The SECC shall indicate via AuthoritzationServices parameter, in AuthorizationSetupRes message, the authorization service(s) offered by the SECC. The SECC could offer EIM or PnC or both as the authorization service(s).

[V2G20-2567] If the SECC offers only EIM as an authorization service, it shall include parameter EIM_ASResAuthorizationMode in AuthorizationSetupRes message.

[V2G20-2568] If the SECC offers PnC as an authorization service, it shall include parameter PnC_ASResAuthorizationMode in AuthorizationSetupRes message.

[V2G20-2570] A private SECC that did not offer OCSP responses for its PE certificate chain shall not provide PnC as an authorization service. Such a private SECC shall not indicate PnC as a supported service in AuthoritzationServices parameter in AuthorizationSetupRes message. Consequently, this private SECC shall not include PnC_ASResAuthorizationMode in AuthorizationSetupRes message.

8.3.4.3.3 AuthorizationReq/Res

This subclause, and all subclauses within it, will provide specific and separate requirements for the private SECC and the SECC. Thus, unless otherwise specified for this subclause or any subclause within it, private SECC and SECC are not considered interchangeable.

8.3.4.3.3.1 AuthorizationReq

[V2G20-1256] The EVCC and the SECC shall implement the message elements as defined in Table 36 and Figure 40.

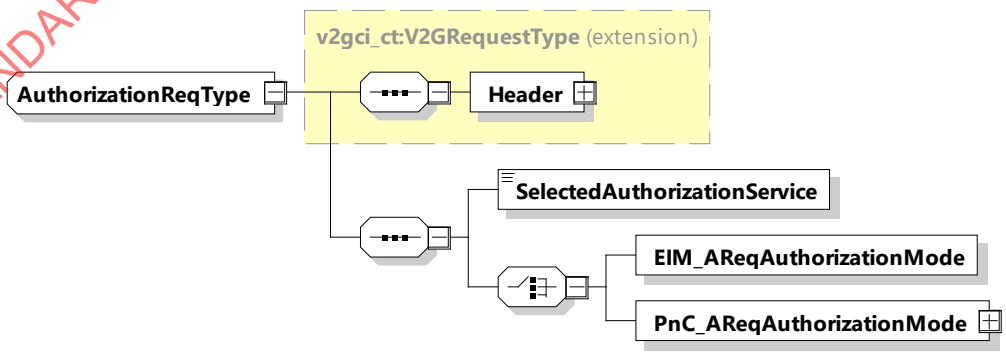


Figure 40 — Schema diagram – AuthorizationReq

The elements of this message are used according to Table 36.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 36 — Semantics and type definition for AuthorizationReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
SelectedAuthorizationService	simple Type: authorizationType enumeration refer to Annex A for the type definition	A parameter that indicates which Authorization Service, which was provided by the EVSE, is chosen by the EV.
EIM_AReqAuthorizationMode	complexType: EIM_AReqAuthorizationModeType refer to 8.3.5.3.31	Element to be sent when EIM is chosen as Authorization Method.
PnC_AReqAuthorizationMode	complexType: PnC_AReqAuthorizationModeType refer to 8.3.5.3.32	This element contains both the challenge sent by the SECC in AuthorizationSetupRes and the EVCC's contract certificate

In case the EVCC has at least one (1) contract certificate and the EVCC wishes to utilize PnC, the EVCC can use SupportedProviders received as part of AuthorizationSetupRes message to identify and select the contract certificate to be provided for that particular session.

SupportedProviders contains the list of providers (eMSPs) supported by the SECC. Each SupportedProvider in SupportedProviders contains data that the EVCC can compare with the data in EMAID of each contract certificate it contains to identify at least one contract certificate that can be utilized at that particular EVSE.

It should be noted that, although not desirable, SupportedProviders may not be exhaustive. That means there might be eMSPs outside of this list that may be supported by the SECC.

In case none of the contract certificates that the EVCC possesses match any of the supported providers in SupportedProviders, the EVCC, at its discretion (or user's discretion, depending upon the OEM implementation), may either choose to still send each of its contract certificates one by one to see if any of them may be accepted or it may switch to EIM.

Similarly, it should be noted that SupportedProviders may be quite long (refer to 8.3.5.3.35 for the allowed length). EVCC, at its (OEM's) discretion, may only accept part of the list provided by the SECC.

[V2G20-2560] In case EIM was selected as authorization service, unless otherwise stated, anytime an element is prefixed with EIM (e.g. EIM_AReqAuthorizationMode), it shall be used. Anytime an element is prefixed with PnC (e.g. PnC_AReqAuthorizationMode), it shall not be used.

[V2G20-2561] In case PnC was selected as authorization service, unless otherwise stated, anytime an element is prefixed with PnC (e.g. PnC_AReqAuthorizationMode), it shall be used. Anytime an element is prefixed with EIM (e.g. EIM_AReqAuthorizationMode), it shall not be used.

[V2G20-2562] In case EVCC did not receive OCSP responses for any of the certificates in the PE certificate chain, it shall not utilize PnC even if the private SECC supports it.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 1 During TLS session setup, the EVCC can determine that the received certificate chain is linked to a PE private root CA certificate. In that case, the received certificate is a PE certificate and the EVCC is connected to a private SECC in a private environment.

NOTE 2 Similarly, the EVCC can determine if the OCSP responses were received for all the certificates in the PE certificate chain.

[V2G20-1063] In case of PnC, the EVCC shall sign the PnC_AReqAuthorizationMode element using the private key associated with the contract certificate.

8.3.4.3.3.2 AuthorizationRes

Finally, in case of PnC, the SECC verifies the challenge signature (and the certificate with its chain if not done before) and sends the corresponding authorization response message.

In case of EIM, the authorization response message is sent based on external inputs and/or SECC setup/configuration.

[V2G20-1257] The EVCC and the SECC shall implement the message elements as defined in Table 37 and Figure 41.

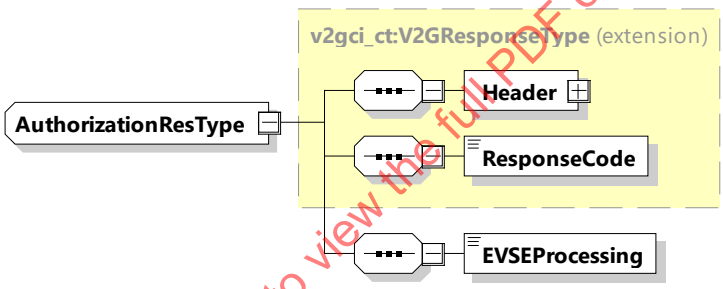


Figure 41 — Schema diagram – AuthorizationRes

The elements of this message are used according to Table 37.

Table 37 — Semantics and type definition for AuthorizationRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
EVSEProcessing	simpleType: processingType enumeration refer to Annex A for the type definition	Parameter indicating that the EVSE has finished the processing that was initiated after the AuthorizationReq or if the EVSE is still processing at the time, the response message was sent.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2563] In case of EIM, the SECC shall complete the authorization at the SECC and provide appropriate response to the EVCC via AuthorizationRes. Refer to 8.6 and its subclauses for details of the response codes.

NOTE 1 It is not in the scope of this document to define how to perform authorization in EIM mode.

[V2G20-2564] In case of PnC, the SECC shall verify the received signature of the AuthorizationReq message by using the provided contract certificate. The SECC shall validate the contract certificate in AuthorizationReq according to [V2G20-1001], [V2G20-2323] and [V2G20-2324]. If any of the aforementioned verifications and validations fail, the SECC shall consider the contract certificate as invalid, and shall not use said contract certificate any further – see [V2G20-2212], [V2G20-2213], [V2G20-2214] and [V2G20-2215].

NOTE 2 The SECC can use a secondary actor for signature verification and for contract certificate validation. It is possible that the certificate failed due to a lack of communication between the SECC and the CSO. It can validate the certificate later. It is up to the CSO's discretion to decide whether to provide services or request authorization using other means.

[V2G20-2565] In case of PnC, the SECC shall verify, that the received GenChallenge matches the GenChallenge that was previously sent by the SECC. If this verification fails, the SECC shall consider the signature as invalid. See [V2G20-2216] and [V2G20-2564]. The SECC may use a secondary actor for signature verification.

[V2G20-1200] In case of EIM, the SECC shall send AuthorizationRes with ResponseCode = "OK" and EVSEProcessing = "Finished" once the external authorization has been successfully completed.

Refer to [V2G20-1583] for details of what options are available to the EVCC after receiving AuthorizationRes message indicating an issue with the contract certificate provided via the previous AuthorizationReq message.

8.3.4.3.4 ServiceDiscoveryReq/Res

8.3.4.3.4.1 ServiceDiscoveryReq/Res handling

The service discovery enables the EVCC to find all services provided by the SECC. This document only describes relevant aspects of the interface between EVCC and SECC with regards to charging/discharging the EV. Nevertheless, the basis for discovery of future value added services is already considered and offers means for extensibility. Therefore, the service discovery differentiates between various service types and scopes.

8.3.4.3.4.2 ServiceDiscoveryReq

By sending the ServiceDiscoveryReq message the EVCC triggers the SECC to send information about all services offered by the SECC. Furthermore, the EVCC can limit for particular services by sending a list of supported service IDs.

[V2G20-1248] The EVCC and the SECC shall implement the message elements as defined in Table 38 and Figure 42.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

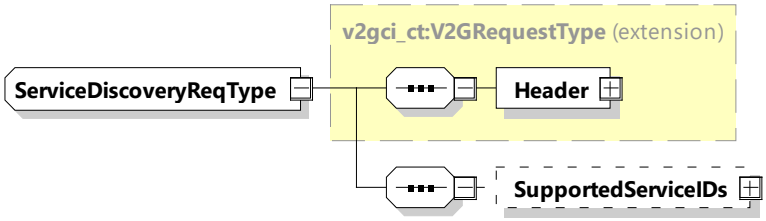


Figure 42 — Schema diagram – ServiceDiscoveryReq

The elements of this message are used according to Table 38.

Table 38 — Semantics and type definition for ServiceDiscoveryReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
SupportedServiceIDs	complexType: ServiceIDListType refer to 8.3.5.3.29	Optional: A list that contains all ServiceIDs that the EV supports. This list can be used to filter the services that the EVSE will offer in the ServiceDiscoveryRes. When omitted, the EVCC intends to receive all provided services by SECC in ServiceDiscoveryRes message

8.3.4.3.4.3 ServiceDiscoveryRes

After receiving the ServiceDisoveryReq message of the EVCC the SECC sends the ServiceDiscoveryRes message. It includes a list of all services available at the SECC.

[V2G20-1249] The EVCC and the SECC shall implement the message elements as defined in Table 39 and Figure 43.

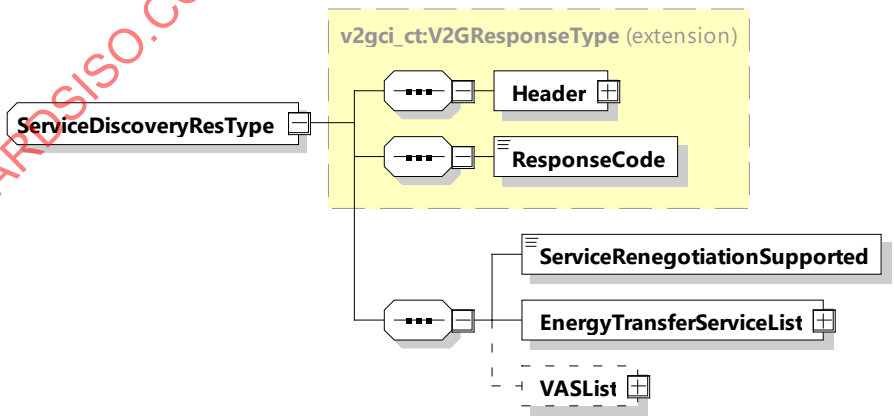


Figure 43 — Schema diagram – ServiceDiscoveryRes

The elements of this message are used according to Table 39.

Table 39 — Semantics and type definition for ServiceDiscoveryRes

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
ServiceRenegotiationSupported	simpleType: xs:boolean	If set to "True" the SECC is capable of ServiceRenegotiation as specified in this document. If set to "FALSE" the SECC is not capable of ServiceRenegotiation. The value of this parameter is valid throughout the service session.
EnergyTransferServiceList	complexType: ServiceListType refer to 8.3.5.3.2	Available energy transfer and BPT services supported by the EVSE.
VASList	complexType: ServiceListType refer to 8.3.5.3.2	Optional: A list containing information on all other services than energy transfer services offered by the EVSE. The returned service list is a filtered list based on the SupportedServiceIDs indicated in the ServiceDiscoveryReq message. The number of service elements is limited to eight.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

8.3.4.3.5 ServiceDetailReq/Res

8.3.4.3.5.1 ServiceDetailReq

By sending the ServiceDetailReq message the EVCC requests the SECC to send specific additional information about services offered by the EVSE.

[V2G20-1250] The EVCC and the SECC shall implement the message elements as defined in Table 40 and Figure 44.

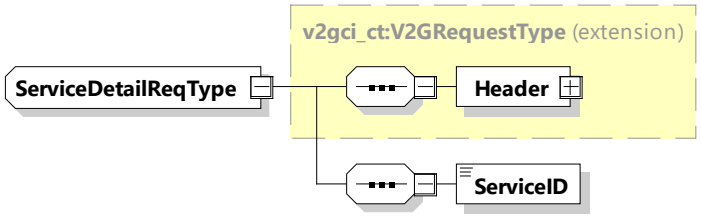


Figure 44 — Schema diagram – ServiceDetailReq

The element of this message is used according to Table 40.

Table 40 — Semantics and type definition for ServiceDetailReq

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
ServiceID	simpleType: serviceIDType xs:unsignedShort	This element identifies a service which has been offered by the SECC in the ServiceDiscoveryRes message for which additional information are needed.

8.3.4.3.5.2 ServiceDetailRes

After receiving the ServiceDetailReq message of an EVCC the SECC sends the ServiceDetailRes message and provides details about services.

[V2G20-1251] The EVCC and the SECC shall implement the message elements as defined in Table 41 and Figure 45.

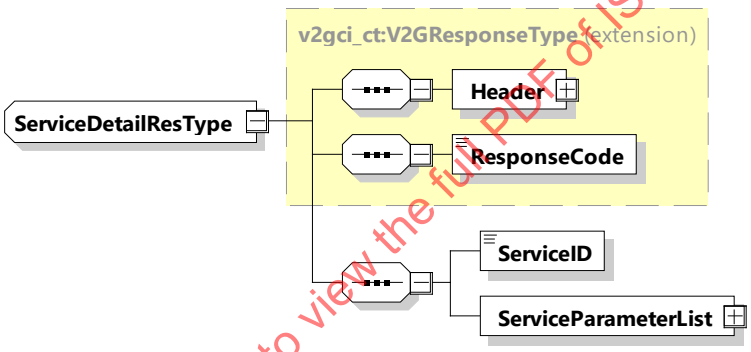


Figure 45 — Schema diagram – ServiceDetailRes

The elements of this message are used according to Table 41.

Table 41 — Semantics and type definition for ServiceDetailRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC in the ServiceDiscoveryRes message and for which additional information has been requested by the EVCC.
ServiceID	simpleType: serviceIDType unsignedShort refer to Annex A for the type definition	This element identifies a service which has been offered by the SECC in the ServiceDiscoveryRes message.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

ServiceParameterList	complexType: ServiceParameterListType refer to 8.3.5.3.21	Includes the list of parameters for a specific serviceID received from the SECC in the ServiceDiscoveryRes message and for which additional information has been requested by the EVCC.

NOTE During the service selection process, EVCC and SECC negotiate the control mode for the charging session. The parameters to be exchanged are dependent on the selected control mode. For details on the scheduled and dynamic control modes see 8.4.2.

8.3.4.3.6 ServiceSelectionReq/Res

8.3.4.3.6.1 ServiceSelection handling

Based on the services provided by the SECC, this message pair allows the transmission of the selected services and related parameter sets.

8.3.4.3.6.2 ServiceSelectionReq

This request message transports the information on the selected services.

VAS requirements are not fully defined yet and will be updated in the next version of this document. As such, the implementers should be careful about implementing VAS.

[V2G20-1252] The EVCC and the SECC shall implement the message elements as defined in Table 42 and Figure 46.

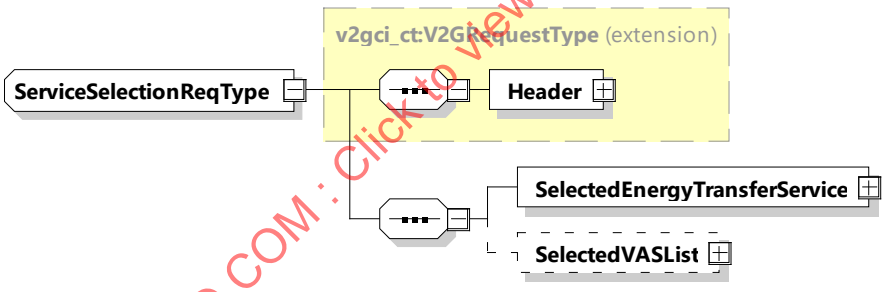


Figure 46 — Schema diagram –ServiceSelectionReq

The elements of this message are used according to Table 42.

Table 42 — Semantics and type definition for ServiceSelectionReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
SelectedEnergyTransferService	complexType: SelectedServiceType refer to 8.3.5.3.25	Contains the selected charge or BPT service.
SelectedVASList	complexType: SelectedServiceListType refer to 8.3.5.3.24	Optional: List contains all selected ServiceIDs and the ParameterSetIDs.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

8.3.4.3.6.3 ServiceSelectionRes

With this message the SECC informs the EVCC whether the selected services were accepted.

[V2G20-1253] The EVCC and the SECC shall implement the message elements as defined in Table 43 and Figure 47.

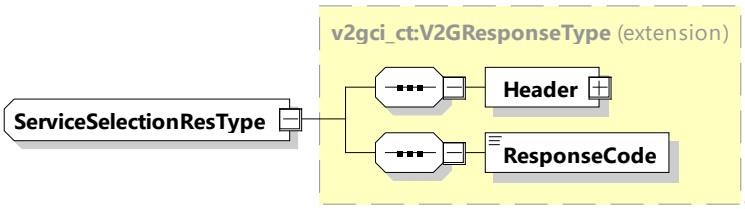


Figure 47 — Schema diagram –ServiceSelectionRes

The elements of this message are used according to Table 43.

Table 43 — Semantics and type definition for ServiceSelectionRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.

8.3.4.3.7 ScheduleExchangeReq/Res

8.3.4.3.7.1 ScheduleExchangeReq/Res handling

After negotiating the energy transfer parameters with the ChargeParameterDiscovery message pair, the SECC provides information about the schedules, which the EVCC might restrict first.

Concepts treated for an optimal supply of energy that corresponds to the customer needs:

When using scheduled control mode, the energy transfer parameters negotiation that precedes the delivery of energy or may be engaged during the energy delivery phase is destined to ensure that the user will be satisfied while at the same time ensuring that the energy will effectively be available and fall within the capacity of power supply grid at the local level (private network) and at the regional level (public network). This required negotiation will become more and more necessary as the number of EVs increase, as well as an increase in volatility of local renewable energy production.

When using the dynamic control mode, the energy transfer parameters can be changed dynamically while in the charging loop, depending on the need of the EVSE.

Initially, before the onset of the energy supply, the EV will negotiate the power profile with the EVSE operator, and third party actors indirectly, to fit to the known or predicted available electric power. The

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

available energy may change once the energy transfer has started due to sudden lack of power source, or increase in demand of other consumptions (e.g. other EV arrival). A schedule renegotiation shall be allowed to cope with difficulties encountered, locally or regionally.

Such a schedule renegotiation is included within the communication protocol between EVSE and EV during the energy transfer period. Upper level systems, to be designed in the future, using this protocol, will manage to combine these functions in order to reach the optimum between satisfaction of user needs and other constraints.

8.3.4.3.7.2 ScheduleExchangeReq

By sending the ScheduleExchangeReq message the EVCC provides its energy transfer parameters to the SECC. This message provides status information about the EV and additional energy transfer parameters, like estimated energy amounts for recharging the EV and the point in time the user intends to leave the EVSE.

[V2G20-1267] The EVCC and the SECC shall implement the message elements as defined in Table 44 and Figure 48.

[V2G20-2642] In case scheduled control mode was selected, if there is no DepartureTime information available, the EVCC shall not include this message element in the ScheduleExchangeReq message.

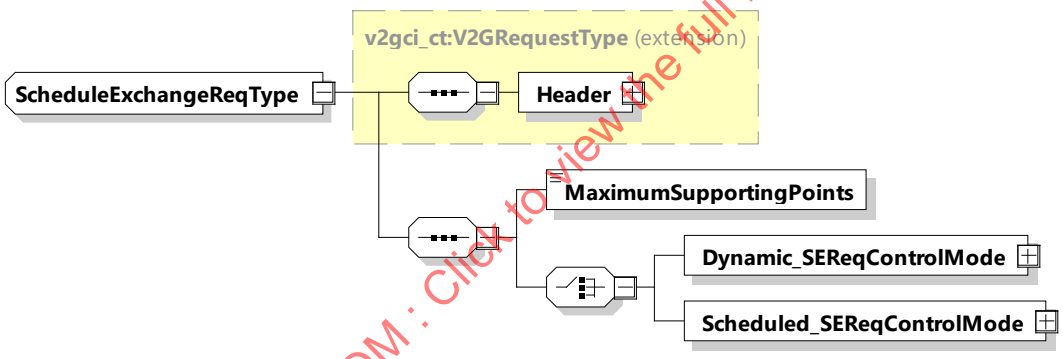


Figure 48 — Schema diagram – ScheduleExchangeReq

The elements of this message are used according to Table 44.

Table 44 — Semantics and type definition for ScheduleExchangeReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
MaximumSupportingPoints	simpleType: maxSupportingPointsScheduleTupleType refer to Annex A for the type definition	Indicates the maximal number of entries in the sub-elements of a ScheduleTuple, where it applies to all elements of PowerScheduleType and PriceRuleType. The SECC can transmit up to the maximum number of entries defined in this parameter.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Dynamic_SEReqControlMode	complexType: Dynamic_SEReqControlModeType refer to 8.3.5.3.13	This element is used by the EVCC for initiating settings for the dynamic control mode.
Scheduled_SEReqControlMode	complexType: Scheduled_SEReqControlModeType refer to 8.3.5.3.14	This element is used by the EVCC for initiating settings for the scheduled control mode.

[V2G20-2175] An EVCC shall set MaximumSupportingPoints to the maximum number of elements of PowerScheduleEntry, PriceRule and PriceLevelScheduleEntries it supports.

[V2G20-1056] The value MaximumSupportPoints shall not exceed 1024.

[V2G20-1201] If more than one ScheduleTuple containing PriceLevelSchedule is sent to the EV, they shall have the same NumberOfPriceLevels and priceLevels inside. Different ScheduleTuples shall correspond to the same energy price level.

[V2G20-1202] An EVCC and an SECC shall support minimum 12 entries for PowerScheduleEntry, PriceRule and priceLevelScheduleEntries elements inside one ScheduleTuple.

[V2G20-1544] An SECC shall send no more than MaximumSupportingPoints entries for PowerScheduleEntry, PriceLevelScheduleEntries and PriceRule.

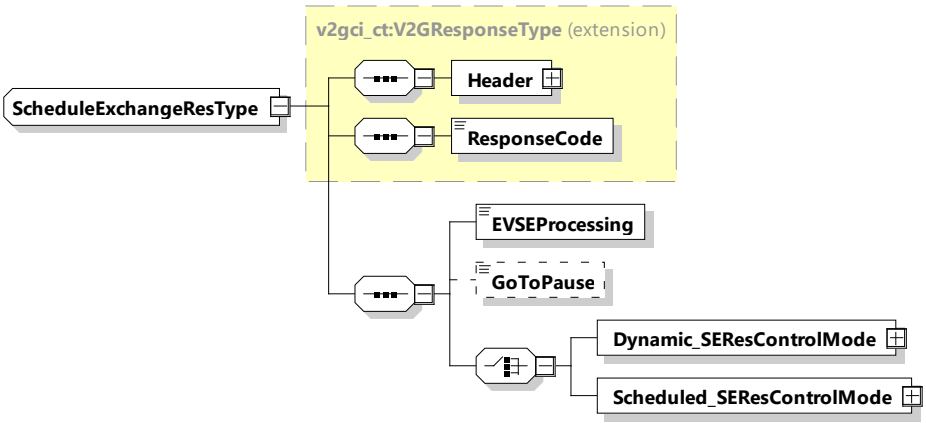
NOTE The parameters related to current, power and voltage provided in ScheduleExchange message pair can be considered as physical limitations, meaning that they are related to the physical abilities of the system under rated operating conditions. Later during the energy transfer process, depending on the external and environmental conditions (State of Charge (SOC), temperatures, etc.), the values of these limitations can change into more conservative values.

8.3.4.3.7.3 ScheduleExchangeRes

With the ScheduleExchangeRes message the SECC provides applicable energy transfer parameters from the grid's perspective. Optionally, this also includes further information on cost over time, cost over demand, cost over consumption or a combination of these. The term cost refers to any kind of cost specified in this document and is not limited to monetary costs. Based on this cost information the EV may optimize its energy transfer schedule for the requested amount of energy.

NOTE 1 By "cost", the EVSE can stimulate - not force - the EV to transfer energy in periods where it is advantageous for the grid (e.g. because in these periods, a lot of wind-power is to be expected).

[V2G20-1259] The EVCC and the SECC shall implement the message elements as defined in Table 45 and Figure 49.



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Figure 49 — Schema diagram – ScheduleExchangeRes

The elements of this message are used according to Table 45.

Table 45 — Semantics and type definition for ScheduleExchangeRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
EVSEProcessing	simpleType: processingType enumeration refer to Annex A for the type definition	Parameter indicating that the EVSE has finished the processing that was initiated after the ScheduleExchangeReq. Alternatively, this parameter can indicate that the EVSE is still processing at the time that the response message was sent.
GoToPause	simpleType: xs:boolean	Optional: When GoToPause is set to TRUE, this indicates that the EVSE does not have any power available and the EVCC can therefore directly go to PowerDeliveryReq.
Dynamic_SEResControlMode	complexType: Dynamic_SEResControlModeType refer refer to 8.3.5.3.15	Includes price schedule for the session. Includes departure time in case EVSE provides it.
Scheduled_SEResControlMode	complexType: Scheduled_SEResControlModeType refer to 8.3.5.3.16	Includes several tuples of schedules from secondary actors. The SECC shall only omit the parameter "ScheduleList" in case EVSEProcessing is set to "Ongoing".

NOTE 2 By using the EVSEProcessing parameter, the EVSE can indicate to the EVCC that the processing is not finished but a response message is sent to fulfil the timeout and performance requirements defined in 8.5.4. This allows continuing the communication session while fulfilling the performance and timeout requirements.

[V2G20-2121] If no power is available at the EVSE, the SECC shall set GoToPause to TRUE and set the first PowerScheduleEntry to 0W.

[V2G20-2122] If DC was selected as the energy transfer mode, the first PowerScheduleEntry in the ScheduleExchangeRes is set to 0W and GoToPause is set to TRUE, the EVCC shall skip DC_CableCheck and DC_PreCharge and directly send a PowerDeliveryReq with ChargeProgress set to Pause.

[V2G20-2123] If the EVCC wants to start with a pause, after having received ScheduleExchangeRes, the EVCC shall send a PowerDeliveryReq with ChargeProgress set to Stop.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 3 V2G20-2123 implies that in case DC was selected as the energy transfer mode, the EVCC will skip DC_CableCheck and DC_PreCharge, similar to V2G20-2122.

8.3.4.3.8 PowerDeliveryReq/Res

8.3.4.3.8.1 PowerDeliveryReq/Res handling

The power delivery message exchange marks the point in time when the EVSE provides voltage to its output power outlet and the EV can start the power transfer.

[V2G20-1260] The value of the ScheduleTupleID element shall be equal to one of the values of the ScheduleTupleID elements (see 8.3.5.3.17) in the list of ScheduleTuple elements (see 8.3.5.3.15) provided in the ScheduleExchangeRes message (see 8.3.4.4.2.3).

[V2G20-1065] If the BPT service was selected in either AC or DC and the reverse power transfer system requires HLC-based control of switching electricity power channels, the parameter BPT_ChannelSelection of PowerDeliveryReq shall be applied.

8.3.4.3.8.2 PowerDeliveryReq

By sending the PowerDeliveryReq the EVCC requests the SECC to provide power. The EVCC also transmits the EVPowerProfile it will follow during the energy transfer process. Additionally, the EVCC can request the SECC to enter a standby or pause period.

NOTE 1 The point in time this message is sent does not necessarily correlate with the start of the energy transfer process. Based on the negotiated EVPowerProfile, the EV could request to start the power flow at a later point in time.

[V2G20-1068] In scheduled control mode, any standby period initiated by the EVCC shall be indicated as zero power period in the currently applied EVPowerProfile, sent in the latest PowerDeliveryReq with ChargeProgress set to "Start", "Standby", "Stop" or "Pause".

A "zero power" period in an EVPowerProfile does not require a pause to be initiated. Only if a pause is requested by the EVCC shall the applied EVPowerProfile indicate this accordingly.

[V2G20-1261] The EVCC and the SECC shall implement the message elements as defined in Table 46 and Figure 50.

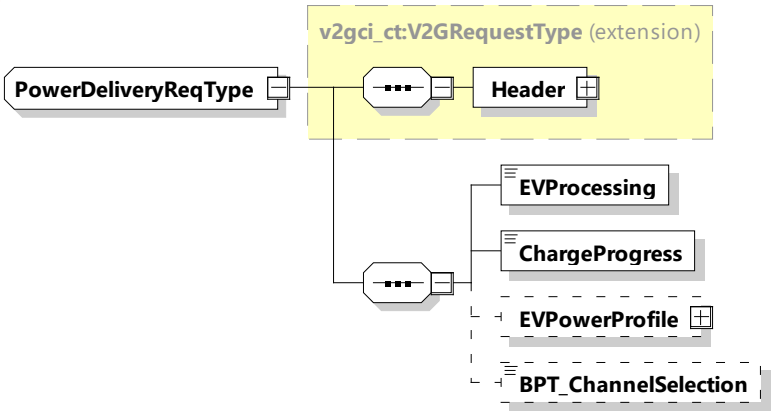


Figure 50 — Schema diagram – PowerDeliveryReq

The elements of this message are used according to Table 46.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 46 — Semantics and type definition for PowerDeliveryReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
EVProcessing	simpleType: processingType enumeration refer to Annex A for the type definition	Parameter indicating that the EV is Finished with the PowerDelivery and will send a different Message next. If set to ongoing, it indicates that the EVCC needs more time to calculate the EVPowerProfile.
ChargeProgress	simpleType: chargeProgressType enumeration refer to Annex A for the type definition	This message element is used to request the EVSE to fulfill all conditions that the energy transfer can start as soon as the EV onboard system begins to retrieve energy without any further action to be taken (i.e. the EVSE is requested to close its contactors successfully). If ChargeProgress is equal to "Start" the EVSE is requested to prepare the energy flow for an immediate start. If ChargeProgress is equal to "Stop" the EVSE is requested to stop the energy flow. If ChargeProgress is equal to "ScheduleRenegotiation" the energy flow is neither stopped nor started, instead the schedule renegotiation mechanisms defined in this document apply. If ChargeProgress is equal to "Standby", the EVSE is notified that EV wants to enter a standby period, and if accepted by EVSE, EVSE shall stop the energy flow. If ChargeProgress is equal to "Pause", the EVSE is notified that EV wants to enter a pause period, and if accepted by EVSE, EVSE shall stop the energy flow and shutdown the communication to be resumed at a later time (as indicated by the EVPowerProfile in scheduled control mode).

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
EVPowerProfile	complexType: EVPowerProfileType refer to 8.3.5.3.9	Optional: Used by the EV to announce and reserve a specific energy transfer profile for the current charging session. In dynamic control mode it describes a simulation from the EVs perspective on the fastest charging profile in order to reach the EVMaximumEnergyRequest under the constraint of the minimum of the EVSEMaximumChargePower and EVMaximumChargePower as communicated during the charge parameter discovery.
BPT_ChannelSelection	simpleType: channelSelectionType refer to Annex A for the type definition	Optional: Information Parameter from EV to show if "Charging" or "Discharging" is planned.

NOTE 2 In dynamic control mode the purpose of the EVPowerProfile is to allow the EVSE to come up with a best effort prediction about the future EVs energy transfer limitations. It by no means defines the real energy transfer profile that will be applied by the EVSE. As the EVPowerProfile is an EV prediction based on the available data at the start of the session, the EVSE can consider the profile as an orientation which is subject to tolerance due to changing energy transfer and boundary conditions.

[V2G20-1069] In scheduled control mode, the SECC shall only communicate the parameter PowerTolerance in ScheduleExchangeRes if it intends to enforce a power transfer behavior which needs to stay within a PowerTolerance band (as defined in [V2G20-1870]), relative to the EVPowerProfile provided by the EVCC during the PowerDeliveryReq. This PowerTolerance band does not apply for time intervals when the power value defined by the EVPowerProfile is "zero". In this case the power and respective current flow shall be as close to zero as technically feasible.

[V2G20-1546] In all control modes the parameter EVPowerProfile, and in scheduled control mode also the parameter ScheduleTupleID, shall be sent if the parameter ChargeProgress in PowerDeliveryReq message is set to "Start", "Standby", "Stop" or "Pause".

8.3.4.3.8.3 PowerDeliveryRes

After receiving the PowerDeliveryReq message of the EVCC the SECC sends the PowerDeliveryRes message including information if power will be available.

[V2G20-1262] The EVCC and the SECC shall implement the message elements as defined in Table 47 and Figure 51.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

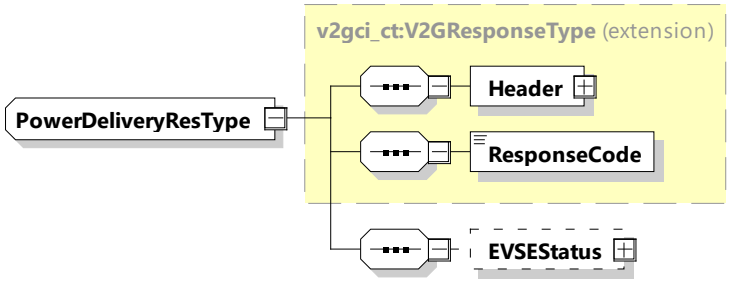


Figure 51 — Schema diagram – PowerDeliveryRes

The elements of this message are used according to Table 47.

Table 47 — Semantics and type definition for PowerDeliveryRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
EVSEStatus	complexType: EVSEStatusType refer to 8.3.5.3.26	Optional: This element is used by the SECC for indicating the EVSE status and for signaling an event the SECC expects the EVCC to react to.

[V2G20-1070] The SECC shall always accept the EVPowerProfile of the EVCC (see 8.3.5.3.9) if it does not violate the rules of requirement [V2G20-1559].

[V2G20-1547] The EV shall adjust its nominal power level in such a way that it at no time exceeds the hard limits as defined by the boundaries of selected ChargingSchedule and — in BPT use cases — the DischargingSchedule. The EV shall ensure that required power ramp limitations are not violated during those adjustments. If the new limit for the power level is "zero", then the resulting active current flow shall be as close to "zero" as technically feasible. In cases where the EV violates any of those hard limits the EVSE may drop the EVs power connection and terminate the charging session.

NOTE 1 The definition of measurement tolerances is out of the scope for this document, but some more background and further references are provided in Annex I.

NOTE 2 For AC connections the defined "zero" rule only applies to the active power (Watt) component.

NOTE 3 For AC the power level is not the measured value but a calculated value based on the nominal voltage. Real implementations might prefer to watch ampere values instead.

8.3.4.3.9 CertificateInstallationReq/Res

8.3.4.3.9.1 CertificateInstallationReq/Res handling

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

When the EVCC does not possess a valid contract certificate or the contract certificate is due to expire soon or the EVCC needs a new contract certificate (for example when the existing contract certificate is not accepted at the particular EVSE where the EV is currently charging, etc.) or EV wants to simply check if a new contract certificate is available, the EVCC can trigger an installation of a new contract certificate into the EVCC. In this use case the EVCC requests available contract certificates from the SECC to be installed into the EVCC. This procedure typically happens before PnC charging since PnC charging with authorization can only be started if a valid contract certificate is available in the EVCC. The SECC may request the certificate from a SA.

The installation of multiple contract certificates is realized with a loop of CertificateInstallation message pairs. Depending on SECC and SA implementations, the SECC may, however, only need to send the first CertificateInstallationReq to the SA in order to retrieve all available contract certificates associated with the OEM provisioning certificate's PCID. Each CertificateInstallationReq/Res message pair between the EVCC and the SECC is used to install exactly one of the available contract certificate chains (including the related sub-CA certificates) and the encrypted private key.

In contrast to ISO 15118-2, both the installation and update of a contract certificate are performed with the CertificateInstallationReq/Res message pair. The CertificateUpdateReq/Res message pair has been removed from this version. The initial installation and later update of one or more contract certificates may take up to several minutes depending on the existing communication link between the SECC and the secondary actors and the number of contract certificates to be installed into the EV. Therefore, it is recommended to not initiate a certificate installation process during each charging session. This avoids unnecessary traffic to the backend as, in most cases, there will not be a new certificate available yet.

The OEM may want to apprise the driver that in cases where contract certificate installation is needed before entering a charging loop, it might take more time than usual for the charging process to start.

The implementation of the CertificationInstallationReq/Res is optional for both EV and EVSE. If the EV does support CertificationInstallationReq/Res messages, the OEM is required to install an OEM provisioning certificate in the EVCC. In such cases, the procedure described here can be used for the installation of the contract certificate.

If no OEM provisioning certificate is available in the EVCC, the procedure described in 8.3.4.3.3.2 (and its sub clauses) cannot be used for contract certificate installation. In these cases the contract certificate should be installed into the EVCC by other means. Mechanisms other than using an OEM provisioning certificate for installing the contract certificate are out of the scope of this document.

For details on OEM provisioning certificates refer to H.4.

NOTE 1 The SECC can request the signed contract data at a secondary actor, if it has online capabilities.

NOTE 2 If the SECC is not able to deliver the requested certificates an appropriate error handling should be performed. If an EVSE is not able to support this function in general, it is supposed to be marked for instance as "offline EVSE" (e.g. by a label at the EVSE). If the EVCC does not possess a valid contract certificate associated with a legal contract, it is not able to use PnC until a certificate installation process is performed successfully.

NOTE 3 For a more detailed explanation of the certificate installation process, see 7.9.2.5 and its subclauses.

8.3.4.3.9.2 CertificateInstallationReq

By sending the CertificateInstallationReq, the EVCC requests the SECC to deliver the certificates that belong to the currently valid contracts of the EV user.

[V2G20-2684] The EVCC shall possess a certificate and corresponding private key usable for signature and key agreement to support the decryption of encrypted information.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Unless specified otherwise, the OEM provisioning certificate and the respective key pair is used for this purpose.

NOTE 1 The EVCC provides the OEM provisioning certificate to the SECC, which then sends it to the SA. The SA uses this certificate to authenticate the EV, find contract certificates associated to this EV and encrypt these contract certificates with a key derived using the OEM provisioning certificate. Details of these steps can be found in the following clauses and in 7.9.2.5.

[V2G20-1265] The EVCC and the SECC shall implement the message elements as defined in Table 48 and Figure 52.

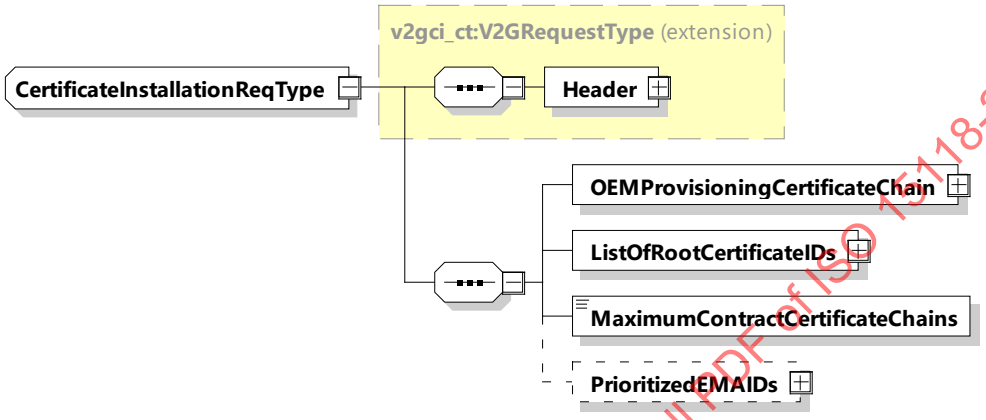


Figure 52 — Schema diagram – CertificateInstallationReq

The elements of this message are used according to Table 48.

Table 48 — Semantics and type definition for CertificateInstallationReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
OEMProvisioningCertChain	complexType: SignedCertificateChainType refer to 8.3.5.3.4	An EV specific certificate chain, consisting of the OEM provisioning certificate and the OEM sub-CA certificates, that was earlier installed in the EVCC typically by an OEM. The ID of the OEM provisioning certificate (PCID), together with the information stored at the SA (contract partner), is used to identify the currently valid contracts of the EV. The certificates shall be DER encoded. Refer to ITU-T X 690 for details of DER encoding. NOTE 1 The OEM provisioning certificate itself (i.e. its public key) is used to encrypt the private key associated with the contract certificate in the CertificateInstallationRes later on. NOTE 2 The PCID can be given to the SA by the customer using a different communication channel. Please refer to H.1 and H.4 for further details.
ListOfRootCertificateIDs	complexType:	This list contains the certificate IDs of all V2G root CA certificates currently installed in the

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
	ListOfRootCertificateIDsType refer to 8.3.5.3.27	EVCC. These root certificates will be used by the EVCC to validate the SA certificates that are included in the CertificateInstallationRes. NOTE 3 The public key from the SA certificate that is included in the CertificateInstallationRes is used to verify the signatures on the CertificateInstallationRes.
MaximumContractCertificateChains	simpleType: xs:unsignedShort	Indicates the maximum number of contract certificate chains the EV wants to install at that time. This can be less than or equal to the maximum number of contract certificate chains the EV can store in its memory. NOTE 4 For example, if the EV can store 5 contract certificates and wants to install all 5, it will set MaximumContractCertificateChains parameter to 5. But if the same EV only wants to install 3 contract certificates, it will set MaximumContractCertificateChains parameter to 3 even though it can store a maximum of 5 contract certificate chains. It is important to note that if the SA only has 2 contract certificates available for this EV, it will only provide those 2 contract certificates even though MaximumContractCertificateChains is higher than the number of contract certificates that the SA has for this EV. However, if the SA has 7 contract certificates available and EV sent CertificateInstallationReq with MaximumContractCertificateChains set to 3, the SA will only provide 3 contract certificates based on the parameter PrioritizedEMAIDs.
PrioritizedEMAIDs	complexType: EMAIDListType Refer to 8.3.5.3.30	Optional: Indicates the list of EMAIDs referencing contract certificates that shall be installed into the EV. The EMAIDs are included in the order of priority from highest priority to lowest priority. The SA will use this parameter to filter the list of contract certificates to be installed in case MaximumContractCertificateChains is smaller than the number of contract certificates available at the SA and ensures that the EV gets the highest priority contract certificates it desires. If this parameter is omitted and the SA has more contract certificates for the EV than the maximum number of contract certificate chains the EV wants to install, indicated by MaximumContractCertificateChains in CertificateInstallationReq, SA may send any MaximumContractCertificateChains contract certificates (applicable to this EV) of the SA's choice.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1548] The EVCC shall sign the body element of CertificateInstallationReq using the private key associated with the "subjectPublicKey" of its OEM provisioning certificate.

NOTE 2 The secondary actor providing the contract certificate will validate the OEM provisioning certificate according to [V2G20-1001], [V2G20-2324] and [V2G20-2325] and verify the signature of the body element of the CertificateInstallationReq using the public key (from "subjectPublicKey") of OEM provisioning certificate included in OEMProvisioningCertChain parameter of CertificateInstallationReq message.

NOTE 3 If necessary, the secondary actor will obtain all of the parent certificates in order to validate the OEM provisioning certificate.

NOTE 4 Refer to B.7 for details of "subjectPublicKey" of OEM provisioning certificate.

[V2G20-2708] In the CertificateInstallationReq message, the EVCC shall use the OEM provisioning certificate in accordance with the configuration mechanism defined in [V2G20-2320]. In case EVCC supports multiple curves, it may send multiple CertificateInstallationReq messages, using the OEM provisioning certificate corresponding to the respective curve.

NOTE 5 SA is expected to generate and encrypt the contract certificate credentials using the same curve as the provided OEM provisioning certificate does. In case SA considers the curve or ECC algorithm used in the provided OEM provisioning certificate insecure, i.e. the SA's configuration parameter from [V2G20-2320] does not match the one of the EVCC, the SA will not be able to provide a contract certificate.

[V2G20-1550] Upon receiving a CertificateInstallationRes, the EVCC shall send another CertificateInstallationReq if the parameter RemainingContractCertificateChains of the CertificateInstallationRes is greater than 0 and the maximum number of contract certificates that can be installed, as indicated by the parameter MaximumContractCertificateChains in CertificateInstallationReq, has not yet been reached.

[V2G20-2571] The EVCC shall stop sending CertificateInstallationReq if the maximum number of contract certificates that can be installed, as indicated by the parameter MaximumContractCertificateChains in CertificateInstallationReq, has been reached while the parameter RemainingContractCertificateChains of the CertificateInstallationRes is greater than zero.

[V2G20-1551] The number of entries of the parameter PrioritizedEMAIDs shall not exceed the value given by MaximumContractCertificateChains.

8.3.4.3.9.3 CertificateInstallationRes

After receiving the CertificateInstallationReq from the EVCC, the SECC sends the CertificateInstallationRes which may include one of the requested certificates. If CertificateInstallationRes includes a certificate, the EVCC installs this certificate as a contract certificate and requests transmission of the other contract certificates, if more are available and EV would prefer to install them all.

[V2G20-1266] The EVCC and the SECC shall implement the message elements as defined in Table 49 and Figure 53.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

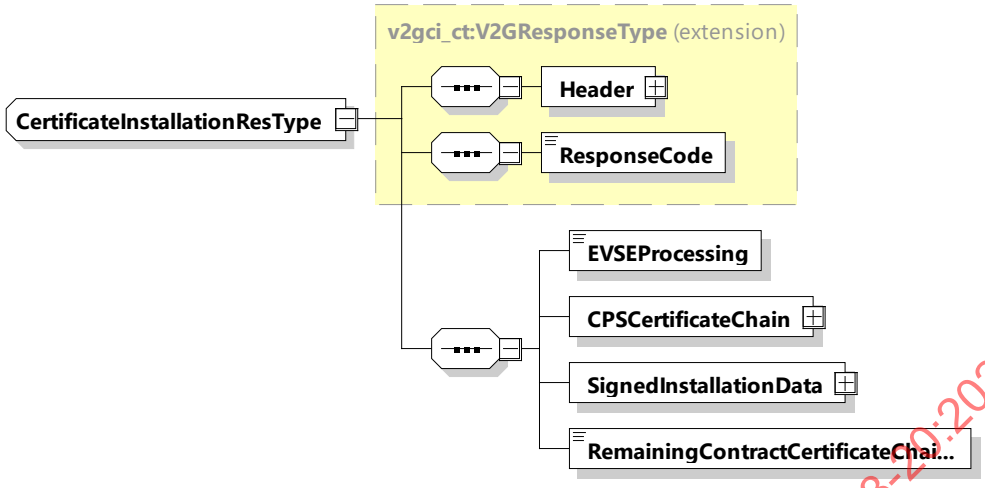


Figure 53 — Schema diagram – CertificateInstallationRes

The elements of this message are used according to Table 49.

Table 49 — Semantics and type definition for CertificateInstallationRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
EVSEProcessing	simpleType: processingType enumeration refer to Annex A for the type definition	Parameter value "Finished" indicates that the EVSE has finished the processing that was initiated after CertificateInstallationReq. Parameter value "Ongoing" indicates that the EVSE is still processing at the time when the response message was sent.
CPSCertificateChain	complexType: CertificateChainType refer to 8.3.5.3.3	The transmitted certificate chain is used by the EVCC to verify the signature in the message header.
SignedInstallationData	complexType: SignedInstallationDataType refer to 8.3.5.3.39	Includes all data to extract contract certificate and private key of contract certificate
RemainingContractCertificateChains	simpleType: xs:unsignedByte	When larger than 0, additional contract certificate chains will be installed.

[V2G20-1552] Upon receiving the first CertificateInstallationReq within a V2G communication session, the SECC shall set the value for the parameter

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

RemainingContractCertificateChains to the minimum of the number of contract certificates available at the SECC minus one and the value given by MaximumContractCertificateChains in CertificateInstallationReq minus one.

[V2G20-1553] If the SECC receives more contract certificates from the secondary actor than indicated by the parameter MaximumContractCertificateChains in CertificateInstallationReq and the parameter PrioritizedEMAIDs is set, then the SECC needs to filter the installation of contract certificates based on PrioritizedEMAIDs.

The SECC shall send a request to a secondary actor upon the first CertificateInstallationReq to download all available contract certificates associated with the PCID of the OEM provisioning certificate that is sent within the CertificateInstallationReq.

[V2G20-2580] If contract certificates for both available (elliptic curve) ECs need to be provided for the same contract, the SECC will need to send multiple CertificateInstallationRes messages according to [V2G20-1550].

NOTE 1 It is up to the eMSP whether it wants to deploy certificates for both curves or only for the currently preferred curve.

[V2G20-1077] The certificate provisioning service shall sign the SignedInstallationData element of the CertificateInstallationRes using the private key associated with the CPS leaf certificate. It shall include the certificate chain for verification of this signature in the field CPSCertificateChain.

NOTE 2 The certificate provisioning service will verify that the data, which is covered by the signature, is received from the preceding secondary actor in an authentic manner.

[V2G20-1078] The EVCC shall verify the signature of the CertificateInstallationRes Message using the signer certificate chain CPSCertificateChain, validate said chain according to [V2G20-1001], [V2G20-2324] and [V2G20-2325] while leaving out the revocation check, and ensure that it traces back to a trusted root certificate.

[V2G20-2648] The EVCC shall ensure that the signature covers the SignedInstallationData element.

[V2G20-2649] If any of the aforementioned fails, the EVCC shall regard the received message as invalid, and discard the message. Otherwise, the EVCC shall continue processing the data received in SignedInstallationData.

[V2G20-2572] The EVCC shall check that the most significant byte (1st byte from left) of DHPublicKey in SignedInstallationData is set to 0x04. If the most significant byte of DHPublicKey is not set to 0x04, the EVCC shall regard the received message as invalid, and discard the message. Otherwise, the EVCC shall continue processing the data received in SignedInstallationData.

[V2G20-2573] When the EVCC receives the parameter ECDHCurve (in SignedInstallationData) set to "SECP521", it shall check that the received DHPublicKey (in SignedInstallationData) is 133 bytes. If the received DHPublicKey is not 133 bytes, the EVCC shall regard the received message as invalid, and discard the message. Otherwise, the EVCC shall continue processing the data received in SignedInstallationData.

[V2G20-2574] When the EVCC receives the parameter ECDHCurve (in SignedInstallationData) set to "X448", it shall check that the received DHPublicKey (in SignedInstallationData) is 57 bytes. If the received DHPublicKey is not 57 bytes, the EVCC shall regard the

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

received message as invalid, and discard the message. Otherwise, the EVCC shall continue processing the data received in SignedInstallationData.

[V2G20-2706] When the EVCC receives the parameter ECDHCurve (in SignedInstallationData) set to the default ECC algorithm according to [V2G20-2674], it shall check that the configuration parameter defined in [V2G20-2320] is also set to this algorithm. If these parameters do not match, the EVCC shall regard the received message as invalid, and discard the message. Otherwise, the EVCC shall continue processing the data received in SignedInstallationData.

NOTE 3 This allows to protect EVCC against downgrade attacks, in case weaknesses in the default curve are discovered.

[V2G20-2707] Upon reception of SignedInstallationData, the EVCC shall check that the received encrypted contract key uses the ECC algorithm in accordance with the configuration parameter [V2G20-2320] or with the OEM provisioning certificate the EVCC provided in the CertificateInstallationReq, otherwise, the EVCC shall regard the received message as invalid, and discard the message.

NOTE 4 This means that if EVCC not equipped with a TPM uses an alternative curve and receives a SECP521_EncryptedPrivateKey, the EVCC will not process the SignedInstallationData.

[V2G20-2578] If all previous checks pass, the EVCC shall store the contract certificate chain and associated private key after having applied requirements as specified in 7.9.2.5 and its subclauses to decrypt the encrypted contract certificate private key and store it securely in the EVCC. Refer to 7.3.6 and its subclauses for secure storage of contract certificate private key.

NOTE 5 An EVCC with a TPM will store/install the contract certificate private key in TPM and follow the requirements for decryption of the private key for EVCCs with TPM. Similarly, an EVCC without a TPM will store/install the contract certificate private key in HSM (or whatever other mechanisms it is using to securely store the private keys) and follow the requirements for decryption of the private key for EVCCs without TPM.

[V2G20-2579] The ContractCertificateChain received by the EVCC in the CertificateInstallationRes Message shall be stored persistently in such a way, that it can be applied later on for the purpose of verifying PriceSchedules. The eMSP sub-CA2 certificate is required to verify PriceSchedules.

NOTE 6 It is not required that the EVCC is able to verify the certificate it has received. It is the task of the certificate provisioning service to provide only valid certificates.

8.3.4.3.10 SessionStopReq/Res

8.3.4.3.10.1 SessionStopReq/Res handling

This V2G message pair shall be used for terminating a V2G communication session initiated by preceding SessionSetupReq message.

8.3.4.3.10.2 SessionStopReq

By sending the SessionStopReq the EVCC requests termination of the energy transfer process.

[V2G20-1271] The EVCC and the SECC shall implement the message elements as defined in Table 50 and Figure 54.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

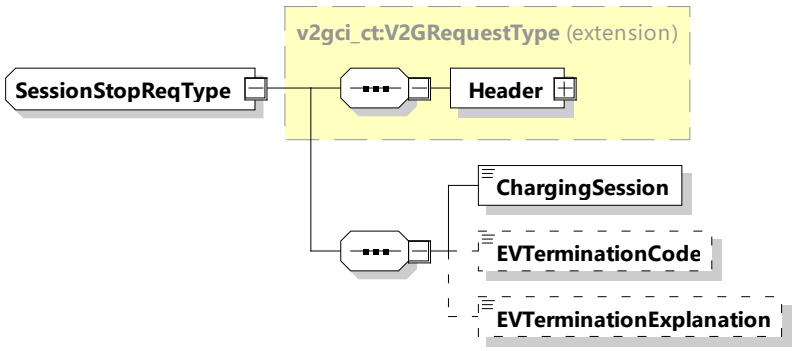


Figure 54 — Schema diagram – SessionStopReq

The elements of this message are used according to Table 50.

Table 50 — Semantics and type definition for SessionStopReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
ChargingSession	simpleType: ChargingSessionType refer to Annex A for the type definition	ChargingSession indicates the intention of the EVCC to either carry out a ServiceRenegotiation ("ServiceRenegotiation"), or to pause ("Pause") or terminate ("Terminate") a V2G communication session.
EVTerminationCode	simpleType: nameType refer to Annex A for the type definition	Optional: A string in URN notation which shall uniquely identify the reason for termination.
EVTerminationExplanation	simpleType: descriptionType refer to Annex A for the type definition	Optional: Indicates the reason for EV termination.

NOTE Future revisions of this document will introduce concrete EVTerminationCode values (e.g. urn:iso:std:iso:15118:-20:EVTerminationCode:ChargerConnectorLockFault). However other documents (e.g. IEC 61851-23) might also define similar codes which also can be expressed as URN values for the EVTerminationCode. The URN namespaces will prevent conflicts in the assigned values.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

8.3.4.3.10.3 SessionStopRes

After receiving the SessionStopReq of the EVCC the SECC sends the SessionStopRes informing the EVCC if terminating the energy transfer process was successful.

[V2G20-1272] The EVCC and the SECC shall implement the message elements as defined in Table 51 and Figure 55.

© ISO 2022 – All rights reserved

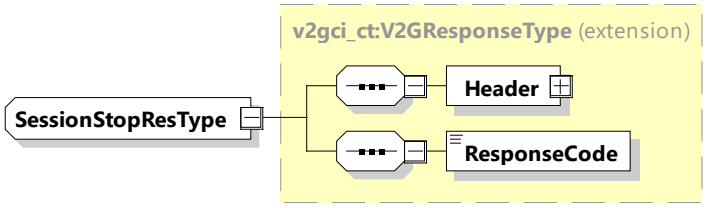


Figure 55 — Schema diagram – SessionStopRes

The elements of this message are used according to Table 51.

Table 51 — Semantics and type definition for SessionStopRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.

[V2G20-1080] After confirming a SessionStopReq with ChargingSession set to "Terminate", by a SessionStopRes with ResponseCode set to "OK", the SECC shall discard all session related information such as session ID, selected charge service or authorization details.

NOTE If a session is terminated it cannot be resumed even if the physical connection has not been disconnected. Any following session can be considered as a new session, requiring a new session ID.

8.3.4.3.11 MeteringConfirmationReq/Res

8.3.4.3.11.1 MeteringConfirmationReq/Res handling

When sending a MeteringConfirmationReq message the EVCC acknowledges that the data elements SessionID, MeterInfo, receipt and the ScheduleTupleID included in the charge loop message prior to this request have been received from the SECC.

Since the EVCC needs to sign the data using the contract certificate's private key, also used for authorization of the services in the currently active V2G communication/service session, the EVCC can only provide this acknowledgement in case PnC is used as the authorization mode. The EVCC cannot provide this acknowledgement when EIM is used as the authorization service.

[V2G20-2704] MeteringConfirmation shall only be used when PnC was selected as the authorization mode during AuthorizationReq.

[V2G20-902] The element MeterInfo sent by the SECC in the message ChargeLoopRes shall be the amount of energy charged during the current service session.

NOTE 1 This would allow the EVCC in general to analyze the meter reading, if it wishes to do so.

[V2G20-1833] If the EVSE is equipped with metering technology and the capability to provide MeterInfo data is supported, then the SECC shall provide initial MeterInfo in the very

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

first charge loop response message. Alternatively, if the SECC knows that MeterInfo data shall be exchanged during an energy transfer session, then the SECC shall provide initial MeterInfo in the very first charge loop response message.

[V2G20-1081] If the EVCC wants to receive the MeterInfo element, the EVCC shall set the parameter MeterInfoRequested to TRUE in the ChargeLoopReq, depending on the charging services on V2GTP payload type EXI encoded V2G messages.

[V2G20-1082] If [V2G20-1081] applies, the SECC shall respond with the ChargeLoopRes including the MeterInfo element.

[V2G20-1083] If the SECC wants to trigger a MeteringConfirmationReq/Res, the SECC shall include the MeterInfo in its ChargeLoopRes and set the EVSENotification to MeteringConfirmation.

[V2G20-2105] If EVSENotification is set to MeteringConfirmation in the ChargeLoopRes, the SECC shall provide a NotificationMaxDelay value. The SECC shall not send another message with EVSENotification set to MeteringConfirmation until it either received a MeteringConfirmationReq or the timeout, which was announced in the NotificationMaxDelay, has been reached.

[V2G20-1084] If [V2G20-1083] applies, the EVCC shall send a MeteringConfirmationReq on V2GTP payload type MeteringConfirmationPayloadID.

[V2G20-1085] If [V2G20-1084] applies, the SECC shall respond with a MeteringConfirmationRes on V2GTP payload type MeteringConfirmationPayloadID.

NOTE 2 After the MeteringConfirmationRes on V2GTP payload type MeteringConfirmationPayloadID messages with ResponseCode = OK has been received by the EVCC, no further message exchange on V2GTP payload type MeteringConfirmationPayloadID messages is expected for this MeteringConfirmation exchange.

8.3.4.3.11.2 MeteringConfirmationReq

[V2G20-1273] The EVCC and the SECC shall implement the message elements as defined in Table 52 and Figure 56.

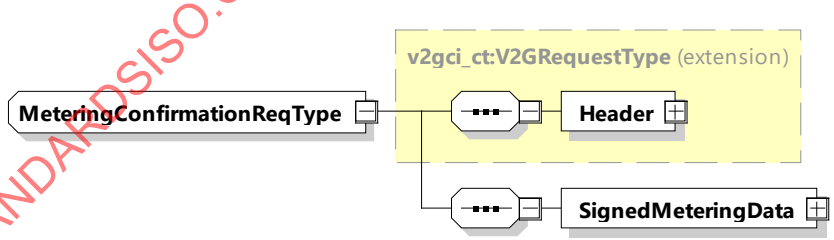


Figure 56 — Schema diagram – MeteringConfirmationReq

The elements of this message are used according to Table 52.

Table 52 — Semantics and type definition for MeteringConfirmationReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

SignedMeteringData	complexType: SignedMeteringData refer to 8.3.5.3.36 for the type definition	Includes all elements that need to be signed by the EVCC.

[V2G20-776] The EVCC shall send the same value of SelectedScheduleTupleID, as it sent it in the PowerDeliveryReq.

[V2G20-2236] If the SECC provided a Receipt in the last ChargeLoopRes, the EVCC shall include this Receipt in the MeteringConfirmationReq.

[V2G20-1808] The EVCC shall sign the SignedMeteringData using the contract certificate's private key, which is also being used for authorization of the services in the currently active V2G communication/service session.

NOTE 1 The signature applied by the EVCC is intended only to confirm that the EVCC, together with the currently applied charging contract certificate, which was selected for this charging session, has received the data elements SessionID, MeterInfo, Receipt and the ScheduleTupleID included in the ChargeLoopRes message prior to this request. It is not intended to confirm that the amount of energy indicated in the previous MeterInfo is correct in the context of billing. However, the SignedMeteringData might be used by any eMSP for billing purposes in general. It is not in the scope of this document to define the billing process which is subject to local regulations.

[V2G20-904] The SECC/SA may verify the signature of the SignedMeteringData element of the MeteringConfirmationReq message using the contract certificate it has received in AuthorizationReq. If this verification fails, the MeteringConfirmationReq shall be regarded as invalid.

NOTE 2 The SECC received the relevant contract certificate in the AuthorizationReq. The SECC accepted this contract certificate as an authorization method when it sent the AuthorizationRes for this AuthorizationReq with the ResponseCode starting with "OK".

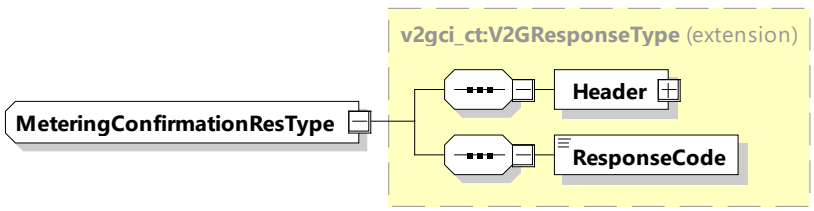
NOTE 3 The SECC can submit the contract certificate to a secondary actor along with the signed SignedMeteringData, so that the secondary actor can later re-verify it. In case the secondary actor has stored the contract certificate already, an ID and the issuing CA for the contract certificate can suffice.

NOTE 4 It is possible that the EVCC is not be able to verify the signature of MeterSignature, which was generated by the SECC and which is included in the MeterInfo element, e.g. because some data necessary for the signature is not transmitted. Therefore, the signature applied by the EVCC in this subclause only serves as an acknowledgement that the EVCC has seen this data and does not constitute any assertion of correctness.

8.3.4.3.11.3 MeteringConfirmationRes

After receiving the MeteringConfirmationReq from the EVCC, the SECC sends the MeteringConfirmationRes informing the EVCC whether the signed data was successfully received and accepted by the SECC.

[V2G20-1274] The EVCC and the SECC shall implement the message elements as defined in Table 53 and Figure 57.



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Figure 57 — Schema diagram – MeteringConfirmationRes

The elements of this message are used according to Table 53.

Table 53 — Semantics and type definition for MeteringConfirmationRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.

8.3.4.4 AC messages

8.3.4.4.1 Overview

Messages defined as AC messages belong to the AC message set(s).

8.3.4.4.2 AC_ChargeParameterDiscoveryReq/Res

8.3.4.4.2.1 AC_ChargeParameterDiscoveryReq/Res handling

After being authorized for charging at the EVSE (SECC) the EVCC and the SECC negotiate the energy transfer parameters with the AC_ChargeParameterDiscovery message pair.

Concepts treated for an optimal supply of energy that corresponds to the customer needs:

When using scheduled control mode, the energy transfer parameters negotiation that precedes the delivery of energy or may be engaged during the energy delivery phase is destined to ensure that the user will be satisfied while at the same time ensuring that the energy will effectively be available and fall within the capacity of power supply grid at the local level (private network) and at the regional level (public network). This required negotiation will become more and more necessary as the number of EVs increase, as well as an increase in volatility of local renewable energy production.

When using the dynamic control mode, the energy transfer parameters can be changed dynamically while in the charging loop, depending on the need of the EVSE.

8.3.4.4.2.2 AC_ChargeParameterDiscoveryReq

By sending the AC_ChargeParameterDiscoveryReq message the EVCC provides its energy transfer parameters to the SECC. This message provides status information about the EV, i.e. the capabilities of the EV charging system.

[V2G20-1258] The EVCC and the SECC shall implement the message elements as defined in Table 54 and Figure 58.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

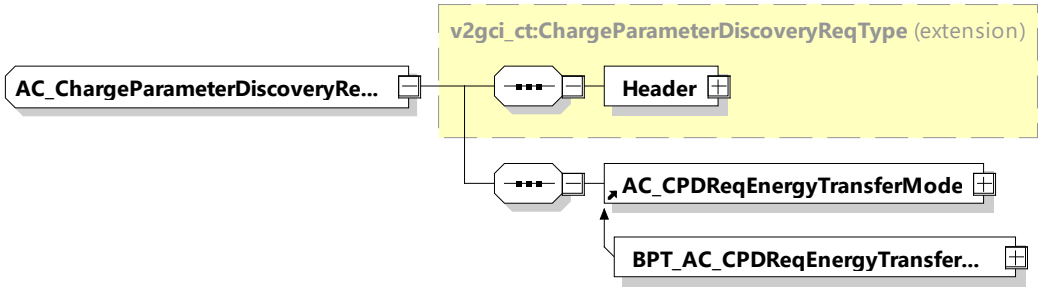


Figure 58 — Schema diagram – AC_ChargeParameterDiscoveryReq

The elements of this message are used according to Table 54.

Table 54 — Semantics and type definition for AC_ChargeParameterDiscoveryReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
AC_CPDReqEnergyTransferMode	complexType: AC_CPDReqEnergyTransferModeType refer to 8.3.5.4.1	This element is used by the EVCC for initiating the target setting process for AC energy transfer.
BPT_AC_CPDReqEnergyTransferMode	complexType: BPT_AC_CPDReqEnergyTransferModeType refer to 8.3.5.4.7.1	This element is used by the EVCC for initiating the target setting process for AC bidirectional energy transfer.

NOTE The parameters related to current, power and voltage provided in AC_ChargeParameterDiscovery message pair can be considered as physical limitations, meaning that they are related to the physical abilities of the system under rated operating conditions. Later during the charging process, depending on the external and environmental conditions (SOC, temperatures, etc.), the values of these limitations can change into more conservative values.

8.3.4.4.2.3 AC_ChargeParameterDiscoveryRes

With the AC_ChargeParameterDiscoveryRes message the SECC provides applicable charge parameters from the grid's perspective.

[V2G20-1206] The EVCC and the SECC shall implement the message elements as defined in Table 55 and Figure 59.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

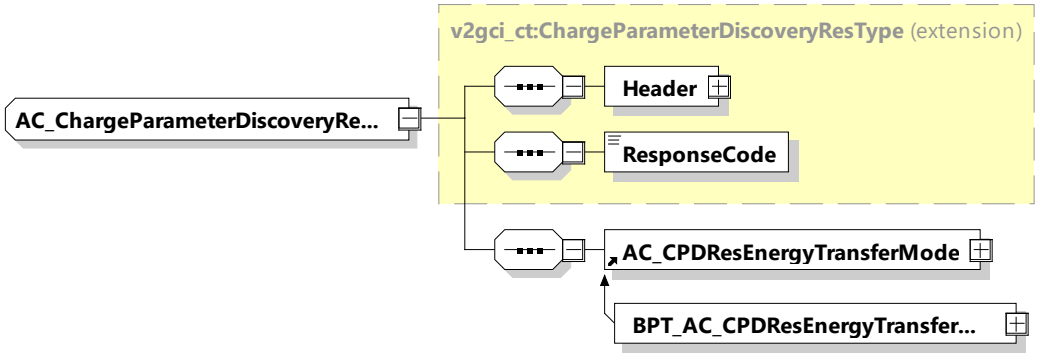


Figure 59 — Schema diagram – AC_ChargeParameterDiscoveryRes

The elements of this message are used according to Table 55.

Table 55 — Semantics and type definition for AC_ChargeParameterDiscoveryRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
AC_CPDResEnergyTransferMode	complexType: AC_CPDResEnergyTransferMode refer to 8.3.5.4.2	This element is used by the SECC for initiating the target setting process for AC energy transfer.
BPT_AC_CPDResEnergyTransferMode	complexType: BPT_AC_CPDResEnergyTransferMode refer to 8.3.5.4.7.2	This element is used by the SECC for initiating the target setting process for AC bidirectional energy transfer.

8.3.4.4.3 AC_ChargeLoopReq/Res

8.3.4.4.3.1 AC_ChargeLoopReq/Res handling

The AC_ChargeLoop message pair provides continuous data exchange between SECC and EVCC. Additionally, it allows sanity checks on the meter readings provided by the SECC.

8.3.4.4.3.2 AC_ChargeLoopReq

[V2G20-1277] The EVCC and the SECC shall implement the message elements as defined in Table 56 and Figure 60.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

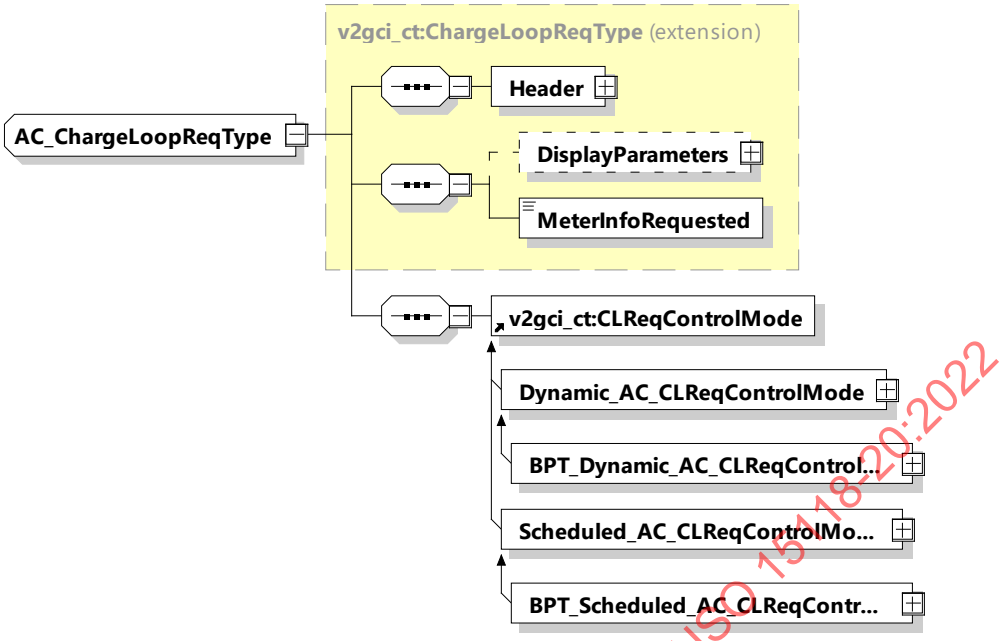


Figure 60 — Schema diagram – AC_ChargeLoopReq

The elements of this message are used according to Table 56.

Table 56 — Semantics and type definition for AC_ChargeLoopReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
DisplayParameters	complexType: DisplayParametersType refer to 8.3.5.3.28	Optional: Parameters that may be displayed on the EVSE or any other user interface which is connected directly or indirectly to the EVSE. They shall under no circumstances influence the V2G communication session.
MeterInfoRequested	simpleType: xs:boolean	When this parameter is set to true, the next AC_ChargeLoopRes shall include the MeterInfo.
Dynamic_AC_CLReqControlMode	complexType: Dynamic_AC_CLReqControlModeType refer to 8.3.5.4.3	This element is used by the EVCC for offering and setting parameters for dynamic control mode energy transfer.
BPT_Dynamic_AC_CLReqControlMode	complexType: BPT_Dynamic_AC_CLReqControlModeType refer to 8.3.5.4.7.3	This element is used by the EVCC for offering and setting parameters for dynamic control mode BPT.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Scheduled_AC_CLReqControlMode	complexType: Scheduled_AC_CLReqControlModeType refer to 8.3.5.4.4	This element is used by the EVCC for offering and setting parameters for scheduled control mode energy transfer.
BPT_Scheduled_AC_CLReqControlMode	complexType: BPT_Scheduled_AC_CLReqControlModeType refer to 8.3.5.4.7.4	This element is used by the EVCC for offering and setting parameters for scheduled control mode BPT.

[V2G20-1810] The absolute value of the following elements, if provided within any AC energy transfer control loop message, shall be less than or equal to the absolute value of the same element provided earlier in the AC_ChargeParameterDiscovery message pair:

- EVMaximumChargePower
- EVMaximumDischargePower

[V2G20-1812] The absolute value of the following elements, if provided within any AC energy transfer control loop message, shall be higher than or equal to the absolute value of the same element provided earlier in the AC_ChargeParameterDiscovery message pair:

- EVMinimumChargePower
- EVMinimumDischargePower

8.3.4.4.3.3 AC_ChargeLoopRes

After receiving the AC_ChargeLoopReq from the EVCC, the SECC sends the AC_ChargeLoopRes.

[V2G20-1278] The EVCC and the SECC shall implement the message elements as defined in Table 57 and Figure 61.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

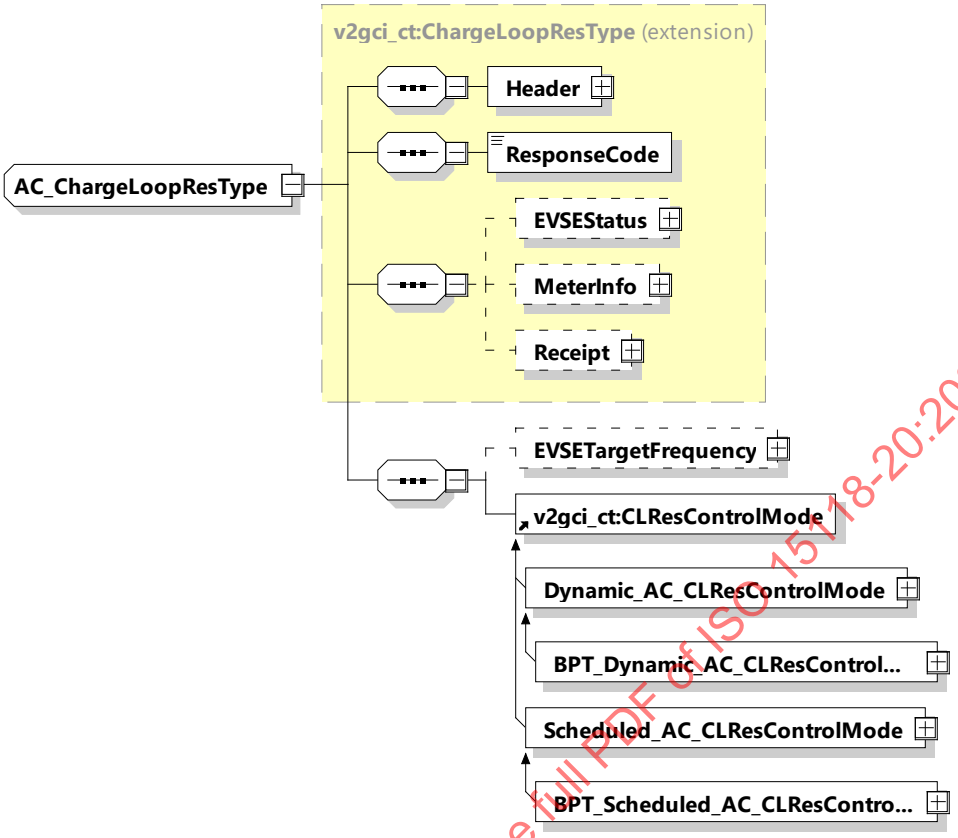


Figure 61 — Schema diagram – AC_ChargeLoopRes

The elements of this message are used according to Table 57.

Table 57 — Semantics and type definition for AC_ChargeLoopRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
EVSEStatus	complexType: EVSEStatusType refer to 8.3.5.3.26	Optional: This element is used by the SECC for indicating the EVSE status and for signaling an event the SECC expects the EVCC to react to.
MeterInfo	complexType: MeterInfoType refer to 8.3.5.3.6	Optional: Includes the energy charged during this service session and other meter relevant data.
Receipt	complexType: ReceiptType Refer to 8.3.5.3.59	Optional: Receipt related information.
EVSETargetFrequency	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target frequency requested by the EVSE
Dynamic_AC_CLResControlMode	complexType: Dynamic_AC_CLResControlModeType refer to 8.3.5.4.5	This element is used by the SECC for offering and setting parameters for dynamic control mode energy transfer.
BPT_Dynamic_AC_CLResControlMode	complexType: BPT_Dynamic_AC_CLResControlModeType refer to 8.3.5.4.7.5	This element is used by the SECC for offering and setting parameters for dynamic control mode charging and discharging.
Scheduled_AC_CLResControlMode	complexType: Scheduled_AC_CLResControlModeType refer to 8.3.5.4.6	This element is used by the SECC for offering and setting parameters for scheduled control mode energy transfer.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
BPT_Scheduled_AC_CLResControlMode	complexType: BPT_Scheduled_AC_CLResControlModeType refer to 8.3.5.4.7.5	This element is used by the SECC for offering and setting parameters for scheduled control mode charging and discharging.

[V2G20-1555] The SECC shall send EVSETargetFrequency values only in situations when the EVSENominalFrequency is no longer the desired equilibrium point.

NOTE 1 This might be necessary in situations like the reconnection of residential power island to the main power grid.

[V2G20-1556] The SECC shall not terminate the charging session only for the reason that an EVSETargetFrequency has not been achieved, as the frequency cannot be attributed to the EV's behavior.

NOTE 2 In AC power grids the frequency is the result of the collective behavior of all connected devices. The frequency is always drifting unless perfect equilibrium has been reached. The grid is typically never running at exactly the EVSENominalFrequency. The EVSENominalFrequency only defines a theoretical target frequency and provides a reference point for the definition of technical requirements which define the detection of and the reaction to abnormal situations. However, in some situations (power grid emergencies, small power islands, etc.) the desired frequency for the equilibrium point intentionally gets pushed outside the normal operating bandwidth. Only in those situations the EVSETargetFrequency can be used. The goal of the EVSETargetFrequency is to communicate the equilibrium point and to enable the EV's power inverter to operate in a robust way under extreme circumstances.

[V2G20-1558] In case EVCC selects the dynamic control mode with the service parameter MobilityNeedsMode set to "2", the SECC shall send a departure time in AC_ChargeLoopRes if it intends to update the DepartureTime sent in the latest ScheduleExchangeRes message.

[V2G20-2179] In dynamic control mode the SECC shall provide the target setpoints for the power transfer by the means of EVSETargetActivePower and EVSETargetReactivePower in AC_ChargeLoopRes.

8.3.4.5 DC messages

8.3.4.5.1 Overview

Messages defined as DC-Messages belong to the DC message set(s).

8.3.4.5.2 DC_ChargeParameterDiscoveryReq/Res

8.3.4.5.2.1 DC_ChargeParameterDiscoveryReq/Res handling

After being authorized for charging at the EVSE (SECC) the EVCC and the SECC negotiate the energy transfer parameters with the DC_ChargeParameterDiscovery message pair.

Concepts treated for an optimal supply of energy that corresponds to the customer needs.

When using scheduled control mode, the energy transfer parameters negotiation that precedes the delivery of energy or may be engaged during the energy delivery phase is destined to ensure that the user

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

will be satisfied while at the same time ensuring that the energy will effectively be available and fall within the capacity of power supply grid at the local level (private network) and at the regional level (public network). This required negotiation will become more and more necessary as the number of EVs increase, as well as an increase in volatility of local renewable energy production.

When using the dynamic control mode, the energy transfer parameters can be changed dynamically while in the charging loop, depending on the need of the EV supply equipment.

8.3.4.5.2.2 DC_ChargeParameterDiscoveryReq

By sending the DC_ChargeParameterDiscoveryReq message the EVCC provides its energy transfer parameters to the SECC. This message provides status information about the EV, i.e. the capabilities of the EV charging system.

[V2G20-1268] The EVCC and the SECC shall implement the message elements as defined in Table 58 and Figure 62.

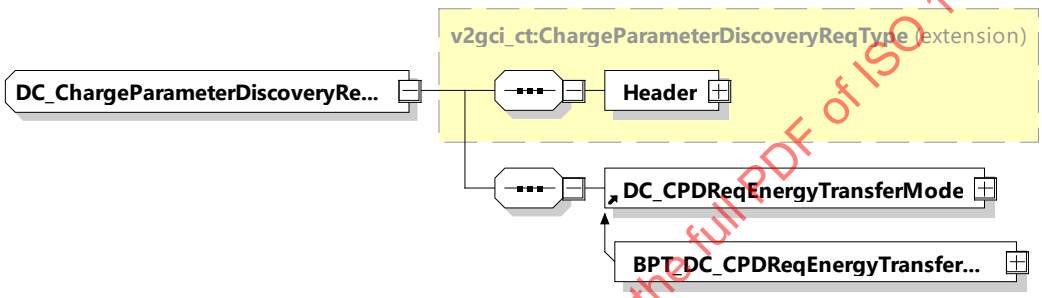


Figure 62 — Schema diagram – DC_ChargeParameterDiscoveryReq

The elements of this message are used according to Table 58.

Table 58 — Semantics and type definition for DC_ChargeParameterDiscoveryReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
DC_CPDReqEnergyTransferMode	complexType: DC_CPDReqEnergyTransferModeType refer to 8.3.5.5.1	This element is used by the EVCC for initiating the target setting process for DC charging.
BPT_DC_CPDReqEnergyTransferMode	complexType: BPT_DC_CPDReqEnergyTransferModeType refer to 8.3.5.5.7.1	This element is used by the EVCC for initiating the target setting process for DC bidirectional charging.

NOTE The parameters related to current, power and voltage provided in DC_ChargeParameterDiscovery message pair can be considered as physical limitations, meaning that they are related to the physical abilities of the system under rated operating conditions. Later during the charging process, depending on the external and environmental conditions (SOC, temperatures, etc.), the values of these limitations can change into more conservative values.

8.3.4.5.2.3 DC_ChargeParameterDiscoveryRes

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

With the DC_ChargeParameterDiscoveryRes message the SECC provides applicable charge parameters from the grid's perspective.

[V2G20-1207] The EVCC and the SECC shall implement the message elements as defined in Table 59 and Figure 63.

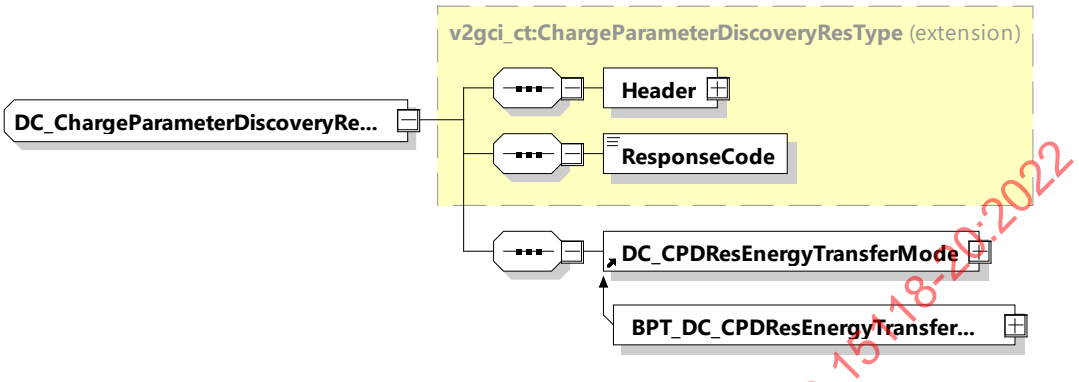


Figure 63 — Schema diagram – DC_ChargeParameterDiscoveryRes

The elements of this message are used according to Table 59.

Table 59 — Semantics and type definition for DC_ChargeParameterDiscoveryRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
DC_CPDResEnergyTransferMode	complexType: DC_CPDResEnergyTransferModeType refer to 8.3.5.5.2	This element is used by the SECC for initiating the target setting process for DC charging.
BPT_DC_CPDResEnergyTransferMode	complexType: BPT_DC_CPDResEnergyTransferModeType refer to 8.3.5.5.7.2	This element is used by the SECC for initiating the target setting process for DC bidirectional charging.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

8.3.4.5.3 DC_CableCheckReq/Res

8.3.4.5.3.1 DC_CableCheckReq/Res handling

[V2G20-1557] To ensure safety in DC energy transfer, a cable check shall be performed.

8.3.4.5.3.2 DC_CableCheckReq

The DC_CableCheckReq asks for the cable check status of the EVSE and, for example, tells the EVSE if the connector is locked on EV side and if the EV is ready to transfer energy.

© ISO 2022 – All rights reserved

[V2G20-1279] The EVCC and the SECC shall implement the message elements as defined in Table 60 and Figure 64.

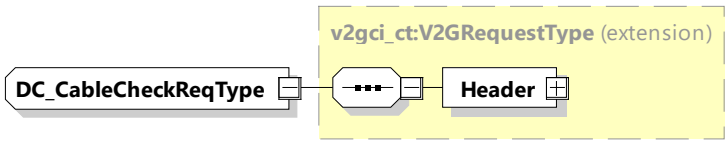


Figure 64 — Schema diagram – DC_CableCheckReq

The element of this message is used according to Table 60.

Table 60 — Semantics and type definition for DC_CableCheckReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.

NOTE DC_CableCheckReq contains no elements

8.3.4.5.3.3 DC_CableCheckRes

After receiving the DC_CableCheckReq from the EVCC the SECC sends the DC_CableCheckRes informing the EVCC about the result of the cable check and EVSE status.

[V2G20-1280] The EVCC and the SECC shall implement the message elements as defined in Table 61 and Figure 65.

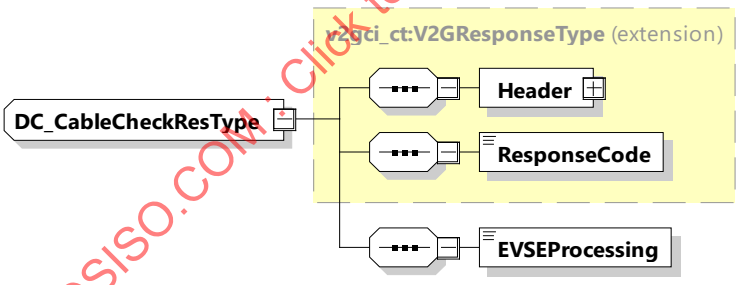


Figure 65 — Schema diagram – DC_CableCheckRes

The elements of this message are used according to Table 61.

Table 61 — Semantics and type definition for DC_CableCheckRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

EVSEProcessing	simpleType: processingType enumeration refer to Annex A for the type definition	Parameter indicating that the EVSE has finished the processing that was initiated after the DC_CableCheckReq or if the EVSE is still processing at the time, the response message was sent.

NOTE By using the EVSEProcessing parameter, the EVSE can indicate to the EVCC that the processing is not finished but a response message is sent to fulfil the timeout and performance requirements defined in 8.5.4. This allows continuing the communication session while fulfilling the performance and timeout requirements.

8.3.4.5.4 DC_PreChargeReq/Res

8.3.4.5.4.1 DC_PreChargeReq/Res handling

PreCharge is used for adjusting the EVSE output voltage to the EV battery voltage.

8.3.4.5.4.2 DC_PreChargeReq

The DC_PreChargeReq is used to start the Pre Charge process from EV side.

[V2G20-1281] The EVCC and the SECC shall implement the message elements as defined in Table 62 and Figure 66.

