

Second edition
2014-08-15

Corrected version
2014-11-15

**Information technology —
Telecommunications and
information exchange between
systems — NFC Security —**

**Part 1:
NFC-SEC NFCIP-1 security services and
protocol**

*Technologies de l'information — Téléinformatique — Sécurité NFC —
Partie 1: Services de sécurité et protocole NFC-SEC NFCIP-1*

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13157-1:2014



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2014

All rights reserved. Unless otherwise specified, 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
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Conformance	1
3 Normative references	1
4 Terms and definitions	1
5 Conventions and notations	2
5.1 Representation of numbers	2
5.2 Names	3
6 Acronyms	3
7 General	4
8 Services	4
8.1 Shared Secret Service (SSE)	4
8.2 Secure Channel Service (SCH)	5
9 Protocol Mechanisms	5
9.1 Key agreement	5
9.2 Key confirmation	5
9.3 PDU security	5
9.4 Termination	5
10 States and Sub-states	6
11 NFC-SEC-PDUs	7
11.1 Secure Exchange Protocol (SEP)	7
11.2 Protocol Identifier (PID)	8
11.3 NFC-SEC Payload	8
11.4 Terminate (TMN)	8
11.5 Error (ERROR)	8
12 Protocol Rules	8
12.1 Protocol and Service Errors	8
12.2 Interworking Rules	9
12.3 Sequence Integrity	9
12.4 Cryptographic Processing	9
Annex A (normative) Protocol Machine Specification	10

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

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).

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: [Foreword - Supplementary information](#)

ISO/IEC 13157-1 was prepared by Ecma International (as ECMA-385) and was adopted, under a special "fast-track procedure", by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

This second edition cancels and replaces the first edition (ISO/IEC 13157-1:2010), which has been technically revised.

ISO/IEC 13157 consists of the following parts, under the general title *Information technology — Telecommunications and information exchange between systems — NFC Security*:

- *Part 1: NFC-SEC NFCIP-1 security services and protocol*
- *Part 2: NFC-SEC cryptography standard using ECDH and AES.*

This corrected version of ISO 13157-1:2014 incorporates the following corrections:

5.1, last list item, the underlined part has been added:

- In octets the lsb is bit number 1, the msb is bit number 8; in n-length bit strings the lsb is bit number 1 and the msb is bit number n.

Introduction

This International Standard specifies common NFC Security services and a protocol. This International Standard is a part of the NFC Security series of standards. The NFC-SEC cryptography standards of the series complement and use the services and protocol specified in this International Standard. This second edition has removed Annex B because it has been included in ISO/IEC 18092:2013 and it allows implementation on generic NFC connections.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13157-1:2014

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 13157-1:2014

Information technology — Telecommunications and information exchange between systems — NFC Security —

Part 1: NFC-SEC NFCIP-1 security services and protocol

1 Scope

This International Standard specifies the NFC-SEC secure channel and shared secret services for NFCIP-1 and the PDUs and protocol for those services.

NOTE This International Standard does not address application specific security mechanisms (as typically needed for smart card related use cases and standardized in the ISO/IEC 7816 series). NFC-SEC may complement application specific security mechanisms of ISO/IEC 7816.

2 Conformance

Conformant implementations implement one or more of the services specified in this International Standard, using the security mechanisms from the NFC-SEC cryptography part identified by the selected Protocol Identifier.

3 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7498-1:1994, *Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*

ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

ISO/IEC 10731:1994, *Information technology — Open Systems Interconnection — Basic Reference Model — Conventions for the definition of OSI services*

ISO/IEC 11770-1:1996, *Information technology — Security techniques — Key management — Part 1: Framework*

ISO/IEC 13157-2:2010, *Information technology — Telecommunications and information exchange between systems — NFC Security — Part 2: NFC-SEC cryptography standard using ECDH and AES* (also published by Ecma as Standard ECMA-386)

ISO/IEC 18092:2013, *Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1)* (also published by Ecma as Standard ECMA-340)

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 18092, ISO/IEC 7498-1, ISO 7498-2, ISO/IEC 10731, ISO/IEC 11770-1 and the following apply.

