
**Intelligent transport systems —
Communication profiles for secure
connections between trusted devices**

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 21185:2019



STANDARDSISO.COM : Click to view the full PDF of ISO/TS 21185:2019



COPYRIGHT PROTECTED DOCUMENT

© ISO 2019

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
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword.....	iv
Introduction.....	v
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions.....	1
4 Symbols and abbreviated terms.....	2
5 OID conventions.....	2
6 Architecture.....	3
7 Communication profiles and protocol stacks — Overview.....	3
7.1 Definitions and methodology.....	3
7.2 Contexts.....	4
7.2.1 ITS-SCPs related to communications between ITS-SCUs.....	4
7.2.2 ITS-SCPs related communications between ITS-SUs.....	4
7.2.3 ITS-SCPs related to SCNs.....	5
8 ITS communication protocols.....	5
8.1 ITS-CP identifiers.....	5
8.2 Initially identified ITS-CPs.....	6
8.2.1 ITS-S access layer.....	6
8.2.2 ITS-S networking & transport layer.....	6
8.2.3 ITS-S facilities layer.....	7
8.2.4 ITS-S security entity.....	8
8.2.5 ITS-S management entity.....	8
8.2.6 Combinations of ITS-S layers and entities.....	8
9 ITS-S communication protocol stacks.....	9
9.1 ITS-SCPS identifiers.....	9
9.2 Initially identified ITS-SCPSs.....	9
9.2.1 ITS-SCPS for "ITS station-internal management communications".....	9
9.2.2 ITS-SCPS for "SCN-access".....	9
9.2.3 ITS-SCPS for "M5 service announcement".....	10
9.2.4 ITS-SCPS for "Secure sessions involving Internet".....	10
9.2.5 ITS-SCPS for "Secure broadcast of messages with the ETSI ITS-G5 Release 1 stack".....	11
10 ITS-S communication profiles.....	11
10.1 ITS-SCP identifiers.....	11
10.2 Initially identified ITS-SCPs.....	12
10.2.1 ITS station-internal management communications.....	12
10.2.2 Access to an SCN for diagnostics purposes.....	12
10.2.3 Service announcement.....	13
10.2.4 General secure sessions involving Internet and using LTE.....	13
10.2.5 Secure broadcast of ETSI road safety messages with the ITS-G5 Release 1 stack.....	13
Annex A (normative) ASN.1 module.....	15
Bibliography.....	19

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO 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).

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.

This document was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

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.

Introduction

ITS Station Communication Profiles (ITS-SCP) used in communications between trusted devices enable

- interoperability between ITS-SUs,
- and portability of ITS applications (that provide the ITS services).

Examples of trusted devices, i.e. ITS-secured communication nodes, are ITS-station units (ITS-SU) specified in ISO 21217:2014. Four implementation contexts of communication nodes in ITS communications networks are identified in ISO 21217:2014, each comprised of ITS-station units (ITS-SU) taking on a particular role: personal, vehicular, roadside, or central. Such ITS-SUs participate in a wide variety of ITS services related to, e.g. sustainability, road safety and transportation efficiency.

NOTE 1 ISO 21217:2014 fully covers the functionality of EN 302 665^[27], which is a predecessor of ISO 21217:2014.

NOTE 2 An ITS-SU can be composed of ITS-SCUs from different vendors where each ITS-SCU is linked to a different ITS-SCU configuration and management centre specified in ISO 24102-2^[16] and ISO 17419. Station-internal management communications between ITS-SCUs of the same ITS-SU are specified in ISO 24102-4^[17]. European C-ITS regulation refers to the "ITS-SCU configuration and management centre" as "C-ITS station operator" meaning the entity responsible for the operation of a C-ITS station. The C-ITS station operator may be responsible for the operation of one single C-ITS station (fixed or mobile), or a C-ITS infrastructure composed of a number of fixed C-ITS stations, or a number of mobile ITS-Stations.

Such ITS-SCPs are essential for many ITS applications and services including time-critical safety applications, automated driving, remote management of ITS-SUs (ISO 24102-2^[16]), and roadside/infrastructure related services.

Over the last decade, ITS services have arisen that require secure access to data from Sensor and Control Networks (SCN), e.g. from In-Vehicle Networks (IVNs) and from Infrastructure/Roadside Networks (IRNs), some of which require secure local access to time-critical information, see [Figures 1](#) and [2](#).

NOTE 3 [Figures 1](#) and [2](#) are functional illustrations not describing or specifying a specific implementation.