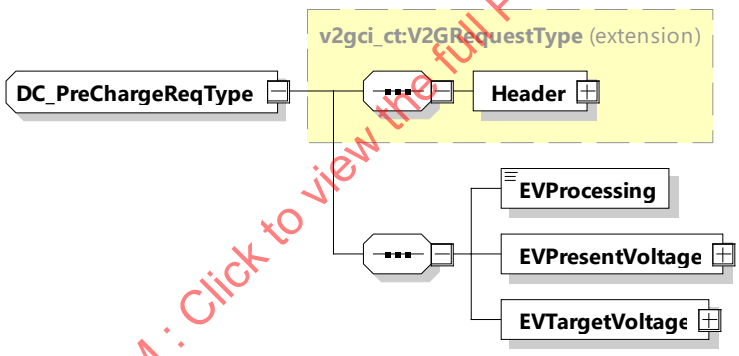


Figure 66 — Schema diagram – DC_PreChargeReq

The elements of this message are used according to Table 62.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 62 — Semantics and type definition for DC_PreChargeReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
EVProcessing	simpleType: processingType enumeration refer to Annex A for the type definition	Parameter that indicates the stop of the DC_PreCharge process by the EV. When the EV wants to continue in the Sequence, the EVProcessing is set to "Finished", while still running it is set to "Ongoing".
EVPresentVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Present voltage of the EV
EVTargetVoltage	complexType RationalNumberType refer to 8.3.5.3.8	Target voltage of the EV (see 8.3.4.5.5.2 for more background)

The SECC shall adjust the voltage on the EVSE side, which is reported in the EVSEPresentVoltage element within the DC_PreChargeRes, to match the EVTargetVoltage as closely as necessary (for details see IEC 61851-23) in order to allow the contactors to close and to exit the PreCharge phase.

8.3.4.5.4.3 DC_PreChargeRes

After receiving the DC_PreChargeReq from the EVCC the SECC sends the DC_PreChargeRes informing the EV about the EVSE status and the present EVSE output voltage.

[V2G20-1282] The EVCC and the SECC shall implement the message elements as defined in Table 63 and Figure 67.

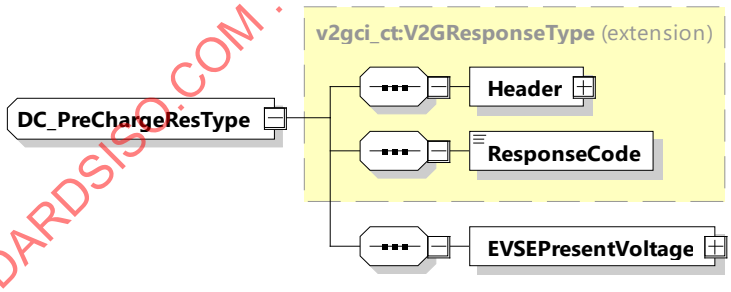


Figure 67 — Schema diagram – DC_PreChargeRes

The elements of this message are used according to Table 63.

Table 63 — Semantics and type definition for DC_PreChargeRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
EVSEPresentVoltage	complexType RationalNumberType refer to 8.3.5.3.8	Present voltage as measured by the EVSE

8.3.4.5.5 DC_ChargeLoopReq/Res

8.3.4.5.5.1 DC_ChargeLoopReq/Res handling

For DC charging control cyclic exchange of the requested current from EV side is necessary. Also, the target voltage and the difference in current and voltages is transferred.

8.3.4.5.5.2 DC_ChargeLoopReq

By sending the DC_ChargeLoopReq the EV requests a certain current from the EVSE. Also, the target voltage, current and voltage difference are transferred.

[V2G20-1283] The EVCC and the SECC shall implement the message elements as defined in Table 64 and Figure 68.

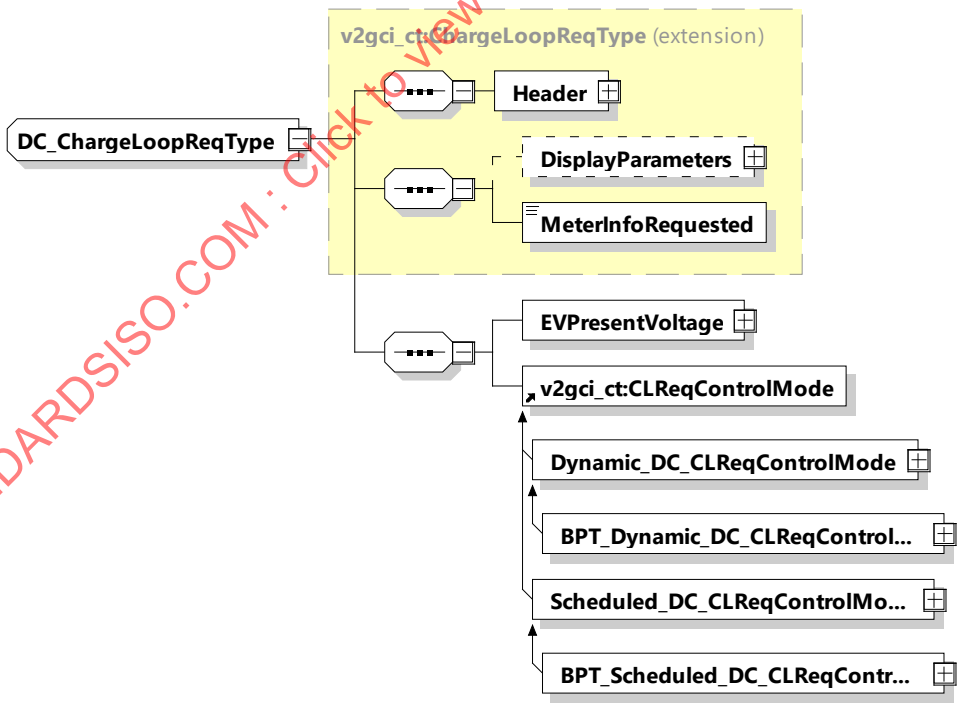


Figure 68 — Schema diagram – DC_ChargeLoopReq

The elements of this message are used according to Table 64.

Table 64 — Semantics and type definition for DC_ChargeLoopReq

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
DisplayParameters	complexType: DisplayParametersType refer to 8.3.5.3.28	Optional: Parameters that may be displayed on the EVSE or any other user interface which is connected directly or indirectly to the EVSE. They shall under no circumstances influence the V2G communication session.
MeterInfoRequested	simpleType: xs:boolean	This Parameter indicates, if set to "TRUE" that the EV wants to receive the MeterInfo by the EVSE.
EVPresentVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Present voltage of the EV
Dynamic_DC_CLReqControlMode	complexType: Dynamic_DC_CLReqControlModeType refer to 8.3.5.5.3	This element is used by the EVCC for offering and setting parameters for dynamic control mode energy transfer.
BPT_Dynamic_DC_CLReqControlMode	complexType: BPT_Dynamic_DC_CLReqControlModeType refer to 8.3.5.5.7.3	This element is used by the EVCC for offering and setting parameters for dynamic control mode BPT.
Scheduled_DC_CLReqControlMode	complexType: Scheduled_DC_CLReqControlModeType refer to 8.3.5.5.4	This element is used by the EVCC for offering and setting parameters for Scheduled control mode energy transfer.
BPT_Scheduled_DC_CLReqControlMode	complexType: BPT_Scheduled_DC_CLReqControlModeType refer to 8.3.5.5.7.4	This element is used by the EVCC for offering and setting parameters for Scheduled control mode BPT.

NOTE 1 EVTargetVoltage and EVTargetCurrent are used by the EV in the scheduled control mode to request a certain voltage or current value from the EVSE. In dynamic control mode, where the EVSE is in charge of choosing the energy transfer plan and the related power setpoints, these elements are not available. In all DC_ChargeLoopReq variations, the EVs limitations are provided by means of EVMaximumChargeCurrent, EVMaximumChargePower, EVMaximumDischargeCurrent, EVMaximumDischargePower, EVMaximumVoltage and EVMinimumVoltage (for example, see [V2G20-2180]).

[V2G20-2180] EVMaximumVoltage and EVMinimumVoltage shall express limits for EVPresentVoltage and shall represent the state at the EV inlet. If a different physical measurement point is used inside the EV than the EVCC shall apply the necessary correction factors before communicating the EVPresentVoltage.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 2 If the SECC sees, that the EVPresentVoltage exceeds one of the limits then there is the risk of a termination of the charging session due to the EV enforcing safety protection measures.

If, for example, the EV is measuring voltage via the BMS inside the battery and is also using a DC-DC converter between the battery and the DC inlet then the EVCC shall apply a meaningful mathematical transformation to the actual measured voltage values. It is important that the EVPresentVoltage multiplied with EVSEPresentCurrent does not contradict any power limitations communicated by the EV because the SECC might use that as a plausibility check to validate its charging strategy.

[V2G20-2198] The absolute value of the following elements, if provided within any DC energy transfer control loop message, shall be less than or equal to the absolute value of the same element provided earlier in the DC_ChargeParameterDiscovery message pair:

- EVMaximumChargeCurrent
- EVMaximumDischargeCurrent
- EVMaximumChargePower
- EVMaximumDischargePower
- EVMaximumVoltage

[V2G20-2199] The absolute value of the following elements, if provided within any DC energy transfer control loop message, shall be higher than or equal to the absolute value of the same element provided earlier in the DC_ChargeParameterDiscovery message pair:

- EVMinimumChargeCurrent
- EVMinimumDischargeCurrent
- EVMinimumChargePower
- EVMinimumDischargePower
- EVMinimumVoltage

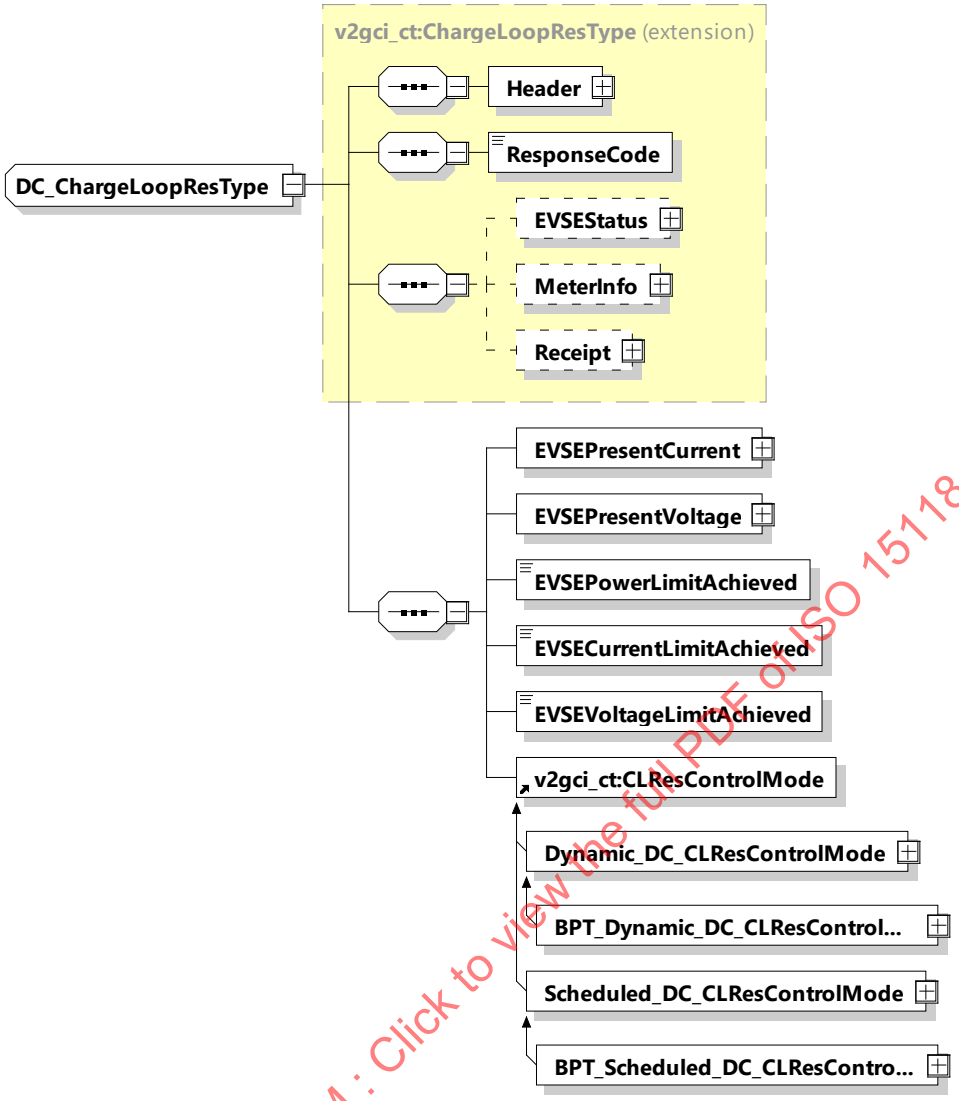
8.3.4.5.5.3 DC_ChargeLoopRes

After receiving the DC_ChargeLoopReq from the EVCC the SECC sends the DC_ChargeLoopRes informing the EV about the EVSE status and the present EVSE output voltage and current.

[V2G20-1284] The EVCC and the SECC shall implement the message elements as defined in Table 65 and Figure 69.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Figure 69 — Schema diagram – DC_ChargeLoopRes

The elements of this message are used according to Table 65.

Table 65 — Semantics and type definition for DC_ChargeLoopRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
EVSEStatus	complexType: EVSEStatusType refer to 8.3.5.3.26	Optional: This element is used by the SECC for indicating the EVSE status and for signalling an event the SECC expects the EVCC to react to.
MeterInfo	complexType: MeterInfoType refer to 8.3.5.3.6	Optional: Includes the energy charged during this service session and other meter relevant data.
Receipt	complexType: ReceiptType refer to 8.3.5.3.59	Optional: Receipt related information.
EVSEPresentCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Present current as measured by the EVSE.
EVSEPresentVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Present voltage as measured by the EVSE.
EVSECurrentLimitAchieved	simpleType: xs:boolean	If set to TRUE, the EVSE has reached its current limit.
EVSEVoltageLimitAchieved	simpleType: xs:boolean	If set to TRUE, the EVSE has reached its voltage limit.
EVSEPowerLimitAchieved	simpleType: xs:boolean	If set to TRUE, the EVSE has reached its power limit.
Dynamic_DC_CLResControlModeType	complexType: Dynamic_DC_CLResControlModeType refer to 8.3.5.5.5	This element is used by the SECC for offering and setting parameters for dynamic control mode energy transfer.
BPT_Dynamic_DC_CLResControlModeType	complexType: BPT_Dynamic_DC_CLResControlModeType refer to 8.3.5.5.7.5	This element is used by the SECC for offering and setting parameters for dynamic control mode BPT.
Scheduled_DC_CLResControlModeType	complexType: Scheduled_DC_CLResControlModeType refer to 8.3.5.5.6	This element is used by the SECC for offering and setting parameters for scheduled control mode energy transfer.
BPT_Scheduled_DC_CLResControlModeType	complexType: BPT_Scheduled_DC_CLResControlModeType refer to 8.3.5.5.7.6	This element is used by the SECC for offering and setting parameters for scheduled control mode BPT.

NOTE EVSEPresentVoltage and EVSEPresentCurrent implicitly communicate the present power that is applied by the EVSE on the charging cable. This information can be used by the EVCC, for example, to validate if the target setpoints in scheduled control mode have been respected by the EVSE or how the active PriceAlgorithm needs to be applied (see 8.3.5.3.49.1).

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1275] In case EVCC selects the dynamic control mode with the service parameter MobilityNeedsMode set to "2", the SECC shall send a departure time in DC_ChargeLoopRes if it intends to update the DepartureTime sent in the latest ScheduleExchangeRes message.

[V2G20-2654] The absolute value of the following elements, if provided within any DC energy transfer control loop message, shall be less than or equal to the absolute value of the same element provided earlier in the DC_ChargeParameterDiscovery message pair:

- EVSEMaximumChargeCurrent
- EVSEMaximumDischargeCurrent
- EVSEMaximumVoltage
- EVSEMaximumChargePower
- EVSEMaximumDishargePower

[V2G20-2655] The absolute value of the following elements, if provided within any DC energy transfer control loop message, shall be higher than or equal to the absolute value of the same element provided earlier in the DC_ChargeParameterDiscovery message pair:

- EVSEMinimumChargeCurrent
- EVSEMinimumDischargeCurrent
- EVSEMinimumVoltage
- EVSEMinimumChargePower
- EVSEMinimumDischargePower

8.3.4.5.6 DC_WeldingDetectionReq/Res

8.3.4.5.6.1 DC_WeldingDetectionReq/Res handling

The Welding Detection messages described in this subclause allow to implement the Welding Detection mechanism according to IEC 61851-23.

8.3.4.5.6.2 DC_WeldingDetectionReq

By sending the DC_WeldingDetectionReq the EV requests welding detection on EVSE side.

[V2G20-1285] The EVCC and the SECC shall implement the message elements as defined in Table 66 and Figure 70.

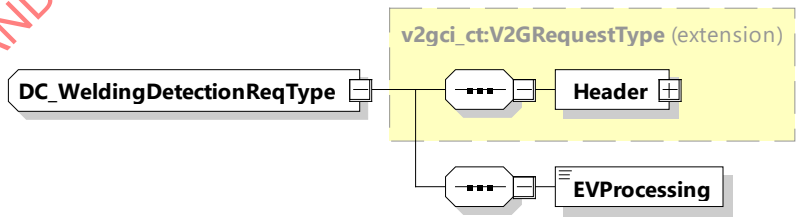


Figure 70 — Schema diagram – DC_WeldingDetectionReq

The elements of this message are used according to Table 66.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 66 — Semantics and type definition for DC_WeldingDetectionReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
EVProcessing	simpleType: processingType enumeration refer to Annex A for the type definition	Parameter that indicates the stop of the DC_WeldingDetection process by the EV. When the EV wants to continue in the Sequence, the EVProcessing is set to "Finished", while still running it is set to "Ongoing".

8.3.4.5.6.3 DC_WeldingDetectionRes

After receiving the DC_WeldingDetectionReq from the EVCC, the SECC sends the Welding Detection Response informing the EV about the EVSE status and the present EVSE output voltage.

[V2G20-1286] The EVCC and the SECC shall implement the message elements as defined in Table 67 and Figure 71.

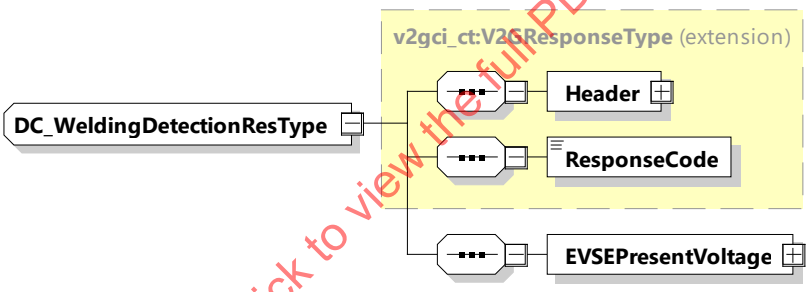


Figure 71 — Schema diagram – DC_WeldingDetectionRes

The elements of this message are used according to Table 67.

Table 67 — Semantics and type definition for DC_WeldingDetectionRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
EVSEPresentVoltage	complexType RationalNumberType refer to 8.3.5.3.8	Present voltage as measured by the EVSE

8.3.4.6 WPT messages

8.3.4.6.1 Overview

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Messages defined as WPT-Messages belong to the WPT message set(s).

8.3.4.6.2 WPT_FinePositioningSetupReq/Res

WPT_FinePositioningSetupReq/Res are used to exchange system setup data between the EVCC and SECC describing the individual positioning system characteristics at the EV device and at the supply device. Additionally, possibilities for the pairing and alignment check methods are exchanged and determined.

8.3.4.6.2.1 WPT_FinePositioningSetupReq/Res handling

After SessionSetup has been done the EVCC sends a WPT_FinePositioningSetupReq in order to determine the possible options of the SECC for fine positioning, pairing and alignment check support. With the WPT_FinePositioningReq the EVCC will inform the SECC about its possible options.

The SECC responds to the request with a WPT_FinePositioningSetupRes containing information about available options with respect to fine positioning, pairing, and alignment check.

After analyzing the available options, the EVCC sends a WPT_FinePositioningSetupReq containing information about the choice for fine position, pairing and alignment check made by the EV.

The SECC responds with a confirmation of the EV's choice in the WPT_FinePositioningSetupRes.

8.3.4.6.2.2 WPT_FinePositioningSetupReq

By sending the WPT_FinePositioningSetupReq message the EVCC provides its WPT_Fine positioning setup parameters to the SECC.

[V2G20-5009] The EVCC and the SECC shall implement the message elements as defined in Figure 72 and Table 68.

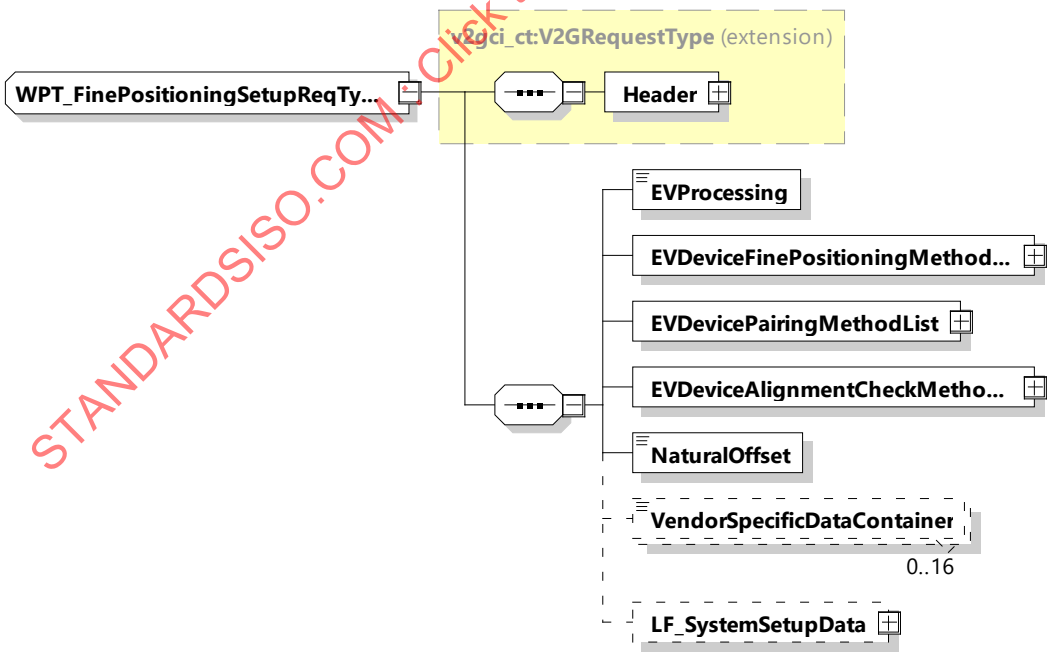


Figure 72 — Schema diagram – WPT_FinePositioningSetupReq

The elements of this message are used according to Table 68.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 68 — Semantics and type definition for WPT_FinePositioningSetupReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
EVProcessing	simpleType: processingType refer to Annex A for the type definition	Indicates the progress of the selection progress for the methods of Fine positioning, pairing and alignment check. The setting of this parameter impacts the usage of the elements "EVDeviceFinePositioningMethodList", "EVDevicePairingMethodList", "EVDeviceAlignmentCheckMethodLists"
EVDeviceFinePositioningMethodList	simpleType: WPT_FinePositioningMethodListType refer to Annex A for the type definition	Fine positioning method intended to be used by the EV: Multiple options are possible, ordered by priority (See IEC 61980-2). – Manual (default): Any fine position method which does not depend on technical data exchange during the positioning process, e.g. positioning by visually detecting specified marking or characteristics – LF_TxEV: LF positioning with transmitter at EV – LF_TxPrimaryDevice: LF positioning with transmitter at primary device – LPE: Low power excitation according – Proprietary: Any proprietary positioning method with individualized data exchange over element VendorSpecificDataContainer in FinePositioningReq/Res messages

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
EVDevicePairingMethodList	simpleType: WPT_PairingMethodListType refer to Annex A for the type definition	Pairing method intended to be used by the EV: Multiple options are possible, ordered by priority (See IEC 61980-2). – External confirmation (default) – LPE: application of low power excitation for pairing – LF_TxEV: application of LF signal transmitted by EV for pairing – LF_TxPrimaryDevice: application of LF signal transmitted by primary device for pairing – Optical: Pairing by means of machine vision, e.g. QR code at primary device which can be read by EV and sent to the SECC – Proprietary: Any proprietary positioning method with individualized data exchange over data block in pairingReq/Res messages
EVDeviceAlignmentCheckMethodList	simpleType: WPT_AlignmentCheckMethodListType refer to Annex A for the type definition	Alignment check method intended to be used by the EV: Multiple options are possible, ordered by priority (See IEC 61980-2). – LPE: application of low power excitation for alignment check – Power check (default): utilization of minimal power transfer and anomaly detection for reasonable confidence of alignment – Proprietary: Anything with individualized message structure
NaturalOffset	simpleType: xs:unsignedShort	Offset of the center alignment point in mm (in x-direction) which results from the coil design of EV and infrastructure.
VendorSpecificDataContainer	simpleType: WPT_DataContainerType refer to Annex A for the type definition	Optional: Data container for proprietary information
LF_SystemSetupData	simpleType: WPT_LF_SystemSetupDataType refer to Annex A for the type definition	Optional: Additional data needed to describe a LF positioning system. This information is needed, when LF_TxEV or LF_TxPrimaryDevice is given in the list EVDevicePositioningMethods.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-5001] As long as EVProcessing is set to "Ongoing" the lists "EVDeviceFinePositioningMethodList", "EVDevicePairingMethodList", "EVDeviceAlignmentCheckMethodList" shall contain more than one element.

[V2G20-5002] If the lists "EVDeviceFinePositioningMethodList", "EVDevicePairingMethodList", "EVDeviceAlignmentCheckMethodList" contain more than one element, the default values shall be part of the list, if the device is a compatibility class A device (see IEC 61980-2 and IEC 61980-3).

[V2G20-5003] If the EVProcessing is set to "Finished", the lists shall contain only one element which represents the EV's choice.

NOTE 1 The value of this element does not need to be the default value.

8.3.4.6.2.3 WPT_FinePositioningSetupRes

With the WPT_FinePositioningSetupRes message the SECC provides information about possible methods for fine positioning, pairing and alignment check together with setup parameters, accordingly.

[V2G20-5010] The EVCC and the SECC shall implement the message elements as defined in Figure 73 and Table 69.

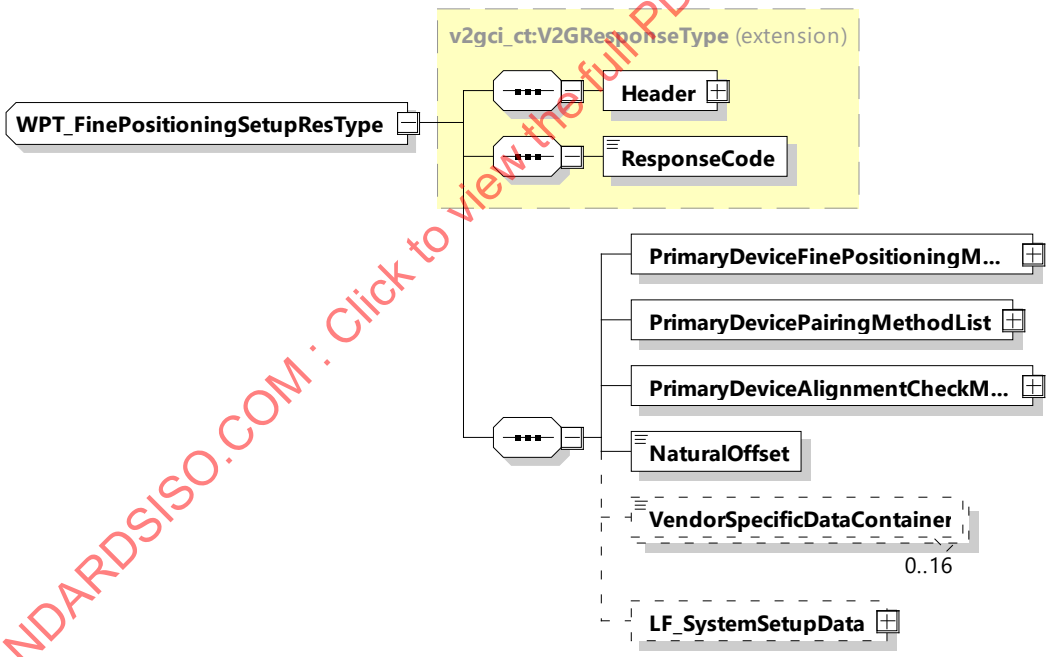


Figure 73 — Schema diagram – WPT_FinePositioningSetupRes

The elements of this message are used according to Table 69.

Table 69 — Semantics and type definition for WPT_FinePositioningSetupRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
PrimaryDeviceFinePositioningMethodList	simpleType: WPT_FinePositioningMethodListType refer to Annex A for the type definition	Fine positioning method intended to be used by the primary device (confirmation of EVs choice) (See IEC 61980-2). The default value is "Manual".
PrimaryDevicePairingMethodList	simpleType: WPT_PairingMethodListType refer to Annex A for the type definition	Pairing method intended to be used by the primary device (confirmation of EVs choice) (See IEC 61980-2) The default value is "External confirmation".
PrimaryDeviceAlignmentCheckMethodList	simpleType: WPT_AlignmentCheckMethodListType refer to Annex A for the type definition	Alignment check method intended to be used by the primary device (confirmation of EVs choice) (See IEC 61980-2) The default value is "PowerCheck".
NaturalOffset	simpleType: xs:unsignedShort	Offset of the center alignment point in mm (in x-direction) which results from the coil design of EV and infrastructure.
VendorSpecificDataContainer	simpleType: WPT_DataContainerType refer to Annex A for the type definition	Optional: Data container for proprietary information.
LF_SystemSetupData	simpleType: WPT_LF_SystemSetupDataType refer to Annex A for the type definition	Optional: Additional data needed to describe a LF positioning system. This information is needed, when LF_TxEV or LF_TxPrimaryDevice is given in the list EVPrimaryDevicePositioningMethodList.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

[V2G20-5004] When the SECC has received a FinePositioningSetupReq with EVProcessing is set to "Ongoing" the lists "PrimaryDeviceFinePositioningMethodList", "PrimaryDevicePairingMethodList", "PrimaryDeviceAlignmentCheckMethodList" shall contain those elements, which represent the technical possibilities of the installation on infrastructure side.

[V2G20-5005] If the lists "PrimaryDeviceFinePositioningMethodList", "PrimaryDevicePairingMethodList", "PrimaryDeviceAlignmentCheckMethodList"

© ISO 2022 – All rights reserved

contain more than one element, the default values shall be part of the list, if the device is a compatibility class A device (See IEC 61980-2 and IEC 61980-3).

[V2G20-5006] When the SECC has received a FinePositioningSetupReq with the EVProcessing set to "Finished", the lists "PrimaryDeviceFinePositioningMethodList", "PrimaryDevicePairingMethodList", "PrimaryDeviceAlignmentCheckMethodList" shall contain only one element which confirm the EV's choice.

NOTE The value of this element does not need to be the default value.

8.3.4.6.3 WPT_FinePositioning

8.3.4.6.3.1 WPT_FinePositioningReq/Res handling

The fine positioning process is started by the EVCC by sending the WPT_FinePositioningSetupReq message. The SECC responds by sending the WPT_FinePositioningSetupRes message.

After this initialization the positioning procedure is continued by looping the WPT_FinePositioningReq/Res message. As long as the vehicle positioning process is not finished the SECC sets the parameter "EVSEProcessing" in the WPT_FinePositioningRes message to "Processing" and the EVCC repeatedly sends the WPT_FinePositioningReq message. The EVCC stops sending WPT_FinePositioningReq when the parameter "EVSEProcessing" in the WPT_FinePositioningRes message is set to "Finished".

8.3.4.6.3.2 WPT_FinePositioningReq

[V2G20-5011] The EVCC and the SECC shall implement the message elements as defined in Figure 74 and Table 70.

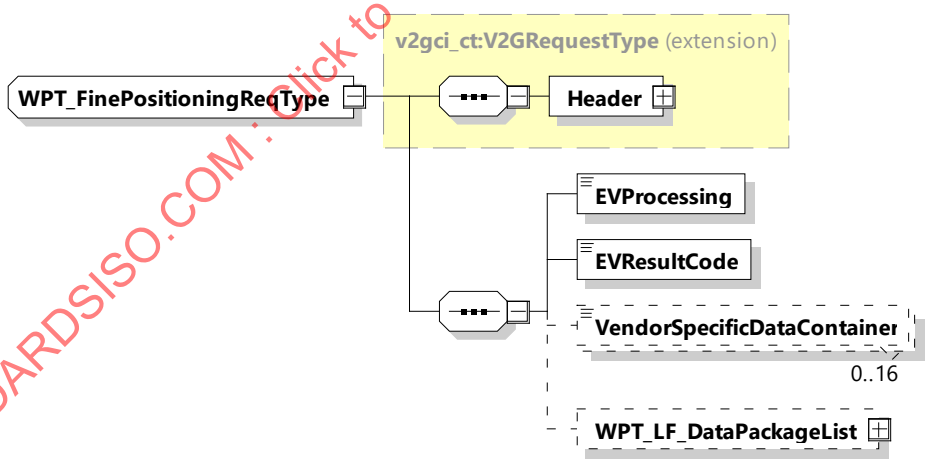


Figure 74 — Schema diagram – WPT_FinePositioningReq

The elements of this message are used according to Table 70.

Table 70 — Semantics and type definition for WPT_FinePositioningReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
EVProcessing	simpleType: processingType enumeration refer to Annex A for the type definition	Parameter that indicates the stop of the Fine positioning process by the EV. When the EV stops the fine positioning process, the EVProcessing is set to "Finished", while still running it is set to "Ongoing".
EVResultCode	simpleType: WPT_EVResultType refer to Annex A for the type definition	Parameter with which the EV can inform the SECC about the result of the fine positioning process: – EVResultUnknown, – EVResultSuccess, – EVResultFailed.
VendorSpecificDataContainer	simpleType: WPT_DataContainerType refer to Annex A for the type definition	Optional: Data container for additional vendor specific information.
WPT_LF_DataPackageList	simpleType: WPT_LF_DataPackageListType refer to Annex A for the type definition	Optional: Used when LF_TxPrimaryDevice of LF_TxEV is chosen as FinePositioning method. The element includes information about received or transmitted LF signal data.

[V2G20-5051] As long as the EVProcessing Element in WPT_FinePositioningReq is "Ongoing" the EVResultCode shall be set to "EVResultUnknown".

[V2G20-5052] If the EVProcessing element in WPT_FinePositioningReq is set to "Finished" the EVResultCode shall not be set to "EVResultUnknown".

8.3.4.6.3.3 WPT_FinePositioningRes

[V2G20-5013] The EVCC and the SECC shall implement the message elements as defined in Figure 75 and Table 71.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

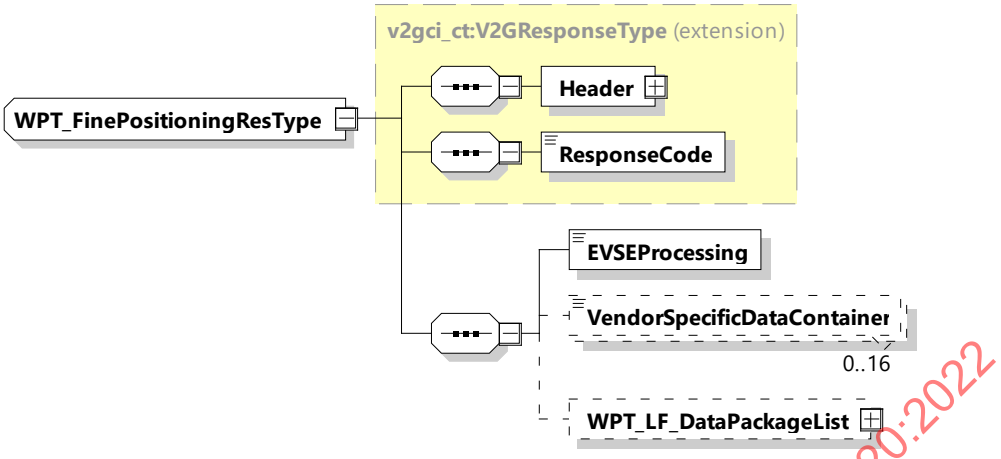


Figure 75 — Schema diagram – WPT_FinePositioningRes

The elements of this message are used according to Table 71.

Table 71 — Semantics and type definition for WPT_FinePositioningRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
EVSEProcessing	simpleType: processingType enumeration refer to Annex A for the type definition	Parameter that indicates the stop of the Fine positioning process by the EV. When the EVSE stops the fine positioning process, the EVSEProcessing is set to "Finished", while still running it is set to "Ongoing".
VendorSpecificDataContainer	simpleType: WPT_DataContainerType, refer to Annex A for the type definition	Optional: Data container for additional vendor specific information.
WPT_LF_DataPackageList	simpleType: WPT_LF_DataPackageListType refer to Annex A for the type definition	Optional: Used when LF_TxPrimaryDevice of LF_TxEV is chosen as FinePositioning method. The element includes information about received or transmitted LF signal data.

8.3.4.6.4 WPT_Pairing

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

The application of pairing for WPT and the sequence of parameter exchange is described in IEC 61980-2. It describes the exchange of parameters between EVCC and SECC for the different possible methods, which are considered in combination with WPT.

After the SDP process, SessionSetup and vehicle positioning have been finished the pairing shall be applied in order to identify the EVSE and the primary device, over which the EV has been positioned.

NOTE The identifier of the EV and the EVSE which are typically determined during pairing might already be exchanged during the SDP process. This, however, does not replace the exchange of the pairing messages together with the pairing process as described in IEC 61980-2.

8.3.4.6.4.1 WPT_PairingReq/Res handling

The EV will start the pairing process by applying the WPT_PairingReq (see 8.3.4.6.4.2). The SECC answers with the WPT_PairingRes (see 8.3.4.6.4.3). The parameters of the messages and their values are used according to the selected pairing method. The selection of the pairing method takes place during WPT_FinePositioningSetup. Refer to IEC 61980-2 for the sequence and application of parameter exchange.

8.3.4.6.4.2 WPT_PairingReq

[V2G20-5100] The EVCC and the SECC shall implement the message elements as defined in Figure 76 and Table 72.

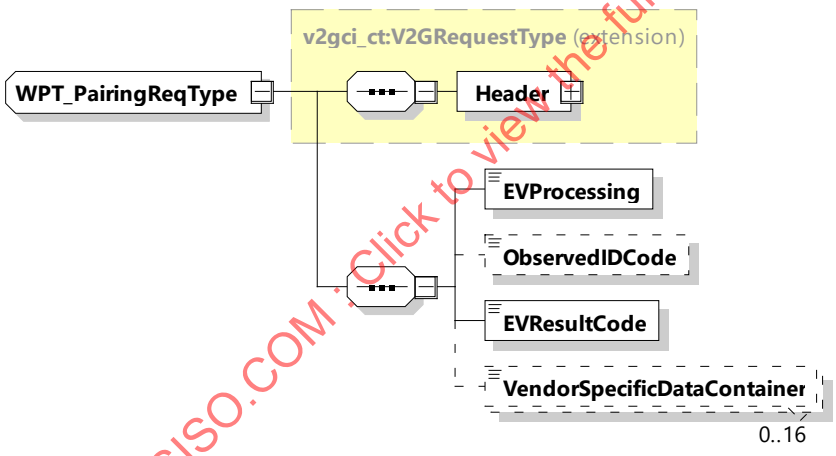


Figure 76 — Schema diagram – WPT_PairingReq

The message elements of this message are used as defined in Table 72.

Table 72 — Semantics and type definition for WPT_PairingReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
EVProcessing	simpleType: processingType enumeration refer to Annex A for the type definition	Parameter that indicates the stop of the Pairing process by the EV. When the EV stops the pairing process, the EVProcessing is set to "Finished", while still running it is set to "Ongoing".

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

ObservedIDCode	simpleType: numericIDType refer to Annex A for the type definition	Optional: The identifier observed by the EV through P2PS signaling according to the pairing method applied. (omitted if not required for the pairing method).
EVResultCode	simpleType: WPT_EVResultType refer to Annex A for the type definition	Parameter with which the EV can inform the SECC about the result of the pairing process: – EVResultUnknown, – EVResultSuccess, – EVResultFailed .
VendorSpecificDataContainer	simpleType: WPT_DataContainerType refer to Annex A for the type definition	Optional: Data container for additional vendor specific information.

8.3.4.6.4.3 WPT_PairingRes

[V2G20-5101] The EVCC and the SECC shall implement the message elements as defined in Figure 77 and Table 73.

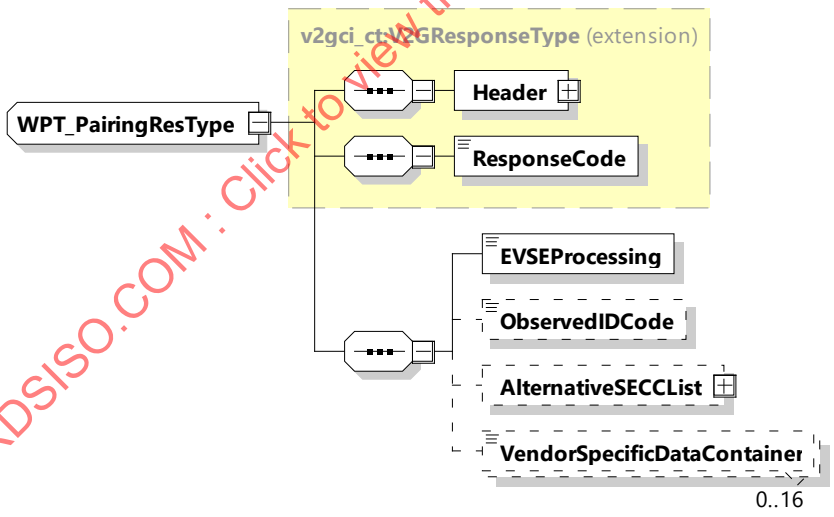


Figure 77 — Schema diagram – WPT_PairingRes

The message elements of this message are used as defined in Table 73.

Table 73 — Semantics and type definition for WPT_PairingRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
EVSEProcessing	simpleType: processingType enumeration refer to Annex A for the type definition	Parameter indicating that the EVSE has finished the processing that was initiated after the WPT_PairingReq or if the EVSE is still processing at the time, the response message was sent.
ObservedIDCode	simpleType: numericIDType refer to Annex A for the type definition	Optional: The identifier observed by the supply device through P2PS signaling according to the pairing method applied (omitted if not required for the pairing method).
AlternativeSECCList	complexType: AlternativeSECCListType refer to 8.3.5.6.1	Optional: List of connection information to alternative SECCs in the order of highest probability in case the pairing failed.
VendorSpecificDataContainer	simpleType: WPT_DataContainerType refer to Annex A for the type definition	Optional: Data container for additional vendor specific information.

8.3.4.6.4.4 General WPT_Pairing Requirements

[V2G20-5007] Both EVCC and SECC shall support the set of WPT pairing messages as described in 8.3.4.6.4, which are required to process the WPT pairing.

8.3.4.6.4.4.1 Requirements for EVCC

[V2G20-5008] To start the pairing process the EVCC shall send a WPT_PairingReq message.

[V2G20-5012] If the EVCC has identified a pairing code it shall send a WPT_PairingReq message with the parameter ObservedIDCode set to the pairing identification code and the EVProcessing parameter set to "Finished".

[V2G20-5049] As long as the EVProcessing Element in WPT_PairingReq is "Ongoing" the EVResultCode shall be set to "EVResultUnknown".

[V2G20-5050] If the EVProcessing element in WPT_PairingReq is set to "Finished" the EVResultCode shall not be set to "EVResultUnknown".

8.3.4.6.4.4.2 Requirements for SECC

[V2G20-5016] If the SECC has received the WPT_PairingReq message with the parameter ObservedIDCode set to a pairing identification code and the validation of the

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

identifier used for pairing fails it shall respond with a WPT_PairingRes message with the parameter ResponseCode equal to FAILED or WARNING_WPT.

NOTE 1 It is up to the implementation whether to give a response code FAILED or WARNING_WPT. In case of FAILED, the communication is terminated. In case of WARNING_WPT, the system allows to repeat the positioning and pairing procedure.

[V2G20-5065] If the SECC has received the WPT_PairingReq message with the parameter EVResultCode set to "EVResultFailed", then the SECC shall respond with a WPT_PairingRes message with the parameter ResponseCode equal to FAILED or WARNING_WPT.

[V2G20-5017] If the SECC has received the WPT_PairingReq message with the parameter ObservedIDCode set to a pairing identification code and the validation of the ObservedIDCode succeeds it shall respond with a WPT_PairingRes message with the parameter ResponseCode equal to "OK".

[V2G20-5018] If the SECC has identified a pairing code it shall respond to a WPT_PairingReq with a WPT_PairingRes message with the parameter ObservedIDCode set to the pairing identification code and the EVSEProcessing parameter set to "Finished".

[V2G20-5053] If [V2G20-5016] applies or the EVCC sent a WPT_PairingReq with the parameter EVResultCode set to "EVResultFailed", then the SECC should include AlternativeSECCList parameter in the PairingRes message when such information is available.

NOTE 2 The AlternativeSECCList provides a list of SECCs that the EVCC is recommended to connect to, in the order of priority, when the pairing process with the current SECC fails. Given the list, the EVCC can connect to those SECCs in the given order. For example, the EVCC connects to the wireless network with the provided SSID and start SDP protocol, or connect to the SECC by provided IP address and port number directly. How the list of alternative SECCs is obtained by the current SECC is not in the scope of this document.

8.3.4.6.5 WPT_ChargeParameterDiscoveryReq/Res

The WPT_ChargeParameterDiscoveryReq and WPT_ChargeParameterDiscoveryRes messages are used to exchange information about the technical characteristics of the power transfer devices in order to tune the system components accordingly.

By exchanging this information the final compatibility check of EV device and the supply device is performed (see IEC 61980-2).

8.3.4.6.5.1 WPT_ChargeParameterDiscoveryReq/Res handling

After being authorized for charging at the EVSE (SECC) the EVCC and the SECC negotiate the energy transfer parameters with the WPT_ChargeParameterDiscovery message pair.

Concepts treated for an optimal supply of energy that corresponds to the customer needs below.

When using scheduled control mode, the energy transfer parameters negotiation that precedes the delivery of energy or may be engaged during the energy delivery phase is destined to ensure that the user will be satisfied while at the same time ensuring that the energy will effectively be available and fall within the capacity of power supply grid at the local level (private network) and at the regional level (public network). This required negotiation will become more and more necessary as the number of EVs increase, as well as an increase in volatility of local renewable energy production.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

When using the dynamic control mode, the energy transfer parameters can be changed dynamically while in the Charging Loop, depending on the need of the EVSE.

8.3.4.6.5.2 WPT_ChargeParameterDiscoveryReq

By sending the WPT_ChargeParameterDiscoveryReq message the EVCC provides its energy transfer parameters to the SECC. This message provides status information about the EV, i.e. the capabilities of the EV charging system.

[V2G20-5019] The EVCC shall send the WPT_ChargeParameterDiscoveryReq message with the elements of the message set according to the technical characteristics of the EV device.

[V2G20-5128] The EVCC and the SECC shall implement the message elements as defined in Figure 78 and Table 74.

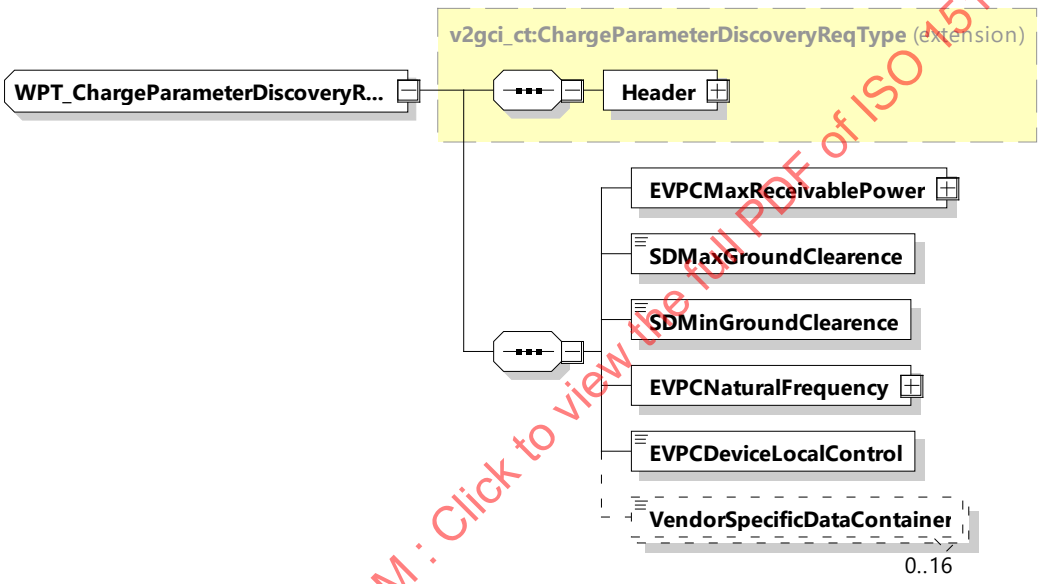


Figure 78 — Schema diagram – WPT_ChargeParameterDiscoveryReq

The elements of this message are used according to Table 74.

Table 74 — Semantics and type definition for WPT_ChargeParameterDiscoveryReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
EVPCMaxReceivablePower	complexType RationalNumberType refer to 8.3.5.3.8	Maximum power in watts which EVPC can receive
SDMaxGroundClearence	simpleType: xs:unsignedShort	Maximum value of secondary device ground clearance in mm
SDMinGroundClearence	simpleType: xs:unsignedShort	Minimum value of secondary device ground clearance in mm

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
EVPCNaturalFrequency	complexType RationalNumberType refer to 8.3.5.3.8	Self-resonance frequency of the EV device under fully loaded condition (primary device not present)
EVPCDeviceLocalControl	simpleType: xs:boolean	True, if EV device has a local control loop, which modifies reactance or power, false otherwise.
VendorSpecificDataContainer	simpleType: WPT_DataContainerType refer to Annex A for the type definition	Optional: Manufacturer specific data container, containing, e.g. manufacturer ID and Model ID

NOTE The parameters related to current, power and voltage provided in WPT_ChargeParameterDiscovery message pair can be considered as physical limitations, meaning that they are related to the physical abilities of the system under rated operating conditions. Later during the charging process, depending on the external and environmental conditions (SOC, temperatures, etc.), the values of these limitations can change into more conservative values.

8.3.4.6.5.3 WPT_ChargeParameterDiscoveryRes

With the WPT_ChargeParameterDiscoveryRes message the SECC provides applicable charge parameters from the grid's perspective.

[V2G20-5021] The SECC shall respond with a WPT_ChargeParameterDiscoveryRes with the ResponseCode = OK when the element values received from the EVCC allow a system setup for successful power transfer at the supply device.

[V2G20-5022] The SECC shall respond with a WPT_ChargeParameterDiscoveryRes with the ResponseCode = FAILED when the element values received from the EVCC do not allow a system setup for any power transfer at the supply device.

[V2G20-5066] The SECC shall respond with a WPT_ChargeParameterDiscoveryRes with the ResponseCode = WARNING_WPT when the element values received from the EVCC only allow a system setup for limited (significantly lower) power transfer at the supply device.

NOTE It is up to the implementation of the SECC when to response with WARNING_WPT or FAILED based on the system behavior.

[V2G20-5127] The EVCC and the SECC shall implement the message elements as defined in Figure 79 and Table 75.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

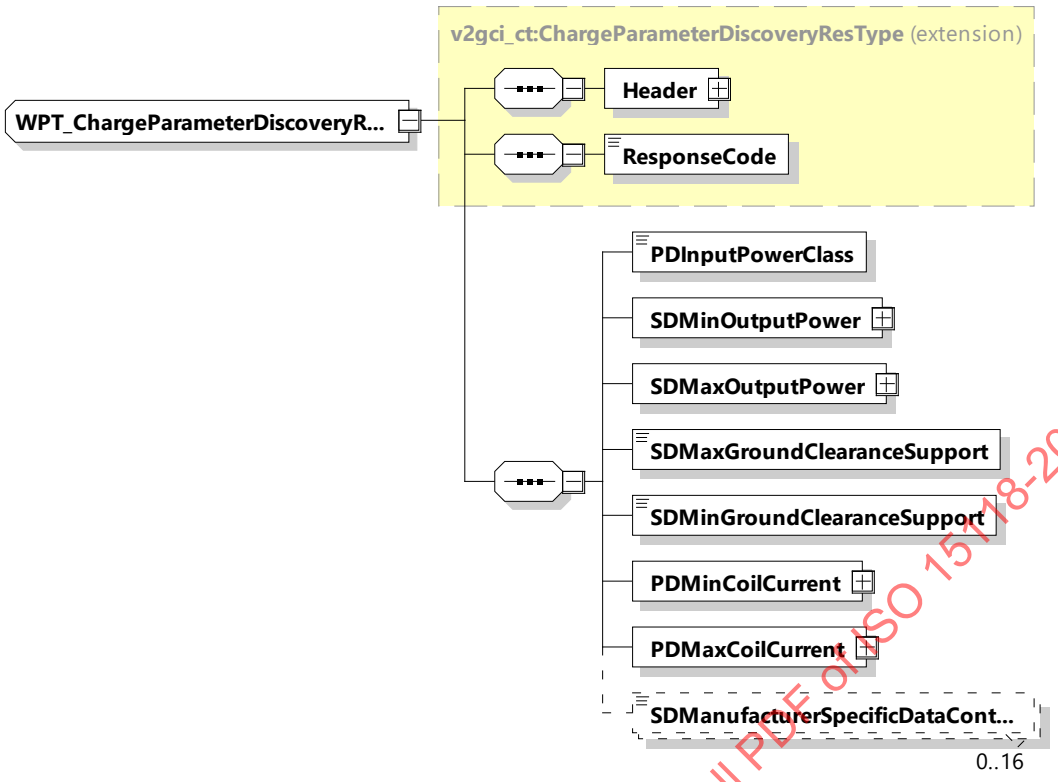


Figure 79 — Schema diagram – WPT_ChargeParameterDiscoveryRes

The elements of this message are used according to Table 75.

Table 75 — Semantics and type definition for WPT_ChargeParameterDiscoveryRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
PDInputPowerClass	simpleType: WPT_PowerClassType refer to Annex A for the type definition	Power class supported by the primary device. Possible values for MF-WPT input power classes are: MF-WPT1, MF-WPT2, MF-WPT3 and MF-WPT4 according to IEC TS 61980-3
SDMinOutputPower	complexType: RationalNumberType refer to 8.3.5.3.8	Minimum power in watts drawn by the secondary device
SDMaxOutputPower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum power in watts drawn by the secondary device

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
SDMaxGroundClearanceSupport	simpleType: xs:unsignedShort	Maximum value of supported secondary device ground clearance in mm
SDMinGroundClearanceSupport	simpleType: xs:unsignedShort	Minimum value of the secondary device ground clearance in mm
PDMinCoilCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Minimum current through the primary coil, which can be controlled by the primary device
PDMaxCoilCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum current through the primary coil, which can be controlled by the primary device
SDManufacturerSpecificDataContainer	simpleType: WPT_DataContainerType refer to Annex A for the type definition	Optional: Manufacturer specific data container, containing, e.g. manufacturer ID and Model ID

8.3.4.6.6 WPT_AlignmentCheckReq/Res

The WPT_AlignmentCheckReq/Res messages are used to exchange information needed to perform the alignment check, with which the proper position of the EV device with the primary device is checked and confirmed (See IEC 61980-2).

8.3.4.6.6.1 WPT_AlignmentCheckReq/Res handling

8.3.4.6.6.2 WPT_AlignmentCheckReq

[V2G20-5015] The EVCC and the SECC shall implement the message elements as defined in Figure 80 and Table 76.

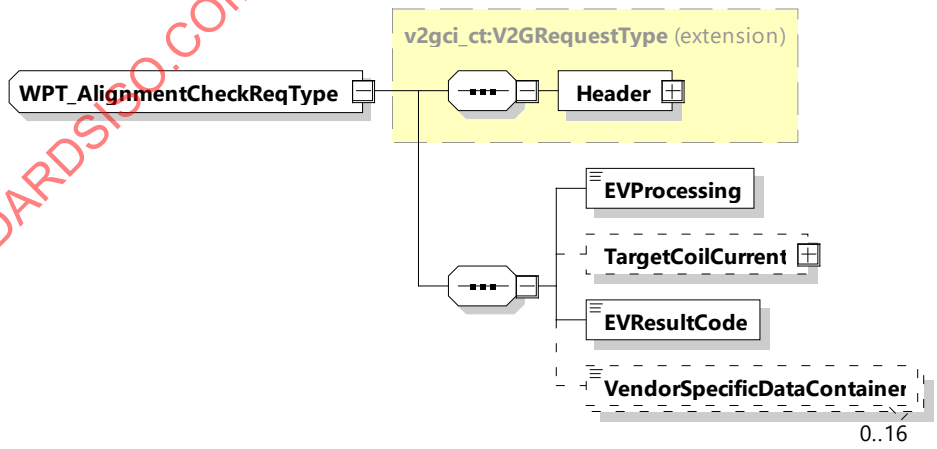


Figure 80 — Schema diagram – WPT_AlignmentCheckReq

The elements of this message are used according to Table 76.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 76 — Semantics and type definition for WPT_AlignmentCheckReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
EVProcessing	simpleType: processingType enumeration refer to Annex A for the type definition	Parameter that indicates the stop of the alignment check process by the EV. When the EV stops the pairing process, the EVProcessing is set to "Finished", while still running it is set to "Ongoing".
TargetCoilCurrent	complexType RationalNumberType refer to 8.3.5.3.8	Optional: Used for Power check and LPE: – Current in amperes, the EVSE shall feed the primary coil with in order to enable the secondary device to perform the alignment check.
EVResultCode	simpleType: WPT_EVResultType refer to Annex A for the type definition	Parameter with which the EV can inform the SECC about the result of the alignment check: – EVResultUnknown, – EVResultSuccess, – EVResultFailed.
VendorSpecificDataContainer	simpleType: WPT_DataContainerType refer to Annex A for the type definition	Optional: Data container for additional vendor specific information. This element is used primarily when a proprietary alignment check method was selected with the FinePositioningSetup.

[V2G20-5047] As long as the EVProcessing Element in WPT_AlignmentCheckReq is "Ongoing" the EVResultCode shall be set to "EVResultUnknown".

[V2G20-5048] If the EVProcessing element in WPT_AlignmentCheckReq is set to "Finished" the EVResultCode shall not be set to "EVResultUnknown".

8.3.4.6.6.3 WPT_AlignmentCheckRes

[V2G20-5014] The EVCC and the SECC shall implement the message elements as defined in Figure 81 and Table 77.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

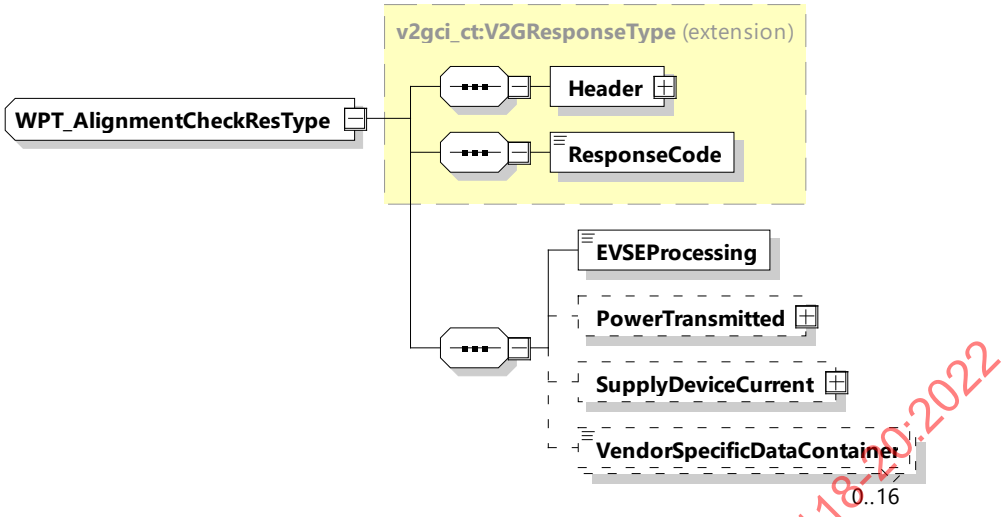


Figure 81 — Schema diagram – WPT_AlignmentCheckRes

The elements of this message are used according to Table 77.

Table 77 — Semantics and type definition for WPT_AlignmentCheckRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
EVSEProcessing	simpleType: processingType refer to Annex A for the type definition	Parameter indicating that the EVSE has finished the processing that was initiated after the WPT_AlignmentCheckReq or if the EVSE is still processing at the time, the response message was sent.
PowerTransmitted	complexType RationalNumberType refer to 8.3.5.3.8	Optional: The amount of power in watts transmitted by the supply device
SupplyDeviceCurrent	complexType RationalNumberType refer to 8.3.5.3.8	Optional: The amount of current in amperes into the supply device coil
VendorSpecificDataContainer	simpleType: WPT_DataContainerType refer to Annex A for the type definition	Optional: Data container for additional vendor specific information. This element is used primarily when a proprietary alignment check method was selected with the FinePositioningSetup

8.3.4.6.7 WPT_ChargeLoopReq/Res

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

For WPT periodic exchange of process control data is requested from EV side, see IEC 61980-2.

8.3.4.6.7.1 WPT_ChargeLoopReq/Res handling

The WPT_ChargeLoopReq/Res messages are used for the periodic exchange of process control data. The messages are derived from the ChargeLoopReq/Res messages defined in the common module (see ChargeLoopReqType) and extended by the parameters necessary for the handling of wireless power transfer according to IEC 61980-2.

8.3.4.6.7.2 WPT_ChargeLoopReq

By sending the WPT_ChargeLoopReq the EV requests a certain power from the EVSE.

[V2G20-1296] The EVCC and the SECC shall implement the message elements as defined Table 78 and Figure 82.

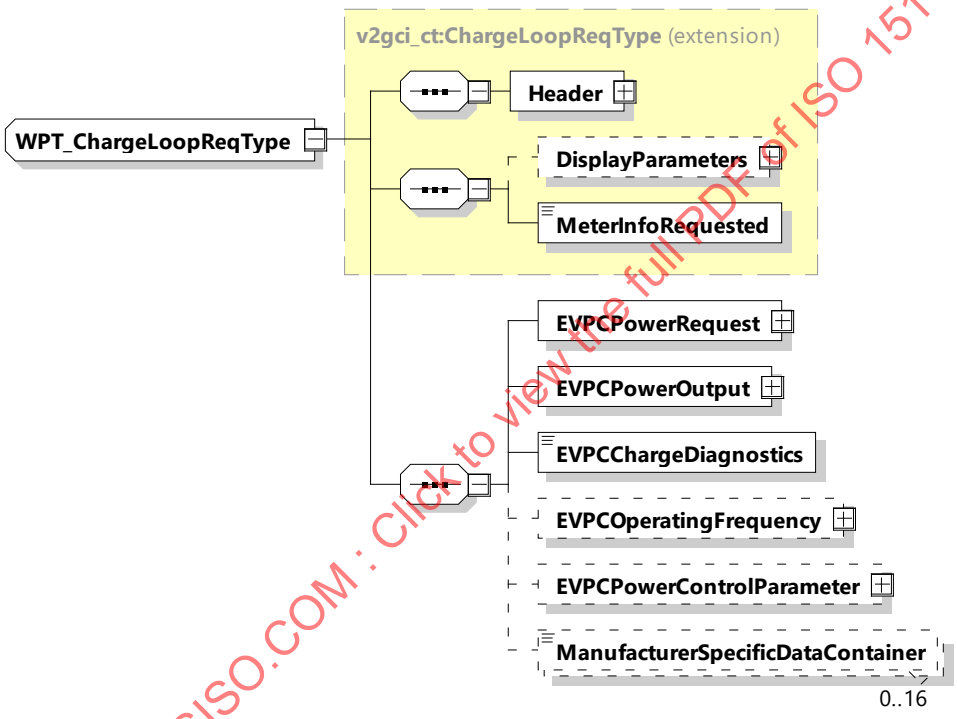


Figure 82 — Schema diagram – WPT_ChargeLoopReq

The elements of this message are used according to Table 78.

Table 78 — Semantics and type definition for WPT_ChargeLoopReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
EVPCPowerRequest	complexType RationalNumberType refer to 8.3.5.3.8	Power the EVPC would like to have as output in Watt. Note that setting this value to zero is valid.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
EVPCPowerOutput	complexType RationalNumberType refer to 8.3.5.3.8	Power measured at the output of the EVPC electronics in Watt
EVPCChargeDiagnostics	simpleType: WPT_ChargeDiagnosticsType refer to Annex A for the type definition	Diagnostics information, can have the following values: – EVPCNoIssue: no anomaly detected, Power Control is running normally; – EVPCTempOverheatDetected: EVPC has detected a temperature anomaly; – EVPCPowerTransferAnomalyDetected: EVPC has detected an unexpected behavior of the magnetic power transfer; – EVPCAnomalyDetected: EVPC has detected an unexpected system behavior.
EVPCOperatingFrequency	complexType RationalNumberType refer to 8.3.5.3.8	Optional: EVPC measured MF-WPT operating frequency
EVPCPowerControlParameter	simpleType: WPT_EVPCPowerControlParameterType refer to Annex A for the type definition	Optional: additional parameters for the applied wireless power transfer method: – EVPC coil current request: EVPC wants the primary device to set a specific (preferred) coil current value. NOTE The EVPCPowerRequest is overriding the value given here in case of mismatch: – EVPC coil current information: information about secondary device coil current (AC); – EVPC current output information: information about DC current supplied to the EV; – EVPC voltage output information: information about DC bus or battery voltage.
ManufacturerSpecificDataContainer	simpleType: WPT_DataContainerType refer to Annex A for the type definition	Optional: Manufacturer specific parameters: additional field for proprietary manufacturer specific information during power transfer

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

8.3.4.6.7.3 WPT_ChargeLoopRes

After receiving the WPT_ChargeLoopReq from the EVCC the SECC sends the WPT_ChargeLoopRes informing the EV about the EVSE status.

© ISO 2022 – All rights reserved

[V2G20-5028] The EVCC and the SECC shall implement the message elements as defined in Table 79 and Figure 83.

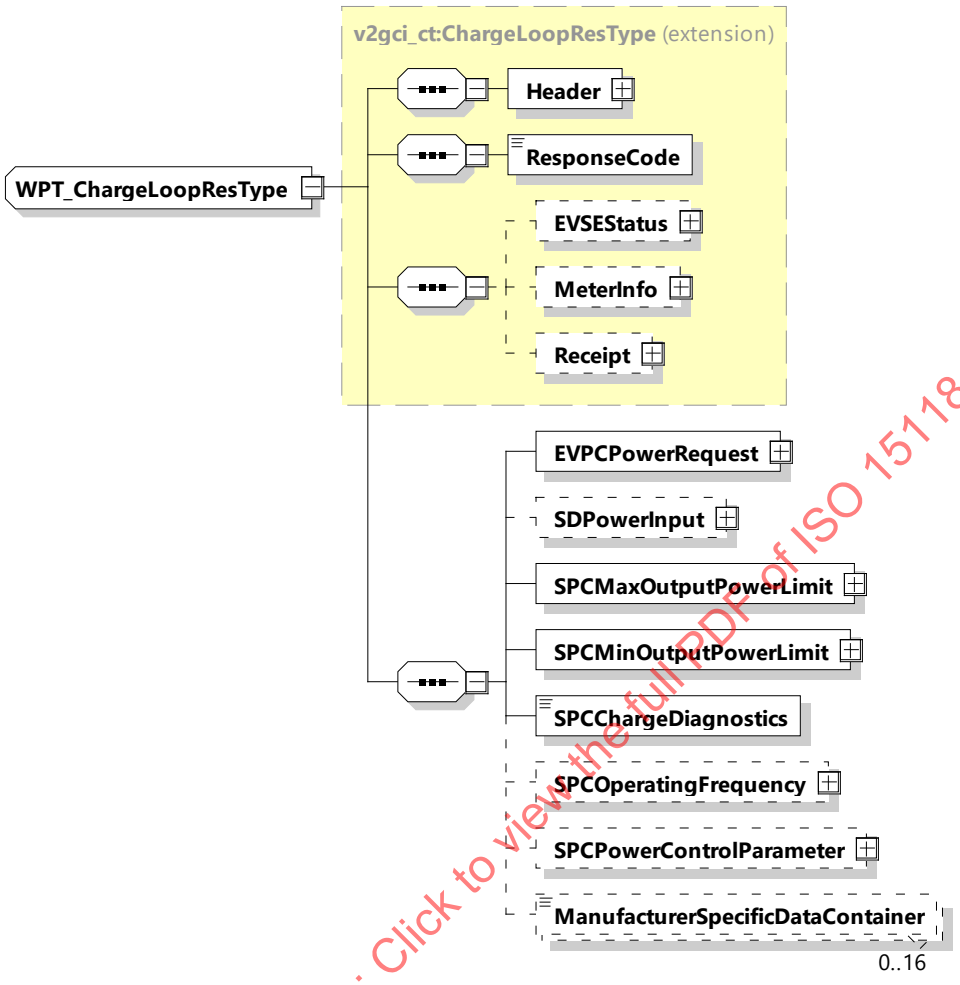


Figure 83 — Schema diagram – WPT_ChargeLoopRes

The elements of this message are used according to Table 79.

Table 79 — Semantics and type definition for WPT_ChargeLoopRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
EVPCPowerRequest	complexType RationalNumberType refer to 8.3.5.3.8	Power value which was requested by the EVCC
SDPowerInput	complexType RationalNumberType refer to 8.3.5.3.8	Optional: DC power consumed from the MF-WPT system input by the supply device in Watt. The EVCC compares the value with the received EVPCPowerOutput in order to detect possible misbehavior. This value is for information only without any impact on safety relative actions.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
SPCMaxOutputPowerLimit	complexType RationalNumberType refer to 8.3.5.3.8	Time varying maximum transmittable power of the supply power circuit given in Watt. The EVCC should not request more than this amount of power
SPCMinOutputPowerLimit	complexType RationalNumberType refer to 8.3.5.3.8	Time varying minimum transmittable power of the supply power circuit given in Watt. The EVCC should not request less than this amount of power, unless it will request 0 watts.
SPCChargeDiagnostics	simpleType: WPT_SPCChargeDiagnosticsType refer to Annex A for the type definition	Diagnostics information, can have the following values: – NoIssue – FODDetected – LOPDetected – SPCTempOverheatDetected – SPCPowerTransferAnomalyDetected – SPCAnomalyDetected
SPCOperatingFrequency	complexType RationalNumberType refer to 8.3.5.3.8	Optional: SPC actual MF-WPT operating frequency in Hz
SPCPowerControlParameter	simpleType: WPT_SPCPowerControlParameterType refer to Annex A for the type definition	Optional: Additional parameters for the applied wireless power transfer method: Primary device coil current information
ManufacturerSpecificDataContainer	simpleType: WPT_DataContainerType refer to Annex A for the type definition	Optional: Manufacturer specific parameters: additional field for proprietary manufacturer specific information during power transfer (vendor specific information)

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

8.3.4.7 ACDP messages

8.3.4.7.1 Introduction and scope

The scope of the following subclause relates to ACDP for infrastructure mounted pantograph used for high power charging of electric busses or other commercial vehicles:

- ACDP with infrastructure mounted pantograph as specified in EN 50696:2021, A.2 and A.3;
- WLAN communication according to this document;
- WLAN communication layer according to ISO 15118-8;
- Electrical safety according to IEC 61851-23-1.

8.3.4.7.2 Overview

The following clause describes the requirements for the WLAN based communication for an infrastructure mounted ACDP according to EN 50696:2021, Annex A using direct current.

© ISO 2022 – All rights reserved

The wireless communication for ACDP with infrastructure mounted pantograph requires early association of the EVCC with the associated SECC before the V2G communication can be started. This is needed to be able to control the EV positioning and ACDP activation processes correctly. For this the early association provides the required information as the EVID and EV position information.

For ACDP the multi SECC communication architecture according Figure 29 applies for multiple SECC architecture as described in 7.10.1.2.2.

For ACDP a pairing and positioning device (PPD) mounted on the infrastructure applies as described in EN 50696:2021, A.2 and A.3.

NOTE 1 An architecture using a single AP with single SECC, and single PPD can be viewed as a special version of the Multiple SECC architecture and is therefore also a permitted communication architecture.

NOTE 2 For ACDP mounted pantograph on the infrastructure the pairing and positioning device can be located on the infrastructure side. The identification object which holds the EVID is located on the EVs ACDP counterpart side. In this case the PPD can be able to read an identification mark positioned on or in the EV. The PPD identification method is used to ensure that the EV's EVID is detected only in close proximity of the EV to the EVSE so crosstalk to another EV is not possible (Partitioning). RFID identification tags are recommended to be present on the EV to ensure a basic level of interoperability. These tags are specified in Annex E.2.

NOTE 3 The EVID can be any unique identifier number or string. For electric bus applications it can comprise a readable name or, e.g. the EV number plate. For any other application it can be any random number which is unique at that time, thus privacy is not concerned.

The ACDP V2G communication consists of the following messages:

- common messages;
- DC messages;
- ACDP specific messages.

8.3.4.7.2.1 ACDP terminology

There are three distinct roles for the pairing and positioning device:

Pairing

The EV connects to the right supply equipment communication controller (SECC) using the wireless SDP protocol in installations where there are several ACDP EVSEs in close proximity. This is a required role.

Partitioning

The area around the ACDP is partitioned into a properly sized acceptancezone, outside which a charging session cannot be started. The zone should not be so small as to restrict the positioning leeway, but small enough that a nearby EV cannot inadvertently start a session and lower the ACDP such that a dangerous situation as a collision between the ACDP and another EV can occur. This is a required role for safety.

Positioning

The driver can position the bus with enough precision that the ACDP contacts will connect with the ACDP counterpart contacts on the EV correctly so that correct charging is assured. This is an optional role for operational efficiency.

The pairing and positioning device provides a spatial selective orthogonal communication channel to the WLAN communication when the EV is in close proximity to the ACDP in order to resolve the undetermined association of the EV communication to the ACDP's EVSE. The PPD consists of a marker located on the EV and a receiver located in the ACDP infrastructure.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

A recommended, basic RFID PPD system with sufficient positional accuracy for Partitioning is defined in E.2.1.3.

8.3.4.7.3 ACDP message overview

ACDP with infrastructure mounted pantograph will use the common message set, the DC V2G message set and will have ACDP specific messages to handle the status information, the EV positioning process and the ACDP control. Table 80 provides an overview of the ACDP communication messages.

Table 80 — ACDP message communication overview

Message/Action	Abbr	Com	DC	ACDP	Msg Looped	Next message(s) on success	Exception handling on app level failure	Exception handling on msg timeout
SupportedAppProtocol	SAP	x			N	SSU	SDP-Restart	SDP-Restart
SessionSetup	SSU	x			N	APOS	SDP-Sestart	SDP-Restart
ACDP_VehiclePositioning	APOS			x	Y	APOS, ASUP	SSP	SDP-Restart
AuthorizationSetup	ASUP	x			N	AUTH, CINS	SSP	SDP-Restart
Authorization	AUTH	x			Y	AUTH, SDI	SSP	SDP-Restart
CertificateInstallation	CINS	x			Y	CINS, AUTH	SSP	SDP-Restart
ServiceDiscovery	SDI	x			N	SDE	SSP	SDP-Restart
ServiceDetail	SDE	x			N	SSEL	SSP	SDP-Restart
ServiceSelection	SSEL	x			N	CPDA	SSP	SDP-Restart
DC_ChargeParameter Discovery	CPDA		x		N	SE	SSP	SDP-Restart
ScheduleExchange	SE	x			Y	SE, CONA	SSP	SDP-Restart
ACDP_Connect	CONA			x	Y	CONA, CC	DISA	ESDW
DC_CableCheck	CC		x		Y	CC, PC	DISA	ESDW
DC_PreCharge	PC		x		N	PD(Start)	DISA	ESDW
PowerDelivery(Start)	PD(Start)		x		N	DCCL	DISA	ESDW
DC_ChargeLoop	DCCL		x		Y	DCCL, MCON, PD(Stop)	PD(Stop)	ESDW
PowerDelivery(Stop)	PD(Stop)		x		N	DISA	DISA	ESDW
ACDP_Disconnect	DISA			x	Y	DISA, SSP	ESDW	ESDW

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Message/Action	Abbr	Com	DC	ACDP	Msg Looped	Next message(s) on success	Exception handling on app level failure	Exception handling on msg timeout
SessionStop	SSP	x			N	SSP	SDP-Restart	ESDW
Wait for new session						SDP-Restart	SDP-Restart	
Multiplexed communication								
MeteringConfirmation	MCON		x		N	MCON		ESDW
ACDP_SystemStatus	SYSS			x	Y	SYSS		SDP-Restart

NOTE 1 Emergency shut down (ESDW) according to IEC 61851-23:2014, Annex CC.5 and wait for change of control pilot to State A.

NOTE 2 ACDP_SystemStatus has a separate payload type, see Table 14.

8.3.4.7.4 SDP parameters for ACDP

For ACDP use case the SDP client needs to select the appropriate configuration compliant with the following requirement:

[V2G20-4003] For ACDP an SDP client shall send the SDP request message with the elements "PPD/P2PS" (Bit 0) set to 1 and "Coupling Type" (Bit 0/1) set to 1 accordingly.

8.3.4.7.5 ACDP_VehiclePositioning

8.3.4.7.5.1 ACDP_VehiclePositioningReq/Res handling

During the EV approaching process the ACDP_VehiclePositioningReq/Res messages may be used to guide the EV to the ACDP infrastructure charging area with defined x and y tolerances of the contact interface according to EN 50696.

The definition of the coordinate system for ACDP for infrastructure mounted pantograph is based on ISO 4130:1978, Annex D.

For ACDP the actual position of the EV contact interface in relation to the ACDP contact interface is determined by the pairing and positioning device.

The position information provided during the EV approaching process as well as the effective tolerance dimensions can be communicated via the ACDP_VehiclePositioningRes message. This information may be forwarded to the EV driver as guiding information.

There are three cases for positioning support between EV and EVSE. Either both the EV and the EVSE support positioning support, the EV does not, or the EV does and the EVSE does not. The sequence is slightly different in these three cases.

Case 1: Positioning support from both sides. The EVCC will start sending ACDP_VehiclePositioningReq with EVPositioningSupport=True, and EVMobilityStatus=Mobilized since it is asking the SECC to help it position the EV. The SECC will reply ACDP_VehiclePositioningRes with EVSEPositioningSupport=True and EVSEProcessing=Ongoing and provide positioning information to assist the EV in moving to the correct charging position. When the EVCC receives this information,

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

it can decide whether it is sufficiently in position to initiate charging or send another ACDP_VehiclePositioningReq. This looping continues until the EVCC decides that it is in position and is also immobilized. Then, it will then send a ACDP_VehiclePositioningReq with EVMobilityStatus=Immobilized. The SECC will reply with a ACDP_VehiclePositioningRes with EVSEProcessing=Finished and the sequence will continue with AuthorizationSetupReq.

Case 2: the EVCC does not support SECC supported positioning. The EVCC will send ACDP_VehiclePositioningReq with EVPositioningSupport=False, and EVMobilityStatus=Mobilized. The SECC will reply with ACDP_VehiclePositioningRes with EVSEPositioningSupport=False/True (do not care) and EVSEProcessing=Ongoing. When the EVCC receives this information, the EV can decide whether it is sufficiently in position (using other means, such as the driver using visual aids to park, or advanced EV sensors) to stop the positioning process, or to send another ACDP_VehiclePositioningReq in a loop. This looping continues until the EV decides that the EV is in position, and is also immobilized. Then it will then send a ACDP_VehiclePositioningReq with EVMobilityStatus=Immobilized. The SECC will reply with a ACDP_VehiclePositioningRes with EVSEProcessing=Finished, and the sequence will continue with AuthorizationSetupReq.

Case 3: the EVCC supports positioning, but the SECC does not. In this case, the EVCC will send ACDP_VehiclePositioningReq with EVPositioningSupport=True, and EVMobilityStatus=Mobilized. The SECC will reply ACDP_VehiclePositioningRes with EVSEPositioningSupport=False and EVSEProcessing=Ongoing. At this point, the EVCC may allow for manual positioning of the EV as described in the second case. If the EVCC decides that it requires SECC positioning support, it may stop the charging process by sending SessionStop.

In all cases where there is an ongoing positioning loop, the SECC monitors its PPD to verify that pairing is still correct. If the EV moves out of the pairing zone, then the SECC will send ACDP_VehiclePositioningRes with ResponseCode=FAILED_AssociationError, the EVCC will send SessionStop and the SDP process will restart.

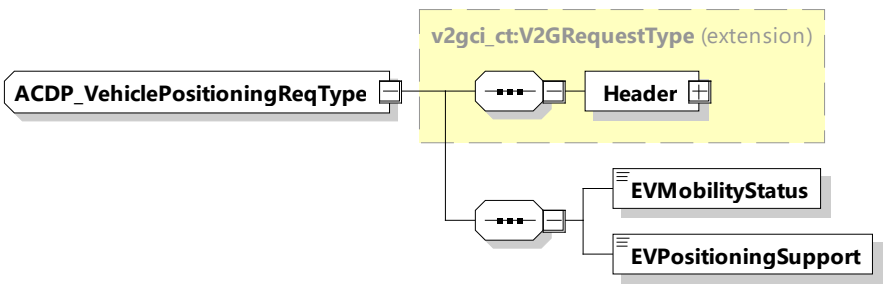
NOTE 1 If the EV already knows it is in position and is also immobilized, then no loop is required, and the EVCC can directly send a ACDP_VehiclePositioningReq with EVMobilityStatus=Immobilized. The SECC will then reply with a ACDP_VehiclePositioningRes with EVSEProcessing=Finished, and the sequence will continue with AuthorizationSetupReq.

NOTE 2 Positioning support with the RFID PPD is very basic. The only information that is returned by the SECC is EV_InChargePosition = True/False. This information indicates that the EV is within/not within the partition zone for charging.

NOTE 3 It is possible that more than one PPD technology is available. For example, the EV and EVSE have both the Basic RFID PPD as well as an advanced optical PPD. Since the active part of the PPD is always on the EVSE, the EVSE can determine the presence of the advanced optical PPD during the SDP pairing for WLAN process and continue using this during the positioning process.

8.3.4.7.5.2 ACDP_VehiclePositioningReq

[V2G20-4004] The EVCC and the SECC shall implement the message elements as defined in Figure 84 and Table 81.



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Figure 84— Schema diagram ACDP_VehiclePositioningReq

The elements of this message are used according to Table 81.

Table 81 — Semantics and type definition for ACDP_VehiclePositioningReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType Refer to 8.3.3	Contains general information, used for all messages.
EVMobilityStatus	simpleType: xs:boolean	– EV is mobilized = 0 – EV is immobilized = 1
EVPositioningSupport	simpleType: xs:boolean	Indicates whether positioning is supported by the EV. – No EV Position Support = 0 – EV Position Support = 1

8.3.4.7.5.3 ACDP_VehiclePositioningRes

[V2G20-4005] The EVCC and the SECC shall implement the message elements as defined in Figure 85 and Table 82.

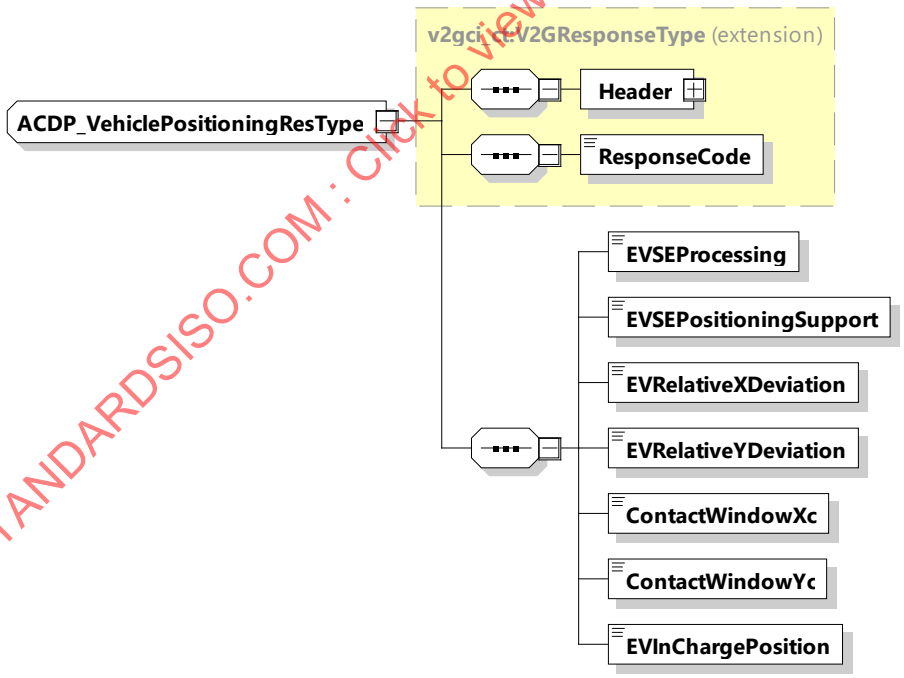


Figure 85— Schema diagram ACDP_VehiclePositioningRes

The elements of this message are used according to Table 82.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 82 — Semantics and type definition for ACDP_VehiclePositioningRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
EVSEProcessing	simpleType: processingType refer to Annex A for the type definition	Parameter indicating that the EVSE has finished the processing that was initiated after the ACDP_VehiclePositioningReq or that the EVSE is still processing at the time, the response message was sent.
EVSEPositioningSupport	simpleType: xs:boolean	Indicates whether positioning is supported by the EVSE.
EVRelativeXDeviation	simpleType: xs:short	Option in case of positioning supported: EV relative ACDP X (counter longitudinal driving direction) deviation in mm.
EVRelativeYDeviation	simpleType: xs:short	Option in case of positioning supported: EV relative ACDP Y (lateral) deviation in mm.
ContactWindowXc	simpleType: xs:short	Option in case of positioning supported: Is used to provide driver information about usable contact position. ContactWindow_Xc defines half of the useable ACDP contact area in driving direction in mm for consideration of a tolerance margin.
ContactWindowYc	simpleType: xs:short	Option in case of positioning supported: Is used to provide driver information about usable contact position. ContactWindow_Yc defines half of the useable contact area lateral to the driving direction in mm for consideration of a tolerance margin.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
EVInChargePosition	simpleType: xs:boolean	Option in case of positioning supported: Indicates whether the EV is positioned within allowed tolerances to ACDP. States: • EVNotInChargePosition = 0 • EVInChargePosition = 1

8.3.4.7.6 ACDP_ConnectReq/Res

8.3.4.7.6.1 ACDP_ConnectReq/Res handling

This message pattern is used to initiate the connecting process of the ACDP.

8.3.4.7.6.2 ACDP_ConnectReq

[V2G20-4006] The EVCC and the SECC shall implement the message elements as defined in Figure 86 and Table 83.

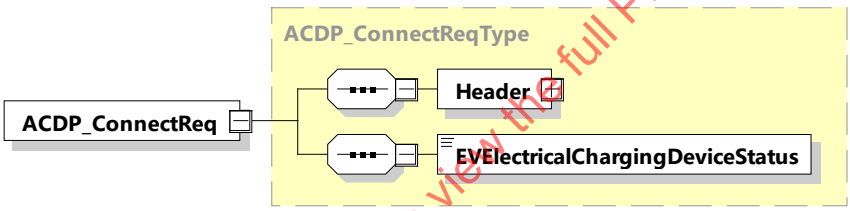


Figure 86 — Schema diagram – ACDP_ConnectReq

The elements of this message are used according to Table 83.

Table 83 — Semantics and type definition for ACDP_ConnectReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
EVElectricalChargingDeviceStatus	simpleType: electricalChargingDeviceStatusType refer to Annex A for the type definition	This element provides the information if the conductive connection between the EV and EVSE is in state "connected" (CP State = B, C or D) or "disconnected" (CP State = A).