4.1
connection

(N)-connection as specified in ISO/IEC 7498-1

4.2
entity

(N)-entity as specified in ISO/IEC 7498-1

4.3
link key

secret key securing communications across a secure channel

4.4
NFC-SEC User

entity using the NFC-SEC service

4.5
protocol

(N)-protocol as specified in ISO/IEC 7498-1

4.6
recipient

NFC-SEC entity that receives ACT_REQ

4.7
secure channel

secure NFC-SEC connection

4.8
sender

NFC-SEC entity that sends ACT_REQ

4.9
service

(N)-service as specified in ISO/IEC 7498-1

4.10
shared secret

secret shared by two peer NFC-SEC Users

5 Conventions and notations

The following conventions and notations apply in this document unless otherwise stated.

5.1 Representation of numbers

The following conventions and notations apply in this document unless otherwise stated.

- Letters and digits in parentheses represent numbers in hexadecimal notation.
- The setting of bits is denoted by ZERO or ONE.
- Numbers in binary notation and bit patterns are represented by sequences of 0 and 1 bits shown with the most significant bit to the left. Within such strings, X may be used to indicate that the setting of a bit is not specified within the string.
- In octets the lsb is bit number 1, the msb is bit number 8; in n-length bit strings the lsb is bit number 1 and the msb is bit number n.

5.2 Names

The names of basic elements, e.g. specific fields, are written with a capital initial letter.

6 Acronyms

For the purposes of this International Standard, the acronyms specified in ISO/IEC 18092 apply. Additionally, the following acronyms apply.

ACT_REQ	Activation Request PDU
ACT_RES	Activation Response PDU
ENC	Encrypted Packet PDU
ERROR	Error PDU
lsb	least significant bit
LSB	Least Significant Byte
msb	most significant bit
MSB	Most Significant Byte
MSG	MesSaGe code
PCI	Protocol Control Information (see ISO/IEC 7498-1)
PDU	Protocol Data Unit (see ISO/IEC 7498-1)
PID	Protocol Identifier
RFU	Reserved for Future Use
SAP	Service Access Point
SCH	Secure Channel service
SDL	Specification and Description Language (as specified in ITU-T Z.100)
SDU	Service Data Unit (see ISO/IEC 7498-1)
SEP	Security Exchange protocol Parameter
SN	Sequence Number
SNV	SN variable
SSE	Shared Secret Service
SVC	SerVicE code
TMN	Terminate PDU
VFY_REQ	Verification Request PDU
VFY_RES	Verification Response PDU

7 General

NFC-SEC as illustrated in [Figure 1](#) uses the OSI reference model specified in ISO/IEC 7498-1.