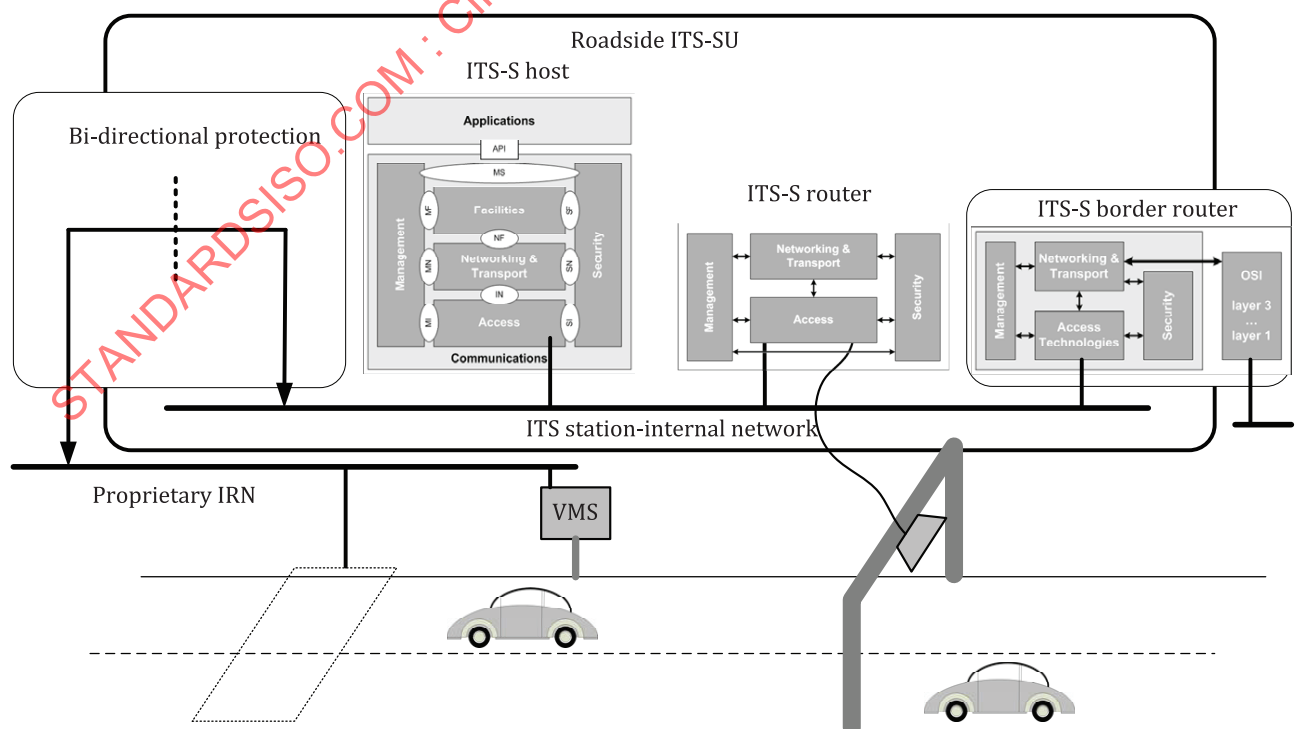


Figure 1 — Example of a roadside ITS-SU connected to a secure proprietary IRN

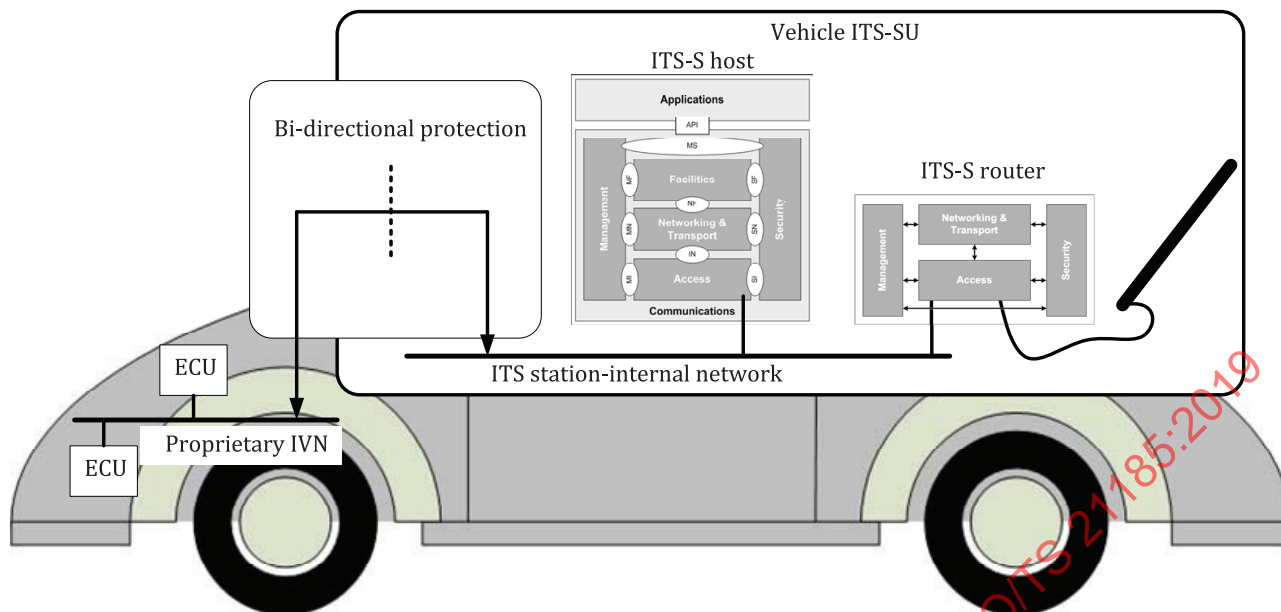


Figure 2 — Example of a vehicle ITS-SU connected to a secure proprietary IVN

Related use cases of these ITS services have largely been derived from regulatory requirements and urban operational needs, and they include:

- secure real-time access to time-critical vehicle-related data for safety of life and property applications, e.g. collision avoidance, emergency electronic brake light and event determination;
- secure local access to detailed real-time data for efficiency applications (traffic management), e.g. intersection interaction, congestion avoidance, dynamic priorities;
- local access to certified real-time data for sustainability applications, e.g. dynamic emission zones (controlled zones as currently standardized in CEN TC 278 within the Project Team PT1705 funded by the European Commission), intersection priorities based on emissions, interactive optimum vehicle settings to minimize fuel consumption.

There are many use cases of ITS services currently identified where real-time exchange of time-critical information between ITS-SUs in close proximity is essential, and the number will grow (see, e.g. the US National ITS Reference Architecture^[30]). It is critical that ultimately all ITS-SUs in a given area are able to be engaged in these distributed services. This, in turn, requires vehicle ITS-SUs to have real-time access to vehicle data and roadside ITS-SUs to have real-time access to infrastructure data, and to be capable of secure software updates.

Another use case involving connectivity between ITS-Ss involves access to ITS-secure SCNs by ITS-SUs over the Internet, i.e. cloud connectivity. Functions and services described in this document and accompanying standards for creating secure communication links can be used to implement such connectivity. Examples include secure communications between a server in a cloud-based ITS-SU and an ITS-SU in a vehicle using a cellular modem, and secure communications between server in an ITS-SU in a traffic control center and a client in an ITS-SU in the roadside “furniture” which it controls using a fibre optic and/or microwave link.

Data and message specifications related to SCNs are provided in ISO/TS 21184^[9].