8.3.4.7.6.3 ACDP_ConnectRes

[V2G20-4007] The EVCC and the SECC shall implement the message elements as defined in Figure 87 and Table 84.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

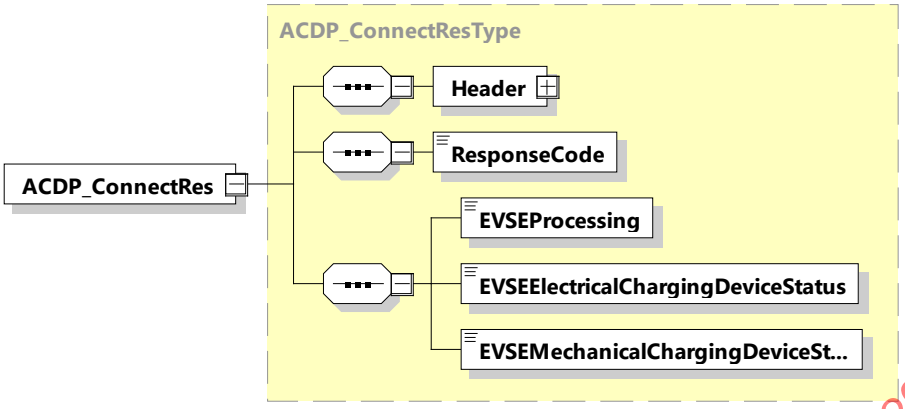


Figure 87 — Schema diagram – ACDP_ConnectRes

The elements of this message are used according to Table 84.

Table 84 — Semantics and type definition for ACDP_ConnectRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
EVSEProcessing	simpleType: processingType refer to Annex A for the type definition	Parameter indicating that the EVSE has finished the processing that was initiated after the ACDP_ConnectReq or if the EVSE is still processing at the time, the response message was sent.
EVSEElectricalChargingDeviceStatus	simpleType: electricalChargingDeviceStatusType refer to Annex A for the type definition	This element provides the information if the conductive connection between the EV and EVSE is in state "connected" (CP State = B, C or D) or "disconnected" (CP State = A).

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
EVSEMechanicalChargingDeviceStatus	simpleType: mechanicalChargingDeviceStatusType refer to Annex A for the type definition	This element provides the information if the ACDP status of the EVSE is in home, or end position or if it is in a moving state.

8.3.4.7.7 ACDP_DisconnectReq/Res

8.3.4.7.7.1 ACDP_DisconnectReq

[V2G20-4008] The EVCC and the SECC shall implement the message elements as defined in Figure 88 and
Table 85.

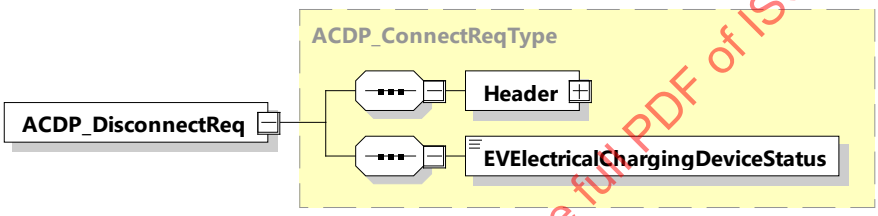


Figure 88 — Schema diagram – ACDP_DisconnectReq

The elements of this message are used according to Table 85.

Table 85 — Semantics and type definition for ACDP_DisconnectReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
EVElectricalChargingDeviceStatus	simpleType: electricalChargingDeviceStatusType refer to Annex A for the type definition	This element provides the information if the conductive connection between the EV and EVSE is in state "connected" (CP State = B, C or D) or "disconnected" (CP State = A).

8.3.4.7.7.2 ACDP_DisconnectRes

[V2G20-4009] The EVCC and the SECC shall implement the message elements as defined in Figure 89 and Table 86.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

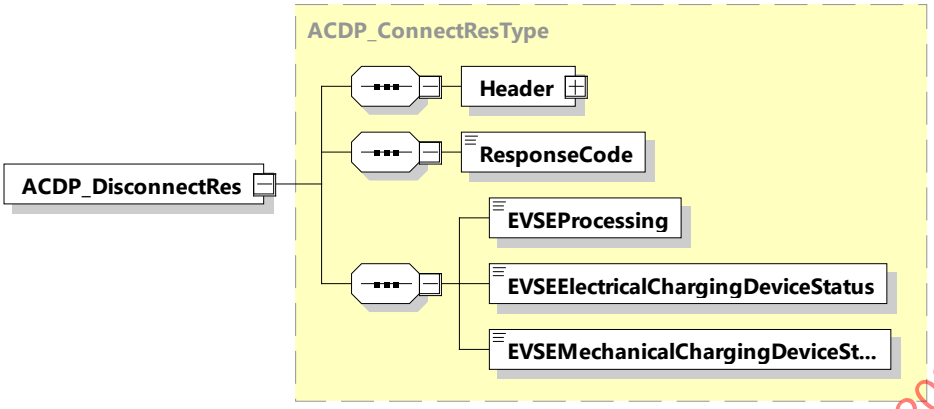


Figure 89 — Schema diagram – ACDP_DisconnectRes

The elements of this message are used according to Table 86.

Table 86 — Semantics and type definition for ACDP_DisconnectRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G Messages received by the SECC.
EVSEProcessing	simpleType: processingType refer to Annex A for the type definition	Parameter indicating that the EVSE has finished the processing that was initiated after the ACDP_ConnectReq or if the EVSE is still processing at the time, the response message was sent.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
EVSEElectricalChargingDeviceStatus	simpleType: electricalChargingDeviceStatusType refer to Annex A for the type definition	This element provides the information if the conductive connection between the EV and EVSE is in state "connected" (CP State = B, C or D) or "disconnected" (CP State = A).
EVSEMechanicalChargingDeviceStatus	simpleType: mechanicalChargingDeviceStatusType refer to Annex A for the type definition	This element provides the information if the ACDP status of the EVSE is in home, or end position or if it is in a moving state.

8.3.4.7.8 ACDP_SystemStatusReq/Res

8.3.4.7.8.1 ACDP_SystemStatusReq/Res handling

This message pattern is used to get current status information of involved charging equipment. The ACDP_SystemStatus message pair provides important diagnostic information as well.

The ACDP_SystemStatus messages have a separate payload type thus they execute in parallel and independent to the V2G messages.

NOTE 1 Safety relevant control with respect to the charging equipment and charging process is not in the scope of this document.

NOTE 2 The V2G communication is kept until the end of the charging session as well in the case of an error until the system is in a safe status after the ACDP has been moved into the home position.

The intended application of ACDP_SystemStatus is:

- first time after successfully processing of SessionSetupRes;
- at any time within the V2G communication process, asynchronous of the primary communication;
- in case of any relevant internal EV status change;
- in case of any EV error after processing of the last EVSE response message with “ResponseCode = OK”;
- in case of any EVSE error indicated by “ResponseCode = FAILED”, or “FAILED_xxx”;
- ACDP_SystemStatus may possibly be omitted in loop messages with “ResponseCode = OK”.

NOTE 3 The ACDP_SystemStatus message pair can also be applied in a synchronous manner in between the charging control V2G messages.

For the usage of ACDP_SystemStatus in error cases see 8.3.4.7.8.5 and 8.3.4.7.8.7.

8.3.4.7.8.2 ACDP_SystemStatusReq

[V2G20-4010] The EVCC and the SECC shall implement the message elements as defined in Figure 90 and Table 87.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

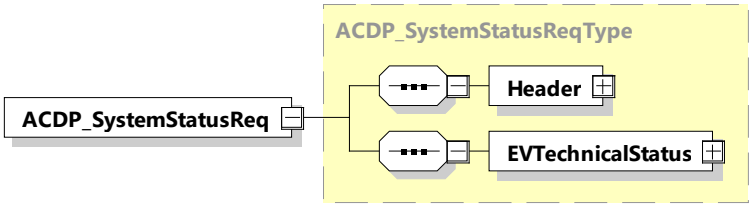


Figure 90 — Schema diagram – ACDP_SystemStatusReq

The elements of this message are used according to Table 87.

Table 87 — Semantics and type definition for ACDP_SystemStatusReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
EVTechnicalStatus	complexType: EVTechnicalStatusType refer to 8.3.5.7.1	This element provides detailed EV technical status

8.3.4.7.8.3 ACDP_SystemStatusRes

[V2G20-4012] The EVCC and the SECC shall implement the message elements as defined in Figure 91 and Table 88.

For ACDP charging method the EV positions itself correctly relative to the position of the ACDP. Before the ACDP can be activated the EV becomes immobilized. At the end of the charging process the EV is kept immobilized as long as the ACDP is not at its home position. The driver can control the immobilization request by the EV hand brake or any other technical means. On the other hand, the driver can end the charging process at any time by releasing the hand brake. In this case the mobilization of the EV waits until the ACDP is in home position.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

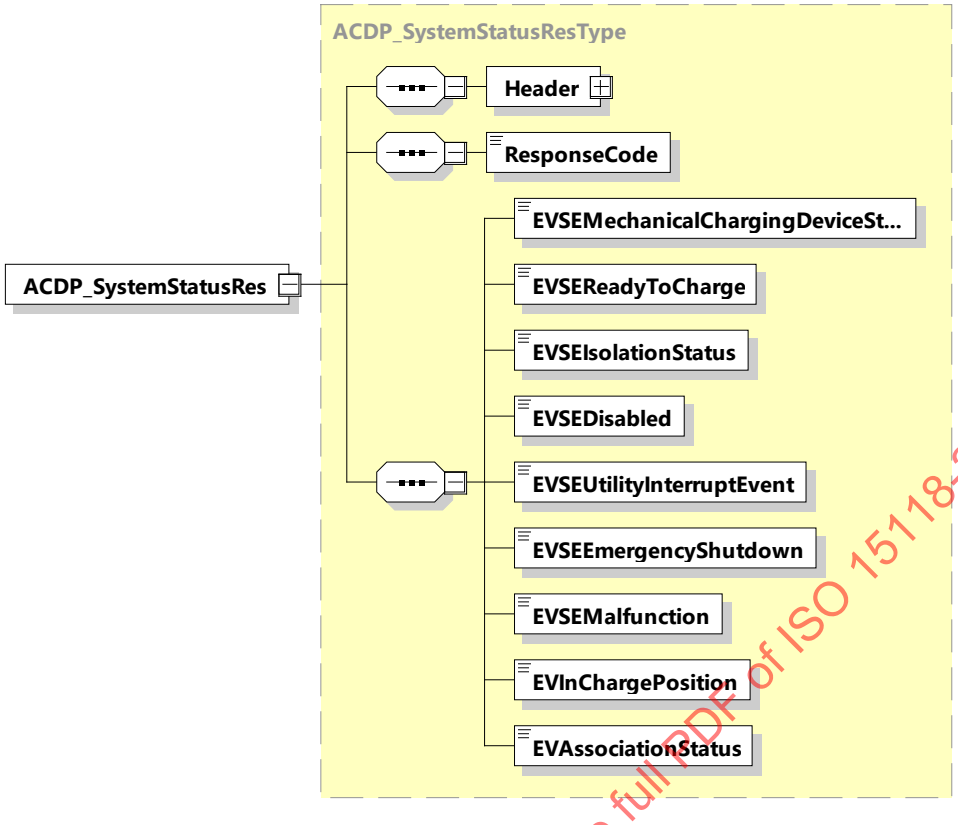


Figure 91 — Schema diagram – ACDP_SystemStatusRes

The elements of this message are used according to Table 88.

Table 88 — Semantics and type definition for ACDP_SystemStatusRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
EVSEMechanicalChargingDeviceStatus	simpleType: mechanicalChargingDeviceStatusType refer to Annex A for the type definition	This element provides the information if the ACDP status of the EVSE is in home, or end position or if it is in a moving state.
EVSEReadyToCharge	simpleType: xs:boolean	Element signalizes when the EVSE is READY or NOT READY to charge. This comprises all required EVSE sub-systems.
EVSEIsolationStatus	simpleType: isolationStatusType refer to Annex A for the type definition	This element provides the information about the isolation status of the EVSE. Possible states are: invalid, safe, warning, fault.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
EVSEDisabled	simpleType: xs:boolean	This element indicates when the EVSE is disabled by the operator or for maintenance. Possible states are: true, false.
EVSEUtilityInterruptEvent	simpleType: xs:boolean	This element indicates a utility power interrupt event. The EVSE control and communication functions may be backed up by an UPS.
EVSEEmergencyShutdown	simpleType: xs:boolean	This element indicates a charging system emergency shutdown or "E-Stop" button pressed at EVSE.
EVSEMalfunction	simpleType: xs:boolean	This element indicates a non-recoverable EVSE fault has occurred (e.g. breaker failure, ...).
EVInChargePosition	simpleType: xs:boolean	Option, only when position detection is available: This element indicates whether the EV is positioned within allowed tolerances to the ACDP.
EVAssociationStatus	simpleType: xs:boolean	Option, only when PPD is available: Indicates whether EV and EVSE are associated correctly.

NOTE 1 For ACDP it is recommended to provide the optional parameters to enable diagnoses of the charge process.

8.3.4.7.8.4 ACDP_SystemStatus EVCC requirements

[V2G20-4013] In case of an EV error the EVCC shall send a ACDP_SystemStatusReq message with Parameter "EV_Status_ReadyToCharge = FALSE" and all EV parameters representing the current EV (error) status and the EVCC shall execute normal shut down of the charging process according to Figure 92.

[V2G20-4014] In case [V2G20-4013] applies and the EVCC receives a ACDP_SystemStatusRes with parameter ResponseCode = OK the EVCC may process the received EVSE status parameters and shall continue to execute the normal shutdown process.

[V2G20-4015] The EVCC shall ignore to process the parameters provided by the ACDP_SystemStatusRes message when the "ResponseCode = FAILED".

8.3.4.7.8.5 Usage of ACDP_SystemStatusReq/Res on EVCC error

Figure 92 depicts an example EV error case during the processing of the DC_ChargeLoop message pair while charging. In this example the EVCC will execute the normal shutdown procedure as defined in IEC 61851-23:2014, Annex CC.3.3 starting with ramping down the target current to zero amp in a ramp down phase. After the present current is zero the EVCC will issue the PowerDeliveryReq with 'ChargeProgress' equal to 'STOP'. At this time the value of the ACDP_SystemStatus element EVImmobilizationRequest will be True, meaning the driver did not initiate to stop the charging process

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

by releasing the hand brake. In that way the ACDP_SystemStatus will provide concrete information about the root cause of a normal shut down process.

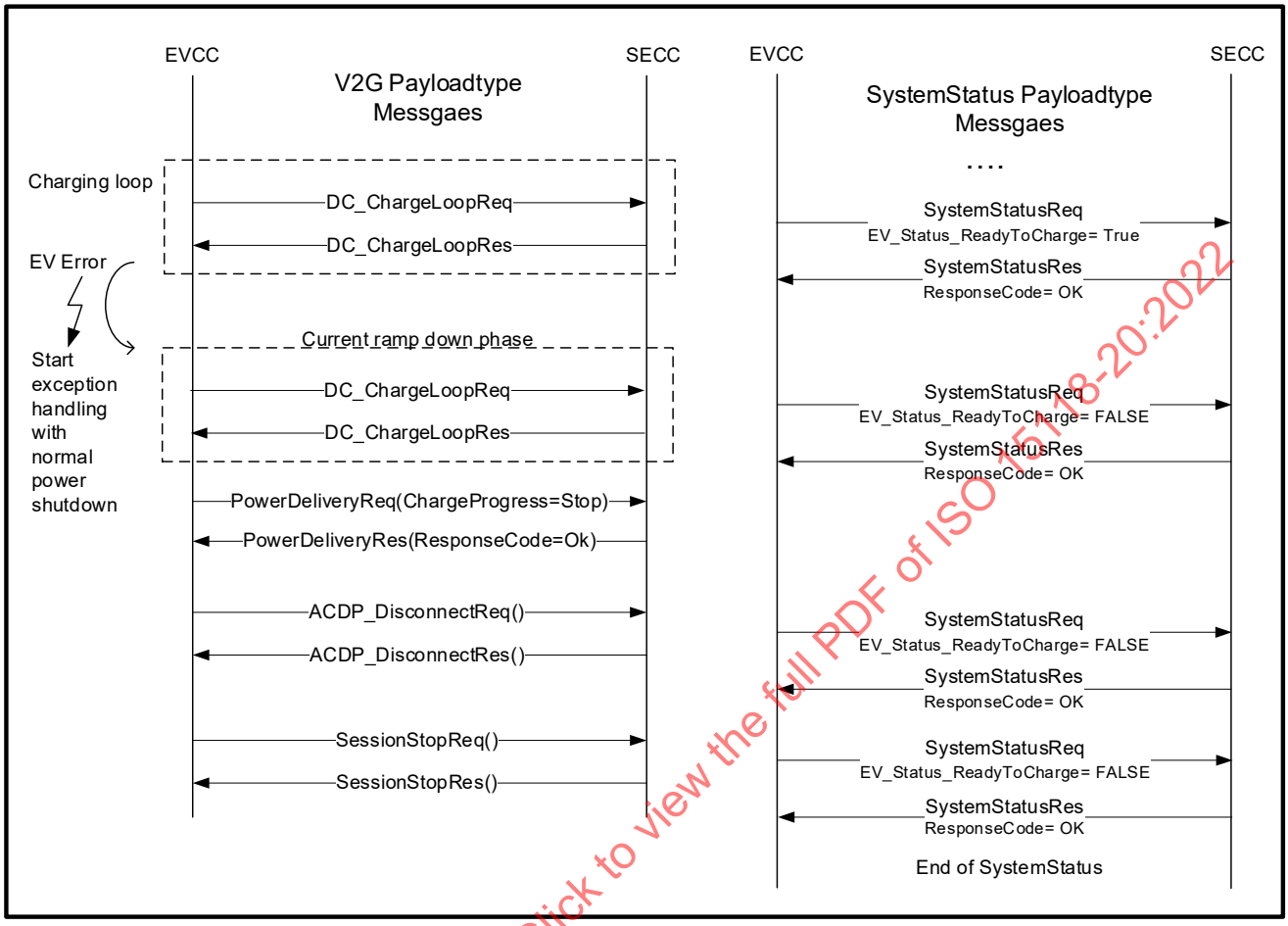


Figure 92 — ACDP exception handling example on EVCC error

In this sample EV initiated error case is due to RESS overtemperature therefore the

EVTechnicalStatus of the ACDP_SystemStatusReq will show the following contents:

- EVReadyToCharge = False;
- EVImmobilizationRequest = True;
- EVWLANStrength = - 66 dBm;
- EVCPStatus = C;
- EVSOC = 74 %;
- EVErrorCode = 4 (RESS overtemperature);
- EVTimeout = False.

The ACDP_SystemStatusRes will provide the following contents:

- ResponseCode = OK;
- EVSEMechanicalChargingDeviceStatus = EndPosition;
- EVSEReadyToCharge = True;
- EVSEIsolationStatus = Valid;
- EVSEDisabled = False;
- EVSEUtilityInterruptEvent = False;

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

- EVSEEmergencyShutdown = False;
- EVSEMalfunction = False;
- EVInChargePosition = True;
- EVAssociationStatus = True.

In the usual case of a normal shut down due to the driver's-initiated end of the charging by releasing the hand brake the EVTechnicalStatus will look like:

- EVReadyToCharge = False;
- EVImmobilizationRequest = False;
- EVWLANStrength = - 66 dBm;
- EVCPStatus = C;
- EVSOC = 74 %;
- EVErrorCode = 0;
- EVTimeout = False.

In this case the status of the element EVImmobilizationRequest = False indicates that the release of the hand brake was the cause to end the charging process.

8.3.4.7.8.6 ACDP_SystemStatus EVSE requirements

[V2G20-4016] After receiving the SessionSetupRes with parameter "ResponseCode = OK" the EVCC shall start to send ACDP_SystemStatusReq messages.

[V2G20-4017] The SECC shall respond to ACDP_SystemStatusReq message with "ResponseCode = OK" when it is able to represent the current EVSE status with the assigned parameters.

[V2G20-4018] The SECC shall respond to ACDP_SystemStatusReq message with "ResponseCode = FAILED" when it is not able to represent the current EVSE status with the assigned parameters.

[V2G20-4019] In case the SECC receives a ACDP_SystemStatusReq message with Parameter "EV_Status_ReadyToCharge = FALSE" it shall respond with ACDP_SystemStatusRes with "ResponseCode = OK" and all other EVSE ACDP_SystemStatus parameters representing the current EVSE status.

The timeout for System_Status_EndTimer is defined in Table 89.

NOTE The System_Status service is stopped after a SessionStopRes with parameter ResposeCode = OK was received.

Table 89 — System_Status service timer timeout value

Element Name	Value[S]	Semantics
System_Status_EndTimer	System_Status_End_Timeout	Duration of system status service
System_Status_End_Timeout	60	Timeout value of system status duration

8.3.4.7.8.7 Usage of ACDP_SystemStatusReq/Res on EVSE error

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Figure 93 depicts an example EVSE error case during the processing of the DC_ChargeLoop message pair. The SECC will respond with DC_ChargeLoopRes with ResponseCode = FAILED to initiate the EV exception handling by sending a ACDP_DisconnectReq. In parallel the EV will send ACDP_SystemStatusReq in order to receive diagnostic information of the EVSE error cause.

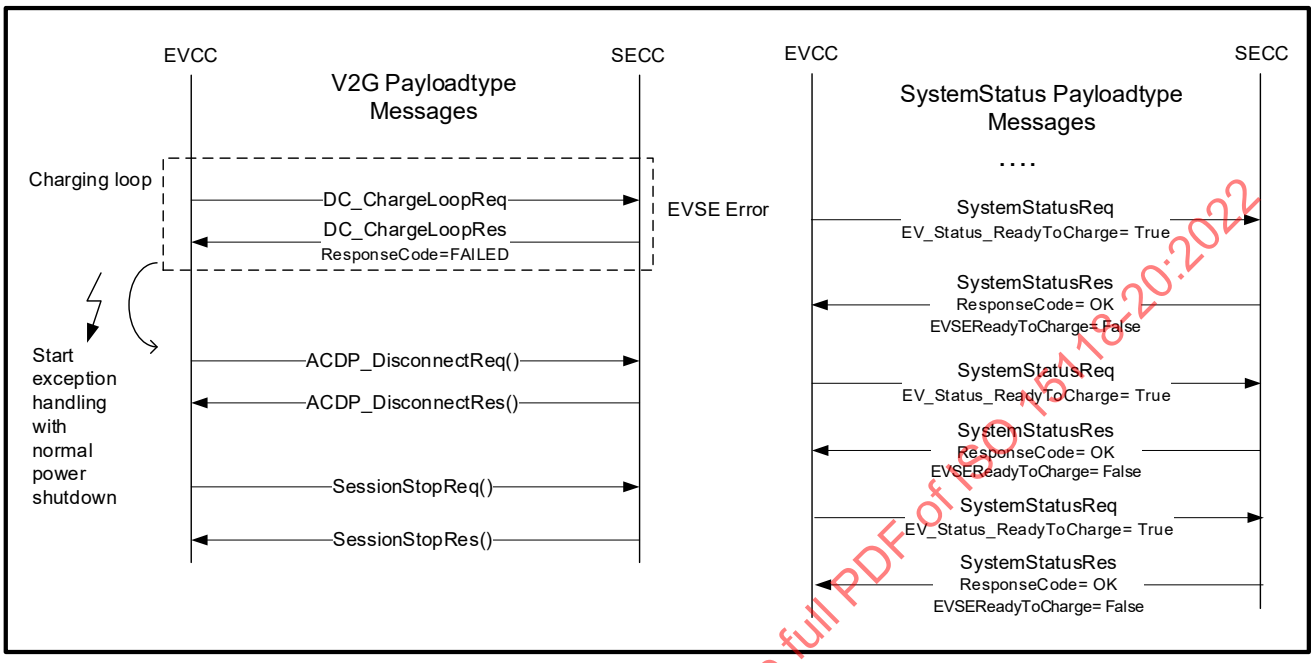


Figure 93 — ACDP Error handling on EVSE error

8.3.4.8 VAS messages

8.3.4.8.1 Parking Status service

8.3.4.8.1.1 VehicleCheckInReq/Res

8.3.4.8.1.1.1 VehicleCheckInReq/Res handling

This message is used by a parking status service for approaching EV to get information about an EVSE. A particular application of this service is an automated valid parking system (AVPS). The main purpose of EV check in message is that EV gets information of the EV target position for optical auto parking. The reference point marked by parking guideline is recognized by optical sensor. Target offset, 3 dimensional distances between pad target point and reference point is provided by this message response. The EV will be able to know the target position by adding the target offset to the reference point. When EVs complete parking to the target space, the EVCC informs the SECC and will exit parking status.

NOTE These messages are part of the parking status service.

Further description about parking status service is provided in 8.4.3.2.7.

8.3.4.8.1.1.2 VehicleCheckInReq

[V2G20-1298] The EVCC and the SECC shall implement the message elements as defined in Table 90 and Figure 94.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

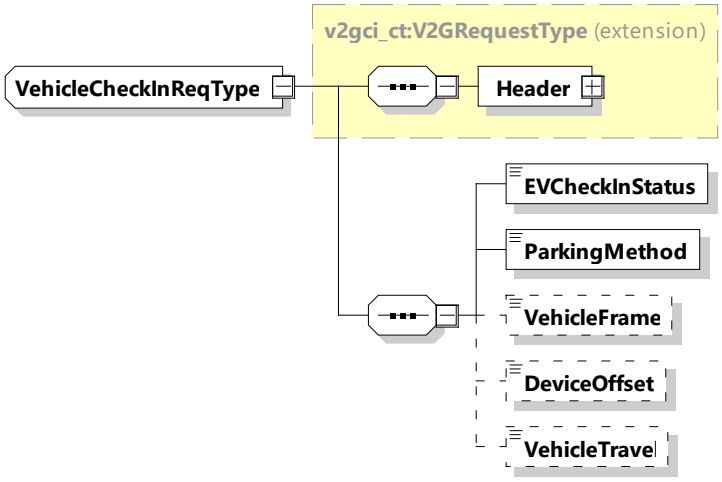


Figure 94 — Schema diagram – VehicleCheckInReq

The elements of this message are used according to Table 90.

Table 90 — Semantics and type definition for VehicleCheckInReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
EVCheckInStatus	simpleType: EVCheckInStatusType enumeration refer to Annex A for the type definition	Set "check in", "processing" or "completed" This element is used to inform to the SECC the check in status.
ParkingMethod	simpleType: parkingMethodType enumeration refer to Annex A for the type definition	Set "auto parking" or "manual" This element is used to inform to the SECC the parking method.
VehicleFrame	simpleType: xs:short	Optional: This element provides the information about 2 dimensional EV enveloping square, given by (VehicleWidth, VehicleLength).
DeviceOffset	simpleType: xs:short	Optional: This element provides information of EV WPT device offset from EV frame, given by (OffsetWidth, OffsetLength).
VehicleTravel	simpleType: xs:short	Optional: This element provides the distance information between WPT parking device and EV device measured by EV, given by (TravelX, TravelY).

Actually, positioning control in parking only requires information about device locations, such as "DeviceOffset" and "DeviceLocation" (see 8.3.4.8.1.1.3). The information about parking lot and EV outline,

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

such as "VehicleFrame" and "ParkingSpace" will have a chance to be applied to the EV geometry and direction check within a parking lot in some cases.

8.3.4.8.1.1.3 VehicleCheckInRes

[V2G20-1299] The EVCC and the SECC shall implement the message elements as defined in Table 91 and Figure 95.

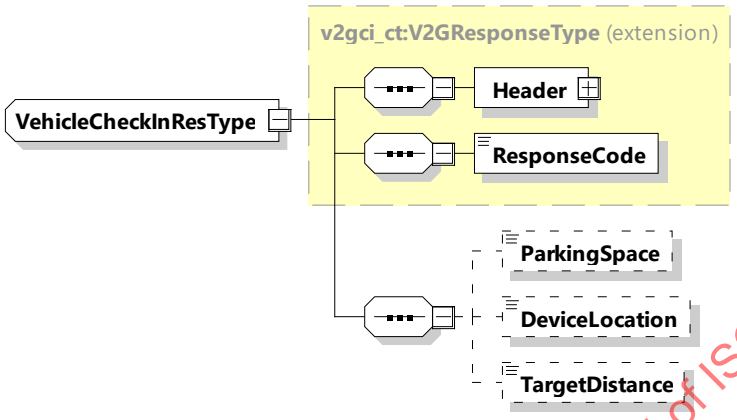


Figure 95 — Schema diagram – VehicleCheckInRes

The elements of this message are used according to Table 91.

Table 91 — Semantics and type definition for VehicleCheckInRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
ParkingSpace	simpleType: xs:short	Optional: This element provides the information about 2 dimensional parking space, given by (ParkingWidth, ParkingLength).
DeviceLocation	simpleType: xs:short	Optional: This element provides information of parking WPT device location in parking space, given by (LocationWidth, LocationLength).
TargetDistance	simpleType: xs:short	Optional: This element provides the distance information between WPT parking device and EV device measured by EVSE, given by (DistanceX, DistanceY).

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

8.3.4.8.1.2 VehicleCheckOutReq/Res

8.3.4.8.1.2.1 VehicleCheckOutReq/Res handling

This message is used by the EVCC to inform the SECC about the departure of the EV. The definition of a charging session includes EV departure, so it is necessary for the SECC to know it. This message is applied to parking status services.

NOTE These messages are part of the parking status service.

8.3.4.8.1.2.2 VehicleCheckOutReq

[V2G20-1300] The EVCC and the SECC shall implement the message elements as defined in Table 92 and Figure 96.

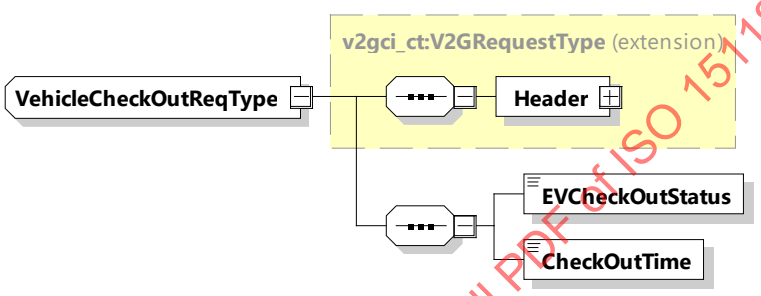


Figure 96 — Schema diagram - VehicleCheckOutReq

The elements of this message are used according to Table 92.

Table 92 — Semantics and type definition for VehicleCheckOutReq

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
EVCheckOutStatus	simpleType: EVCheckOutStatusType enumeration refer to Annex A for the type definition	Set "check out", "processing" or "completed" This element is used to inform to the SECC the CheckOut status.
CheckOutTime	simpleType: xs:unsignedLong	This element is used to inform to the SECC about the planned/estimated/expected departure time of the EV expressed as an absolute time stamp in SECC Time [in seconds].

8.3.4.8.1.2.3 VehicleCheckOutRes

[V2G20-1301] The EVCC and the SECC shall implement the message elements as defined in Table 93 and Figure 97.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

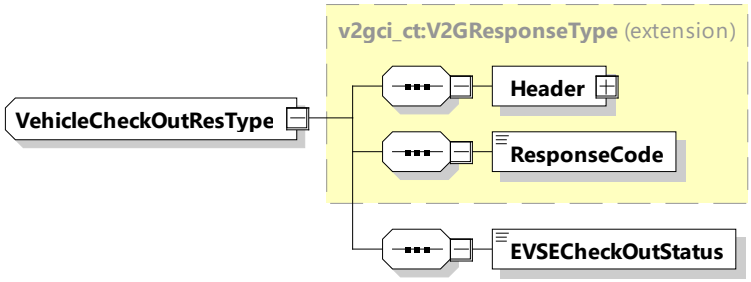


Figure 97 — Schema diagram – VehicleCheckOutRes

Table 93 — Semantics and type definition for VehicleCheckOutRes

Element Name	Type	Semantics
Header	complexType: MessageHeaderType refer to 8.3.3	Contains general information, used for all messages.
ResponseCode	simpleType: responseCodeType enumeration refer to Annex A for the type definition	ResponseCode indicating the acknowledgment status of any of the V2G messages received by the SECC.
EVSECheckOutStatus	simpleType: evseCheckOutStatusType enumeration refer to Annex A for the type definition	Set "scheduled" or "completed". This element is used to inform to the EVCC the CheckOut status.

8.3.5 Complex data types

8.3.5.1 Overview

This subclause defines complex data types (complexType), which are used in the messages. Complex data types are composed of several elements which themselves are based on simple data types.

NOTE Types starting with xs: are defined by W3C XML Schema 2 documents.

8.3.5.2 Physical Values

[V2G20-1813] The absolute value of the element defining the maximum shall always be greater than the absolute value defining the matching minimum, e.g. EVMaximumChargePower and EVMinimumChargeCurrent. This relationship shall also be maintained if the values of an element pair get communicated in two different messages.

[V2G20-1204] For all message elements of type RationalNumberType the SECC and the EVCC shall apply the value range and unit definition as according to Table 94.

Table 94 — Value range and unit definition for message elements using RationalNumberType

Element Name	Physical unit
BatteryEnergyCapacity	Wh
EVEnergyRequest	Wh
EVMaximumChargeCurrent	A

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Physical unit
EVMaximumChargePower	W
EVMaximumCurrent	A
EVMaximumCurrentLimit	A
EVMaximumDischargeCurrent	A
EVMaximumDischargePower	W
EVMaximumEnergyRequest	Wh
EVMaximumPowerLimit	W
EVMaximumVoltage	V
EVMinimumChargeCurrent	A
EVMinimumCurrent	A
EVMinimumDischargeCurrent	A
EVMinimumEnergyRequest	Wh
EVPresentActivePower	W
EVPresentReactivePower[_L2,_L3]	W
EVPresentVoltage	Volt
EVSEMaximumChargeCurrent	A
EVSEMaximumChargePower	W
EVSEMaximumCurrent	A
EVSEMaximumCurrentLimit	A
EVSEMaximumDischargeCurrent	A
EVSEMaximumDischargePower	W
EVSEMaximumPowerLimit	W
EVSEMinimumChargePower	W
EVSEMinimumCurrentLimit	A
EVSEMinimumDischargePower	W
EVSENominalFrequency	Hz
EVSENominalVoltage	V
EVSEPresentActivePower [_L2,_L3]	W
EVSEPresentCurrent	A
EVSEPresentVoltage	V
EVSETargetActivePower[_L2,_L3]	W
EVSETargetFrequency	Hz
EVSETargetReactivePower[_L2,_L3]	VA
EVTargetCurrent	A
EVTargetEnergyRequest	Wh
EVTargetVoltage	V
Power	W

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Physical unit
PowerTolerance	W
RemainingTimeToFullSOC	s

NOTE 1 The maximum and minimum transmittable values are calculated using the boundaries of the RationalNumberType. They are given through the signed 16-bit Integer (Range: -32 768 to +32 767) of the value and the exponent.

NOTE 2 Values from -32 768 – +32 767 can be changed till the last digit, but when the exponent is used the changeable amount changes. For example if an exponent of 1 is used the changes can only be made until the 10 digit range or if the exponent of 2 is used the number can only be changed till 100 digit range.

NOTE 3 The transmittable range is not the range of allowed values for the used system. It is important that these ranges are implemented according to the limits of the implementation and the corresponding IEC documents, to follow safety regulations.

8.3.5.2.1 Common rules for physical values

[V2G20-1034] For all applications a positive value for elements with the physical unit "W", "Wh" and "A" shall represent a power transfer from the EVSE to the EV (charging mode).

[V2G20-1035] Negative values shall be used to define energy transfer from the EV to the EVSE (discharging mode).

[V2G20-1783] For all applications in AC power transfer the elements with the physical unit:

- "V" and "A" shall be interpreted as root mean square values;
- "V" shall always be measured between one phase and neutral, unless stated otherwise;
- "W" shall be based on the assumption of a purely resistive AC circuit with a power factor of 1.0;
- for the "VA reactive" unit positive values shall represent inductive and negative values shall represent capacitive reactive power.

Equipment with other characteristics shall apply proper adjustments during related value calculations.

In the case of AC (dis)charging the EVSETargetActivePower and EVSETargetReactive elements serve two purposes. In dynamic control mode they are the normal means of operation while in Scheduled control mode they should only be used as a technique to guarantee that the mandatory local technical requirements from the grid code or urgent local requirements can be satisfied.

[V2G20-1823] EVSETargetActivePower and EVSETargetReactivePower shall always be based on EVSENominalVoltage.

NOTE From the perspective of the EV the EVSETargetActivePower and EVSETargetReactivePower elements therefore primarily communicate target setpoints for the active and reactive currents and the resulting phi angle ("power factor") as the grids voltage can and will be fluctuating, even during the delay resulting from the communication processing.

[V2G20-1824] For the EVSETargetReactivePower positive values shall represent inductive and negative values shall represent capacitive reactive power.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1825] The EV shall adjust its energy transfer behavior to the new setpoints, that have been communicated by the EVSETargetActivePower and/or the EVSETargetReactive elements, as fast as technically feasible.

8.3.5.2.2 Rules related to asymmetric polyphaser values

In order to support asymmetric polyphase energy transfers many elements which are related to power in the context of AC messages are provided in sets with phase specific variants. The following requirements apply to all such element sets unless explicitly stated otherwise in different requirements.

[V2G20-1814] For AC power phase specific element sets the line names L1, L2 and L3 shall identify the associated pins on the charging connector (e.g. as defined in IEC 62196).

NOTE This document only controls the energy exchange between the EV and the EVSE. In that context L1, L2 and L3 are clearly defined by the connector. A mapping to the associated lines at the grid connection point is only possible in the context of a specific installation within the premises and therefore out of the scope for this document.

[V2G20-1815] In the context of AC services with the connector choice SinglePhase only the power phase specific base elements (e.g. EVMaximumChargePower) shall be used. Elements with the suffix "_L2" and "_L3" shall not be used.

[V2G20-1816] In the context of AC services with the connector choice ThreePhase power phase specific elements with the suffix "_L2" and "_L3" shall be allowed.

[V2G20-1817] In the context of AC services with the connector choice ThreePhase the power phase specific base elements (e.g. EVMaximumChargePower) shall represent the sum of all three lines if neither the element sets peer with the suffix "_L2" nor "_L3" is present in the same message. If a sum value is communicated an even distribution across all three power phases shall be applied.

[V2G20-1818] In the context of AC services with the connector choice ThreePhase the power phase specific base elements (e.g. EVMaximumChargePower) shall identify the value associated with the L1 line if either the element sets peer with the suffix "_L2" or "_L3" is present in the same message.

[V2G20-1819] All requirements which apply to the base element (e.g. EVMaximumChargePower) of a power phase specific element set shall also apply to the peers with the suffix "_L2" or "_L3" in an equivalent way.

8.3.5.2.3 Rules related to EV energy request values

The EV energy request parameters defined below are used by the EV to inform the EVSE of its energy demands and limitations. They are instantaneous values that will change over time during the energy transfer loops. They are calculated, updated and sent during the energy transfer loop by the EV and they form the foundation for the DynamicControlMode.

[V2G20-1217] The EV shall ensure that at any time: EV Minimum Energy Level ≤ EV Target Energy Level ≤ EV Maximum Energy Level and therefore the resulting energy requests satisfy the following relationship: EVMinimumEnergyRequest ≤ EVTargetEnergyRequest ≤ EVMaximumEnergyRequest.

[V2G20-2191] In dynamic control mode the objective of the energy transfer plan shall be that at the end of the service session the EVTargetEnergyRequest will be less than or equal to zero.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 1 This means that the SECC is allowed to reach a target range defined between EV maximum energy level and EV target energy level.

NOTE 2 When the EVMaximumEnergyRequest value is negative then an immediate discharge is requested by the EV.

EVMinimumEnergyRequest is used to indicate the minimum amount of energy requested by the EV at any given time during the energy transfer loop. It is the difference between the minimum level of energy requested by the EV to be transferred as soon as possible and the present level of energy of the EV battery.

NOTE 3 When the EVMinimumEnergyRequest value is positive then an immediate charge is requested by the EV.

NOTE 4 When the EVMinimumEnergyRequest value is equal to zero or negative then charging can be delayed or discharging can be applied.

EVMaximumEnergyRequest is used to indicate the maximum energy level accepted by the EV at any given time during the energy transfer loop. It is the difference between the maximum level of energy accepted by the EV and the present level of energy of the EV battery.

EVTargetEnergyRequest is used to indicate the amount of energy requested by the EV before departure time. It is the difference between the amount of energy required by the EV at departure time and the present level of energy in the EV battery.

NOTE 5 When the EVMinimumEnergyRequest value is equal to zero or negative and the EVMaximumEnergyRequest value is equal to zero or positive then charging or discharging is possible.

Since the energy request values get constantly updated by the EV to the actual conditions this mechanism allows to compensate for auxiliary energy demand (e.g. due to cabin heating or cooling) that over time will drain the storage system. Such type of energy "leakage" would be reflected in a reduced EV present energy level, which then would be reflected by adjusted EV[*]EnergyRequest parameters. The SECC gets a chance to derive educated guesses on leakage behavior and can include such assumptions in its energy transfer strategy. On the other hand the EVCC should include a known leakage energy demand in its energy request description as early as possible to give the SECC a better foundation for planning its strategy.

8.3.5.3 Common

8.3.5.3.1 ServiceType

This type represents a tag for a specific service. It gives a short definition and identification of a specific service.

[V2G20-1308] The SECC and the EVCC shall implement this type as defined in Table 95 and Figure 98.

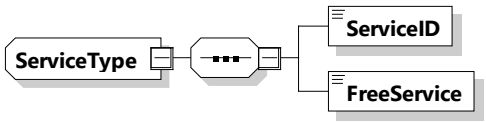


Figure 98 — Schema diagram – ServiceType

The elements of this message are used according to Table 95.

Table 95 — Semantics and type definition for ServiceType

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
ServiceID	simpleType: xs:unsignedShort	Unique identifier of the service
FreeService	simpleType: xs:boolean	This element is used by the SECC to indicate if a service can be used by the EVCC free of charge or not. If FreeService is equal to true, the EV can use the offered service without an additional cost. If FreeService is equal to false, the service, if used by the EV, will be billed using the method negotiated during the authorization phase.

8.3.5.3.2 ServiceListType

[V2G20-1309] The SECC and the EVCC shall implement this type as defined in Table 96 and Figure 99.

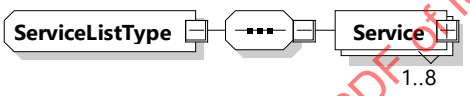


Figure 99 — Schema diagram – ServiceListType

The elements of this message are used according to Table 96.

Table 96 — Semantics and type definition for ServiceListType

Element Name	Type	Semantics
Service	complexType: serviceType refer to 8.3.5.3.1	Contains all information for identifying a service. The ServiceList includes at least one service and may include up to 8 services.

8.3.5.3.3 CertificateChainType

This data type stores the leaf certificate, and all certificates in the chain up to the root. The root certificate is not included in this data type. In the special (but unlikely) case, that a leaf certificate is directly signed by the root, the "SubCertificates" field is empty. In all other cases, this field contains an ordered list of sub-CA certificates to follow the trust-path from the leaf certificate up to the root.

[V2G20-1312] The SECC and the EVCC shall implement this type as defined in Table 97 and Figure 100.

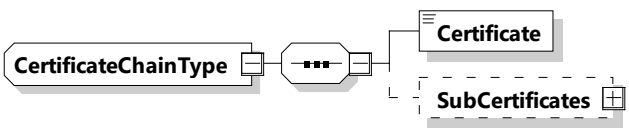


Figure 100 — Schema diagram – CertificateChainType

The elements of this message are used according to Table 97.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 97 — Semantics and type definition for CertificateChainType

Element Name	Type	Semantics
Certificate	simpleType: certificateType refer to Annex A for the type definition	A x.509v3 leaf certificate (the "client" certificate). The certificate is DER encoded. Refer to ITU-T X.690 for details of DER encoding.
SubCertificates	complexType: SubCertificatesType refer to 8.3.5.3.6	Optional: The certificate chain containing all sub-certificates leading up to the CA certificate, but not including the root CA certificate

[V2G20-2683] If the certificate provided in element "Certificate" included in the parameter of "CertificateChainType" is not directly signed by a root CA certificate, element "SubCertificates" shall be included in the parameter of "CertificateChainType".

NOTE If the certificate included in element "Certificate" is directly signed by a root CA certificate, element "SubCertificates" is not included in the parameter of "CertificateChainType".

8.3.5.3.4 SignedCertificateChainType

This data type stores the leaf certificate, and all certificates in the chain up to the root. The root certificate is not included in this data type. In the special (but unlikely) case that a leaf certificate is directly signed by the root, the "SubCertificates" field is empty. In all other cases, this field contains an ordered list of sub-CA-certificates to follow the trust-path from the leaf certificate up to the root. In addition to 8.3.5.3.3, this element may be signed, since an Id attribute is included.

[V2G20-1312] The SECC and the EVCC shall implement this type as defined in Table 98 and Figure 101.

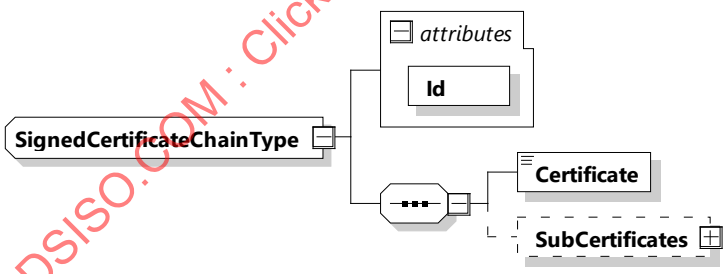


Figure 101 — Schema diagram – SignedCertificateChainType

The elements of this message are used according to Table 98.

Table 98 — Semantics and type definition for SignedCertificateChainType

Element Name	Type	Semantics
Id	Attribute	Allows inclusion of this element into a signature.
Certificate	simpleType: certificateType refer to Annex A for the type definition	A x.509v3 leaf certificate (the "client" certificate). The certificate is DER encoded. Refer to ITU-T X690 for details of DER encoding.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

SubCertificates	complexType: SubCertificatesType refer to 8.3.5.3.6	Optional: The chain with all subcertificates to the root certificate (not including root certificate).

8.3.5.3.5 ContractCertificateChainType

[V2G20-1859] The SECC and the EVCC shall implement this type as defined in Figure 102 and Table 99.

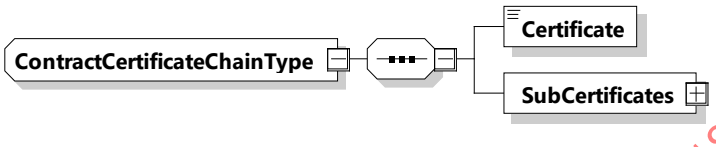


Figure 102 — Schema diagram – ContractCertificateChainType

The elements of this message are used according to Table 99.

Table 99 — Semantics and type definition for ContractCertificateChainType

Element Name	Type	Semantics
Certificate	simpleType: certificateType refer to Annex A for the type definition	An x.509v3 certificate (the "client" certificate). The certificate is DER encoded.
SubCertificates	complexType: SubCertificatesType refer to 8.3.5.3.6	The chain with all subcertificates to the root-certificate (not including root certificate).

8.3.5.3.6 SubCertificatesType

[V2G20-1336] The SECC and the EVCC shall implement this type as defined in Table 100 and Figure 103.

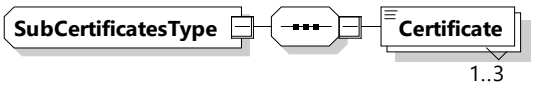


Figure 103 — Schema diagram – SubCertificatesType

The elements of this message are used according to Table 100.

Table 100 — Semantics and type definition for SubCertificatesType

Element Name	Type	Semantics
Certificate	simpleType: certificateType refer to Annex A for the type definition	An x.509v3 certificate. The certificate is DER encoded. Number of occurrences is limited to three.

8.3.5.3.7 MeterInfoType

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1313] The SECC and the EVCC shall implement this type as defined in Table 101 and Figure 104.

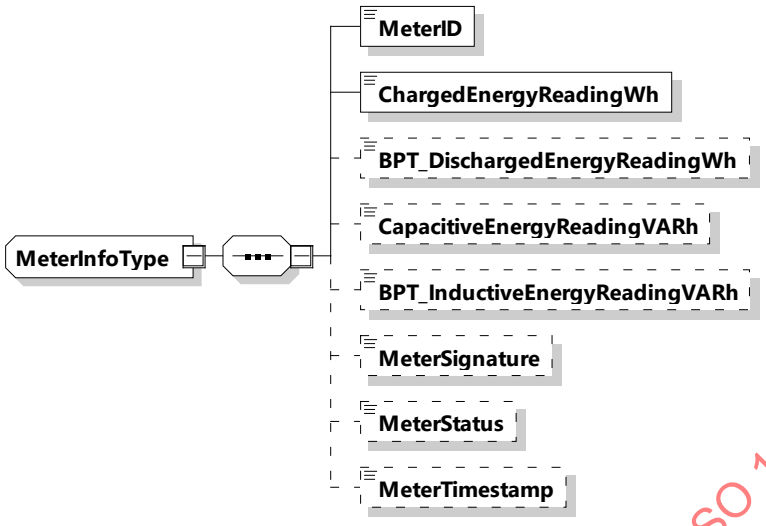


Figure 104 — Schema diagram – MeterInfoType

The elements of this message are used according to Table 101.

Table 101 — Semantics and type definition for MeterInfoType

Element Name	Type	Semantics
MeterID	simpleType: meterIDType refer to Annex A for the type definition	Unique identifier of the EVSE meter.
ChargedEnergyReadingWh	simpleType: xs:unsignedLong	The meter reading in Watthours that counts the energy flow from the EVSE to the EV, which is related to the normal charging process. The value is not guaranteed to start at zero during every energy transfer session.
BPT_DischargedEnergyReadingWh	simpleType: xs:unsignedLong	Optional for BPT, not applicable for other energy transfer services: The meter reading in Watthours that counts the energy flow from the EV to the EVSE, which is related to the discharging process. The value is not guaranteed to start at zero during every energy transfer session.
CapacitiveEnergyReadingVARh	simpleType: xs:unsignedLong	Optional: The meter reading in volt-ampere-reactive-hour (varh) which reflects the amount of capacitive reactive energy exchanged with the grid. The value is not guaranteed to start at zero during every energy transfer session.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
BPT_InductiveEnergyReadingVARh	simpleType: xs:unsignedLong	Optional for BPT, not applicable for other energy transfer services: The meter reading in volt-ampere-reactive-hour (varh) which reflects the amount of inductive reactive energy exchanged with the grid. The value is not guaranteed to start at zero during every energy transfer session.
MeterSignature	simpleType: meterSignatureType base64Binary (max length: 64) refer to Annex A for the type definition	Optional: Signature of the meter reading. This signature is generated by the EVSE meter. It is not verified at the EVCC. It might be used by a SA system for billing purposes if local regulations on metering permit it
MeterStatus	simpleType: meterStatusType short refer to Annex A for the type definition	Optional: Present status of the meter. The definition of the content of the MeterStatus is not in the scope of this document. The content may be defined by the EVSE operator or utility.
MeterTimeStamp	simpleType xs:unsignedLong	Optional: Timestamp of the time when the last element of the provided meter readings has been registered. The value is encoded at microseconds resolution in SECC time, a concept that is defined in 8.3.3.3. For use cases that require metering SECC time would be aligned with UTC.

[V2G20-1415] As exception to [V2G20-1034] and [V2G20-1035], the values of the element DischargedEnergyReadingWh shall always be positive numbers.

Due to legal metrology requirements in some countries it cannot be guaranteed that the elements ChargedEnergyReadingWh, DischargedEnergyReadingWh, MeterReadingVARhCapacitive and MeterReadingVARhInductive will always start at zero when a new charging session begins. Therefore, it is necessary to compute deltas in order to derive energy amounts for a particular charging session. Requirement [V2G20-1833] guarantees that a MeterInfoType element is transmitted prior to the beginning of the actual energy flow. This is the base line which allows the EV to compute proper deltas for an individual charging session.

NOTE The definition of value ranges for legal metrology is out of the scope for this document. As general guidance one can assume that values for elements ChargedEnergyReadingWh, DischargedEnergyReadingWh, MeterReadingVARhCapacitive and MeterReadingVARhInductive, at a household level, commonly can reach up to 999,999,999 (Wh, VARh). But at industrial level (e.g. for electric truck charging) even higher value ranges are likely. Implementations, therefore, can support the full range of the underlying unsignedLong value type.

8.3.5.3.8 RationalNumberType

[V2G20-1314] The SECC and the EVCC shall implement this type as defined in Table 102 and Figure 105.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

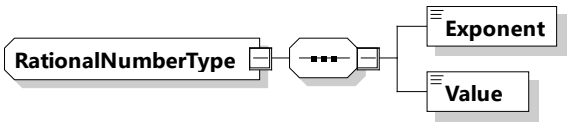


Figure 105 — Schema diagram – RationalNumberType

The elements of this message are used according to Table 102.

Table 102 — Semantics and type definition for RationalNumberType

Element Name	Type	Semantics
Exponent (exp)	simpleType: ExponentType xs:byte	The exponent to base 10 (dec). The final physical value is determined by: $x_{\text{RationalNumberType}} = y \times 10^{\text{exp}}$
Value (y)	simpleType xs:short	Value which shall be multiplied

NOTE For more information on the aspect of measurement tolerances of RationalNumberType elements see Annex I.

8.3.5.3.9 EVPowerProfileType

[V2G20-1316] The SECC and the EVCC shall implement this type as defined in Table 103 and Figure 106.

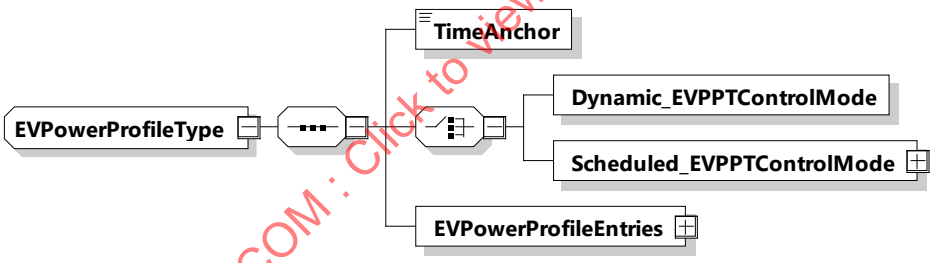


Figure 106 — Schema diagram – EVPowerProfileType

The elements of this message are used according to Table 103.

Table 103 — Semantics and type definition for EVPowerProfileType

Element Name	Type	Semantics
TimeAnchor	simpleType: xs:unsignedLong	The time that defines the starting point for the first EVPowerProfileEntry in this power profile. The value is encoded at microseconds resolution in SECC time, a concept that is defined in 8.3.3.3. Commonly the TimeAnchor will define a time that either is the present or some point in the near future.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
Dynamic_EVPPTControlMode	complexType: Dynamic_EVPPTControlModeType refer to 8.3.5.3.11	Contains all elements that are only required in case the control mode "Dynamic" is chosen.
Scheduled_EVPPTControlMode	complexType: Scheduled_EVPPTControlModeType refer to 8.3.5.3.11	Contains all elements that are only required in case the control mode "Scheduled" is chosen.
EVPowerProfileEntries	complexType: EVPowerProfileEntryListType refer to 8.3.5.3.10	Element used for encapsulating an individual power profile entry of the charge schedule. The number of EVPowerProfileEntry elements is limited to 2048.

[V2G20-1861] The TimeAnchor element shall defined the point in time when the first EVPowerProfileEntry element starts to be active.

[V2G20-1559] The power values of the EVPowerProfileEntry elements at no time shall exceed the corresponding hard limits of the power boundaries defined by the PowerSchedule and PowerDischargeSchedule of the last correctly negotiated ScheduleTuple which was selected by the EV during the related ScheduleExchangeReq/Res phase.

[V2G20-1010] The power values of the EVPowerProfileEntry elements shall represent the projected average target power levels.

NOTE 1 An average target power value allows the SECC to guess the required energy per EVPowerProfileEntry.

NOTE 2 As the EVPowerProfile can communicate charging and discharging phases at the same time the power values can be either positive or negative.

8.3.5.3.10 EVPowerProfileEntryListType

[V2G20-1867] The SECC and the EVCC shall implement this type as defined in Figure 107 and Table 104.

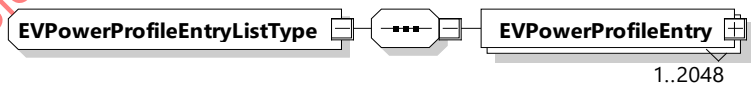


Figure 107 — Schema diagram – EVPowerProfileEntryListType

The elements of this message are used according to Table 104.

Table 104 — Semantics and type definition for EVPowerProfileEntryListType

Element Name	Type	Semantics
EVPowerProfileEntry	complexType: PowerScheduleEntryType refer to 8.3.5.3.20	List of EVPowerProfileEntry elements. The maximum amount of elements shall be 2 048.

8.3.5.3.11 Dynamic_EVPPTControlModeType

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

This type contains all elements of the EVPowerProfile that are only required in case the control mode "Dynamic" is chosen.

[V2G20-1875] The SECC and the EVCC shall implement this type as defined in Table 105 and Figure 108.



Figure 108 — Schema diagram – Dynamic_EVPPTControlModeType

Table 105 — Semantics and type definition for Dynamic_EVPPTControlModeType

Element Name	Type	Semantics
n/a	n/a	n/a

NOTE This parameter does not contain any elements.

8.3.5.3.12 Scheduled_EVPPTControlModeType

This type contains all elements of the EVPowerProfile that are only required in case the control mode "Scheduled" is chosen.

[V2G20-1782] The SECC and the EVCC shall implement this type as defined in Table 106 and Figure 109.

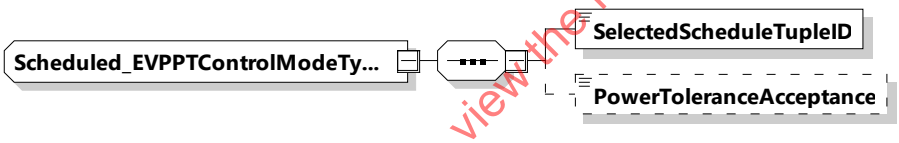


Figure 109 — Schema diagram – Scheduled_EVPPTControlModeType

The elements of this message are used according to Table 106.

Table 106 — Semantics and type definition for Scheduled_EVPPTControlModeType

Element Name	Type	Semantics
SelectedScheduleTupleID	simpleType: numericIDType refer to Annex A for the type definition	Unique identifier of the selectedScheduleTuple
PowerToleranceAcceptance	simpleType: powerToleranceAcceptanceType refer to Annex A for the type definition	Optional: This value is used to indicate if the EVCC acknowledges the PowerTolerance(s) sent by the SECC in ScheduleExchangeRes that was selected by the EVCC with the SelectedScheduleTupleID. This value can be set to "PowerToleranceConfirmed" for a positive reply or set to "PowerToleranceNotConfirmed" for a negative reply. This Element shall always be sent if a PowerTolerance has been provided by the SECC in the latest ScheduleExchangeRes.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

8.3.5.3.13 Dynamic_SEReqControlModeType

This type contains all elements of the ScheduleExchangeReq message that are only required in case the control mode "Dynamic" is chosen.

[V2G20-1755] The SECC and the EVCC shall implement this type as defined in Table 107 and Figure 110.

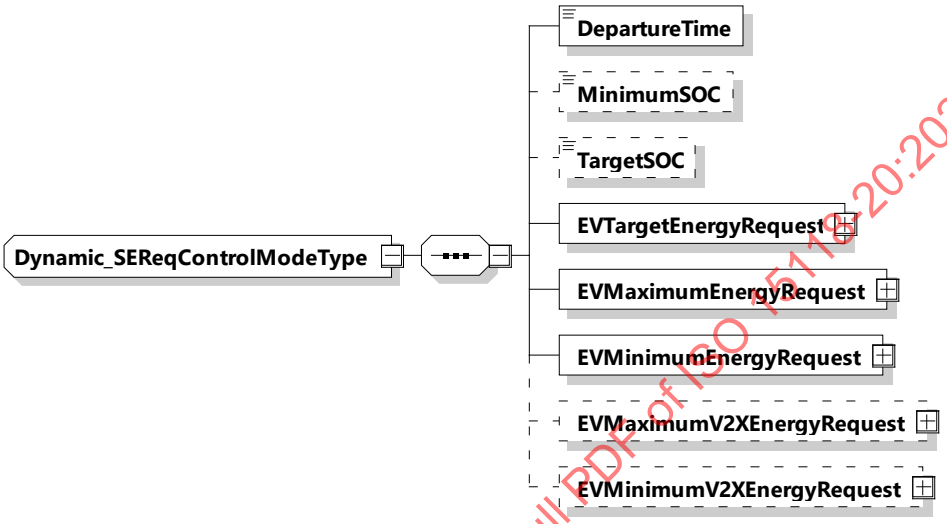


Figure 110 — Schema diagram – Dynamic_SEReqControlModeType

The elements of this message are used according to Table 107.

Table 107 — Semantics and type definition for Dynamic_SEReqControlModeType

Element Name	Type	Semantics
DepartureTime	simpleType: xs:unsignedInt	This element is used to indicate when the EV intends to finish the energy transfer process. The value is encoded in seconds since the TimeStamp of the message header (see [V2G20-2104]).
MinimumSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: Minimum State of Charge EV needs to keep throughout the charging session. Mandatory when service parameter MobilityNeedsMode was set to 2.
TargetSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: Target State of Charge of the EV Battery EV needs after charging. Mandatory when service parameter MobilityNeedsMode was set to 2.
EVTargetEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	The energy request of the EV it needs to fulfil the target SOC as specified by the owner.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
EVMaximumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum acceptable energy level of the EV.
EVMinimumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	The energy request of the EV it needs to fulfil the minimum SOC as specified by the owner. NOTE This value is not to be understood as a guaranteed minimal amount of energy that is to be consumed by or factured to the EV.
EVMaximumV2XEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Energy which may be charged until the PresentSOC has left the range dedicated for cycling activity. A negative value indicates that PresentSOC is above the V2X range.
EVMinimumV2XenergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Energy which needs to be charged until the PresentSOC enters the range dedicated for cycling activity. A positive value indicates that PresentSOC is below the V2X range.

NOTE If the EVCC sends the parameters EVMaximumV2XEnergyRequest and EVMinimumV2XEnergyRequest, it is indicating a preferred operational V2X range (i.e. for bidirectional cycling) and the SECC can attempt to stay within these limits as long as possible.

[V2G20-2103] Unless defined otherwise DepartureTime in all messages shall always be larger than zero.

[V2G20-2104] Unless defined otherwise DepartureTime in all messages shall express the offset in seconds from the point in time of sending this message, which is marked in the TimeStamp element of the common V2G message header.

[V2G20-2681] If EVMaximumV2XEnergyRequest and EVMinimumV2XEnergyRequest are sent by the EVCC, they always need to be sent together.

[V2G20-2682] If the EVCC provides EVMaximumV2XEnergyRequest and EVMinimumV2XEnergyRequest, EVMinimumEnergyRequest shall be less than or equal to EVMinimumV2XEnergyRequest, which shall be less than or equal to EVMaximumV2XEnergyRequest, which shall be less than or equal to EVMaximumEnergyRequest.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

8.3.5.3.14 Scheduled_SEReqControlModeType

This type contains all elements of the ScheduleExchangeReq message that are only required in case the control mode Scheduled is chosen.

[V2G20-1753] The SECC and the EVCC shall implement this type as defined in Table 108 and Figure 111.

© ISO 2022 – All rights reserved

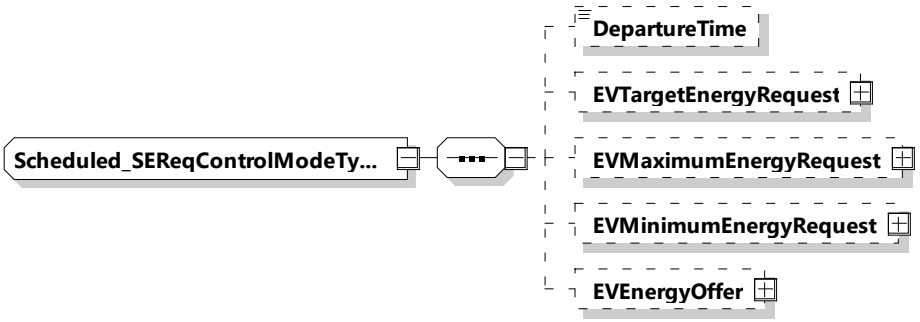


Figure 111 — Schema diagram – Scheduled_SEReqControlModeType

The elements of this message are used according to Table 108.

Table 108 — Semantics and type definition for scheduled_SEReqControlModeType

Element Name	Type	Semantics
DepartureTime	simpleType: xs:unsignedInt	Optional: This element is used to indicate when the EV intends to finish the energy transfer process. The value is encoded in seconds since the TimeStamp of the message header (see [V2G20-2104]).
EVTargetEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: The energy request of the EV it needs to fulfil the target SOC as specified by the owner.
EVMaximumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum acceptable energy level of the EV.
EVMinimumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: The energy request of the EV it needs to fulfil the minimum SOC as specified by the owner.
EVEnergyOffer	complexType: EVEnergyOfferType refer to 8.3.5.3.41	Optional: Includes several tuples of schedules from the EV.

NOTE If the EVTargetEnergyRequest has a negative value and the EVCC communicates an EVEnergyOffer, it is to be set as the amount of Energy the EV offers in the EVEnergyOffer at a certain price per kWh at a certain power-over-time.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

8.3.5.3.15 Dynamic_SEResControlModeType

This type contains all elements of the ScheduleExchangeRes message that are only required in case the control mode "Dynamic" is chosen.

[V2G20-1868] The SECC and the EVCC shall implement this type as defined in Table 109 and Figure 112.

© ISO 2022 – All rights reserved

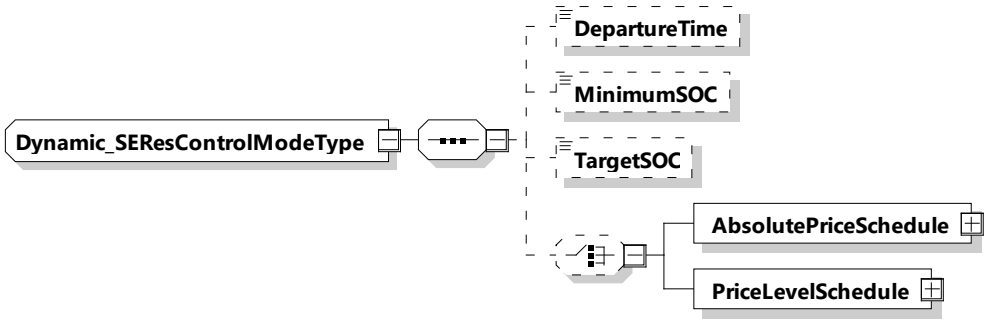


Figure 112 — Schema diagram – Dynamic_SEResControlModeType

The elements of this message are used according to Table 109.

Table 109 — Semantics and type definition for Dynamic_SEResControlModeType

Element Name	Type	Semantics
DepartureTime	simpleType: xs:unsignedInt	Optional: This element is used to indicate when the EV intends to finish the charging process. Only used when service parameter MobilityNeedsMode was set to 2. The value is encoded in seconds since the TimeStamp of the message header (see [V2G20-2104]).
TargetSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: New TargetSOC value updated by the user from EVSE's side Only used when service parameter MobilityNeedsMode was set to 2.
MinimumSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: New MinimumSOC value updated by the user from EVSE's side Only used when service parameter MobilityNeedsMode was set to 2.
AbsolutePriceSchedule	complexType: AbsolutePriceScheduleType refer to 8.3.5.3.49	Optional: Absolute price schedule for this session.
PriceLevelSchedule	complexType: PriceLevelScheduleType refer to 8.3.5.3.62	Optional: PriceLevel schedule for this session.

[V2G20-1640] The SECC shall only send MinimumSOC that is less than or equal to TargetSOC.

[V2G20-2660] If the EVCC selected the service parameter "MobilityNeedsMode" set to 2 and the SECC received new values for departure time, target SOC or minimum SOC from a secondary actor, the SECC shall include those updated values in DepartureTime, TargetSOC or MinimumSOC, respectively.

[V2G20-1648] If the EVCC selected the service parameter MobilityNeedsMode set to 2 and the EVCC receives a ScheduleExchangeRes with DepartureTime, TargetSOC or MinimumSOC in Dynamic_SEResControlMode, and if the EVCC accepts this DepartureTime,

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

TargetSOC or MinimumSOC as new Mobility Need information, the EVCC shall send updated DepartureTime, TargetSOC or MinimumSOC in the subsequent ChargeLoopReq.

[V2G20-1649] If the EVCC selected the service parameter MobilityNeedsMode set to 2 and the EVCC receives a ScheduleExchangeRes with DepartureTime, TargetSOC or MinimumSOC in Dynamic_SEResControlMode, and if the EV cannot accept this DepartureTime, TargetSOC or MinimumSOC, e.g. for internal reasons, the EVCC shall send different values in the subsequent ChargeLoopReq than the values in the ScheduleExchangeRes.

NOTE 1 In this case, the behavior of the SECC is not in scope.

NOTE 2 Both EVCC and SECC are expected to adapt the respective valid parameter and, if applicable, update their system, user interface, etc. with the information that is used for the session to ensure a high level of transparency and to avoid conflicting information to be displayed.

8.3.5.3.16 Scheduled_SEResControlModeType

[V2G20-1318] The SECC and the EVCC shall implement this type as defined in Table 110 and Figure 113.

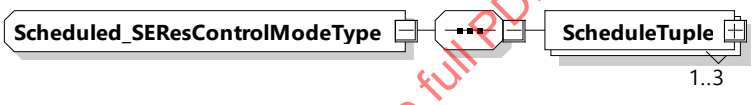


Figure 113 — Schema diagram – Scheduled_SEResControlModeType

The elements of this message are used according to Table 110.

Table 110 — Semantics and type definition for Scheduled_SEResControlModeType

Element Name	Type	Semantics
ScheduleTuple	complexType: ScheduleTupleType refer to 8.3.5.3.17	Includes several tuples of schedules from secondary actors. The number of ScheduleTuple elements is limited to 3. If this element includes discharging service, relevant parameter especially power in PowerSchedule will be used with negative value.

NOTE 1 The EVCC can implement a mechanism to compare different ScheduleTuple elements in order to optimize the charge schedule considering any given kind of cost.

[V2G20-297] The first ScheduleTuple element shall be defined as the default schedule.

[V2G20-298] If the EVCC is not capable of comparing different ScheduleTuple elements or comparison fails, the EVCC shall choose the default ScheduleTuple according to [V2G20-297].

NOTE 2 If the SECC (or a secondary actor) is interested in the energy offered by the EVCC, it can use the information provided in the EVEnergyOffer and integrate it into one of the provided ScheduleTuples.

NOTE 3 The schedule to which an EVCC refers to via the ScheduleTupleID in the PowerDeliveryReq, always originates from the SECC.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1835] The currency which is used within one ScheduleTupleType with one ScheduleTupleID in the charge and the discharge schedule shall be the same.

8.3.5.3.17 ScheduleTupleType

[V2G20-1319] The SECC and the EVCC shall implement this type as defined in Table 111 and Figure 114.

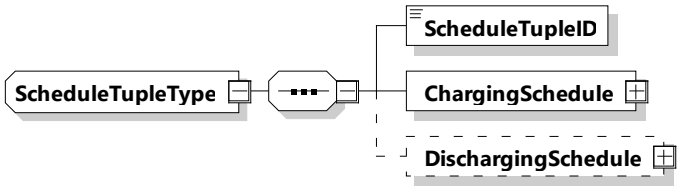


Figure 114 — Schema diagram – ScheduleTupleType

The elements of this message are used according to Table 111.

Table 111 — Semantics and type definition for ScheduleTupleType

Element Name	Type	Semantics
ScheduleTupleID	simpleType: numericIDType refer to Annex A for the type definition	Mandatory for scheduled control mode, not applicable for dynamic control mode: Unique identifier within an energy transfer session for a ScheduleTuple element. An SAID remains a unique identifier for one schedule throughout an energy transfer session.
ChargingSchedule	complexType: ChargingScheduleType refer to 8.3.5.3.40	Encapsulating element describing all relevant details for the charging schedule.
DischargingSchedule	complexType: ChargingScheduleType refer to 8.3.5.3.40	Optional: Encapsulating element describing all relevant details for the discharging schedule.

NOTE 1 A ScheduleTuple contains different elements, two schedules (ChargingSchedule, DischargingSchedule) which all can originate from different secondary actors and therefore can communicate contradicting incentives. While the EV is required to operate within the given physical limits it is free to choose which incentive it wants to follow when deciding on the planned EVPowerProfile.

[V2G20-773] The SECC shall use the values 1 to 255 for the parameter ScheduleTupleID.

[V2G20-1560] The ScheduleTupleID element shall be unique for each ScheduleTuple during the entire charging session.

[V2G20-1561] The SECC shall provide a PowerSchedule element based upon the limits of the local installation if no secondary actor provides a PowerSchedule.

[V2G20-1011] If a secondary actor provided a PowerSchedule, the SECC shall ensure that no power value within the PowerSchedule exceeds the matching EVSEMaximumChargePower limit.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 2 The EVCC assumes that the hard capability limits communicated in an EVSEMaximumChargePower [_L2,L3] value always will overrule any matching values provided within a PowerSchedule.

[V2G20-1012] If a secondary actor provided a PowerSchedule for discharging, the SECC shall ensure that no Power value within the PowerSchedule exceeds the matching EVSEMaximumDischargePower limit.

NOTE 3 The EVCC assumes that the hard capability limits communicated in an EVSEMaximumDischargePower[_L2,L3] value always will overrule any matching values provided within a PowerDischargeSchedule.

[V2G20-1562] The sum of the individual time intervals described in the PowerSchedule and PowerSchedule for Discharge (refer to 8.3.5.3.19) and PriceSchedule provided in the ScheduleExchangeRes message should match the period of time indicated by the EVCC in the message element DepartureTime of the ScheduleExchangeReq message.

[V2G20-1563] If the EVCC did not provide a DepartureTime Target Setting (refer to 8.3.4.4.2.2 and 8.3.5.4.1) in the ScheduleExchangeReq message, the sum of the individual time intervals described in the PowerSchedule and PriceSchedule provided in the ScheduleExchangeRes message, shall be greater or equal to 24 h.

[V2G20-1564] If the PriceSchedule or PowerSchedule provided by the secondary actor(s) are not covering the entire period of time until DepartureTime, the target setting EVTargetEnergyRequest (refer to 8.3.4.4.2.2 and 8.3.5.4.1) has not been met and the communication session has not been finished, it is the responsibility of the EVCC to request a new ScheduleTuple as soon as the last element of PowerSchedule or PriceSchedule becomes active by triggering a schedule renegotiation.

NOTE 4 The EVCC can request an update of tariff information by applying the schedule renegotiation process at any time during the charging loop.

[V2G20-1565] If the number of PriceSchedule elements provided by the secondary actor is not covering the entire time period until the EV has reached its mobility needs, it is in the responsibility of the EVCC to optimize the schedule based on the available information.

NOTE 5 The algorithm for optimizing the energy transfer profile is out of the scope of this document.

NOTE 6 Independent of the selected authorization mode of PnC or EIM, the secondary actor can decide to sign the PriceSchedule. This is not mandatory, as security is expected to provide through the CSMS, CSO, and EVSE trust chain. It is not in the scope of this document whether signing a PriceSchedule and/or validating an attached signature is mandatory or not. This can be defined by the legislative or other entities.

[V2G20-1567] The SECC shall not change the signature attached to the PriceSchedule, when receiving a signed PriceSchedule from a secondary actor.

NOTE 7 This presumes that the data structure used by the secondary actor for the provisioning of the PriceSchedule is identical with the data structure defined in this document.

[V2G20-2130] If the SA provided a PriceSchedule along with a signature, the SECC shall include the PriceSchedule along with the signature in the ScheduleExchangeRes.

[V2G20-1568] If the PriceSchedule is signed, it shall be signed by the same private key that was used to issue the leaf contract certificate that the EVCC used during this V2G communication session during the Authorization phase.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 8 This allows the EVCC to verify the integrity of the sales tariff by performing unique SECC verification. SECC/SA implementation is supposed to use the EVCC contract certificate chain which was transmitted in the element ContractCertificateChain of the message AuthorizationReq to identify the private key which can be used for signing the PriceSchedule. This requirement could be fulfilled by cooperation between SECC and SA including online communication; or the signed PriceSchedule can be cached.

[V2G20-907] In case of PnC, the EVCC, after receiving the PriceSchedule, should verify the signature using the same sub-CA certificate that was used to issue the contract certificate that the EVCC previously used during authorization. If this verification fails, the EVCC may treat the PriceSchedule as invalid. See [V2G20-1569].

NOTE 9 In case of EIM, the EVCC can ignore the signature (if it exists).

[V2G20-1569] If the EVCC treats the PriceSchedule as invalid, it shall ignore the PriceSchedule, i.e. the behavior of the EVCC shall be the same as if this invalid PriceSchedule was not received. Furthermore, the EVCC may close the connection. It then may reopen the connection again.

[V2G20-1869] The pricing within one ScheduleTupleID shall be consistent.

8.3.5.3.18 PowerScheduleType

[V2G20-310] The SECC and the EVCC shall implement this type as defined in Table 112 and Figure 115.

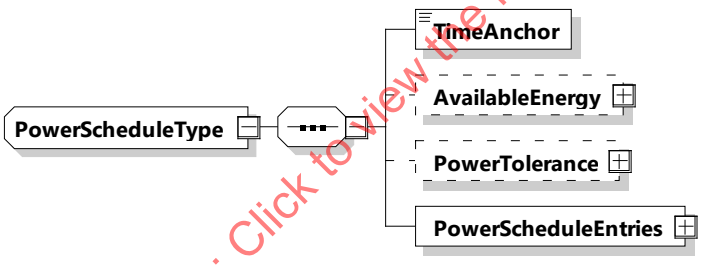


Figure 115 — Schema diagram – PowerScheduleType

The elements of this message are used according to Table 112.

Table 112 — Semantics and type definition for PowerScheduleType

Element Name	Type	Semantics
TimeAnchor	simpleType: xs:unsignedLong	The time that defines the starting point for the first PowerScheduleEntry in this power schedule. The value is encoded at ms resolution in SECC time, a concept that is defined in 8.3.3.2. For use cases that involve external secondary actors SECC time would be aligned with UTC. Commonly the TimeAnchor will define some point in time that lies in the past.
AvailableEnergy	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Gives the Available Energy the EVSE can offer with this Schedule.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
PowerTolerance	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: A value greater than zero which defines the highest acceptable deviation from the power values communicated via the EVPowerProfile. The SECC forms each PowerTolerance band by applying the PowerTolerance symmetrically to each EVPowerProfile entry. The SECC shall only send the parameter PowerTolerance if it requires the EVCC to stay within a certain tolerance band.
PowerScheduleEntries	complexType: PowerScheduleEntryListType refer to 8.3.5.3.19	List of PowerScheduleEntry elements. The number of PowerScheduleEntry elements is limited by the parameter MaximumSupportingPoints (according to [V2G20-1544]).

[V2G20-1016] The TimeAnchor of a PowerScheduleType element shall define the point in time when the first PowerScheduleEntry element starts to be active.

[V2G20-1863] In case the applied power profile violates the accepted band provided by the parameter PowerTolerance and exceeds the boundaries referred to by [V2G20-1547] the SECC may respond with the response code "WARNING_EVPowerProfileViolation" and trigger a schedule renegotiation. In case the EVCC fails to comply with the renegotiated EVPowerProfile, the SECC may stop the charging session and respond with the response code "FAILED_EVPowerProfileViolation".

[V2G20-1864] If a PowerTolerance band was defined (see [V2G20-1870]), then the SECC shall issue a "WARNING_EVPowerProfileViolation", as defined in [V2G20-1947], [V2G20-1948] and [V2G20-5078], whenever the applied power is outside the presently valid boundaries of the PowerTolerance band. This shall not apply if any of the exception conditions of [V2G20-1865] are met.

[V2G20-1865] If a PowerTolerance band was defined (see [V2G20-1870]), then the SECC shall issue a "FAILED_EVPowerProfileViolation", as defined in [V2G20-1950], [V2G20-1951] and [V2G20-5079], whenever the arithmetic average of the applied power over a time period of the last 30 s is outside the presently valid boundaries of the PowerTolerance band. This shall not apply if the violation of the PowerTolerance band is the result of other instructions issued by the SECC which have a higher priority (e.g. EVTargetActivePower goals).

[V2G20-1866] The EVCC shall always send the parameter PowerToleranceAcceptance in PowerDeliveryReq if the parameter PowerTolerance has been provided by the SECC in the schedule that was selected by the EVCC with the SelectedScheduleTupleID.

[V2G20-1870] The parameter PowerTolerance defines the absolute allowed deviation in relation to the power values communicated via the EVPowerProfile in PowerDeliveryReq message. As the EVPowerProfile is defining the average power over time ([V2G20-1010]), the PowerTolerance parameter is applied symmetrically (+/-) in order to define what is called the PowerTolerance band. The PowerTolerance band defines the boundaries of the acceptable true power flow. This does not apply, if the

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

PowerTolerance band at any point in time, is in conflict with the maximum power value provided by the selected PowerSchedule(s) in the latest ScheduleExchangeRes message [V2G20-1559].

NOTE 1 For example, if the requested charge power for a time segment within the EVPowerProfile is 20 kW and PowerTolerance is set to 1,5 kW, the acceptable PowerTolerance band for charging during that segment is (18,5 – 21,5) kW.

Since the EV energy transfer process is impacted by external factors (e.g. environmental conditions) the predictions of the EVPowerProfile are already subject to uncertainty. Therefore, it is not recommended for the SECC to set a too tight PowerTolerance parameter below 5 % of the EVSEMaximumChargePower because it makes unintended violations of the PowerTolerance band more likely.

[V2G20-1871] The parameter PowerTolerance shall be a value greater than zero.

[V2G20-2189] The AvailableEnergy element shall only be included in instances of PowerScheduleType which are describing charging limits within a ChargingSchedule element.

[V2G20-2190] If used in the context of a ChargingSchedule element then the AvailableEnergy element shall only contain values greater than zero.

NOTE 2 For example, the AvailableEnergy information can be used by EVSEs which are part of a micro grid system. It would allow the EVCC to detect very early in the charging process that the desired mobility needs (energy demand) cannot be met.

8.3.5.3.19 PowerScheduleEntryListType

[V2G20-1873] The SECC and the EVCC shall implement this type as defined in Figure 116 and Table 113.

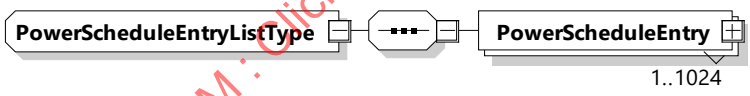


Figure 116 — Schema diagram – PowerScheduleEntryListType

The elements of this message are used according to Table 113.

Table 113 — Semantics and type definition for PowerScheduleEntryListType

Element Name	Type	Semantics
PowerScheduleEntry	complexType: PowerScheduleEntryType refer to 8.3.5.3.208.3.5.3.19	List of PowerScheduleEntry elements. The number of PowerScheduleEntry elements is limited by the parameter MaximumSupportingPoints (according to [V2G20-1056]).

8.3.5.3.20 PowerScheduleEntryType

[V2G20-1320] The SECC and the EVCC shall implement this type as defined in Table 114 and Figure 117.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

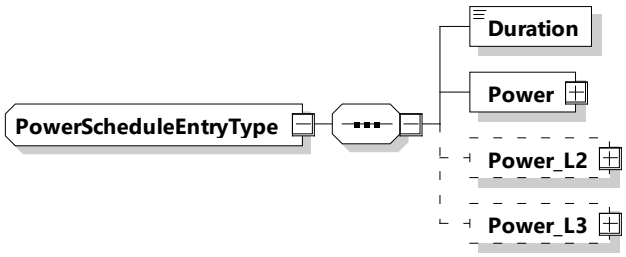


Figure 117 — Schema diagram – PowerScheduleEntryType

The elements of this message are used according to Table 114.

Table 114 — Semantics and type definition for PowerScheduleEntryType

Element Name	Type	Semantics
Duration	complexType: xs:unsignedInt	The amount of seconds that define the duration of the given power schedule entry.
Power	complexType: RationalNumberType refer to 8.3.5.3.8	Defines the amount of power (as defined in 8.3.5.3.8) for the given duration.
Power_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Defines the amount of power on phase L2 (as defined in 8.3.5.3.8) for the given duration.
Power_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Defines the amount of power on phase L3 (as defined in 8.3.5.3.8) for the given duration.

NOTE 1 The power values of the PowerScheduleEntryType follow the common semantic rules as defined in the clause on the RationalNumberType (8.3.5.3.8), where also the rules for asymmetric polyphase values are provided (8.3.5.2.2). Additional semantic requirements depend on the parent elements which utilize the PowerScheduleEntryType. For more details see the definitions related to: EVPowerProfile, PowerSchedule and PowerDischargeSchedule.

NOTE 2 The precise physical meaning of power is related to the chosen energy transfer technology. Refer to 8.3.5.3.8.

NOTE 3 According to [V2G20-1035] all power values in a DischargingSchedule need to be negative or zero.

[V2G20-1872] The duration element shall define the active period of time (in seconds) for the respective parent element of type PowerScheduleEntryType.

NOTE 4 In a list of consecutive elements the start time of the first PowerScheduleEntryType element is defined by the parent elements which utilize the PowerScheduleEntryType with their TimeAnchor element. See the definitions related to: EVPowerProfile, PowerSchedule and PowerDischargeSchedule.

[V2G20-1874] The start time of each element in a list of consecutive PowerScheduleEntryType elements shall be defined as the point in time when the previous element becomes inactive (see [V2G20-1872]).

[V2G20-1811] Before the start time of the first element and after the last element in a list of elements of type PowerScheduleEntryType becomes inactive the Power[_L2,L3] value shall be defined as the value "zero".

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

8.3.5.3.21 ServiceParameterListType

[V2G20-1331] The EVCC and the SECC shall implement this type as defined in Table 115 and Figure 118.

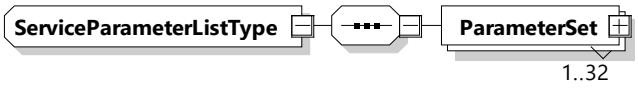


Figure 118 — Schema diagram – ServiceParameterListType

The elements of this message are used according to Table 115.

Table 115 — Semantics and type definition for ServiceParameterListType

Element Name	Type	Semantics
ParameterSet	complexType: ParameterSetType refer to 8.3.5.3.22	Defines parameters for a specific serviceID received from the SECC in the ServiceDiscoveryRes message.

8.3.5.3.22 ParameterSetType

[V2G20-1332] The EVCC and the SECC shall implement this type as defined in Table 116 and Figure 119.

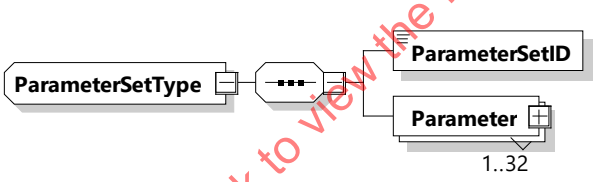


Figure 119 — Schema diagram – ParameterSetType

The elements of this message are used according to Table 116.

Table 116 — Semantics and type definition for ParameterSetType

Element Name	Type	Semantics
ParameterSetID	simpleType: serviceIDType refer to Annex A for the type definition	This element is used to select a specific parameter set for a specific ServiceID when selecting a service using the ServiceSelectionReq message.
Parameter	complexType: ParameterType refer to 8.3.5.3.23	This element is used by the SECC to indicate which service specific parameters can be selected for a certain service using the ParameterSetID. The number of Parameter elements is limited to 32.

8.3.5.3.23 ParameterType

[V2G20-1333] The EVCC and the SECC shall implement this type as defined in Table 117 and Figure 120.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

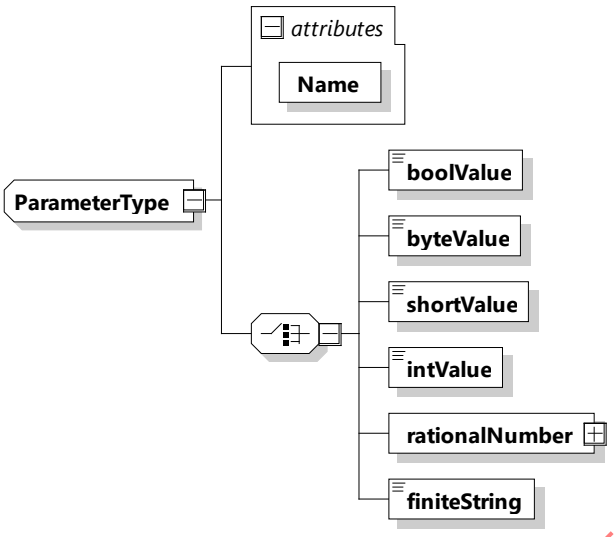


Figure 120 — Schema diagram – ParameterType

The elements of this message are used according to Table 117.

