DRAFT INTERNATIONAL STANDARD ISO/IEC 13157

Attributed to ISO/IEC JTC 1 by the Central Secretariat (see page iii)

Voting begins on	Voting terminates on
2009-03-27	**2009-08-27**

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОММИСИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

FAST-TRACK PROCEDURE

Information technology — Telecommunications and information exchange between systems — NFC-SEC: NFCIP-1 Security Services and Protocol

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

ICS 35.110

In accordance with the provisions of Council Resolution 21/1986 this DIS is circulated in the English language only.

Conformément aux dispositions de la Résolution du Conseil 21/1986, ce DIS est distribué en version anglaise seulement.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

© International Organization for Standardization, 2009
© International Electrotechnical Commission, 2009

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

Copyright notice

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user's country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to 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

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2009 — All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

NOTE FROM ITTF

This draft International Standard is submitted for JTC 1 national body vote under the Fast-Track Procedure.

In accordance with Resolution 30 of the JTC 1 Berlin Plenary 1993, the proposer of this document recommends assignment of ISO/IEC 13157 to JTC 1/SC 6.

"FAST-TRACK" PROCEDURE

1 Any P-member and any Category A liaison organization of ISO/IEC JTC 1 may propose that an existing standard from any source be submitted directly for vote as a DIS. The criteria for proposing an existing standard for the fast-track procedure are a matter for each proposer to decide.

2 The proposal shall be received by the ITTF which will take the following actions.

2.1 To settle the copyright and/or trade mark situation with the proposer, so that the proposed text can be freely copied and distributed within JTC 1 without restriction.

2.2 To assess in consultation with the JTC 1 secretariat which SC is competent for the subject covered by the proposed standard and to ascertain that there is no evident contradiction with other International Standards.

2.3 To distribute the text of the proposed standard as a DIS. In case of particularly bulky documents the ITTF may demand the necessary number of copies from the proposer.

3 The period for combined DIS voting shall be five months. In order to be accepted the DIS must be supported by 75 % of the votes cast (abstention is not counted as a vote) and by two-thirds of the P-members voting of JTC 1.

4 At the end of the voting period, the comments received, whether editorial only or technical, will be dealt with by a working group appointed by the secretariat of the relevant SC.

5 If, after the deliberations of this WG, the requirements of 3 above are met, the amended text shall be sent to the ITTF by the secretariat of the relevant SC for publication as an International Standard.

If it is impossible to agree to a text meeting the above requirements, the proposal has failed and the procedure is terminated.

In either case the WG shall prepare a full report which will be circulated by the ITTF.

6 If the proposed standard is accepted and published, its maintenance will be handled by JTC 1.

© ISO/IEC 2000 - All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ecma INTERNATIONAL

Standard ECMA-385

1st Edition / December 2008

NFC-SEC:
NFCIP-1 Security Services and Protocol

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Rue du Rhône 114 CH-1204 Geneva T: +41 22 849 6000 F: +41 22 849 6001

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

Standard
ECMA-385
1st Edition / December 2008

NFC-SEC:
NFCIP-1 Security Services and Protocol

DRAFT 2009

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

--`,,```,,,,````-`-`,,,,`,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

Introduction

This Standard specifies common NFC-SEC services and a protocol. This Standard is a part of the NFC-SEC series of standards.The NFC-SEC cryptography standards of the series complement and use the services and protocol specified in this Standard.

DRAFT 2009

This Ecma Standard has been adopted by the General Assembly of December 2008.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table of contents

1 Scope 1

2 Conformance 1

3 References 1

4 Terms and definitions 1

4.1 Connection 1
4.2 Entity 1
4.3 Link key 1
4.4 NFC-SEC User 1
4.5 Protocol 1
4.6 Recipient 1
4.7 Secure channel 2
4.8 Sender 2
4.9 Service 2
4.10 Shared Secret 2