Cyber security means related to “Secure Sessions between Trusted Devices” (SSTD) in general, and particularly to SCNs, are specified in ISO/TS 21177^[8].

Cyber security means related to information dissemination (broadcast of messages) are specified in IEEE Std. 1609.2TM^[21].

Intelligent transport systems — Communication profiles for secure connections between trusted devices

1 Scope

This document specifies a methodology to define ITS-S communication profiles (ITS-SCPs) based on standardized communication protocols to interconnect trusted devices. These profiles enable secure information exchange between such trusted devices, including secure low-latency information exchange, in different configurations. The present document also normatively specifies some ITS-SCPs based on the methodology, yet without the intent of covering all possible cases, in order to exemplify the methodology.

Configurations of trusted devices for which this document defines ITS-SCPs include:

- a) ITS station communication units (ITS-SCU) of the same ITS station unit (ITS-SU), i.e. station-internal communications;
- b) an ITS-SU and an external entity such as a sensor and control network (SCN), or a service in the Internet;
- c) ITS-SUs.

Other ITS-SCPs can be specified at a later stage.

The specifications given in this document can also be applied to unsecured communications and can be applied to groupcast communications as well.

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/IEC 8825-1, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) — Part 1*

ISO 17419, *Intelligent transport systems — Cooperative systems — Globally unique identification*

ISO 17423:2018, *Intelligent transport systems — Cooperative systems — Application requirements and objectives*

ISO 21217:2014, *Intelligent transport systems — Communications access for land mobiles (CALM) — Architecture*

3 Terms and definitions

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

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

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

3.1

ITS-S communication profile

parameterized ITS-S communication protocol stack

[SOURCE: ISO 17423:2018, 3.6]

3.2

ITS communication protocol

communication protocol applicable in ITS

3.3

ITS-S communication protocol stack

consistent set of ITS-S communication protocols enabling communications between an ITS-SCU and other nodes which may be identified by a registered globally unique reference number

[SOURCE: ISO 17423:2018, 3.7]

4 Symbols and abbreviated terms

CSP communication service parameter

[SOURCE: ISO 17423:2018]

ITS-CP ITS communication protocol

ITS-SCP ITS station communication profile

[SOURCE: ISO 17423:2018]

ITS-SCPS ITS station communication protocol stack

[SOURCE: ISO 17423:2018]

ITS-SCU ITS station communication unit

[SOURCE: ISO 21217:2014]

ITS-SU ITS station unit

[SOURCE: ISO 21217:2014]

IRN infrastructure/roadside network

IVN in-vehicle network

SCN sensor and control network

SSTD secure session between trusted devices

OID object identifier

5 OID conventions

The following OIDs are specified and used in this document:

- 1) Identifying this document:

{ iso (1) standard (0) cptd21185 (21185) }

- 2) Identifying ASN.1 module specifications of this document:

{ iso (1) standard (0) cptd21185 (21185) asn1 (1) }

- 3) Identifying an ITS communications protocol:
 { iso (1) standard (0) cptd21185 (21185) commProtocol (2) }
- 4) Identifying an ITS-S communication protocol stack (ITS-SCPS):
 { iso (1) standard (0) cptd21185 (21185) its-scps (3) }
- 5) Identifying an ITS-S communications profile (ITS-SCP):
 { iso (1) standard (0) cptd21185 (21185) its-scp (4) }

6 Architecture

This document considers the ITS station and communication architecture specified in ISO 21217:2014 and specifies globally unique identifiers of ITS-S communication profiles (ITS-SCPs) for e.g.

- interconnecting ITS-SCUs in an ITS-SU,
- interconnecting ITS-SUs, and for,
- interconnecting an ITS-SU with a SCN,

using OIDs identifying

- ITS communication protocols,
- ITS-S communication protocol stacks (ITS-SCPS),
- ITS-S communication profiles (ITS-SCP),

also specified in this document. The approach is based on the methodology for protocol parameters CSP_Protocol and CSP_SpecificCommsProts specified in ISO 17423:2018 and illustrated in [7.1](#).

7 Communication profiles and protocol stacks — Overview

7.1 Definitions and methodology

An ITS-SCP is defined in ISO 17423:2018 as a "parameterized ITS-S communication protocol stack". ISO 17423:2018 further specifies how ITS-S application processes can present their communication needs by means of "Communication Service Parameters" (CSP) to the ITS-S management, and how the ITS-S management selects applicable ITS-S communication profiles. This document uses the following two CSPs for specifying ITS-SCPs:

- a) CSP_Protocol:

Identification of a complete non-parameterized communication protocol stack by means of a globally unique registered communication protocol stack identifier of ASN.1 type `ProtocolReq ::= ITSprotocolStackID`, with `ITSprotocolStackID` specified in ISO 17419; see [Clause 8.2.6](#).

NOTE 1 ISO 17419 specifies `ITSprotocolStackID` as an INTEGER.

- b) CSP_SpecificCommsProts:

Identification of selected non-parameterized communications protocol stack elements by means of a sequence of protocol identifiers of ASN.1 type `SpecCommProts ::= SEQUENCE OF ITSprotID`, with `ITSprotID` specified in ISO 17419 as a sequence of a ITS-S protocol location of ASN.1 type `ItssProtocolLocation` followed by an ITS protocol identifier of ASN.1 type `ItsProtocolIdentifier`; see [Table 1](#) and [Clause 8](#).

NOTE 2 ISO 17419 specifies `ItsProtocolIdentifier` as an INTEGER.

NOTE 3 ITSprotID is used in Service Announcement specified in ISO 22418^[14].

Table 1 — Named Integer values of ItsProtocolLocation as specified in ISO 17419

ITS-S layer or entity (ISO 21217:2014)	ItsProtocolLocation ^a	
	Acronym	Value
ITS-S access layer	"acLayer"	1
ITS-S networking & transport layer	"ntLayer"	2
ITS-S facilities layer	"fcLayer"	4
ITS-S management entity	"mgEntity"	8
ITS-S security entity	"scEntity"	16
Other location	"other"	32

^a For ITS protocols residing in more than one layer or entity, the acronym to be used in the context of this document is "several" with a value given by the sum of the values of the respective layers and entities. Alternatively, the parts of such an ITS protocol may be identified separately.