Table 117 — Semantics and type definition for ParameterType

Element Name	Type	Semantics
Name	simpleType: nameType refer to Annex A for the type definition	This element is used to indicate the name of the parameter.
One of the elements: – boolValue – byteValue – shortValue – intValue – rationalNumber – finiteString	xs:boolean (boolValue) xs:byte (byteValue) xs:short (shortValue) xs:int (intValue) nameType (finiteString) refer to Annex A for the type definition RationalNumberType (rationalNumber) refer to 8.3.5.3.8	This element is used to indicate the value for the parameter indicated by the element Name. A choice of 6 different element types. Only one for each parameter can be selected.

8.3.5.3.24 SelectedServiceListType

[V2G20-1334] The EVCC and the SECC shall implement this type as defined in Table 118 and Figure 121.

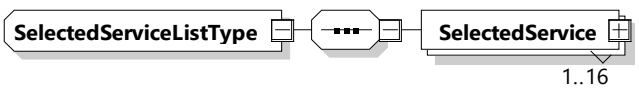


Figure 121 — Schema diagram – SelectedServiceListType

The elements of this message are used according to Table 118.

Table 118 — Semantics and type definition for SelectedServiceListType

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
SelectedService	complexType: SelectedServiceType refer to 8.3.5.3.25	This element is used to indicate the selected ServiceID and the associated parameterSet.

8.3.5.3.25 SelectedServiceType

[V2G20-1335] The EVCC and the SECC shall implement this type as defined in Table 119 and Figure 122.

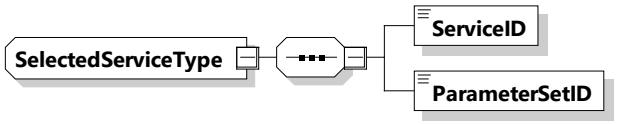


Figure 122 — Schema diagram – SelectedServiceType

The elements of this message are used according to Table 119.

Table 119 — Semantics and type definition for SelectedServiceType

Element Name	Type	Semantics
ServiceID	simpleType: serviceIDType refer to Annex A for the type definition	Unique identifier of the service
ParameterSetID	simpleType: serviceIDType refer to Annex A for the type definition	This element is used to select a specific parameter set for a specific ServiceID when selecting a service using the ServiceSelectionReq message.

8.3.5.3.26 EVSEStatusType

[V2G20-1338] The EVCC and the SECC shall implement this type as defined in Table 120 and Figure 123.

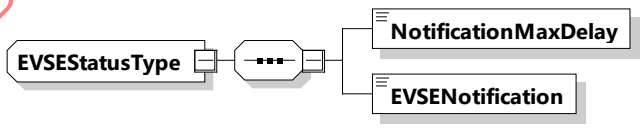


Figure 123 — Schema diagram – EVSEStatusType

The elements of this message are used according to Table 120.

Table 120 — Semantics and type definition for EVSEStatusType

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
NotificationMaxDelay	simpleType: xs:unsignedShort	This value is the time in seconds from the point in time this message is sent (relative time) and expected to perform the action immediately. The SECC uses the NotificationMaxDelay element in the EVSEStatus to indicate the time until it expects the EVCC to react on the action request indicated in EVSENotification.
EVSENotification	simpleType: EVSENotificationType Enumeration refer to Annex A for the type definition	This value is used by the SECC to influence the behavior of the EVCC. The EVSENotification contains an action that the SECC wants the EVCC to perform. The requested action is expected by the EVCC until the time provided in NotificationMaxDelay. If the target time is not in the future, the EVCC is expected to perform the action immediately. Requestable actions are: – ScheduleRenegotiation, – ServiceRenegotiation, – MeteringConfirmation, – Pause, – ExitStandby, – Terminate.

8.3.5.3.27 ListOfRootCertificateIDsType

[V2G20-1339] The SECC and the EVCC shall implement this type as defined in Table 121 and Figure 124.

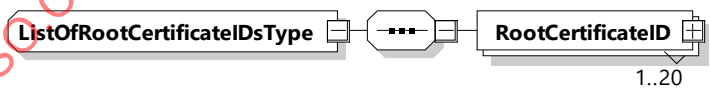


Figure 124 — Schema diagram – ListOfRootCertificateIDsType

The elements of this message are used according to Table 121.

Table 121 — Semantics and type definition for ListOfRootCertificateIDsType

Element Name	Type	Semantics
RootCertificateID	complexType: xmlsig:X509IssuerSerialType	This message element uniquely identifies a V2G root certificate installed in the EVCC.

8.3.5.3.28 DisplayParametersType

[V2G20-1343] The SECC and the EVCC shall implement this type as defined in Table 122 and Figure 125.

NOTE 1 The DisplayParameters have no influence on the energy transfer and are optional for both sides.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

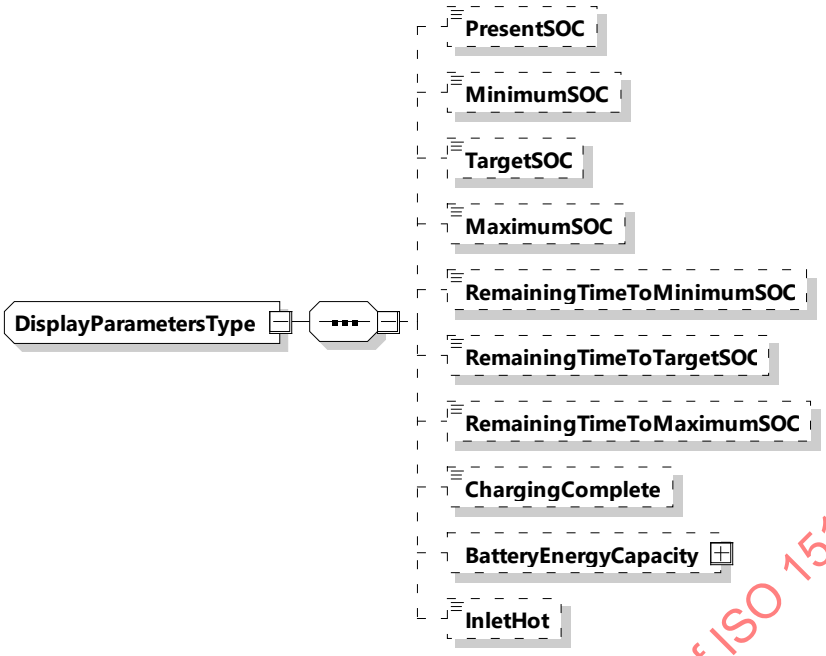


Figure 125 — Schema diagram - DisplayParametersType

The elements of this message are used according to Table 122.

Table 122 — Semantics and type definition for – DisplayParametersType

Element Name	Type	Semantics
PresentSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: Current State of Charge of the EV battery Mandatory when service parameter MobilityNeedsMode was set to 2
MinimumSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: Minimum State of Charge EV needs after charging of the EV battery the EV to keep throughout the charging session. Mandatory when service parameter MobilityNeedsMode was set to 2
TargetSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: Target State of Charge of the EV battery EV needs after charging Mandatory when service parameter MobilityNeedsMode was set to 2
MaximumSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: The SOC at which the EV will prohibit any further charging.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element Name	Type	Semantics
RemainingTimeToMinimumSOC	simpleType: xs:unsignedInt	Optional: This element is used to indicate the remaining time it takes to reach the minimum SOC. It is communicated as the offset in seconds from the point in time of sending this message, which is marked in the TimeStamp element of the common V2G message header.
RemainingTimeToTargetSOC	simpleType: xs:unsignedInt	Optional: This element is used to indicate the remaining time it takes to reach the TargetSOC. It is communicated as the offset in seconds from the point in time of sending this message, which is marked in the TimeStamp element of the common V2G message header.
RemainingTimeToMaximumSOC	simpleType: xs:unsignedInt	Optional: This element is used to indicate the remaining time it takes to reach the maximum SOC. It is communicated as the offset in seconds from the point in time of sending this message, which is marked in the TimeStamp element of the common V2G message header.
ChargingComplete	simpleType: xs:boolean	Optional: Indication if the charging is complete from EV point of view (value = 1).
BatteryEnergyCapacity	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: It is the calculated amount of electrical Energy in Wh stored in the battery when the displayed SOC equals 100 %.
InletHot	simpleType: xs:boolean	Optional: Inlet temperature too high to accept specific operating condition.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

[V2G20-1340] When EVCC selects the service parameter "MobilityNeedsMode" set to 2, ChargeLoopReq shall contain a DisplayParameter with PresentSOC, TargetSOC, and MinimumSOC.

NOTE 2 For given TargetSOC, MinimumSOC and MaximumSOC values the EV in dynamic control mode will continuously estimate the amount of energy needed to reach those states. See the definition of EVTargetEnergyRequest, EVMinimumEnergyRequest, and EVMaximumEnergyRequest for more details.

8.3.5.3.29 ServiceIDListType

[V2G20-1575] The EVCC and the SECC shall implement this type as defined in Table 123 and Figure 126.

© ISO 2022 – All rights reserved

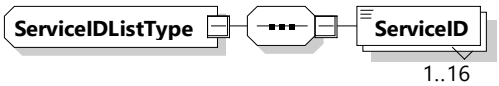


Figure 126 — Schema diagram – ServiceIDListType

The elements of this message are used according to Table 123.

Table 123 — Semantics and type definition for ServiceIDListType

Element Name	Type	Semantics
ServiceID	simpleType: serviceIDType refer to Annex A for the type definition	This element identifies a service which has been offered by the SECC in the ServiceDiscoveryRes message.

8.3.5.3.30 EMAIDListType

[V2G20-1588] The SECC and the EVCC shall implement this type as defined in Figure 127 and Table 124.

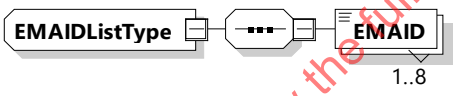


Figure 127 — Schema diagram – EMAIDListType

The elements of this message are used according to Table 124.

Table 124 — Semantics and type definition for EMAIDListType

Element Name	Type	Semantics
EMAID	simpleType identifierType refer to Annex A for the type definition	Contains the EMAID as defined in C.1.

8.3.5.3.31 EIM_AReqAuthorizationModeType

This type contains all elements of the AuthorizationReq message that are only required in case the authorization mode EIM is chosen.

[V2G20-1875] The SECC and the EVCC shall implement this type as defined in Table 125 and Figure 128.



Figure 128 — Schema diagram – EIM_AReqAuthorizationModeType

Table 125 — Semantics and type definition for EIM_AReqAuthorizationModeType

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
n/a	n/a	n/a

NOTE This parameter does not contain any elements.

8.3.5.3.32 PnC_AReqAuthorizationModeType

This type contains all elements of the AuthorizationReq message that are only required in case the authorization mode PnC is chosen.

[V2G20-1782] The SECC and the EVCC shall implement this type as defined in Table 126 and Figure 129.

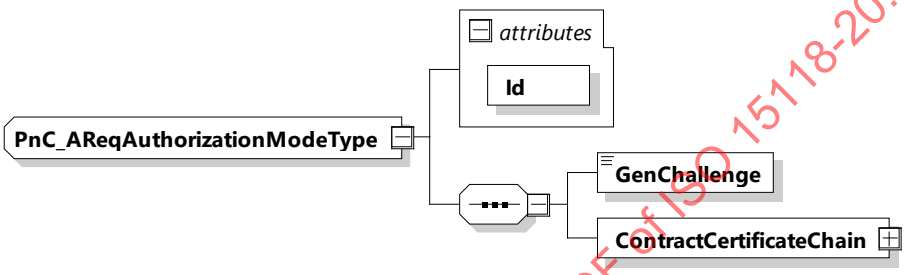


Figure 129 — Schema diagram – PnC_AReqAuthorizationModeType

The elements of this message are used according to Table 126.

Table 126 — Semantics and type definition for PnC_AReqAuthorizationModeType

Element name	Type	Semantics
Id	simpleType: xs:ID	This attribute is used for referencing the GenChallenge element in the signature header.
GenChallenge	simpleType: genChallengeType	The challenge sent by the SECC in AuthorizationSetupRes message. This element contains the generated random number.
ContractCertificateChain	complexType: ContractCertificateChainType refer 8.3.5.3.5	The certificate chain to be used for authorization of the service(s) being utilized at the EVSE.

[V2G20-2110] The GenChallenge field shall be exactly 128 bits long, as stated in [V2G20-697].

[V2G20-2107] The EVCC shall send one (1) contract certificate chain in the element ContractCertificateChain.

NOTE 1 In case EVCC contains more than one (1) contract certificate chains, it is up to the EVCC how to determine the contract certificate chain to be provided.

NOTE 2 One methodology to determine the ontract certificate chain to be provided is the use of the SupportedProviders list. Refer to 8.3.5.3.35 for more details.

8.3.5.3.33 EIM_ASResAuthorizationModeType

[V2G20-1876] The SECC and the EVCC shall implement this type as defined in Figure 130 and Table 127.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved



Figure 130 — Schema diagram – EIM_ASResAuthorizationModeType

Table 127 — Semantics and type definition for EIM_ASResAuthorizationModeType

Element name	Type	Semantics
n/a	n/a	n/a

NOTE This parameter does not contain any elements.

8.3.5.3.34 PnC_ASResAuthorizationModeType

[V2G20-1877] The SECC and the EVCC shall implement this type as defined in Table 128 and Figure 131.

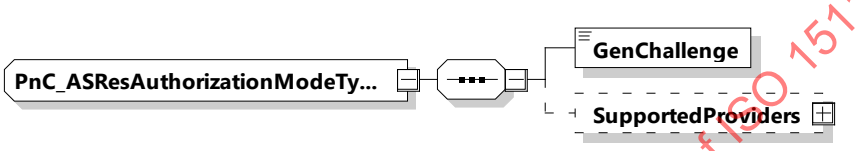


Figure 131 — Schema diagram – PnC_ASResAuthorizationModeType

The elements of this message are used according to Table 128.

Table 128 — Semantics and type definition for PnC_ASResAuthorizationModeType

Element name	Type	Semantics
GenChallenge	simpleType: genChallengeType refer to Annex A for the type definition	The challenge sent by the SECC in AuthorizationSetupRes message. This element contains the generated random number.
SupportedProviders	complexType: SupportedProvidersListType refer to 8.3.5.3.35 for the type definition	Optional: Provides a list of eMSPs supported by the SECC. This parameter allows EVCC to filter the list of contract certificates to be utilized during the payment authorization. Refer to 8.3.4.3.3.1 for further details.

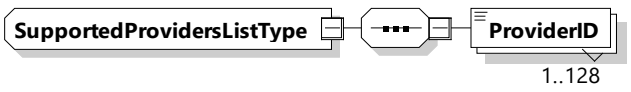
[V2G20-697] The GenChallenge field shall be exactly 128 bits long.

[V2G20-2108] GenChallenge shall be generated per random number generation requirements as defined by 7.3.7.

[V2G20-698] The entropy of the GenChallenge field shall be at least 120 bits.

8.3.5.3.35 SupportedProvidersListType

[V2G20-2703] The SECC and the EVCC shall implement this type as defined in Figure 132 and Table 129.



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Figure 132 — Schema diagram – SupportedProvidersListType

The elements of this message are used according to Table 129.

Table 129 — Semantics and type definition for SupportedProvidersListType

Element name	Type	Semantics
ProviderID	simpleType: nameType refer to Annex A for the type definition	Alphanumeric characters referring to the eMSP. These are nominally the country code and the provider ID similar to those included in the EMAID. Refer to C.1 for more details of EMAID. The list shall be in ascending order with 0-9 followed by A-Z. All characters shall be in uppercase only. The SupportedProviders includes at least 1 Provider and may include up to 128 providers.

8.3.5.3.36 SignedMeteringDataType

[V2G20-2647] The SECC and the EVCC shall implement this type as defined in Figure 133 and Table 130.

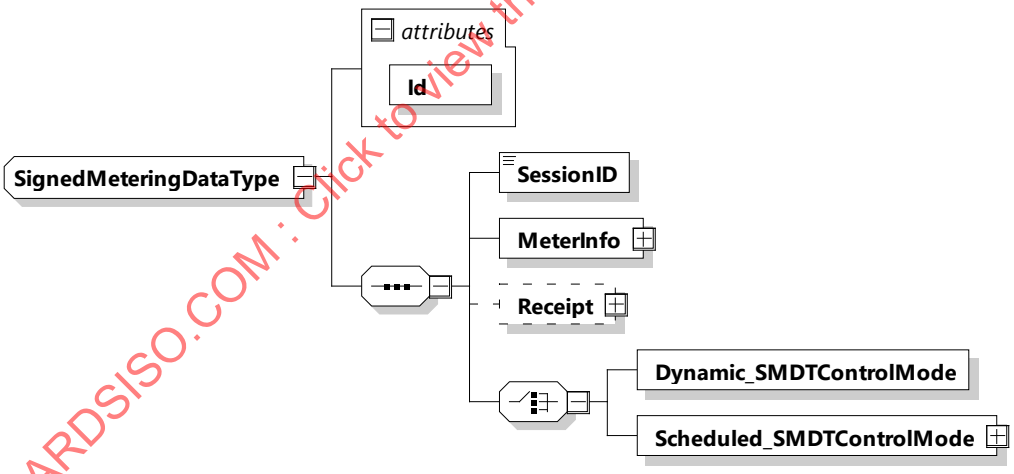


Figure 133 — Schema diagram – SignedMeteringDataType

The elements of this message are used according to Table 130.

Table 130 — Semantics and type definition for SignedMeteringDataType

Element name	Type	Semantics
SessionID	simpleType: sessionIDType refer to Annex A for the type definition	This message element is used by EVCC and SECC for uniquely identifying a V2G communication session. This element is identical with the one included in the message header. It is placed in the body in addition to be able to apply a signature to it (complete body is signed).

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
MeterInfo	complexType: MeterInfoType refer to 8.3.5.3.6 for the type definition	Includes the energy charged during this service session and other meter relevant data.
Receipt	complexType: ReceiptType refer to 8.3.5.3.59 for the type definition	Optional: Includes the receipt as provided by the SECC.
Dynamic_SMDTControlMode	complexType: Dynamic_SMDTControlModeType refer to 8.3.5.3.37 for the type definition	Contains all elements that are only required in case the dynamic control mode was chosen.
Scheduled_SMDTControlMode	complexType: Scheduled_SMDTControlModeType refer to 8.3.5.3.38 for the type definition	Contains all elements that are only required in case the scheduled control mode was chosen.

8.3.5.3.37 Dynamic_SMDTControlMode

This type contains all elements of the SignedMeteringDataType that are only required in case the dynamic control mode is chosen.

[V2G20-1875] The SECC and the EVCC shall implement this type as defined in Figure 134 and Table 131.



Figure 134 — Schema diagram – Dynamic_SMDTControlMode

Table 131 — Semantics and type definition for Dynamic_SMDTControlMode

Element name	Type	Semantics
n/a	n/a	n/a

NOTE This parameter does not contain any elements.

8.3.5.3.38 Scheduled_SMDTControlMode

This type contains all elements of the SignedMeteringDataType that are only required in case the scheduled control mode is chosen.

[V2G20-1875] The SECC and the EVCC shall implement this type as defined in Figure 135 and Table 132.

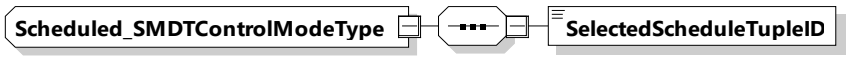


Figure 135 — Schema diagram – Scheduled_SMDTControlMode

The elements of this message are used according to Table 132.

Table 132 — Semantics and type definition for Scheduled_SMDTControlMode

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
SelectedScheduleTupleID	simpleType: numericIDType refer to Annex A for the type definition	This element includes the ScheduleTupleID the EV chose for this session.

8.3.5.3.39 SignedInstallationDataType

[V2G20-1878] The SECC and the EVCC shall implement this type as defined in Figure 136 and Table 133.

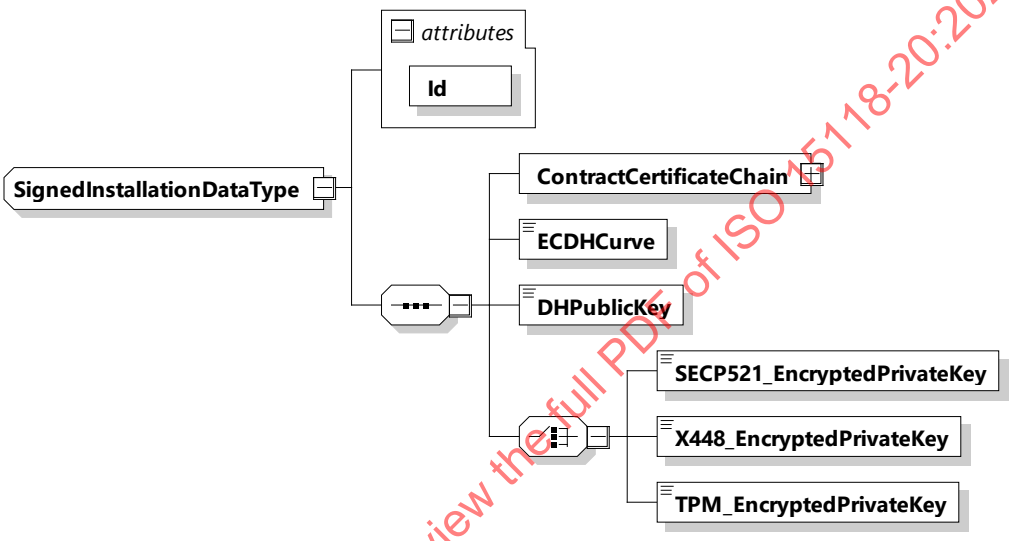


Figure 136 — Schema diagram – SignedInstallationDataType

The elements of this message are used according to Table 133.

Table 133 — Semantics and type definition for SignedInstallationDataType

Element name	Type	Semantics
ContractCertificateChain	complexType: ContractCertificateChainType refer 8.3.5.3.5	The certificate chain to be used for authorization of the service(s) being utilized at the EVSE.
ECDHCurve	simpleType: ECDHCurveType refer to Annex A for the type definition	Parameter indicating which (elliptic curve) EC the eMSP wants to use for generating the session key (seed) used to encrypt the contract certificate private key.
DHPublicKey	simpleType: dhPublicKeyType refer to Annex A for the type definition	Diffie Hellman public key from the SA for generating the session key at the EVCC in order to encrypt the contract signature private key at the SA and decrypt it a the EVCC. Refer to 7.9.2.5.4 for details.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
SECP521_EncryptedPrivateKey	simpleType: secp521_EncryptedPrivateKeyType refer to Annex A for the type definition	The 521-bit private key that belongs to the new contract certificate encrypted for EVCCs without the TPM. This is secret data and therefore shall be encrypted. Refer to 7.9.2.5.2 and its subclauses for details.
X448_EncryptedPrivateKey	simpleType: x448_EncryptedPrivateKeyType refer to Annex A for the type definition	The 448-bit private key that belongs to the new contract certificate encrypted for EVCCs without the TPM. This is secret data and therefore shall be encrypted. Refer to 7.9.2.5 and its subclauses for details.
TPM_EncryptedPrivateKey	simpleType: tpm_EncryptedPrivateKeyType refer to Annex A for the type definition	The private key that belongs to the new contract certificate encrypted for EVCCs with the TPM. This is secret data and therefore shall be encrypted. Refer to 7.9.2.5.3 and its subclauses for details.

NOTE Details of various elements in SignedInstallationDataType can be found in 7.9.2.5 and 8.3.4.3.9 and their subclauses.

8.3.5.3.40 ChargingScheduleType

[V2G20-1879] The SECC and the EVCC shall implement this type as defined in Figure 137 and Table 134.

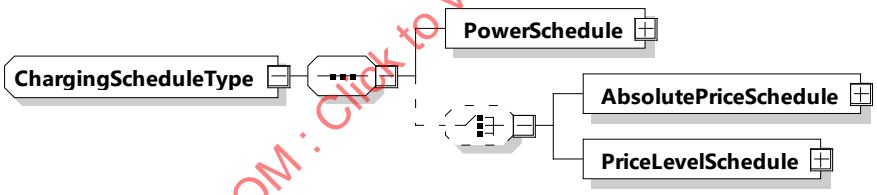


Figure 137 — Schema diagram – ChargingScheduleType

The elements of this message are used according to Table 134.

Table 134 — Semantics and type definition for ChargingScheduleType

Element name	Type	Semantics
PowerSchedule	complexType: PowerScheduleType refer to 8.3.5.3.18	Encapsulating element describing all relevant details for one PowerSchedule as defined by the secondary actor or the SECC. It is used to communicate the hard limit of charging power
AbsolutePriceSchedule	complexType: AbsolutePriceScheduleType PriceScheduleType refer to 8.3.5.3.49	Optional: Absolute Price schedule for this session

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
PriceLevelSchedule	complexType: PriceLevelScheduleType PriceScheduleType refer to 8.3.5.3.62	Optional: PriceLevel schedule for this session

[V2G20-2176] The SECC shall either provide an AbsolutePriceSchedule or a PriceLevelSchedule as part of the ChargingScheduleType.

8.3.5.3.41 EVEnergyOfferType

The EVEnergyOffer extends the scheduled control mode by adding the possibility for EVCCs to offer energy (discharging capabilities) for a certain price per kWh to the infrastructure. This offer can be included by the SECC into the DischargingSchedule and be offered back to the EVCC again. The EVPowerSchedule describes the maximum flexibility to feedback energy regarding time and power, the energy amount is limited and defined by the absolute value of EVTargetEnergyRequest. A negative value indicates the willingness to discharge under specific conditions, a positive value indicates that the EV currently is not able to offer energy to discharge.

[V2G20-1881] The SECC and the EVCC shall implement this type as defined in Figure 138 and Table 135.

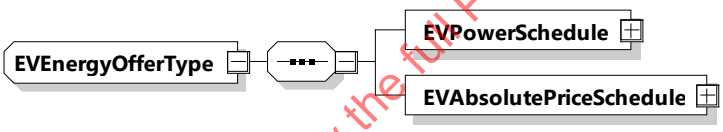


Figure 138 — Schema diagram – EVEnergyOfferType

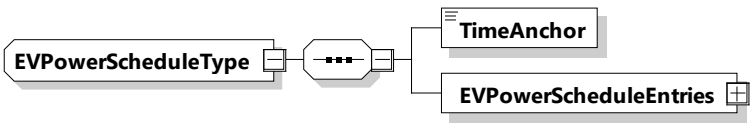
The elements of this message are used according to Table 135.

Table 135 — Semantics and type definition for EVEnergyOfferType

Element name	Type	Semantics
EVPowerSchedule	complexType: EVPowerScheduleType refer to 8.3.5.3.42	Encapsulating element describing all relevant details for one EVPowerSchedule as defined by the EVCC. It is used to communicate the hard limit of discharging power.
EVAbsolutePriceSchedule	complexType: EVAbsolutePriceScheduleType refer to 8.3.5.3.45	Optional: EVAbsolutePriceSchedule for this session. It is used to communicate the Price for which the EV offers to discharge its stored energy.

8.3.5.3.42 EVPowerScheduleType

[V2G20-1882] The SECC and the EVCC shall implement this type as defined in Figure 139 and Table 136.



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Figure 139 — Schema diagram – EVPowerScheduleType

The elements of this message are used according to Table 136.

Table 136 — Semantics and type definition for EVPowerScheduleType

Element name	Type	Semantics
TimeAnchor	simpleType: xs:unsignedLong	The time that defines the starting point for the EVEnergyOffer. The value is encoded at microseconds resolution in SECC time, a concept that is defined in 8.3.3.3.
EVPowerScheduleEntries	complexType: EVPowerScheduleEntryListType refer to 8.3.5.3.43	List of EVPowerScheduleEntry elements. The number of EVPowerScheduleEntry elements is limited by the parameter MaximumSupportingPoints (according to [V2G20-1056]).

[V2G20-2138] The TimeAnchor of an EVPowerScheduleType element shall define the point in time when the first EVPowerScheduleEntry element starts to be active.

8.3.5.3.43 EVPowerScheduleEntryListType

[V2G20-1883] The SECC and the EVCC shall implement this type as defined in Figure 140 and Table 137.

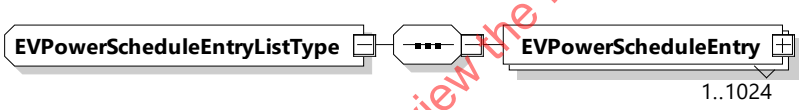


Figure 140 — Schema diagram – EVPowerScheduleEntryListType

The elements of this message are used according to Table 137.

Table 137 — Semantics and type definition for EVPowerScheduleEntryListType

Element name	Type	Semantics
EVPowerScheduleEntry	complexType: EVPowerScheduleEntryType refer to 8.3.5.3.44	List of EVPowerScheduleEntry elements. The number of EVPowerScheduleEntry elements is limited by the parameter MaximumSupportingPoints (according to [V2G20-1056]).

8.3.5.3.44 EVPowerScheduleEntryType

[V2G20-1884] The SECC and the EVCC shall implement this type as defined in Figure 141 and Table 138.

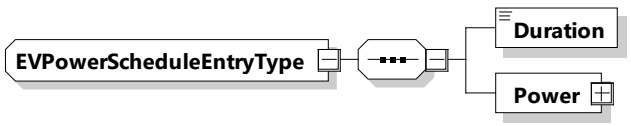


Figure 141 — Schema diagram – EVPowerScheduleEntryType

The elements of this message are used according to Table 138.

Table 138 — Semantics and type definition for EVPowerScheduleEntryType

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
Duration	simpleType: xs:unsignedInt	Duration of the EVPowerScheduleEntries. The amount of seconds that define the duration of the given EVPowerScheduleEntries.
Power	complexType: RationalNumberType refer to 8.3.5.3.8	Defines maximum amount of power for the duration of this EVPowerScheduleEntry to be discharged from the EV battery through EVSE power outlet. Negative values are used for discharging.

NOTE The precise physical meaning of Power is related to the chosen charging technology. Refer to 8.3.5.3.8.

[V2G20-2139] The duration element shall define the active period of time (s) for the respective parent element of EVPowerScheduleEntryType.

[V2G20-2140] If AC was selected as energy transfer mode, the Power element shall define the maximum amount of apparent power to be drawn from the EV when the element of type EVPowerScheduleEntryType is active. The power can freely be drawn from any phase, but the real AC polyphase discharging behavior should always respect the maximum allowed asymmetry at the grid connection point as defined by the local grid code.

[V2G20-2141] The power elements in the EVPowerScheduleType shall always be smaller or equal to zero as they communicate the discharging capabilities of the EV.

8.3.5.3.45 EVAbsolutePriceScheduleType

[V2G20-1885] The SECC and the EVCC shall implement this type as defined in Figure 142 and Table 139.

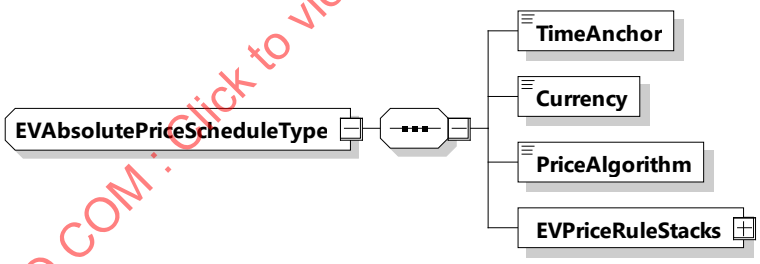


Figure 142 — Schema diagram – EVAbsolutePriceScheduleType

The elements of this message are used according to Table 139.

Table 139 — Semantics and type definition for EVAbsolutePriceScheduleType

Element name	Type	Semantics
TimeAnchor	complexType: xs:unsignedLong	The time that defines the starting point for the EVEnergyOffer. The value is encoded at microseconds resolution in SECC time, a concept that is defined in 8.3.3.3
Currency	complexType: currencyType refer to Annex A for the type definition	Currency for the pricing according to ISO 4217

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
PriceAlgorithm	simpleType: identifierType refer to Annex A for the type definition	A string in URN notation which shall uniquely identify an algorithm that defines how to compute an energy fee sum for a specific power profile based on the EnergyFee information from the EVPriceRule elements
EVPriceRuleStacks	complexType: EVPriceRuleStackListType Refer to 8.3.5.3.46	A set of pricing rules for energy costs

[V2G20-2142] Only one currency shall be used for all EVAbsolutePriceSchedules.

NOTE 1 It is possible that the currency in EVAbsolutePriceSchedules can be different from the currency in AbsolutePriceSchedule.

NOTE 2 It is up to the SECC to decide on how to react to currencies that are unexpected.

[V2G20-2143] The number of EVPriceRules shall not exceed value of MaximumSupportingPoints.

NOTE 3 For requirements and informative text regarding PriceAlgorithm, please refer to 8.3.5.3.49.1 PriceAlgorithm identifiers.

8.3.5.3.46 EVPriceRuleStackListType

[V2G20-1886] The SECC and the EVCC shall implement this type as defined in Figure 143 and Table 140.

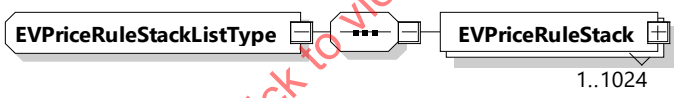


Figure 143 — Schema diagram – EVPriceRuleStackListType

The elements of this message are used according to Table 140.

Table 140 — Semantics and type definition for EVPriceRuleStackListType

Element name	Type	Semantics
EVPriceRuleStack	complexType: EVPriceRuleStackType refer to 8.3.5.3.47	Contains the EVPriceRules.

[V2G20-2144] An EVPriceRuleStack shall become active when the previous EVPriceRuleStack has expired, or when it is the first EVPriceRuleStack in the EVAbsolutePriceSchedule.

[V2G20-2145] An EVPriceRuleStack expires when the current time is greater than the starting time of the EVPriceRuleStack plus the Duration.

[V2G20-2146] The first EVPriceRule in the EVPriceRuleStack shall start at the same time as the parent EVAbsolutePriceScheduleType's TimeAnchor.

8.3.5.3.47 EVPriceRuleStackType

[V2G20-2147] The SECC and the EVCC shall implement this type as defined in Figure 144 and Table 141.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

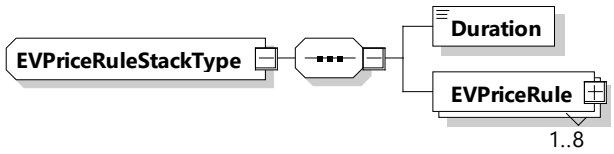


Figure 144 — Schema diagram – EVPriceRuleStackType

The elements of this message are used according to Table 141.

Table 141 — Semantics and type definition for EVPriceRuleStackType

Element name	Type	Semantics
Duration	simpleType: xs:unsignedInt	Duration of the stack of price rules. The amount of seconds that define the duration of the given EVPriceRuleStack.
EVPriceRule	complexType: EVPriceRuleType refer to 8.3.5.3.48	A set of pricing rules for energy costs.

[V2G20-2148] Overlapping (stacked) EVPriceRules shall all start at the same time.

NOTE EVPriceRulesStack allows for EVPriceRules with different PowerRangeStart values.

8.3.5.3.48 EVPriceRuleType

[V2G20-2149] The SECC and the EVCC shall implement this type as defined in Figure 145 and Table 142.

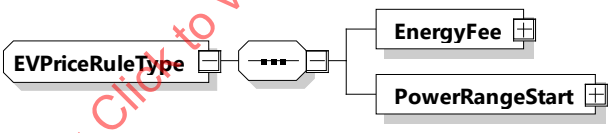


Figure 145 — Schema diagram – EVPriceRuleType

The elements of this message are used according to Table 142.

Table 142 — Semantics and type definition for EVPriceRuleType

Element name	Type	Semantics
EnergyFee	complexType: RationalNumberType refer to 8.3.5.3.8	Cost per kWh NOTE If the energy is free, then this value is zero.
PowerRangeStart	complexType: RationalNumberType refer to 8.3.5.3.8	The EnergyFee applies between this value and the value of the PowerRangeStart of the subsequent EVPriceRule. If the power is below this value, the EnergyFee of the previous EVPriceRule applies.

[V2G20-2150] An EVPriceRule shall become active when the current power is at or below the PowerRangeStart value.

[V2G20-2152] At least one active EVPriceRule shall have a PowerRangeStart with a value of zero.

[V2G20-2153] PowerRangeStart shall be less than or equal to zero.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

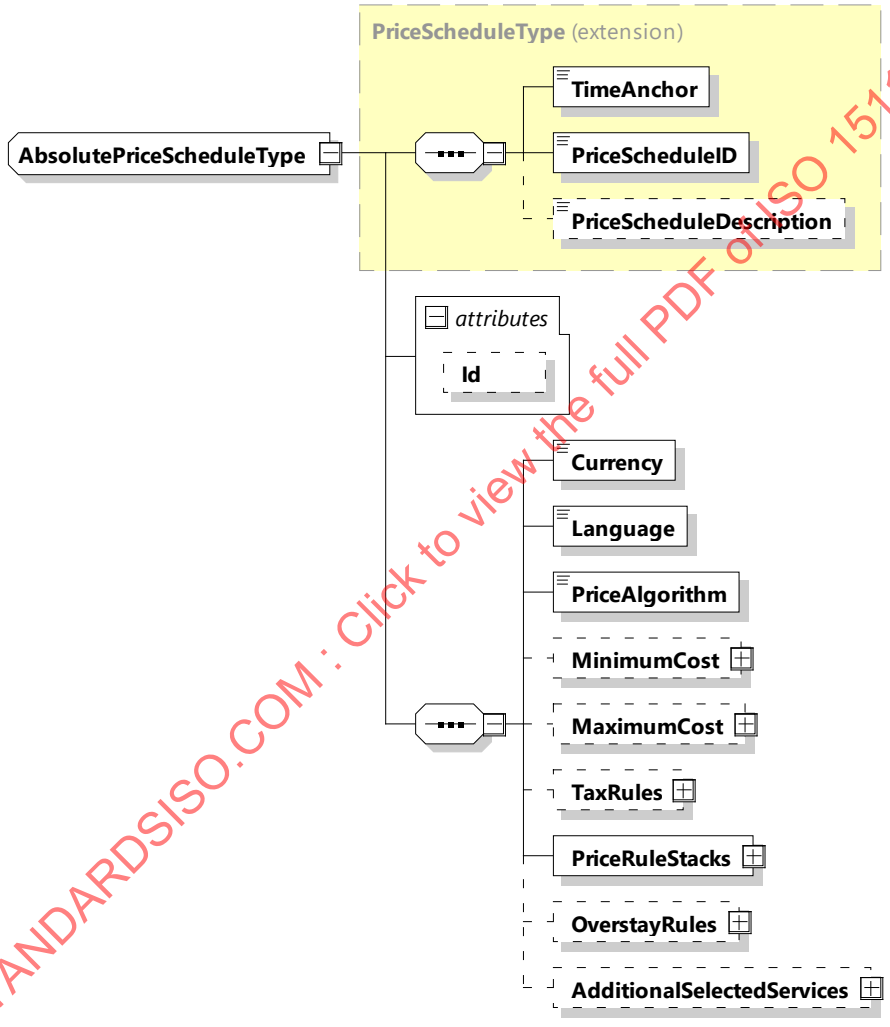
[V2G20-2154] PowerRangeStart values shall be unique within the same EVPriceRuleStack.

8.3.5.3.49 AbsolutePriceScheduleType

This type represents the actual cost for a charging session. For examples showing the usage, please refer to Annex J.

NOTE IDs within AbsolutePrice are not used in this document, rather, they are provided for informational purposes (e.g. logging).

[V2G20-1887] The SECC and the EVCC shall implement this type as defined in Figure 146 and Table 143.



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Figure 146 — Schema diagram – AbsolutePriceScheduleType

The elements of this message are used according to Table 143.

Table 143 — Semantics and type definition for AbsolutePriceScheduleType

Element name	Type	Semantics
Id	simpleType: xs:ID	This element is used for referencing the remaining elements of this table in the message header when a signature needs to be applied.

© ISO 2022 – All rights reserved

Element name	Type	Semantics
TimeAnchor	simpleType: xs:unsignedLong	The time that defines the starting point for the AbsolutePriceSchedule. The value is encoded at microseconds resolution in SECC time, a concept that is defined in 8.3.3.3
PriceScheduleID	simpleType: numericIDType refer to Annex A for the type definition	Unique ID for the price schedule.
PriceScheduleDescription	simpleType: descriptionType refer to Annex A for the type definition	Optional: Human readable text describing a schedule.
Currency	simpleType: currencyType refer to Annex A for the type definition	Currency for the pricing according to ISO 4217
Language	simpleType: languageType refer to Annex A for the type definition	String that indicates what language is used for the human readable strings in the price schedule. Based on ISO 639.
PriceAlgorithm	simpleType: identifierType refer to Annex A for the type definition	A string in URN notation which shall uniquely identify an algorithm that defines how to compute an energy fee sum for a specific power profile based on the EnergyFee information from the PriceRule elements
MinimumCost	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Minimum amount to be billed for the overall charging session (e.g. including energy, parking, and overstay)
MaximumCost	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum amount to be billed for the overall charging session (e.g. including energy, parking, and overstay)
TaxRules	complexType: TaxRuleListType refer to 8.3.5.3.50	Optional: Describes the applicable tax rule(s) for this price schedule
PriceRuleStacks	complexType: PriceRuleStackListType refer to 8.3.5.3.52	A set of pricing rules for parking and energy costs
OverstayRules	complexType OverstayRuleListType refer to 8.3.5.3.55	Optional: A set of overstay rules that allows for escalation of charges after the overstay is triggered

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
AditonalSelectedServices	complexType AdditionalServicesListType refer to 8.3.5.3.57	Optional: A set of price rules for optional services (e.g. valet, carwash)

[V2G20-1888] Only one currency shall be used for all AbsolutePriceSchedules.

NOTE 1 It is possible that the currency in EVAbsolutePriceSchedules can be different from the currency in AbsolutePriceSchedule.

NOTE 2 It is up to the SECC and EVCC to decide on how to handle currencies that are unexpected.

[V2G20-1889] The number of PriceRules shall not exceed the value of MaximumSupportingPoints.

[V2G20-1890] If MaximumCost is specified, then the element defines the maximum that may be billed.

[V2G20-1891] If MinimumCost is specified, then the element defines the minimum that may be billed.

[V2G20-2640] AdditionalSelectedServices shall not be included in the calculation of MaximumCost or MinimumCost.

[V2G20-1892] Each PriceScheduleID shall be unique.

[V2G20-1893] When a fee parameter is not sent, it shall mean this fee does not apply.

NOTE 3 This applies to all fee parameters: MaximumCost, MinimumCost, EnergyFee, ParkingFee and ServiceFee.

8.3.5.3.49.1 PriceAlgorithm identifiers

This document defines three identifiers for the PriceAlgorithm element:

- urn:iso:std:iso:15118:-20:PriceAlgorithm:1-Power;
- urn:iso:std:iso:15118:-20:PriceAlgorithm:2-PeakPower;
- urn:iso:std:iso:15118:-20:PriceAlgorithm:3-StackedEnergy.

Their definition is based on the following, generic observations, which are illustrated in Figure 147, Figure 148 and Figure 149. In Figure 147, the example is for a set of PriceRule elements and their associated EnergyFee definitions. In the first hour after midnight (00:00) a PowerSchedule limit of 15 kW is in place and only one PriceRule exists. In the next hour (01:00 to 02:00) the PowerSchedule limit has increased to 30 kW and there are three different PriceRule entries, which are stacked based on their PowerRangeStart value. The pictured EnergyFee values are just examples and not relevant for the definition of the PriceAlgorithm choices.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

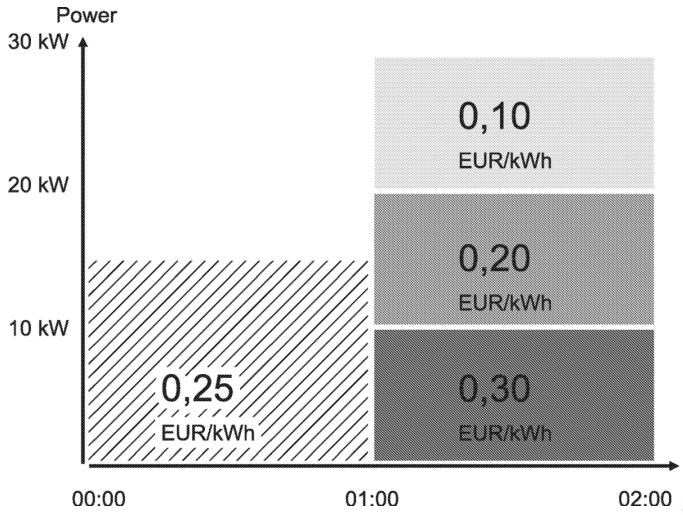


Figure 147 — Example for a set of PriceRule elements and their associated EnergyFee

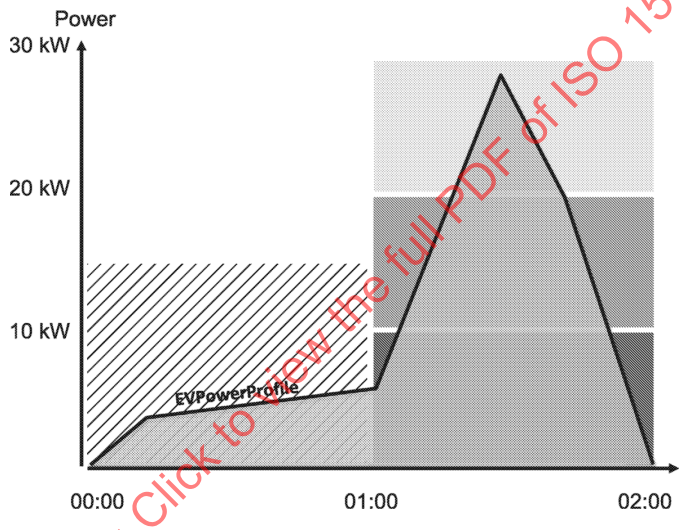


Figure 148 — Example for boundaries of different PriceRules with an EVPowerProfile

Given a hypothetical EVPowerProfile (Figure 148) each intersection of its curve with the boundaries of the different PriceRules will result in an area that defines a particular energy content.

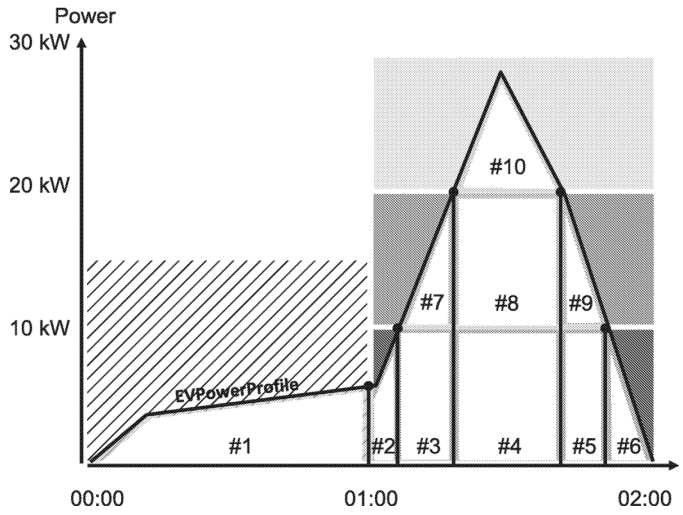


Figure 149 — Example with for the PriceAlgorithm with different PriceRules

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

In this example (Figure 149), one will end up with 10 distinct areas. While those areas are always the same each, PriceAlgorithm will apply a different rule which determines the price (EnergyFee) that each of the 10 energy content areas need to be multiplied with in order to compute and predict a resulting energy fee sum.

Figure 150, Figure 151 and Figure 152 below show how the three PriceAlgorithm options would be applied. Figure 150 shows "1-Power", Figure 151 shows "2-PeakPower" and Figure 152 shows the "3-StackedEnergy" PriceAlgorithm. The energy content of each of the 10 areas is multiplied with the EnergyFee of the PriceRule with the corresponding color and then a sum is computed.

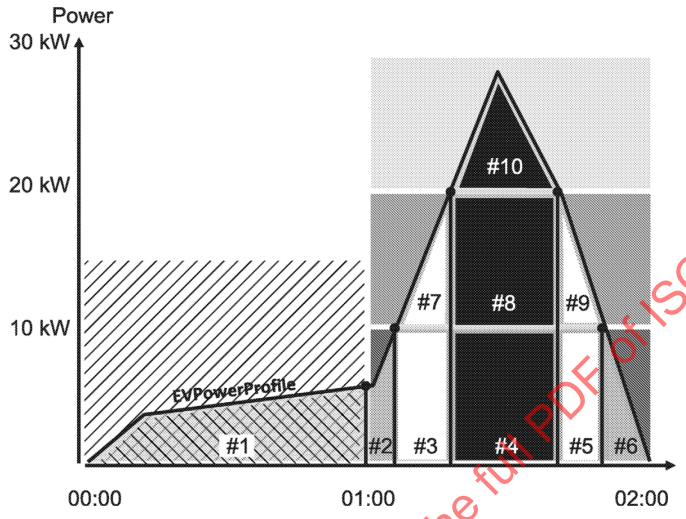


Figure 150 — Applying the PriceAlgorithm for 1-Power

[V2G20-1894] The PriceAlgorithm identifier "urn:iso:std:iso:15118:-20:PriceAlgorithm:1-Power" shall identify an algorithm that follows the principles illustrated in Figure 150. For every given point in time the EnergyFee shall be applied which is defined in the PriceRule for the present power which is applied by the chosen charging technology.

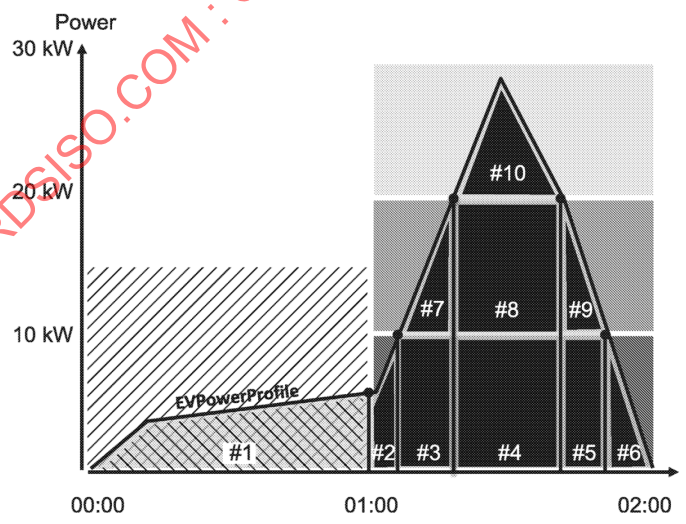


Figure 151 — Applying the PriceAlgorithm for 2-PeakPower

[V2G20-1895] The PriceAlgorithm identifier "urn:iso:std:iso:15118:-20:PriceAlgorithm:2-PeakPower" shall identify an algorithm that follows the principles illustrated in Figure 151. For every time span with one or multiple stacked PriceRules, all energy within that time span shall be priced according to the EnergyFee defined in the PriceRule that matches the highest peak power applied by the chosen charging technology during that time span.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

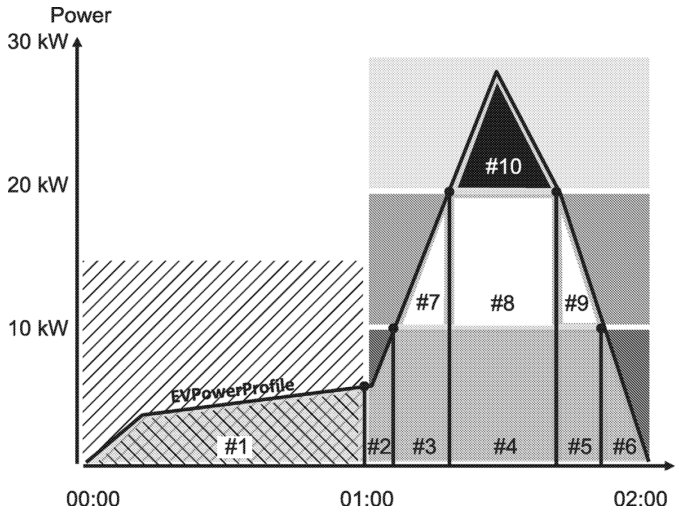


Figure 152 — Applying the PriceAlgorithm for 3-StackedEnergy

[V2G20-1896] The PriceAlgorithm identifier "urn:iso:std:iso:15118:-20:PriceAlgorithm:3-StackedEnergy" shall identify an algorithm that follows the principles illustrated in Figure 152. Energy shall be priced based on the EnergyFee defined in the PriceRules to the individual power bands and the amount of energy that was transferred within each corresponding power band.

NOTE 1 During the actual charging loop the present power level which is relevant for the PriceAlgorithm can be observed by the EVCC in different ways. For AC charging it is provided by the SECC via the EVSEPresentActivePower element. For DC charging it needs be computed based on the EVSEPresentVoltage and EVSEPresentCurrent elements.

NOTE 2 The use of unique URN based identifiers for the PriceAlgorithm allows an interoperable and well defined support of future proprietary use cases like fleet applications or special algorithms which can possibly be mandated by individual national regulation.

8.3.5.3.50 TaxRuleListType

This type represents the list of tax rules to be applied to a charging session.

[V2G20-1894] The SECC and the EVCC shall implement this type as defined in Figure 153 and Table 144.

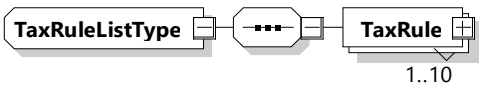


Figure 153 — Schema diagram – TaxRuleListType

The elements of this message are used according to Table 144.

Table 144 — Semantics and type definition for TaxRuleListType

Element name	Type	Semantics
TaxRule	complexType: TaxRuleType refer to 8.3.5.3.51	Individual entry of a list of tax rules

8.3.5.3.51 TaxRuleType

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

This type represents the tax rule to be applied to a charging session.

[V2G20-1898] The SECC and the EVCC shall implement this type as defined in Figure 154 and Table 145.

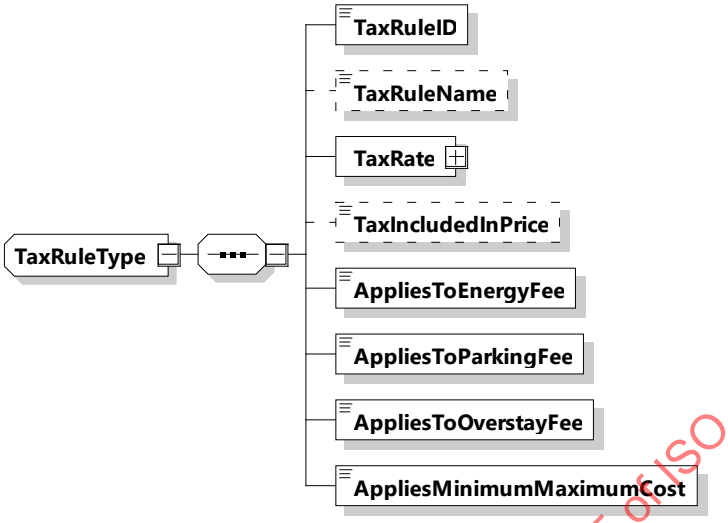


Figure 154 — Schema diagram – TaxRuleType

The elements of this message are used according to Table 145.

Table 145 — Semantics and type definition for TaxRuleType

Element name	Type	Semantics
TaxRuleID	simpleType: numericIDType refer to Annex A for the type definition	Identifier for the tax rule.
TaxRuleName	simpleType: nameType refer to Annex A for the type definition	Optional: Human readable string to identify the tax rule.
TaxRate	complexType: RationalNumberType Refer to 8.3.5.3.8	Percentage of the total amount of applying fee (energy, parking, overstay, MinimumCost and/or MaximumCost)
TaxIncludedInPrice	simpleType: xs:boolean	Optional: Indicates whether the tax is included in any price or not.
AppliesToEnergyFee	simpleType: xs:boolean	Indicates whether this tax applies to Energy Fees.
AppliesToParkingFee	simpleType: xs:boolean	Indicates whether this tax applies to Parking Fees.
AppliesToOverstayFee	simpleType: xs:boolean	Indicates whether this tax applies to Overstay Fees.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
AppliesToMinimumMaximumCost	simpleType: xs:boolean	Indicates whether this tax applies to MinimumCost and/or MaximumCost.

[V2G20-1899] Each TaxRuleID shall be unique in AbsolutePrice.

8.3.5.3.52 PriceRuleStackListType

This type contains all of the pricing rules that will apply to a charging session.

[V2G20-2155] The SECC and the EVCC shall implement this type as defined in Figure 155 and Table 146.

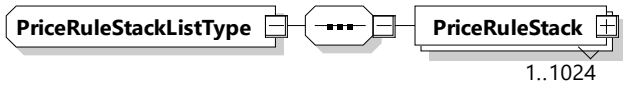


Figure 155 — Schema diagram – PriceRuleStackListType

The elements of this message are used according to Table 146.

Table 146 — Semantics and type definition for PriceRuleStackListType

Element name	Type	Semantics
PriceRuleStack	complexType: PriceRuleStackType Refer to 8.3.5.3.53	Contains the PriceRules. The number of PriceRuleStack elements is limited by the parameter MaximumSupportingPoints (according to [V2G20-1056]).

8.3.5.3.53 PriceRuleStackType

This type represents the collection of pricing rules that will apply to a charging session. This element defines how long the various price rules will be active.

[V2G20-1900] The SECC and the EVCC shall implement this type as defined in Figure 156 and Table 147.

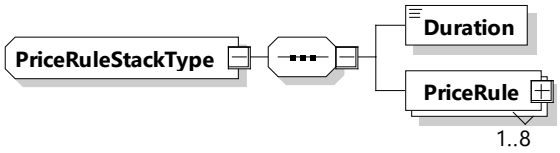


Figure 156 — Schema diagram – PriceRuleStackType

The elements of this message are used according to Table 147.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 147 — Semantics and type definition for PriceRuleStackType

Element name	Type	Semantics
Duration	simpleType: xs:unsignedInt	Duration of the stack of price rules The amount of seconds that define the duration of the given PriceRule(s). Note that this allows for roughly 17,8 h per PriceRuleStack.
PriceRule	complexType: PriceRuleType Refer to 8.3.5.3.54	Contains the PriceRule(s).

[V2G20-1901] All PriceRule elements in PriceRuleStackType shall all start at the same time.

NOTE 1 PriceRuleStack allows for PriceRule elements with different PowerRangeStart values.

[V2G20-1902] A PriceRuleStack shall become active when the previous PriceRuleStack has expired, or when it is the first PriceRuleStack in the AbsolutePriceSchedule.

[V2G20-1903] A PriceRuleStack expires when the current time is greater than the starting time of the PriceRuleStack plus the Duration.

[V2G20-1904] The first PriceRuleStack shall start at the same time as the parent AbsolutePriceScheduleType's TimeAnchor.

NOTE 2 There can be more than one PriceRule in a PriceRuleStack, in which case those PriceRule elements are stacked.

NOTE 3 If the PriceRuleStack is not intended to be stacked, then there will only be one PriceRule in that PriceRuleStack.

8.3.5.3.54 PriceRuleType

[V2G20-1764] The SECC and the EVCC shall implement this type as defined in Figure 157 and Table 148.

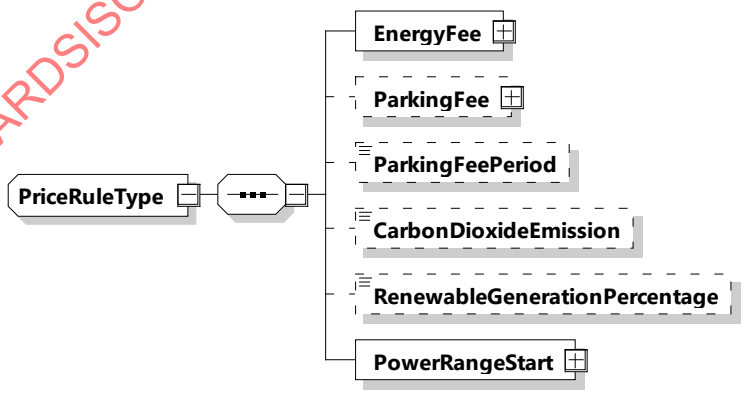


Figure 157 — Schema diagram – PriceRuleType

The elements of this message are used according to Table 148.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 148 — Semantics and type definition for PriceRuleType

Element name	Type	Semantics
EnergyFee	complexType: RationalNumberType refer to 8.3.5.3.8	Cost per kWh NOTE If the energy is free, then this value is zero.
ParkingFee	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Cost of parking. Mandatory whenever a parking fee applies.
ParkingFeePeriod	simpleType: xs:unsignedInt	Optional: The duration of the parking fee period (in seconds). When the time enters into a ParkingFeePeriod, the ParkingFee will apply to the session. Note that this is 32 bits to allow for legal requirements.
CarbonDioxideEmission	simpleType: xs:unsignedShort	Optional: Number of grams of CO2 per kWh.
RenewableGenerationPercentage	simpleType: xs:unsignedByte	Optional: Percentage of the power that is created by renewable resources.
PowerRangeStart	complexType: RationalNumberType refer to 8.3.5.3.8	For values 0 and above, this is the power level above which this price rule applies. If there is another PriceRule with a higher value, and the current power is above that value, then that other PriceRule applies. For negative values, this is the power level below which this price rule applies. If there is another PriceRule with a lower value, and the current power is below that value, then that other PriceRule applies.

[V2G20-1905] A PriceRule with a PowerRange with positive value shall become active when the current power is at or above the PowerRange value.

[V2G20-1906] A PriceRule with a PowerRange with negative value shall become active when the current power is at or below the PowerRange value.

[V2G20-1908] At least one active PriceRule shall have a PowerRangeStart with a value of zero.

[V2G20-2156] PowerRangeStart shall be greater than or equal to zero if the enclosing AbsolutePriceSchedule is used as a sub-element of a ChargingSchedule.

[V2G20-2157] PowerRangeStart shall be less than or equal to zero if the enclosing AbsolutePriceSchedule is used as a sub-element of a DischargingSchedule.

[V2G20-2158] CarbonDioxideEmission and RenewableGenerationPercentage shall only be used when the enclosing AbsolutePriceSchedule is used as a sub-element of a ChargingSchedule and the PowerRangeStart is equal to zero.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

8.3.5.3.55 OverstayRuleListType

This type represents rules used to discourage EVs from staying too long at an EVSE. The typical scenario would be an EV finishes charging, but the driver does not return to move the car for several hours causing other people to not be able to charge.

The overstay would become active by either a time trigger (OverstayTimeThreshold) or a power level trigger (OverstayPowerThreshold). Once either of those triggers become active, then the OverstayRule becomes active. The price of the overstay is defined in list of OverstayRules.

Once the overstay is triggered, the OverstayRules become active when the time from triggering is greater than their StartTime.

[V2G20-1909] The SECC and the EVCC shall implement this type as defined in Figure 158 and Table 149.

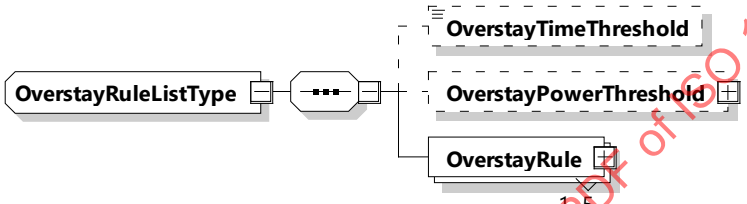


Figure 158 — Schema diagram – OverstayRuleListType

The elements of this message are used according to Table 149.

Table 149 — Semantics and type definition for OverstayRuleListType

Element name	Type	Semantics
OverstayTimeThreshold	simpleType xs:unsignedInt	Optional: Time till overstay is applied.
OverstayPowerThreshold	complexType: RationalNumberType Refer to 8.3.5.3.8	Optional: Power threshold at which the overstay applies.
OverstayRule	complexType: OverstayRuleType Refer to 8.3.5.3.56	Overstay rules that will be applied.

[V2G20-1910] There shall be only one overstay active at any time.

[V2G20-1911] The OverstayRule(s) shall become active when the time matches the OverstayTimeThreshold + the time when the OverstayRuleList became active or when the power being transferred is less than OverstayPowerThreshold.

[V2G20-1912] When a new overstay becomes active, the overstay that was previously active shall become inactive.

[V2G20-1913] Each OverstayListID shall be unique.

NOTE 1 Overstay rules are active in parallel to PriceRules.

[V2G20-2159] Once the overstay is triggered (e.g. by low power levels or timer), then the overstay remains triggered until replaced by another overstay.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2160] If OverstayPowerThreshold is set, and the power level has risen above the value, then the overstay will trigger if the power drops below this threshold.

NOTE 2 This is to prevent the overstay being triggered prior to actual power transfer.

8.3.5.3.56 OverstayRuleType

This type represents individual rules that add up to an overall overstay charge. Each of these OverstayRule elements apply relative to when the parent OverstayRules was triggered.

[V2G20-1914] The SECC and the EVCC shall implement this type as defined in Figure 159 and Table 150.

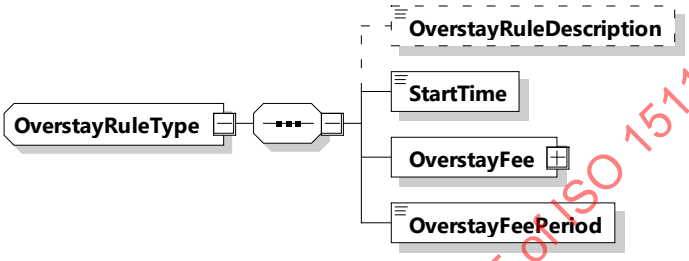


Figure 159 — Schema diagram – OverstayRuleType

The elements of this message are used according to Table 150.

Table 150 — Semantics and type definition for OverstayRuleType

Element name	Type	Semantics
OverstayRuleDescription	simpleType: descriptionType refer to Annex A for the type definition	Optional: Human readable string to identify the overstay rule.
StartTime	simpleType: xs:unsignedInt	Time in seconds after trigger of the parent OverstayRules for this particular fee to apply
OverstayFee	complexType: RationalNumberType Refer to 8.3.5.3.8	Fee that applies with this overstay
OverstayFeePeriod	simpleType: xs:unsignedInt	Time till overstay will be reapplied

[V2G20-2161] Each OverstayID shall be unique.

8.3.5.3.57 AdditionalServiceListType

This type represents the list of additional services.

[V2G20-1915] The SECC and the EVCC shall implement this type as defined in Figure 160 and Table 151.

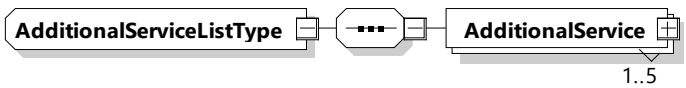


Figure 160 — Schema diagram – AdditionalServiceListType

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

The elements of this message are used according to Table 151.

Table 151 — Semantics and type definition for AdditionalServiceListType

Element name	Type	Semantics
AditonalSelectedServices	complexType: AdditionalServicesType Refer to 8.3.5.3.58	A set of price rules for optional services (e.g. valet, carwash)

8.3.5.3.58 AdditionalServiceType

This type represents rules used to describe any additional services that have already been selected, such as valet or carwash.

[V2G20-1925] The SECC and the EVCC shall implement this type as defined in Figure 161 and Table 152.

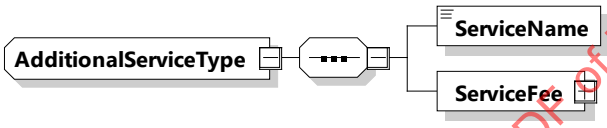


Figure 161 — Schema diagram – AdditionalServiceType

The elements of this message are used according to Table 152.

Table 152 — Semantics and type definition for AdditionalServiceType

Element name	Type	Semantics
ServiceName	simpleType: nameType refer to Annex A for the type definition	Human readable string to identify the service
ServiceFee	complexType: RationalNumberType Refer to 8.3.5.3.8	Cost of the service

[V2G20-1916] Each ServiceName shall be unique.

8.3.5.3.59 ReceiptType

This type details a transaction in the session, providing a time anchor, and information on energy costs, occupancy costs, overstay costs, taxes, and any additional services.

[V2G20-1917] The SECC and the EVCC shall implement this type as defined in Figure 162 and Table 153.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

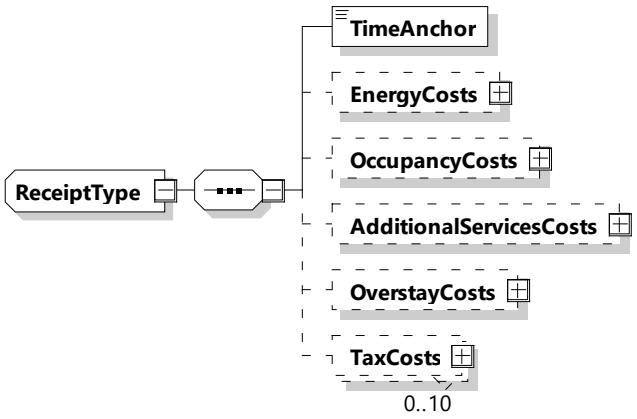


Figure 162 — Schema diagram — ReceiptType

The elements of this message are used according to Table 153.

Table 153 — Semantics and type definition for ReceiptType

Element name	Type	Semantics
TimeAnchor	simpleType: xs:unsignedLong	The time at which the receipt was issued. The value is encoded at microseconds resolution in SECC time, a concept that is defined in 8.3.3.3.
EnergyCosts	complexType: DetailedCostType refer to Annex A for the type definition	Optional: Energy cost – reported in amount (kWh) and costPerUnit (current per kWh).
OccupancyCosts	complexType: DetailedCostType refer to Annex A for the type definition	Optional: Occupancy cost – reported in amount (duration) and costPerUnit (cost per duration).
AdditionalServicesCosts	complexType: DetailedCostType refer to Annex A for the type definition	Optional: Cost of additional services – name of service, and cost of the service
OverstayCosts	complexType: DetailedCostType refer to Annex A for the type definition	Optional: Overstay cost – reported in amount (duration) and costPerUnit (current per duration).
TaxCosts	complexType: DetailedTaxType refer to 8.3.5.3.60	Optional: Tax cost – name of tax rule and cost of the tax

[V2G20-1918] There shall be at least one cost per ReceiptType.

[V2G20-1919] If the receipt is based on kWh measurements, then the associated MeterInfo shall be sent as well.

8.3.5.3.60 DetailedTaxType

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1920] The SECC and the EVCC shall implement this type as defined in Figure 163 and Table 154.

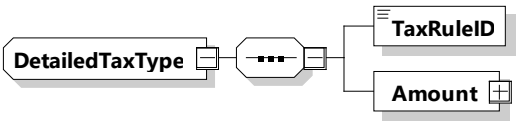


Figure 163 — Schema diagram — DetailedTaxType

The elements of this message are used according to Table 154.

Table 154 — Semantics and type definition for DetailedTaxType

Element name	Type	Semantics
TaxRuleID	simpleType: numericIDType refer to Annex A for the type definition	ID of the tax rule
Amount	complexType: RationalNumberType Refer to 8.3.5.3.8	Amount of the tax cost

8.3.5.3.61 DetailedCostType

This type is used to indicate how much a transaction cost.

[V2G20-1921] The SECC and the EVCC shall implement this type as defined in Table 155 and Figure 164.

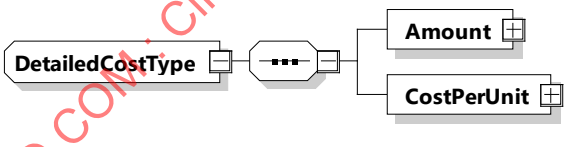


Figure 164 — Schema diagram — DetailedCostType

The elements of this message are used according to Table 155.

Table 155 — Semantics and type definition for DetailedCostType

Element name	Type	Semantics
Amount	complexType: RationalNumberType Refer to 8.3.5.3.8	How much the single transaction costs.
CostPerUnit	complexType: RationalNumberType Refer to 8.3.5.3.8	What the cost was on a per-unit basis.

8.3.5.3.62 PriceLevelScheduleType

[V2G20-1922] The SECC and the EVCC shall implement this type as defined in Figure 165 and Table 156.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

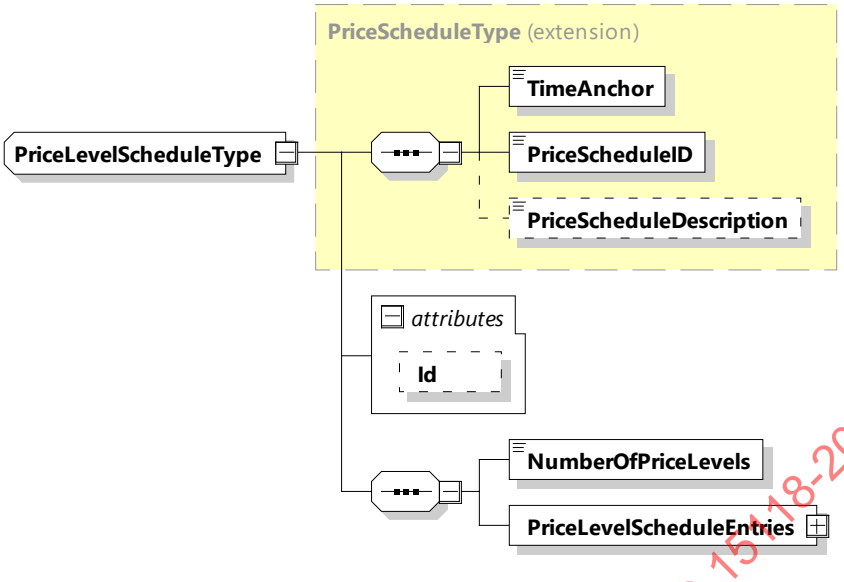


Figure 165 — Schema diagram — PriceLevelScheduleType

The elements of this message are used according to Table 156.

Table 156 — Semantics and type definition for PriceLevelScheduleType

Element name	Type	Semantics
Id	simpleType: xs:ID	This element is used for referencing this type in the message header when a signature needs to be applied.
TimeAnchor	simpleType: xs:unsignedLong	The time that defines the starting point for the PriceLevelSchedule. The value is encoded at microseconds resolution in SECC time, a concept that is defined in 8.3.3.3. In context of price level the TimeAnchor will define a time that either is the present or some point in the near past.
PriceScheduleID	simpleType: numericIDType refer to Annex A for the type definition	Unique ID for the price schedule
PriceScheduleDescription	simpleType: descriptionType refer to Annex A for the type definition	Optional: Optional description of the PriceSchedule.
NumberOfPriceLevels	simpleType: xs:unsignedByte	Defines the overall number of distinct PriceLevel elements used across all PriceLevelSchedules.
PriceLevelScheduleEntries	complexType: PriceLevelScheduleEntryListType Refer 8.3.5.3.63	List of entries of the PriceLevelSchedule

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2162] If more than one ScheduleTuple containing PriceLevelSchedule is sent to the EVCC, they shall have the same NumberOfPriceLevels and priceLevels inside different ScheduleTuples shall correspond to the same energy price.

[V2G20-2163] The TimeAnchor of a PriceLevelScheduleType element shall define a time that either is the present or some point in the near past.

[V2G20-2164] The NumberOfPriceLevels element shall be defined as the overall number of distinct PriceLevel elements used across all PriceLevelSchedules under the ScheduleTupleType elements.

EXAMPLE 1 If a PriceLevelSchedule is provided as part of the corresponding ScheduleTupleType element, where three different price levels for, for example, off-peak 0,5 € kWh ~ price level 1/3, for mid-peak 0,55 € kWh ~ price level 2/3, and for on-peak 1 € kWh ~ price level 3/3, are defined, the resulting value for NumberOfPriceLevels element is set to 3.

EXAMPLE 2 If only one flat rate PriceLevelSchedule is provided as part of the corresponding ScheduleTupleType element, with one price level at all times, the resulting value for the NumberOfPriceLevels element is set to 1.

EXAMPLE 3 If two PriceLevelSchedule are provided as part of the ScheduleTuple element, where the first PriceLevelSchedule S1 has three different price levels and the second PriceLevelSchedule S2 has another two differing price levels, the corresponding NumberOfPriceLevels element shall be set to 5.

[V2G20-2165] Both, EVCC and SECC shall support up to 100 pricelevels for the element NumberOfPriceLevels.

[V2G20-2166] In case the value of NumberOfPriceLevels is equal to "0", the value of PriceLevel shall be "0".

NOTE 1 The elements PriceLevel and NumEPriceLevels are set to "0" in case the secondary actor is not providing any price indication information for this schedule.

[V2G20-2167] A PriceLevelSchedule that is communicated as part of a ChargingScheduleType shall only present the price levels for power values that are equal to, or greater than 0 kW.

NOTE 2 For the PowerScheduleEntryType positive power values are to be used for charging of the EV.

[V2G20-2168] A PriceLevelSchedule that is communicated as part of a DischargingSchedule shall only present the price levels for all power levels that are less than 0 kW.

NOTE 3 For the PowerScheduleEntryType negative power values are to be used for discharging of the EV.

NOTE 4 A PriceLevel communicated as part of a DischargingSchedule is to be understood as indication of refund for the energy (power over duration) that is transferred from the EV into the grid.

8.3.5.3.63 PriceLevelScheduleEntryListType

[V2G20-1923] The SECC and the EVCC shall implement this type as defined in Table 157 and Figure 166.

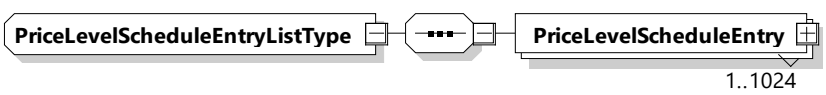


Figure 166 — Schema diagram — PriceLevelScheduleEntryListType

The elements of this message are used according to Table 157.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 157 — Semantics and type definition for PriceLevelScheduleEntryListType

Element name	Type	Semantics
PriceLevelScheduleEntry	complexType: PriceLevelScheduleEntryType refer to 8.3.5.3.64	Encapsulating element describing all relevant details for one price level entry. The number of PowerScheduleEntry elements is limited by the parameter MaximumSupportingPoints (according to [V2G20-1056]).

[V2G20-2169] The valid range for the value of the PriceLevelScheduleEntry element shall be defined as being between zero and the value of NumberOfPriceLevels element, including the boundary values.

8.3.5.3.64 PriceLevelScheduleEntryType

[V2G20-1924] The SECC and the EVCC shall implement this type as defined in Figure 167 and Table 158.

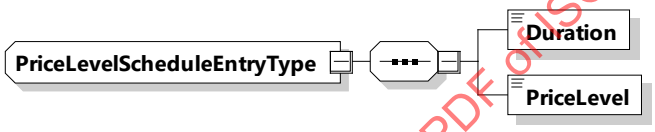


Figure 167 — Schema diagram — PriceLevelScheduleEntryType

The elements of this message are used according to Table 158.

Table 158 — Semantics and type definition for PriceLevelScheduleEntryType

Element name	Type	Semantics
Duration	simpleType: xs:unsignedInt	The amount of seconds that define the duration of the given PriceLevelScheduleEntry.
PriceLevel	simpleType: xs:unsignedByte	Defines the price level of this PriceLevelScheduleEntry (referring to NumberOfPriceLevels). Small values for the PriceLevel represent a cheaper PriceLevelScheduleEntry. Large values for the PriceLevel represent a more expensive PriceLevelScheduleEntry.

[V2G20-2170] The value of PriceLevel element shall indicate which price level is used for the duration of this PriceLevelScheduleEntry.

NOTE 1 The PriceLevel element is provided to enable the EVCC to calculate a price optimized charging profile in addition to the power limits.

NOTE 2 During the actual charging loop the present power level which is relevant for the PriceLevel can be observed by the EVCC in different ways. For AC charging it is provided by the SECC via the element EVSEPresentActivePower. For DC charging it is computed based on the EVSEPresentVoltage and EVSEPresentCurrent elements.

[V2G20-2171] The PriceLevel shall adhere to the following rule: The smaller the value for PriceLevel, the cheaper is the actual energy price level for the respective duration. The higher the value for PriceLevel, the more expensive is the actual energy price level for the respective duration.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 3 The value of PriceLevel element only defines which price level is valid for the duration of the PriceLevelScheduleEntry in the PriceLevelSchedule. The value of the PriceLevel element does not indicate the actual costs (for charging), or actual refund (for discharging) within the timeframe for which the price level is valid.

[V2G20-2172] The TimeAnchor of a PriceLevelScheduleType element shall define the point in time when the first PriceLevelScheduleEntry element starts to be active.

[V2G20-2173] The Duration element shall define the active period of time (in seconds) for the respective parent element of PriceLevelScheduleEntryType.

NOTE 4 In a list of consecutive elements the start time of the first PriceLevelScheduleEntryType element is defined by the TimeAnchor of the parent element PriceLevelScheduleType.

[V2G20-2174] The start time of each element in a list of consecutive PriceLevelScheduleEntryType elements shall be defined as the point in time when the previous element becomes inactive (see [V2G20-2173])

NOTE 5 The start time of an element is defined by the expiration of the duration of the previous element in the list of consecutive PriceLevelScheduleEntryType elements.

Before the start time of the first element and after the last element in a list of elements of type PriceLevelScheduleEntryType becomes inactive the PriceLevel is not defined. In such case it is recommended to use the schedule renegotiation mechanism in order to receive valid price level information via a new PricelevelSchedule.

8.3.5.4 AC

8.3.5.4.1 AC_CPDReqEnergyTransferModeType

[V2G20-1344] The EVCC and the SECC shall implement this type as defined in Table 159 and Figure 168.

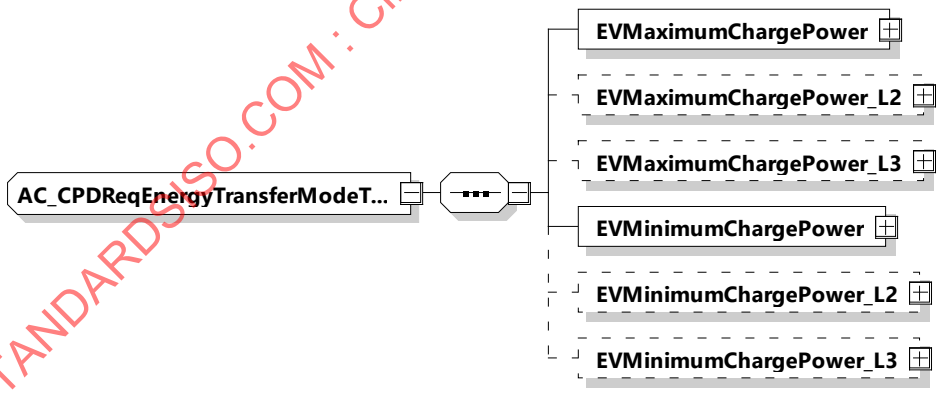


Figure 168 — Schema diagram – AC_CPDReqEnergyTransferModeType

The elements of this message are used according to Table 159.

Table 159 — Semantics and type definition for AC_CPDReqEnergyTransferModeType

Element name	Type	Semantics
EVMaximumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum power supported by the EV

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVMaximumChargePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum power supported by the EV on phase L2 (as defined in 8.3.5.2.2)
EVMaximumChargePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum power supported by the EV on phase L3 (as defined in 8.3.5.2.2)
EVMinimumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMinimumChargePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L2 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMinimumChargePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L3 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.

[V2G20-1820] In the context of ThreePhase energy transfer, if an EV is only capable of symmetric energy transfer, it shall during the ChargeParameterDiscoveryReq only communicate an EVMaximumChargePower and EVMinimumChargePower, which represent the sum of all three phases in accordance to requirement [V2G20-1814].

[V2G20-1821] In the context of ThreePhase energy transfer, if an EV is capable of asymmetric energy transfer, it shall during the ChargeParameterDiscoveryReq communicate an EVMaximumChargePower and EVMinimumChargePower with phase specific power values (see 8.3.5.2.2).

NOTE If the EVCC only sent the base elements in case of ThreePhase energy transfer in the ChargeParameterDiscoveryReq, it implicitly states that it is only capable of symmetric energy transfer. In case it sends the phase specific elements with the suffixes L2 and L3, it implicitly states, that it is capable of asymmetric energy transfer.

[V2G20-1209] SECC shall not send _L2, _L3 values in any messages (ChargeParameterDiscoveryRes, AC_ChargeLoopRes) if it neither received _L2 nor _L3 values in ChargeParameterDiscoveryReq.

[V2G20-1822] In the context of ThreePhase energy transfer, if an EV is only capable of 2 phase energy transfer, it shall during the ChargeParameterDiscoveryReq communicate its capabilities in accordance to requirement [V2G20-1821] and mark the unused phase by using the value zero.

8.3.5.4.2 AC_CPDResEnergyTransferModeType

[V2G20-1345] The EVCC and the SECC shall implement this type as defined in Table 160 and Figure 169.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

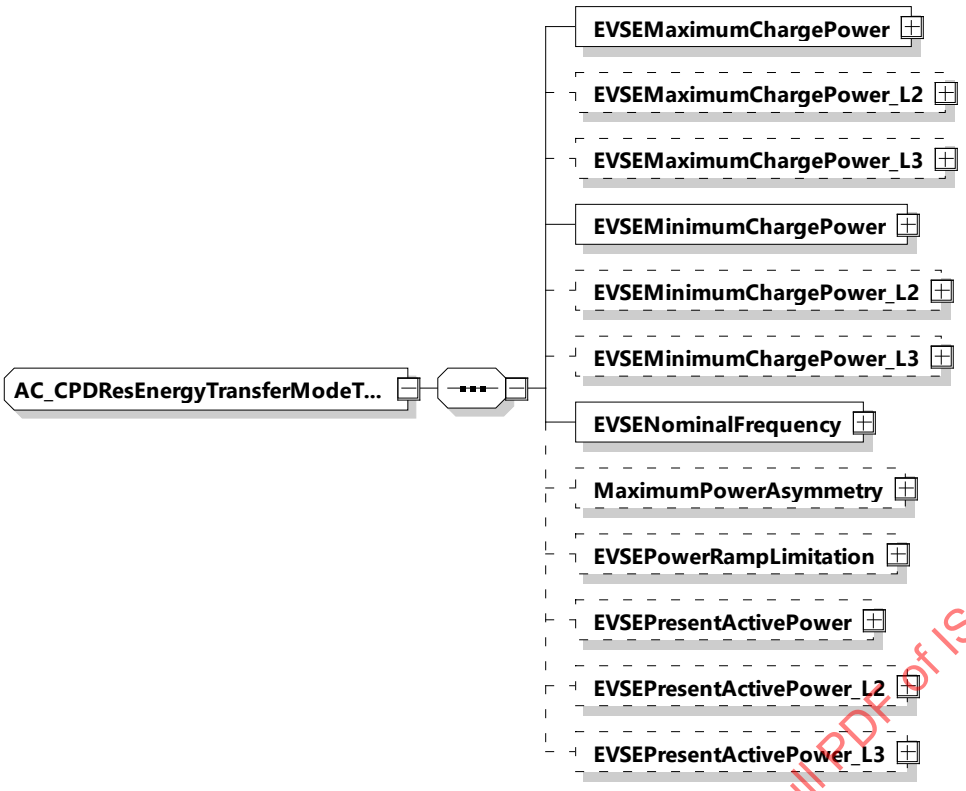


Figure 169 — Schema diagram – AC_CPDResEnergyTransferModeType

The elements of this message are used according to Table 160.

Table 160 — Semantics and type definition for AC_CPDResEnergyTransferModeType

Element name	Type	Semantics
EVSEMaximumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum power allowed by the EVSE
EVSEMaximumChargePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum power allowed by the EVSE on phase L2 (as defined in 8.3.5.2.2)
EVSEMaximumChargePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum power allowed by the EVSE on phase L3 (as defined in 8.3.5.2.2)
EVSEMinimumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts
EVSEMinimumChargePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L2 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVSEMinimumChargePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L3 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVSENominalFrequency	complexType: RationalNumberType refer to 8.3.5.3.8	This is the nominal frequency supported by the EVSE.
MaximumPowerAsymmetry	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum asymmetric power in Watt. The maximal difference in Watt between any two of the up to three available phases.
EVSEPowerRampLimitation	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Limitation of the power variation in %/min
EVSEPresentActivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE. This value is based on the actual voltage and not the EVSENominalVoltage.
EVSEPresentActivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE on phase L2 (as defined in 8.3.5.2.2). This value is based on the actual voltage and not the EVSENominalVoltage.
EVSEPresentActivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE on phase L3 (as defined in 8.3.5.2.2). This value is based on the actual voltage and not the EVSENominalVoltage.