5 Conventions and notations 2

5.1 Representation of numbers 2
5.2 Names 2

6 Acronyms 2

7 General 3

8 Services 4

8.1 Shared Secret Service (SSE) 4
8.2 Secure Channel Service (SCH) 4

9 Protocol Mechanisms 4

9.1 Key agreement 4
9.2 Key confirmation 4
9.3 PDU security 4
9.4 Termination 4

10 States and Sub-states 5

DRAFT 2009

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

11 NFC-SEC-PDUs 6

11.1 Secure Exchange Protocol (SEP) 6

11.2 Protocol Identifier (PID) 7

11.3 NFC-SEC Payload 7

11.4 Terminate (TMN) 7

11.5 Error (ERROR) 7

12 Protocol Rules 7

12.1 Protocol Errors 7

12.2 Interworking Rules 7

12.3 Sequence Integrity 8

12.4 Cryptographic Processing 8

Annex A (normative) Protocol Machine Specification 9

Annex B (normative) Additional requirements for ECMA-340 (NFCIP-1) 15

DRAFT 2009

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

1 Scope

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

2 Conformance

Conformant implementations employ the security mechanisms in the NFC-SEC cryptography standards identified by the selected PIDs using one or more of the services specified in this Standard.

Conformant implementations that use the NFCIP-1 protocol shall also conform to the requirements in Annex B.

3 References

ECMA-340	Near Field Communication Interface and Protocol (NFCIP-1)
ECMA-386	NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES
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

4 Terms and definitions

For the purpose of this Standard, the terms and definitions specified in ECMA-340, ISO/IEC 7498-1, ISO 7498-2, ISO/IEC 10731 and ISO/IEC 11770-1 apply. In addition, the following terms and definitions 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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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 bit number 8.

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 Standard, the acronyms specified in ECMA-340 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
SCH	Secure Channel service

DRAFT 2009

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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 follows concepts specified in the OSI reference model specified in ISO/IEC 7498-1.

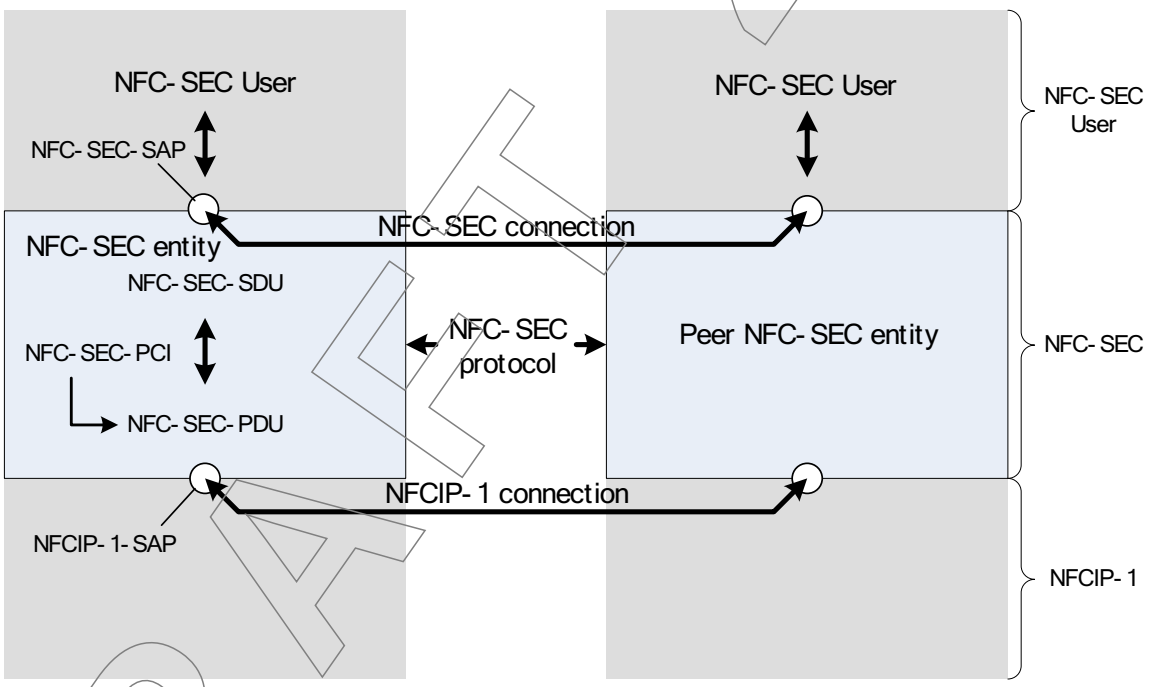


Figure 1 – NFC-SEC architecture

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 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 communicate with each other accessing the NFCIP-1 data service through NFCIP-1 Service Access Points (NFCIP-1-SAP), sending and receiving NFC-SEC-PDUs. A NFC-SEC-PDU consists of NFC-SEC Protocol Control Information (NFC-SEC-PCI) and a single NFC-SEC-SDU.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8 Services

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 standard identified by 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 standard identified by 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 standard identified by 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 standard identified by 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 standard identified by 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. After Release or Deselect of NFCIP-1, or when the NFCIP-1 device is powered off, SSE and SCH instances shall be terminated and the associated shared secret and the link key shall be destroyed.