The methodology for specifying ITS-SCPs in this document is given by the following steps:

- 1) Identify ITS communication protocols (ITS-CPs) by means of an "Object Identifier" (OID) reference to the standard or specification of the protocol based on the methodology for CSP_SpecificCommsProts specified in ISO 17423:2018; see 8.1.
- 2) Identify ITS-SCPs by means of an "Object Identifier" (OID) reference to a set of ITS-CPs based on the methodology for CSP_Protocol specified in ISO 17423:2018; see 9.1.
- 3) Identify ITS-SCPs by means of an "Object Identifier" (OID) reference to an ITS-SCPs and parameterization information, see 10.1.

7.2 Contexts

7.2.1 ITS-SCPs related to communications between ITS-SCUs

An example of an ITS-SCP for the links between ITS-SCUs of the same ITS-SU (see Figure 3) is presented in 10.2.1.

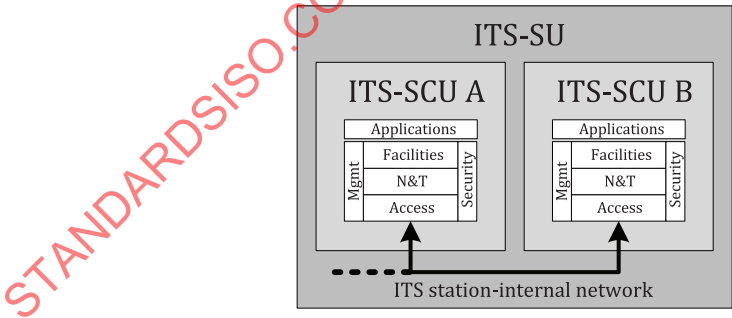


Figure 3 — Interconnection of ITS-SCUs in an ITS-SU

7.2.2 ITS-SCPs related communications between ITS-SUs

An example of an ITS-SCP for the link between ITS-SUs (see Figure 4) is presented in 10.2.3.

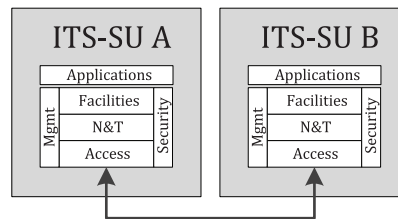


Figure 4 — Interconnection of ITS-SUs

7.2.3 ITS-SCPs related to SCNs

An example of an ITS-SCP for the link between ITS-SUs (ITS-SCUs) and the interface towards sensor and control networks (see Figure 5) is presented in 10.2.2.

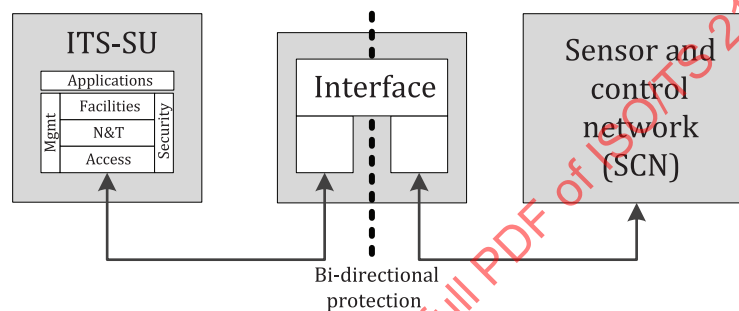


Figure 5 — Interface between ITS-SU and sensor and control network

While the "Interface" in Figure 5 has to be ITS trusted and secured, the SCN may be ITS trusted and secured or not. This document only considers the communications link between the ITS-SU and the ITS-secured "Interface". Details on security are specified in ISO/TS 21177[8].

8 ITS communication protocols

8.1 ITS-CP identifiers

ITS-CPs are identified by an "ITS protocol identifier" of type OID (see 7.1) pointing to a standard or specification. Sub-clauses 8.2, 8.2.2, 8.2.3, 8.2.4, and 8.2.5 specify the OID value of ITS-CPs in the ITS-S access layer, ITS-S networking & transport layer, ITS-S facilities layer, ITS-S security entity, and ITS-S management entity, respectively. These layers and entities are specified in ISO 21217:2014.

The "ITS-CP identifier" OID values specified in Tables 2, 3, 4, 5, and 6 identify communication protocol stack elements for the purpose of this document. Combinations of such protocols, i.e. ITS communication protocol stacks, are specified in Clause 9.

Requirement 1: The generation of an OID for identifying an ITS-CP shall follow the following structure:

- {iso (1) standard (0) cptd21185 (21185) commProtocol (2) <itssProtocolLocation> (itssProtocolLocation) itsProtocolIdentifier-'n' ('n')}

with

- <itssProtocolLocation> and *itssProtocolLocation* as specified in Table 1;
- itsProtocolIdentifier-'n': 'n': equals *ItsProtocolIdentifier* with values assigned in this document.

8.2 Initially identified ITS-CPs

8.2.1 ITS-S access layer

[Table 2](#) presents ITS protocol identifiers of ITS-CPs residing in the ITS-S access layer.

NOTE 1 The ITS-S access layer covers the OSI layers one and two; see ISO 21217:2014.

Table 2 — Communication protocol stack elements — ITS-S access layer

Standard reference	ITS communication protocol identifier	Comment
ISO 17515-1 ^[7]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-1 (1)}	Networked communications, i.e. general access to the Internet. This standard reference is used in the general meaning of "applying LTE cellular network technology for accessing the Internet".
ISO 21214 ^[11]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-2 (2)}	Localised communications using infrared light.
ISO 21215 ^[12]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-3 (3)}	Localised communications using microwaves. This can be either ordinary WiFi mode or OCB mode in different frequency bands.
ISO 21218 ^[13]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-4 (4)}	Hybrid communications support. This is an optional station-internal support protocol. It may become mandatory for ITS station-internal communications.
IEEE Std. 802-3 TM ^[20]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-5 (5)}	Wired Ethernet communications.
ISO 13400-3 ^[2]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-6 (6)}	DoIP — Wired interface based on IEEE std. 802.3 TM
ETSI EN 302 663 ^[26]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-7 (7)}	Localised communications using microwaves at 5,9 GHz in OCB mode with LPD.