[V2G20-1346] The EVSE shall calculate the Power values in the ScheduleTuple based on the parameter EVSENominalVoltage.

[V2G20-1347] The EVCC shall use the value EVSENominalVoltage provided by the SECC to calculate the maximum available charging current based on the Power values provided in the PowerSchedule of the ScheduleExchangeRes and the Power values in the element EVPowerProfile of the PowerDeliveryReq message.

[V2G20-1828] When charging or discharging the EV shall respect the maximum power imbalance between all 3 phases (utilized or not) using the limit defined by MaximumPowerAsymmetry. This, however, shall not apply if the power asymmetry is the result of a technique which implements a grid code requirement that has a higher priority than the static MaximumPowerAsymmetry parameter.

NOTE 1 If the element MaximumPowerAsymmetry is not present, no asymmetric limitation applies.

NOTE 2 One example for a higher priority grid code requirement would arise from the fact that asymmetry limits typically apply to the grid connection point. So if the energy management of the building sees extreme asymmetries it might compensate them. In the ISO 15118 series this would be communicated via phase specific EVSETargetActivePower(_L2/L3) values, which would override the default behavior defined in the MaximumPowerAsymmetry.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1829] The EVSEPowerRampLimitation shall be applied as a %/min factor to either the EVMaximumChargePower or the EVMaximumDischargePower in order to calculate the highest allowed absolute power change rate per minute.

[V2G20-1830] An EVSEPowerRampLimitation value of 0 %/min shall be interpreted as if the parameter was not present. In those cases the SECC does not require any local power ramp limits.

[V2G20-1831] The EVSEPowerRampLimitation shall be respected by the EV when adjusting its power level to external setpoint commands. This includes the reaction to changing maximum power levels as prescribed by the different entries in power schedules or the changes made by the EV user via other input means, like for example a mobile app.

[V2G20-1832] The EVSETargetActivePower control shall be able to override any limitation that was derived from the EVSEPowerRampLimitation. The same shall apply to any technique which implements a grid code requirement that has a higher priority than power ramp limitation.

[V2G20-1826] In scheduled control mode within the context of the AC_ChargeLoopRes the elements EVSETargetActivePower and EVSETargetReactivePower shall only be used by the SECC in situations where the technical requirements of the local grid code mandate such ad-hoc interference with the EV's power profile.

NOTE 3 A typical example is "Active response to frequency deviation - P(f)" which is mandatory in some regions even for adjustable loads when the grid enters a highly critical state (sometimes referred to as "red phase").

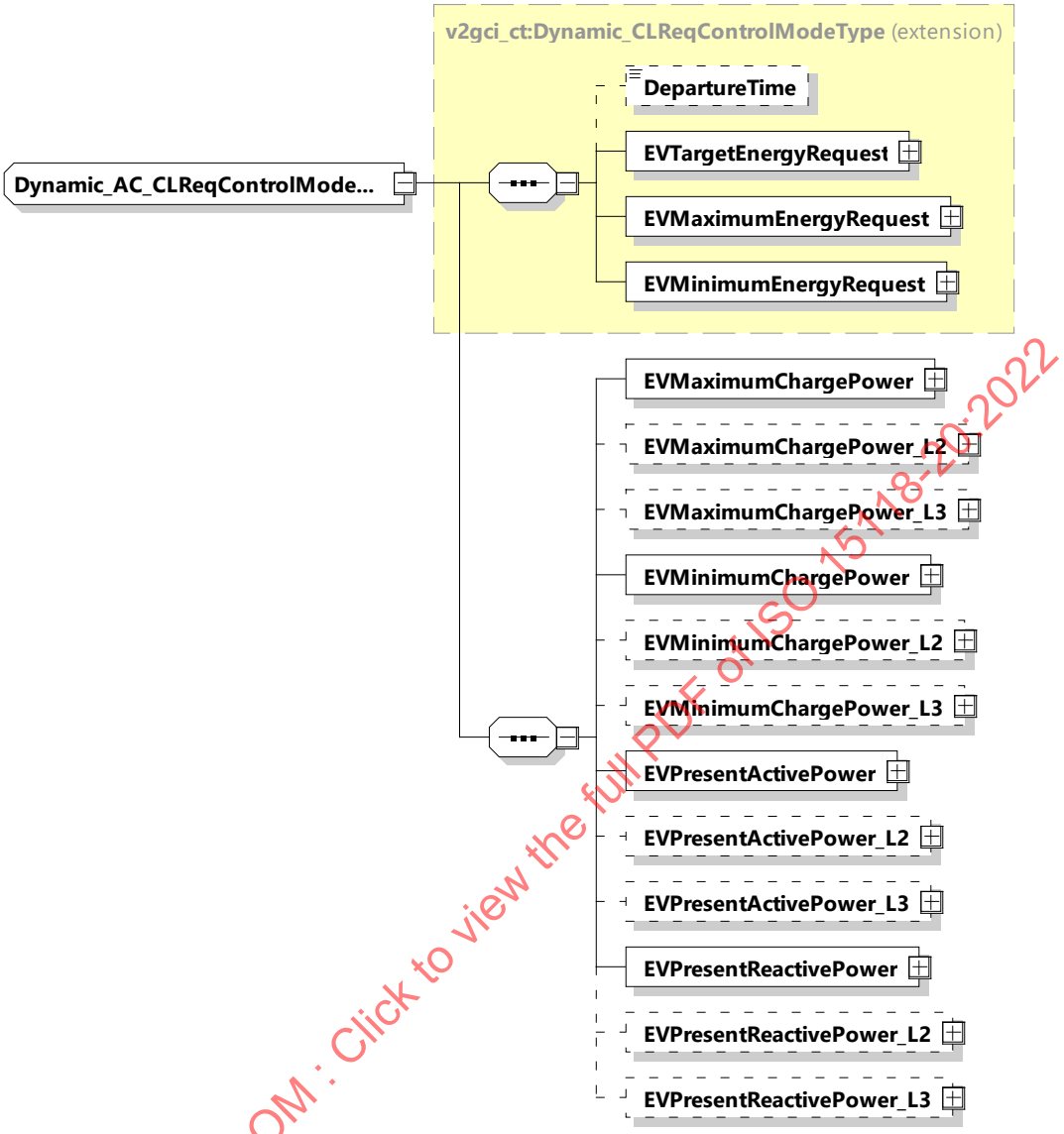
8.3.5.4.3 Dynamic_AC_CLReqControlModeType

This type contains all elements of the AC_ChargeLoopReq message that are only required in case the control mode Dynamic is chosen.

[V2G20-1758] The SECC and the EVCC shall implement this type as defined in Table 161 and Figure 170.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Figure 170 — Schema diagram – Dynamic_AC_CLReqControlModeType

The elements of this message are used according to Table 161.

Table 161 — Semantics and type definition for Dynamic_AC_CLReqControlModeType

Element name	Type	Semantics
DepartureTime	simpleType: xs:unsignedInt	Optional: DepartureTime given to the EVCC by the user, will overwrite the last given DepartureTime. This element is used to indicate when the EV intends to finish the energy transfer process. The value is encoded in seconds since the TimeStamp of the message header (see [V2G20-2104]).
EVTargetEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	The energy request of the EV it needs to fulfil the target SOC as specified by the owner.

© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVMaximumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum acceptable energy level of the EV
EVMinimumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	The energy request of the EV it needs to fulfil the minimum SOC as specified by the owner.
EVMaximumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum charge power allowed by the EV
EVMaximumChargePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum power supported by the EV on phase L2 (as defined in 8.3.5.2.2)
EVMaximumChargePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum power supported by the EV on phase L3 (as defined in 8.3.5.2.2)
EVMinimumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMinimumChargePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L2 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMinimumChargePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L3 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVPresentActivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Present active power achieved by the EV
EVPresentActivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Present active power achieved by the EV on phase L2 (as defined in 8.3.5.2.2)
EVPresentActivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Present active power achieved by the EV on phase L3 (as defined in 8.3.5.2.2)
EVPresentReactivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Present reactive power achieved by the EV
EVPresentReactivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Present reactive power achieved by the EV on phase L2 (as defined in 8.3.5.2.2)

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

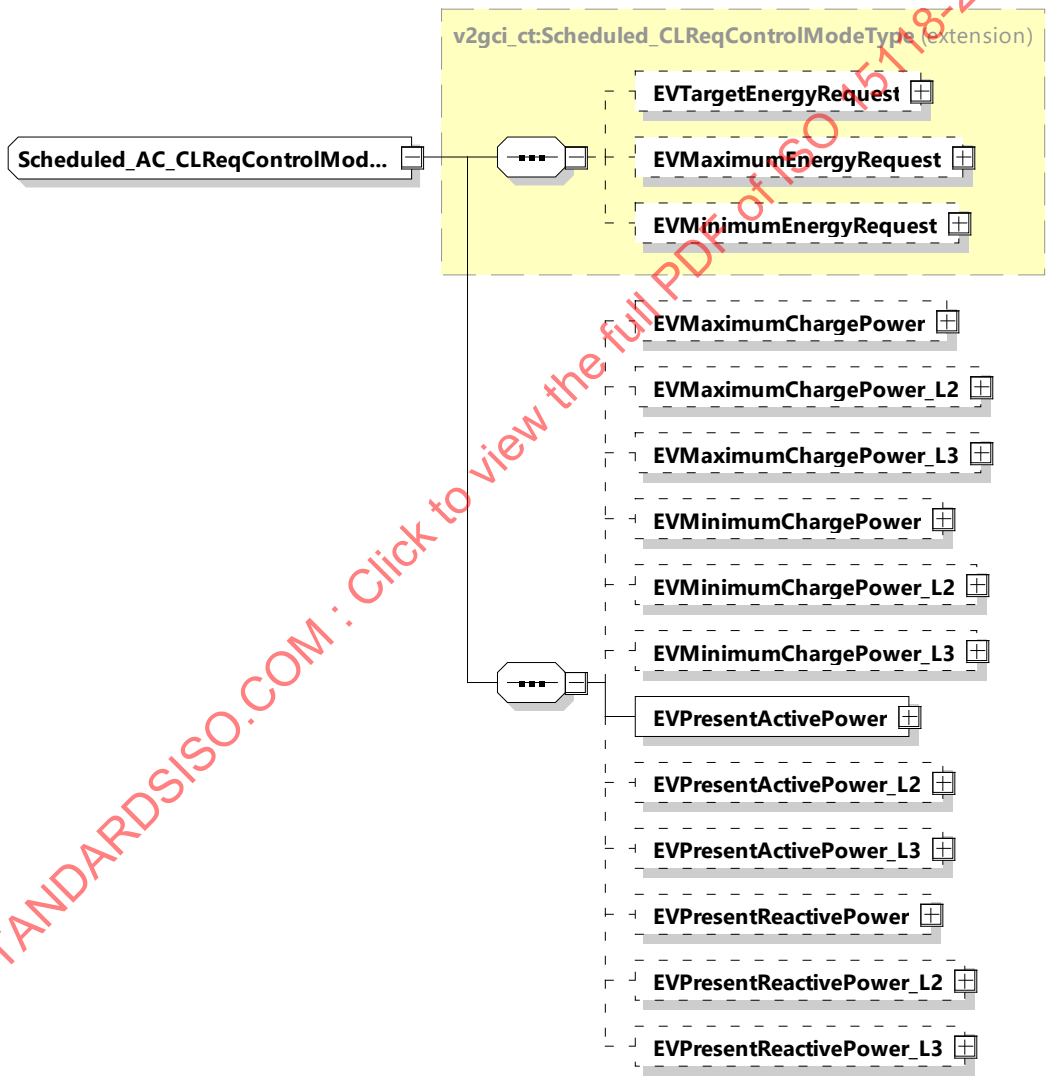
© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVPresentReactivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Present reactive power achieved by the EV on phase L3 (as defined in 8.3.5.2.2)

8.3.5.4.4 Scheduled_AC_CLReqControlModeType

This type contains all elements of the AC_ChargeLoopReq message that are only required in case the control mode Scheduled is chosen.

[V2G20-1757] The SECC and the EVCC shall implement this type as defined in Table 162 and Figure 171.



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Figure 171 — Schema diagram – Scheduled_AC_CLReqControlModeType

The elements of this message are used according to Table 162.

© ISO 2022 – All rights reserved

Table 162 — Semantics and type definition for Scheduled_AC_CLReqControlModeType

Element name	Type	Semantics
EVTargetEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: The energy request of the EV it needs to fulfil the target SOC as specified by the owner.
EVMaximumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum acceptable energy level of the EV
EVMinimumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: The energy request of the EV it needs to fulfil the minimum SOC as specified by the owner.
EVMaximumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum charge power allowed by the EV
EVMaximumChargePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum power supported by the EV on phase L2 (as defined in 8.3.5.2.2)
EVMaximumChargePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum power supported by the EV on phase L3 (as defined in 8.3.5.2.2)
EVMinimumChargePower	complexType: RationalNumberType refer to 8.5.2.5	Optional: Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMinimumChargePower_L2	complexType: RationalNumberType refer to 8.5.2.5	Optional: Any target power on phase L2 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMinimumChargePower_L3	complexType: RationalNumberType refer to 8.5.2.5	Optional: Any target power on phase L3 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVPresentActivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Present active power achieved by the EV
EVPresentActivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Present active power achieved by the EV on phase L2 (as defined in 8.3.5.2.2)
EVPresentActivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Present active power achieved by the EV on phase L3 (as defined in 8.3.5.2.2)

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVPresentReactivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Present reactive power achieved by the EV
EVPresentReactivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Present reactive power achieved by the EV on phase L2 (as defined in 8.3.5.2.2)
EVPresentReactivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Present reactive power achieved by the EV on phase L3 (as defined in 8.3.5.2.2)

8.3.5.4.5 Dynamic_AC_CLResControlModeType

This type contains all elements of the AC_ChargeLoopRes message that are only required in case the control mode Dynamic is chosen.

[V2G20-1759] The SECC and the EVCC shall implement this type as defined in Figure 172 and Table 163.

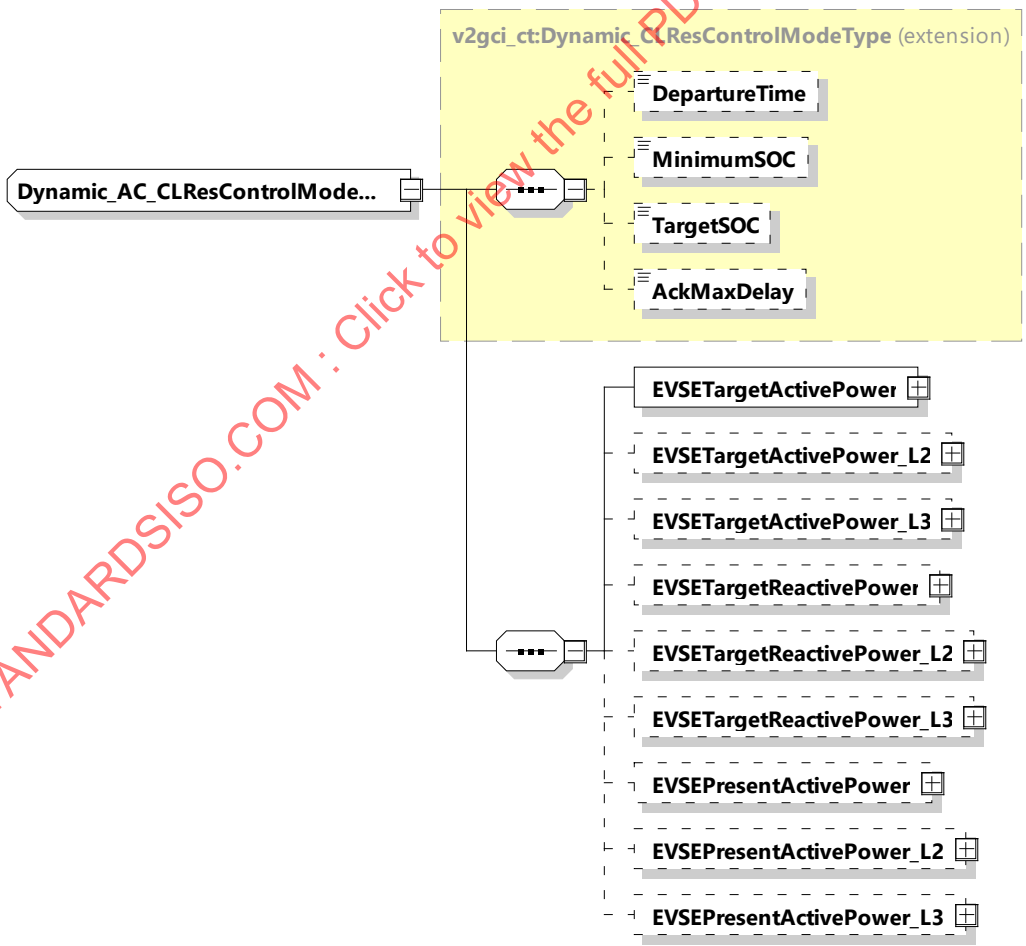


Figure 172 — Schema diagram – Dynamic_AC_CLResControlModeType

The elements of this message are used according to Table 163.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 163 — Semantics and type definition for Dynamic_AC_CLResControlModeType

Element name	Type	Semantics
DepartureTime	simpleType: xs:unsignedInt	Optional: DepartureTime given to the EVCC by the User, will overwrite the last given DepartureTime. Only used when service parameter MobilityNeedsMode was set to 2. The value is encoded in seconds since the TimeStamp of the message header (see [V2G20-2104]).
MinimumSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: New MinimumSOC value updated by the user from EVSE's side Only used when service parameter MobilityNeedsMode was set to 2.
TargetSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: New TargetSOC value updated by the user from EVSE's side. Only used when service parameter MobilityNeedsMode was set to 2
AckMaxDelay	simpleType: xs:unsignedShort	Optional: This value indicates the maximum delay in seconds that SECC expects the EVCC to apply new mobility needs (DepartureTime or TargetSOC or MinimumSOC) and send updated values in a Charge Loop message since the reception of the message stating the AckMaxDelay.
EVSETargetActivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Target active power requested by the EVSE
EVSETargetActivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target active power requested by the EVSE on phase L2 (as defined in 8.3.5.2.2)
EVSETargetActivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target active power requested by the EVSE on phase L3 (as defined in 8.3.5.2.2)
EVSETargetReactivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target reactive power requested by the EVSE
EVSETargetReactivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target reactive power requested by the EVSE on phase L2 (as defined in 8.3.5.2.2)

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVSETargetReactivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target reactive power requested by the EVSE on phase L3 (as defined in 8.3.5.2.2)
EVSEPresentActivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE. This value is based on the actual voltage and not the EVSENominalVoltage.
EVSEPresentActivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE on phase L2 (as defined in 8.3.5.2.2). This value is based on the actual voltage and not the EVSENominalVoltage.
EVSEPresentActivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE on phase L3 (as defined in 8.3.5.2.2). This value is based on the actual voltage and not the EVSENominalVoltage.

[V2G20-1366] The SECC shall only send MinimumSOC that is less than or equal to TargetSOC.

[V2G20-1367] If the EVCC selected the service parameter "MobilityNeedsMode" set to 2 and the SECC received new values for departure time, target SOC or minimum SOC from a secondary actor, the SECC shall include those updated values in DepartureTime, TargetSOC or MinimumSOC, respectively. If TargetSOC or MinimumSOC are included, then the SECC shall also include AckMaxDelay.

[V2G20-1368] If the EVCC selected the service parameter MobilityNeedsMode set to 2 and receives a AC_ChargeLoopRes message with DepartureTime, TargetSOC or MinimumSOC, and if the EVCC accepts this DepartureTime, TargetSOC or MinimumSOC, then the EVCC shall send updated values in a AC_ChargeLoopReq within the number of seconds stated in AckMaxDelay of AC_ChargeLoopRes.

[V2G20-1369] If the EVCC selected the service parameter MobilityNeedsMode set to 2 and EVCC receives a AC_ChargeLoopRes message with DepartureTime, TargetSOC or MinimumSOC, and if the EVCC cannot accept this DepartureTime, TargetSOC or MinimumSOC, e.g. for internal reasons, then the EVCC shall send different values in a AC_ChargeLoopReq than the values in AC_ChargeLoopRes within the number of seconds stated in AckMaxDelay of AC_ChargeLoopRes.

NOTE 1 In this case, the behavior of the SECC is not in the scope.

[V2G20-1210] If the charging session is subject to metering and an AbsolutePriceSchedule with power specific pricing rules has been selected, then the SECC shall provide the EVSEPresentActivePower[_L2,_L3] measurements during the charging process. The values shall reflect the same quantities which are used by the SECC to determine the pricing.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 2 Due to the uncertainties of measurement, see Annex O, and voltage drops on the cables, the EVCC can only understand how its charging behavior will impact the final bill of the customer, if the SECC provides the EVSEPresentActivePower, which is a key parameter for selecting the applied pricing rules.

8.3.5.4.6 Scheduled_AC_CLResControlModeType

[V2G20-1756] The SECC and the EVCC shall implement this type as defined in Table 164 and Figure 173.

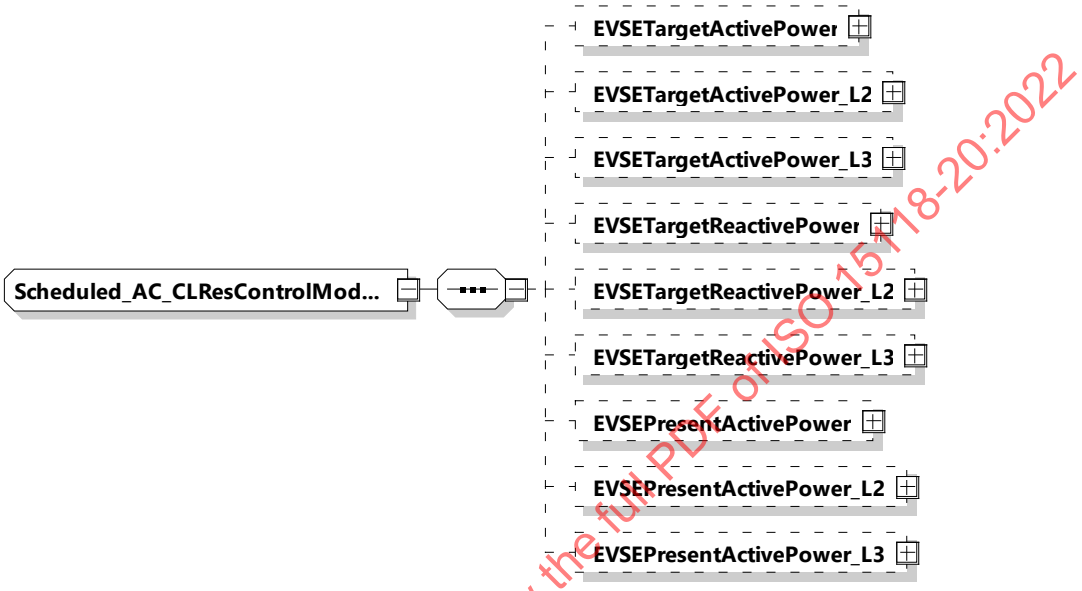


Figure 173 — Schema diagram – Scheduled_AC_CLResControlModeType

The elements of this message are used according to Table 164.

Table 164 — Semantics and type definition for Scheduled_AC_CLResControlModeType

Element name	Type	Semantics
EVSETargetActivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target active power requested by the EVSE
EVSETargetActivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target active power requested by the EVSE on phase L2 (as defined in 8.3.5.2.2)
EVSETargetActivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target active power requested by the EVSE on phase L3 (as defined in 8.3.5.2.2)
EVSETargetReactivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target reactive power requested by the EVSE
EVSETargetReactivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target reactive power requested by the EVSE on phase L2 (as defined in 8.3.5.2.2)

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVSETargetReactivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target reactive power requested by the EVSE on phase L3 (as defined in 8.3.5.2.2)
EVSEPresentActivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE. This value is based on the actual voltage and not the EVSENominalVoltage.
EVSEPresentActivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE on phase L2 (as defined in 8.3.5.2.2). This value is based on the actual voltage and not the EVSENominalVoltage.
EVSEPresentActivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE on phase L3 (as defined in 8.3.5.2.2). This value is based on the actual voltage and not the EVSENominalVoltage.

8.3.5.4.7 AC BPT

[V2G20-1213] Parameters used for discharging the EV battery shall be set with a negative value, parameters used for charging shall be set with positive value. The following shall also apply for DC BPT (refer to 8.3.5.5.7).

Additionally, a typical reverse power transfer system can be equipped with new functionalities. This induces the need to add optional parameters to existing messages which, for example, indicate the direction of the energy transfer.

The technical characteristics of reverse power transfer systems can be defined with the help of two groups of parameters:

- BPT Channel (Single channel or Dual Channel):

  This parameter describes the usage of one or two channels, i.e. current line paths, for the use of transmitting Power for Charging and/or Discharging. In the single Channel Configuration the Power Transfer Channel is shared between charging and discharging. With the dual Channel Configuration there are two separate power transfer channels, one for the charging and one for discharging.

- Generator Mode (GridFollowing or GridForming):

  The GeneratorMode parameter indicates if the system {EV + EVSE} operates as a grid following generator (only injecting active and reactive power) or as a grid forming generator, which is able to control the voltage and frequency of the network. For more details see 8.4.2.

8.3.5.4.7.1 BPT_AC_CPDReqEnergyTransferModeType

[V2G20-1456] The EVCC and the SECC shall implement this type as defined in Table 165 and Figure 174.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

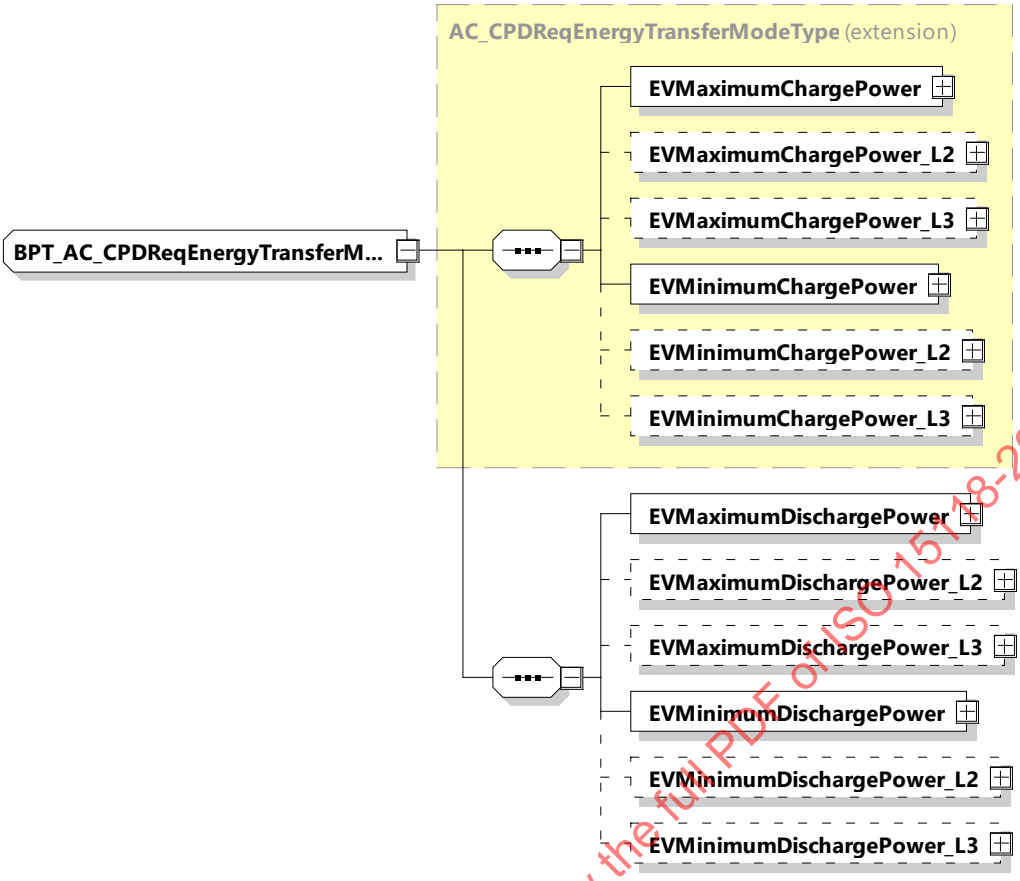


Figure 174 — Schema diagram – BPT_AC_CPDReqEnergyTransferModeType

The elements of this message are used according to Table 165.

Table 165 — Semantics and type definition for BPT_AC_CPDReqEnergyTransferModeType

Element name	Type	Semantics
EVMaximumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum charge power supported by the EV
EVMaximumChargePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum power supported by the EV on phase L2 (as defined in 8.3.5.2.2)
EVMaximumChargePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum power supported by the EV on phase L3 (as defined in 8.3.5.2.2)
EVMinimumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVMinimumChargePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L2 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMinimumChargePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L3 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMaximumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum discharge power supported by the EV
EVMaximumDischargePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum discharge power supported by the EV on phase L2 (as defined in 8.3.5.2.2)
EVMaximumDischargePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum discharge power supported by the EV on phase L3 (as defined in 8.3.5.2.2)
EVMinimumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMinimumDischargePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L2 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMinimumDischargePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L3 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

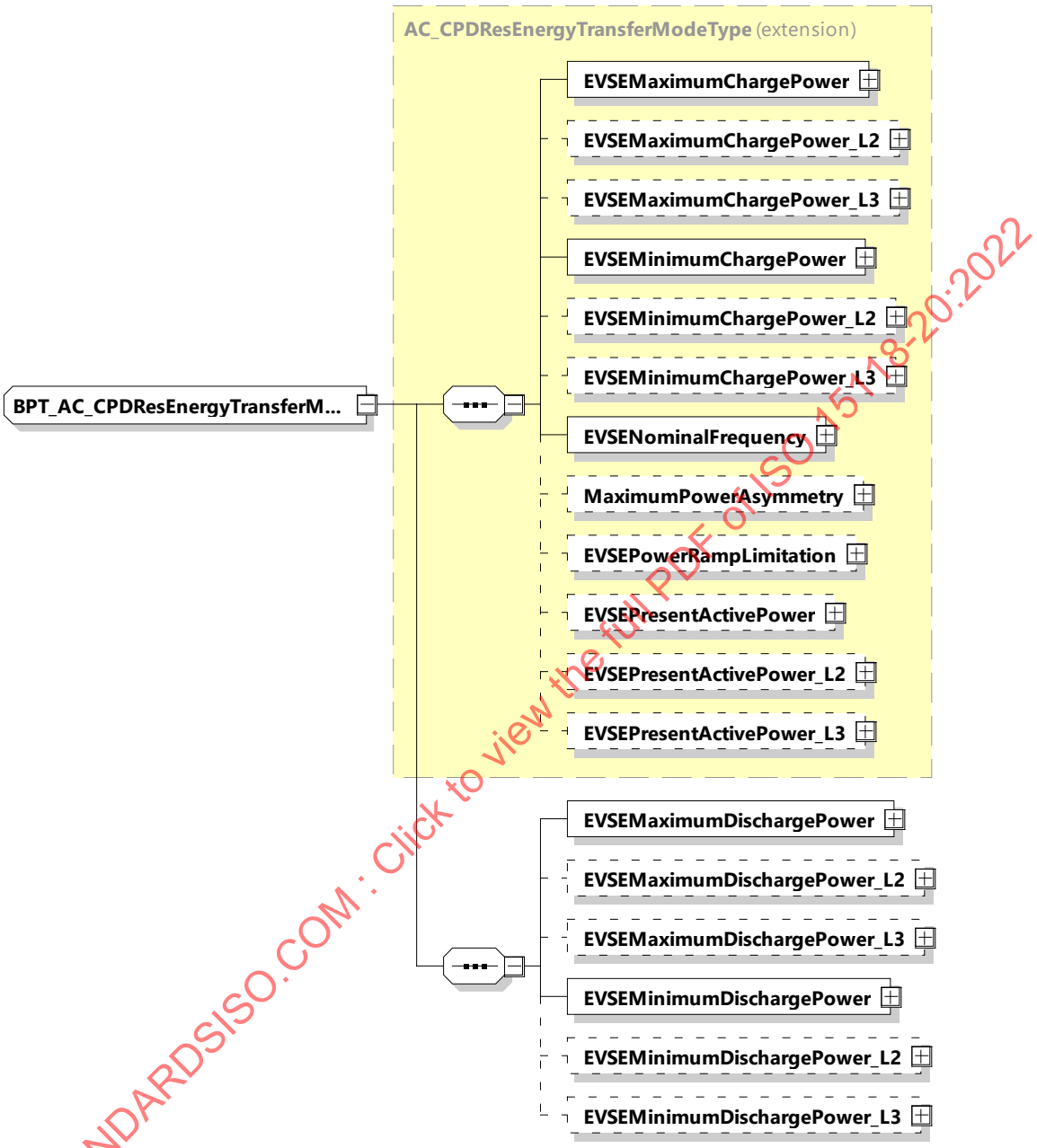
[V2G20-2656] In the context of ThreePhase energy transfer, if an EV is only capable of symmetric energy transfer, it shall during the ChargeParameterDiscoveryReq only communicate an EVMaximumChargePower, EVMinimumChargePower, EVMaximumDischargePower and EVMinimumDischargePower which represent the sum of all three phases in accordance to requirement [V2G20-1814].

[V2G20-2657] In the context of ThreePhase energy transfer, if an EV is capable of asymmetric energy transfer, it shall during the ChargeParameterDiscoveryReq communicate an EVMaximumChargePower, EVMinimumChargePower, EVMaximumDischargePower and EVMinimumDischargePower with phase specific power values (see 8.3.5.2.2).

8.3.5.4.7.2 BPT_AC_CPDResEnergyTransferModeType

© ISO 2022 – All rights reserved

[V2G20-1457] The EVCC and the SECC shall implement this type as defined Figure 175 and Table 166.



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Figure 175 — Schema diagram – BPT_AC_CPDResEnergyTransferModeType

The elements of this message are used according to Table 166.

Table 166 — Semantics and type definition for BPT_AC_CPDResEnergyTransferModeType

Element name	Type	Semantics
EVSEMaximumChargePower	complexType RationalNumberType refer to 8.3.5.3.8	Maximum power allowed by the EVSE

© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVSEMaximumChargePower_L2	complexType RationalNumberType refer to 8.3.5.3.8	Optional: Maximum power allowed by the EVSE on phase L2 (as defined in 8.3.5.2.2)
EVSEMaximumChargePower_L3	complexType RationalNumberType refer to 8.3.5.3.8	Optional: Maximum power allowed by the EVSE on phase L3 (as defined in 8.3.5.2.2)
EVSEMinimumChargePower	complexType RationalNumberType refer to 8.3.5.3.8	Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVSEMinimumChargePower_L2	complexType RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L2 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVSEMinimumChargePower_L3	complexType RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L3 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVSENominalFrequency	complexType RationalNumberType refer to 8.3.5.3.8	This is the nominal frequency supported by the EVSE.
MaximumPowerAsymmetry	complexType RationalNumberType refer to 8.3.5.3.8	Optional: Maximum asymmetric power in Watt.
EVSEPowerRampLimitation	complexType RationalNumberType refer to 8.3.5.3.8	Optional: Limitation of the power variation in %/min
EVSEPresentActivePower	complexType RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE. This value is based on the actual voltage and not the EVSENominalVoltage.
EVSEPresentActivePower_L2	complexType RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE on phase L2 (as defined in 8.3.5.2.2). This value is based on the actual voltage and not the EVSENominalVoltage.
EVSEPresentActivePower_L3	complexType RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE on phase L3 (as defined in 8.3.5.2.2). This value is based on the actual voltage and not the EVSENominalVoltage.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVSEMaximumDischargePower	complexType RationalNumberType refer to 8.3.5.3.8	Maximum power allowed by the EVSE
EVSEMaximumDischargePower_L2	complexType RationalNumberType refer to 8.3.5.3.8	Optional: Maximum power allowed by the EVSE on phase L2 (as defined in 8.3.5.2.2)
EVSEMaximumDischargePower_L3	complexType RationalNumberType refer to 8.3.5.3.8	Optional Maximum power allowed by the EVSE on phase L3 (as defined in 8.3.5.2.2)
EVSEMinimumDischargePower	complexType RationalNumberType refer to 8.3.5.3.8	Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVSEMinimumDischargePower_L2	complexType RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L2 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVSEMinimumDishargePower_L3	complexType RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L3 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.

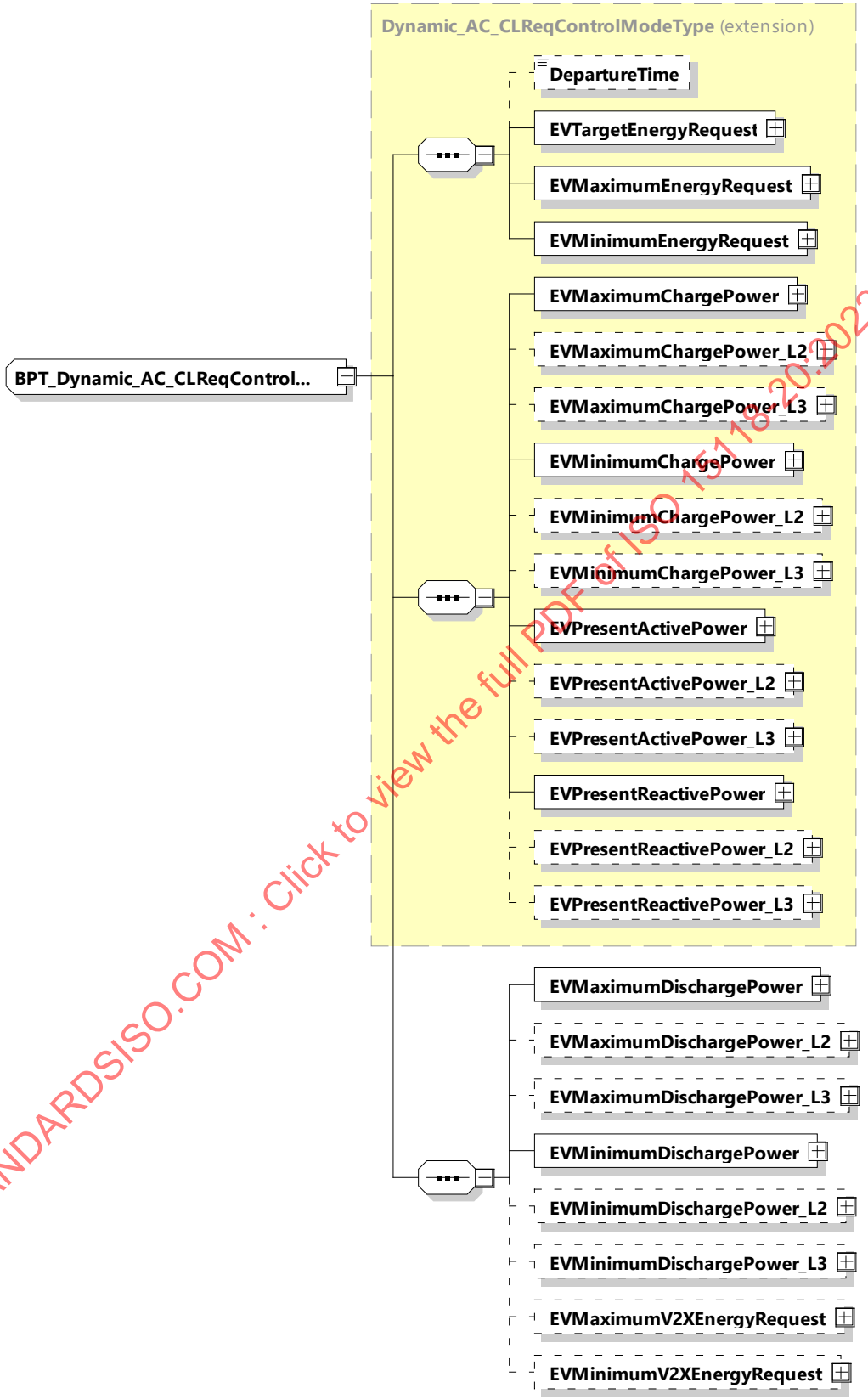
8.3.5.4.7.3 BPT_Dynamic_AC_CLReqControlModeType

This type contains all elements of the AC_ChargeLoopReq message that are only required in case the control mode Dynamic is chosen and BPT is used.

[V2G20-1768] The SECC and the EVCC shall implement this type as defined in Figure 176 and Table 167.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Figure 176 — Schema diagram – BPT_Dynamic_AC_CLReqControlModeType

The elements of this message are used according to Table 167.

© ISO 2022 – All rights reserved

Table 167 — Semantics and type definition for BPT_Dynamic_AC_CLReqControlModeType

Element name	Type	Semantics
DepartureTime	simpleType: xs:unsignedInt	Optional: DepartureTime given to the EVCC by the user, will overwrite the last given DepartureTime. This element is used to indicate when the EV intends to finish the energy transfer process. The value is encoded in seconds since the TimeStamp of the message header (see [V2G20-2104]).
EVTargetEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	The energy request of the EV it needs to fulfil the target SOC as specified by the owner.
EVMaximumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum acceptable energy level of the EV
EVMinimumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	The energy request of the EV it needs to fulfil the minimum SOC as specified by the owner
EVMaximumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum charge power allowed by the EV
EVMaximumChargePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum power supported by the EV on phase L2 (as defined in 8.3.5.2.2)
EVMaximumChargePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum power supported by the EV on phase L3 (as defined in 8.3.5.2.2)
EVMinimumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMinimumChargePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L2 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVMinimumChargePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L3 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVPresentActivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Present active power achieved by the EV
EVPresentActivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Present active power achieved by the EV on phase L2 (as defined in 8.3.5.2.2)
EVPresentActivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Present active power achieved by the EV on phase L3 (as defined in 8.3.5.2.2)
EVPresentReactivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Present reactive power achieved by the EV
EVPresentReactivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Present reactive power achieved by the EV on phase L2 (as defined in 8.3.5.2.2)
EVPresentReactivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Present reactive power achieved by the EV on phase L3 (as defined in 8.3.5.2.2)
EVMaximumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum discharge power supported by the EV
EVMaximumDischargePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum discharge power supported by the EV on phase L2 (as defined in 8.3.5.2.2)
EVMaximumDischargePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum discharge power supported by the EV on phase L3 (as defined in 8.3.5.2.2)
EVMinimumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVMinimumDischargePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L2 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMinimumDischargePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional Any target power on phase L3 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMaximumV2XEnergyRequest	complexType: rationalNumberType refer to 8.3.5.3.8	Optional: Energy which may be charged until the PresentSOC has left the range dedicated for cycling activity. A negative value indicates that PresentSOC is above the V2X range.
EVMinimumV2XEnergyRequest	complexType: rationalNumberType refer to 8.3.5.3.8	Optional: Energy which needs to be charged until the PresentSOC enters the range dedicated for cycling activity. A positive value indicates that PresentSOC is below the V2X range.

NOTE If the EVCC sends the parameters EVMaximumV2XEnergyRequest and EVMinimumV2XEnergyRequest, it is indicating a preferred operational V2X range (i.e. for bidirectional cycling) and the SECC can attempt to stay within these limits as long as possible.

[V2G20-2124] If EVMaximumV2XEnergyRequest and EVMinimumV2XEnergyRequest are sent by the EVCC, they always need to be sent together.

[V2G20-2125] If the EVCC provides EVMaximumV2XEnergyRequest and EVMinimumV2XEnergyRequest, they shall follow the following mathematical relationship:
EVMinimumEnergyRequest ≤ EVMinimumV2XEnergyRequest ≤ EVMaximumV2XEnergyRequest ≤ EVMaximumEnergyRequest

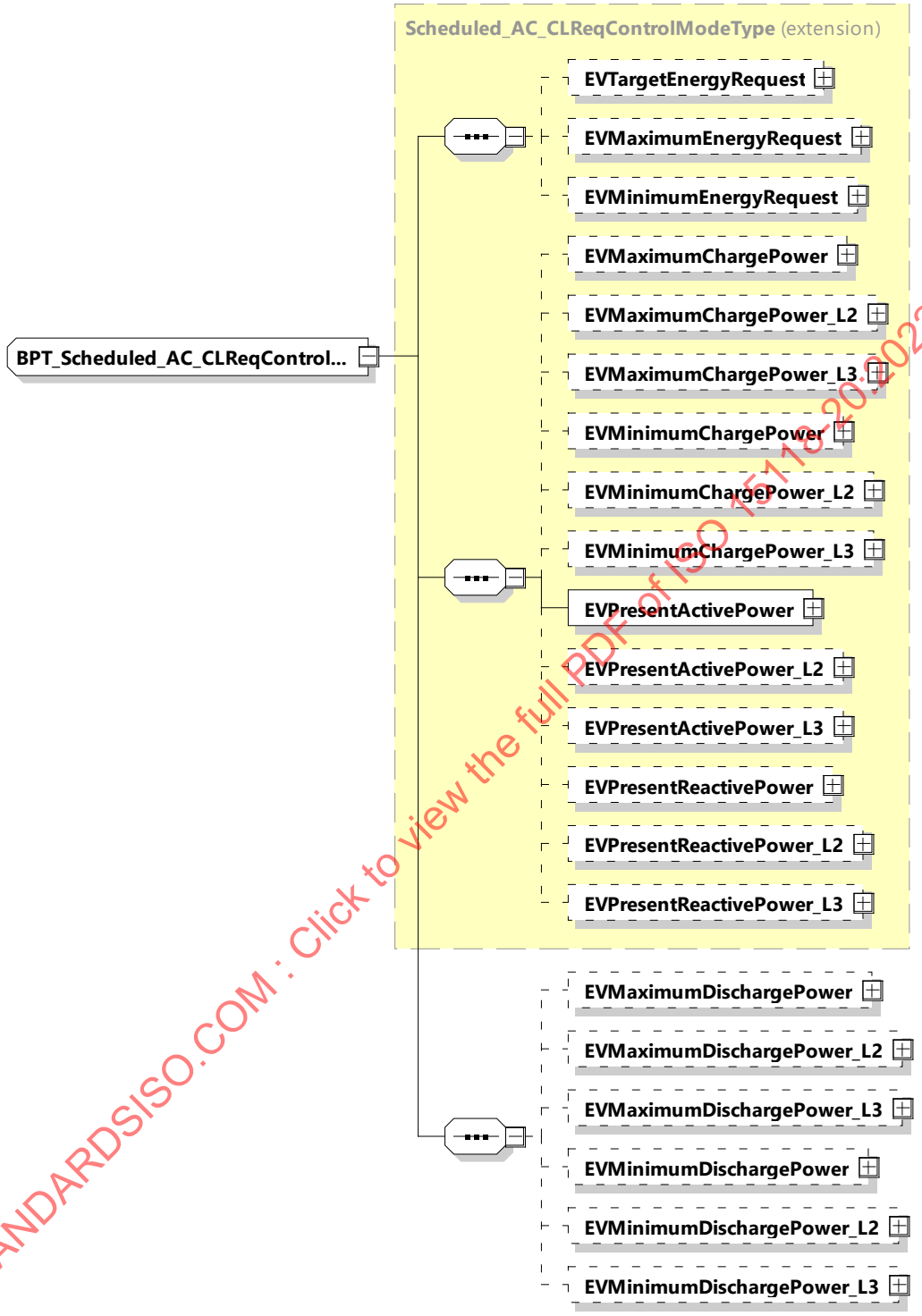
8.3.5.4.7.4 BPT_Scheduled_AC_CLReqControlModeType

This type contains all elements of the AC_ChargeLoopReq message that are only required in case the control mode Scheduled is chosen.

[V2G20-1766] The SECC and the EVCC shall implement this type as defined in Figure 177 and Table 168.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Figure 177 — Schema diagram – BPT_Scheduled_AC_CLReqControlModeType

The elements of this message are used according to Table 168.

Table 168 — Semantics and type definition for BPT_Scheduled_AC_CLReqControlModeType

© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVTargetEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: The energy request of the EV it needs to fulfil the target SOC as specified by the owner.
EVMaximumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum acceptable energy level of the EV.
EVMinimumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: The energy request of the EV it needs to fulfil the minimum SOC as specified by the owner.
EVMaximumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum charge power allowed by the EV.
EVMaximumChargePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum power supported by the EV on phase L2 (as defined in 8.3.5.2.2)
EVMaximumChargePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum power supported by the EV on phase L3 (as defined in 8.3.5.2.2).
EVMinimumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMinimumChargePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L2 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMinimumChargePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L3 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVPresentActivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Present active power achieved by the EV.
EVPresentActivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Present active power achieved by the EV on phase L2 (as defined in 8.3.5.2.2).

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVPresentActivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Present active power achieved by the EV on phase L3 (as defined in 8.3.5.2.2).
EVPresentReactivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Present reactive power achieved by the EV.
EVPresentReactivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Present reactive power achieved by the EV on phase L2 (as defined in 8.3.5.2.2)
EVPresentReactivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Present reactive power achieved by the EV on phase L3 (as defined in 8.3.5.2.2)
EVMaximumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum discharge power supported by the EV.
EVMaximumDischargePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum discharge power supported by the EV on phase L2 (as defined in 8.3.5.2.2).
EVMaximumDischargePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum discharge power supported by the EV on phase L3 (as defined in 8.3.5.2.2).
EVMinimumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMinimumDischargePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L2 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMinimumDischargePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power on phase L3 between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

8.3.5.4.7.5 BPT_Dynamic_AC_CLResControlModeType

This type contains all elements of the ACBidirectionalControlRes message that are only required in case the control mode dynamic is chosen.

© ISO 2022 – All rights reserved

[V2G20-1769] The SECC and the EVCC shall implement this type as defined in Figure 178 and Table 169.

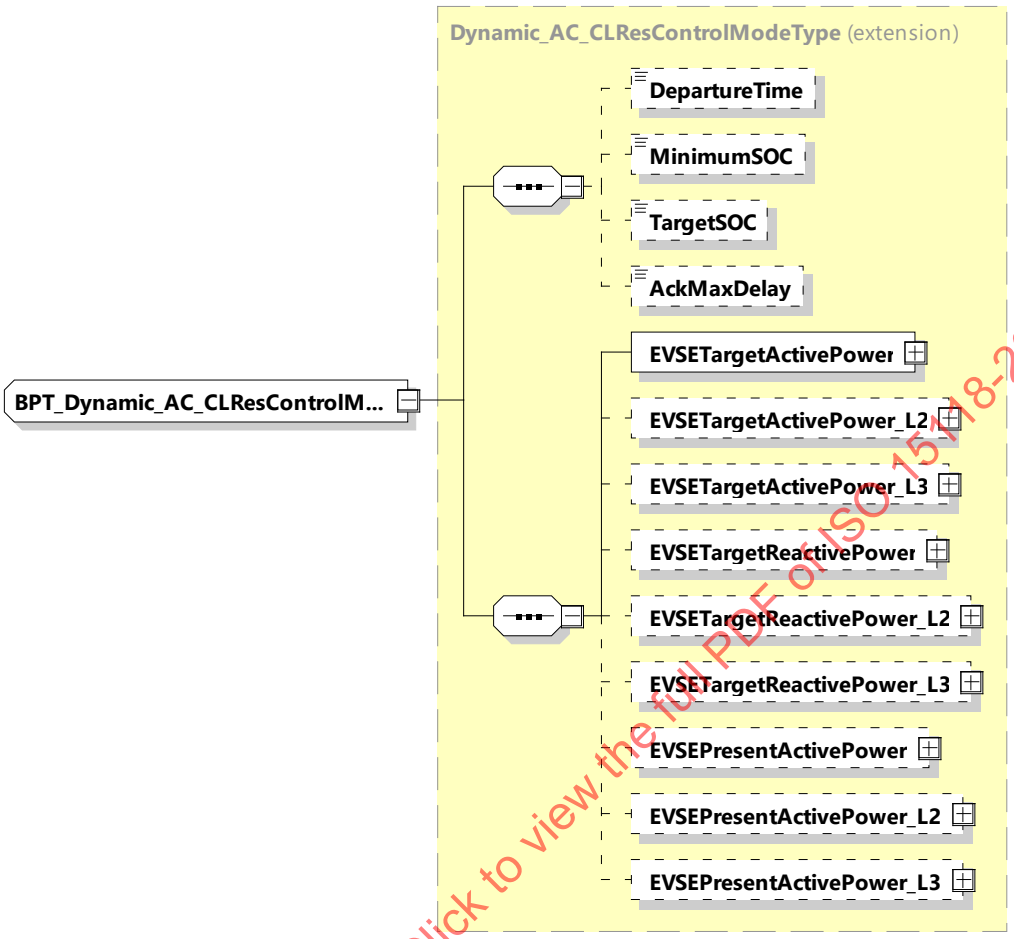


Figure 178 — Schema diagram – BPT_Dynamic_AC_CLResControlModeType

The elements of this message are used according to Table 169.

Table 169 — Semantics and type definition for BPT_Dynamic_AC_CLResControlModeType

Element name	Type	Semantics
DepartureTime	simpleType: xs:unsignedInt	Optional: This element is used to indicate when the EV intends to finish the charging process. Only used when service parameter MobilityNeedsMode was set to 2 The value is encoded in seconds since the TimeStamp of the message header (see [V2G20-2104]).
MinimumSOC	simpleType : percentValueType refer to Annex A for the type definition	Optional: New MinimumSOC value updated by the user from EVSE's side Only used when service parameter MobilityNeedsMode was set to 2.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
TargetSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: New TargetSOC value updated by the user from EVSE's side. Only used when service parameter MobilityNeedsMode was set to 2
AckMaxDelay	simpleType: xs:unsignedShort	Optional: This value indicates the maximum delay in seconds that SECC expects the EVCC to apply new mobility needs (DepartureTime or TargetSOC or MinimumSOC) and send updated values in a Charge Loop message since the reception of the message stating the AckMaxDelay.
EVSETargetActivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Target active power requested by the EVSE.
EVSETargetActivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target active power requested by the EVSE on phase L2 (as defined in 8.3.5.2.2).
EVSETargetActivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target active power requested by the EVSE on phase L3 (as defined in 8.3.5.2.2).
EVSETargetReactivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target reactive power requested by the EVSE.
EVSETargetReactivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target reactive power requested by the EVSE on phase L2 (as defined in 8.3.5.2.2).
EVSETargetReactivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target reactive power requested by the EVSE on phase L3 (as defined in 8.3.5.2.2).
EVSEPresentActivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE. This value is based on the actual voltage and not the EVSENominalVoltage.
EVSEPresentActivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE on phase L2 (as defined in 8.3.5.2.2). This value is based on the actual voltage and not the EVSENominalVoltage.
EVSEPresentActivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE on phase L3 (as defined in 8.3.5.2.2). This value is based on the actual voltage and not the EVSENominalVoltage.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2661] The SECC shall only send MinimumSOC that is less than or equal to TargetSOC.

[V2G20-2667] If the EVCC selected the service parameter "MobilityNeedsMode" set to 2 and the SECC received new values for departure time, target SOC or minimum SOC from a secondary actor, the SECC shall include those updated values in DepartureTime, TargetSOC or MinimumSOC, respectively. If TargetSOC or MinimumSOC are included, then the SECC shall also include AckMaxDelay.

[V2G20-2668] If the EVCC selected the service parameter MobilityNeedsMode set to 2 and receives a AC_ChargeLoopRes message with DepartureTime, TargetSOC or MinimumSOC, and if the EVCC accepts this DepartureTime, TargetSOC or MinimumSOC, then the EVCC shall send updated values in a AC_ChargeLoopReq within the number of seconds stated in AckMaxDelay of AC_ChargeLoopRes.

[V2G20-2669] If the EVCC selected the service parameter MobilityNeedsMode set to 2 and EVCC receives a AC_ChargeLoopRes message with DepartureTime, TargetSOC or MinimumSOC, and if the EVCC cannot accept this DepartureTime, TargetSOC or MinimumSOC, e.g. for internal reasons, then the EVCC shall send different values in a AC_ChargeLoopReq than the values in AC_ChargeLoopRes within the number of seconds stated in AckMaxDelay of AC_ChargeLoopRes.

8.3.5.4.7.6 BPT_Scheduled_AC_CLResControlModeType

This type contains all elements of the ACBidirectionalControlRes message that are only required in case the control mode Scheduled is chosen.

[V2G20-1767] The SECC and the EVCC shall implement this type as defined in Figure 179 and Table 170.

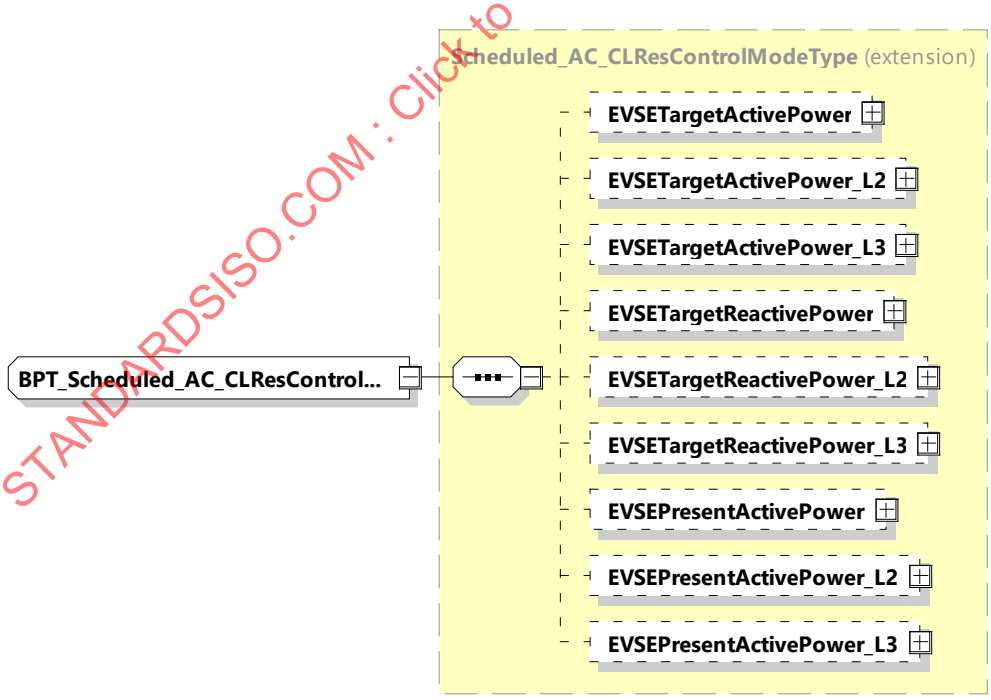


Figure 179 — Schema diagram – BPT_Scheduled_AC_CLResControlModeType

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

The elements of this message are used according to Table 170.

Table 170 — Semantics and type definition for BPT_Scheduled_AC_CLResControlModeType

Element name	Type	Semantics
EVSETargetActivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target active power requested by the EVSE.
EVSETargetActivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target active power requested by the EVSE on phase L2 (as defined in 8.3.5.2.2).
EVSETargetActivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target active power requested by the EVSE on phase L3 (as defined in 8.3.5.2.2).
EVSETargetReactivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target reactive power requested by the EVSE.
EVSETargetReactivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target reactive power requested by the EVSE on phase L2 (as defined in 8.3.5.2.2).
EVSETargetReactivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target reactive power requested by the EVSE on phase L3 (as defined in 8.3.5.2.2).
EVSEPresentActivePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE. This value is based on the actual voltage and not the EVSENominalVoltage.
EVSEPresentActivePower_L2	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE on phase L2 (as defined in 8.3.5.2.2). This value is based on the actual voltage and not the EVSENominalVoltage.
EVSEPresentActivePower_L3	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Active power as presently measured by the EVSE on phase L3 (as defined in 8.3.5.2.2). This value is based on the actual voltage and not the EVSENominalVoltage.

[V2G20-1827] In scheduled control mode, when the grid code only demands a specific reactive power behavior (e.g. resulting from a Q(U) rule, see IEEE 1547-2018 or other regional/national regulations), the SECC shall only send an EVSETargetReactivePower element without a corresponding EVSETargetActivePower element.

NOTE Q(U) requirements are often applicable during the entire operating period. The above requirement allows to satisfy grid code requirements without interfering in the normal EVPowerProfile.

8.3.5.5 DC

8.3.5.5.1 DC_CPDReqEnergyTransferModeType

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1348] The EVCC and the SECC shall implement this type as defined in Table 171 and Figure 180.

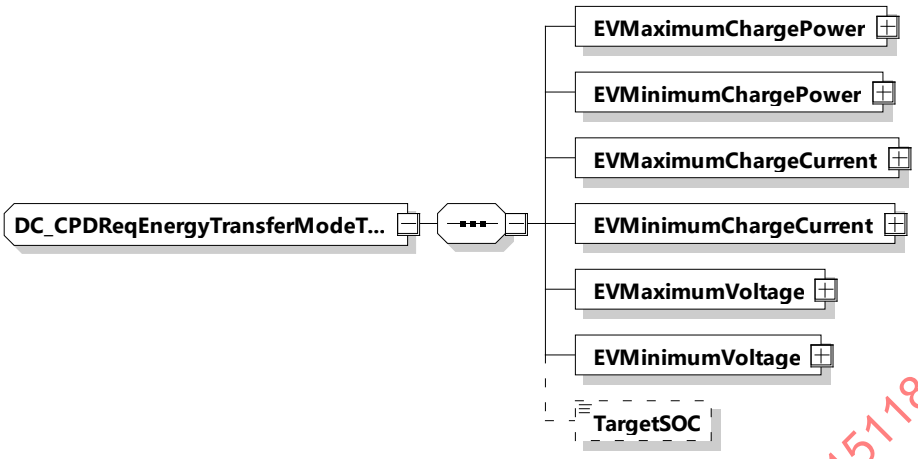


Figure 180 — Schema diagram – DC_CPDReqEnergyTransferModeType

The elements of this message are used according to Table 171.

Table 171 — Semantics and type definition for DC_CPDReqEnergyTransferModeType

Element name	Type	Semantics
EVMaximumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum charge power supported by the EV.
EVMinimumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMaximumChargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum charge current supported by the EV.
EVMinimumChargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Any target current between this level and zero may, for technical reasons, result in a drop of the actual current to zero ampere.
EVMaximumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum voltage allowed by the EV.
EVMinimumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Minimum voltage allowed by the EV.
TargetSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: SOC at which the EV considers the battery to be fully charged.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2181] During charging the SECC shall always respect the limits defined by EVMaximumChargePower, EVMaximumChargeCurrent, EVMaximumVoltage and EVMinimumVoltage.

NOTE 1 All limits are communicated in ChargeParameterDiscoveryReq initially and additionally can be updated in case of need in DC_ChargeLoopReq during the charging loop.

[V2G20-2182] During discharging the SECC shall always respect the limits defined by EVMaximumDischargePower, EVMaximumDischargeCurrent, EVMaximumVoltage and EVMinimumVoltage.

NOTE 2 All limits are communicated in ChargeParameterDiscoveryReq initially and additionally can be updated in case of need in DC_ChargeLoopReq during the charging loop.

8.3.5.5.2 DC_CPDResEnergyTransferModeType

[V2G20-1349] The EVCC and the SECC shall implement this type as defined in Table 172 and Figure 181.

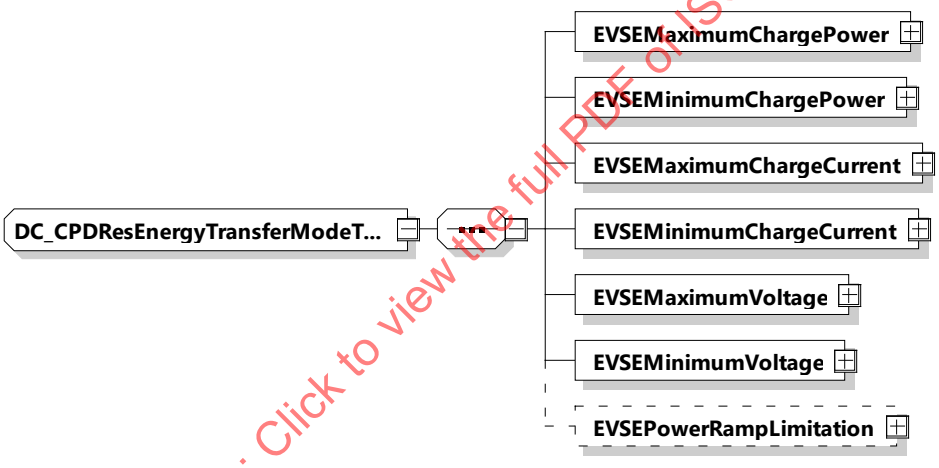


Figure 181 — Schema diagram – DC_CPDResEnergyTransferModeType

The elements of this message are used according to Table 172.

Table 172 — Semantics and type definition for DC_CPDResEnergyTransferModeType

Element name	Type	Semantics
EVSEMaximumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum power the EVSE can deliver.
EVSEMinimumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVSEMaximumChargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum current the EVSE can deliver.
EVSEMinimumChargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Minimum current the EVSE can deliver with the expected accuracy.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

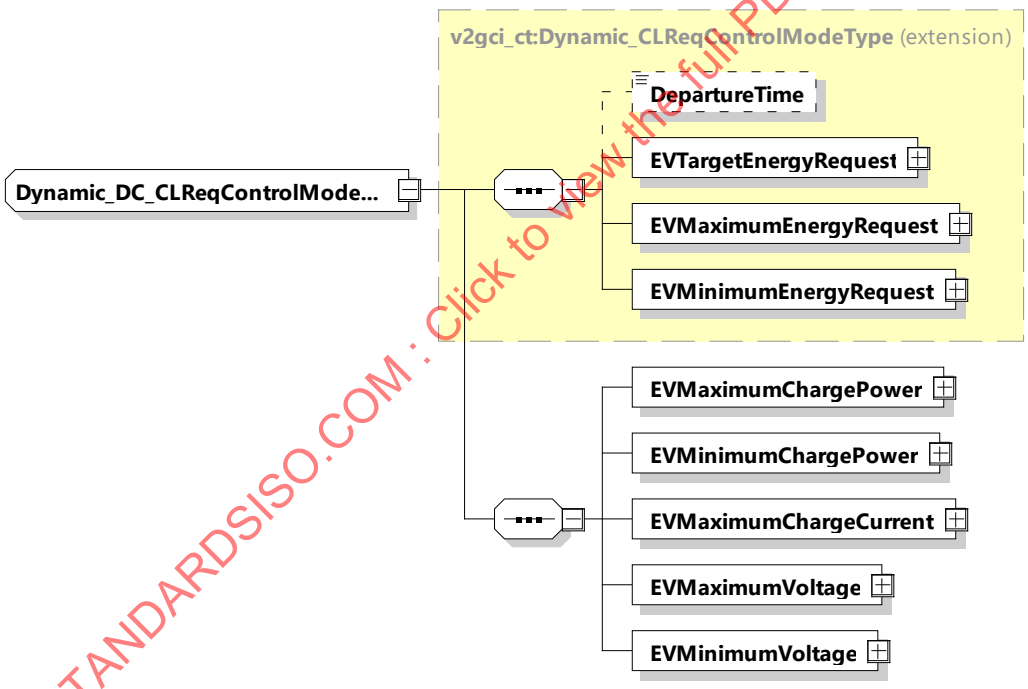
© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVSEMaximumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum voltage the EVSE can deliver.
EVSEMinimumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Minimum voltage the EVSE can deliver with the expected accuracy.
EVSEPowerRampLimitation	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Limitation of the power variation in %/min.

8.3.5.5.3 Dynamic_DC_CLReqControlModeType

This type contains all elements of the DC_ChargeLoopReq message that are only required in case the control mode Dynamic is chosen.

[V2G20-1762] The SECC and the EVCC shall implement this type as defined in Figure 182 and Table 173.



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Figure 182 — Schema diagram – Dynamic_DC_CLReqControlModeType

The elements of this message are used according to Table 173.

Table 173 — Semantics and type definition for Dynamic_DC_CLReqControlModeType

© ISO 2022 – All rights reserved

Element name	Type	Semantics
DepartureTime	simpleType: xs:unsignedInt	Optional: This element is used to indicate when the EV intends to finish the charging process. The value is encoded in seconds since the TimeStamp of the message header (see [V2G20-2104]).
EVTargetEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	The energy request of the EV it needs to fulfil the target SOC as specified by the owner.
EVMaximumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum acceptable energy level of the EV.
EVMinimumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	The energy request of the EV it needs to fulfil the minimum SOC as specified by the owner
EVMaximumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum charge power allowed by the EV.
EVMinimumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Minimum charge power allowed by the EV.
EVMaximumChargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum charge current allowed by the EV.
EVMaximumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum voltage allowed by the EV.
EVMinimumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Minimum voltage allowed by the EV.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

8.3.5.5.4 Scheduled_DC_CLReqControlModeType

This type contains all elements of the DC_ChargeLoopReq message that are only required in case the control mode Scheduled is chosen.

[V2G20-1760] The SECC and the EVCC shall implement this type as defined in Figure 183 and Table 174.

© ISO 2022 – All rights reserved

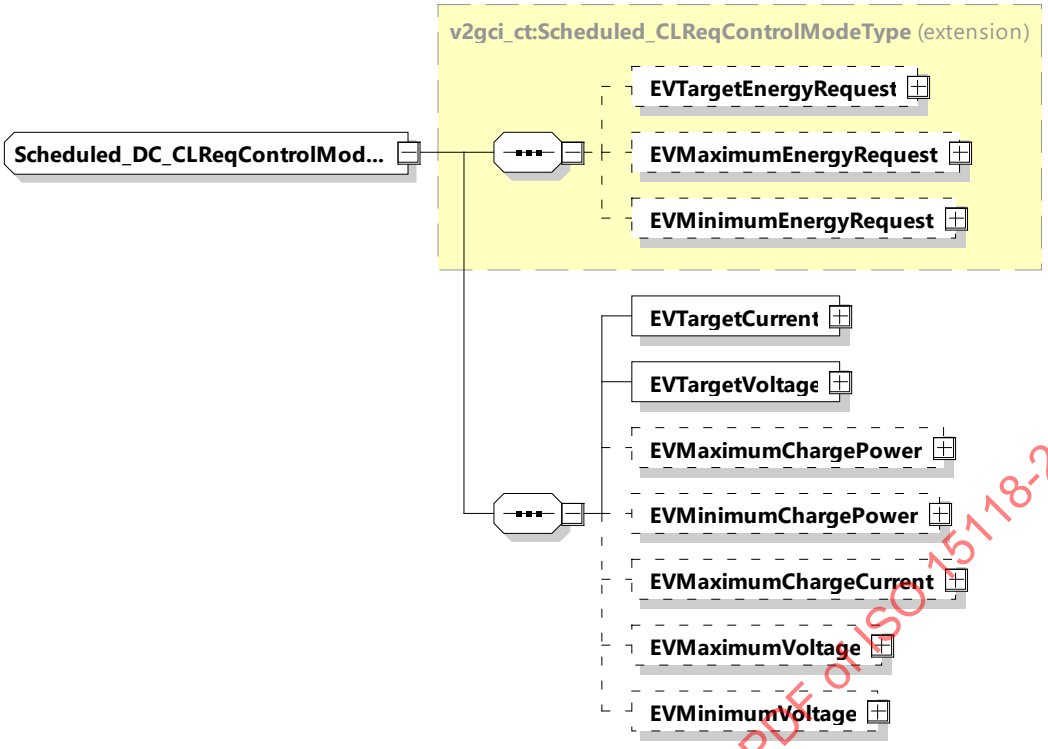


Figure 183 — Schema diagram – Scheduled_DC_CLReqControlModeType

The elements of this message are used according to Table 174.

Table 174 — Semantics and type definition for Scheduled_DC_CLReqControlModeType

Element name	Type	Semantics
EVTargetEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: The energy request of the EV it needs to fulfil the target SOC as specified by the owner.
EVMaximumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum acceptable energy level of the EV.
EVMinimumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: The energy request of the EV it needs to fulfil the minimum SOC as specified by the owner.
EVTargetCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target current requested by the EV
EVTargetVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Target voltage requested by the EV.
EVMaximumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum charge power allowed by the EV.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVMinimumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Minimum charge power allowed by the EV.
EVMaximumChargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum charge current allowed by the EV.
EVMaximumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum voltage allowed by the EV.
EVMinimumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Minimum voltage allowed by the EV.

[V2G20-2183] In a DC_ChargeLoopReq the EVCC shall either provide a EVTargetVoltage or EVTargetCurrent value. The EVCC shall never provide both values in the same message.

[V2G20-2184] If the EVCC provides an EVTargetVoltage value, the EVTargetVoltage shall be defined in such a way, that it is logically consistent with the reported EVPresentVoltage. The target is reached if EVPresentVoltage is equal to EVTargetVoltage.

[V2G20-2185] The SECC shall adjust the voltage on the EVSE side in such a way, that the reported EVPresentVoltage matches the requested EVTargetVoltage as rapidly and closely as technically possible.

[V2G20-2186] If the EVCC provides an EVTargetCurrent value, the EVTargetCurrent shall be defined in such a way, that it is logically consistent with the reported EVSEPresentCurrent. The target is reached if EVSEPresentCurrent is equal to EVTargetCurrent.

[V2G20-2187] The SECC shall adjust the current on the EVSE side in such a way, that the reported EVSEPresentCurrent matches the requested EVTargetCurrent as rapidly and closely as technically possible.

[V2G20-2188] In its attempt to reach an EVTargetVoltage or EVTargetCurrent setpoint, the SECC shall never initiate an EVSE behavior which would violate any of the communicated and applicable limits (maximum and minimum values; for example, see [V2G20-2181] and [V2G20-2182]).

NOTE 1 Implementers can be aware that EVTargetVoltage and EVTargetCurrent will not necessarily be defining a simple CC/CV (constant current constant voltage) energy transfer strategy. For example, in the case of dynamic grid services the resulting power levels could change very rapidly. For this reason EVTargetVoltage and EVTargetCurrent can be interpreted as real targets and not as a replacement for upper limitation. Limits are communicated in other elements.

NOTE 2 In contrast to high voltage charging systems, where the EVPresentVoltage and EVSEPresentVoltage values might be almost identical, in very low voltage DC charging there might be a considerable voltage drop on the charging cable. For this reason it is important that [V2G20-2185] is implemented dutifully.

8.3.5.5.5 Dynamic_DC_CLResControlModeType

This type contains all elements of the DC_ChargeLoopRes message that are only required in case the control mode "Dynamic" is chosen.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1763] The SECC and the EVCC shall implement this type as defined in Table 175 and Figure 184.

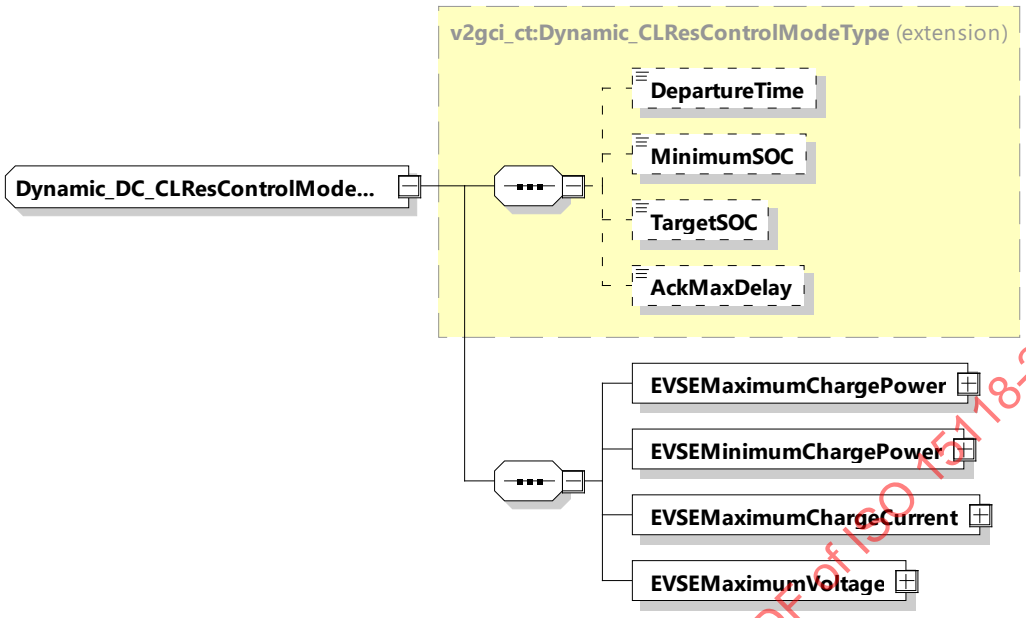


Figure 184 — Schema diagram – Dynamic_DC_CLResControlModeType

The elements of this message are used according to Table 175.

Table 175 — Semantics and type definition for Dynamic_DC_CLResControlModeType

Element name	Type	Semantics
DepartureTime	simpleType: xs:unsignedInt	Optional: This element is used to indicate when the user intends to finish the charging process. Only used when service parameter MobilityNeedsMode was set to 2 The value is encoded in seconds since the TimeStamp of the message header (see [V2G20-2104]).
MinimumSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: New MinimumSOC value updated by the user from EVSE's side Only used when service parameter MobilityNeedsMode was set to 2.
TargetSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: New TargetSOC value updated by the user from EVSE's side Only used when service parameter MobilityNeedsMode was set to 2.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
AckMaxDelay	simpleType: xs:unsignedShort	Optional: This value indicates the maximum delay in seconds that SECC expects the EVCC to apply new mobility needs (DepartureTime or TargetSOC or MinimumSOC) and send updated values in a Charge Loop message since the reception of the message stating the AckMaxDelay.
EVSEMaximumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum power the EVSE can deliver.
EVSEMinimumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVSEMaximumChargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum current the EVSE can deliver.
EVSEMaximumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum voltage the EVSE can deliver.

[V2G20-1290] The SECC shall only send MinimumSOC that is less than or equal to TargetSOC.

[V2G20-1291] If the EVCC selected the service parameter "MobilityNeedsMode" set to 2 and the SECC received new values for departure time, target SOC or minimum SOC from a secondary actor, the SECC shall include those updated values in DepartureTime, TargetSOC or MinimumSOC, respectively. If TargetSOC or MinimumSOC are included, then the SECC shall also include AckMaxDelay.

[V2G20-1292] If the EVCC selected the service parameter MobilityNeedsMode set to 2 and receives a DC_ChargeLoopRes message with DepartureTime, TargetSOC or MinimumSOC, and if the EVCC accepts this DepartureTime, TargetSOC or MinimumSOC, then the EVCC shall send updated values in a DC_ChargeLoopReq within the number of seconds stated in AckMaxDelay of DC_ChargeLoopRes.

[V2G20-1294] If the EVCC selected the service parameter MobilityNeedsMode set to 2 and EVCC receives a DC_ChargeLoopRes message with DepartureTime, TargetSOC or MinimumSOC, and if the EVCC cannot accept this DepartureTime, TargetSOC or MinimumSOC, e.g. for internal reasons, then the EVCC shall send different values in a DC_ChargeLoopReq than the values in DC_ChargeLoopRes within the number of seconds stated in AckMaxDelay of the DC_ChargeLoopRes.

NOTE In this case, the behavior of the SECC is not in the scope.

8.3.5.5.6 Scheduled_DC_CLResControlModeType

This type contains all elements of the DC_ChargeLoopRes message that are only required in case the control mode "Scheduled" is chosen.

[V2G20-1761] The SECC and the EVCC shall implement this type as defined in Table 176 and Figure 185.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

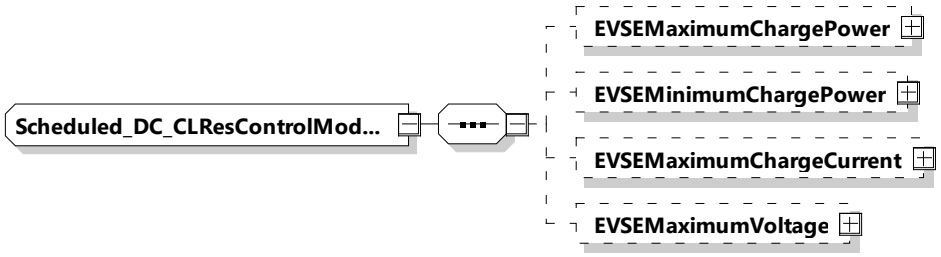


Figure 185 — Schema diagram – Scheduled_DC_CLResControlModeType

The elements of this message are used according to Table 176.

Table 176 — Semantics and type definition for Scheduled_DC_CLResControlModeType

Element name	Type	Semantics
EVSEMaximumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum power the EVSE can deliver.
EVSEMinimumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Minimum power the EVSE can deliver.
EVSEMaximumChargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum current the EVSE can deliver.
EVSEMaximumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum voltage the EVSE can deliver.

8.3.5.5.7 DC BPT

8.3.5.5.7.1 BPT_DC_CPDReqEnergyTransferModeType

[V2G20-1458] The EVCC and the SECC shall implement this type as defined in Table 177 and Figure 186.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

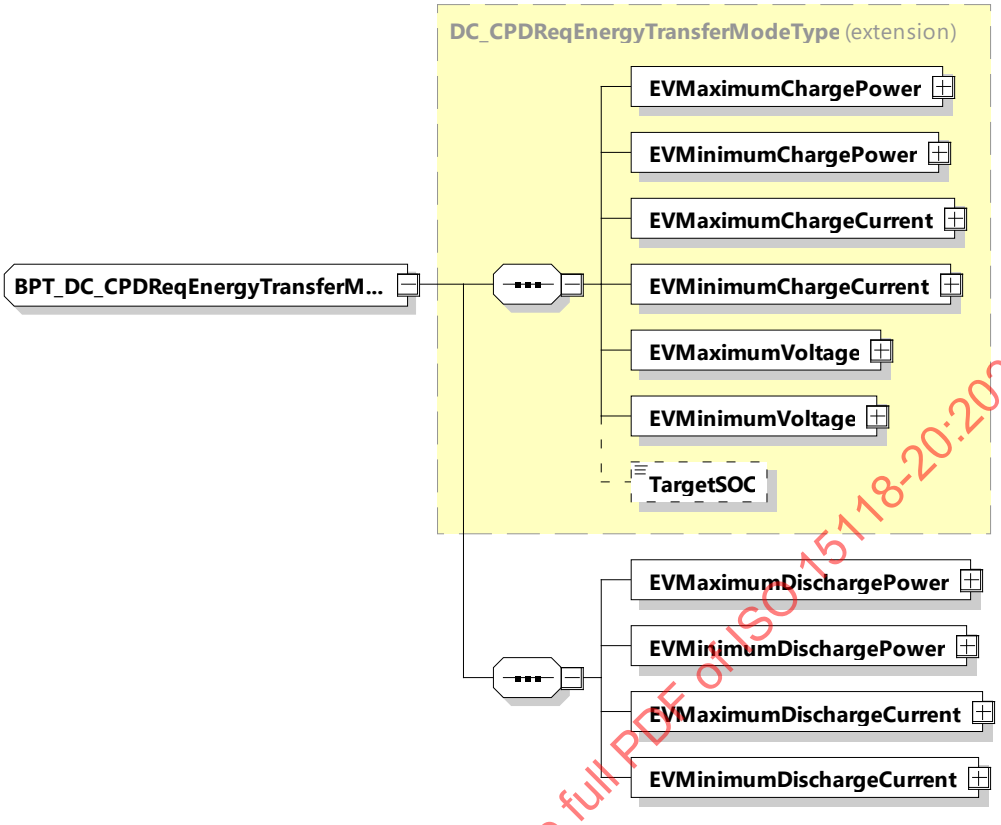


Figure 186 — Schema diagram – BPT_DC_CPDReqEnergyTransferModeType

The elements of this message are used according to Table 177.

Table 177 — Semantics and type definition for BPT_DC_CPDReqEnergyTransferModeType

Element name	Type	Semantics
EVMaximumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum charge power supported by the EV.
EVMinimumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMaximumChargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum charge current supported by the EV.
EVMinimumChargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Any target current between this level and zero may, for technical reasons, result in a drop of the actual current to zero ampere.
EVMaximumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum voltage supported by the EV.
EVMinimumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Minimum voltage supported by the EV.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
TargetSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: SOC at which the EV considers the battery to be fully charged.
EVMaximumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum discharge power supported by the EV.
EVMinimumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVMaximumDischargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum discharge current supported by the EV.
EVMinimumDischargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Any target current between this level and zero may, for technical reasons, result in a drop of the actual current to zero ampere.

8.3.5.5.7.2 BPT_DC_CPDResEnergyTransferModeType

[V2G20-1459] The EVCC and the SECC shall implement this type as defined in Figure 187 and Table 178.

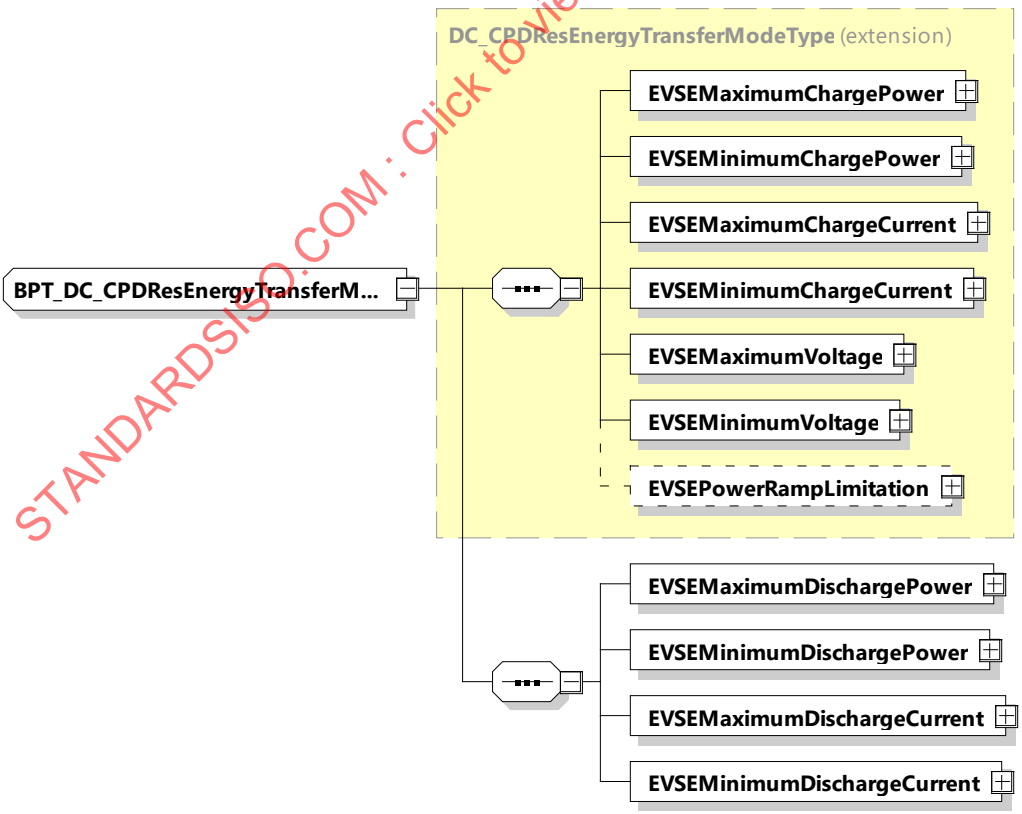


Figure 187 — Schema diagram – BPT_DC_CPDResEnergyTransferModeType

The elements of this message are used according to Table 178.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 178 — Semantics and type definition for BPT_DC_CPDResEnergyTransferModeType

Element name	Type	Semantics
EVSEMaximumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum charge power the EVSE can deliver.
EVSEMinimumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVSEMaximumChargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum charge current the EVSE can deliver.
EVSEMinimumChargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Minimum charge current the EVSE can deliver with the expected accuracy.
EVSEMaximumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum voltage the EVSE can deliver.
EVSEMinimumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Minimum voltage the EVSE can deliver with the expected accuracy.
EVSEPowerRampLimitation	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Limitation of the power variation in %/min.
EVSEMaximumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum discharge power the EVSE can deliver.
EVSEMinimumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVSEMaximumDischargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum discharge current the EVSE can deliver.
EVSEMinimumDischargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Minimum discharge current the EVSE can deliver with the expected accuracy.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

8.3.5.5.7.3 BPT_Dynamic_DC_CLReqControlModeType

[V2G20-1772] The SECC and the EVCC shall implement this type as defined in Figure 188 and Table 179.