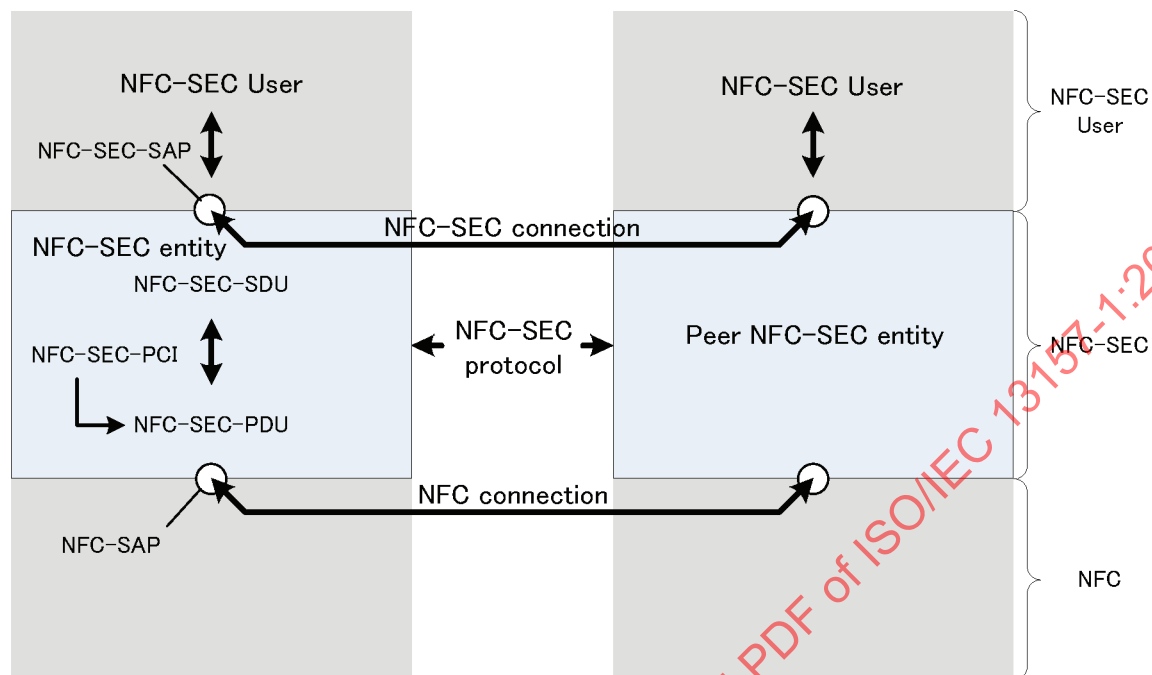


Figure 1 — NFC-SEC architecture

NFC-SEC Users invoke and access the NFC-SEC services through NFC-SEC Service Access Points (NFC-SEC-SAP). NFC-SEC entities obtain NFC-SEC-SDUs (requests) from NFC-SEC Users and return NFC-SEC-SDUs (confirmations) to them.

This International Standard specifies the Secure Channel Service (SCH) and the Shared Secret Service (SSE).

To provide the NFC-SEC services, Peer NFC-SEC entities exchange NFC-SEC-PDUs by conforming to the NFC-SEC protocol over NFC-SEC connections.

Peer NFC-SEC entities send and receive NFC-SEC-PDUs through NFC Service Access Points (NFC-SAP). A NFC-SEC-PDU consists of NFC-SEC Protocol Control Information (NFC-SEC-PCI) and a single NFC-SEC-SDU.

8 Services

This Clause specifies two services, SSE and SCH, that NFC-SEC provides to the NFC-SEC User. When invoked, these services enable the cryptographic protected transmission of NFC-SEC User messages between the peer entities by means of a protocol described in [Clause 9](#).

Shared secrets established with the services specified below shall be cryptographically uncorrelated from any shared secrets established beforehand or afterwards.

8.1 Shared Secret Service (SSE)

The SSE establishes a shared secret between two peer NFC-SEC Users, which they can use at their discretion.

Invocation of the SSE shall establish a shared secret by the key agreement and key confirmation mechanisms, according to the NFC-SEC cryptography part that defines the PID.

8.2 Secure Channel Service (SCH)

The SCH provides a secure channel.

Invocation of the SCH shall establish a link key, by derivation from a shared secret established by the key agreement and key confirmation mechanisms, and shall subsequently protect all communications in either direction across the channel, according to the NFC-SEC cryptography part that defines the PID.

9 Protocol Mechanisms

The NFC-SEC protocol comprises the following mechanisms. [Figure 2](#) specifies the sequence of the protocol mechanisms.

9.1 Key agreement

The peer NFC-SEC entities shall establish a shared secret using ACT_REQ and ACT_RES, according to the NFC-SEC cryptography part that defines the PID.

9.2 Key confirmation

The peer NFC-SEC entities shall verify their agreed shared secret using VFY_REQ and VFY_RES, according to the NFC-SEC cryptography part that defines the PID.

9.3 PDU security

PDU security is a mechanism of SCH service only.

The peer NFC-SEC entities shall protect data exchange using ENC, according to the NFC-SEC cryptography part that defines the PID.

This mechanism shall comprise one or more of the following, as specified in the respective NFC-SEC cryptography standard:

- Sequence Integrity, conforming to the requirements of [12.3](#);
- Confidentiality;
- Data integrity;
- Origin authentication.

9.4 Termination

The peer NFC-SEC entities shall terminate SSE and SCH using TMN.

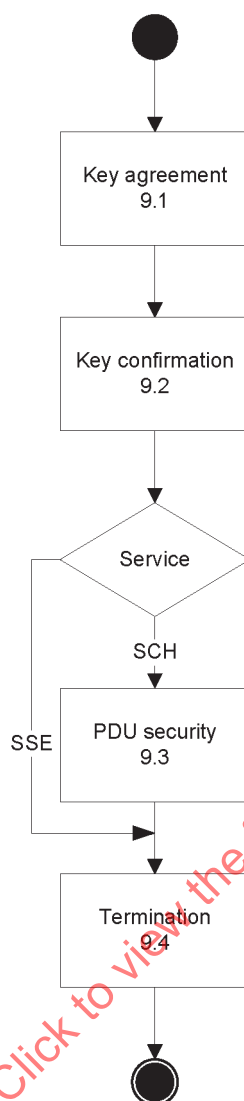


Figure 2 — General flow of the NFC-SEC services

10 States and Sub-states

The NFC-SEC protocol machine in [Annex A](#) specifies the state transitions for the states and sub-states in [Table 1](#).