NOTE 2 Further standard references can be identified and linked to an ITS protocol identifier at a later stage.

8.2.2 ITS-S networking & transport layer

[Table 3](#) presents ITS protocol identifiers of ITS-CPs residing in the ITS-S networking & transport layer.

NOTE 1 The ITS-S networking & transport layer covers the OSI layers three and four; see ISO 21217:2014.

Table 3 — Communication protocol stack elements — ITS-S networking & transport layer

Standard reference	ITS communication protocol identifier	Comment
ISO 29281-1 ^[18]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-1 (1)}	Localised communications messaging protocol (FNTP) — partly interoperable with IEEE WSMP (IEEE Std. 1609.3 TM) ^a .
IEEE Std. 1609-3 TM ^[22]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-2 (2)}	Localised communications messaging protocol (WSMP) — interoperable with ISO FNTP (ISO 29281-1) ^a .

^a Interoperability is at least given for the information dissemination mode (broadcast communications), as IEEE Std. 1609-3TM^[22] only requires this mode out of the set of all modes identified in ISO/TS 16460^[5] and ISO 29281-1^[18].

Table 3 (continued)

Standard reference	ITS communication protocol identifier	Comment
ISO 21210 ^[10]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-3 (3)}	Networked communications using IPv6.
EN 302 636-4-1 ^[28]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-4 (4)}	Localised communications messaging protocol (GeoNetworking).
EN 302 636-5-1 ^[29]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-5 (5)}	GeoNetworking Basic Transport Protocol.
^a Interoperability is at least given for the information dissemination mode (broadcast communications), as EEE Std. 1609-3 TM ^[22] only requires this mode out of the set of all modes identified in ISO/TS 16460 ^[21] and ISO 29281-1 ^[18] .		

NOTE 2 Further standard references can be identified and linked to an ITS protocol identifier at a later stage.

8.2.3 ITS-S facilities layer

Table 4 presents ITS protocol identifiers of ITS-CPs residing in the ITS-S facilities layer.

NOTE 1 The ITS-S facilities layer covers the OSI layers five, six and seven; see ISO 21217:2014.

Table 4 — Communication protocol stack elements — ITS-S facilities layer

Standard reference	ITS communication protocol identifier	Comment
ISO 13185-2 ^[1]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) fcLayer (4) itsProtocolIdentifier-1 (1)}	Universal gateway protocol
ISO 14229-2 ^[3]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) fcLayer (4) itsProtocolIdentifier-2 (2)}	Unified diagnostic services - session layer services
ISO 17429 ^[6]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) fcLayer (4) itsProtocolIdentifier-3 (3)}	"Communication profile handler" (CPH). Various facility layer services
ISO/TS 21184 ^[9]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) fcLayer (4) itsProtocolIdentifier-4 (4)}	Management of messages containing information of sensor and control networks
ISO 22900-2 ^[15]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) fcLayer (4) itsProtocolIdentifier-5 (5)}	Application programming interface for diagnostic protocol data unit
ISO 14229-5 ^[4]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) fcLayer (4) itsProtocolIdentifier-6 (6)}	Unified diagnostic services on Internet Protocol implementation (UDSonIP)
ISO 24102-2 ^[16]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) fcLayer (4) itsProtocolIdentifier-7 (7)}	Remote ITS station management protocol: Remote management communication handler (RMCH)
ISO 22418 ^[14]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) fcLayer (4) itsProtocolIdentifier-8 (8)}	Service announcement protocol: FSAP communication manager

Table 4 (continued)

Standard reference	ITS communication protocol identifier	Comment
ISO 24102-4 ^[17]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) fcLayer (4) itsProtocolIdentifier-9 (9)}	Station-internal management communications protocol: ITS station-internal management communication agent (IICA)

NOTE 2 Further standard references can be identified and linked to an ITS protocol identifier at a later stage.

8.2.4 ITS-S security entity

[Table 5](#) presents ITS protocol identifiers of ITS-CPs residing in the ITS-S security entity.

Table 5 — Communication protocol stack elements — ITS-S security entity support

Standard reference	ITS communication protocol identifier	Comment
IEEE Std. 1609-2™ ^[21]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) scEntity (16) itsProtocolIdentifier-1 (1)}	Security services for broadcast messages
ISO/TS 21177 ^[8]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) scEntity (16) itsProtocolIdentifier-2 (2)}	Security services for sessions
ETSI TS 103 097 ^[23]	{iso (1) standard (0) cptd21185 (21185) commProtocol (2) scEntity (16) itsProtocolIdentifier-3 (3)}	Security of broadcast of road safety messages in the European Union

NOTE Further standard references can be identified and linked to an ITS protocol identifier at a later stage.

8.2.5 ITS-S management entity

[Table 5](#) presents ITS protocol identifiers of ITS-CPs residing in the ITS-S security entity.

Table 6 — Communication protocol stack elements — ITS-S management entity support

Standard reference	ITS communication protocol identifier	Comment
		None identified so far ^a
^a This empty table is maintained for completeness of the tool presentation.		

NOTE Further standard references can be identified and linked to an ITS protocol identifier at a later stage.

8.2.6 Combinations of ITS-S layers and entities

[Table 7](#) presents ITS protocol identifiers of ITS-CPs residing in several ITS-S layers and entities.

Table 7 — Communication protocol stack elements — Several layers and entities

Standard reference	ITS communication protocol identifier	Comment
		None identified so far ^a
^a This empty table is maintained for completeness of the tool presentation.		