© ISO 2022 – All rights reserved

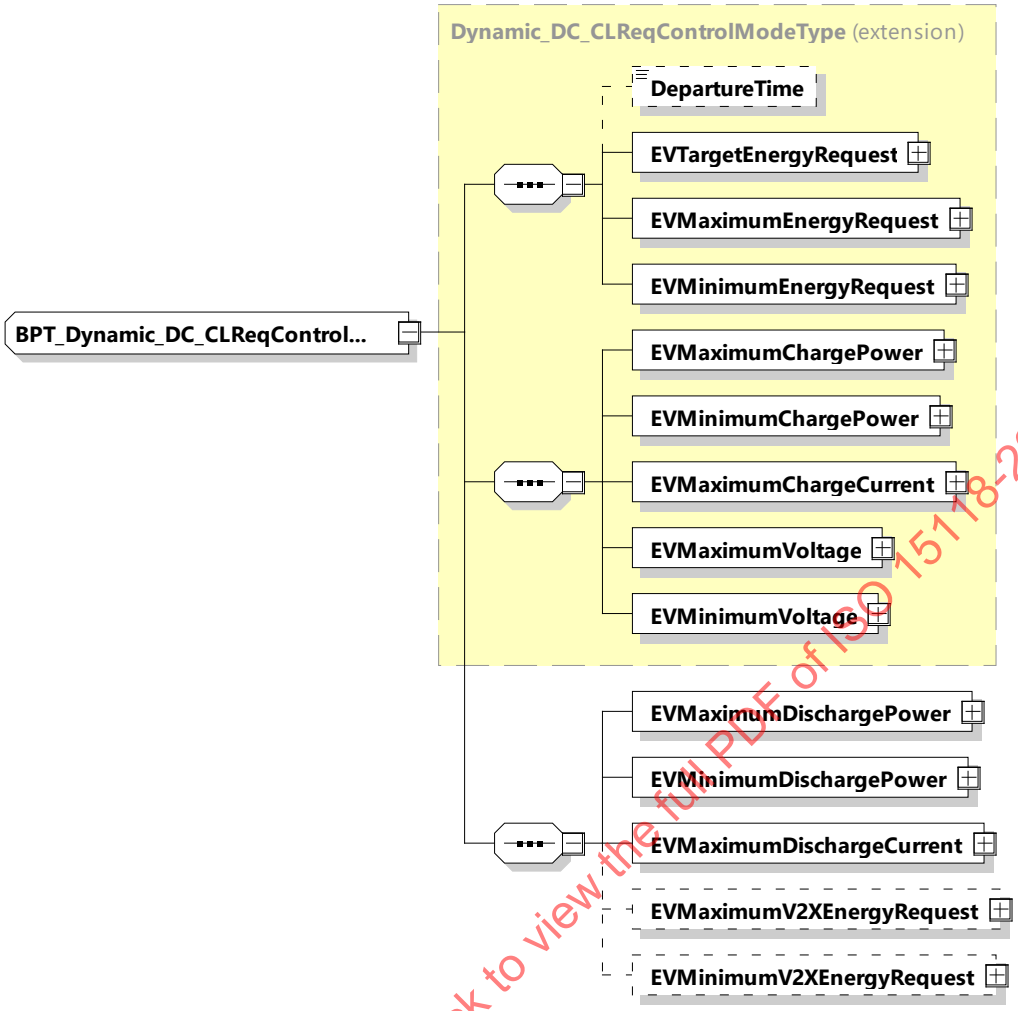


Figure 188 — Schema diagram – BPT_Dynamic_DC_CLReqControlModeType

The elements of this message are used according to Table 179.

Table 179 — Semantics and type definition for BPT_Dynamic_DC_CLReqControlModeType

Element name	Type	Semantics
DepartureTime	simpleType: xs:unsignedInt	Optional: This element is used to indicate when the EV intends to finish the charging process. The value is encoded in seconds since the TimeStamp of the message header (see [V2G20-2104]).
EVTargetEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	The energy request of the EV it needs to fulfil the target SOC as specified by the owner.
EVMaximumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum acceptable energy level of the EV.
EVMinimumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	The energy request of the EV it needs to fulfil the minimum SOC as specified by the owner.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVMaximumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum charge power allowed by the EV.
EVMinimumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Minimum charge power allowed by the EV.
EVMaximumChargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum charge current allowed by the EV.
EVMaximumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum voltage allowed by the EV.
EVMinimumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Minimum voltage allowed by the EV.
EVMaximumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum discharge power allowed by the EV.
EVMinimumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Minimum discharge power allowed by the EV.
EVMaximumDischargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum discharge current allowed by the EV.
EVMaximumV2XEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Energy which may be charged until the PresentSOC has left the range dedicated for cycling activity. A negative value indicates that PresentSOC is above the V2X range.
EVMinimumV2XEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Energy which needs to be charged until the PresentSOC enters the range dedicated for cycling activity. A positive value indicates that PresentSOC is below the V2X range.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

NOTE If the EVCC sends the parameters EVMaximumV2XEnergyRequest and EVMinimumV2XEnergyRequest, it is indicating a preferred operational V2X range (i.e. for bidirectional cycling) and the SECC can attempt to stay within these limits as long as possible.

[V2G20-2679] If EVMaximumV2XEnergyRequest and EVMinimumV2XEnergyRequest are sent by the EVCC, they always need to be sent together.

[V2G20-2680] If the EVCC provides EVMaximumV2XEnergyRequest and EVMinimumV2XEnergyRequest, EVMinimumEnergyRequest shall be less than or equal to EVMinimumV2XEnergyRequest, which shall be less than or equal to EVMaximumV2XEnergyRequest, which shall be less than or equal to EVMaximumEnergyRequest.

© ISO 2022 – All rights reserved

8.3.5.5.7.4 BPT_Scheduled_DC_CLReqControlModeType

[V2G20-1770] The SECC and the EVCC shall implement this type as defined in Table 180 and Figure 189.

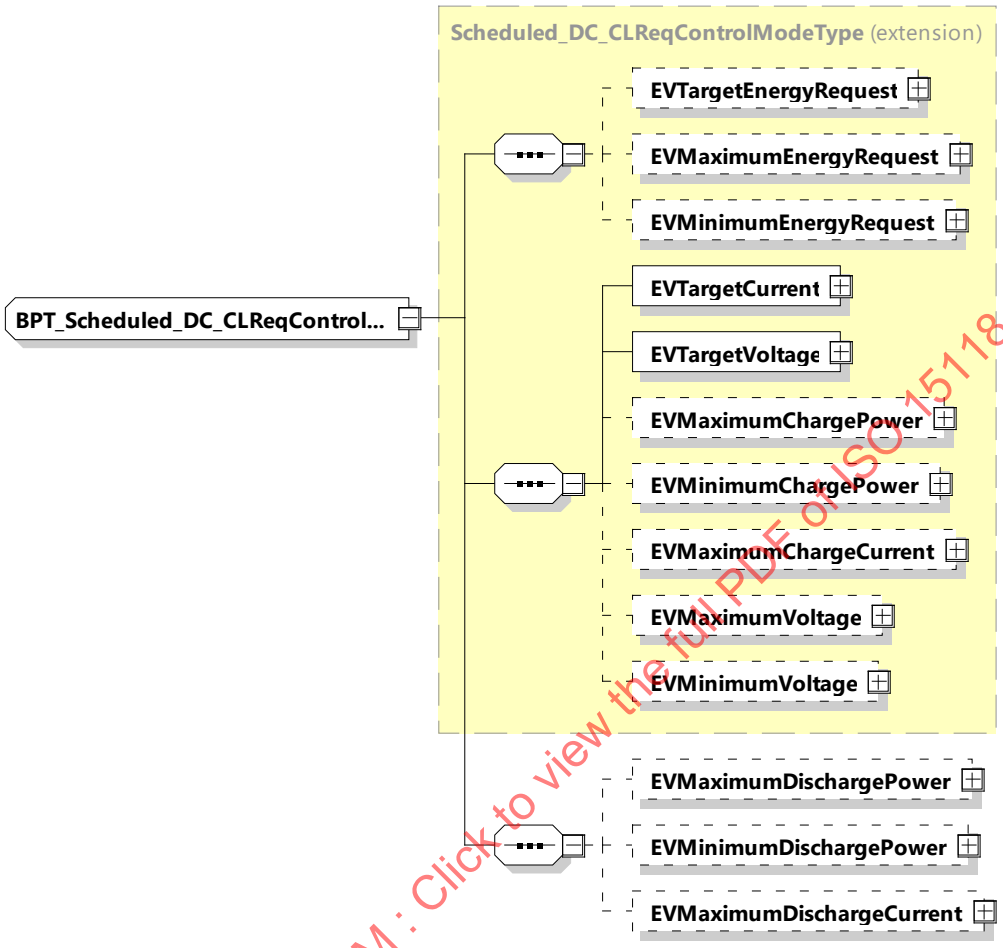


Figure 189 — Schema diagram – BPT_Scheduled_DC_CLReqControlModeType

The elements of this message are used according to Table 180.

Table 180 — Semantics and type definition for BPT_Scheduled_DC_CLReqControlModeType

Element name	Type	Semantics
EVTargetEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: The energy request of the EV it needs to fulfil the target SOC as specified by the owner.
EVMaximumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum acceptable energy level of the EV.
EVMinimumEnergyRequest	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: The energy request of the EV it needs to fulfil the minimum SOC as specified by the owner.
EVTargetCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Target current requested by the EV

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVTargetVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Target voltage requested by the EV.
EVMaximumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum charge power allowed by the EV.
EVMinimumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Minimum charge power allowed by the EV.
EVMaximumChargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum charge current allowed by the EV.
EVMaximumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum voltage allowed by the EV.
EVMinimumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Minimum voltage allowed by the EV.
EVMaximumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum discharge power allowed by the EV.
EVMinimumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Minimum discharge power allowed by the EV.
EVMaximumDischargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum discharge current allowed by the EV.

8.3.5.5.7.5 BPT_Dynamic_DC_CLResControlModeType

[V2G20-1773] The SECC and the EVCC shall implement this type as defined in Figure 190 and Table 181.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

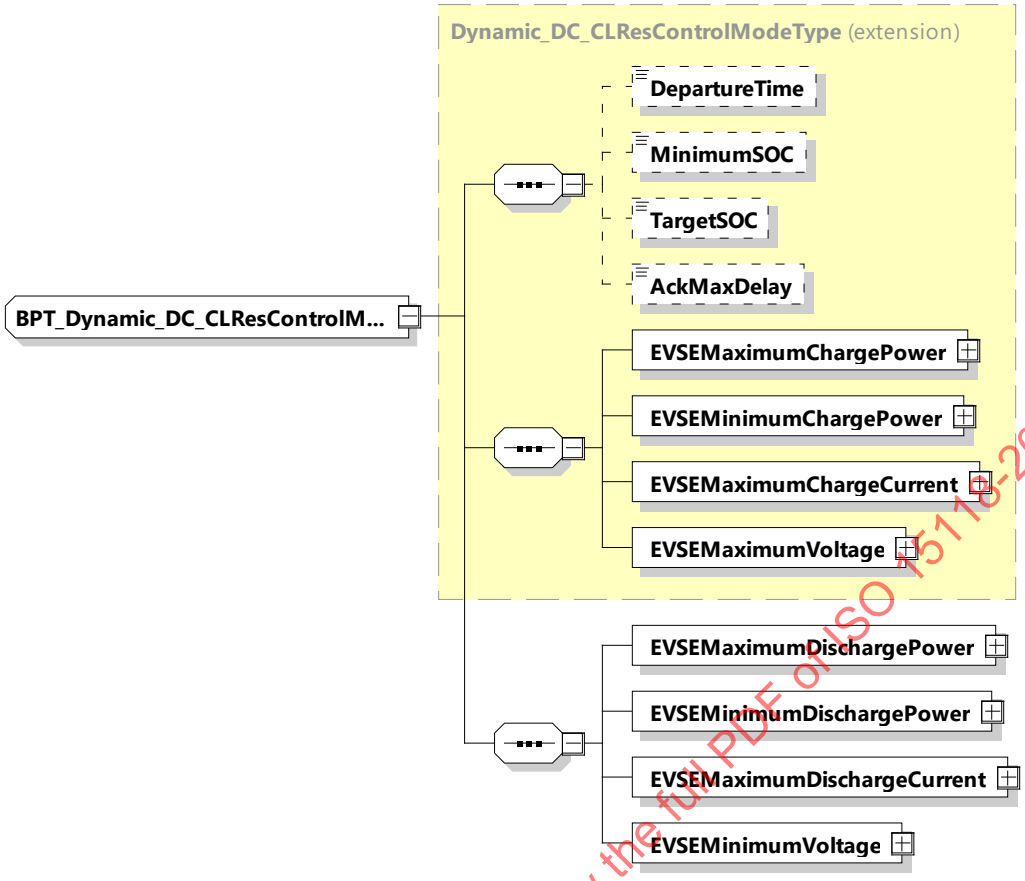


Figure 190 — Schema diagram – BPT_Dynamic_DC_CLResControlModeType

The elements of this message are used according to Table 181.

Table 181 — Semantics and type definition for BPT_Dynamic_DC_CLResControlModeType

Element name	Type	Semantics
DepartureTime	simpleType: xs:unsignedInt	Optional: This element is used to indicate when the user intends to finish the charging process. Only used when service parameter MobilityNeedsMode was set to 2 The value is encoded in seconds since the TimeStamp of the message header (see [V2G20-2104]).
MinimumSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: New MinimumSOC value updated by the user from EVSE's side Only used when service parameter MobilityNeedsMode was set to 2.
TargetSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: New TargetSOC value updated by the user from EVSE's side Only used when service parameter MobilityNeedsMode was set to 2.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
AckMaxDelay	simpleType: xs:unsignedShort	Optional: This value indicates the maximum delay in seconds that SECC expects the EVCC to apply new mobility needs (DepartureTime or TargetSOC or MinimumSOC) and send updated values in a Charge Loop message since the reception of the message stating the AckMaxDelay.
EVSEMaximumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum power the EVSE can deliver.
EVSEMinimumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Minimum power the EVSE can deliver.
EVSEMaximumChargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum current the EVSE can deliver.
EVSEMaximumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum voltage the EVSE can deliver.
EVSEMaximumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum discharge power the EVSE can deliver.
EVSEMinimumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVSEMaximumDischargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Maximum discharge current the EVSE can deliver.
EVSEMinimumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Minimum voltage the EVSE can deliver.

[V2G20-2662] The SECC shall only send a MinimumSOC that is less than or equal to TargetSOC.

[V2G20-2670] If the EVCC selected the service parameter "MobilityNeedsMode" set to 2 and the SECC received new values for departure time, target SOC or minimum SOC from a secondary actor, the SECC shall include those updated values in DepartureTime, TargetSOC or MinimumSOC, respectively. If TargetSOC or MinimumSOC are included, then the SECC shall also include AckMaxDelay.

[V2G20-2671] If the EVCC selected the service parameter MobilityNeedsMode set to 2 and receives a DC_ChargeLoopRes message with DepartureTime, TargetSOC or MinimumSOC, and if the EVCC accepts this DepartureTime, TargetSOC or MinimumSOC, then the EVCC shall send updated values in a DC_ChargeLoopReq within the number of seconds stated in AckMaxDelay of DC_ChargeLoopRes.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2672] If the EVCC selected the service parameter MobilityNeedsMode set to 2 and EVCC receives a DC_ChargeLoopRes message with DepartureTime, TargetSOC or MinimumSOC, and if the EVCC cannot accept this DepartureTime, TargetSOC or MinimumSOC, e.g. for internal reasons, then the EVCC shall send different values in a DC_ChargeLoopReq than the values in DC_ChargeLoopRes within the number of seconds stated in AckMaxDelay of the DC_ChargeLoopRes.

8.3.5.5.7.6 BPT_Scheduled_DC_CLResControlModeType

[V2G20-1771] The SECC and the EVCC shall implement this type as defined in Table 182 and Figure 191.

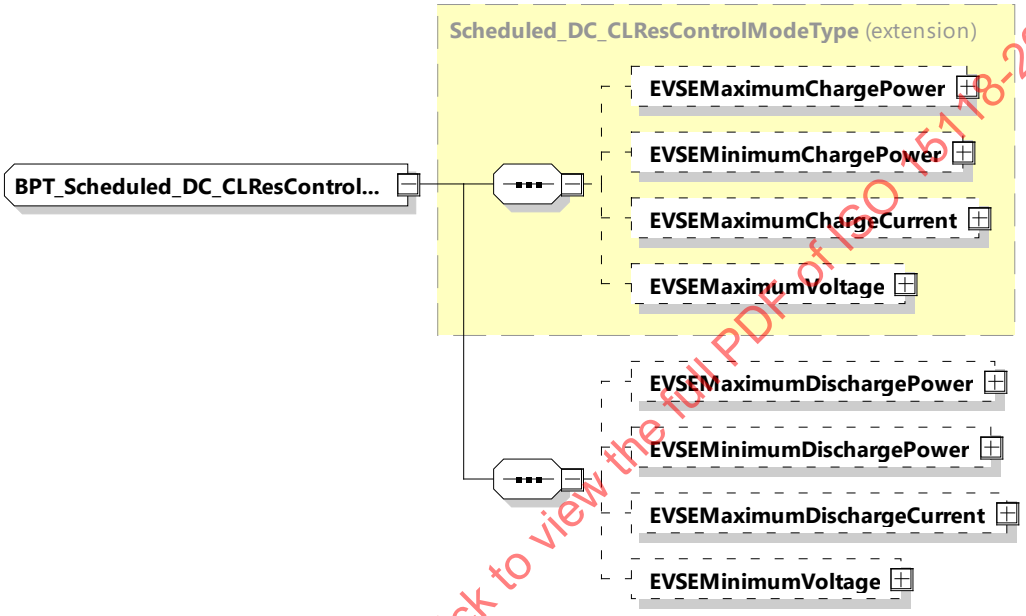


Figure 191 — Schema diagram – BPT_Scheduled_DC_CLResControlModeType

The elements of this message are used according to Table 182.

Table 182 — Semantics and type definition for BPT_Scheduled_DC_CLResControlModeType

Element name	Type	Semantics
EVSEMaximumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum power the EVSE can deliver.
EVSEMinimumChargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVSEMaximumChargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum current the EVSE can deliver.
EVSEMaximumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum voltage the EVSE can deliver.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVSEMaximumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum discharge power the EVSE can deliver.
EVSEMinimumDischargePower	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Any target power between this level and zero may, for technical reasons, result in a drop of the actual power to zero watts.
EVSEMaximumDischargeCurrent	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Maximum discharge current the EVSE can deliver.
EVSEMinimumVoltage	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Minimum voltage the EVSE can deliver.

8.3.5.6 WPT

8.3.5.6.1 AlternativeSECCListType

[V2G20-5102] The EVCC and the SECC shall implement this type as defined in Figure 192 and Table 183.

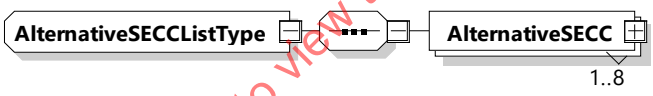


Figure 192 — Schema diagram – AlternativeSECCListType

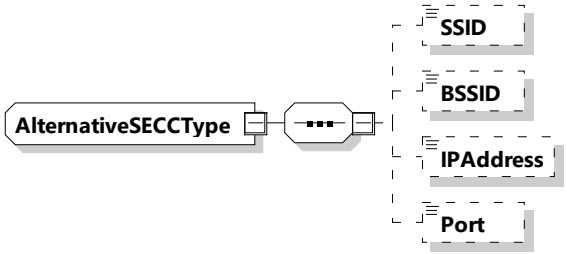
The elements of this message are used according to Table 183.

Table 183 — Semantics and type definition for AlternativeSECCListType

Element name	Type	Semantics
AlternativeSECC	complexType: AlternativeSECCType refer to 8.3.5.6.2	Contains a list of SECC connection information. AlternativeSECCList includes at least one AlternativeSECC and may include up to 8 AlternativeSECCs.

8.3.5.6.2 AlternativeSECCType

[V2G20-5103] The EVCC and the SECC shall implement this type as defined in Figure 193 and Table 184.



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Figure 193 — Schema diagram – AlternativeSECCType

The elements of this message are used according to Table 184.

Table 184 — Semantics and type definition for AlternativeSECCType

Element name	Type	Semantics
SSID	simpleType: identifierType refer to Annex A for the type definition	Optional: SSID (Service Set ID) of the WLAN of the SECC
BSSID	simpleType: bssidType refer to Annex A for the type definition	Optional: BSSID (Basic Service Set ID) of the WLAN of the SECC (MAC address of the AP)
IPAddress	simpleType: ipaddressType refer to Annex A for the type definition	Optional: IP address of the SECC
Port	simpleType xs:unsignedShort	Optional: TCP port number of the SECC

8.3.5.6.3 Data types related to power transfer

The following complex data types are used in messages which are controlling power transfer.

8.3.5.6.3.1 WPT_EVPCPowerControlParameterType

[V2G20-5104] The EVCC and the SECC shall implement this type as defined in Figure 194 and Table 185.

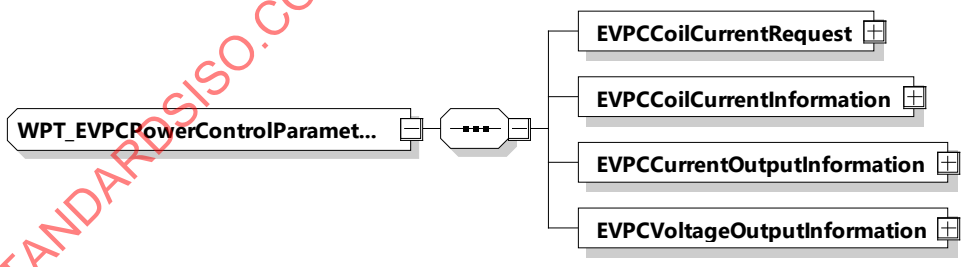


Figure 194 — Schema diagram – WPT_EVPCPowerControlParameterType

The elements of this message are used according to Table 185.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 185 — Semantics and type definition for WPT_EVPCPowerControlParameterType

Element name	Type	Semantics
EVPCCoilCurrentRequest	complexType: RationalNumberType refer to 8.3.5.3.8	EVPC wants the primary device to set a specific (preferred) coil current value in amperes. NOTE The EVPCPowerRequest element is overriding the value given here in case of mismatch.
EVPCCoilCurrentInformation	complexType: RationalNumberType refer to 8.3.5.3.8	Information about secondary device coil current (AC) in amperes
EVPCCurrentOutputInformation	complexType: RationalNumberType refer to 8.3.5.3.8	Information about DC current supplied to the EV in amperes
EVPCVoltageOutputInformation	complexType RationalNumberType refer to 8.3.5.3.8	Information about DC bus or battery voltage in volts

8.3.5.6.3.2 WPT_SPCPowerControlParameterType

[V2G20-5105] The EVCC and the SECC shall implement this type as defined in Figure 195 and Table 186.

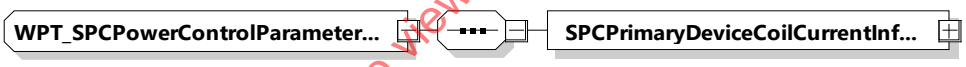


Figure 195 — Schema diagram – WPT_SPCPowerControlParameterType

The elements of this message are used according to Table 186.

Table 186 — Semantics and type definition for WPT_SPCPowerControlParameterType

Element name	Type	Semantics
SPCPrimaryDeviceCoilCurrentInformation	complexType: RationalNumberType refer to 8.3.5.3.8	Information about the primary device coil current (AC) in amperes

8.3.5.6.4 Data types related to fine positioning

The following complex data types are used in messages related to fine positioning. Refer to IEC 61980-2 for detailed in formation of the individual data and their application.

8.3.5.6.4.1 WPT_LF_SystemSetupDataType

This data type contains information exchanged during the fine positioning setup. It relates to fine positioning methods LF_TxEV or LF_TxPrimaryDevice.

[V2G20-5106] The EVCC and the SECC shall implement this type as defined in Figure 196 and Table 187.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

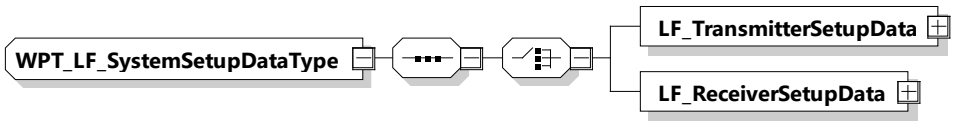


Figure 196 — Schema diagram – WPT_LF_SystemSetupDataType

The elements of this message are used according to Table 187.

Table 187 — Semantics and type definition for WPT_LF_SystemSetupDataType

Element name	Type	Semantics
LF_TransmitterSetupData	complexType: WPT_LF_TransmitterDataType refer to 8.3.5.6.4.2	Setup data for the set of LF transmitters installed
LF_ReceiverSetupData	complexType: WPT_LF_ReceiverDataType refer to 8.3.5.6.4.3	Setup data for the set of receivers installed

[V2G20-5107] Either TransmitterSetupData or ReceiverSetupData can be given. See 8.3.5.6.4.2 and 8.3.5.6.4.3 for more information.

8.3.5.6.4.2 WPT_LF_TransmitterDataType

[V2G20-5108] The EVCC and the SECC shall implement this type as defined in Figure 197 and Table 188.

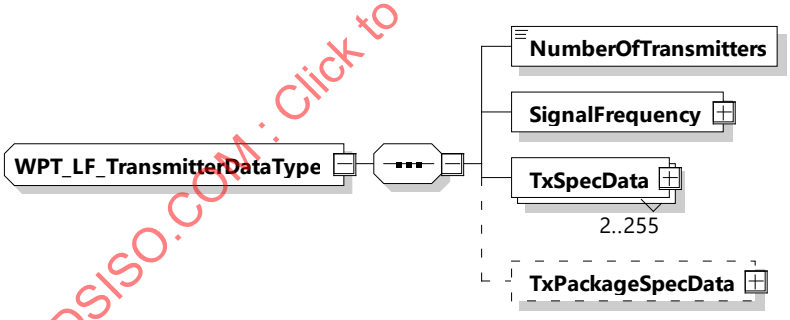


Figure 197 — Schema diagram – WPT_LF_TransmitterDataType

The elements of this message are used according to Table 188.

Table 188 — Semantics and type definition for WPT_LF_TransmitterDataType

Element name	Type	Semantics
NumberOfTransmitters	simpleType: xs:unsignedByte	Number of transmitters of the auxiliary antenna system installed
SignalFrequency	complexType RationalNumberType refer to 8.3.5.3.8	Frequency in Hz of the signal to be used
TxSpecData	complexType: WPT_TxRxSpecDataType refer to 8.3.5.6.4.4	For each transmitter this element is given with information about position and orientation of the transmitter.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
TxPackageSpecData	complexType: WPT_TxRxPackageSpecDataType refer to 8.3.5.6.4.6	Optional: Information about the order how signals are emitted from the individual transmitters

8.3.5.6.4.3 WPT_LF_ReceiverDataType

[V2G20-5109] The EVCC and the SECC shall implement this type as defined in Figure 198 and Table 189.

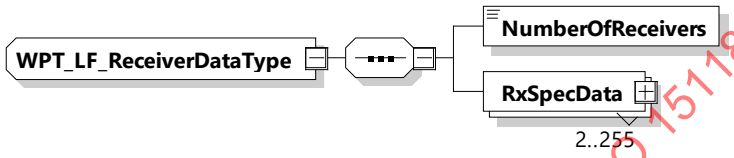


Figure 198 — Schema diagram – WPT_LF_ReceiverDataType

The elements of this message are used according to Table 189.

Table 189 — Semantics and type definition for WPT_LF_ReceiverDataType

Element name	Type	Semantics
NumberOfReceivers	simpleType: xs:unsignedByte	Number of receivers of the auxiliary antenna system installed
RxSpecData	complexType: WPT_TxRxSpecDataType refer to 8.3.5.6.4.4	For each receiver this element is given with information about position and orientation of the receiver.

8.3.5.6.4.4 WPT_TxRxSpecDataType

[V2G20-5110] The EVCC and the SECC shall implement this type as defined in Figure 199 and Table 190.

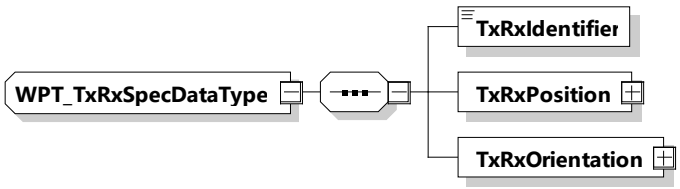


Figure 199 — Schema diagram – WPT_TxRxSpecDataType

The elements of this message are used according to Table 190.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 190 — Semantics and type definition for WPT_TxRxSpecDataType

Element name	Type	Semantics
TxRxIdentifier	simpleType: numericIDType refer to Annex A for the type definition	Identifier of the transmitter/receiver
TxRxPosition	complexType: WPT_CoordinateXYZType refer to 8.3.5.6.4.5	x,y,z coordinates of the transmitter/receiver given in EV coordinates relative to the center of the secondary device or rather the primary device given in mm
TxRxOrientation	complexType: WPT_CoordinateXYZType refer to 8.3.5.6.4.5	x,y,z,unit vector given the direction of measurement. If no direction is applicable, all three values are set to zero.

8.3.5.6.4.5 WPT_CoordinateXYZType

[V2G20-5111] The EVCC and the SECC shall implement this type as defined in Figure 200 and Table 191.

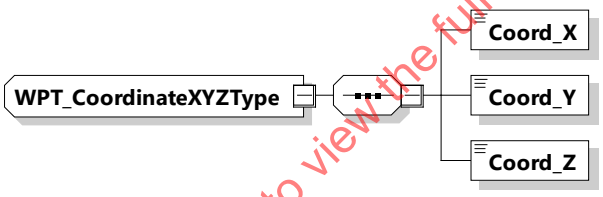


Figure 200 — Schema diagram – WPT_CoordinateXYZType

The elements of this message are used according to Table 191.

Table 191 — Semantics and type definition for WPT_CoordinateXYZType

Element name	Type	Semantics
Coord_X	simpleType: xs:short	X value in the related coordinate system
Coord_Y	simpleType: xs:short	Y value in the related coordinate system
Coord_Z	simpleType: xs:short	Z value in the related coordinate system

8.3.5.6.4.6 WPT_TxRxPackageSpecDataType

[V2G20-5112] The EVCC and the SECC shall implement this type as defined in Figure 201 and Table 192.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

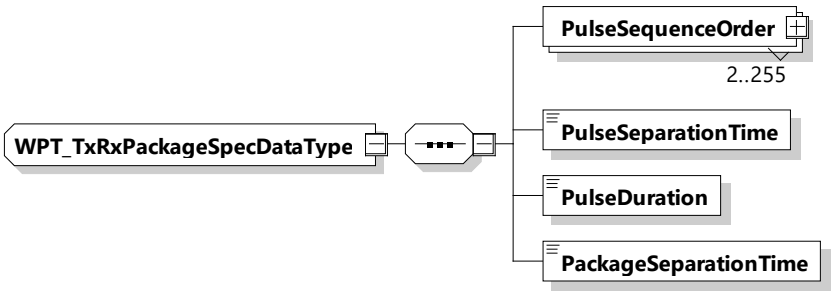


Figure 201 — Schema diagram – WPT_TxRxPackageSpecDataType

The elements of this message are used according to Table 192.

Table 192 — Semantics and type definition for WPT_TxRxPackageSpecDataType

Element name	Type	Semantics
PulseSequenceOrder	complexType: WPT_TxRxPulseOrderType See 8.3.5.6.4.7	Ordered list of the antenna identifiers, which describes the order with which the transmitters send out a signal as one pulse package. The list defines a pulse package, which contains the ordered collection of pulses from each EV transmitter. For each transmitter this element shall be given once.
PulseSeparationTime	simpleType: xs:unsignedShort	Time in ms between the individual pulses within the pulse package
PulseDuration	simpleType: xs:unsignedShort	Time duration in ms of each individual pulse within the pulse package
PackageSeparationTime	simpleType: xs:unsignedShort	Time in ms between two subsequent pulse packages

8.3.5.6.4.7 WPT_TxRxPulseOrderType

[V2G20-5113] The EVCC and the SECC shall implement this type as defined in Figure 202 and Table 193.

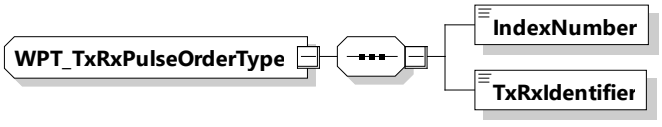


Figure 202 — Schema diagram – WPT_TxRxPulseOrderType

The elements of this message are used according to Table 193.

Table 193 — Semantics and type definition for WPT_TxRxPulseOrderType

Element name	Type	Semantics
IndexNumber	simpleType: xs:unsignedShort	Position in the ordered list

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
TxIdentifier	simpleType: numericIDType refer to Annex A for the type definition	Identifier of the transmitter at this position in the ordered list

8.3.5.6.4.8 WPT_LF_TxDataListType

[V2G20-5115] The EVCC and the SECC shall implement this type as defined in Figure 203 and Table 194.

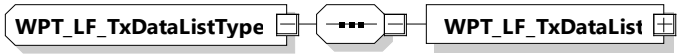


Figure 203 — Schema diagram – WPT_LF_TxDataListType

The elements of this message are used according to Table 194.

Table 194 — Semantics and type definition for WPT_LF_TxDataListType

Element name	Type	Semantics
WPT_LF_TxDataList	complexType: WPT_LF_TxDataType refer to 8.3.5.6.4.9	List of WPT_LF_TxData. This list is carrying the data for each transmitter of a set of transmitters installed

8.3.5.6.4.9 WPT_LF_TxDataType

[V2G20-5114] The EVCC and the SECC shall implement this type as defined in Figure 204 and Table 195.

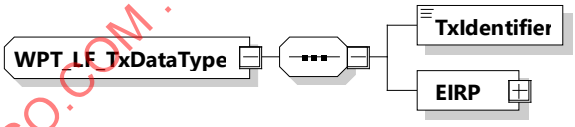


Figure 204 — Schema diagram – WPT_LF_TxDataType

The elements of this message are used according to Table 195.

Table 195 — Semantics and type definition for WPT_LF_TxDataType

Element name	Type	Semantics
TxIdentifier	simpleType: numericIDType refer to Annex A for the type definition	Identifier of transmitter
EIRP	complexType: RationalNumberType refer to 8.3.5.3.8	EIRP value (signal strength of the emitted signal); is used by the transmitting component

8.3.5.6.4.10 WPT_LF_RxDataListType

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-5117] The EVCC and the SECC shall implement this type as defined in Figure 205 and Table 196.

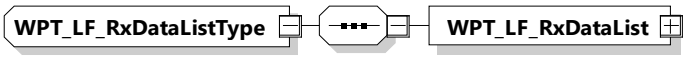


Figure 205 — Schema diagram – WPT_LF_RxDataListType

The elements of this message are used according to Table 196.

Table 196 — Semantics and type definition for WPT_LF_RxDataListType

Element name	Type	Semantics
WPT_LF_RxDataList	complexType: WPT_LF_RxDataType See 8.3.5.6.4.11	Element which contains the information about the received LF signals for a set of receivers.

8.3.5.6.4.11 WPT_LF_RxDataType

[V2G20-5116] The EVCC and the SECC shall implement this type as defined in Figure 206 and Table 197.

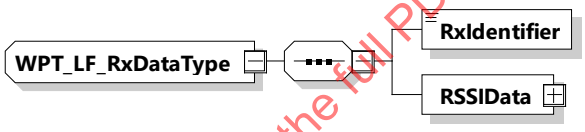


Figure 206 — Schema diagram – WPT_LF_RxDataType

The elements of this message are used according to Table 197.

Table 197 — Semantics and type definition for WPT_LF_RxDataType

Element name	Type	Semantics
RxIdentifier	simpleType: numericIDType refer to Annex A for the type definition	Identifier of the receiver
RSSIData	complexType: WPT_LF_RxRSSIListType refer to 8.3.5.6.4.12	List which contains the RSSI values for the individual signals (pulses) received from the different transmitters

8.3.5.6.4.12 WPT_LF_RxRSSIListType

[V2G20-5119] The EVCC and the SECC shall implement this type as defined in Figure 207 and Table 198.

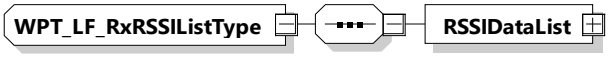


Figure 207 — Schema diagram – WPT_LF_RxRSSIListType

The elements of this message are used according to Table 198.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 198 — Semantics and type definition for WPT_LF_RxRSSIListType

Element name	Type	Semantics
RSSIDataList	complexType: WPT_LF_RxRSSIType See 8.3.5.6.4.13	List of received RSSI signals The order of the RSSI values listed here should correspond to the PulseOrder which was given during fine positioning setup

8.3.5.6.4.13 WPT_LF_RxRSSIType

[V2G20-5118] The EVCC and the SECC shall implement this type as defined in Figure 208 and Table 199.

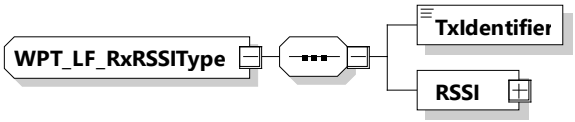


Figure 208 — Schema diagram – WPT_LF_RxRSSIType

The elements of this message are used according to Table 199.

Table 199 — Semantics and type definition for WPT_LF_RxRSSIType

Element name	Type	Semantics
TxIdentifier	simpleType: numericIDType refer to Annex A for the type definition	Identifier of the transmitter which is assigned to the LF signal (pulse) received
RSSI	complexType: RationalNumberType refer to 8.3.5.3.8	(Pre-processed) RSSI value of the received LF signal (pulse)

8.3.5.6.4.14 WPT_LF_DataPackageListType

[V2G20-5121] The EVCC and the SECC shall implement this type as defined in Figure 209 and Table 200.

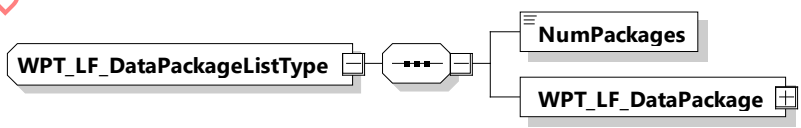


Figure 209 — Schema diagram – WPT_LF_DataPackageListType

The elements of this message are used according to Table 200.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 200 — Semantics and type definition for WPT_LF_DataPackageListType

Element name	Type	Semantics
NumPackages	simpleType: xs:unsignedByte	Number of data packages
WPT_LF_DataPackage	complexType: WPT_LF_DataPackageType Refer to 8.3.5.6.4.15	Data packages

8.3.5.6.4.15 WPT_LF_DataPackageType

[V2G20-5120] The EVCC and the SECC shall implement this type as defined in Figure 210 and Table 201.

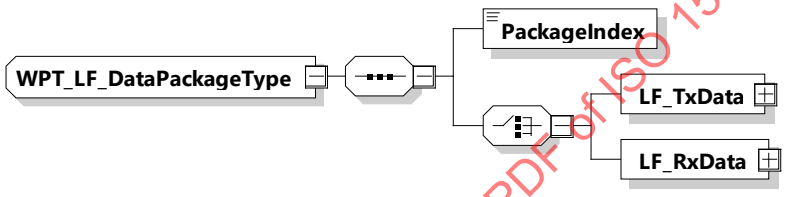


Figure 210 — Schema diagram – WPT_LF_DataPackageType

The elements of this message are used according to Table 201.

Table 201 — Semantics and type definition for WPT_LF_DataPackageType

Element name	Type	Semantics
PackageIndex	simpleType: xs:unsignedByte	Index number of the signal package (consecutive numbered for each positioning process)
LF_TxData	complexType: WPT_LF_TxDataListType See 8.3.5.6.4.8	Data package(s) containing information of transmitted data
LF_RxData	complexType: WPT_LF_RxDataListType See 8.3.5.6.4.10	Data package(s) containing information of received data

8.3.5.7 ACDP

8.3.5.7.1 EVTechnicalStatusType

[V2G20-4011] The EVCC and the SECC shall implement the message elements as defined in Figure 211 and Table 202.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

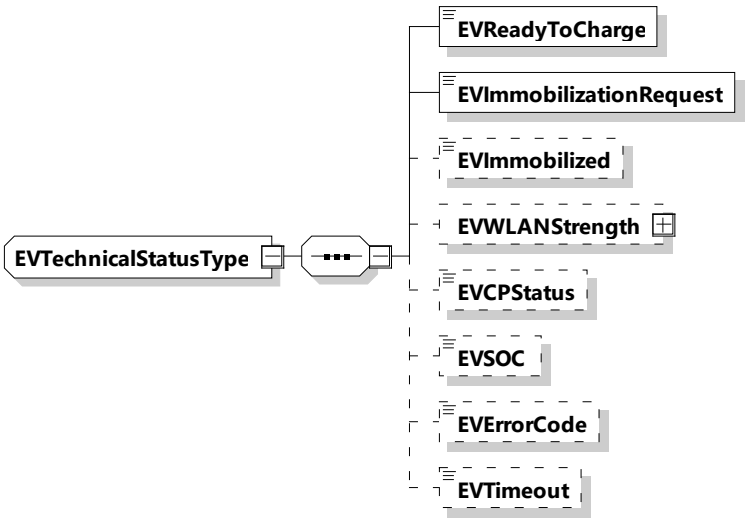


Figure 211 – Schema diagram – EVTechnicalStatusType

The elements of this message are used according to Table 202.

Table 202 — Semantics and type definition for EVTechnicalStatusType

Element name	Type	Semantics
EVReadyToCharge	simpleType: xs:boolean	Element signalizes if the EV is READY or NOT READY to charge. This status shall consider all sub-systems and conditions in the EV that are relevant for the charging process. Possible states are: True, False
EVImmobilizationRequest	simpleType: xs:boolean	Represents the request of immobilization of the EV. This may be related to the hand brake status. Possible states are: True, False
EVImmobilized	simpleType: xs:boolean	Optional: The immobilization of the EV is a mandatory precondition to activate the pantograph. Possible states are: True, False
EVWLANStrength	complexType: RationalNumberType refer to 8.3.5.3.8	Optional: Element signalizes EV WiFi reception signal strength (-dBm)
EVCPStatus	simpleType: cpStatusType refer to Annex A for the type definition	Optional: Element is used to indicate the CP status as recognized by the EVCC (A, B, C, D, E). This may differ in error cases from the CP state recognition of the SECC. Refer to IEC 61851-23-1.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Element name	Type	Semantics
EVSOC	simpleType: percentValueType refer to Annex A for the type definition	Optional: For operation usable SOC status in %. This value may differ from physical SOC of the battery. This parameter can be same as PresentSOC in DisplayParameter.
EVErrorCode	simpleType: errorCodeType refer to Annex A for the type definition	Optional: Element signalizes the EV error status code of the technical fault.
EVTimeout	simpleType: xs:boolean	Optional: Indicates the occurrence of a timeout in the EVCC. Possible states are: True, False

NOTE The EVImmobilizationRequest element provides information whether the charging process was aborted due to an error or otherwise intentionally by the driver releasing the hand brake. This information is important for remote diagnosis.

Table 203 below lists the EV errorCodeType related to the ACDP_SystemStatus.

Table 203 — Enumeration for errorCodeType

Element name	Comment
No_EV_Error	Indicates that the EV has no error
EV_FAILED_EmergencyEvent	EV had an emergency event and stopped charging
EV_FAILED_Breaker	EV had a breaker failure, charging not possible
EV_FAILED_RESSTemperatureInhibit	EV had an RESS overtemperature event, charging not possible
EV_FAILED_RESS	EV had an RESS failure, charging not possible
EV_FAILED_ChargingCurrentDifferential	EV had an over current event and stopped charging
EV_FAILED_ChargingVoltageOutOfRange	EV had an over voltage event and stopped charging
EV_FAILED	EV had an undefined other event and stopped charging
Reserved_by_ISO_1	
Reserved_by_ISO_2	

8.4 Service selection

8.4.1 General

ISO 15118-1 defines use case elements covering different services such as charging, WPT and BPT scenarios. Depending on a use case and a service scenario only one subset of the messages and parameters defined in this document are applied and transmitted by the EVCC and the SECC, respectively.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

This subclause defines the selection method with respect to service and applied message set. The respective service will be selected through service discovery, service detail and service selection message exchanges.

Each request and response message exchange will select relevant service. These are summarized as follows.

- Service discovery:

  The EVCC will request the available services from the SECC. The EVCC may pre-filter by sending the respective service IDs to only ask the SECC for services it is interested in. The SECC will answer with an appropriate list of supported services it can offer the EVCC. These may include user specific services.

- Service detail:

  The EVCC will select the services it intends to use and sends the service IDs to the SECC for more detailed information. The SECC will answer with the parameter list of the chosen Service. This happens in a loop, for each Service the EVCC wants information it will send one service detail with one ServiceID.

- Service selection:

  The EVCC will select the services by sending the selected ServiceID and the respective ParameterSetID to the SECC.

- Charge parameter discovery:

  EVCC and SECC exchange the physical limitations under rated operating conditions for the chosen energy transfer service.

EVCC and SECC will select and negotiate the service operation applied to the established service session through this message exchange. After the service operation is selected, the applied message set will be decided uniquely. A message set consists of multiple mandatory or optional messages with parameters, and it may cover multiple operation modes.

8.4.2 General description of configuration parameters

8.4.2.1 Control modes

Two control modes are available. Basically, a distinction is made between two main situations: (a) the EVCC is in charge of ensuring the mobility needs (scheduled control mode), or (b) ensuring the mobility needs is delegated to an off-board system (dynamic control mode).

- **Scheduled**: In the scheduled control mode, the SECC and the EVCC negotiate a power profile based on the information exchanged in the ScheduleList element. In this control mode, the EVCC is responsible for computing an EVPowerProfile compliant with the user's mobility needs.
- **Dynamic**: In the dynamic control mode, the control is fully delegated to an off-board system. There are no negotiations needed in this mode. The EVCC sends parameters which describe the boundaries of the EV battery for energy usage to the SECC. The SECC then sends single power setpoints to the EVCC, which the EV should abide to. The off-board system in charge of the control is responsible for ensuring that the user's mobility needs will be satisfied. This control mode is particularly adapted to fast responding grid services.

[V2G20-1460] EVCC shall support dynamic and scheduled control mode for all supported energy transfer services.

[V2G20-1464] SECC shall support dynamic and scheduled control mode for all supported energy transfer services.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Depending on the selected control mode, dynamic or sheduled, different elements may be mandatory or not used.

[V2G20-1214] In case dynamic control mode was selected, unless otherwise stated, anytime an element is prefixed with dynamic (e.g. Dynamic_SEReqControlMode), it shall be used. Anytime an element is prefixed with scheduled (e.g. Scheduled_SEReqControlMode), it shall not be used.

[V2G20-1215] In case scheduled control mode was selected, unless otherwise stated, anytime an element is prefixed with Scheduled (e.g. Scheduled_SEReqControlMode), it shall be used. Anytime an element is prefixed with dynamic (e.g. Dynamic_SEReqControlMode), it shall not be used.

As dynamic control mode delegate the energy transfer control to an off-board system, one could argue that this control mode is not necessary in DC. However, it is required to keep both control modes because the processes and information exchanges differ.

8.4.2.2 Generator modes

The "GeneratorMode" parameter indicates if the system consisting of EV and EVSE operates as a grid following generator (only injecting active and reactive power) or as a grid forming generator.

- **GridForming**: The system is able to control the voltage and frequency of the network and to power wires that would not be powered otherwise ("bootstrap" the network). The GridForming generator mode should be selected, for example, if the system consisting of EV and EVSE is powering up a remote load or the microgrid of a house.
- **GridFollowing**: This mode should be used in situations when the system consisting of EV and EVSE is connected to the upstream distribution network, and would not act as one of the main grid forming generators of the network.

In DC energy transfer mode, one could argue that the GeneratorMode parameter might not be necessary, as the power electronic unit is located in the EVSE. However, the charging / discharging patterns will be different depending on the generator mode (ramps, depth of discharge, etc.) so the EV should still be informed at the beginning of the charging session in which mode it will be operating, and should still be able to refuse one mode.

8.4.3 Selection of service and service parameters

8.4.3.1 Overview

This subclause defines the reserved ServiceID ranges and the relevant services. These are exchanged and negotiated between the EVCC and the SECC by exchanging service discovery and service detail request response messages.

[V2G20-1355] The EVCC and the SECC shall implement the ServiceIDs as defined in Table 204.

NOTE 1 It is not mandatory for the EVCC or SECC to implement all these services. Table 204 simply defines the ServiceIDs to be used for the respective service if supported by the EVCC or SECC.

Table 204 — Definition of ServiceID, ServiceName and ServiceCategory

ServiceID (unsignedShort)	ServiceName	Description
0		Reserved by this document

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

ServiceID (unsignedShort)	ServiceName	Description
1	AC	AC energy transfer, physical layer according to ISO 15118-3 and ISO 15118-8
2	DC	DC energy transfer, physical layer according to ISO 15118-3 and ISO 15118-8
3	WPT	WPT, physical layer according to ISO 15118-8
4	DC_ACDP	DC Charging with ACDP, physical layer according to ISO 15118-8
5	AC_BPT	AC Charging with BPT, physical layer according to ISO 15118-3 and ISO 15118-8
6	DC_BPT	DC Charging with BPT, physical layer according to ISO 15118-3 and ISO 15118-8
7	DC_ACDP_BPT	DC Charging with ACDP and BPT, physical layer according to ISO 15118-8
8-64		Reserved by this document
65	Internet	Service for standard protocols like HTTP, HTTPs, FTP, etc. Refer to 8.4.3.2.6 for further details
66	ParkingStatus	service for approach and departure of EV
67 - 32767		Reserved by this document
32768 - 65535		reserved for implementation specific use

NOTE 2 The ACDP_SystemStatus will terminate together with the V2G communication at the end of the energy transfer session.

NOTE 3 The SECC and EVCC can chose which services they want to support. The full support of this document is not necessary.

[V2G20-1597] The EVCC shall only send one ServiceDetailReq per ServiceID.

[V2G20-1216] The EVCC shall only use ServiceIDs and ParameterSetIDs that were provided by the SECC during the current session, either via ServiceDiscoveryRes or ServiceDetailRes.

[V2G20-425] The SECC shall respond with a negative ResponseCode "FAILED_ServiceIDInvalid" if the EVCC provided a not previously offered ServiceID in the ServiceDetailReq.

[V2G20-433] The SECC shall respond with a negative ResponseCode "FAILED_ServiceSelectionInvalid" if the EVCC provided a not previously offered ServiceID, ParameterSetID pair in the ServiceSelectionReq.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1931] To indicate that SECC is capable of a ServiceRenegotiation, the SECC shall set the parameter ServiceRenegotiationSupported to "True" in the first ServiceDiscoveryRes message of the service session. To indicate that the SECC is not capable of ServiceRenegotiation, the SECC shall set the parameter ServiceRenegotiationSupported to "False" in the first ServiceDiscoveryRes message of the service session.

[V2G20-1932] The SECC shall send the identical value for the parameter ServiceRenegotiationSupported for all ServiceDiscoveryRes messages throughout a service session.

8.4.3.2 Service parameters for selected services

8.4.3.2.1 General

This subclause defines the service parameter list tables sent in ServiceDetailRes for each of the defined services.

[V2G20-2712] Whenever an EVCC or SECC intends to use one of the services listed below, the requirements defined for the service that is intended to be used shall be supported. In case a service is not used, the respective clauses may be ignored.

8.4.3.2.2 AC service

[V2G20-1356] The EVCC and the SECC shall implement the ServiceParameterList for AC charging as defined in Table 205.

Table 205 — Configuration parameters for AC_Charging

ParameterName	ParameterType	Values	Description
Connector	intValue	1: SinglePhase 2: ThreePhase	Usage of the connector.
ControlMode	intValue	1: Scheduled 2: Dynamic	Selection of which party (SECC or EVCC) is responsible to fulfill the mobility needs of this service session.
EVSENominalVoltage	intValue	0 to 500	Line voltage supported by the EVSE. This is the voltage measured between one phase and neutral. If the EVSE supports multiple phase energy transfer the EV might easily calculate the voltage between phases. This parameter is also used as reference for calculating the corresponding maximum charging current out of the Power values in the Schedule entities.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

MobilityNeedsMode	intValue	1: Mobility needs provided by EVCC 2: Mobility needs provided by SECC allowed	Indicate who can provide mobility needs information. Value 2 indicates that not only EVCC but also SECC can provide mobility-needs information (however, the EVCC shall always provide an initial mobility-needs information including DepartureTime). Value 2 can be selected only if Dynamic ControlMode was selected.
Pricing	intValue	0: No pricing 1: Absolute Pricing 2: Price Levels	Providing information about which pricing structure will be used in the offered schedules.

NOTE 1 Each ParameterSetID includes all parameters for a specific setup.

NOTE 2 In case a pricing method is offered that will not be used by the EVCC, the EVCC can ignore the provided information.

[V2G20-2651] In case the AC service was selected, unless otherwise stated, anytime an element is prefixed with AC (e.g. AC_CPDReqEnergyTransferMode), it shall be used.

[V2G20-2663] The SECC shall only offer MobilityNeedsMode equal to "2" when ControlMode is set to "2" (Dynamic).

8.4.3.2.2.1 AC BPT

[V2G20-1361] The EVCC and the SECC shall implement the ServiceParameterList for AC bidirectional power transfer services as defined Table 206.

Table 206 — Configuration parameters for AC BPT service

ParameterName	ParameterType	Values	Description
Connector	intValue	1: SinglePhase 2: ThreePhase	Usage of the connector.
ControlMode	intValue	1: Scheduled 2: Dynamic	Selection of which party (SECC or EVCC) is responsible to fulfill the mobility needs of this service session.
EVSENominalVoltage	intValue	0 to 500	Line voltage supported by the EVSE. This is the voltage measured between one phase and neutral. If the EVSE supports multiple phase energy transfer the EV might easily calculate the voltage between phases. This parameter is also used as reference for calculating the corresponding maximum charging current out of the power values in the schedule entities.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

MobilityNeedsMode	intValue	1: Mobility needs provided by EVCC 2: Mobility needs provided by SECC allowed	Indicate who can provide mobility needs information. Value 2 indicates that not only EVCC but also SECC can provide mobility-needs information (however, the EVCC shall always provide an initial mobility-needs information including DepartureTime). Value 2 can be selected only if DynamicControlMode was selected.
Pricing	intValue	0: No pricing 1: Absolute Pricing 2: Price Levels	Providing information about which pricing structure will be used in the offered schedules.
BPTChannel	intValue	1: Unified 2: Separated	Type of installed power transfer channel. Unified: Single channel Separated: Dual channel
GeneratorMode	intValue	1: GridFollowing 2: GridForming	Power converter behavior. For details see the IEC/TS 62898 series.
GridCodeIslandingDetectionMethod	intValue	1. ActiveDetection 2. PassiveDetection	Parameter to determine what method is used to detect landing.

NOTE 1 Each ParameterSetID includes all parameters for a specific setup.

NOTE 2 The EV can maintain islanding situation, until the EVSE shuts it down.

[V2G20-2652] In case the AC BPT service was selected, unless otherwise stated, anytime an element is prefixed with BPT or AC (e.g. BPT_AC_CPDReqEnergyTransferMode), it shall be used. In case both elements are available exclusively, BPT takes precedence.

The BPT channel parameter is used to make a distinction between single and dual channel architectures. In the former one, one single meter is used for the energy flows. In the later one, two separate meters are used for the two opposite energy flows. As a consequence, two switches are used and turned on / off depending on the current flow direction. The BPT channel parameter is used in both AC and DC charging services.

The following requirements apply in case of AC_BPT channel is equal to "separated" (e.g. dual channel) and the energy transfer needs to move from a charging phase to a discharging phase (or vice-versa):

[V2G20-1468] In case a service was selected where parameter BPTChannel was set to "2" (Separated), the SECC shall apply a power of 0 kW until contactors position are ready for the new phase.

In AC energy transfer mode, one could argue that the BPT Channel parameter might not be necessary, as the switch control operation is performed by the SECC. However, in case of a negotiated power profile (scheduled control mode), the EVCC should take into account the physical architecture (e.g. by planning 0 kW steps between charging and discharging phases).

[V2G20-1469] In case of bidirectional power transfer where parameter BPTChannel was set to "2" (Separated), both SECC and EVCC shall include 0 kW steps when switching from charging to discharging or vice versa.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2664] The SECC shall only offer MobilityNeedsMode equal to "2" when ControlMode is set to "2" (dynamic).

8.4.3.2.3 DC service

[V2G20-1357] The EVCC and the SECC shall implement the ServiceParameterList for DC charging as defined in Table 207.

Table 207 — Configuration parameters for DC_Charging

ParameterName	ParameterType	Values	Description
Connector	intValue	1: Core 2: Extended 3: Dual2 4: Dual4	Usage of the connector.
ControlMode	intValue	1: Scheduled 2: Dynamic	Selection of which party (SECC or EVCC) is responsible to fulfill the mobility needs of this service session.
MobilityNeedsMode	intValue	1: Mobility needs provided by EVCC 2: Mobility needs provided by SECC allowed	Indicate who can provide mobility needs information. Value 2 indicates that not only EVCC but also SECC can provide mobility-needs information (however, the EVCC shall always provide an initial mobility-needs information including DepartureTime). Value 2 can be selected only if DynamicControlMode was selected.
Pricing	intValue	0: No pricing 1: Absolute Pricing 2: Price Levels	Providing information about which pricing structure will be used in the offered schedules.

NOTE 1 Each ParameterSetID includes all parameters for a specific setup.

NOTE 2 In case a pricing method is offered that will not be used by the EVCC, the EVCC can ignore the provided information.

[V2G20-2653] In case the DC service was selected, unless otherwise stated, anytime an element is prefixed with DC (e.g. DC_CPDReqEnergyTransferMode), it shall be used.

[V2G20-2666] The SECC shall only offer MobilityNeedsMode equal to "2" when ControlMode is set to "2" (Dynamic).

8.4.3.2.3.1 DC BPT

If the EVCC requires DC BPT service, the SECC provides relevant service parameter list.

[V2G20-1360] The EVCC and the SECC shall implement the ServiceParameterList for DC bidirectional power transfer services as defined in Table 208.

Table 208 — Configuration parameters for DC BPT service

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

ParameterName	ParameterType	Values	Description
Connector	intValue	1: Core 2: Extended 3: Dual2 4: Dual4	Usage of the connector.
ControlMode	intValue	1: Scheduled 2: Dynamic	Selection of which party (SECC or EVCC) is responsible to fulfill the mobility needs of this service session.
MobilityNeedsMode	intValue	1: Mobility needs provided by EVCC 2: Mobility needs provided by SECC allowed	Indicate who can provide mobility needs information. Value 2 indicates that not only EVCC but also SECC can provide mobility-needs information (however, the EVCC shall always provide an initial mobility-needs information including DepartureTime). Value 2 can be selected only if DynamicControlMode was selected.
Pricing	intValue	0: No pricing 1: Absolute Pricing 2: Price Levels	Providing information about which pricing structure will be used in the offered schedules.
BPTChannel	intValue	1: Unified 2: Separated	Type of installed power transfer channel. Unified: Single channel Separated: Dual channel
GeneratorMode	intValue	1: GridFollowing 2: GridForming	Power converter behavior. For details see the IEC/TS 62898 series.

NOTE Each ParameterSetID includes all parameters for a specific setup.

[V2G20-2650] In case the DC BPT service was selected, unless otherwise stated, anytime an element is prefixed with BPT or DC (e.g. BPT_DC_CPDReqEnergyTransferMode), it shall be used. In case both elements are available exclusively, BPT takes precedence.

The following requirements apply in case of DC_BPT channel is equal to "separated" (e.g. Dual channel) and the energy transfer needs to move from a charging phase to a discharging phase (or vice-versa).

[V2G20-1467] In case a service was selected where parameter BPTChannel was set to "2" (Separated), the SECC shall apply a power of 0 kW until contactors position are ready for the new phase.

In DC energy transfer mode, one could argue that the BPT Channel parameter might not be necessary, as the switch control operation is performed by the SECC. However, in case of a negotiated power profile (scheduled control mode), the EVCC should take into account the physical architecture (e.g. by planning 0 kW steps between charging and discharging phases).

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1933] In case of bidirectional power transfer where parameter BPTChannel was set to "2" (Separated), both SECC and EVCC shall include 0 kW steps when switching from charging to discharging or vice versa.

[V2G20-2665] The SECC shall only offer MobilityNeedsMode equal to "2" when ControlMode is set to "2" (Dynamic).

8.4.3.2.4 WPT service

An EV and an EVSE that can employ WPT as an energy transfer mode, will support all WPT related services as listed in Table 204 indicated by their corresponding ServiceIDs. For each service, extra information can be exchanged and validated for compatibility during the ServiceDetailReq/Res messaging.

8.4.3.2.4.1 WPT_Charging

For ServiceName "WPT" different service configurations can be supported. The SECC provides the supported configurations in a list of parameters as defined in Table 209.

[V2G20-5059] The SECC shall implement the ServiceParameterList for WPT service as defined in Table 209.

Table 209 — Configuration parameters for WPT service

ParameterName	ParameterType	Values	Description
ControlMode	intValue	1: Scheduled 2: Dynamic	Selection of which party (SECC or EVCC) is responsible to fulfill the mobility needs of this service session
Pricing	intValue	0: No pricing 1: Absolute Pricing 2: Price Levels	Providing information about which pricing structure will be used in the offered schedules.

The following applies if the EVCC enters a standby period while using WPT:

[V2G20-5023] After receiving a WPT_AligmentCheckRes, the EVCC shall not send a PowerDeliveryReq with ChargeProgress set to "Standby".

[V2G20-5060] When the EVCC wants to enter a standby period, after having received WPT_ChargeLoopRes, the EVCC shall send a PowerDeliveryReq with parameter ChargeProgress set to "Standby", while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time.

[V2G20-5064] After receiving the PowerDeliveryRes with ResponseCode equal to "OK" as a response to a previous PowerDeliveryReq message with ChargeProgress equal to "Standby", the EVCC shall send a WPT_ChargeLoopReq with PowerRequest set to zero, while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time.

[V2G20-5068] When the EVCC wants to exit a standby period, after having received WPT_ChargeLoopRes, the EVCC shall send a PowerDeliveryReq with ChargeProgress set to "Start", "Stop" or "ScheduleRenegotiation" while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time.

8.4.3.2.5 ACDP service

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

For ServiceName "DC_ACDP" and "DC_ACDP_BPT" different service configurations can be supported. The SECC provides the supported configurations in a list of parameters as defined in Table 210 and Table 211.

[V2G20-4108] The EVCC and the SECC shall implement the ServiceParameterList for ACDP service as defined in Table 210 and Table 211 respectively.

Table 210 – Configuration parameters for DC_ACDP service

ParameterName	ParameterType	Values	Description
ControlMode	intValue	1: Scheduled 2: Dynamic	Selection of which party (SECC or EVCC) is responsible to fulfill the mobility needs of this service session.
MobilityNeedsMode	intValue	1: Mobility needs provided by EVCC 2: Mobility needs provided by SECC allowed	Indicate who can provide mobility needs information. Value 2 indicates that not only EVCC but also SECC can provide mobility-needs information (however, the EVCC shall always provide an initial mobility-needs information including DepartureTime). Value 2 can be selected only if DynamicControlMode was selected.

Table 211 — Configuration parameters for DC_ACDP_BPT service

ParameterName	ParameterType	Values	Description
ControlMode	intValue	1: Scheduled 2: Dynamic	Selection of which party (SECC or EVCC) is responsible to fulfill the mobility needs of this service session.
MobilityNeedsMode	intValue	1: Mobility needs provided by EVCC 2: Mobility needs provided by SECC allowed	Indicate who can provide mobility needs information. Value 2 indicates that not only EVCC but also SECC can provide mobility-needs information (however, the EVCC shall always provide an initial mobility-needs information including DepartureTime). Value 2 can be selected only if DynamicControlMode was selected.
BPTChannel	intValue	1: Unified 2: Separated	Type of installed power transfer channel. Unified: Single channel Separated: Dual channel
GeneratorMode	intValue	1: CurrentSource 2: VoltageSource	Power converter regulation mode.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

8.4.3.2.6 Internet service

Internet service is an optional value added service (VAS). This subclause provides some details of the parameters necessary to implement this service.

[V2G20-1362] The EVCC and the SECC shall implement the ServiceParameterList for internet service as defined in Table 212.

NOTE 1 This subclause simply provides some of the parameters necessary for implementing this service. It is up to the SA/CSO and OEM to define the security mechanisms necessary to secure this service.

Table 212 — ServiceParameterList for internet service

ParameterSetID (unsignedshort)	ParameterName = Protocol	ParameterName = Port	Description
0			Reserved by ISO.
1	stringValue = ftp	intValue = 20	Service to use internet access using FTP protocol via port 20.
2	stringValue = ftp	intValue = 21	Service to use internet access using FTP protocol via port 21.
3	stringValue = http	intValue = 80	Service to use internet access using HTTP protocol via port 80.
4	stringValue = https	intValue = 443	Service to use internet access using HTTPS protocol via port 443.
5 – 65535	service name according to IANA Service & Port Registry	port number according to IANA Service & Port Registry	Additional protocol port combinations which are supported by the SECC for internet access.

[V2G20-430] If the SECC supports additional protocol / port combinations beyond the definitions in Table 212, it shall use the service names and the assigned port numbers according according to IANA Service & Port Registry (i.e. the service name defined in IANA Service & Port Registry is transmitted as the "Protocol" and the port number defined in IANA Service & Port Registry is transmitted as "Port").

NOTE 2 It is assumed if an IANA Service & Port Registry defined service name and port number combination is applicable for both transport protocols, TCP and UDP, the SECC supports connections on TCP or UDP or on both for the respective combination.

8.4.3.2.7 Parking status service

Parking status is a VAS, applied in case that the EV is approaching a parking lot or leaving from it. It requires wireless communication for the reason that both use cases cannot have charging cable be connected. This use case covers separate sessions between parking status and charging with a couple of hours.

As for vehicle check in, one of main two objects is notification the completion of EV locating to EVSE and another is measured position exchange in order to help the EV locate the collect position.

Locating policy has two type variations, one is EV lead, measuring by EV with some of optical or other type of sensors, only inform the result to the EVSE. Another is EVSE lead, measuring by EVSE with similar

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

way as EV lead. This case requires communication session exchange measured position in form of difference from target.

Also locating control within an EV has two varieties, one is manual driving by customer with indication of difference information from target position, and another is auto parking function. Target position consists of device position within a parking lot and install offset within vehicle frame. Vehicle frame is defined as enveloping square to vehicle outline. These values are exchanged as ones of service parameter lists. Usually these requires calibration with registration to EVSEs in advance.

As for vehicle check out, main object is to inform EVSE of EV departure and vacant parking lot. It seems to be considered necessary for the EVSE detect vacation of EV without dedicated devices for it. Recently such devices have become more popular, so that this service is confirmed by them in some cases.

[V2G20-1365] The EVCC and the SECC shall implement the ServiceParameterList for parking status as defined in Table 213.

Table 213 — Configuration parameters for parking status

ParameterName	ParameterType	Values	Description
IntendedService	intValue	1: VehicleCheckIn 2: VehicleCheckOut	intended service during parking status session
ParkingStatusType	intValue	1: Auto/Internal 2: Auto/External 3: Manual/Internal 4: Manual/External	Type parking status; Auto: auto parking Manual: manual parking Internal: information exchange inside ISO 15118 External: information exchange outside ISO 15118

[V2G20-2136] If the EVCC and the SECC agree to select "VehicleCheckIn" with setting value of 1 to "IntendedService", "VehicleCheckIn" request and response shall apply to selected "ParkingStatusService" as unique type of message exchange set.

[V2G20-2137] If the EVCC and the SECC agree to select "VehicleCheckOut" with setting value of 2 to "IntendedService", "VehicleCheckOut" request and response shall apply to selected "ParkingStatusService" as unique type of message exchange set.

8.5 V2G communication timing

8.5.1 Overview

This subclause describes the timing and error handling for the V2G communication session with EXI encoded messages of V2GTP payload type in the range of 0x8001 up to 0x81FF. The error handling is based on timers enabling the EVCC and the SECC to monitor the V2G message exchange. For the detection of missing or delayed messages the EVCC and the SECC use predefined timeout values as error criteria. Whenever a timer is equal or larger than the related timeout the related error handling is processed.

The monitoring of a V2G communication message exchange is based on two timer categories:

- message timer: monitors the exchange of a request message and the corresponding response message (request-response-pair);
- sequence timer: monitors the exchange of multiple request-response-pairs.

8.5.2 Common

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

To enable error handling for a V2G communication session setup the EVCC monitors the time between reception of SECC discovery response, SessionSetupRes and PowerDeliveryRes, respectively. This allows the EVCC to decide about a successful or failed charging session after the defined timeouts.

The monitoring of a V2G communication session is based on the following timing concepts:

- message timing: monitors the timing between the request and the response of a Request-Response-Pair. This allows, for example, the EVCC application to initiate the error handling if no response is sent;
- sequence timing: monitors the timing of subsequent request-response-pairs. This allows, for example, the SECC application to initiate the error handling if an expected next request message was not sent;
- ongoing timing: monitors the timing in case of sending a request-response-pair repeatedly based on the parameter EVSEProcessing equal to "Ongoing". This allows, for example, the EVCC to initiate the error handling in case the SECC exceeds the processing time;
- communication setup timing: monitors the time from the moment of an established data link until the session setup message. It allows deciding if the communication setup was successful within a defined time.

The timers are compared to predefined time values as decision criterion. The EVCC and the SECC distinguish between two categories:

- timeout: if the specified time is exceeded the related error handling is initiated;
- performance time: if the specified time is exceeded the performance requirement is not fulfilled.

NOTE 1 While exceeding a timeout always causes an error handling, the performance time does not necessarily cause error handling if not defined differently by requirements. Depending on the system behavior (e.g. transmission time) no error can occur if the corresponding communication partner does not detect a timeout but the probability for causing a timeout is high.

NOTE 2 Timeouts are observed at the application layer where they are also enforced (according to requirement [V2G20-1966] for example). It is important for each sending party to keep in mind that all processing (e.g. TLS encryption) and transmission delays between both application layer sides will be part of the observed timing on the receiving side. See Figure 212 for a detailed illustration.

NOTE 3 This document supports PLC and WiFi communication. Both technologies come with different average and worst case latencies as well as congestion and retransmissions characteristics. For example, in WiFi networks real world round trip latencies can reach up to 25 ms to 100 ms or even more. As mentioned before it is important that those latencies are taken into account when deciding on the implementation of a message timing strategy in the application layer of the sending side. The timing requirements of Table 215 have been defined with the assumption that round trip end-to-end transmission delays will never exceed 250 ms.

8.5.3 DC service

The monitoring of a DC V2G communication session includes the following timing concepts:

- DC_CableCheck timing: The monitoring of the cable check is carried out by the EV using the V2G_EVCC_DC_CableCheck_Timer. It is started when the EV requests the EVSE to start the Cable Check, and ends when the EVSE has finished the cable check, or when the V2G_EVCC_DC_CableCheck_Timer expires;
- DC_PreCharge timing: The monitoring of the pre charge is carried out by the EV using the V2G_EVCC_DC_PreCharge_Timer. It is started when the EV starts the pre charging by sending the first DC_PreChargeReq message, and ends when the pre charging has finished, indicated by the EV determining that the EVSE output voltage, as measured inside the EV, has sufficiently been adjusted to the EV RESS voltage, or when the V2G_EVCC_DC_PreCharge_Timer expires.

8.5.4 Message sequence and communication session

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

8.5.4.1 Common

Message timers, sequence timers, timeouts, and performance times are defined for EVCC and SECC separately and are summarized in Table 214. Timeouts and performance times are parameterized for messages separately to describe different processing times. Table 215 defines the common values for each V2G message type.

[V2G20-434] The EVCC shall implement the EVCC specific timeouts and performance times defined in Table 214 and Table 215.

[V2G20-435] The SECC shall implement the SECC specific timeouts and performance times defined in Table 214 and Table 215.

Table 214 — Common EVCC and SECC timers, timeouts, performance times

Name	Type	Applicable for	
		EVCC	SECC
V2G_EVCC_Msg_Timer	Message timer in the EVCC	x	
V2G_SECC_Msg_Timer	Message timer in the SECC		x
V2G_EVCC_Sequence_Timer	Sequence timer in the EVCC	x	
V2G_SECC_Sequence_Timer	Sequence timer in the SECC		x
V2G_EVCC_Ongoing_Timer	Ongoing timer in the EVCC	x	
V2G_SECC_Ongoing_Timer	Ongoing timer in the SECC		x
V2G_EVCC_Msg_Timeout (MessageType)	Timeout for the message timer The value is defined depending on the parameter MessageType as defined in Table 215.	x	
V2G_SECC_Msg_Performance_Time (MessageType)	Performance time for the message timer The value is defined depending on the parameter MessageType as defined in Table 215.		x
V2G_EVCC_Sequence_Performance_Time	Performance time for the sequence timer as defined in Table 215.	x	
V2G_SECC_Sequence_Timeout	Timeout for the sequence timer as defined in Table 215.		x
V2G_EVCC_Ongoing_Timeout	Timeout for ongoing timer	x	
V2G_SECC_Ongoing_Performance_Time	Performance time for ongoing timer		x

Table 215 — Common EVCC and SECC message sequence and session timing parameter values

Name	MessageType	Value [s]
V2G_EVCC_Msg_Timeout(MessageType)	SupportedAppProtocolReq	2
	SessionSetupReq	2
	VehicleCheckInReq	2

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Name	MessageType	Value [s]
	VehicleCheckOutReq	2
	AuthorizationSetupReq	2
	AuthorizationReq	2
	CertificateInstallationReq	5
	ServiceDiscoveryReq	2
	ServiceDetailReq	5
	ServiceSelectionReq	2
	ChargeParameterDiscoveryReq	2
	ScheduleExchangeReq	2
	PowerDeliveryReq	2
	MeteringConfirmationReq	2
	SessionStopReq	2
V2G_SECC_Msg_Performance_Time(MessageType)	SupportedAppProtocolRes	1,5
	SessionSetupRes	1,5
	VehicleCheckInRes	1,5
	VehicleCheckOutRes	1,5
	AuthorizationSetupRes	1,5
	AuthorizationRes	1,5
	CertificateInstallationRes	4,5
	ServiceDiscoveryRes	1,5
	ServiceDetailRes	4,5
	ServiceSelectionRes	1,5
	ChargeParameterDiscoveryRes	1,5
	ScheduleExchangeRes	1,5
	PowerDeliveryRes	1,5
	MeteringConfirmationRes	1,5
	SessionStopRes	1,5
V2G_EVCC_Sequence_Performance_Time	(all other messages)	40
V2G_SECC_Sequence_Timeout	(all other messages)	60
V2G_EVCC_Ongoing_Timeout	Response messages with parameter EVSEProcessing equal to "Ongoing"	60
V2G_SECC_Ongoing_Timeout	Request messages with parameter EVProcessing equal to "Ongoing"	60

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

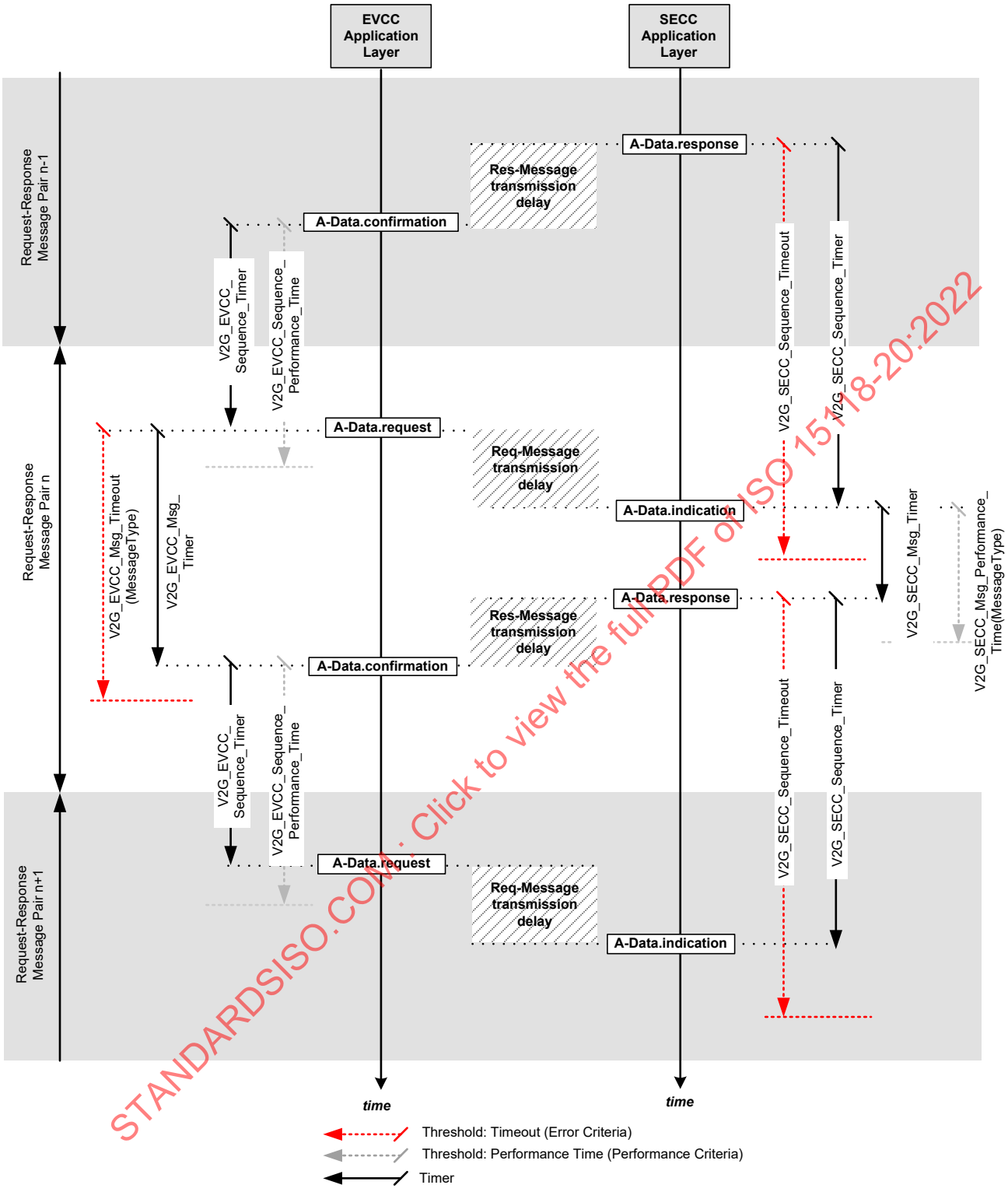
© ISO 2022 – All rights reserved

Name	MessageType	Value [s]
V2G_EVCC_Ongoing_Performance_Time	Request messages with parameter EVProcessing equal to "Ongoing"	55
V2G_SECC_Ongoing_Performance_Time	Response messages with parameter EVSEProcessing equal to "Ongoing"	55

Figure 212 illustrates how the common message timers, sequence timers, timeouts, and performance times are applied in the EVCC and the SECC.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Figure 212 — Message sequence and session timing

8.5.4.1.1 EVCC timing for request-response message pairs

[V2G20-436] The EVCC shall set the timeout V2G_EVCC_Msg_Timeout depending on the value MessageType as defined in Table 215, reset the V2G_EVCC_Msg_Timer and start monitoring the V2G_EVCC_Msg_Timer when it sends a request message.

NOTE 1 In this document sending a request message is described by A-Data.request.

© ISO 2022 – All rights reserved

[V2G20-437] The EVCC shall wait for the response message corresponding to the request message sent before.

[V2G20-438] The EVCC shall stop waiting for the response message and stop monitoring the V2G_EVCC_Msg_Timer when V2G_EVCC_Msg_Timer is equal or larger than V2G_EVCC_Msg_Timeout(MessageType) and no response message was received. It shall then apply the error handling as defined in 8.6.

NOTE 2 In this document receiving a response message is described by A-DATA.confirmation.

[V2G20-439] The EVCC shall stop waiting for the response message and stop monitoring the V2G_EVCC_Msg_Timer when V2G_EVCC_Msg_Timer is smaller than V2G_EVCC_Msg_Timeout(MessageType) and it received a response message. It shall then process the response message as defined in 8.6.

NOTE 3 In this document receiving a response message is described by A-Data.confirmation.

[V2G20-440] The EVCC shall ignore any message that is not a valid response message.

8.5.4.1.2 SECC timing for response-request message sequence

[V2G20-441] The SECC shall set the timeout V2G_SECC_Sequence_Timeout to the value as defined in Table 215, reset the V2G_SECC_Sequence_Timer and start monitoring the V2G_SECC_Sequence_Timer when it sends a response message.

NOTE 4 In this document sending a response message is described by A-Data.response.

[V2G20-442] The SECC shall wait for a request message.

[V2G20-443] The SECC shall stop waiting for a request message and stop monitoring the V2G_SECC_Sequence_Timer when V2G_SECC_Sequence_Timer is equal or larger than V2G_SECC_Sequence_Timeout and no request message was received. It shall then stop the V2G communication session.

NOTE 5 In this document receiving a request message is described by A-Data.indication. A-Data.indication (A_Msg="message name") signalizes the successful reception of a valid request message for the V2G message that is given by A_Msg where "Valid message" means that all mandatory elements are filled in so that it can be deserialized.

[V2G20-444] The SECC shall stop waiting for a request message and stop monitoring the V2G_SECC_Sequence_Timer when V2G_SECC_Sequence_Timer is smaller than V2G_SECC_Sequence_Timeout and it received a request message. It shall then process the response message as defined in 8.6.

NOTE 6 In this document receiving a request message is described by A-Data.indication.

[V2G20-445] The SECC shall ignore any message that is not a valid request message.

8.5.4.2 AC specific message sequence and session timing

[V2G20-1499] The EVCC shall implement the EVCC specific AC timeouts and performance times defined in Table 216.

[V2G20-1500] The SECC shall implement the SECC specific AC timeouts and performance times defined in Table 216.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 216 — AC EVCC and SECC timeouts and performance times

Name	MessageType	Value [s]
V2G_EVCC_Msg_Timeout(MessageType)	AC_ChargeLoopReq	0,5
V2G_SECC_Msg_Performance_Time(MessageType)	AC_ChargeLoopReq	0,25
V2G_EVCC_Sequence_Performance_Time	AC_ChargeLoopReq	0,25
V2G_SECC_Sequence_Timeout	AC_ChargeLoopRes	0,5

8.5.4.3 DC specific message sequence and session timing

[V2G20-1501] The EVCC shall implement the EVCC specific DC timeouts and performance times defined in Table 217.

[V2G20-1502] The SECC shall implement the SECC specific DC timeouts and performance times defined in Table 217.

Table 217 — DC EVCC and SECC timeouts and performance times

Name	MessageType	Value [s]
V2G_EVCC_Msg_Timeout(MessageType)	DC_CableCheckReq	2
	DC_PreChargeReq	2
	DC_ChargeLoopReq	0.5
	DC_WeldingDetectionReq	2
V2G_SECC_Msg_Performance_Time(MessageType)	DC_CableCheckReq	1,5
	DC_PreChargeReq	1,5
	DC_ChargeLoopReq	0,25
	DC_WeldingDetectionReq	1,5
V2G_EVCC_Sequence_Performance_Time	DC_ChargeLoopReq	0,25
V2G_SECC_Sequence_Timeout	DC_ChargeLoopRes	0,5

8.5.4.4 WPT specific message sequence and session timing

[V2G20-5069] The EVCC shall implement the EVCC specific WPT timeouts and performance times defined in Table 218.

[V2G20-5070] The SECC shall implement the SECC specific WPT timeouts and performance times defined in Table 218.

Table 218 — WPT EVCC and SECC timeouts and performance times

Name	MessageType	Value [s]
V2G_EVCC_Msg_Timeout(MessageType)	WPT_FinePositioningSetupReq	2
	WPT_FinePositioningReq	2
	WPT_PairingReq	2
	WPT_AlignmentCheckReq	2

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

	WPT_ChargeLoopReq	0,5
V2G_SECC_Msg_Performance_Time(MessageType)	WPT_FinePositioningSetupReq	1,5
	WPT_FinePositioningReq	1,5
	WPT_PairingReq	1,5
	WPT_AlignmentCheckReq	1,5
	WPT_ChargeLoopReq	0,25
V2G_EVCC_Sequence_Performance_Time	WPT_ChargeLoopReq	0,25
V2G_SECC_Sequence_Timeout	WPT_ChargeLoopRes	0,5

8.5.4.5 ACDP specific message sequence and session timing

[V2G20-4020] The EVCC shall implement the EVCC specific ACDP timeouts and performance times defined in Table 219.

[V2G20-4021] The SECC shall implement the SECC specific ACDP timeouts and performance times defined in Table 219.

Table 219 — ACDP EVCC and SECC timeouts and performance times

Name	MessageType	Value [s]
V2G_EVCC_Msg_Timeout(MessageType)	ACDP_VehiclePositioningReq	2
	ACDP_ConnectReq	2
	ACDP_DisconnectReq	2
	ACDP_SystemStatusReq	2
V2G_SECC_Msg_Performance_Time(MessageType)	ACDP_VehiclePositioningReq	1,5
	ACDP_ConnectReq	1,5
	ACDP_DisconnectReq	1,5
	ACDP_SystemStatusReq	1,5

8.5.5 Session setup and ready to charge

8.5.5.1 Common

Timing parameters applicable to the common communication session setup and ready to charge time defined in this document are shown in Table 220. Table 221 defines the values for the related common performance times and the timeouts.

Table 220 — Common EVCC and SECC V2G communication session setup timing parameters

Parameter name	Definition	Implementation	
		EVCC	SECC
V2G_EVCC_CommunicationSetup_Timer	Communication setup timer in the EVCC	x	
V2G_SECC_CommunicationSetup_Timer	Communication setup timer in the SVCC		x

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Parameter name	Definition	Implementation	
		EVCC	SECC
V2G_EVCC_CommunicationSetup_Timeout	Timeout for the communication setup timer as defined in Table 221.	x	
V2G_SECC_CommunicationSetup_Performance_Time	Performance time for the communication setup timer as defined in Table 221.		x

[V2G20-605] The EVCC and SECC shall implement the timing parameter values defined in Table 221.