Table 1 — State

State	Description
Idle	NFC-SEC is ready to start a new service upon request from the NFC-SEC User or the peer NFC-SEC Entity.
Select	NFC-SEC is awaiting an ACT_RES.
Established	An NFC-SEC Service is requested. The established state contains two sub-states In the Established_Sender sub-state it is awaiting a VFY_RES. In the Established_Recipient Sub-state it is awaiting a VFY_REQ.
Confirmed	An NFC-SEC service is established. The Confirmed State contains two sub-states, In the Confirmed_SSE sub-state, the shared secret is ready to be retrieved. In the Confirmed_SCH sub-state, secure data exchange is ready.

Upon transition to the Idle state any shared secret and link key shall be destroyed.

11 NFC-SEC-PDUs

Secure data shall be conveyed in the NFC-SEC Payload field of the NFC-SEC-PDU as specified in [Figure 3](#).

SEP	PID	NFC-SEC Payload
-----	-----	-----------------

Figure 3 — Structure of NFC-SEC PDU

[Table 2](#) specifies the *NFC-SEC-PDUs* fields for the NFC-SEC commands as mandatory (m), prohibited (p), conditional (c). The conditionality (c) is further specified in [11.3](#).

Table 2 — NFC-SEC-PDU Fields

NFC-SEC commands	SEP	PID	NFC-SEC Payload
ACT_REQ	m	m	c
ACT_RES	m	p	c
VFY_REQ	m	p	c
VFY_RES	m	p	c
ENC	m	p	c
TMN	m	p	p
ERROR	m	p	c

11.1 Secure Exchange Protocol (SEP)

The 1-byte Secure Exchange Protocol (SEP) field is specified as follows:

- The value of 00b in the SVC indicates that the PDU is part of an SSE exchange. The value of 01b in the SVC indicates that the PDU is part of an SCH exchange.
- The MSG code identifies the PDU type as specified in [Table 3](#). All other codes are RFU.
- The RFU bits shall be set ZERO. Receivers shall reject PDUs with RFU bits set to ONE.

[Figure 4](#) specifies the bit assignment.

msb				lsb			
Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
RFU		SVC		MSG			

Figure 4 — Bit assignment of SEP

Table 3 — PDU types and their MSG codes

Code	NFC-SEC command	Description
0000	ACT_REQ	Activation request to request a new service.
0001	ACT_RES	Activation response, to accept a service request.
0010	VFY_REQ	Verification request to submit check values for verification of the Sender's shared secret.
0011	VFY_RES	Verification response to submit check values for verification of the Recipient's shared secret.
0100	ENC	Encrypted packet for secure data exchange.
0110	TMN	Terminate request to terminate a service.
1111	ERROR	Error an Indication of an error.
Other		RFU

11.2 Protocol Identifier (PID)

Each NFC-SEC cryptography part of this International Standard defines a distinct 8-bit PID that is only included in ACT_REQ.

11.3 NFC-SEC Payload

The TMN PDU shall contain no NFC-SEC Payload field. The NFC-SEC Payload field shall consist of an integer number of octets. Its use in the ERROR PDU is specified in the Error sub-clause below. Its use, structure and encoding in all other PDUs is specified in NFC-SEC cryptography part that defines the PID.

11.4 Terminate (TMN)

The TMN PDU consists of the SEP field only as specified in [Table 2](#).

11.5 Error (ERROR)

The ERROR PDU starts with the SEP field and, if it contains a payload, this payload shall contain a zero-terminated octet string in the NFC-SEC Payload field.

12 Protocol Rules

This Clause specifies rules for the NFC-SEC protocol.