9 ITS-S communication protocol stacks

9.1 ITS-SCPS identifiers

ITS-SCPSs specified in this document are referenced by an Object Identifier (OID) value of the following structure:

— {iso (1) standard (0) cptd21185 (21185) its-scps (3) its-scps-'n' ('n')}

with

— its-scps-'n': 'n' equals `ITSprotocolStackID` with values assigned in this document; see also [7.1](#).

Some ITS-SCPS specifications are presented in 0. Further ITS-SCPSs may be specified at a later stage based on requirements from ITS stakeholders. Uniqueness of reference numbers of ITS-SCPSs will be ensured by ISO TC 204, e.g. by means of amendments to this document.

NOTE A `SEQUENCE OF ITSprotID`, i.e. the identification of an ITS-SCPS, is used in Service Announcement specified in ISO 22418^[14]. In the current revision of ISO 22418 towards EN ISO 22418 it is intended to change this usage beneficially, i.e. replace `SEQUENCE OF ITSprotID` by `ITSprotocolStackID`.

9.2 Initially identified ITS-SCPSs

9.2.1 ITS-SCPS for "ITS station-internal management communications"

Requirement 2: The OID {iso (1) standard (0) cptd21185 (21185) its-scps (3) its-scps-1 (1)} shall be used to identify the ITS-SCPS specified in [Table 8](#).

Table 8 — ITS-SCPS "ITS station-internal management communications secure sessions using Ethernet and IPv6"

ITS communication protocol		Comments
OID	Standard reference	
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-5 (5)}	IEEE Std. 802-3 TM ^[20]	Ethernet access technology.
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-4 (4)}	ISO 21218 ^[13]	Access layer management
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-3 (3)}	ISO 21210 ^[10]	IPv6 communications
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) fcLayer (4) itsProtocolIdentifier-9 (9)}	ISO 24102-4 ^[17]	ITS station-internal management communication agent (IICA)
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) scEntity (16) itsProtocolIdentifier-2 (2)}	ISO/TS 21177 ^[8]	Manages secure ITS station-internal communications between IICMs

9.2.2 ITS-SCPS for "SCN-access"

Requirement 3: The OID {iso(1) standard(0) cptd21185 (21185) its-scps (3) its-scps-2 (2)} shall be used to identify the ITS-SCPS specified in [Table 9](#).

Table 9 — ITS-SCPS "SCN-access for SCN diagnostic using Ethernet and IPv6"

ITS-S communication protocol		Comments
OID	Standard reference	
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-5 (5)}	IEEE Std. 802-3™ ^[20]	Ethernet access technology
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-6 (6)}	ISO 13400-3 ^[2]	DoIP — Wired interface based on IEEE Std. 802.3™
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-3 (3)}	ISO 21210 ^[10]	IPv6 communications
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) fcLayer (4) itsProtocolIdentifier-4 (4)}	ISO/TS 21184 ^[9]	Data and messages for sensor and control networks
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) fcLayer (4) itsProtocolIdentifier-5 (5)}	ISO 22900-2 ^[15]	Application programming interface for diagnostic protocol data unit
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) scEntity (16) itsProtocolIdentifier-2 (2)}	ISO/TS 21177 ^[8]	Manages secure sessions between ITS trusted devices

9.2.3 ITS-SCPS for "M5 service announcement"

Requirement 4: The OID {iso(1) standard(0) cptd21185 (21185) its-scps (3) its-scps-3 (3)} shall be used to identify the ITS-SCPS specified in [Table 10](#).

Table 10 — ITS-SCPS "Service announcement using ITS-M5 and FNTF"

ITS-S communication protocol		Comments
OID	Standard reference	
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-3 (3)}	ISO 21215 ^[12]	IEEE 802.11 @ 5,9 GHz.
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-4 (4)}	ISO 21218 ^[13]	Optional
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-1 (1)}	ISO 29281-1 ^[18]	FNTF general session mode
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) fcLayer (4) itsProtocolIdentifier-8 (8)}	ISO 22418 ^[14]	FSAP communication manager
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) scEntity (16) itsProtocolIdentifier-1 (1)}	IEEE Std. 1609-2™ ^[21]	Security services for signing the service announcement message (broadcast)

9.2.4 ITS-SCPS for "Secure sessions involving Internet"

Requirement 5: The OID {iso(1) standard(0) cptd21185 (21185) its-scps (3) its-scps-4 (4)} shall be used to identify the ITS-SCPS specified in [Table 11](#).

Table 11 — Profile "General secured sessions involving Internet"

ITS-S communication protocol		Comments
OID	Standard reference	
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-3 (3)}	ISO 21210 ^[10]	IPv6 communications suite
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) scEntity (16) itsProtocolIdentifier-2 (2)}	ISO/TS 21177 ^[8]	Manages secure sessions between ITS-S application processes in different ITS-SUs.

9.2.5 ITS-SCPS for "Secure broadcast of messages with the ETSI ITS-G5 Release 1 stack"

Requirement 6: The OID {iso(1) standard(0) cptd21185 (21185) its-scps (3) its-scps-5 (5)} shall be used to identify the ITS-SCPS specified in [Table 12](#).

Table 12 — ITS-SCPS "Secure broadcast of messages with the ETSI ITS-G5 Release 1 stack"

ITS-S communication protocol		Comments
OID	Standard reference	
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-7 (7)}	EN 302 663 V1.2.1 ^[26]	Localised communications using microwaves at 5,9 GHz in OCB mode with LPD (ITS-G5 Release 1)
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-4 (4)}	EN 302 636-4-1 V1.3.1 ^[28]	Localised communications messaging protocol (GeoNetworking).
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-5 (5)}	ETSI EN 302 636-5-1 V2.1.1 ^[29]	GeoNetworking Basic Transport Protocol.
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) scEntity (16) itsProtocolIdentifier-3 (3)}	ETSI TS 103 097 V1.3.1 ^[23]	Security of broadcast of road safety messages in the European Union

10 ITS-S communication profiles

10.1 ITS-SCP identifiers

ITS-SCPs specified in this document are referenced by an Object Identifier (OID) value of the following structure

— {iso (1) standard (0) cptd21185 (21185) its-scp (4) its-scp-'n' ('n')}

with

— its-scp-'n': 'n' being a unique unsigned Integer number with values assigned in this document.