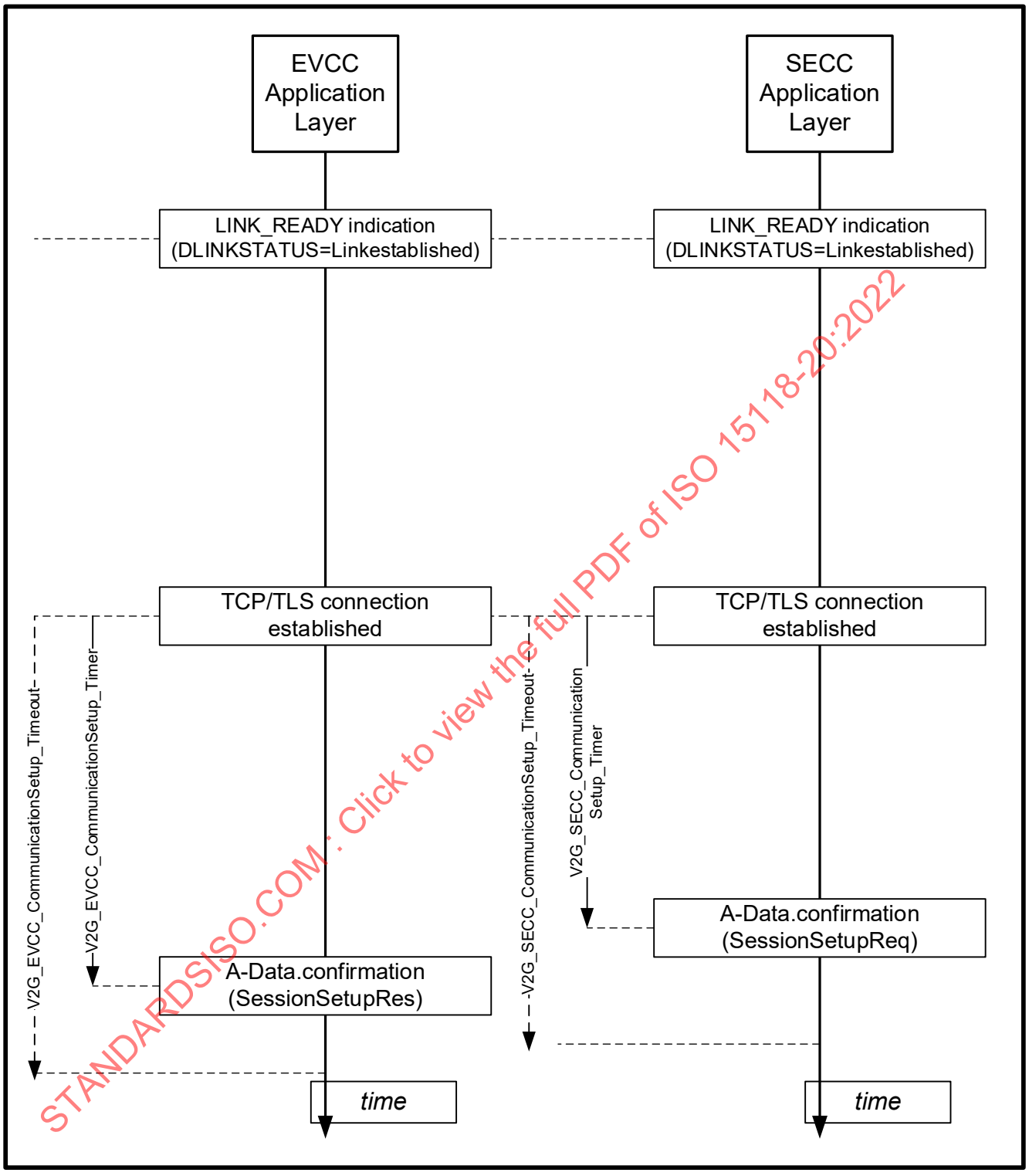
Table 221 — Common EVCC and SECC message sequence and session timing parameter values

Parameter name	Value [s]	Implementation	
		EVCC	SECC
V2G_SECC_CommunicationSetup_Performance_Time	18		x
V2G_EVCC_CommunicationSetup_Timeout	20	x	

Figure 213 illustrates how the timing parameters defined in Table 220 are applied.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Figure 213 — CommunicationSetup timing

8.5.5.1.1 EVCC Timing for communication session setup

[V2G20-2295] If the EVCC receives an SDP response message with parameter DiagStatus equal to "Ongoing" for the first time it shall start the timer V2G_EVCC_Ongoing_Timer and wait

© ISO 2022 – All rights reserved

for parameter DiagStatus equal to "Finished with EVSEID" or parameter DiagStatus equal to "Finished without EVSEID".

[V2G20-2296] If [V2G20-2295] applies, the EVCC shall stop and then restart the SDP process when V2G_EVCC_Ongoing_Timer is equal or larger than V2G_EVCC_Ongoing_Timeout and no parameter EVSEProcessing equal to "Finished" has been received.

[V2G20-2298] The EVCC shall set the timeout V2G_EVCC_CommunicationSetup_Timeout to the value as defined in Table 221, reset the V2G_EVCC_CommunicationSetup_Timer and start monitoring the V2G_EVCC_CommunicationSetup_Timer when a successful TCP/TLS connection has been established.

[V2G20-447] The EVCC shall wait for the SessionSetupRes message.

[V2G20-448] The EVCC shall stop waiting for the SessionSetupRes message and stop monitoring the V2G_EVCC_CommunicationSetup_Timer when V2G_EVCC_CommunicationSetup_Timer is equal or larger than V2G_EVCC_CommunicationSetup_Timeout and no SessionSetupRes message was received. It shall then stop the V2G communication session.

NOTE 1 In this document receiving the response message "SessionSetupRes" is described by A-Data.confirmation (SessionSetupRes).

[V2G20-449] The EVCC shall stop waiting for the SessionSetupRes message and stop monitoring the V2G_EVCC_CommunicationSetup_Timer when V2G_EVCC_CommunicationSetup_Timer is smaller than V2G_EVCC_CommunicationSetup_Timeout and a SessionSetupRes message was received. It shall then process the response message as defined in 8.6.

NOTE 2 In this document receiving the response message "SessionSetupRes" is described by A-Data.confirmation (SessionSetupRes).

8.5.5.1.2 SECC Timing for communication session setup

[V2G20-2303] The SECC shall set the timeout V2G_SECC_CommunicationSetup_Performance_Time the value as defined in Table 221, reset the V2G_SECC_CommunicationSetup_Timer and start monitoring the V2G_SECC_CommunicationSetup_Timer when a successful TCP/TLS connection has been established.

[V2G20-715] The SECC shall wait for the SessionSetupReq message.

[V2G20-2300] The SECC shall stop waiting for SessionSetupReq and stop monitoring the V2G_SECC_CommunicationSetup_Timer when V2G_SECC_CommunicationSetup_Timer is smaller than V2G_SECC_CommunicationSetup_Performance_Time and a SessionSetupRes message was received. It shall then process the response message as defined in 8.6.

[V2G20-716] The SECC shall stop waiting for SessionSetupReq and stop monitoring the V2G_SECC_CommunicationSetup_Timer when V2G_SECC_CommunicationSetup_Timer is equal or larger than V2G_SECC_CommunicationSetup_Performance_Time and no SessionSetupRes message was sent. It shall then apply [V2G20-034].

NOTE In this document sending the response message "SessionSetupRes" is described by A-Data.response(SessionSetupRes).

8.5.5.1.3 EVCC Timing for EVSEProcessing parameter

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-710] If the EVCC receives a V2G response message with parameter EVSEProcessing equal to "Ongoing" for the first time in a response message it shall start the timer V2G_EVCC_Ongoing_Timer and wait for parameter EVSEProcessing equal to "Finished".

[V2G20-2101] If [V2G20-710] applies, the EVCC may stop the V2G communication session when V2G_EVCC_Ongoing_Timer is equal or larger than V2G_EVCC_Ongoing_Timeout and no parameter EVSEProcessing equal to "Finished" has been received.

8.5.5.1.4 SECC Timing for EVSEProcessing parameter

[V2G20-712] If the SECC sends a V2G response message with parameter EVSEProcessing equal to "Ongoing" for the first time in a response message it shall start the timer V2G_SECC_Ongoing_Timer.

[V2G20-2102] If [V2G20-712] applies, the SECC may send ResponseCode equal to "FAILED" when V2G_SECC_Ongoing_Timer is equal or larger than V2G_SECC_Ongoing_Performance_Time and no parameter EVSEProcessing equal to "Finished" has been sent. The SECC shall stop the V2G communication session.

8.5.5.2 DC specific timings

Timing parameters applicable to the DC communication session setup and ready to charge time defined in this document are shown in Table 222. Table 223 defines the values for the related DC performance times and the timeouts.

Table 222 — DC specific EVCC and SECC V2G communication session setup timing parameters

Parameter name	Definition	Implementation	
		EVCC	SECC
V2G_EVCC_DC_CableCheck_Timer	Cable check timer in the EVCC	x	
V2G_SECC_DC_CableCheck_Timer	Cable check timer in the SECC		x
V2G_EVCC_DC_PreCharge_Timer	DC_PreCharge timer in the EVCC	x	
V2G_SECC_DC_PreCharge_Timer	DC_PreCharge timer in the SECC		x
V2G_EVCC_DC_CableCheck_Timeout	Timeout for the DC_CableCheck timer as defined in Table 223.	x	
V2G_SECC_DC_CableCheck_Performance_Time	Performance time for the DC_CableCheck timer as defined in Table 223.		x
V2G_EVCC_DC_PreCharge_Timeout	Timeout for the DC_PreCharge timer as defined in Table 223.	x	
V2G_SECC_DC_PreCharge_Performance_Time	Performance time for the DC_PreCharge timer as defined in Table 223.		x

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1774] The EVCC and SECC shall implement the DC timing parameter values defined in Table 223.

Table 223 — DC specific EVCC and SECC message sequence and session timing parameter values

Parameter name	Value [s]	Implementation	
		EVCC	SECC
V2G_SECC_DC_CableCheck_Performance_Time	38		x
V2G_EVCC_DC_CableCheck_Timeout	40	x	
V2G_SECC_DC_PreCharge_Performance_Time	9		x
V2G_EVCC_DC_PreCharge_Timeout	10	x	

8.5.5.2.1 EVCC Timing for cable check

[V2G20-700] The EVCC shall set the timeout V2G_EVCC_DC_CableCheck_Timeout to the value as defined in Table 223, reset the V2G_EVCC_DC_CableCheck_Timer and start monitoring the V2G_EVCC_DC_CableCheck_Timer when sending the message DC_CableCheckReq for the first time in a charging session.

NOTE 1 In this document, sending a request message is described by A-Data.request.

[V2G20-1397] The EVCC shall wait for the cable check of the EVSE to finish indicated by the reception of a DC_CableCheckRes with ResponseCode equal to "OK" and EVSEProcessing equal to "Finished".

NOTE 2 In this document, receiving a response message is described by A-Data.confirmation.

[V2G20-1398] The EVCC shall stop waiting for the Cable check of the EVSE to finish and stop monitoring the V2G_EVCC_DC_CableCheck_Timer when V2G_EVCC_DC_CableCheck_Timer is equal or larger than V2G_EVCC_DC_CableCheck_Timeout. It shall then apply the error handling as defined in 8.6.

[V2G20-1399] The EVCC shall stop waiting for the cable check of the EVSE to finish and stop monitoring the V2G_EVCC_DC_CableCheck_Timer if V2G_EVCC_DC_CableCheck_Timer is smaller than V2G_EVCC_DC_CableCheck_Timeout and a DC_CableCheckRes message with ResponseCode equal to "OK" and EVSEProcessing equal to "Finished" was received. It shall then process the response message as defined in 8.6.

NOTE 3 In this document, receiving a response message is described by A-Data.confirmation.

8.5.5.2.2 EVCC Timing for pre charging

[V2G20-704] The EVCC shall set the timeout V2G_EVCC_DC_PreCharge_Timeout to the value as defined in Table 223, reset the V2G_EVCC_DC_PreCharge_Timer and start monitoring the V2G_EVCC_DC_PreCharge_Timer when sending the message DC_PreChargeReq for the first time in a charging session.

NOTE 4 In this document, sending a request message is described by A-Data.request.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1400] The EVCC shall wait for the pre charging to finish, indicated by the EV determining that the EVSE output voltage, as measured inside the EV, has sufficiently been adjusted to the EV RESS voltage.

[V2G20-706] The EVCC shall stop waiting for the pre charging to finish and stop monitoring the V2G_EVCC_DC_PreCharge_Timer when V2G_EVCC_DC_PreCharge_Timer is equal or larger than V2G_EVCC_DC_PreCharge_Timeout. It shall then apply the error handling as defined in 8.6.

[V2G20-1401] The EVCC shall stop monitoring the V2G_EVCC_DC_PreCharge_Timer when V2G_EVCC_DC_PreCharge_Timer is smaller than V2G_EVCC_DC_PreCharge_Timeout and pre charging has finished, indicated by the EV determining that the EVSE output voltage, as measured inside the EV, has sufficiently been adjusted to the EV RESS voltage. It shall then process the response message as defined in 8.6.

8.5.5.3 WPT specific timings

Operational timing requirements are given in IEC 61980-2.

8.5.6 V2G message synchronization for AC and DC with IEC 61851-1 signalling

8.5.6.1 Overview

ISO 15118 based energy transfer control extends PWM signal over a control pilot wire according to IEC 61851-1:2017, Annex A. For this, the messaging on application layer is synchronized with the CP states defined in IEC 61851-1:2017, Annex A.

ISO 15118 based messaging is able to manage the AC and DC charging process for a complete charging session from the beginning to the end in 5 % or 100 % duty cycle case.

In this subclauses, terms and definitions in requirements are applied as defined in ISO 15118-3 and IEC 61851-1:2017, Annex A.

Figure 214 shows an example for AC energy transfer with BC and HLC-C in relation to service session and phases of data link setup, V2G setup and V2G power transfer loop during a V2G communication session.

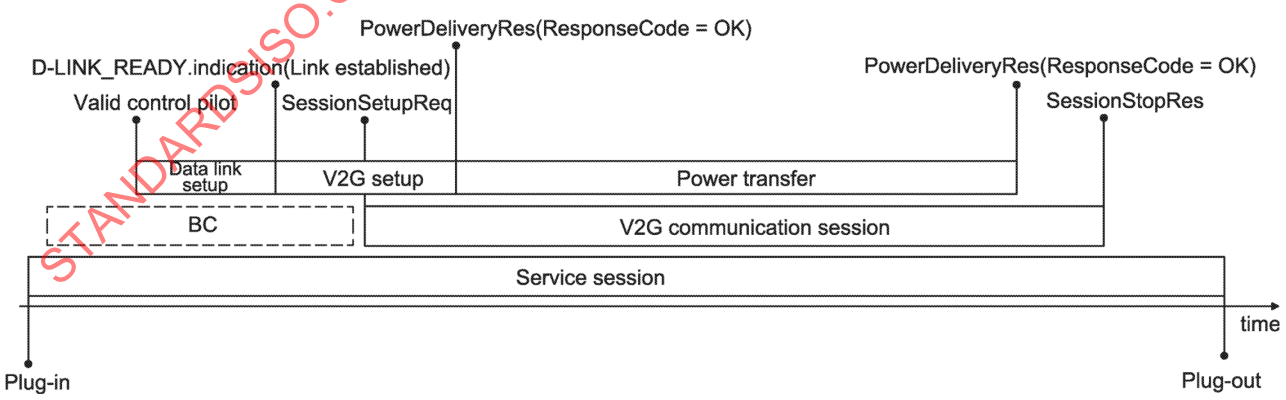


Figure 214 — AC example for BC and HLC-C energy transfer in relation to service session

The V2G power transfer loop is defined as V2G messaging phase for controlling the energy transfer process by the ISO 15118 series in normal operation. The power transfer phase under control of the ISO 15118 series is defined as high level communication charging (HLC-C).

The entry and exit conditions for the V2G power transfer loop are as follows:

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

- entry condition: PowerDeliveryRes message with parameter ResponseCode equal to OK after PowerDeliveryReq with ChargeProgress equals "Start";
- exit condition: PowerDeliveryRes with parameter ResponseCode equal to OK after PowerDeliveryReq with ChargeProgress equals "Stop".

Besides the requirements for request-response message pairs and request-response message sequences as defined in 8.6.4, the EVCC and the SECC shall conform to the requirements as defined in 8.5.6.2, 8.5.6.3, and 8.5.6.4.

8.5.6.2 Common requirements for AC and DC

The following requirements apply for the EVCC.

[V2G20-1615] The EVCC shall use the message PowerDeliveryReq with parameter ChargeProgress set to "Start" to start HLC-C based energy transfer.

[V2G20-1616] If [V2G20-1615] applies and the PowerDeliveryRes message has been received with ResponseCode set to OK, the EV shall apply the energy transfer limits according to the V2G messaging.

[V2G20-1310] The EV shall stop the energy transfer (no current drawn by EV) before sending the message PowerDeliveryReq with the parameter ChargeProgress set to "Stop".

[V2G20-1311] The EVCC shall use the message PowerDeliveryReq with parameter ChargeProgress set to "Stop" to stop HLC-C based energy transfer.

In general, the ISO 15118 series is based on the requirements as defined in IEC 61851-1.

[V2G20-843] An ISO 15118-enabled EV shall conform to IEC 61851-1.

[V2G20-731] If [V2G20-1463] applies, the EVCC can establish a new or resumed V2G communication session by applying [V2G20-014].

[V2G20-2200] If [V2G20-728] applies, the EVCC can establish a new V2G communication session by applying [V2G20-014].

Since the V2G session was terminated due to an error, the EVCC has to mitigate the conditions that resulted in the error before establishing a new V2G communication session.

The following requirements apply for the SECC.

[V2G20-1404] ISO 15118-enabled EVSE shall conform to IEC 61851-1.

[V2G20-2030] If [V2G20-1632] applies, the SECC shall be allowed to establish a new or resumed V2G communication session by applying [V2G20-027].

[V2G20-2115] At the point in time when requesting pause by setting the parameter EVSENotification to "Pause" in dynamic control mode, the SECC shall ensure that the applied power level is equal to 0 kW (no current drawn by EV or EVSE).

The following applies for the EVCC during a standby period.

[V2G20-1390] When the EVCC wants to enter a standby period, after having received the ScheduleExchangeRes with parameter "EVSEProcessing" set to "Finished", the EVCC shall send a PowerDeliveryReq with parameter ChargeProgress set to "Standby",

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time.

[V2G20-2113] After receiving the PowerDeliveryRes with ResponseCode equal to "OK" as a response to a previous PowerDeliveryReq message with ChargeProgress equal to "Standby", the EVCC shall send a ChargeLoopReq while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time.

[V2G20-2116] At the point in time when requesting standby by PowerDeliveryReq with parameter ChargeProgress= "Standby", the EVCC shall ensure that the applied power level is equal to zero kW (no current drawn by EV or EVSE).

[V2G20-2117] After receiving a PowerDeliveryRes with ResponseCode equal to "OK" as a response to the previous PowerDeliveryReq message with ChargeProgress equal to "Standby", the EVCC shall not process any elements in the ChargeLoopRes except EVSEStatus, ResponseCode, MeterInfo and Receipt, until the next PowerDeliveryReq message with ChargeProgress set to "Start", "Stop", or "Renegotiate" is send.

During standby both EV and EVSE contactors are to stay closed. The standby concept is solely used as communication state within this document and therefore is not reflected in related documents, e.g. IEC 61851-1 or IEC 61851-23.

[V2G20-1391] When the EVCC wants to enter a standby period, after having received ChargeLoopRes, the EVCC shall send a PowerDeliveryReq with parameter ChargeProgress set to "Standby", while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time.

[V2G20-1393] When the EVCC wants to exit a standby period, after having received ChargeLoopRes, the EVCC shall send a PowerDeliveryReq with parameter ChargeProgress set to "Start", "Stop", or "Renegotiate", while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time.

[V2G20-1394] When the EVCC wants to enter a standby period, after having received MeteringConfirmationRes, the EVCC shall send a PowerDeliveryReq with parameter ChargeProgress set to "Standby", while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time.

[V2G20-1395] When the EVCC wants to exit a standby period, after having received MeteringConfirmationRes, the EVCC shall send a PowerDeliveryReq with parameter ChargeProgress set to "Start", "Stop", or "Renegotiate", while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time.

The following applies for the SECC during a standby period.

[V2G20-1385] The SECC shall enter standby, after having received PowerDeliveryReq with ChargeProgress set to "Standby", by sending a PowerDeliveryRes with ResponseCode is set to "OK" while V2G_SECC_Sequence_Timer is smaller than V2G_SECC_Sequence _Timeout.

[V2G20-2118] After sending a PowerDeliveryRes with ResponseCode equal to "OK" as a response to the previous PowerDeliveryReq message with ChargeProgress equal to "Standby", the SECC shall not process any elements in the ChargeLoopReq except MeterInfoRequested and DisplayParameters, until the next PowerDeliveryReq message with ChargeProgress set to "Start", "Stop", or "Renegotiate" is received.

STANDARDSISO.COM Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

During standby both EV and EVSE contactors are to stay closed. The standby concept is solely used as communication state within this document and therefore is not reflected in related documents, e.g. IEC 61851-1 or IEC 61851-23.

[V2G20-1386] The SECC shall exit standby, after having received PowerDeliveryReq with ChargeProgress set to "Start", "Stop", or "Renegotiate", by sending a PowerDeliveryRes with ResponseCode set to "OK", while V2G_SECC_Sequence_Timer is smaller than V2G_SECC_Sequence_Timeout.

[V2G20-1700] The message PowerDeliveryRes shall contain the ResponseCode "WARNING_StandbyNotAllowed" if the EVCC has sent a PowerDeliveryReq containing the parameter ChargeProgress set to "Standby" and the SECC does not allow for a standby period. All mandatory parameters shall be filled in with arbitrary XSD conform values. All values shall be chosen in a way that results in a minimal size of the response message.

The following applies if the EVCC is unable to enter a standby period.

[V2G20-1396] After receiving the message "PowerDeliveryRes" with ResponseCode equal to "WARNING_StandbyNotAllowed", the EVCC shall ignore all other parameters of the response message and shall do one (1) of the following:

- Proceed with the initially agreed EVPowerProfile or in dynamic control mode follow the demand of the SECC within V2G_EVCC_Sequence_Performance_Timeout according to Table 215. The next allowed message shall be the ChargeLoopReq message. Refer to 8.3.1 and 8.3.4.1 for details of requesting standby of the V2G session.

OR

- Request schedule renegotiation within V2G_EVCC_Sequence_Performance_Timeout according to Table 215. Refer to Annex F for further details.

OR

- Stop the V2G communication according to requirements defined 7.4.

The following applies if the SECC declines a request to enter a standby period from the EVCC.

[V2G20-1387] After receiving the PowerDeliveryReq with ChargeProgress set to "Standby", the SECC shall send a PowerDeliveryRes with ResponseCode set to "WARNING_StandbyNotAllowed" while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Timeout, if the SECC does not allow a standby period. All mandatory parameters shall be filled in with arbitrary XSD conform values. All values shall be chosen in a way that results in a minimal size of the response message.

NOTE After declining a standby request from the EVCC, the SECC expects the EVCC to proceed according to [V2G20-1396].

8.5.6.3 AC specific requirements

The following requirements apply for the EVCC.

[V2G20-930] The EVCC shall measure a PWM of 5 % duty cycle before sending the message ChargeParameterDiscoveryReq.

NOTE 1 In the case of AC energy transfer, the HLC can be started with using a 5 % PWM or a 100 % PWM (static current).

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1617] The EVCC shall signal CP State B before sending the first PowerDeliveryReq with ChargeProgress equals "Start" within V2G communication session.

[V2G20-847] The EVCC shall signal CP State C or D no later than 250 ms after sending the first PowerDeliveryReq with ChargeProgress equals "Start" within V2G communication session.

[V2G20-848] The EVCC shall signal CP State B no later than 250 ms after sending PowerDeliveryReq with ChargeProgress equals "Stop".

[V2G20-849] If [V2G20-847] applies and no error has been identified, the EVCC shall not change the CP State until [V2G20-848] applies.

NOTE 2 In case of schedule renegotiation, the contactor stays closed to allow energy transfer based on the existing energy transfer limits during schedule renegotiation.

The following applies for the EVCC during a standby period.

[V2G20-2120] After receiving a PowerDeliveryRes with ResponseCode equal to "OK" as a response to the previous PowerDeliveryReq message with ChargeProgress equal to "Standby", and if EVCC selected the service parameter MobilityNeedsMode set to 2, the EVCC shall process the elements TargetSOC, MinimumSOC, DepartureTime and AckMaxDelay in the AC_ChargeLoopRes messages.

The following requirements apply for the SECC supply equipment. The SECC contactor is closed before sending the PowerDeliverRes message.

[V2G20-858] After receiving a PowerDeliveryReq with parameter ChargeProgress equal to "Start" the SECC shall monitor the Contactor status and start the V2G_SECC_Msg_Performance_Timer.

[V2G20-1317] In case of High-level communication based energy transfer, the SECC shall not close the Contactor before receiving PowerDeliveryReq(ChargeProgress = Start).

[V2G20-860] If no error is detected, the SECC shall close the Contactor no later than 3s after measuring CP State C or D.

[V2G20-861] The SECC shall respond with PowerDeliveryRes containing "ResponseCode = OK" within V2G_SECC_Msg_Performance_Time according to Table 215, if the SECC measures a closed Contactor and [V2G20-858] has applied before.

[V2G20-862] The SECC shall respond with PowerDeliveryRes containing "ResponseCode = FAILED_ContactorError" if V2G_SECC_Msg_Timer is equal or larger than V2G_SECC_Msg_Performance of "PowerDelivery" according to Table 215 and SECC measures opened Contactor.

[V2G20-863] After receiving a PowerDeliveryReq with parameter ChargeProgress equal to "Stop", the SECC shall monitor the Contactor status and start the V2G_SECC_Msg_Performance_Timer.

[V2G20-864] The SECC shall respond with PowerDeliveryRes containing "ResponseCode = OK" within V2G_SECC_Msg_Performance_Time according to Table 215, if the SECC measures an open Contactor and [V2G20-863] has applied before.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 3 The ISO 15118 series does not require a specific implementation for controlling the contactor in an EVSE. Control of the power contactor depends on the EVSE architecture.

8.5.6.4 DC specific requirements

The following requirements apply for the EVCC.

[V2G20-912] After receiving a ScheduleExchangeRes with EVSEProcessing set to "Finished" and before sending a DC_CableCheckReq message, the EVCC shall change to CP State C or D as defined in IEC 61851-1.

[V2G20-913] After sending a PowerDeliveryReq message with ChargeProgress equal to "Stop" and receiving the corresponding PowerDeliveryRes message, the EVCC shall change to CP State B as defined in IEC 61851-1 before sending the next request message.

[V2G20-914] If [V2G20-912] applies and no error has been identified, the EVCC shall not change the CP State until [V2G20-913] applies.

The following applies for the EVCC during a standby period.

[V2G20-1380] When the EVCC wants to enter a standby period, after having received DC_PreChargeRes with ResponseCode equal to "OK" and if the EVCC determines that the EVSE output voltage, as measured inside the EV, has sufficiently been adjusted to the EV RESS voltage, the EVCC shall send a PowerDeliveryReq with ChargeProgress equal to "Standby, while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time.

[V2G20-2119] After receiving a PowerDeliveryRes with ResponseCode equal to "OK" as a response to the previous PowerDeliveryReq message with ChargeProgress equal to "Standby", and if EVCC selected the service parameter MobilityNeedsMode set to 2, the EVCC shall process the elements TargetSOC, MinimumSOC, DepartureTime and AckMaxDelay in the DC_ChargeLoopRes messages.

[V2G20-1381] When the EVCC wants to enter a standby period, after having received DC_ChargeLoopRes, the EVCC shall send a PowerDeliveryReq with parameter ChargeProgress equal to "Standby", while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time.

[V2G20-1383] When the EVCC wants to exit a standby period, after having received DC_ChargeLoopRes, the EVCC shall send a PowerDeliveryReq while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time according to Table 215.

NOTE The SECC handles the DC_PreChargeReq as described in [V2G20-858], [V2G20-861], [V2G20-862].

The following requirements apply for the SECC.

[V2G20-1408] The SECC shall apply a CP duty cycle of 5% from start of data link setup until end of V2G communication session.

The SECC waits for positive authorization and availability of energy before entering the charging loop.

[V2G20-916] After receiving a DC_CableCheckReq message, the SECC shall monitor the CP State and start the V2G_SECC_Msg_Performance_Timer.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-917] The SECC shall respond with DC_CableCheckRes containing "ResponseCode = OK" within V2G_SECC_Msg_Performance_Time according to Table 215, if the SECC measures a CP State C or D.

[V2G20-918] The SECC shall respond with DC_CableCheckRes containing "ResponseCode = "FAILED" within V2G_SECC_Msg_Performance_Time according to Table 215, if the SECC measures no CP State C or D.

[V2G20-919] After sending a PowerDeliveryRes message with parameter ResponseCode set to "OK" in response to a PowerDeliveryReq with parameter ChargeProgress set to "Stop", the SECC shall try to measure CP state B.

[V2G20-920] After receiving a DC_WeldingDetectionReq message or a SessionStopReq message, the SECC shall wait for a maximum of V2G_SECC_Msg_Performance_Time to measure CP state B.

[V2G20-921] After receiving a DC_WeldingDetectionReq message or a SessionStopReq message, the SECC shall send the corresponding response message with parameter ResponseCode set to "OK" within V2G_SECC_Msg_Performance_Time according to Table 103, if CP State B was measured.

[V2G20-922] After receiving a DC_WeldingDetectionReq message or a SessionStopReq message, the SECC shall send the corresponding response message with parameter ResponseCode set to "FAILED" within V2G_SECC_Msg_Performance_Time according to Table 103, if CP State B was not measured.

8.5.6.5 AC and DC reverse power transfer specific requirements

8.5.6.5.1 General

In the discharging services, EVCC and SECC shall align to IEC 61851-1 signalling in the same way as in the charging services. Until the discharging service is added in IEC 61851-1, it is defined as an extension within this document. Basic status definitions between charging and discharging are similar, but trigger conditions for charging and discharging loops are defined for reverse power transfer system. It shall be given by HLC control under the condition of IEC 61851-1 signalling agreement.

8.5.6.5.2 Common BPT specific requirements for AC and DC

Most of common requirements defined in 8.5.6.2 shall be applied with following exceptions.

[V2G20-1138] ISO 15118 enabled EVCC shall confirm to IEC 61851-1 in case of charging. Also ISO 15118 enabled EVCC shall similarly work as defined in IEC 61851-1 in case of discharging.

[V2G20-1409] ISO 15118 enabled SECC shall confirm to IEC 61851-1 in case of charging. Also ISO 15118 enabled SECC shall similarly work as the EVSE defined in IEC 61851-1 in case of discharging.

8.5.6.6 ACDP specific requirements

The following requirements apply for the EVCC.

[V2G20-4022] After receiving a ACDP_ConnectRes message with "ResponseCode = OK" and before sending a DC_CableCheckReq message, the EVCC shall change to CP State C or State D as defined in IEC 61851-1.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-4023] If [V2G20-4022] applies and no error has been identified, the EV shall not change the CP State until [V2G20-913] applies.

The following requirements apply for the SECC.

[V2G20-4024] The EVSE shall apply a CP duty cycle of 100 % from start of Data Link Setup until end of V2G communication session as defined in IEC 61851-23-1.

NOTE 1 For ACDP noise robustness CP line uses only a DC signal. PWM is not allowed.

NOTE 2 The following DC specific requirements apply: [V2G20-917].

8.5.7 V2G message synchronization with IEC 61980-2 signalling for WPT

8.5.7.1 Overview

In general, the ISO 15118 series is based on the requirements as defined in IEC 61851-1.

[V2G20-5071] An ISO 15118-enabled EV shall conform to IEC 61980-2 and ISO 19363:2020.

[V2G20-5072] During HLC-C, the EV shall apply all energy transfer limits as negotiated by the ISO 15118 series in addition to the limits defined by IEC 61980-2.

[V2G20-5073] ISO 15118-enabled EVSE shall conform to IEC 61980-2.

8.6 Message sequencing and error handling

8.6.1 Overview

In a V2G communication session the EVCC and the SECC exchange request-response message pairs based on a predefined sequence. In this document this is referenced as request-response message sequence. These request-response message sequences allow both sides to synchronize the process in any situation and to control the communication between two V2G entities.

The basic error handling concept is based on application level timers for request-response message sequences. This enables a V2G entity to manage any processing error and communication error on application level after waiting for the expected behavior until a specified timeout. Therefore, a V2G entity can decide on a successful processing after waiting for the positive result until a timeout. In case there is no error in the communication layers below the application layer, the application has the option to terminate the TCP communication in case of application error. A terminated TCP connection before a SessionStopRes is always interpreted as an error by the EVCC or the SECC.

Besides the timeout concept defined in this document, it does not limit additional error detection mechanisms as long as such mechanisms do not lead to incompatibility.

Within a charging session, an EVCC can establish a new V2G communication session after an error by applying the V2G communication state processing as described in 7.4. In this case, the EVCC and the SECC start the communication in the same way as for the first V2G session setup.

In general, the processing time of a request message in an SECC is limited by the performance requirements defined in 8.5.4. If an SECC requires more processing time it may apply the parameter EVSEProcessing (set to Ongoing) to avoid a timeout at the EVCC by explicitly indicating that the processing is not finished yet and the EVCC waits for finishing the processing before proceeding with the message sequence. The EVCC will then repeat the request message periodically until the EVSE signals the finishing of the processing by the parameter EVSEProcessing (set to finished).

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

8.6.2 Basic definitions for error handling

The basic error handling for a request-response-message pair and a request-response message sequence is based on the ResponseCode included in the response message of the SECC. Depending on the value in the ResponseCode the EVCC decides if it can proceed with the standard request-response message sequence or if it handles an error.

In this document, the ResponseCode as defined in Annex A is interpreted by the EVCC as follows.

- OK:

  Any value starting with "OK" or "OK_" indicates a positive response. Detailed information may be provided by OK_<additional info>. This information may be used to differentiate the reaction on the positive response.

- FAILED:

  Any value starting with "FAILED" or "FAILED_" indicates a negative response. Detailed information may be provided by FAILED_<additional info>. This information may be used to differentiate the reaction on the negative response. This response is considered a fatal error. The SECC and EVCC will terminate the communication session after sending/receiving this response code.

- WARNING:

  Any value starting with "WARNING_" indicates a response that requires an adjustment or reaction by the EVCC, otherwise a subsequent negative response is to be expected in the next message pair. Detailed information is to be provided by WARNING_<additional info>. This information is to be used to differentiate the reaction on the response. This response is not considered a fatal error. The SECC and EVCC will not terminate the communication session after sending/receiving this response. They can continue the communication if proper remedial actions (as defined for that particular response) are taken by the EVCC.

The processing of the remaining parameters in a response message in the EVCC depends on the parameter ResponseCode. If the ResponseCode contains a value starting with OK indicating that no error was detected, the EVCC can process other parameters of the response message mandatorily or optionally as defined in 8.3.5.7.1. If the ResponseCode contains a value starting with FAILED indicating that an error was detected, the EVCC is expected to ignore other parameters of the response message. If the ResponseCode contains a value starting with WARNING indicating that something is not as expected, the EVCC may either process the parameters or ignore them depending on the specifications defined for that particular message.

As long as the message content of the received request message is valid and the request message is accepted in the current SECC state (sequencing), the ResponseCode is set to OK. This is also true for response messages with EVSEProcessing set to Ongoing. With the ResponseCode set to OK the SECC indicates that the request message is accepted and valid, but cannot be finally answered at this moment and more time is needed to send the valid values in the response message. When the valid values are sent in the response message, the SECC indicates this with the parameter EVSEProcessing (set to Finished) and the EVCC can proceed with the sequence as expected for the first request message before receiving the parameter EVSEProcessing (set to Ongoing). If the SECC sets the ResponseCode to FAILED it identified an error in processing or an invalid message and the standard error handling applies.

8.6.3 ResponseCode handling

8.6.3.1 Common requirements

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Besides the requirements for request-response message pairs and request-response message sequences as defined in 8.6.4 the EVCC and the SECC shall conform to the following requirements.

[V2G20-734] If the ResponseCode contains a value starting with OK, the EVCC shall process the other parameters of the response message as defined in 8.6.

[V2G20-735] If the ResponseCode contains a value starting with FAILED, the EVCC shall ignore the other parameters of the response message.

[V2G20-736] If the SECC sends a ResponseCode containing a value starting with FAILED all mandatory parameters shall be filled in with arbitrary XSD conform values. Additionally, all values shall be chosen in a way that results in a minimal size of the response message.

[V2G20-2201] If the ResponseCode contains a value starting with WARNING, the EVCC shall take appropriate actions as defined for that particular WARNING response for that particular message.

NOTE 1 Each WARNING ResponseCode can have different reaction requirements for the EVCC. In some cases the EVCC can be required to ignore the other parameters of the response message and take a pre-defined action while in other cases the EVCC can be required to take an action based on the parameters received in the message but act in a different way than when it receives OK ResponseCode for the same message.

[V2G20-2202] If the SECC sends a ResponseCode containing a value starting with WARNING all mandatory parameters shall be filled as defined for that particular WARNING response for that particular message.

NOTE 2 Each WARNING ResponseCode can have a different requirements for the parameters. In some cases the SECC can be required to send default/arbitrary XSD conform values while in others the SECC can be required to send some specific values so that the EVCC can take an action based on the parameters received in the message.

In general each response message can contain two types of ResponseCode values "OK" or "FAILED". In addition some response messages can further contain the ResponseCode value "WARNING_" (see Table 224).

[V2G20-457] A response message shall contain the ResponseCode "OK" in the "ResponseCode" attribute if the processing of the request message was successful. If later on a specific positive "ResponseCode" is defined for a dedicated situation, this ResponseCode shall be used.

[V2G20-458] A response message shall contain the ResponseCode "FAILED" in the "ResponseCode" attribute if the processing of the request message was not successful and no specific "ResponseCodeType" is defined for the concrete error case.

[V2G20-459] The response message shall contain the ResponseCode "FAILED_SequenceError" if the SECC has received an unexpected request message.

[V2G20-460] The response message shall contain the ResponseCode "FAILED_UnknownSession" if the SessionID in any request message except SessionSetupReq is not equal to the SessionID value stored for the currently active V2G communication session.

[V2G20-461] The response message shall contain the ResponseCode "FAILED_SignatureError" if the validation of the Security element in the message header failed.

[V2G20-462] The message "SessionSetupRes" shall contain the specific ResponseCode "OK_NewSessionEstablished" if processing of the SessionSetupReq message was

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

successful and a different SessionID is contained in the response message than the SessionID in the request message.

[V2G20-463] The message "SessionSetupRes" shall contain the specific ResponseCode "OK_OldSessionJoined" if processing of the SessionSetupReq message was successful and the same SessionID as used in the request message is contained in the response message.

[V2G20-464] The message "ServiceDetailRes" shall contain the ResponseCode "FAILED_ServiceIDInvalid" if the ServiceID contained in the ServiceDetailReq message was not part of the offered EnergyTransferServiceList or VASList during ServiceDiscovery.

[V2G20-467] The message "ServiceSelectionRes" shall contain the ResponseCode "FAILED_ServiceSelectionInvalid" if the SelectedServiceList contained in the ServiceSelectionReq message contains a ServiceID which was not contained in the offered EnergyTransferServiceList or VASList of ServiceDiscoveryRes.

[V2G20-1618] The message "ServiceSelectionRes" shall contain the ResponseCode "FAILED_NoEnergyTransferServiceSelected" if the SelectedServiceList contained in the ServiceSelectionReq message does not contain a ServiceID value equal to one which was offered by the SECC with the parameter ChargeService or BPT service in the ServiceDiscoveryRes.

[V2G20-2203] The message "CertificateInstallationRes" shall contain the ResponseCode "WARNING_CertificateExpired" if the SECC (or SA) deduces that one (or more) of the certificates in the OEMProvisioningCertificate chain it received in the CertificateInstallationReq message has expired. This includes any cross certificates (if applicable).

[V2G20-2204] The message CertificateInstallationRes shall contain the ResponseCode "WARNING_CertificateNotYetValid" if the SECC (or SA) deduces that one (or more) of the certificates in the OEMProvisioningCertificate chain it received in the CertificateInstallationReq message is not yet valid. This includes any cross certificates (if applicable).

[V2G20-1412] The message "CertificateInstallationRes" shall contain the ResponseCode "WARNING_CertificateRevoked" if the SECC (or SA) deduces (using OCSP responses or CRL) that one (or more) of the certificates in the OEMProvisioningCertificate chain it received in CertificateInstallationReq message is revoked. This includes any cross certificates (if applicable).

[V2G20-2205] The message "CertificateInstallationRes" shall contain the ResponseCode "WARNING_CertificateValidationError" if certificate validation of one (or more) of the certificates in the OEMProvisioningCertificate chain it received in the CertificateInstallationReq message fails due to any issue other than those identified by [V2G20-2203], [V2G20-1412] and [V2G20-2204]. This includes any cross certificates (if applicable).

NOTE 3 ResponseCode "WARNING_CertificateValidationError" for message "CertificateInstallationRes" is a catch-all response code for cases that are not covered by the specific certificate validation error response codes defined in other requirements for "CertificateInstallationRes" message. This includes cases where certificate validation fails due to a mismatch in the curves in the OEM provisioning certificate received in "CertificateInstallationReq" message and the curves the SECC/SA is allowed to process per the configuration parameter as defined by [V2G20-2320]. For example, in case the SECC/SA is unable to validate the OEM provisioning

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

certificate because the SECC/SA cannot process the curves in the OEM provisioning certificate (due to changes to configuration parameter as defined by [V2G20-2320]), the SECC will send the ResponseCode "WARNING_CertificateValidationError".

[V2G20-2206] The message "CertificateInstallationRes" shall contain the ResponseCode "WARNING_NoContractMatchingPCIDFound" if the SA(s) indicate to the SECC that after a complete search, no contract could be found for the PCID contained in the OEM provisioning certificate received in the OEMProvisioningCertificate chain contained in the CertificateInstallationReq message.

[V2G20-2207] The message "CertificateInstallationRes" shall contain the ResponseCode "WARNING_NoCertificateAvailable" if a new contract certificate cannot be retrieved from secondary actor within V2G_SECC_Msg_Performance_Time according to Table 215.

NOTE 4 This response code indicates a timeout. The timeout could be due to many reasons including communication errors, taking longer than the timeout allows to retrieve the contract certificate from the secondary actor, etc.

[V2G20-2208] The message CertificateInstallationRes shall contain the ResponseCode "WARNING_eMSPUnknown" if the SECC does not recognize any one (or more) of the eMSPs indicated by the EMAID included in the PrioritizedEMAIDs list it received in CertificateInstallationReq message.

[V2G20-2209] The message "AuthorizationRes" shall contain the ResponseCode "WARNING_AuthorizationSelectionInvalid" if the SelectedAuthorizationService contained in the AuthorizationReq message was not part of the offered AuthoritzationServices of AuthorizationSetupRes message.

[V2G20-2210] The message AuthorizationRes shall contain the ResponseCode "WARNING_ContractCancelled" if the SECC received the information (potentially from SA; it is not in the scope of this document to define how the SECC received this information) that the contract associated with the ContractCertificate it received in AuthorizationReq message, in attribute ContractSignatureCertChain, has been cancelled.

NOTE 5 This response code is related to the actual customer contract between the SA and the customer. It is not related to the contract certificate itself. For example, the contract certificate can still be valid while the customer possibly cancelled the actual contract with the eMSP. In that case, at the SA's discretion, this response code is expected to be utilized.

[V2G20-2211] The message AuthorizationRes shall contain the ResponseCode "WARNING_eMSPUnknown" if the SECC does not recognize the eMSP indicated by the EMAID included in the ContractCertificate it received in AuthorizationReq message, in attribute ContractSignatureCertChain.

[V2G20-2212] The message "AuthorizationRes" shall contain the ResponseCode "WARNING_CertificateExpired" if the SECC (or SA) deduces that one (or more) of the certificates in the ContractCertificate chain it received in the AuthorizationReq message, in attribute ContractSignatureCertChain, is expired. This includes any cross certificates (if applicable).

[V2G20-2213] The message "AuthorizationRes" shall contain the ResponseCode "WARNING_CertificateNotYetValid" if the SECC (or SA) deduces that one (or more) of the certificates in the ContractCertificate chain it received in the AuthorizationReq

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

message, in attribute ContractSignatureCertChain, is not yet valid. This includes any cross certificates (if applicable).

[V2G20-2214] The message "AuthorizationRes" shall contain the ResponseCode "WARNING_CertificateRevoked" if the SECC (or SA) deduces (using OCSP responses or CRL) that one (or more) of the certificates in the ContractCertificate chain it received in AuthorizationReq message, in attribute ContractSignatureCertChain, is revoked. This includes any cross certificates (if applicable).

[V2G20-2215] The message "AuthorizationRes" shall contain the ResponseCode "WARNING_CertificateValidationError" if certificate validation of one (or more) of the certificates in the ContractCertificate chain it received in AuthorizationReq message, in attribute ContractSignatureCertChain, fails due to any issue other than those identified by [V2G20-2212], [V2G20-2213] and [V2G20-2214]. This includes any cross certificates (if applicable).

NOTE 6 ResponseCode "WARNING_CertificateValidationError" for message "AuthorizationRes" is a catch-all response code for cases that are not covered by the specific certificate validation error response codes defined in other requirements for "AuthorizationRes" message. This includes cases where certificate validation fails due to a mismatch in the curves in the contract certificate received in "AuthorizationReq" message and the curves the SECC/SA is allowed to process per the configuration parameter as defined by [V2G20-2320]. For example, in case the SECC/SA is unable to validate the contract certificate because the SECC/SA cannot process the curves in the contract certificate (due to changes to configuration parameter as defined by [V2G20-2320]), the SECC will send the ResponseCode "WARNING_CertificateValidationError".

[V2G20-2216] The message "AuthorizationRes" shall contain the ResponseCode "WARNING_ChallengeInvalid" if the challenge response contained in the AuthorizationReq message, in attribute GenChallenge, is not valid versus the GenChallenge provided in AuthorizationSetupRes.

[V2G20-2217] The message AuthorizationRes shall contain the ResponseCode "WARNING_GeneralPnCAuthorizationError" when the SECC received the information (potentially from SA; t is not in the scope of this document to define how the SECC received this information) that there is an issue either with the contract associated with the ContractCertificate message or with the ContractCertificate it received in AuthorizationReq message and conditions are not met to apply any of the response codes as defined by [V2G20-2209], [V2G20-2210], [V2G20-2211], [V2G20-2212], [V2G20-2213], [V2G20-2214], [V2G20-2215] and [V2G20-2216].

NOTE 7 This response code could indicate an intermittent or temporary issue at the SA. It can also indicate an unknown issue with the customer contract. It can additionally be used in cases where the SA does not wish to provide detailed error information.

[V2G20-2218] If the SECC (either on its own or via SA) is capable of comparing the validity of a ContractCertificate with the current time, the SECC shall set the ResponseCode for the AuthorizationRes to "OK_CertificateExpiresSoon" if the received contract certificate will expire in 14 days or fewer and conditions are not met to apply [V2G20-2212].

[V2G20-2219] The message "AuthorizationRes" shall contain the ResponseCode "WARNING_EIMAuthorizationFailure" if EIM Authorization fails due to any reason. This includes customer cancelling EIM Authorization or any other errors with EIM Authorization.

[V2G20-478] The message "PowerDeliveryRes" shall contain the ResponseCode "FAILED_EVPowerProfileInvalid" if the content of attribute "EVPowerProfile" in the

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

PowerDeliveryReq message violates a power limitation provided in ScheduleExchangeRes.

[V2G20-479] The message "PowerDeliveryRes" shall contain the ResponseCode "FAILED_TariffSelectionInvalid" if the content of element "EVPowerProfile" in the PowerDeliveryReq message contains a SelectedScheduleTupleID which was not contained in the "ScheduleList" element provided in ScheduleExchangeRes.

[V2G20-1411] The message "PowerDeliveryRes" shall contain the ResponseCode "FAILED_PowerDeliveryNotApplied" if the EVSE is not able to deliver energy.

[V2G20-1944] The message PowerDeliveryRes shall contain the ResponseCode "OK_PowerToleranceConfirmed" if the EVCC has sent a PowerDeliveryReq containing the parameter PowerToleranceAcceptance with the value set to "PowerToleranceConfirmed".

[V2G20-1945] The message PowerDeliveryRes shall contain the ResponseCode "FAILED_PowerToleranceNotConfirmed" if the EVCC has sent a PowerDeliveryReq containing the parameter PowerToleranceAcceptance with the value set to "PowerToleranceNotConfirmed" and based on this the SECC intends to stop the V2G communication session, according to [V2G20-1402].

[V2G20-1946] The message PowerDeliveryRes shall contain the ResponseCode "WARNING_PowerToleranceNotConfirmed" if the EVCC has sent a PowerDeliveryReq containing the parameter PowerToleranceAcceptance with the value set to "PowerToleranceNotConfirmed" and based on this the SECC intends to initiate a schedule renegotiation according to [V2G20-1601].

[V2G20-1953] The EVCC shall interpret the response code "WARNING_EVPowerProfileViolation" as Information that the EVSE has detected an immediate unacceptable deviation from the EVPowerProfile. The EV is expected to correct the power transfer within the timing limitations according to [V2G20-1865] or the V2G communication session will be terminated accordingly.

NOTE 8 The response code "WARNING_EVPowerProfileViolation" is sent continuously by the SECC as long as an immediate unacceptable deviation from the EVPowerProfile is detected. However, the timing requirements as specified in [V2G20-1865] are always considered based on the first SECC sent "WARNING_EVPowerProfileViolation" response code in a sequence.

[V2G20-1954] If the response code "WARNING_PowerToleranceNotConfirmed" has been sent, and EVSENotification in EVSEStatus has been set to "ScheduleRenegotiation" in the latest PowerDeliveryRes message the EVCC shall initiate a schedule renegotiation.

[V2G20-1955] The message "SessionStopRes" shall contain the ResponseCode "FAILED_NoServiceRenegotiationSupported" if a SessionStopReq with ChargingSession set to "ServiceRenegotiation" is received, and the first ServiceDiscoveryRes message of the service session had the ServiceRenegotiationSupported set to "False".

[V2G20-1956] The message "ServiceSelectionRes" shall contain the ResponseCode "FAILED_NoServiceRenegotiationSupported" if the first ServiceDiscoveryRes message of the service session had the ServiceRenegotiationSupported set to "False" and the EVCC, after waking up from a Pause, is selecting a different set of ServiceIDs or ParameterSetIDs from the first ServiceSelectionReq of the service session.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1195] The message "SessionStopRes" shall contain the ResponseCode "FAILED_PauseNotAllowed" if the EVCC requests a pause in dynamic control mode, which has not been initiated by the SECC according to [V2G20-1850].

[V2G20-1196] The message "SessionStopRes" shall contain the ResponseCode "FAILED_PauseNotAllowed" if the EVCC requests a pause in scheduled control mode that is not indicated by a 0kW period in the currently applied EVPowerProfileEntry.

Details of "WARNING_StandbyNotAllowed" are provided in 8.5.6.2.

Table 224 shows an overview of the common ResponseCode values and the messages as defined above.

Table 224 — Overview on application of common ResponseCodes

ResponseCode (Enumeration)	V2G application layer protocol handshake messages			V2G application layer messages							
	SessionSetupRes	ServiceDiscoveryRes	ServiceDetailRes	ServiceSelectionRes	AuthorizationSetupRes	AuthorizationRes	ScheduleExchangeRes	PowerDeliveryRes	MeteringConfirmationRes	CertificateInstallationRes	SessionStopRes
OK	x	x	x	x	x	x	x	x	x	x	x
OK_NewSessionEstablished	x										
OK_OldSessionJoined	x										
OK_CertificateExpiresSoon						x					
OK_PowerToleranceConfirmed								x			
WARNING_CertificateExpired						x				x	
WARNING_CertificateNotYetValid						x				x	
WARNING_CertificateRevoked						x				x	
WARNING_CertificateValidationError						x				x	
WARNING_eMSPUnknown						x				x	
WARNING_GeneralPnCAuthorizationError						x					
WARNING_ChallengeInvalid						x					
WARNING_AuthorizationSelectionInvalid						x					
WARNING_EIMAuthorizationFailure						x					
WARNING_PowerToleranceNotConfirmed								x			
WARNING_StandbyNotAllowed								x			
WARNING_NoCertificateAvailable										x	
WARNING_NoContractMatchingPCIDFound										x	
FAILED	x	x	x	x	x	x	x	x	x	x	x
FAILED_SequenceError	x	x	x	x	x	x	x	x	x	x	x
FAILED_UnknownSession		x	x	x	x	x	x	x	x	x	x

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

ResponseCode (Enumeration)	V2G application layer protocol handshake messages			V2G application layer messages							
	SessionSetupRes	ServiceDiscoveryRes	ServiceDetailRes	ServiceSelectionRes	AuthorizationSetupRes	AuthorizationRes	ScheduleExchangeRes	PowerDeliveryRes	MeteringConfirmationRes	CertificateInstallationRes	SessionStopRes
FAILED_ServiceIDInvalid			x								
FAILED_ServiceSelectionInvalid				x							
FAILED_NoEnergyTransferServiceSelected				x							
FAILED_NoServiceRenegotiationSupported				x							x
FAILED_SignatureError						x			x	x	
FAILED_ContactorError								x			
FAILED_EVPowerProfileInvalid								x			
FAILED_ScheduleSelectionInvalid								x			
FAILED_PowerDeliveryNotApplied								x			
FAILED_PowerToleranceNotConfirmed								x			
FAILED_MeteringSignatureNotValid									x		
FAILED_PauseNotAllowed											x

8.6.3.2 AC requirements

[V2G20-1619] The message "AC_ChargeParameterDiscoveryRes" shall contain the ResponseCode "FAILED_WrongChargeParameter" if the content of attribute "EV_EnergyTransferParameter" in the AC_ChargeParameterDiscoveryReq message is not valid, for example, wrong parameter set is provided, one or multiple parameters cannot be interpreted.

[V2G20-1948] The message AC_ChargeLoopRes shall contain the ResponseCode "WARNING_EVPowerProfileViolation" if a violation of the PowerTolerance band was detected according to the conditions defined in [V2G20-1864].

[V2G20-1951] The message AC_ChargeLoopRes shall contain the ResponseCode "FAILED_EVPowerProfileViolation" if a violation of the PowerTolerance band was detected according to the conditions defined in [V2G20-1865].

[V2G20-1990] The message "MeteringConfirmationRes" shall contain the ResponseCode "FAILED_MeteringSignatureNotValid" if the SECC is not able to validate the signature, or the contained meter reading does not fit to the provided meter reading during "AC_ChargeLoopRes" and the SECC requires that the signature is valid.

Table 225 shows an overview of the AC ResponseCode values and the messages as defined above.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Table 225 — Overview on application of AC ResponseCodes

ResponseCode (Enumeration)	V2G application layer messages	
	AC_ChargeParameterDiscvoeryRes	AC_ChargeLoopRes
OK	x	x
WARNING_EVPowerProfileViola		x
WARNING_ScheduleRenegotiati		x
FAILED	x	x
FAILED_SequenceError	x	x
FAILED_UnknownSession	x	x
FAILED_WrongChargeParameter	x	
FAILED_EVPowerProfileViolatio		x
FAILED_ScheduleRenegotiation		x

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

8.6.3.3 DC requirements

[V2G20-2272] The message "DC_ChargeParameterDiscoveryRes" shall contain the ResponseCode "FAILED_WrongChargeParameter" if the content of attribute "EV_EnergyTransferParameter" in the DC_ChargeParameterDiscoveryReq message is not valid, for example, wrong parameter set is provided, one or multiple parameters cannot be interpreted.

[V2G20-1947] The message DC_ChargeLoopRes shall contain the ResponseCode "WARNING_EVPowerProfileViolation" if a violation of the PowerTolerance band was detected according to the conditions defined in [V2G20-1864].

[V2G20-1950] The message DC_ChargeLoopRes shall contain the ResponseCode "FAILED_EVPowerProfileViolation" if a violation of the PowerTolerance band was detected according to the conditions defined in [V2G20-1865].

Table 226 shows an overview of the DC ResponseCode values and the messages as defined above.

© ISO 2022 – All rights reserved

Table 226 — Overview on application of DC ResponseCodes

ResponseCode (Enumeration)	V2G application layer messages				
	DC_ChargeParameterDiscvoeryRes	DC_CableCheckRes	DC_PreChargeRes	DC_ChargeLoopRes	DC_WeldingDetectionRes
OK	x	x	x	x	x
WARNING_EVPowerProfileViolation				x	
WARNING_ScheduleRenegotiationFailed				x	
FAILED	x			x	x
FAILED_SequenceError	x	x	x	x	x
FAILED_UnknownSession	x	x	x	x	x
FAILED_WrongChargeParameter	x				
FAILED_EVPowerProfileViolation				x	
FAILED_ScheduleRenegotiation				x	
FAILED_AssociationError (ACDP only)				x	

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

8.6.3.4 WPT requirements

[V2G20-5122] The message "WPT_ChargeParameterDiscoveryRes" shall contain the ResponseCode "FAILED_WrongChargeParameter" if the content of attribute "EV_EnergyTransferParameter" in the WPT_ChargeParameterDiscoveryReq message is not valid, for example, wrong parameter set is provided, one or multiple parameters cannot be interpreted.

[V2G20-5074] The message "PowerDeliveryRes" shall contain the ResponseCode "WARNING_WPT" after the supply device has detected an alignment error or other anomaly.

[V2G20-5075] The message "WPT_ChargeLoopRes" shall contain the ResponseCode "WARNING_WPT" after the supply device has detected an alignment error or other anomaly.

[V2G20-5076] The message "WPT_ChargeLoopRes" shall contain the ResponseCode "FAILED" after the supply device has detected an unrecoverable error or exception.

[V2G20-5077] The message "WPT_AlignmentCheckRes" shall contain the ResponseCode "WARNING_WPT" after the supply device has detected an alignment error.

[V2G20-5056] If the SECC has received the WPT_FinePositioningReq message with the parameter EVResultCode set to a "EVResultFailed" it shall respond with a WPT_FinePositioningRes message with the parameter ResponseCode equal to FAILED or WARNING_WPT.

© ISO 2022 – All rights reserved

NOTE It is up to the implementation whether to give a response code FAILED or WARNING_WPT: In case of FAILED, the communication will be terminated. In case of WARNING_WPT, the system allows to repeat the positioning procedure.

[V2G20-5078] The message WPT_ChargeLoopRes shall contain the ResponseCode "WARNING_EVPowerProfileViolation" if a violation of the PowerTolerance band was detected according to the conditions defined in [V2G20-1864].

[V2G20-5079] The message WPT_ChargeLoopRes shall contain the ResponseCode "FAILED_EVPowerProfileViolation" if a violation of the PowerTolerance band was detected according to the conditions defined in [V2G20-1865].

Table 227 shows an overview of the WPT ResponseCode values and the messages as defined above.

Table 227 — Overview on application of WPT ResponseCodes

ResponseCode (Enumeration)	V2G application layer messages					
	WPT_FinePositioningSetupRes	WPT_FinePositioningRes	WPT_PairingRes	WPT_AlignmentCheckRes	WPT_ChargeParameterDiscoveryRes	WPT_ChargeLoopRes
OK	x	x	x	x	x	x
WARNING_WPT	x	x	x	x	x	x
WARNING_EVPowerProfileViola						x
WARNING_ScheduleRenegotiati						x
FAILED	x	x	x	x	x	x
FAILED_SequenceError	x	x	x	x	x	x
FAILED_UnknownSession	x	x	x	x	x	x
FAILED_WrongChargeParameter					x	
FAILED_EVPowerProfileViolatio						x
FAILED_ScheduleRenegotiation						x

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

8.6.3.5ACDP requirements

Table 228 shows an overview of the ACDP ResponseCode values and the messages as defined above.

Table 228 — Overview on application of ACDP ResponseCodes

ResponseCode (Enumeration)	V2G application layer messages			
	ACDP_VehiclePositioningRes	ACDP_ConnectRes	ACDP_DisconnectRes	ACDP_SystemStatusRes
OK	x	x	x	
FAILED	x	x	x	
FAILED_SequenceError	x	x	x	
FAILED_UnknownSession	x	x	x	
FAILED_AssociationError	x			

8.6.4 Request-response message sequence requirements

NOTE In this document the sequence of the requirements is output driven.

8.6.4.1 General requirements

The EVCC behavior defining all valid request-response message sequences for WLAN and PLC based communication is shown in 8.6.6. The messages shown in the diagram do not contain the multiplexed messages. If message names are used, they always reference the payload type Part20MainstreamPayloadID, unless noted otherwise.

[V2G20-1413] If the EVCC sends a valid parameter EVPowerProfile (as defined in [V2G20-1070]) in the message PowerDeliveryReq the SECC shall ensure that the power envelope defined by the PowerSchedule in the ChargingSchedule as well as, if present, the DischargingSchedule, can be utilized for the entire time span which they cover.

[V2G20-1009] As soon as the SECC becomes aware of the fact that [V2G20-1413] can no longer be satisfied it shall trigger a proper schedule renegotiation procedure.

[V2G20-1402] When the SECC wants to trigger a termination of the session, it shall set the parameter EVSENotification to "Terminate" and send the parameter until the awaited action has been processed by the EV.

[V2G20-1414] If the EVCC sends PowerDeliveryReq with ChargeProgress=Renegotiate it shall not send an EVPowerProfile.

NOTE 1 [V2G20-1414] is only relevant after leaving the standby phase.

[V2G20-1416] If the parameter EVSENotification in EVSEStatus is equal to Terminate, the EVCC shall stop charging within the number of seconds provided in NotificationMaxDelay.

NOTE 2 After indication of a terminate the SECC can stop the charging from EVSE side, e.g. by turning-off the pilot signal or opening the main contactors after the duration of NotificationMaxDelay.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1621] If the parameter EVSENotification in EVSEStatus is equal to MeteringConfirmation the EVCC shall send a MeteringConfirmationReq using the multiplexed communication within the number of seconds provided in NotificationMaxDelay.

[V2G20-1622] The parameter EVSENotification in EVSEStatus shall only use MeteringConfirmation after the exchange of the first ChargeLoop Messages.

[V2G20-1850] In the case the SECC wants to initiate a pause, it shall trigger the EVCC via EVSEStatus Parameter EVSENotification set to "Pause" and NotificationMaxDelay set to 60s. The EVCC shall then either initiate a pause period according to [V2G20-1540] or enter a standby period according to [V2G20-1380], [V2G20-1381], and [V2G20-1394].

[V2G20-1854] In the case the SECC wants to exit a standby period, it shall trigger the EVCC via EVSEStatus Parameter EVSENotification set to "ExitStandby". The EVCC shall than exit a standby period according to [V2G20-1393], [V2G20-1383] and [V2G20-1395].

[V2G20-1959] The EVSE shall set EVSENotification to "Terminate" while decreasing the power at the same time, if it wants to stop charging in dynamic control mode.

[V2G20-1698] In case the SECC wants to end the service session, the SECC shall notify the EVCC by setting EVSENotification in EVSEStatus to "Terminate."

[V2G20-1960] If the parameter EVSENotification in EVSEStatus is equal to "Terminate", the EVCC shall initiate a shutdown sequence and finally send a SessionStopReq with ChargingSession set to "Terminate".

[V2G20-2644] If the EVCC wishes to stop the session for a non-critical reason (e.g. user interaction, errors which are not emergency related) after having sent a SessionSetupReq message and before having sent a PowerDeliveryReq message with ChargeProgress = "Start", the EVCC shall send a SessionStopReq message with parameter "ChargingSession" set to "Terminate" and the optional EVTerminationCode within V2G_EVCC_Sequence_Performance_Timeout according to Table 215, if not otherwise specified within this document. It shall then wait for a SessionStopRes message and proceed according to [V2G20-1463], [V2G20-728] and [V2G20-025] afterwards.

[V2G20-2645] In case the SECC receives a SessionStopReq after having sent a SessionSetupRes message and before having received a PowerDeliveryReq message with ChargeProgress = "Start", the SECC shall proceed according to [V2G20-1632] and [V2G20-1633].

8.6.4.2 AC requirements

[V2G20-1961] For AC charging with WiFi communication only WiFi communication will be used even when there is PLC available.

[V2G20-1964] If the first ServiceDiscoveryRes message of the service session had the parameter ServiceRenegotiationSupported set to "True" and if the parameter EVSENotification in EVSEStatus is equal to "ServiceRenegotiation" in AC_ChargeLoopRes, the EVCC shall initiate a ServiceRenegotiation as defined by [V2G20-1969] within the number of seconds provided in NotificationMaxDelay.

[V2G20-1965] If the first ServiceDiscoveryRes message of the service session had the parameter ServiceRenegotiationSupported set to "False" and if the parameter EVSENotification in EVSEStatus is equal to "ServiceRenegotiation" in AC_ChargeLoopRes, the EVCC shall not initiate a ServiceRenegotiation.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

8.6.4.3 DC Requirements

[V2G20-1650] For DC charging with WiFi communication only WiFi communication will be used even when there is PLC available.

[V2G20-1651] If the first ServiceDiscoveryRes message of the service session had the parameter ServiceRenegotiationSupported set to "True" and if the parameter EVSENotification in EVSEStatus is equal to "ServiceRenegotiation" in DC_ChargeLoopRes, the EVCC shall initiate a ServiceRenegotiation as defined by [V2G20-1661] within the number of seconds provided in NotificationMaxDelay.

[V2G20-1652] If the first ServiceDiscoveryRes message of the service session had the parameter ServiceRenegotiationSupported set to "False" and if the parameter EVSENotification in EVSEStatus is equal to "ServiceRenegotiation" in DC_ChargeLoopRes, the EVCC shall not initiate a ServiceRenegotiation.

8.6.4.4 WPT Requirements

[V2G20-5080] If the first ServiceDiscoveryRes message of the service session had the parameter ServiceRenegotiationSupported set to "True" and if the parameter EVSENotification in EVSEStatus is equal to "ServiceRenegotiation" WPT_ChargeLoopRes, the EVCC shall initiate a ServiceRenegotiation as defined by [V2G20-1661] within the number of seconds provided in NotificationMaxDelay.

[V2G20-5081] If the first ServiceDiscoveryRes message of the service session had the parameter ServiceRenegotiationSupported set to "False" and if the parameter EVSENotification in EVSEStatus is equal to "ServiceRenegotiation" in WPT_ChargeLoopRes, the EVCC shall not initiate a ServiceRenegotiation.

8.6.4.5 EVCC

8.6.4.5.1 General

The EVCC behavior defining all valid request-response message sequence.

8.6.4.5.2 Error handling

[V2G20-1966] For all messages, the EVCC shall stop the V2G communication according to 7.4 after V2G_EVCC_Msg_Timeout according to Table 215.

[V2G20-1967] After receiving a response message with "ResponseCode = FAILED", the EVCC shall stop the V2G communication according to requirements defined 7.4.

[V2G20-1968] After receiving any message with "ResponseCode = FAILED_SequenceError", the EVCC shall react according to 7.4.

[V2G20-2220] After the EVCC receives a ResponseCode starting with 'FAILED' or 'FAILED_' it shall terminate the communication by applying [V2G20-728].

8.6.4.5.2.1 ACDP error handling

NOTE 1 ACDP deploys the same basic error handling concept for DC charging with the following exception. In case of an application error when there is no error in the communication layers below the application layer the communication can be continued until the last message pair of the exception handling procedure has been executed.

[V2G20-4025] If EVCC is using ServiceName = DC_ACDP, [V2G20-1967] does not apply.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-4026] In case of any exception handling the EVCC shall continue the communication to the SECC until the last message pair of the exception handling procedure has been executed.

NOTE 2 The EV initiates an emergency shut down by changing the CP state from C/D to B. The EVSE ramps down the charging current rapidly, opens the DC contactors and raises the pantograph. The EVCC issues the ACDP_Disconnect message then in order to determine the status of the pantograph. After the ACDP_Disconnect response indicates the pantograph being in home position the EVCC issues the SessionStop message to end the process. The ACDP_SystemStatus messages meanwhile unveils the EV causing the emergency shut down, as described in IEC 61851-23.

[V2G20-4027] When EVCC experiences an emergency situation, and EVCC is using ServiceName = DC_ACDP as defined in Table 204 the EVCC shall set CP state to B and start sending ACDP_DisconnectReq.

If the EV detects a situation that requires an emergency termination of the charging process, the EV will use other means to indicate that an emergency shutdown is required, change to CP State B in accordance with IEC 61851-1.

NOTE 3 If the EVSE detects a CP state C to CP state B change, it will execute an emergency shutdown according to IEC 61851-23-1. It can keep communication open to allow the disconnection of the ACDP and to give status information about the ACDP to the EV.

[V2G20-4028] If EVCC is using ServiceName = DC_ACDP in Table 204 and the EVCC measures CP State change from C/D to E or F it shall start sending ACDP_DisconnectReq.

[V2G20-4030] The EVCC shall stop the V2G communication session when "ResponseCode ≠ OK" of "SessionSetupRes".

[V2G20-4031] If EVCC is using ServiceName = DC_ACDP in Table 204, the EVCC shall send SessionStopReq when the "ResponseCode ≠ OK" of "ACDP_VehiclePositioningRes".

[V2G20-4032] If EVCC is using ServiceName = DC_ACDP in Table 204, the EVCC shall send a SessionStopReq when "ResponseCode ≠ OK" of "ServiceDiscoveryRes".

[V2G20-4033] If EVCC is using ServiceName = DC_ACDP in Table 204, the EVCC shall send a SessionStopReq when "ResponseCode ≠ OK" of "ServiceDetailRes".

[V2G20-4034] If EVCC is using ServiceName = DC_ACDP in Table 204, the EVCC shall send a SessionStopReq when "ResponseCode ≠ OK" of "ServiceSelectionRes".

[V2G20-4035] If EVCC is using ServiceName = DC_ACDP in Table 204, the EVCC shall send a SessionStopReq when "ResponseCode ≠ OK" of "AuthorizationSetupRes".

[V2G20-4036] If EVCC is using ServiceName = DC_ACDP in Table 204, the EVCC shall send a SessionStopReq "ResponseCode ≠ OK" of "AuthorizationRes".

[V2G20-4037] If EVCC is using ServiceName = DC_ACDP in Table 204, the EVCC shall send a SessionStopReq when "ResponseCode ≠ OK" of "CertificateInstallationRes".

[V2G20-4038] If EVCC is using ServiceName = DC_ACDP in Table 204, the EVCC shall send a SessionStopReq when "ResponseCode ≠ OK" of "DC_ChargeParameterDiscoveryRes".

[V2G20-4079] If EVCC is using ServiceName = DC_ACDP in Table 204, the EVCC shall send a SessionStopReq when "ResponseCode ≠ OK" of ScheduleExchangeRes".

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-4039] If EVCC is using ServiceName = DC_ACDP in Table 204, the EVCC shall send a "ACDP_DisconnectReq" when "ResponseCode ≠ OK" of "ACDP_ConnectRes".

[V2G20-4040] If EVCC is using ServiceName = DC_ACDP in Table 204, the EVCC shall send a "ACDP_DisconnectReq" when "ResponseCode ≠ OK" of "CableCheckRes".

[V2G20-4041] If EVCC is using ServiceName = DC_ACDP in Table 204, the EVCC shall send a "ACDP_DisconnectReq" when "ResponseCode ≠ OK" of "PreChargeRes".

[V2G20-4042] If EVCC is using ServiceName = DC_ACDP in Table 204, the EVCC shall send a "ACDP_DisconnectReq" when "ResponseCode ≠ OK" of "PowerDeliveryRes".

[V2G20-4043] If EVCC is using ServiceName = DC_ACDP in Table 204, the EVCC shall send a ACDP_DisconnectReq when "ResponseCode = FAILED" of "DC_ChargeLoopRes".

[V2G20-4044] If EVCC is using ServiceName = DC_ACDP in Table 204, after receiving the ACDP_DisconnectRes with "ResponseCode ≠ OK", the EVCC shall send a SessionStopReq.

8.6.4.5.3 Message Flow

8.6.4.5.3.1 Common message flow

[V2G20-1746] The EVCC shall send a supportedAppProtocolReq after the fulfilment of [V2G20-024].

[V2G20-1747] After receiving the supportedAppProtocolRes with "ResponseCode = OK_SuccessfulNegotiation", the EVCC shall send a SessionSetupReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1089] The SECC shall not send ResponseCode set to OK_SuccessfulNegotiationWithMinorDeviation in supportedAppProtocolRes, since deviations are not supported by ISO 15118-20 (this document).

[V2G20-1090] In case the EVCC receives a supportedAppProtocolRes with ResponseCode set to OK_SuccessfulNegotiationWithMinorDeviation, the EVCC shall treat it the same as when the SECC would have sent OK_SuccessfulNegotiation.

[V2G20-1749] If the EVCC is using PLC, after receiving the SessionSetupRes with "ResponseCode = OK", the EVCC shall send an AuthorizationSetupReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1576] If the EVCC intends to install or update a contract certificate after receiving the AuthorizationSetupRes with "ResponseCode = OK" and CertificateInstallationService set to "True", the EVCC shall send a CertificateInstallationReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1577] After receiving the AuthorizationSetupRes with "ResponseCode = OK" and CertificateInstallationService set to "False", the EVCC shall send an AuthorizationReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1578] After receiving the CertificateInstallationRes with "ResponseCode = OK" and the EVSEProcessing set to "Ongoing", the EVCC shall send another unaltered CertificateInstallationReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1579] After receiving the CertificateInstallationRes with "ResponseCode = OK" and the EVSEProcessing set to "Finished", and RemainingContractCertificateChains set to a value higher than "0", the EVCC shall send another unaltered CertificateInstallationReq to continue the installation or shall send a AuthorizationReq to abort the installation of remaining certificates within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1581] After receiving the CertificateInstallationRes with "ResponseCode = OK", EVSEProcessing set to "Finished" and RemainingContractCertificateChains set to "0", the EVCC shall send an AuthorizationReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1580] After receiving the CertificateInstallationRes with EVSEProcessing set to "Finished" and ResponseCode starting with "WARNING", the EVCC shall ignore all other parameters of the response message and shall do one (1) of the following.

- If the ResponseCode from the SECC was "WARNING_eMSPUnknown", send another CertificateInstallationReq without including the PrioritizedEMAIDs list. Refer to 8.3.4.3.9 and its subclauses for further details of CertificateInstallationReq.

OR

- Send an AuthorizationReq to authorize at the EVSE (using EIM) within V2G_EVCC_Sequence_Performance_Timeout according to Table 215. Refer to 8.3.4.3.3 and its subclauses for further details of AuthorizationReq.

OR

- Stop the V2G communication according to requirements defined 7.4.

NOTE 1 Even if no contract certificate was installed in the current service session, it is possible the EVCC has already installed contractcertificates or it can select to use EIM for authorization (if it was offered by the SECC).

[V2G20-1582] After receiving the AuthorizationRes with "ResponseCode = OK" and the EVSEProcessing set to "Ongoing", the EVCC shall send another unaltered AuthorizationReq (with the exception of TimeStamp) within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1583] After receiving the AuthorizationRes with the EVSEProcessing set to "Finished" and ResponseCode starting with "WARNING", the EVCC shall ignore all other parameters of the response message and shall do one (1) of the following.

- Send an AuthorizationReq with a different ContractCertificateChain (and corresponding GenChallenge) within V2G_EVCC_Sequence_Performance_Timeout according to Table 215. Refer to 8.3.4.3.3 and its subclauses for further details of AuthorizationReq.

OR

- If previously the SelectedAuthorizationService was set to "PnC" and the SECC additionally offered "EIM", send an AuthorizationReq with SelectedAuthorizationService set to "EIM" within V2G_EVCC_Sequence_Performance_Timeout according to Table 215. Refer to 8.3.4.3.3 and its subclauses for further details of AuthorizationReq.

OR

- If previously the SelectedAuthorizationService was set to "EIM" and the SECC additionally offered "PnC", send an AuthorizationReq with SelectedAuthorizationService set to "PnC" within

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

V2G_EVCC_Sequence_Performance_Timeout according to Table 215. Refer to 8.3.4.3.3 and its subclauses for further details of AuthorizationReq.

OR

– If the AuthorizationSetupRes was sent with CertificateInstallationService set to "True", send a CertificateInstallationReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215 to install a new contract certificate. Refer to 8.3.4.3.9 and its subclauses for further details of CertificateInstallationReq.

OR

– Stop the V2G communication according to requirements defined in 7.4.

NOTE 2 It is necessary for EVCC to "remember" the SelectedAuthorizationService service and ContractCertificateChain (if applicable) it has already used during the current service session. Without that the EVCC can be stuck in a continuous loop. The implementers are advised to be careful about such implementation issues.

NOTE 3 If the EVCC previously sent CertificateInstallationReq which resulted in CertificateInstallationRes message with ResponseCode starting with "WARNING", sending another CertificateInstallationReq after the EVCC received AuthorizationRes message with ResponseCode starting with "WARNING" can send EVCC and SECC into an error loop. The implementers are advised to be careful about such implementation issues.

NOTE 4 Although this allows looping behavior and going back and forth between the EIM and PnC based authorization the requirements are written to allow jumping to a different authorization method if the initially selected authorization method fails. Unrestricted looping between different authorization methods can result in the EVCC and SECC being stuck in a loop. The implementers are advised to be careful about such implementation issues.

[V2G20-2221] After receiving the AuthorizationRes with EVSEProcessing set to "Finished" and ResponseCode per [V2G20-2218], the EVCC shall do one (1) of the following.

– Send a ServiceDiscoveryReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

OR

– If the AuthorizationSetupRes was sent with CertificateInstallationService set to "True", send a CertificateInstallationReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215 to install a new contract certificate. Refer to 8.3.4.3.9 and its subclauses for further details of CertificateInstallationReq.

[V2G20-1584] After receiving the AuthorizationRes with EVSEProcessing set to "Finished" and ResponseCode set to "OK", the EVCC shall send a ServiceDiscoveryReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1585] After receiving the ServiceDiscoveryRes with "ResponseCode = OK", the EVCC shall send a ServiceDetailReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1586] After receiving the ServiceDetailRes with "ResponseCode = OK", if further ServiceDetailReq are necessary to retrieve detailed information from the SECC, the EVCC shall send another ServiceDetailReq, within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1587] After receiving the ServiceDetailRes with "ResponseCode = OK", if the EVCC does not require to retrieve more detail about any service from the SECC, the EVCC shall send

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

a ServiceSelectionReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1590] After receiving the ServiceSelectionRes with "ResponseCode = OK", the EVCC shall send a ChargeParameterDiscoveryReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1591] After receiving the ServiceSelectionRes with "ResponseCode = OK", the EVCC may start Internet_Service or ParkingStatus_Service as listed in Table 204.

[V2G20-1592] After receiving the ServiceSelectionRes with "ResponseCode = OK", if there are already existing services, i.e. Internet_Service or ParkingStatus_Service as listed in Table 204, which have not been stopped earlier, these services shall be stopped.

[V2G20-2658] After receiving the ChargeParameterDiscoveryReq, the SECC shall send an ChargeParameterDiscoveryRes within V2G_SECC_Msg_Performance_Time according to Table 215. The next allowed request shall be ScheduleExchangeReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-2659] After receiving the ChargeParameterDiscoveryRes with "ResponseCode = OK", the EVCC shall send a ScheduleExchangeReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1593] After receiving the ScheduleExchangeRes with "ResponseCode = OK" and EVSEProcessing set to "Ongoing", the EVCC shall send another ScheduleExchangeReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1436] If the EVCC is not finished calculating the EVPowerProfile, the EVCC shall send a PowerDeliveryReq with EVProcessing set to "Ongoing" within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1446] After receiving the PowerDeliveryRes with "ResponseCode = OK" and if the previous PowerDeliveryReq message has ChargeProgress = "Stop", the EVCC shall stop all multiplexed communication.

[V2G20-1463] After receiving the SessionStopRes with "ResponseCode = OK", the EVCC shall terminate the communication according to 7.4.

[V2G20-728] After the EVCC stopped the V2G communication session with an error it shall terminate the communication by applying [V2G20-025].

[V2G20-1610] After receiving a response message from the SECC with EVSENotification set to "Terminate" and the corresponding duration of the NotificationMaxDelay has elapsed, the EVCC shall send a SessionStopReq with parameter "ChargingSession" set to "Terminate" while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time.

[V2G20-1476] If the first ServiceDiscoveryRes of the service session had the parameter ServiceRenegotiationSupported set to "True" and the EVCC decided to perform a ServiceRenegotiation, the EVCC shall send a SessionStopReq with ChargingSession set to "ServiceRenegotiation".

[V2G20-1477] If the last SessionStopReq in the sequence had ChargingSession set to "ServiceRenegotiation", after receiving the SessionStopRes with ResponseCode set to

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

"OK", the EVCC shall send a ServiceDiscoveryReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1478] If in the first ServiceDiscoveryRes of the service session the SECC has set ServiceRenegotiationSupported to "False", after waking up from a Pause, the EVCC shall select exactly the same ServiceIDs and ParameterSetIDs it previously selected in the last ServiceSelectionReq. This means it shall not select additional services, deselect previously selected services or change ParameterSetID of a service.

[V2G20-1479] If in the first ServiceDiscoveryRes of the service session the SECC has set ServiceRenegotiationSupported to "True", after waking up from a Pause, the EVCC may select any offered services and parameters independent of the selection in the last ServiceSelectionReq.

[V2G20-1480] The EVCC shall only consider the status of the parameter ServiceRenegotiationSupported sent in the first ServiceDiscoveryRes of the service session.

[V2G20-1661] If the first ServiceDiscoveryRes message of the service session had the parameter ServiceRenegotiationSupported set to "True" and the EVCC decided to perform a ServiceRenegotiation for adapting its service selection, the EVCC shall send a PowerDeliveryReq with parameter ChargeProgress set to "Stop" after ChargeLoopRes has been received while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time.

NOTE 5 As the renegotiation of a service requires to properly end the current charging session (energy transfer) the EVCC will process all required messages (depending on currently selected service) to session stop where the request for a ServiceRenegotiation is to be set according to [V2G20-1476].

8.6.4.5.3.2 AC message flow

[V2G20-2097] After receiving the SessionSetupRes with ResponseCode equal to "OK", the EVCC shall send the proper AC_ChargeParameterDiscoveryReq while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time, in case the EVCC resumes a previously paused V2G communication session.

NOTE 1 In case of a resumed session, the authorization is not required, as authorization details of the previous communication session are valid for the whole service session, see [V2G20-1844].

[V2G20-1596] If EVCC is using ServiceName = AC or AC_BPT in Table 204, after receiving the ScheduleExchangeRes with "ResponseCode = OK", and EVSEProcessing set to "Finished", the EVCC shall send a PowerDeliveryReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1437] If EVCC uses ServiceName = AC or AC_ACDP or AC_BPT or AC_ACD_BPT from Table 204, after receiving the PowerDeliveryRes with "ResponseCode = OK" or "ResponseCode = WARNING_PowerToleranceNotConfirmed", the EVCC shall send an AC_ChargeLoopReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 216 to start the energy transfer, a schedule renegotiation or to enter a standby period.

NOTE 2 During standby both EV and EVSE contactors are to stay closed. The standby concept is solely used as communication state within this documents and therefore is not reflected in related documents, e.g. IEC 61851-1 or IEC 61851-23.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

[V2G20-1440] If the EVCC wants to continue the energy transfer and received the AC_ChargeLoopRes with "ResponseCode = OK", the EVCC shall send another AC_ChargeLoopReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 216.

[V2G20-1443] If the EVCC wants to stop the energy transfer and received the AC_ChargeLoopRes with "ResponseCode = OK, the EVCC shall send a PowerDeliveryReq with ChargeProgress = "Stop" within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-2193] If the EVCC wants to enter a standby phase and received the AC_ChargeLoopRes with "ResponseCode = OK, the EVCC shall send a PowerDeliveryReq with ChargeProgress = "Standby" within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1969] If the first ServiceDiscoveryRes message of the service session had the parameter ServiceRenegotiationSupported set to "True" and the EVCC decided to perform a ServiceRenegotiation for adapting its service selection, the EVCC shall send a PowerDeliveryReq with parameter ChargeProgress set to "Stop" after AC_ChargeLoopRes has been received while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time.

NOTE 3 As the renegotiation of a service requires to properly end the current charging session (energy transfer) the EVCC will process all required messages (depending on currently selected service) to SessionStopReq where the request for a ServiceRenegotiation is to be set according to [V2G20-1476].

8.6.4.5.3.3 DC message flow

[V2G20-2098] After receiving the SessionSetupRes with ResponseCode equal to "OK", the EVCC shall send the proper DC_ChargeParameterDiscoveryReq while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time, in case the EVCC resumes a previously paused V2G communication session.

NOTE In case of a resumed session, the authorization is not required, as authorization details of the previous communication session are valid for the whole service session, see [V2G20-1844].

[V2G20-1594] If EVCC is using ServiceName= DC or DC_BPT in Table 204, after receiving the ScheduleExchangeRes with "ResponseCode = OK", and EVSEProcessing set to "Finished", the EVCC shall send a DC_CableCheckReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 217.

[V2G20-1431] After receiving the DC_CableCheckRes with "ResponseCode = OK" and EVSEProcessing set to "Ongoing", the EVCC shall send another DC_CableCheckReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 217.

[V2G20-1432] After receiving the DC_CableCheckRes with "ResponseCode = OK", and EVSEProcessing set to "Finished", the EVCC shall send a DC_PreChargeReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 217.

[V2G20-1433] After receiving the DC_PreChargeRes with "ResponseCode = OK", the EVCC shall send a DC_PreChargeReq with EVProcessing set to "Ongoing" within V2G_EVCC_Sequence_Performance_Timeout according to Table 217 while the precharge process is not finished.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1434] After receiving the DC_PreChargeRes with "ResponseCode = OK", the EVCC shall send a DC_PreChargeReq with EVProcessing set to "Finished" within V2G_EVCC_Sequence_Performance_Timeout according to Table 217 when the precharge process is finished.

[V2G20-1435] After receiving the DC_PreChargeRes message with "ResponseCode = OK", the EVCC shall send a PowerDeliveryReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1438] If EVCC uses ServiceName = DC or DC_BPT from Table 204, after receiving the PowerDeliveryRes with "ResponseCode = OK" or "ResponseCode = WARNING_PowerToleranceNotConfirmed", the EVCC shall send a DC_ChargeLoopReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 217 to start the energy transfer, a schedule renegotiation or enter a standby period.

During standby both EV and EVSE contactors are to stay closed. The standby concept is solely used as communication state within this document and therefore is not reflected in related documents, e.g. IEC 61851-1 or IEC 61851-23.

[V2G20-1441] If the EVCC wants to continue the energy transfer and received the DC_ChargeLoopRes with "ResponseCode = OK", the EVCC shall send another DC_ChargeLoopReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 217.

[V2G20-1444] If the EVCC wants to stop the energy transfer and received the DC_ChargeLoopRes with "ResponseCode = OK", the EVCC shall send a PowerDeliveryReq with ChargeProgress = "Stop" within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-2195] If the EVCC wants to enter a standby phase and received the DC_ChargeLoopRes with "ResponseCode = OK", the EVCC shall send a PowerDeliveryReq with ChargeProgress = "Standby" within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-1448] If the EVCC is using ServiceName = DC or DC_BPT in Table 204, after receiving the PowerDeliveryRes with "ResponseCode = OK" and if the previous PowerDeliveryReq message has ChargeProgress = "Stop", the EVCC shall send a DC_WeldingDetectionReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 217.

[V2G20-1573] After receiving the DC_WeldingDetectionRes with "ResponseCode = OK", the EVCC shall send a DC_WeldingDetectionReq with EVProcessing set to "Ongoing" within V2G_EVCC_Sequence_Performance_Timeout according to Table 217 while the welding detection process is not finished.

[V2G20-1461] After receiving the DC_WeldingDetectionRes with "ResponseCode = OK", the EVCC shall send a DC_WeldingDetectionReq with EVProcessing set to "Finished" within V2G_EVCC_Sequence_Performance_Timeout according to Table 217 when the welding detection process is finished.

[V2G20-1462] After receiving the DC_WeldingDetectionRes message with "ResponseCode = OK", the EVCC shall send a SessionStopReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

8.6.4.5.3.4 WPT message flow

[V2G20-5042] If the EVCC is using the WPT module, after receiving the SessionSetupRes with "ResponseCode = OK", the EVCC shall send a WPT_FinePositioningSetupReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-5046] After receiving the SessionSetupRes with ResponseCode equal to "OK", the EVCC shall send a WPT_ChargeParameterDiscoveryReq while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time, in case EVCC resumes a previously paused V2G communication session.

NOTE In case of a resumed session, the authorization is not required, as authorization details of the previous communication session are valid for the whole service session, see [V2G20-1844].

[V2G20-5067] After receiving one of the messages WPT_FinePositioningSetupRes, WPT_FinePositioningRes, WPT_PairingRes, WPT_AlignmentCheckRes, WPT_ChargeLoopRes with ResponseCode = FAILED, the EVCC shall send a SessionStopReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 218 to terminate the session.

[V2G20-5024] After receiving a WPT_FinePositioningSetupRes with "ResponseCode = OK", the EVCC shall send a WPT_FinePositioningReq or a WPT_FinePositioningSetupReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 218.

[V2G20-5025] After receiving a WPT_FinePositioningRes with "ResponseCode = OK" and EVSEProcessing set to "Ongoing", the EVCC shall send a WPT_FinePositioningReq with EVProcessing set to "Ongoing" while the vehicle positioning is still ongoing within V2G_EVCC_Sequence_Performance_Timeout according to Table 218.

[V2G20-5026] After receiving a WPT_FinePositioningRes with "ResponseCode = OK" and EVSEProcessing set to "Ongoing", the EVCC shall send a WPT_FinePositioningReq with EVProcessing set to "Finished" when the vehicle positioning is finished within V2G_EVCC_Sequence_Performance_Timeout according to Table 218.

[V2G20-5027] After sending a WPT_FinePositioningReq with EVProcessing set to "Finished", and receiving the next response message with "ResponseCode = OK", the EVCC shall send a WPT_PairingReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 218.

[V2G20-5029] After receiving a WPT_FinePositioningRes with "ResponseCode = OK" and EVSEProcessing set to "Finished", the EVCC shall send a WPT_PairingReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 218.

[V2G20-5055] After receiving a WPT_FinePositioningRes with "ResponseCode = WARNING_WPT" and EVSEProcessing set to "Finished", the EVCC shall send a WPT_FinePositioningSetupReq or terminate by sending a SessionStopReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 218.