12.1 Protocol and Service Errors

- When a NFC-SEC entity receives a PDU in a state where it is not allowed, it shall respond with an ERROR PDU.
- When a NFC-SEC entity receives a PDU that it does not support or with invalid contents as specified in NFC-SEC cryptography standard, it shall respond with an ERROR PDU.
- When a NFC-SEC entity receives or sends an ERROR PDU, it shall set the protocol state to Idle.
- When a NFC-SEC entity receives or sends an ERROR PDU, it shall send an ERROR SDU to the NFC-SEC User.
- When a NFC-SEC entity receives a SDU in a state where it is not allowed or with invalid contents, it shall respond with an ERROR SDU and leave the state unchanged.

12.2 Interworking Rules

- A NFC-SEC implementation may set an upper bound on the NFC-SEC-SDU length. Send Data requests specified in [A.2](#) with longer SDUs shall be rejected.
- One NFC-SEC-PDU shall contain exactly one NFC-SEC-SDU.
- NFC-SEC Entities shall discard any duplicate NFC-SEC-PDUs, as specified in the Sequence Integrity clause.

12.3 Sequence Integrity

- NFC-SEC cryptography standards providing sequence integrity shall specify the sequence integrity mechanism in conformance to the following:
- Each NFC-SEC Entity shall maintain its SNV.
- Upon SCH establishment, the Recipient shall initialise its SNV with the same initial value as the Sender's SNV as specified in the NFC-SEC cryptography part that defines the PID.
- The NFC-SEC cryptography part that defines the PID specifies a range on the SNV values.
- Upon sending of ENC, the NFC-SEC Entity shall increase their SNV by 1, and then place it into the SN field.
- The SN field shall be protected by the PDU security mechanism to make any change detectable.
- Upon receipt of an ENC, the NFC-SEC Entity shall extract the SN field and compare it with its SNV. If $SN == SNV$, then the PDU shall not be submitted to the NFC-SEC User but discarded, and the state and SNV shall remain unchanged as specified in [A.4.4](#).
- The NFC-SEC entity shall increase its SNV by 1.

The 'PDU content valid?' condition in [A.4.4](#) shall be true if SN equals SNV and false otherwise.

NOTE In case of sequence integrity errors, NFC-SEC aborts the SCH and notifies both peer-NFC-SEC-USERS of the incident. It is up to the NFC-SEC-USERS to re-establish a SCH with new keys or to abort the transaction.

12.4 Cryptographic Processing

Before sending and after receipt of PDUs other than TMN and ERROR, cryptographic processing occurs as specified by the cryptography part that defines the PID. If the outcome of the cryptographic processing of incoming PDUs is negative, then the 'PDU content valid' decision in [Annex A](#) is false.

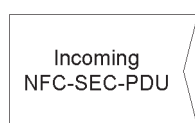
Annex A (normative)

Protocol Machine Specification

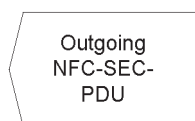
The NFC-SEC protocol machine in this Annex specifies the sequence of PDUs to establish and terminate the SSE, and to establish, use and terminate the SCH.

In addition the Protocol machine specifies which PDUs may be sent or received in which state.

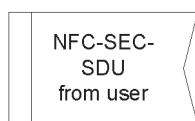
A.1 SDL Symbols



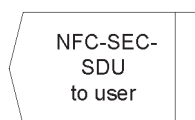
NFC-SEC-PDU received from the peer NFC-SEC entity, delivered by the local NFC entity.



NFC-SEC-PDU sent to the peer NFC-SEC entity, submitted to the local NFC entity.



NFC-SEC-SDU obtained from the NFC-SEC User, requesting the NFC-SEC entity to perform an action.



NFC-SEC-SDU submitted to the NFC-SEC User, either in response to a previous request or to indicate an event.



State. In a state the protocol machine awaits an event. Events not foreseen in the diagrams constitute protocol errors.



A branching condition in the processing of events.

A.2 Request SDUs

Request SDUs are submitted by NFC-SEC Users to request the NFC-SEC service. Parameters are given in brackets. Requirements on the parameter values are specified in NFC-SEC cryptography standards.

NOTE The actual implementation method of the request primitives (e.g. method calls, inter-process PDUs), is outside the scope of this International Standard.

Service Invocation	Request the invocation of a new service (type of service, PID).
Send Data	Request the sending of data. Admitted only to SCH (data).
Retrieve Data	Request the retrieval of data received. Admitted only to SCH.