Such an OID points to

- the OID identifying an ITS-S communication protocol stack specified in [9.1](#), and
- additional parameterization information, if applicable.

Assignments of ITS-SCPs for the various usage contexts are out of scope of this document. Normative requirements on using specific ITS-SCPs are expected to be presented in standards on ITS-S application processes, or as part of system specifications.

Some ITS-SCP specifications are presented in 10.2. Further ITS-SCPs may be specified at a later stage based on requirements from ITS stakeholders. Uniqueness of reference numbers of ITS-SCPs will be ensured by ISO TC 204, e.g. by means of amendments to this document.

10.2 Initially identified ITS-SCPs

10.2.1 ITS station-internal management communications

Requirement 7: The OID {iso (1) standard (0) cptd21185 (21185) its-scp (4) its-scp-1 (1)} shall be used to identify the ITS-SCP specified in Table 13.

Table 13 — ITS-SCP for station-internal management communications secure sessions using Ethernet and IPv6

ITS-SCPS:	{iso (1) standard (0) cptd21185 (21185) its-scps (3) its-scps-1 (1)}
ITS communication protocol	Parameterization
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-5 (5)}	Standard wired Ethernet communications
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-4 (4)}	None
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-3 (3)}	None
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) fcLayer (4) itsProtocolIdentifier-9 (9)}	None
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) scEntity (16) itsProtocolIdentifier-2 (2)}	None

10.2.2 Access to an SCN for diagnostics purposes

Requirement 8: The OID {iso (1) standard (0) cptd21185 (21185) its-scp (4) its-scp-2 (2)} shall be used to identify the ITS-SCP specified in Table 14.

Table 14 — ITS-SCP for SCN diagnostics using Ethernet and IPv6

ITS-SCPS:	{iso(1) standard(0) cptd21185 (21185) its-scps (3) its-scps-2 (2)}
ITS communication protocol	Parameterization
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-5 (5)}	Standard Ethernet. See also below: {iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-6 (6)}
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-6 (6)}	DoIP initial configuration detection
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-3 (3)}	None
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) fcLayer (4) itsProtocolIdentifier-4 (4)}	Configuration files for given SCN

Table 14 (continued)

ITS-SCPS:	{iso(1) standard(0) cptd21185 (21185) its-scps (3) its-scps-2 (2)}
ITS communication protocol	Parameterization
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) fcLayer (4) itsProtocolIdentifier-5 (5)}	None
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) scEntity (16) itsProtocolIdentifier-2 (2)}	None

10.2.3 Service announcement

Requirement 9: The OID {iso (1) standard (0) cptd21185 (21185) its-scp (4) its-scp-2 (2)} shall be used to identify the ITS-SCP specified in [Table 15](#).

Table 15 — ITS-SCP for broadcast of service announcement messages using ITS-M5 and FNTF

ITS-SCPS:	{iso(1) standard(0) cptd21185 (21185) its-scps (3) its-scps-3 (3)}
ITS communication protocol	Parameterization
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-3 (3)}	Physical frequency channel settings as given by regulation for the SaCH (see ISO 17419).
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-4 (4)}	Optional support. Does not affect interoperability. No parameterization.
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-1 (1)}	None
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) fcLayer (4) itsProtocolIdentifier-8 (8)}	None
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) scEntity (16) itsProtocolIdentifier-1 (1)}	Keys as given by regulation.

10.2.4 General secure sessions involving Internet and using LTE

Requirement 10: The OID {iso (1) standard (0) cptd21185 (21185) its-scp (4) its-scp-4 (4)} shall be used to identify the ITS-SCP specified in [Table 16](#).

Table 16 — ITS-SCP for general secure sessions involving Internet

ITS-SCPS:	{iso(1) standard(0) cptd21185 (21185) its-scps (3) its-scps-4 (4)}
ITS communication protocol	Parameterization
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-3 (3)}	None
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) scEntity (16) itsProtocolIdentifier-2 (2)}	Keys as given by regulation.

10.2.5 Secure broadcast of ETSI road safety messages with the ITS-G5 Release 1 stack

Requirement 11: The OID {iso (1) standard (0) cptd21185 (21185) its-scp (4) its-scp-5 (5)} shall be used to identify the ITS-SCP specified in [Table 17](#).

Table 17 — ITS-SCP for secure broadcast of ETSI road safety messages such as CAM^[24] and DENM^[25] using the ETSI ITS-G5 Release 1 stack

ITS-SCPS:	{iso(1) standard(0) cptd21185 (21185) its-scps (3) its-scps-5 (5)}	
ITS communication protocol		Parameterization
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-7 (7)}		Control Channel allocated in the European Union
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-4 (4)}		No multi-hop forwarding
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-5 (5)}		Port numbers of respective message
{iso (1) standard (0) cptd21185 (21185) commProtocol (2) scEntity (16) itsProtocolIdentifier-3 (3)}		Security framework for the European Union

Annex A (normative)

ASN.1 module

A.1 Overview

The ASN.1 basic notation is specified in ISO/IEC 8824-1^[19]. The following ASN.1 module is specified in this normative annex:

— SstdProfiles {iso (1) standard (0) cptd21185 (21185) asn1 (1) profiles (1) version0 (0)}

This ASN.1 module is provided at <https://standards.iso.org/iso/ts/21185/ed-1/en>.

Requirement (conditional) 12: In case the specifications of ASN.1 types and values given in the file mentioned above are not in accordance with illustrations or specifications provided elsewhere in this document, the specifications given in the file mentioned above shall prevail.

Encodings of the types and values defined in the ASN.1 module specified in A.2 are subject to requirements set up in other standards.

Requirement (conditional) 13: ASN.1 BASIC-PER, UNALIGNED specified in ISO/IEC 8825-1 shall apply if no other explicit requirement on encoding is given.