[V2G20-5030] After receiving a WPT_PairingRes with "ResponseCode = OK" and EVSEProcessing = "Ongoing", the EVCC shall send a WPT_PairingReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 218. While the pairing process is still on-going, the EVCC shall send the WPT_PairingReq with EVProcessing set to "Ongoing".

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-5031] After receiving the WPT_PairingRes with "ResponseCode = OK" and EVSEProcessing = "Ongoing", the EVCC shall send a WPT_PairingReq with EVProcessing set to "Finished" within V2G_EVCC_Sequence_Performance_Timeout according to Table 190 if the pairing process is finished (see also [V2G20-5012]).

[V2G20-5032] After sending a WPT_PairingReq with EVProcessing set to "Finished", and receiving the next response message with ResponseCode = "OK", the EVCC shall send an AuthorizationSetupReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-5033] After receiving a WPT_PairingRes with ResponseCode = "OK" and EVSEProcessing set to "Ongoing", the EVCC shall send a WPT_PairingReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 218.

[V2G20-5034] After receiving a WPT_PairingRes with "ResponseCode = OK", and EVSEProcessing set to "Finished", the EVCC shall send an AuthorizationSetupReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-5054] After receiving a WPT_PairingRes with ResponseCode = "WARNING_WPT", and EVSEProcessing set to "Finished", the EVCC shall send a WPT_FinePositioningSetupSetupReq or terminate by sending a SessionStopReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-5045] After receiving a ScheduleExchangeRes with ResponseCode = "OK" and EVSEProcessing set to "Finished" the EVCC shall send a WPT_AlignmentCheckReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 218.

[V2G20-5062] After receiving a WPT_ChargeParameterDiscoveryRes with ResponseCode = "WARNING_WPT" the EVCC shall send a WPT_FinePositioningSetupReq or terminate by sending a SessionStopReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 218.

[V2G20-5041] If the EVCC is using ServiceName = WPT, after receiving the ServiceSelectionRes with "ResponseCode = OK", the EVCC shall send a WPT_ChargeParameterDiscoveryReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-5035] After receiving a WPT_AlignmentCheckRes with ResponseCode = "OK", and EVSEProcessing set to "Ongoing", the EVCC shall send a WPT_AlignmentCheckReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 218.

[V2G20-5057] After receiving a WPT_AlignmentCheckRes with ResponseCode = "WARNING_WPT", and EVSEProcessing set to "Finished", the EVCC shall send a WPT_FinePositioningSetupReq or terminate by sending a SessionStopReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-5036] After sending a WPT_AlignmentCheckReq with EVProcessing set to "Finished", and received the next response message with "ResponseCode = OK", the EVCC shall send a PowerDeliveryReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-5037] If EVCC uses ServiceName = WPT from Table 204, after receiving the PowerDeliveryRes with "ResponseCode = OK", the EVCC shall send an WPT_ChargeLoopReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 218 to start the energy transfer.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-5061] If EVCC uses ServiceName = WPT from Table 204, after receiving the PowerDeliveryRes with "ResponseCode = WARNING_WPT", the EVCC shall send a WPT_FinePositioningSetupReq or terminate by sending a SessionStopReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 218.

[V2G20-5058] After receiving a WPT_ChargeLoopRes with "ResponseCode = WARNING_WPT", the EVCC shall send a WPT_AlignmentCheckReq or a WPT_PairingReq or terminate by sending a SessionStopReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-5039] If the EVCC wants to continue the energy transfer and received the WPT_ChargeLoopRes with "ResponseCode = OK", the EVCC shall send another WPT_ChargeLoopReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 218.

[V2G20-5082] If the EVCC wants to stop the energy transfer and received the WPT_ChargeLoopRes with "ResponseCode = OK" the EVCC shall send a PowerDeliveryReq with ChargeProgress = "Stop" within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-5129] If the EVCC wants to enter a standby phase and received the WPT_ChargeLoopRes with "ResponseCode = OK" the EVCC shall send a PowerDeliveryReq with ChargeProgress = "Standby" within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-5040] If EVCC is using ServiceName = WPT in Table 204, after receiving the PowerDeliveryRes with "ResponseCode = OK", and if the previous PowerDeliveryReq message has ChargeProgress = "Stop", the EVCC shall send a SessionStopReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

8.6.4.5.3.5 ACDP message flow

[V2G20-4045] The following requirement is not applicable when using ServiceName = DC_ACDP: [V2G20-1446].

NOTE 1 The common requirements [V2G20-1746] and [V2G20-1747] apply.

[V2G20-4046] If the EVCC is using WLAN, after receiving the SessionSetupRes with "ResponseCode = OK", the EVCC shall send a ACDP_VehiclePositioningReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-4047] After receiving the ACDP_VehiclePositioningRes with "ResponseCode = OK" and EVSEProcessing set to "Ongoing", the EVCC shall send another ACDP_VehiclePositioningReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-4048] When the EV has determined that it is sufficiently well positioned to meet the requirement 201.1 of IEC 61851-23, and is immobilized, the EVCC shall send a ACDP_VehiclePositioningReq with EVMobilityStatus set to "EV is immobilized", within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-4049] After receiving the ACDP_VehiclePositioningRes with "ResponseCode = OK", and EVSEProcessing set to "Finished", the EVCC shall send an AuthorizationSetupReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

NOTE 2 The common requirements [V2G20-1577], [V2G20-1576], [V2G20-1580], [V2G20-1581], [V2G20-1578], [V2G20-1579], [V2G20-1582], [V2G20-1583], [V2G20-1584], [V2G20-1585], [V2G20-1586], [V2G20-1587], [V2G20-1590] and [V2G20-1593] apply.

[V2G20-4050] If EVCC is using ServiceName = DC_ACDP, in Table 204, after receiving the ScheduleExchangeRes with "ResponseCode = OK", and EVSEProcessing set to "Finished", the EVCC shall send a ACDP_ConnectReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-4051] If EVCC is using ServiceName = DC_ACDP, after receiving the ACDP_ConnectRes with "ResponseCode = OK" and EVSEProcessing set to "Ongoing", the EVCC shall send another ACDP_ConnectReq within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

[V2G20-4052] If EVCC is using ServiceName = DC_ACDP, after receiving the ACDP_ConnectRes with "ResponseCode = OK", and EVSEProcessing set to "Finished", the EVCC shall send a DC_CableCheckReq if ServiceName = DC_ACDP or DC_ACDP_BPT in Table 204 was selected within V2G_EVCC_Sequence_Performance_Timeout according to Table 215.

NOTE 3 The DC requirements [V2G20-1431], [V2G20-1432], [V2G20-1433], [V2G20-1434], [V2G20-1435], [V2G20-1436], [V2G20-1438], [V2G20-1441], [V2G20-1444] and [V2G20-913] apply.

NOTE 4 The general requirement [V2G20-1416] applies for an EVSE initiated stop.

When the EV intends to stop the charge session it is recommended to request 0A in the DC_ChargeLoopReq, to allow the EVSE to ramp down the current with the minimum rate of 100A/s (as defined in IEC 61851-23).

[V2G20-4053] If EVCC is using ServiceName = DC_ACDP in Table 204, after receiving the PowerDeliveryRes as a response to a previous PowerDeliveryReq message with ChargeProgress equal to "Stop", the EVCC shall send a ACDP_DisconnectReq while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time.

[V2G20-4054] After receiving the ACDP_DisconnectRes with ResponseCode = "OK" and "EVSEProcessing =Ongoing", the EVCC shall send a ACDP_DisconnectReq while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time.

[V2G20-4055] After receiving the ACDP_DisconnectRes with "ResponseCode = OK" and with parameter "EVSEProcessing" set to "Finished", the EVCC shall send a SessionStopReq while V2G_EVCC_Sequence_Timer is smaller than V2G_EVCC_Sequence_Performance_Time.

[V2G20-4056] If EVCC is using ServiceName = DC_ACDP after receiving the SessionStopRes with "ResponseCode = OK" the EVCC shall stop all multiplexed communication.

NOTE 5 The common requirement [V2G20-1463] applies.

8.6.4.6 SECC

8.6.4.6.1 General

The following clauses contain the SECC behavior, which defines all valid request-response message sequences.

8.6.4.6.2 Error handling

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

[V2G20-1481] At any stage of the V2G communication session, the SECC shall stop the V2G communication according to the requirements defined 7.4 when V2G_SECC_Sequence_Timer is equal or larger than V2G_SECC_Sequence_Timeout according to Table 215.

[V2G20-538] The SECC shall respond with the corresponding response message containing a "ResponseCode = FAILED_SequenceError" within V2G_SECC_Msg_Performance_Time according to Table 215, if request message was received that the SECC does not expect in the wait state.

[V2G20-1482] After sending a message containing a "ResponseCode = FAILED_SequenceError", the SECC shall behave according to the requirements defined in 7.4.

[V2G20-2222] After the SECC sent a ResponseCode starting with 'FAILED' or 'FAILED_' it shall terminate the communication by applying [V2G20-034].

8.6.4.6.2.1 ACDP error handling

[V2G20-4057] If SECC is using ServiceName = DC_ACDP, [V2G20-1482] does not apply.

[V2G20-4058] In case of any exception handling the SECC shall continue the communication to the EVCC until the last message pair of the exception handling procedure has been executed.

NOTE 1 The EVSE initiates an emergency shut down by ramping down the charging current, open its DC contactors and setting the CP signal to state E (0V). The EVSE will then raise the pantograph. Then the EVCC issues the SessionStop message to end the process. The ACDP_SystemStatus reflects the EVSE causing the emergency shut down. As described in IEC 61851-23.

[V2G20-4059] When SECC experiences an emergency situation, and EVCC is using ServiceName = DC_ACDP in Table 204 the EVSE shall set CP state to E.

NOTE 2 In case high level communication is disturbed or the ACDP is actually blocked from reaching the predefined safe position a procedure can be agreed upon to mobilize the EV in a safe way. A visual confirmation by the driver that the pantograph is actually in a safe position, after which he can manually get the EV in a mobilized state.

[V2G20-4060] If SECC is using ServiceName = DC_ACDP in Table 204, the SECC shall allow a SessionStopReq in case no ACDP_ConnectReq has been received.

[V2G20-4061] If SECC is using ServiceName = DC_ACDP in Table 204, the SECC shall allow receiving a ACDP_DisconnectReq after sending ACDP_ConnectDeviceRes, CableCheckRes, DC_ChargeLoopRes or PowerDeliveryRes.

[V2G20-4062] If SECC is using ServiceName = DC_ACDP in Table 204, after sending a message containing a "ResponseCode = FAILED" in SessionSetupRes or SupportedAppProtocolRes, the SECC shall behave according to the requirements defined in 7.4.

8.6.4.6.2.2 ACDP exception handling in case of association loss

After the SDP process has been completed successfully the EV and the EVSE are associated correctly and the high-level communication starts. EV and EVSE are in the state "Associated". The association status of EVCC and SECC/EVSE shall continuously be supervised by the consistency of the received EVID by the PPD until the ACDP is activated successfully.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

A typical reason for losing the association status is when the driver was closely approaching an ACDP and decides to head for another ACDP afterwards. In this case the EV to EVSE association will be established according to the ACDP which the EV approached first. As soon as the EV leaves the PPD detection zone the association will quit. This is then a loss of association event. Then the SDP process will restart from the beginning.

[V2G20-4063] For early association support the association status between EV and EVSE shall be considered as being correctly associated as long as the continuously updated PPD information provides the same EVID as received by the SDP request when the element PPD/P2PS of the SDP request was set to value "PPD on infrastructure" according to Table 23.

[V2G20-4064] For early association support the association status between EV and EVSE shall be continuously supervised by the SECC when the element PPD/P2PS of the SDP request was set to value "PPD on infrastructure" according to Table 23.

[V2G20-4065] For early association support the SECC shall respond the latest V2G message request with the ResponseCode= FAILED_AssociationError when EV and EVSE are not correctly associated and then wait for a new SDP request when the element PPD/P2PS of the SDP request was set to value "PPD on infrastructure" according to Table 23.

[V2G20-4066] For early association support the SECC shall stop the supervision of the association status after the ACDP_VehiclePositioning has been finished with ResponseCode = OK and EVSEProcessing=Finished when the element PPD/P2PS of the SDP request was set to value "PPD on infrastructure" according to Table 23.

8.6.4.6.3 Message flow

8.6.4.6.3.1 Common message flow

[V2G20-1483] The SECC shall wait for supportedAppProtocolReq, set the timeout V2G_SECC_Sequence_Timeout to the value MessageType as defined in Table 215, reset the V2G_SECC_Sequence_Timer and start monitoring the V2G_SECC_Sequence_Timer.

NOTE 1 Before the first message, the SECC did not send any response message. Therefore, the SECC starts its sequence timer when starting to wait for the first message.

[V2G20-1484] After receiving a supportedAppProtocolReq, the SECC shall respond with a supportedAppProtocolRes within V2G_SECC_Msg_Performance_Time according to Table 215. The allowed next request shall be SessionSetupReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-1486] After receiving a SessionSetupReq, the SECC shall respond with a SessionSetupRes within V2G_SECC_Msg_Performance_Time according to Table 215. If the SECC is using "PLC", the allowed next request shall be AuthorizationSetupReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-1970] After receiving the AuthorizationSetupReq, the SECC shall respond with an AuthorizationSetupRes within V2G_SECC_Msg_Performance_Time according to Table 215. If the AuthorizationSetupRes is sent with CertificateInstallationService set to "True", the next allowed request shall be CertificateInstallationReq or AuthorizationReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1971] After receiving the AuthorizationSetupReq, the SECC shall send an AuthorizationSetupRes within V2G_SECC_Msg_Performance_Time according to Table 215. If the AuthorizationSetupRes is sent with CertificateInstallationService set to "False", the next allowed request shall be AuthorizationReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-1972] After receiving the CertificateInstallationReq, if the data required for the CertificateInstallationRes is not yet available, the SECC shall respond with a CertificateInstallationRes with EVSEProcessing set to "Ongoing" within V2G_SECC_Msg_Performance_Time according to Table 215. The next allowed request shall be CertificateInstallationReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-1973] After receiving the CertificateInstallationReq, if the data required for the CertificateInstallationRes is available and additional contract certificate chains are available, the SECC shall respond with a CertificateInstallationRes with RemainingContractCertificateChains set to the number of remaining contract certificate chains and EVSEProcessing set to "Finished" within V2G_SECC_Msg_Performance_Time according to Table 215. The next allowed request shall be CertificateInstallationReq or AuthorizationReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-1974] The SECC shall not provide more contract certificate chains than supported by the EVCC, which was communicated by the EVCC in the CertificateInstallationReq through the parameter MaximumContractCertificateChains.

[V2G20-1975] After receiving the CertificateInstallationReq, if the data required for the CertificateInstallationRes is available and no additional contract certificate chains are available, the SECC shall respond with a CertificateInstallationRes with EVSEProcessing set to "Finished" and RemainingContractCertificateChains set to "0" within V2G_SECC_Msg_Performance_Time according to Table 215. The next allowed request shall be AuthorizationReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-2223] After receiving the CertificateInstallationReq, if an issue was detected with the provided OEM provisioning certificate chain, the SECC shall respond with a CertificateInstallationRes with EVSEProcessing set to "Finished" and ResponseCode starting with "WARNING", specifying the detected issue with the provided OEMProvisioningCertificate chain (refer to [V2G20-2203], [V2G20-1412], [V2G20-2204] and [V2G20-2205] for further details of the ResponseCode to be provided) within V2G_SECC_Msg_Performance_Time according to Table 215. All mandatory parameters shall be filled in with arbitrary XSD conform values. All values shall be chosen in a way that results in a minimal size of the response message. The next allowed request shall be AuthorizationReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-2224] After receiving the CertificateInstallationReq, if the SECC does not recognize any one (or more) of the eMSPs indicated by the EMAID included in the PrioritizedEMAIDs list the SECC shall respond with a CertificateInstallationRes with EVSEProcessing set to "Finished" and ResponseCode per [V2G20-2208] within V2G_SECC_Msg_Performance_Time according to Table 215. All mandatory parameters shall be filled in with arbitrary XSD conform values. All values shall be chosen in a way that results in a minimal size of the response message. The next

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

allowed request shall be AuthorizationReq or another CertificateInstallationReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-1976] After receiving the CertificateInstallationReq, if no contract certificate chain for the provided PCID could be found, the SECC shall respond with a CertificateInstallationRes with EVSEProcessing set to "Finished" and ResponseCode per [V2G20-2206] within V2G_SECC_Msg_Performance_Time according to Table 215. All mandatory parameters shall be filled in with arbitrary XSD conform values. All values shall be chosen in a way that results in a minimal size of the response message. The next allowed request shall be AuthorizationReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-2225] After receiving the CertificateInstallationReq, if the new contract certificate cannot be retrieved from secondary actor within V2G_SECC_Msg_Performance_Time (according to Table 215), the SECC shall respond with a CertificateInstallationRes with EVSEProcessing set to "Finished" and ResponseCode per [V2G20-2207] within V2G_SECC_Msg_Performance_Time according to Table 215. All mandatory parameters shall be filled in with arbitrary XSD conform values. All values shall be chosen in a way that results in a minimal size of the response message. The next allowed request shall be AuthorizationReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-1977] After receiving the AuthorizationReq, the SECC shall respond with an AuthorizationRes with EVSEProcessing set to "Ongoing" within V2G_SECC_Msg_Performance_Time according to Table 215, while the authorization is still ongoing. The next allowed request shall be another unaltered AuthorizationReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

NOTE 2 This applies to both EIM and PnC authorization modes.

[V2G20-2226] After receiving the AuthorizationReq with SelectedAuthorizationService set to a value that was not part of the offered AuthoritzationServices of AuthorizationSetupRes message, the SECC shall respond with an AuthorizationRes with EVSEProcessing set to "Finished" and ResponseCode per [V2G20-2209] within V2G_SECC_Msg_Performance_Time according to Table 215. All mandatory parameters shall be filled in with arbitrary XSD conform values. All values shall be chosen in a way that results in a minimal size of the response message. The next allowed request shall be one (1) of the following.

- Another AuthorizationReq with a SelectedAuthorizationService that was offered via AuthoritzationServices of AuthorizationSetupRes. The V2G_SECC_Sequence_Timeout shall be according to Table 215.

OR

- CertificateInstallationReq within the V2G_SECC_Sequence_Timeout according to Table 215, if the AuthorizationSetupRes was sent with CertificateInstallationService set to "True".

NOTE 3 This allows SECC to ensure that it can terminate connection with an EVCC that can be stuck sending the same AuthorizationReq with the same invalid SelectedAuthorizationService.

[V2G20-2227] After receiving the AuthorizationReq with SelectedAuthorizationService set to a value that was not part of the offered AuthoritzationServices of AuthorizationSetupRes message, the SECC shall respond with an AuthorizationRes with EVSEProcessing set to "Finished" and ResponseCode per [V2G20-2209] within V2G_SECC_Msg_Performance_Time according to Table 215. All mandatory

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

parameters shall be filled in with arbitrary XSD conform values. All values shall be chosen in a way that results in a minimal size of the response message. The next allowed request shall be another AuthorizationReq with a SelectedAuthorizationService that was offered via AuthoritzationServices of AuthorizationSetupRes, if the AuthorizationSetupRes was sent with CertificateInstallationService set to "False". The V2G_SECC_Sequence_Timeout shall be according to Table 215.

NOTE 4 This allows SECC to ensure that it can terminate connection with an EVCC that can be stuck sending the same AuthorizationReq with the same invalid SelectedAuthorizationService.

[V2G20-1978] After receiving the AuthorizationReq with SelectedAuthorizationService set to "PnC" when an issue is detected (either by SECC or by SA) with the provided contract certificate chain, the SECC shall respond with an AuthorizationRes with EVSEProcessing set to "Finished" and ResponseCode starting with "WARNING", specifying the detected issue with the provided contractcertificate (refer to [V2G20-2210], [V2G20-2211], [V2G20-2212], [V2G20-2213], [V2G20-2214] and [V2G20-2215] for further details of the ResponseCode to be provided) within V2G_SECC_Msg_Performance_Time according to Table 215. All mandatory parameters shall be filled in with arbitrary XSD conform values. All values shall be chosen in a way that results in a minimal size of the response message. The next allowed request shall be one (1) of the following:

- another AuthorizationReq with a different ContractCertificateChain (and corresponding GenChallenge). The V2G_SECC_Sequence_Timeout shall be according to Table 215;

OR

- another AuthorizationReq with SelectedAuthorizationService set to "EIM", if "EIM" was offered via AuthoritzationServices of AuthorizationSetupRes. The V2G_SECC_Sequence_Timeout shall be according to Table 215;

OR

- CertificateInstallationReq within the V2G_SECC_Sequence_Timeout according to Table 215, if the AuthorizationSetupRes was sent with CertificateInstallationService set to "True".

NOTE 5 This allows SECC to ensure that it can terminate connection with an EVCC that can be stuck sending the same AuthorizationReq with the same invalid ContractCertificateChain.

[V2G20-2131] After receiving the AuthorizationReq with SelectedAuthorizationService set to "PnC" when an issue is detected (either by SECC or by SA) with the provided contractcertificate chain, the SECC shall respond with an AuthorizationRes with EVSEProcessing set to "Finished" and ResponseCode starting with "WARNING", specifying the detected issue with the provided contractcertificate (refer to [V2G20-2210], [V2G20-2211], [V2G20-2212], [V2G20-2213], [V2G20-2214] and [V2G20-2215] for further details of the ResponseCode to be provided) within V2G_SECC_Msg_Performance_Time according to Table 215. All mandatory parameters shall be filled in with arbitrary XSD conform values. All values shall be chosen in a way that results in a minimal size of the response message. The next allowed request shall be one (1) of the following, if the AuthorizationSetupRes was sent with CertificateInstallationService set to "False":

- another AuthorizationReq with a different ContractCertificateChain (and corresponding GenChallenge). The V2G_SECC_Sequence_Timeout shall be according to Table 215;

OR

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

– another AuthorizationReq with SelectedAuthorizationService set to "EIM", if "EIM" was offered via AuthoritzationServices of AuthorizationSetupRes. The V2G_SECC_Sequence_Timeout shall be according to Table 215.

NOTE 6 This allows SECC to ensure that it can terminate connection with an EVCC that can be stuck sending the same AuthorizationReq with the same invalid ContractCertificateChain.

[V2G20-2228] After receiving the AuthorizationReq with SelectedAuthorizationService set to "PnC" if the challenge response contained in the AuthorizationReq message (in attribute GenChallenge) is not valid versus the GenChallenge provided in AuthorizationSetupRes, the SECC shall respond with an AuthorizationRes with EVSEProcessing set to "Finished" and ResponseCode per [V2G20-2216] within V2G_SECC_Msg_Performance_Time according to Table 215. All mandatory parameters shall be filled in with arbitrary XSD conform values. All values shall be chosen in a way that results in a minimal size of the response message. The next allowed request shall be one (1) of the following:

– another AuthorizationReq with a different ContractCertificateChain (and corresponding GenChallenge). The V2G_SECC_Sequence_Timeout shall be according to Table 215;

OR

– another AuthorizationReq with SelectedAuthorizationService set to "EIM", if "EIM" was offered via AuthoritzationServices of AuthorizationSetupRes. The V2G_SECC_Sequence_Timeout shall be according to Table 215;

OR

– CertificateInstallationReq within the V2G_SECC_Sequence_Timeout according to Table 215, if the AuthorizationSetupRes was sent with CertificateInstallationService set to "True".

NOTE 7 This allows SECC to ensure that it can terminate connection with an EVCC that can be stuck sending the same AuthorizationReq with the same invalid ContractCertificateChain.

[V2G20-2229] After receiving the AuthorizationReq with SelectedAuthorizationService set to "PnC" if the challenge response contained in the AuthorizationReq message (in attribute GenChallenge) is not valid versus the GenChallenge provided in AuthorizationSetupRes, the SECC shall respond with an AuthorizationRes with EVSEProcessing set to "Finished" and ResponseCode per [V2G20-2216] within V2G_SECC_Msg_Performance_Time according to Table 215. All mandatory parameters shall be filled in with arbitrary XSD conform values. All values shall be chosen in a way that results in a minimal size of the response message. The next allowed request shall be one (1) of the following, if the AuthorizationSetupRes was sent with CertificateInstallationService set to "False":

– another AuthorizationReq with a different ContractCertificateChain (and corresponding GenChallenge). The V2G_SECC_Sequence_Timeout shall be according to Table 215;

OR

– another AuthorizationReq with SelectedAuthorizationService set to "EIM", if "EIM" was offered via AuthoritzationServices of AuthorizationSetupRes. The V2G_SECC_Sequence_Timeout shall be according to Table 215.

NOTE 8 This allows SECC to ensure that it can terminate connection with an EVCC that can be stuck sending the same AuthorizationReq with the same invalid ContractCertificateChain.

[V2G20-2232] After receiving the AuthorizationReq with SelectedAuthorizationService set to "PnC", the SECC shall respond with an AuthorizationRes with EVSEProcessing set to

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

"Finished" and ResponseCode per [V2G20-2218] within V2G_SECC_Msg_Performance_Time according to Table 215, when authorization has completed successfully but the received contract certificate will expire in 14 days or fewer. The next allowed request shall be one (1) of the following:

- ServiceDiscoveryReq within the V2G_SECC_Sequence_Timeout according to Table 215;

OR

- CertificateInstallationReq within the V2G_SECC_Sequence_Timeout according to Table 215, if the AuthorizationSetupRes was sent with CertificateInstallationService set to "True".

NOTE 9 This allows EVCC to install a new contract certificate if it so chooses.

[V2G20-2233] After receiving the AuthorizationReq with SelectedAuthorizationService set to "PnC", the SECC shall respond with an AuthorizationRes with EVSEProcessing set to "Finished" and ResponseCode per [V2G20-2218] within V2G_SECC_Msg_Performance_Time according to Table 215, when authorization has completed successfully but the received contract certificate will expire in 14 days or fewer. The next allowed request shall be ServiceDiscoveryReq, if the AuthorizationSetupRes was sent with CertificateInstallationService set to "False". The V2G_SECC_Sequence_Timeout shall be according to Table 215.

[V2G20-2230] After receiving the AuthorizationReq with SelectedAuthorizationService set to "EIM", the SECC shall respond with an AuthorizationRes with EVSEProcessing set to "Finished" and ResponseCode per [V2G20-2219] within V2G_SECC_Msg_Performance_Time according to Table 215, when authorization has failed due to any reason. All mandatory parameters shall be filled in with arbitrary XSD conform values. All values shall be chosen in a way that results in a minimal size of the response message. The next allowed request shall be one (1) of the following:

- another AuthorizationReq with SelectedAuthorizationService set to "PnC", if "PnC" was offered via AuthoritzationServices of AuthorizationSetupRes. The V2G_SECC_Sequence_Timeout shall be according to Table 215;

OR

- CertificateInstallationReq within the V2G_SECC_Sequence_Timeout according to Table 215, if the AuthorizationSetupRes was sent with CertificateInstallationService set to "True".

NOTE 10 This allows SECC to ensure that it can terminate connection with an EVCC that can be stuck sending the same AuthorizationReq with the same invalid ContractCertificateChain.

[V2G20-2231] After receiving the AuthorizationReq with SelectedAuthorizationService set to "EIM", the SECC shall respond with an AuthorizationRes with EVSEProcessing set to "Finished" and ResponseCode per [V2G20-2219] within V2G_SECC_Msg_Performance_Time according to Table 215, when authorization has failed due to any reason. All mandatory parameters shall be filled in with arbitrary XSD conform values. All values shall be chosen in a way that results in a minimal size of the response message. The next allowed request shall be another AuthorizationReq with SelectedAuthorizationService set to "PnC", if "PnC" was offered via AuthoritzationServices of AuthorizationSetupRes and the AuthorizationSetupRes was sent with CertificateInstallationService set to "False". The V2G_SECC_Sequence_Timeout shall be according to Table 215.

NOTE 11 This allows SECC to ensure that it can terminate connection with an EVCC can be stuck sending the same AuthorizationReq with the same invalid ContractCertificateChain.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-1979] After receiving the AuthorizationReq with SelectedAuthorizationService set to "PnC", the SECC shall respond with an AuthorizationRes with EVSEProcessing set to "Finished" and ResponseCode set to "OK" within V2G_SECC_Msg_Performance_Time according to Table 215, when authorization has completed successfully and the received contractcertificate will expire in more than 14 days. The next allowed request shall be ServiceDiscoveryReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-2234] After receiving the AuthorizationReq with SelectedAuthorizationService set to "EIM", the SECC shall respond with an AuthorizationRes with EVSEProcessing set to "Finished" and ResponseCode starting with "OK" within V2G_SECC_Msg_Performance_Time according to Table 215, when authorization has completed successfully. The next allowed request shall be ServiceDiscoveryReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-1980] After receiving the ServiceDiscoveryReq, the SECC shall respond with a ServiceDiscoveryRes within V2G_SECC_Msg_Performance_Time according to Table 215, the allowed next request shall be ServiceDetailReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-1957] If the first ServiceDiscoveryRes of the service session had the parameter ServiceRenegotiationSupported set to "False" and, after waking up from a Pause, if the SECC does not offer the same ServiceIDs and parameterSetIDs that were selected previously by the EV, then EVCC shall stop the session by sending the message SessionStopReq with parameter ChargingSession equal to "Terminate".

[V2G20-1981] After receiving the ServiceDetailReq the SECC shall respond with a ServiceDetailRes within V2G_SECC_Msg_Performance_Time according to Table 215. The allowed next requests shall be either ServiceDetailReq or ServiceSelectionReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-1983] After receiving the ServiceSelectionReq, the SECC shall respond with ServiceSelectionRes within V2G_SECC_Msg_Performance_Time according to Table 215.

[V2G20-1984] After sending the ServiceSelectionRes with ResponseCode = "OK", the SECC shall be ready to offer any of the value added services it may support, i.e. Internet_Service, ParkingStatus_Service, and/or ACDP_SystemStatus_Service as listed in Table 204.

[V2G20-1985] After receiving the ServiceSelectionReq, if there are already existing services, i.e. Internet_Service, ParkingStatus_Service, and/or ACDP_SystemStatus_Service as listed in Table 204 which have not been stopped earlier, these services shall be stopped.

[V2G20-1986] After receiving the ScheduleExchangeReq, the SECC shall respond with a ScheduleExchangeRes with EVSEProcessing set to "Ongoing" within V2G_SECC_Msg_Performance_Time according to Table 215, while the process is still ongoing. The next allowed request shall be ScheduleExchangeReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-1987] After receiving the ScheduleExchangeReq, the SECC shall respond with a ScheduleExchangeRes with EVSEProcessing set to "Finished" and ResponseCode starting with "OK" within V2G_SECC_Msg_Performance_Time according to Table 215, if all parameters are available.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2007] After receiving the PowerDeliveryReq with EVProcessing set to "Ongoing" and ResponseCode starting with "OK", the SECC shall ignore the other contents of the PowerDeliveryReq and respond with a PowerDeliveryRes within V2G_SECC_Msg_Performance_Time according to Table 215. The next allowed request shall be PowerDeliveryReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-2008] After receiving the PowerDeliveryReq with EVProcessing set to "Finished", the SECC shall respond with a PowerDeliveryRes within V2G_SECC_Msg_Performance_Time according to Table 215.

[V2G20-1601] In case the SECC intends to renegotiate after having received a PowerDeliveryReq with PowerToleranceAcceptance set to "PowerToleranceNotConfirmed", the SECC shall send the response code "WARNING_PowerToleranceNotConfirmed" in PowerDeliveryRes and set EVSENotification in EVSEStatus to "Renegotiation"

NOTE 12 Based on local supply, or other boundary conditions the SECC can renegotiate the applicable power tolerance for a particular charging session.

[V2G20-2018] If the PowerDeliveryReq received has ChargeProgress = "Renegotiate", the SECC shall respond with a PowerDeliveryRes with ResponseCode = "FAILED_SequenceError".

[V2G20-1632] After receiving the SessionStopReq, the SECC shall respond with a SessionStopRes within V2G_SECC_Msg_Performance_Time according to Table 215.

[V2G20-1633] After sending a SessionStopRes, the SECC shall wait at least 5s before closing the TCP connection.

[V2G20-1643] If the first ServiceDiscoveryRes of the service session had the parameter ServiceRenegotiationSupported set to "True", after receiving the SessionStopReq with ChargingSession set to "ServiceRenegotiation" the SECC shall respond with a SessionStopRes with ResponseCode set to "OK" within V2G_SECC_Sequence_Timeout according to Table 215. The next allowed request shall be ServiceDiscoveryReq within V2G_SECC_Sequence_Timeout according to Table 215.

[V2G20-1644] If the first ServiceDiscoveryRes of the service session had the parameter ServiceRenegotiationSupported set to "False", after waking up from a Pause, the SECC shall only offer the ServiceIDs and ParameterSetIDs that were selected by the EVCC in the first ServiceSelectionReq of the service session.

[V2G20-1645] If the first ServiceDiscoveryRes of the service session had the parameter ServiceRenegotiationSupported set to "True", after waking up from a Pause, the SECC shall offer all available services, independent of what the EVCC selected previously.

Details of "WARNING_StandbyNotAllowed" are provided in 8.5.6.2.

8.6.4.6.3.2 AC message flow

[V2G20-1989] After receiving the ScheduleExchangeReq, the SECC shall respond with a ScheduleExchangeRes with EVSEProcessing set to "Finished" within V2G_SECC_Msg_Performance_Time according to Table 215, if the process is finished. The next allowed request shall be PowerDeliveryReq if ServiceName= AC or AC_BPT in Table 204 was selected. The V2G_SECC_Sequence_Timeout is set according to Table 215.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2009] If the PowerDeliveryReq received has ChargeProgress = "Start" and ServiceName = AC or AC_BPT in Table 204 was selected, the next allowed request shall be AC_ChargeLoopReq and the V2G_SECC_Sequence_Timeout is set according to Table 216.

[V2G20-2192] If the PowerDeliveryReq received has ChargeProgress = "Standby" and ServiceName = AC or AC_BPT in Table 204 was selected, the next allowed request shall be AC_ChargeLoopReq and the V2G_SECC_Sequence_Timeout is set according to Table 216.

[V2G20-2012] After receiving the AC_ChargeLoopReq, the SECC shall respond with an AC_ChargeLoopRes with "ResponseCode = OK" within V2G_SECC_Msg_Performance_Time according to Table 215. The next allowed request shall be AC_ChargeLoopReq or PowerDeliveryReq and the V2G_SECC_Sequence_Timeout is set according to Table 216.

[V2G20-1623] If ServiceName = AC or AC_BPT in Table 204 is used, and the PowerDeliveryReq received has ChargeProgress = "Stop", the next allowed request shall be SessionStopReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-1641] The SECC shall be able to set the parameter EVSENotification in EVSEStatus to "ServiceRenegotiation" only in AC_ChargeLoopRes.

[V2G20-1642] If the first ServiceDiscoveryRes of the service session had the parameter ServiceRenegotiationSupported set to "True" and the SECC decides to perform a ServiceRenegotiation for adapting its service offering, it shall set the parameter EVSENotification in EVSEStatus to "ServiceRenegotiation" in AC_ChargeLoopRes.

8.6.4.6.3.3 DC message flow

[V2G20-1611] After receiving the ScheduleExchangeReq, the SECC shall respond with a ScheduleExchangeRes with EVSEProcessing set to "Finished" within V2G_SECC_Msg_Performance_Time according to Table 215, if the process is finished. The next allowed request shall be DC_CableCheckReq if ServiceName= DC or DC_BPT in Table 204 was selected. The V2G_SECC_Sequence_Timeout is set according to Table 217.

[V2G20-2003] After receiving the DC_CableCheckReq, the SECC shall respond with a DC_CableCheckRes with EVSEProcessing set to "Ongoing" within V2G_SECC_Msg_Performance_Time according to Table 217, while the cable check process is still ongoing. The next allowed request shall be DC_CableCheckReq and the V2G_SECC_Sequence_Timeout is set according to Table 217.

[V2G20-2004] After receiving the DC_CableCheckReq, the SECC shall respond with a DC_CableCheckRes with EVSEProcessing set to "Finished" within V2G_SECC_Msg_Performance_Time according to Table 217, if the cable check process is finished. The next allowed request shall be DC_PreChargeReq and the V2G_SECC_Sequence_Timeout is set according to Table 217.

[V2G20-2005] After receiving the DC_PreChargeReq with EVProcessing set to "Ongoing", the SECC shall respond with a DC_PreChargeRes within V2G_SECC_Msg_Performance_Time according to Table 217. The next allowed request shall be DC_PreChargeReq and the V2G_SECC_Sequence_Timeout is set according to Table 217.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2006] After receiving the DC_PreChargeReq with EVProcessing set to "Finished", the SECC shall respond with a DC_PreChargeRes within V2G_SECC_Msg_Performance_Time according to Table 217. The next allowed request shall be PowerDeliveryReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-2010] If the PowerDeliveryReq received has ChargeProgress = "Start" and ServiceName = DC or DC_BPT in Table 204 was selected, the next allowed request shall be DC_ChargeLoopReq and the V2G_SECC_Sequence_Timeout is set according to Table 217.

[V2G20-2013] After receiving the DC_ChargeLoopReq, the SECC shall respond with a DC_ChargeLoopRes with "ResponseCode = OK" within V2G_SECC_Msg_Performance_Time according to Table 217. The next allowed request shall be DC_ChargeLoopReq or PowerDeliveryReq and the V2G_SECC_Sequence_Timeout is set according to Table 217.

[V2G20-2020] If ServiceName = DC or DC_BPT in Table 204 is used, and the PowerDeliveryReq received has ChargeProgress = "Stop", the next allowed request shall be DC_WeldingDetectionReq and the V2G_SECC_Sequence_Timeout is set according to Table 217.

[V2G20-1630] After receiving the DC_WeldingDetectionReq with EVProcessing set to "Ongoing", the SECC shall respond with a DC_WeldingDetectionRes within V2G_SECC_Msg_Performance_Time according to Table 217. The next allowed request shall be DC_WeldingDetectionReq and the V2G_SECC_Sequence_Timeout is set according to Table 217.

[V2G20-1631] After receiving the DC_WeldingDetectionReq with EVProcessing set to "Finished", the SECC shall respond with a DC_WeldingDetectionRes within V2G_SECC_Msg_Performance_Time according to Table 217. The next allowed request shall be SessionStopReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-1598] The SECC shall be able to set the parameter EVSENotification in EVSEStatus to "ServiceRenegotiation" only in DC_ChargeLoopRes.

[V2G20-1599] If the first ServiceDiscoveryRes of the service session had the parameter ServiceRenegotiationSupported set to "True" and the SECC decides to perform a ServiceRenegotiation for adapting its service offering, it shall set the parameter EVSENotification in EVSEStatus to "ServiceRenegotiation" in DC_ChargeLoopRes.

8.6.4.6.3.4 WPT message flow

[V2G20-5043] After receiving a SessionSetupReq, the SECC shall respond with a SessionSetupRes within V2G_SECC_Msg_Performance_Time according to Table 215. If the WPT module is applied, the allowed next request shall be WPT_FinePositioningSetupReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-5085] After receiving a WPT_FinePositioningSetupReq, the SECC shall respond with a WPT_FinePositioningSetupRes within V2G_SECC_Msg_Performance_Time according to Table 218. The allowed next request shall be WPT_FinePositioningReq or WPT_FinePositioningSetupReq and the V2G_SECC_Sequence_Timeout is set according to Table 218.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-5086] After receiving a WPT_FinePositioningReq with EVProcessing set to "Finished", the SECC shall respond with a WPT_FinePositioningRes with EVSEProcessing set to "Finished" within V2G_SECC_Msg_Performance_Time according to Table 218. The next allowed request shall be WPT_PairingReq or WPT_FinePositioningSetupReq and the V2G_SECC_Sequence_Timeout is set according to Table 218.

[V2G20-5087] After receiving a WPT_FinePositioningReq with EVProcessing set to "Ongoing", the SECC shall respond with a WPT_FinePositioningRes with EVSEProcessing set to "Ongoing" within V2G_SECC_Msg_Performance_Time according to Table 218, while the vehicle positioning is still ongoing. The next allowed request shall be WPT_FinePositioningReq and the V2G_SECC_Sequence_Timeout is set according to Table 218.

[V2G20-5088] After receiving a WPT_FinePositioningReq with EVProcessing set to "Ongoing", the SECC shall respond with a WPT_FinePositioningRes with EVSEProcessing set to "Finished" within V2G_SECC_Msg_Performance_Time according to Table 218, when the vehicle positioning has finished. The next allowed request shall be WPT_PairingReq and the V2G_SECC_Sequence_Timeout is set according to Table 218.

[V2G20-5089] After receiving the WPT_PairingReq with EVProcessing set to "Finished", the SECC shall respond with a WPT_PairingRes with EVSEProcessing set to "Finished" within V2G_SECC_Msg_Performance_Time according to Table 215. The next allowed request shall be AuthorizationSetupReq or WPT_FinePositioningSetupReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-5090] After receiving a WPT_PairingReq with EVProcessing set to "Ongoing", the SECC shall respond with a WPT_PairingRes with EVSEProcessing set to "Ongoing" within V2G_SECC_Msg_Performance_Time according to Table 218, while the pairing process is still ongoing. The next allowed request shall be WPT_PairingReq and the V2G_SECC_Sequence_Timeout is set according to Table 218.

[V2G20-5091] After receiving a WPT_PairingReq, the SECC shall respond with a WPT_PairingRes with EVSEProcessing set to "Finished" within V2G_SECC_Msg_Performance_Time according to Table 218, when the pairing process has finished (see also [V2G20-5018]). The next allowed request shall be AuthorizationSetupReq or WPT_FinePositioningSetupReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-5044] After receiving the ScheduleExchangeReq, the SECC shall respond with a ScheduleExchangeRes within V2G_SECC_Msg_Performance_Time according to Table 215. If EVSEProcessing was set to "Finished", the next allowed request shall be WPT_AlignmentCheckReq or WPT_FinePositioningSetupReq if ServiceName= WPT in Table 204 was selected. The V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-5092] After receiving a WPT_AlignmentCheckReq, the SECC shall respond with a WPT_AlignmentCheckRes with EVSEProcessing set to "Finished" within V2G_SECC_Msg_Performance_Time according to Table 218, if the alignment process is finished. The next allowed request shall be PowerDeliveryReq or WPT_FinePositioningSetupReq. The V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-5093] After receiving a WPT_AlignmentCheckReq, the SECC shall respond with a WPT_AlignmentCheckRes with EVSEProcessing set to "Ongoing" within V2G_SECC_Msg_Performance_Time according to Table 218, if the alignment process

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

is still ongoing. The next allowed request shall be WPT_AlignmentCheckReq. The V2G_SECC_Sequence_Timeout is set according to Table 218.

[V2G20-5123] If the PowerDeliveryReq received has ChargeProgress = "Start" and ServiceName = WPT in Table 204 was selected, the next allowed request shall be WPT_ChargeLoopReq or WPT_FinePositioningSetupReq and the V2G_SECC_Sequence_Timeout is set according to Table 218.

[V2G20-5124] After receiving the WPT_ChargeLoopReq, the SECC shall respond with a WPT_ChargeLoopRes with "ResponseCode = OK" within V2G_SECC_Msg_Performance_Time according to Table 218. The next allowed request shall be WPT_ChargeLoopReq or PowerDeliveryReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-5094] If the PowerDeliveryReq received has ChargeProgress = "Stop", and ServiceName = WPT in Table 204, the next allowed request shall be SessionStopReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-5095] The SECC shall be able to set the parameter EVSENotification in EVSEStatus to "ServiceRenegotiation" only in WPT_ChargeLoopRes.

[V2G20-5096] If the first ServiceDiscoveryRes of the service session had the parameter ServiceRenegotiationSupported set to "True" and the SECC decides to perform a ServiceRenegotiation for adapting its service offering, it shall set the parameter EVSENotification in EVSEStatus to "ServiceRenegotiation" in WPT_ChargeLoopRes.

8.6.4.6.3.5 ACDP message flow

NOTE 1 The common requirements [V2G20-1483] and [V2G20-1484] apply.

[V2G20-4067] After receiving a SessionSetupReq, the SECC shall respond with a SessionSetupRes within V2G_SECC_Msg_Performance_Time according to Table 215. If the SECC is using "WLAN", the allowed next request shall be ACDP_VehiclePositioningReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-4068] If SECC is using ServiceName = DC_ACDP, after receiving the ACDP_VehiclePositioningReq, the SECC shall respond with a ACDP_VehiclePositioningRes with EVSEProcessing set to "Ongoing" within V2G_SECC_Msg_Performance_Time according to Table 215, while the vehicle positioning is still ongoing. The next allowed request shall be ACDP_VehiclePositioningReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-4069] After receiving a ACDP_VehiclePositioningReq with EVMobilityStatus set to "EV is immobilized", the SECC shall respond with a ACDP_VehiclePositioningRes with EVSEProcessing set to "Finished" within V2G_SECC_Msg_Performance_Time according to Table 215. The next allowed request shall be AuthorizationSetupReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

NOTE 2 The common requirements apply [V2G20-1971], [V2G20-1970], [V2G20-1975], [V2G20-1973], [V2G20-1976], [V2G20-1972], [V2G20-1977], [V2G20-1978], [V2G20-1979], [V2G20-1980], [V2G20-1981], [V2G20-1983] and [V2G20-1986].

[V2G20-4070] After receiving the ScheduleExchangeReq, the SECC shall respond with a ScheduleExchangeRes with EVSEProcessing set to "Finished" within

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

V2G_SECC_Msg_Performance_Time according to Table 196, if the charge parameter discovery process is finished. The next allowed request shall be ACDP_ConnectReq if ServiceName= DC_ACDP, in Table 204 was selected. The V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-4071] If SECC is using ServiceName = DC_ACDP, after receiving the ACDP_ConnectReq, the SECC shall respond with a ACDP_ConnectRes with EVSEProcessing set to "Ongoing" within V2G_SECC_Msg_Performance_Time according to Table 215 while the device connection is still ongoing. The next allowed request shall be ACDP_ConnectReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-4072] If SECC is using ServiceName = DC_ACDP, after receiving the ACDP_ConnectReq, the SECC shall respond with a ACDP_ConnectRes with EVSEProcessing set to "Finished" within V2G_SECC_Msg_Performance_Time according to Table 215, when the device connection has finished. The next allowed request shall be DC_CableCheckReq if ServiceName = DC_ACDP or DC_ACDP_BPT in Table 204 was selected and the V2G_SECC_Sequence_Timeout is set according to Table 215.

NOTE 3 The following DC requirements apply [V2G20-2003], [V2G20-2004], [V2G20-2005], [V2G20-2006], [V2G20-2007] (common), [V2G20-2008] (common), [V2G20-2013] and [V2G20-919].

NOTE 4 The general requirement [V2G20-1959] applies for an EVSE initiated stop.

[V2G20-4073] If SECC is using ServiceName = DC_ACDP in Table 204, after receiving the PowerDeliveryReq with ChargeProgress set to "Stop", the SECC shall respond with PowerDeliveryRes containing "ResponseCode=OK" within V2G_SECC_Msg_Performance_Time according to Table 215. The allowed next request shall be ACDP_DisconnectReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-4074] After receiving the ACDP_DisconnectReq, the SECC shall respond with ACDP_DisconnectRes containing "ResponseCode = OK" and "EVSEProcessing=Ongoing" within V2G_SECC_Msg_Performance_Time according to Table 215, if the processing of the information is successfully passed and the ACDP_Disconnect is ongoing. The allowed next request shall be ACDP_DisconnectReq and the V2G_SECC_Sequence_Timeout is set according to Table 215.

[V2G20-4075] After receiving the ACDP_DisconnectReq, the SECC shall respond with ACDP_DisconnectRes containing "ResponseCode = OK" and "EVSEProcessing=Finished" within V2G_SECC_Msg_Performance_Time according to Table 215, if the charging device is in the home position as defined in IEC 61851-23-1. The allowed next request shall be SessionStopReq and V2G_SECC_Sequence_Timeout is set according to Table 215.

NOTE 5 The common requirements [V2G20-1632] and [V2G20-1633] apply.

8.6.5 Multiplexed communication

Besides the regular main stream message flow with EXI encoded V2GTP payload types in the range 0x8001 up to 0x80FF, a multiplexed communication is enabled by making use of other V2GTP payload types (schedule renegotiation V2G messages, ACDP_SystemStatus messages, MeteringConfirmation Messages, ParkingStatus messages (see Table 14)). This subclause refers to communication using EXI encoded messages with V2GTP payload type in the range 0x8101 up to 0x81FF as the side stream.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

For example, while in the message exchange loop of AC_ChargeLoopReq/Res, if either the EVCC or the SECC would like to change the EVPowerProfile, they can trigger a schedule renegotiation without interruption of the existing energy transfer message exchange. The schedule renegotiation is done in a parallel side stream with V2GTP payload type ScheduleRenegotiationPayloadID. Refer to Annex F for the message sequence on EVCC triggered and SECC triggered schedule renegotiation.

[V2G20-1040] The conditions defined for the CP state and PWM within the message sequence requirements shall only apply to the main stream EXI encoded messages with V2GTP payload types in the range 0x8001 up to 0x80FF.

[V2G20-1041] The timeout of the messages in the side stream shall be independent of the timeout of the messages in the main stream.

[V2G20-1042] All timeout requirements that apply for the main stream shall be accordingly applied for the side stream messages.

[V2G20-1043] If SessionStopRes with ResponseCode set to "OK" is encountered, then all communication shall terminate.

8.6.5.1 Schedule Renegotiation

[V2G20-1045] For all schedule renegotiation related messages, V2GTP payload type ScheduleRenegotiationPayloadID shall be applied.

The following requirements apply to EVCC triggered schedule renegotiation.

[V2G20-1046] The EVCC shall use the message ChargeParameterDiscoveryReq on V2GTP payload type ScheduleRenegotiationPayloadID as the first message of a schedule renegotiation message flow.

[V2G20-1846] The EVCC shall send ChargeParameterDiscoveryReq on V2GTP payload type ScheduleRenegotiationPayloadID only after having sent at least one ChargeLoopReq message depending on the selected energy transfer services.

[V2G20-1047] The SECC shall respond to the ChargeParameterDiscoveryReq with ChargeParameterDiscoveryRes on V2GTP payload type ScheduleRenegotiationPayloadID V2G messages.

[V2G20-1048] After receiving the ChargeParameterDiscoveryRes, the EVCC shall send a ScheduleExchangeReq on V2GTP payload type ScheduleRenegotiationPayloadID.

[V2G20-2316] If the SECC needs more time to provide the PowerSchedule and optionally a PriceSchedule, the SECC shall respond to the ScheduleExchangeReq with ScheduleExchangeRes with EVSEProcessing set to "Ongoing" on V2GTP payload type ScheduleRenegotiationPayloadID.

[V2G20-2713] If the SECC is ready to provide the PowerSchedule and optionally a PriceSchedule, the SECC shall respond to the ScheduleExchangeReq with ScheduleExchangeRes with EVSEProcessing set to "Finished" on V2GTP payload type ScheduleRenegotiationPayloadID.

[V2G20-2714] After receiving the ScheduleExchangeRes with EVSEProcessing set to "Ongoing", the EVCC shall send another unaltered ScheduleExchangeReq on V2GTP payload type ScheduleRenegotiationPayloadID.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2317] After receiving the ScheduleExchangeRes with EVSEProcessing set to "Finished", the EVCC shall send a PowerDeliveryReq on V2GTP payload type ScheduleRenegotiationPayloadID with EVPowerProfile based on the ScheduleList in the response received from SECC.

[V2G20-1049] To exit the schedule renegotiation process, the SECC shall send a PowerDeliveryRes on V2GTP payload type ScheduleRenegotiationPayloadID with ResponseCode = OK.

NOTE 1 After the PowerDeliveryRes on V2GTP payload type ScheduleRenegotiationPayloadID with ResponseCode = OK, no further message exchange on V2GTP payload type ScheduleRenegotiationPayloadID is expected for this schedule renegotiation session.

[V2G20-1050] The new EVPowerProfile as a result from the schedule renegotiation session shall be applied in the next ChargeLoopReq on the mainstream communication channel.

NOTE 2 During schedule renegotiation, the SECC can use EVSETargetActivePower (phase specific if necessary) in the ChargeLoopRes on the mainstream communication channel to limit the power drawn by the EVCC temporarily.

[V2G20-1051] During schedule renegotiation according to [V2G20-1045] the EVCC shall maintain the charging behavior based on [V2G20-1825].

The following requirements apply to SECC triggered schedule renegotiation.

[V2G20-1845] When the SECC wants to trigger a schedule renegotiation, it shall set the parameter EVSENotification to ScheduleRenegotiation in ChargeLoopRes on the mainstream communication channel.

[V2G20-1052] When the EVCC received a message where the EVSENotification is set to ScheduleRenegotiation, it shall send a ChargeParameterDiscoveryReq within the number of seconds provided in NotificationMaxDelay with updated parameters based on the current situation on V2GTP payload type ScheduleRenegotiationPayloadID.

[V2G20-2235] If a schedule renegotiation has not completed successfully within the ScheduleRenegotiationPayloadID sidestream, then the SECC shall decide if it wants to abort or retry the schedule renegotiation. If the SECC wants to retry the schedule renegotiation it shall restart the process according to [V2G20-1845] and set the ResponseCode of the ChargeLoopRes to WARNING_ScheduleRenegotiationFailed. If the following schedule renegotiation fails to complete again, then the SECC is allowed to escalate by setting the ResponseCode of the ChargeLoopRes to FAILED_ScheduleRenegotiation and to terminate the charging session (see 8.8.2 on general FAILED behavior).

[V2G20-1053] Requirements [V2G20-1047], [V2G20-1048], [V2G20-1049] and [V2G20-1050] shall apply as subsequent steps.

8.6.5.2 Metering confirmation

For more information, see at 8.3.4.3.11.1.

8.6.5.3 Parking status

Parking status is applied to the EV arriving to the parking area or leaving from there. It will be used by an EV to inform the EVSE either about its arrival and exchange necessary information for guidance to a

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

 © ISO 2022 – All rights reserved

free/reserved parking area, or about its departure that the occupied parking area is now changed to vacant and available to another vehicle. Detailed specifications are provided in Table 14 and 8.4.3.2.7.

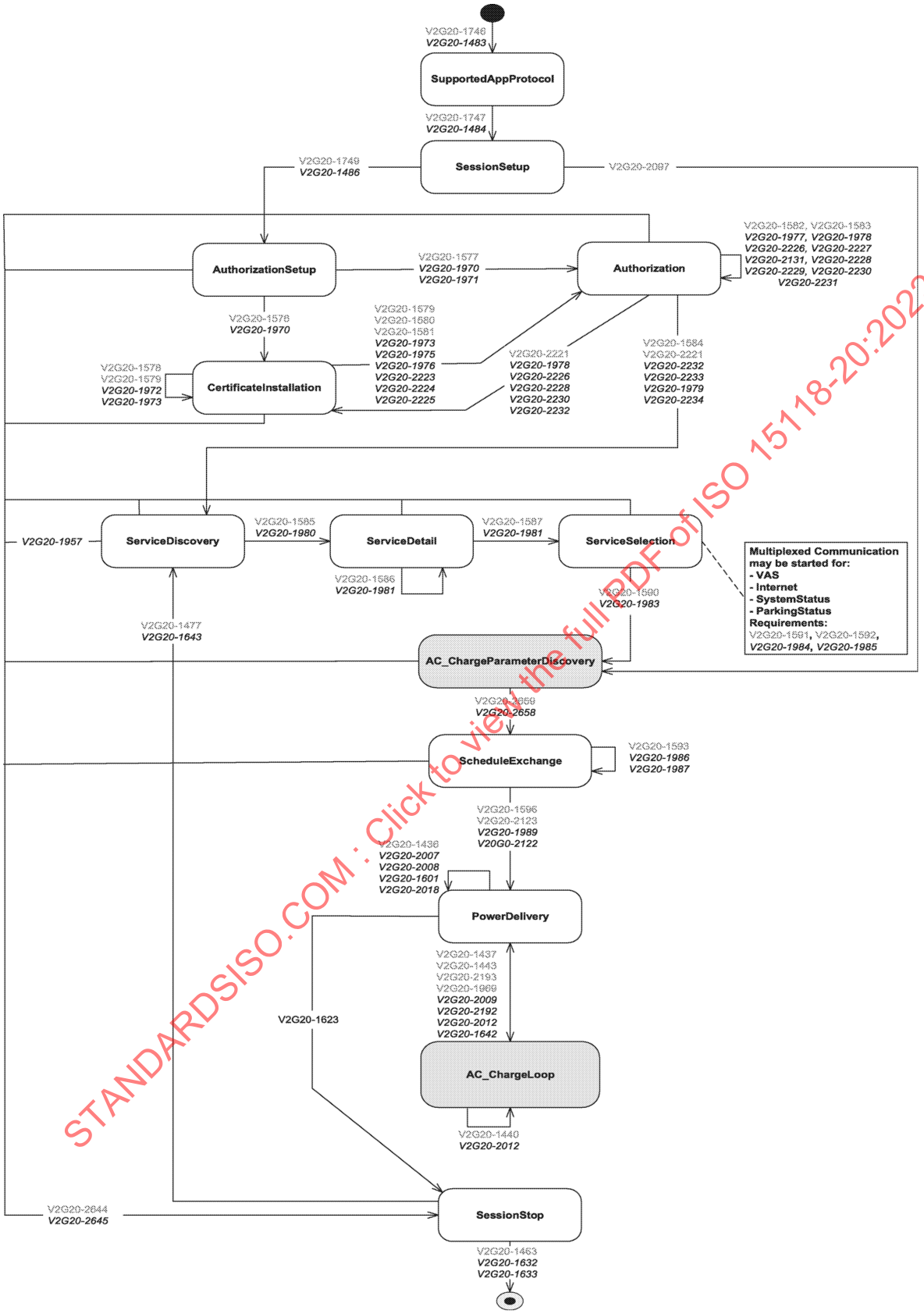
[V2G20-1054] For all messages related to parking assistance service, V2GTP payload type ParkingStatusPayloadID shall be applied.

8.6.6 Message sequence diagrams

Figure 215 shows the AC message sequence diagram.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Key

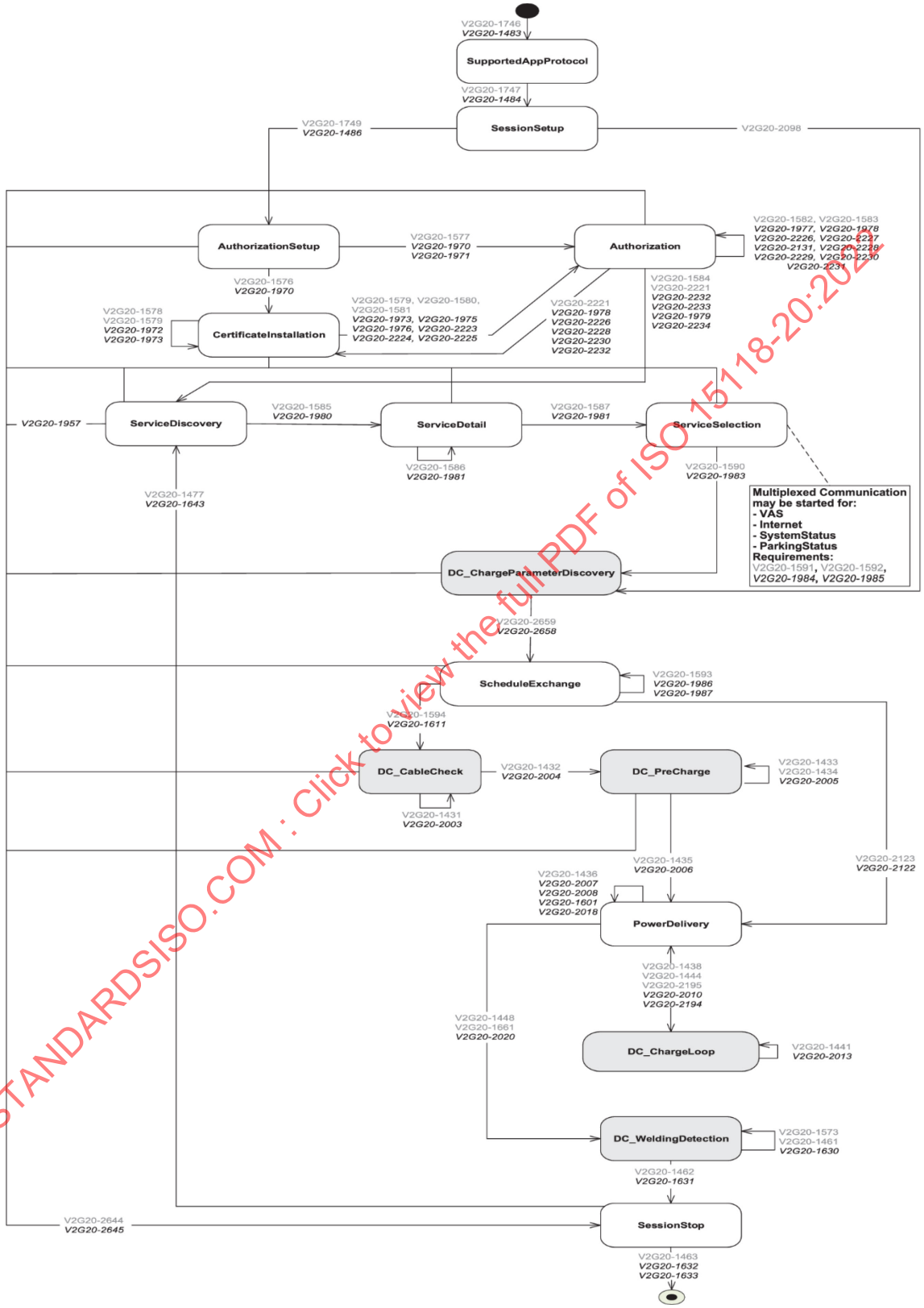
Text EVCC

Text SECC

Figure 215 — AC message sequence diagram

© ISO 2022 – All rights reserved

Figure 216 shows the DC message sequence diagram.



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Key

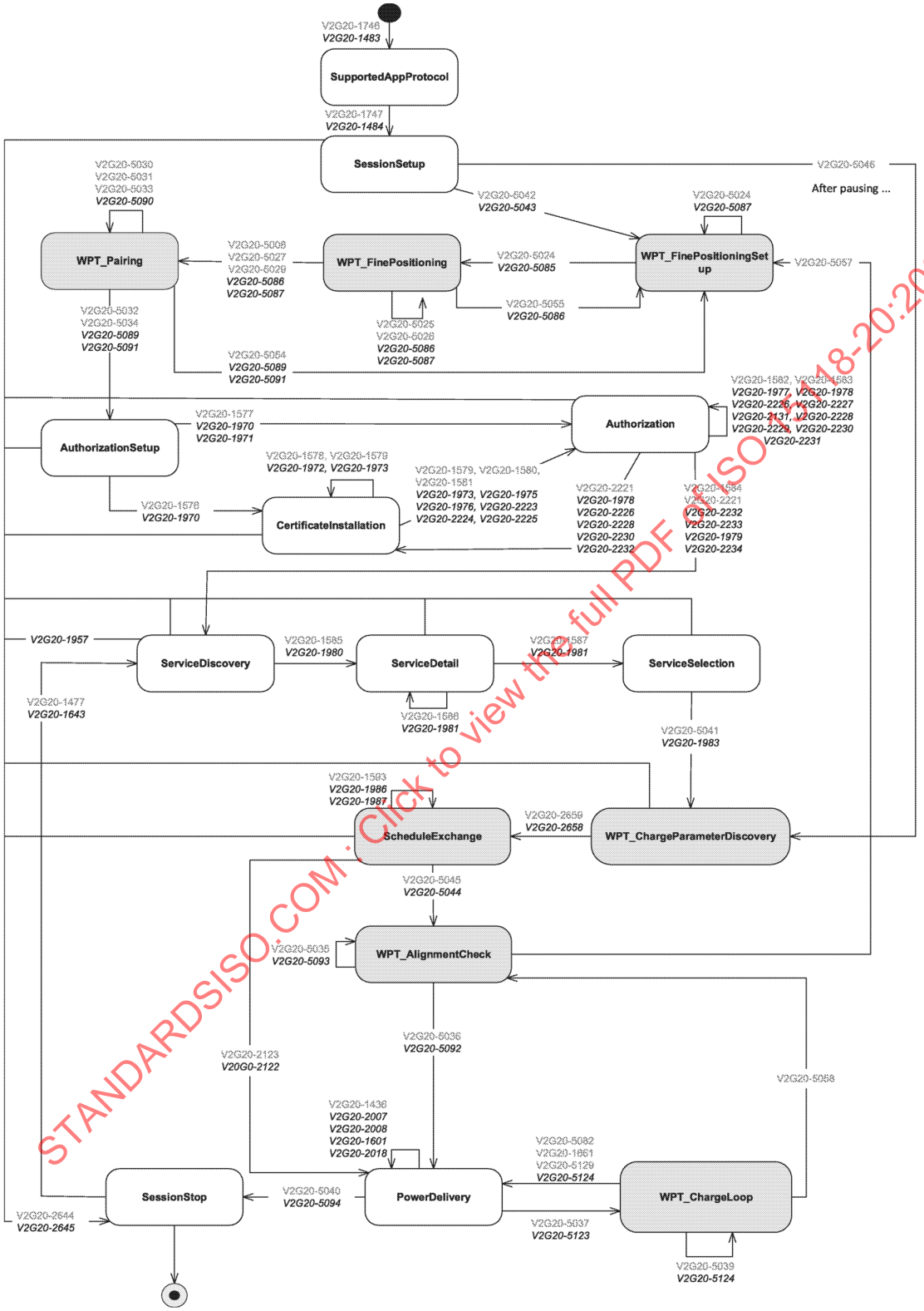
Text EVCC

Text SECC

Figure 216 — DC message sequence diagram

© ISO 2022 – All rights reserved

Figure 217 shows the WPT message sequence diagram.



Key

Text EVCC

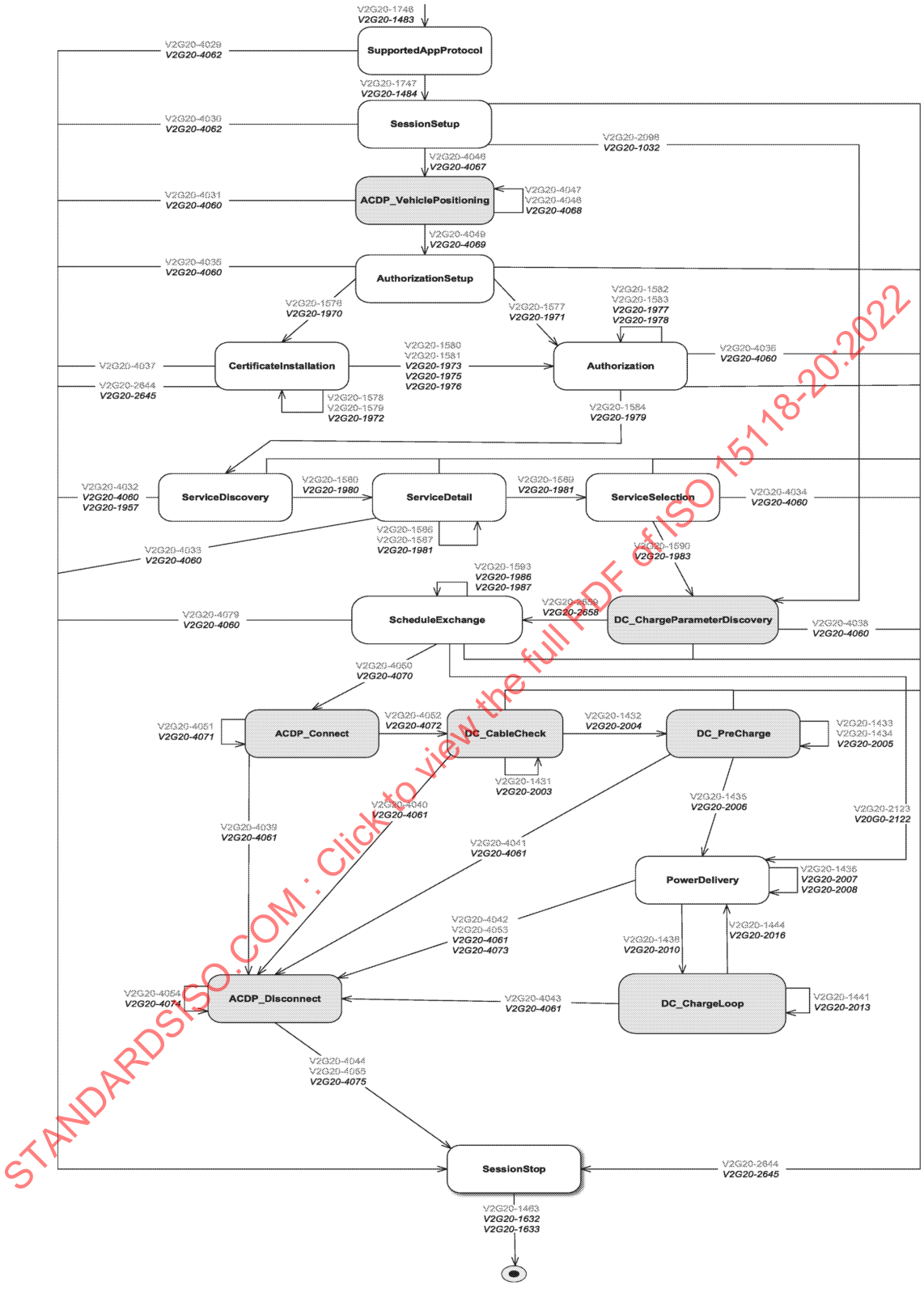
Text SECC

Figure 217 — WPT message sequence diagram

Figure 218 shows the ACDP message sequence diagram.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved



STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

Key

Text EVCC

Text SECC

Figure 218 — ACDP message sequence diagram

© ISO 2022 – All rights reserved

Annex A
(normative)

Schema definition

The V2G application layer message specification consists of the following XML Schema documents with the following scope:

– "V2G_CI_AppProtocol": defines the protocol handshake (SAP) messages. The XSD file can be downloaded from:
https://standards.iso.org/iso/15118/-20/ed-1/en/V2G_CI_AppProtocol.xsd;

– "V2G_CI_CommonTypes": defines the common types used by all defined messages (except SAP). The XSD file can be downloaded from:
https://standards.iso.org/iso/15118/-20/ed-1/en/V2G_CI_CommonTypes.xsd;

– "V2G_CI_CommonMessages": defines the common messages that are not specific to any energy transfer mode. The XSD file can be downloaded from:
https://standards.iso.org/iso/15118/-20/ed-1/en/V2G_CI_CommonMessages.xsd;

– "V2G_CI_AC": defines the messages exclusively used for AC charging. The XSD file can be downloaded from:
https://standards.iso.org/iso/15118/-20/ed-1/en/V2G_CI_AC.xsd;

– "V2G_CI_DC": defines the messages exclusively used for DC charging. The XSD file can be downloaded from:
https://standards.iso.org/iso/15118/-20/ed-1/en/V2G_CI_DC.xsd;

– "V2G_CI_ACDP": defines the messages exclusively used for ACDP. The XSD file can be downloaded from:
https://standards.iso.org/iso/15118/-20/ed-1/en/V2G_CI_ACDP.xsd;

– "V2G_CI_WPT": defines the messages exclusively used for WPT. The XSD file can be downloaded from:
https://standards.iso.org/iso/15118/-20/ed-1/en/V2G_CI_WPT.xsd;

– "xmldsig-core-schema": defines the W3C schema for XML signatures. The XSD file can be downloaded from:
https://standards.iso.org/iso/15118/-20/ed-1/en/xmldsig-core-schema.xsd.

Figure A.1 shows the dependency graph for all five XML schema documents.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

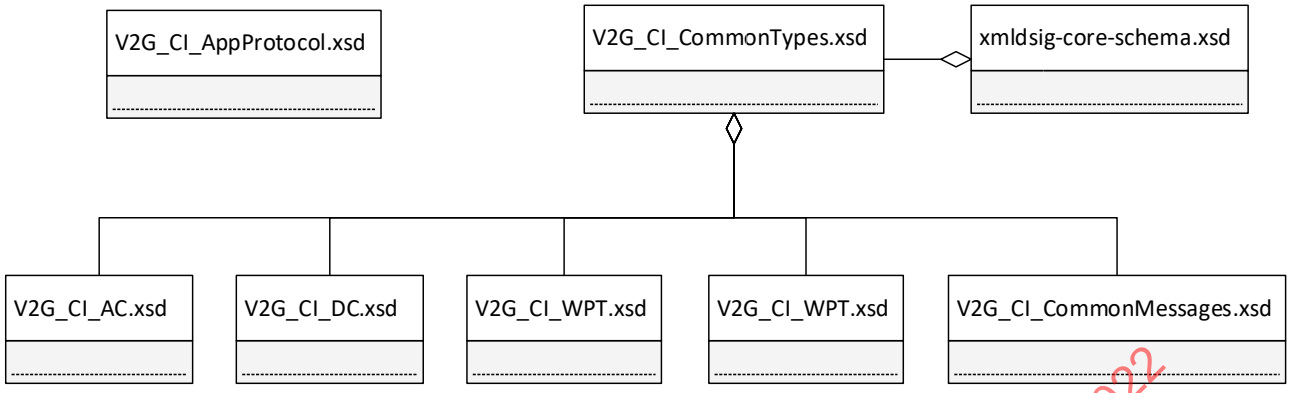


Figure A.1 — Dependency chart of the V2G CI XML schema definitions

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

Annex B
(normative)

Certificate profiles

B.1 Overview

Certificate profiles are presented in tables, divided into several thematic clusters each containing profiles for specific certificate types. Certificate profiles are based on ITU-T X.509 and IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399).

Tables B.x (like Table B.3, Table B.5, Table B.7, Table B.9, Table B.11, Table B.13, Table B.15 or Table B.17) provide certificate profiles for certificates based on the curve as defined by [V2G20-2674].

Tables B.y (like Table B.4, Table B.6, Table B.8, Table B.10, Table B.12, Table B.14, Table B.16 or Table B.18) provide certificate profiles for certificates based on the curve as defined by [V2G20-2319].

A cell's content in the certificate profiles in Table B.1 have the following meaning.

Table B.1 — Certificate profile cell content meaning

Cell content	Description
x	Required/mandatory – Issuing CA ensures that this extension is present. – Certificate validating entity ensures that this extension is present.
(x)	Optional – It is up to the discretion of the issuing CA and/or certificate requester to either include or omit this extension. – Certificate validating entity ignores the absence of this extension.
-	Should not be present – Issuing CA ensures that this extension is not present. – Certificate validating entity ensures that this extension is not present.
c	This extension is **critical** see IETF RFC 5280 – If this extension is present, the certificate validating entity processes it. If an implementation recognizes that a "critical" extension is present, but the implementation cannot interpret the extension, the implementation rejects the certificate. Quote from IETF RFC 5280: "A certificate-using system rejects the certificate if it encounters a critical extension it does not recognize or a critical extension that contains information that it cannot process." NOTE IETF RFC 5280 has been updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399. These updates are considered to be included in this document.
nc	This extension is **non-critical**, see IETF RFC 5280 – If this extension is present, the certificate validating entity may ignore it if the entity is unable to process the extension. If an implementation recognizes that a "non-critical" extension is present, but the implementation cannot interpret the extension, the extension can be ignored. Quote from IETF RFC 5280: "A non-critical extension MAY be ignored if it is not recognized, but is processed if it is recognized." NOTE IETF RFC 5280 has been updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399. These updates are considered to be included in this document.
( )	For "(x)": – See above For cases other than "(x)": Details of the parameter

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[ ]	CA discretionary detail
" "	Exact string value that the parameter shall be set to
Number	Exact numerical value that the parameter shall be set to (could be real number or dot notation of the OID according to IETF RFC 6712)
String starting with "id-"	OID value (if permitted by applicable RFCs, dot notation of the OID (see IETF RFC 6712) may be used instead of the string value)
PCID	Provisioning certificate ID (see [V2G20-1780])
SECCID	Supply equipment communication controller ID (see [V2G20-2583])
EVCCID	Electric vehicle communication controller ID (see [V2G20-2597])
PEID	Private environment ID (ID as assigned by PE operator to uniquely identify the particular private SECC in a particular private operation) (see [V2G20-2697])

NOTE 1 The following OIDs apply (ASN.1 notation):

- { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 }
- { iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) 1 }
- { iso(1) identified-organization(3) certicom(132) curve(0) 35 }
- { iso(1) identified-organization(3) thawte(101) id-EdDSA448(113) }
- { iso(1) identified-organization(3) thawte(101) id-X448(111) }
- { joint-iso-itu-t(2) ds(5) certificateExtension(29) authorityKeyIdentifier(35) }
- { joint-iso-itu-t(2) ds(5) certificateExtension(29) subjectKeyIdentifier(14) }
- { joint-iso-itu-t(2) ds(5) certificateExtension(29) keyUsage(15) }
- { joint-iso-itu-t(2) ds(5) certificateExtension(29) extKeyUsage(37) }
- { joint-iso-itu-t(2) ds(5) certificateExtension(29) basicConstraints(19) }
- { joint-iso-itu-t(2) ds(5) certificateExtension(29) cRLDistributionPoints(31) }
- { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) pe(1) authorityInfoAccess(1) }
- { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) pe(1) subjectInfoAccess(11) }
- { iso(1) standard(0) 15118 part20(20) extensions(0) contractOperatorName(1) }
- { iso(1) standard(0) 15118 part20(20) extensions(0) contractTariffName(2) }
- { iso(1) standard(0) 15118 part20(20) extensions(0) contractDynamicInformationUrl(3) }
- { iso(1) standard(0) 15118 part20(20) extensions(0) tpmStorageKey(4) }
- { iso(1) standard(0) 15118 part20(20) extensions(0) tpmPolicyDigest(5) }
- { iso(1) standard(0) 15118 part20(20) extensions(0) crossCertIndication(6) }
- { joint-iso-itu-t(2) ds(5) certificateExtension(29) id-ce-subjectAltPublicKeyInfo(72) }
- { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) kp(3) id-kp-serverAuth(1) }
- { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) kp(3) id-kp-clientAuth(2) }
- { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) kp(3) id-kp-OCSPSigning(9) }
- { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) ocsp(1) }

NOTE 2 The online certificate status protocol (OCSP), defined in IETF RFC 6960 (as updated IETF RFC 8954) is a protocol used for obtaining the revocation status of an X.509 certificate. OCSP is an alternative to certificate revocation lists (CRL), OCSP is an online service. This means, that a backend infrastructure supports OCSP services in order to be able to use that service.

NOTE 3 Refer to ITU-T X.680 for details of ASN.1 notation.

When the certificate status is provided via OCSP services, id-pe-authorityInfoAccess OID is used within the AuthorityInfoAccess extension. The OID repository [99] also refers to id-pe-authorityInfoAccess as authorityInfoAccess(1) (see NOTE 1 above providing the OID value for id-pe-authorityInfoAccess).

Within a x.509 certificate, the id-ad-ocsp OID is used within the AuthorityInfoAccess extension as accessMethod if revocation information for the certificate containing this extension is available using the online certificate status protocol (OCSP). When id-ad-ocsp appears as accessMethod, the accessLocation

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

field is the location of the OCSP responder, using the conventions defined IETF RFC 6960 as updated IETF RFC 8954.

id-ad-ocsp is also known as id-pkix-ocsp. The OID repository [99] also refers to id-ad-ocsp as ocsp(1) (see NOTE 1 in this subclause providing the OID value for id-ad-ocsp).

If the certificate status is provided via a certificate revocation list (CRL), id-ce-cRLDistributionPoints OID is used within the CRLDistributionPoints extension. The OID repository [99] also refers to id-ce-cRLDistributionPoints as cRLDistributionPoints(31) (see NOTE 1 in this subclause providing the OID value for id-ce-cRLDistributionPoints).

The OID for "ecdsa-with-SHA512" is defined as { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 } in ASN.1 notation (refer to ITU-T X.680 for details of ASN.1 notation).

The OID for "id-ecPublicKey" is defined as { iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) 1 } in ASN.1 notation (refer to ITU-T X.680 for details of ASN.1 notation).

The OID for "secp521r1" is defined as { iso(1) identified-organization(3) certicom(132) curve(0) 35 } in ASN.1 notation (refer to ITU-T X.680 for details of ASN.1 notation).

When subject information access is provided, id-pe-subjectInfoAccess OID is used within the subjectInfoAccess extension. The OID repository [99] also refers to id-pe-subjectInfoAccess as subjectInfoAccess(11) (see NOTE 1 in this subclause providing the OID value for id-pe-subjectInfoAccess).

The OID repository [99] provides the EdDSA448 algorithm identifier as id-EdDSA448 while the IETF RFC 8410 provides the identifier as id-Ed448. Both OID values are actually same and as such these identifiers can be used interchangeably (see NOTE 1 in this subclause providing the OID value for id-EdDSA448).

The OID repository [99] also refers to id-ce-authorityKeyIdentifier as authorityKeyIdentifier(35) (see NOTE 1 in this subclause providing the OID value for id-ce-authorityKeyIdentifier).

The OID repository [99] also refers to id-ce-subjectKeyIdentifier as subjectKeyIdentifier(14) (see NOTE 1 in this subclause providing the OID value for id-ce-subjectKeyIdentifier).

The OID repository [99] also refers to id-ce-keyUsage as keyUsage(15) (see NOTE 1 in this subclause providing the OID value for id-ce-keyUsage).

The OID repository [99] also refers to id-ce-basicConstraints as basicConstraints(19) (see NOTE 1 in this subclause providing the OID value for id-ce-basicConstraints).

The OID repository [99] also refers to id-ce-extKeyUsage as extKeyUsage(37) (see NOTE 1 in this subclause providing the OID value for id-ce-extKeyUsage).

The OID repository [99] also refers to id-contractOperatorName as contractOperatorName(1) (see NOTE 1 in this subclause providing the OID value for id-contractOperatorName).

The OID repository [99] also refers to id-contractTariffName as contractTariffName(2) (see NOTE 1 in this subclause providing the OID value for id-contractTariffName).

The OID repository [99] also refers to id-contractDynamicInformationUrl as contractDynamicInformationUrl(3) (see NOTE 1 in this subclause providing the OID value for id-contractDynamicInformationUrl).

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

The OID repository [99] also refers to id-tpmStorageKey as tpmStorageKey(4) (see NOTE 1 in this subclause providing the OID value for id-tpmStorageKey).

The OID repository [99] also refers to id-tpmPolicyDigest as tpmPolicyDigest(5) (see NOTE 1 in this subclause providing the OID value for id-tpmPolicyDigest).

The OID repository [99] also refers to id-crossCertIndication as crossCertIndication(6) (see NOTE 1 in this subclause providing the OID value for id-crossCertIndication).

GeneralizedTime in Greenwich Mean Time (GMT) is utilized for certificate validity purposes as some of the certificates can have expiration date beyond year 2049 as, per ITU-T X.509 [and IETF RFC 5280 (as updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399)], Coordinated Universal Time (UTC) based time can only be used in certificates that expire before year 2050.

It should be noted that although the certificate validity of each certificate type will be as per the definition in this annex, the certificate validity remaining at the time of V2G entity production or deployment may be less than the requirements as specified in this annex. This is because the certificate may have been generated long before the V2G entity was produced and/or deployed.

Furthermore, the certificate validity is not directly related to the date of issuance of a certificate, but is rather tied to "notBefore" and "notAfter" fields of the certificate.

For example, if a V2G root CA certificate has a "notBefore" field of 20100301180000Z (March 1 18:00:00 2010 GMT) and a "notAfter" field of 203503011759597 (March 1 17:59:59 2035 GMT), this results in a validity of 25 years. If a vehicle manufactured in March 2020 uses that V2G root CA certificate, that root certificate will only have 15 more years of validity left before the certificate expires.

B.2 General

This subclause applies to all certificate types and profiles.

[V2G20-2685] Any extension or field/parameter/attribute/data type (or sub-field/sub-parameter/sub-attribute/sub-data type or sub-sub-field/sub-sub-parameter/sub-sub-attribute/sub-sub-data type or etc.) not defined in the certificate profiles defined by this document shall not be included in any certificate conforming to this document.

Per ITU-T X.509 and IETF RFC 5280 as updated by updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399), some fields/parameters/attributes/data types (or sub-fields/sub-parameters/sub-attributes/sub-data types or sub-sub-fields/sub-sub-parameters/sub-sub-attributes/sub-sub-data types or etc.) can take multiple sub-fields/sub-parameters/sub-attributes/sub-data types (or sub-sub-fields/sub-sub-parameters/sub-sub-attributes/sub-sub-data types or etc.). Certificate profiles defined by this annex limit the number of sub-fields/sub-parameters/sub-attributes/sub-data types (or sub-sub-fields/sub-sub-parameters/sub-sub-attributes/sub-sub-data types or etc.) to as defined by this document.

Per ITU-T X.509 and IETF RFC 5280 (as updated by updated by IETF RFC 6818, IETF RFC 8398 and IETF RFC 8399), some fields/parameters/attributes/data types (or sub-fields/sub-parameters/sub-attributes/sub-data types or sub-sub-fields/sub-sub-parameters/sub-sub-attributes/sub-sub-data types or etc.) can take a sequence of sub-fields/sub-parameters/sub-attributes/sub-data types (or a sequence of sub-sub-fields/sub-sub-parameters/sub-sub-attributes/sub-sub-data types or etc.). Certificate profiles defined by this annex limit the number of sequences of sub-fields/sub-parameters/sub-attributes/sub-data types (or sub-sub-fields/sub-sub-parameters/sub-sub-attributes/sub-sub-data types or etc.) to as defined by this document.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved

[V2G20-2686] The relying party shall reject any certificate that contains an extension or field/parameter/attribute/data type not defined in the certificate profile for that certificate type in this document.

B.2.1 Mandatory versus optional

The certificate profiles defined below mark some fields/parameters/attributes/data types as optional while other fields/parameters/attributes/data types in that certificate profile are marked as mandatory/required to be supported.

[V2G20-2687] All mandatory/required fields/parameters/attributes/data types shall be included in a certificate conforming to a particular certificate profile.

[V2G20-2688] Any optional fields/parameters/attributes/data types may or may not be included in the certificate at the CA's discretion, unless specified otherwise by the requirements in this document.

If a certificate requester needs any of these optional fields/parameters/attributes/data types to be included, the requester will need to work with its CA to include those fields/parameters/attributes/data types in the certificate chain. It is out of the scope of this document to define the methodologies for the certificate requester to indicate to the CA whether a particular optional field/parameter/attribute/data type should be included or not.

A field/parameter/attribute/data type in the certificate could contain sub-fields/sub-parameters/sub-attributes/sub-data types. These sub-fields/sub-parameters/sub-attributes/sub-data types are indented within the field/parameter/attribute/data type in the certificate profiles defined below.

[V2G20-2689] All mandatory/required sub-fields/sub-parameters/sub-attributes/sub-data types shall be included in a mandatory/required field/parameter/attribute/data type within a certificate conforming to a particular certificate profile.

[V2G20-2690] Unless specified otherwise by the requirements in this document, at the CA's discretion, any optional sub-fields/sub-parameters/sub-attributes/sub-data types may or may not be included in a mandatory/required field/parameter/attribute/data type within a certificate conforming to a particular certificate profile.

If a certificate requester needs any of these optional sub-fields/sub-parameters/sub-attributes/sub-data types to be included, the requester will need to work with its CA to include those sub-fields/sub-parameters/sub-attributes/sub-data types in the certificate chain. It is out of the scope of this document to define the methodologies for the certificate requester to indicate to the CA whether a particular optional sub-field/sub-parameter/sub-attribute/sub-data type should be included or not.

Some of the optional fields/parameters/attributes/data types contain sub-fields/sub-parameters/sub-attributes/sub-data types which may then be individually marked as mandatory/required to be supported in that certificate profile while other sub-fields/sub-parameters/sub-attributes/sub-data types contained within that field/parameter/attribute/data type may be marked as optional to be supported in that certificate profile.

[V2G20-2691] If the optional field/parameter/attribute/data type is omitted, then all sub-fields/sub-parameters/sub-attributes/sub-data types included in that field/parameter/attribute/data type shall also be omitted from the certificate conforming to that particular certificate profile. This shall be done whether a particular sub-field/sub-parameter/sub-attribute/sub-data type is indicated as mandatory or optional in the certificate profile.

STANDARDSISO.COM : Click to view the full PDF of ISO 15118-20:2022

© ISO 2022 – All rights reserved