DRAFT 2009

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

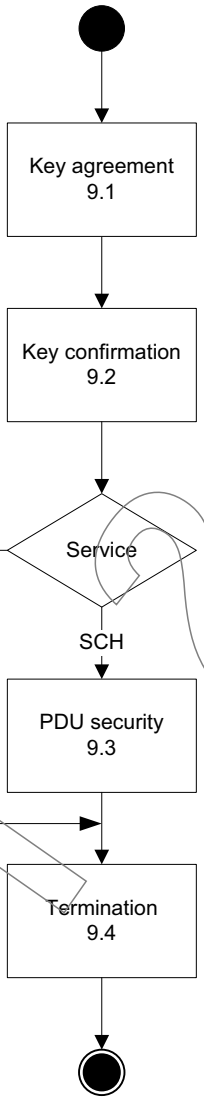


Figure 2 – General flow of the NFC-SEC service

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.

DRAFT 2009

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

11 NFC-SEC-PDUs

NFC-SEC-PDUs shall be conveyed in NFCIP-1 DEP "Secure Data" PDUs placing the SEP byte into byte 0 of the DEP transport data bytes. The DEP transport data bytes shall contain exactly one NFC-SEC-PDU.

The NFC-SEC-PDU structure is specified in Figure 3.

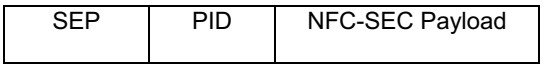


Figure 3 – Structure of NFC-SEC PDU

Table 2 specifies the *NFC-SEC-PDUs* fields as mandatory (m), prohibited (p), conditional (c). The conditionality (c) is further specied below.

Table 2 – *NFC-SEC-PDU* Fields

NFC-SEC-PDU	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.
- The RFU bits shall be set ZERO. Receivers shall reject PDUs with RFU bits set to ONE.

Figure 4 specifies the bit assignment.

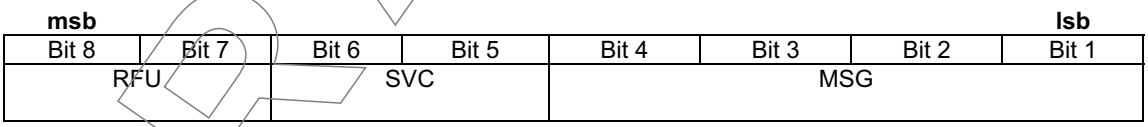


Figure 4 – Bit assignment of SEP

Table 3 specifies the coding of MSG. The codes not specified Table 3 are RFU.

DRAFT

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table 3 – PDU types and their MSG codes

Code	Name	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..

11.2 Protocol Identifier (PID)

PIDs are 8-bit values that identify NFC-SEC cryptography standards or specifications. PID values are registered at

http://www.ecma-international.org/publications/standards/Ecma-386.html.

The PID field is present in the ACT_REQ, but omitted in all other PDUs.

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 in all other PDUs depends on the PID and is specified in the respective NFC-SEC cryptography standard.

11.4 Terminate (TMN)

The TMN PDU consists of the SEP field only.

11.5 Error (ERROR)

The ERROR PDU starts with the SEP field and shall contain a zero-terminated byte string in the NFC-SEC Payload field.

12 Protocol Rules

This clause specifies rules for the NFC-SEC protocol.

12.1 Protocol 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.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PROOF

- 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 standard identified by the PID.
- The NFC-SEC cryptography standard identified by 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 standard identified by 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.