A.2 Module SISOprofiles

```
SstdProfiles {iso (1) standard (0) cptd21185 (21185) asn1 (1) profiles
(1) version0 (0)}
DEFINITIONS AUTOMATIC TAGS ::= BEGIN

IMPORTS

-- ISO 17419
ItssProtocolLocation, ItsProtocolIdentifier FROM CITSapplMgmtApplReg2
{iso(1) standard(0) cits-applMgmt (17419) applRegistry (2) version2 (2)}

; -- End of IMPORTS

-- ITS protocol location
protLocUnknown ItssProtocolLocation::=0
protLocAcLayer ItssProtocolLocation::=1
protLocNtLayer ItssProtocolLocation::=2
protLocFcLayer ItssProtocolLocation::=4
protLocmgEntity ItssProtocolLocation::=8
protLocScEEntity ItssProtocolLocation::=16

-- ITS-S access layer
-- ITS communication protocol identifiers
protIDiso17515p1 ItsProtocolIdentifier::=1
protIDiso21214 ItsProtocolIdentifier::=2
protIDiso21215 ItsProtocolIdentifier::=3
protIDiso21218 ItsProtocolIdentifier::=4
protIDieee802p3 ItsProtocolIdentifier::=5
protIDiso13400p3 ItsProtocolIdentifier::=6
protIDetsiEN302663 ItsProtocolIdentifier::=7

-- ITS communication protocols
cpIso17515p1 OBJECT IDENTIFIER ::= {1 0 21185 2 protLocAcLayer
protIDiso17515p1} -- {iso (1) standard (0) cptd21185 (21185)
```

```

commProtocol (2) acLayer (1) itsProtocolIdentifier-1 (1)}

cpIso21214-Edition2 OBJECT IDENTIFIER ::= {1 0 21185 2 protLocAcLayer
protIDiso21214} -- {iso (1) standard (0) cptd21185 (21185) commProtocol
(2) acLayer (1) itsProtocolIdentifier-2 (2)}

cpIso21215-Edition2 OBJECT IDENTIFIER ::= {1 0 21185 2 protLocAcLayer
protIDiso21215} -- {iso (1) standard (0) cptd21185 (21185) commProtocol
(2) acLayer (1) itsProtocolIdentifier-3 (3)}

cpIso21218-Edition2015 OBJECT IDENTIFIER ::= {1 0 21185 2 protLocAcLayer
protIDiso21218} -- {iso (1) standard (0) cptd21185 (21185) commProtocol
(2) acLayer (1) itsProtocolIdentifier-4 (4)}

cpIeee802p3-Edition2 OBJECT IDENTIFIER ::= {1 0 21185 2 protLocAcLayer
protIDieee802p3} -- {iso (1) standard (0) cptd21185 (21185) commProtocol
(2) acLayer (1) itsProtocolIdentifier-5 (5)}

cpIso13400p3-Edition2 OBJECT IDENTIFIER ::= {1 0 21185 2 protLocAcLayer
protIDiso13400p3} -- {iso (1) standard (0) cptd21185 (21185)
commProtocol (2) acLayer (1) itsProtocolIdentifier-6 (6)}

cpEtsi302663-Version1-2-1 OBJECT IDENTIFIER ::= {1 0 21185 2
protLocAcLayer protIDetsiEN302663} -- {iso (1) standard (0) cptd21185
(21185) commProtocol (2) acLayer (1) itsProtocolIdentifier-7 (7)}

-- ITS-S networking & transport layer
-- ITS communication protocol identifiers
protIDiso29281p1 ItsProtocolIdentifier::=1
protIDieee1609p3 ItsProtocolIdentifier::=2
protIDiso21210 ItsProtocolIdentifier::=3
protIDetsi302636p4sp1 ItsProtocolIdentifier::=4
protIDetsi302636p5sp1 ItsProtocolIdentifier::=5

-- ITS communication protocols
cpIso29281p1-Edition2 OBJECT IDENTIFIER ::= {1 0 21185 2 protLocNtLayer
protIDiso29281p1} -- {iso (1) standard (0) cptd21185 (21185)
commProtocol (2) ntLayer (2) itsProtocolIdentifier-1 (1)}

cpIeee1609p3-Edition2016 OBJECT IDENTIFIER ::= {1 0 21185 2
protLocNtLayer protIDieee1609p3} -- {iso (1) standard (0) cptd21185
(21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-2 (2)}

cpIso21210-Edition2 OBJECT IDENTIFIER ::= {1 0 21185 2 protLocNtLayer
protIDiso21210} -- {iso (1) standard (0) cptd21185 (21185) commProtocol
(2) ntLayer (2) itsProtocolIdentifier-3 (3)}

cpEtsi302636p4sp1-Edition1-3-1 OBJECT IDENTIFIER ::= {1 0 21185 2
protLocNtLayer protIDetsi302636p4sp1} -- {iso (1) standard (0) cptd21185
(21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-4 (4)}

cpEtsi302636p5sp1-Edition2-1-1 OBJECT IDENTIFIER ::= {1 0 21185 2
protLocNtLayer protIDetsi302636p5sp1} -- {iso (1) standard (0) cptd21185
(21185) commProtocol (2) ntLayer (2) itsProtocolIdentifier-5 (5)}

-- ITS-S facilities layer
-- ITS communication protocol identifiers
protIDiso13185p2 ItsProtocolIdentifier::=1
protIDiso14229p2 ItsProtocolIdentifier::=2
protIDiso17429 ItsProtocolIdentifier::=3
protIDiso21184 ItsProtocolIdentifier::=4
protIDiso22900p2 ItsProtocolIdentifier::=5
protIDiso14229p5 ItsProtocolIdentifier::=6
protIDiso24102p2 ItsProtocolIdentifier::=7
protIDiso22418 ItsProtocolIdentifier::=8
protIDiso24102p4 ItsProtocolIdentifier::=9

-- ITS communication protocols
cpIso13185p2 OBJECT IDENTIFIER ::= {1 0 21185 2 protLocFcLayer

```