DRAFT 2009

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

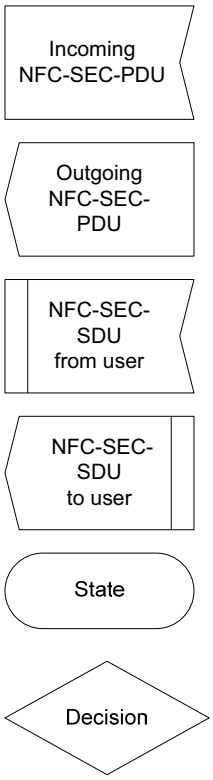
Annex A
(normative)

Protocol Machine Specification

The NFC-SEC protocol machine in this Annex specifies the sequence of PDUs to establish 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 NFCIP-1 entity.

NFC-SEC-PDU sent to the peer NFC-SEC entity, submitted to the local NFCIP-1 entity.

NFC-SEC-SDU obtained from the NFC-SEC User, requesting the NFC-SEC entity to perfom 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 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.

DRAFT 2009

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Retrieve Secret	Request the retrieval of a shared secret established. Admitted only to SSE.
Terminate	Request termination of service (type of service).

A.3 Confirm SDUs

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

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

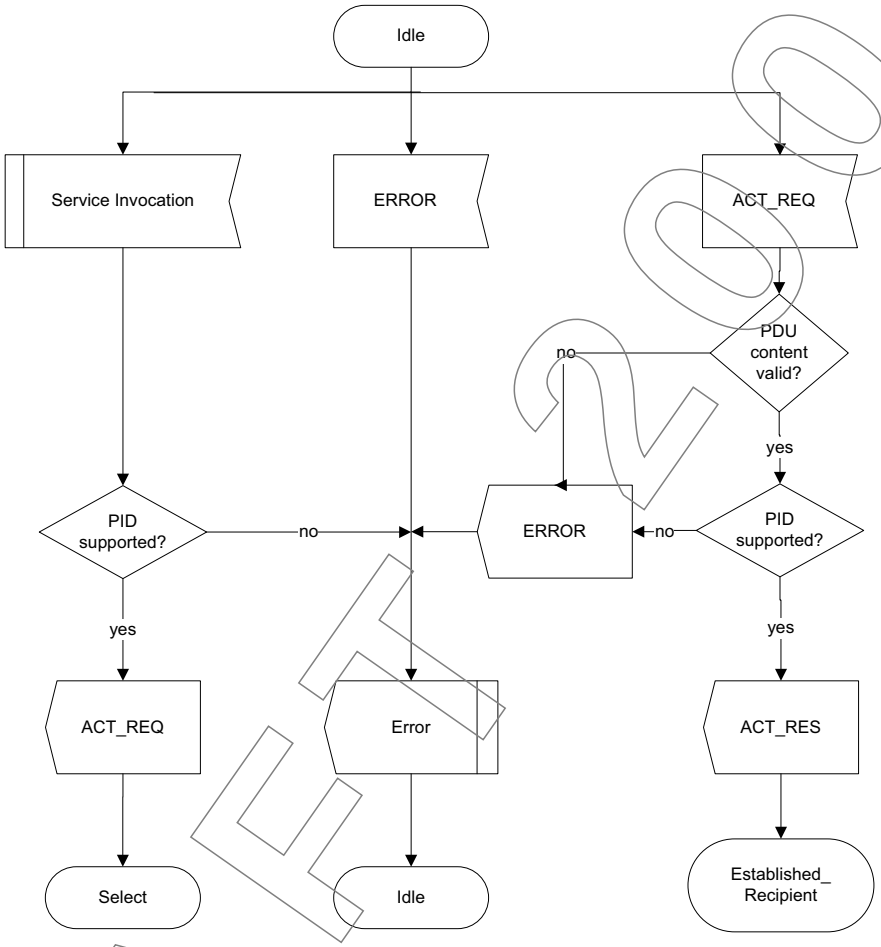
Established	Indicates the successful establishment of a service (type of service).
Data Sent	Indicates the result of a Send Data request (status). This result may be positive or negative, the latter due to a send error, or because the NFC-SEC entity was not ready for sending.
Data Available	Indicates the receipt of data.
Return Data	Response to a Retrieve Data request (data).
Return Secret	Response to a Retrieve Secret request (shared secret).
Terminated	Indicates to a user the termination of a service (type of service).
Error	Indicates an error during processing of a request or a PDU, or any other error. The parameters may reflect the error reason and details (details).

DRAFT 2009

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.4 SDL Diagrams

A.4.1 Idle State

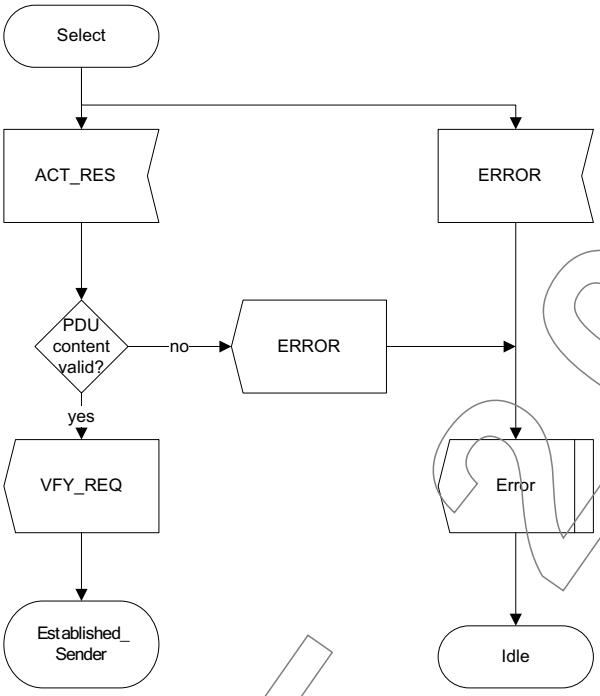


DRAFT 2009

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

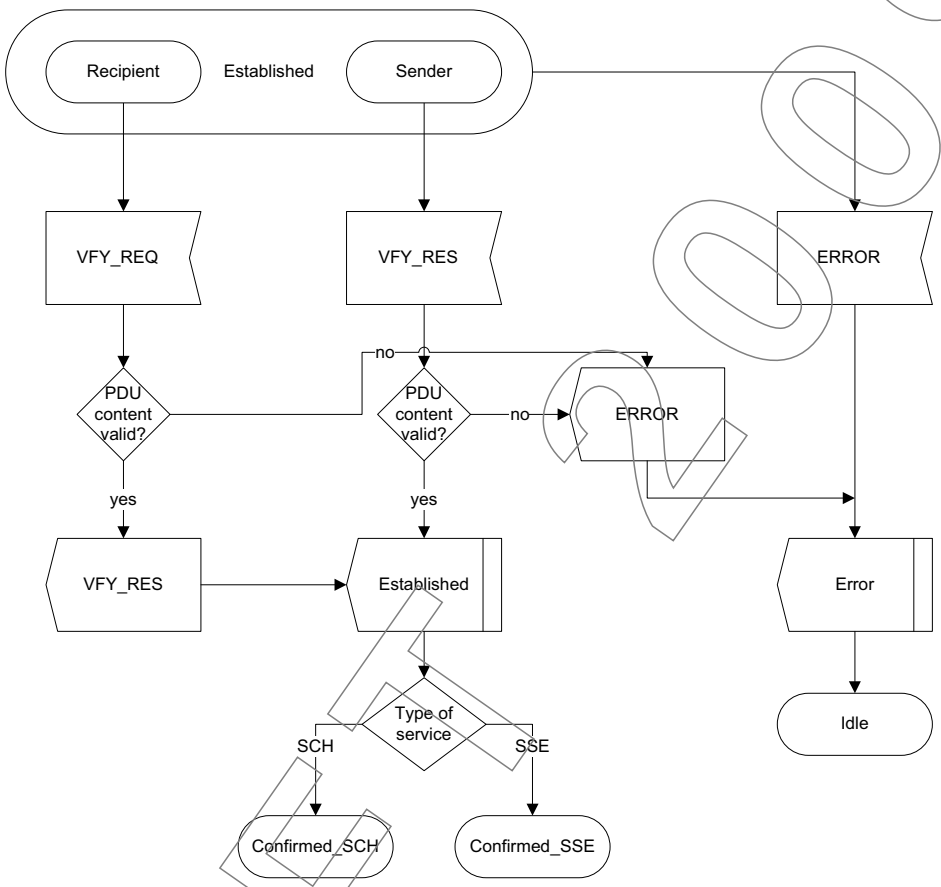
A.4.2 Select State



DRAFT 2009

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.4.3 Established State

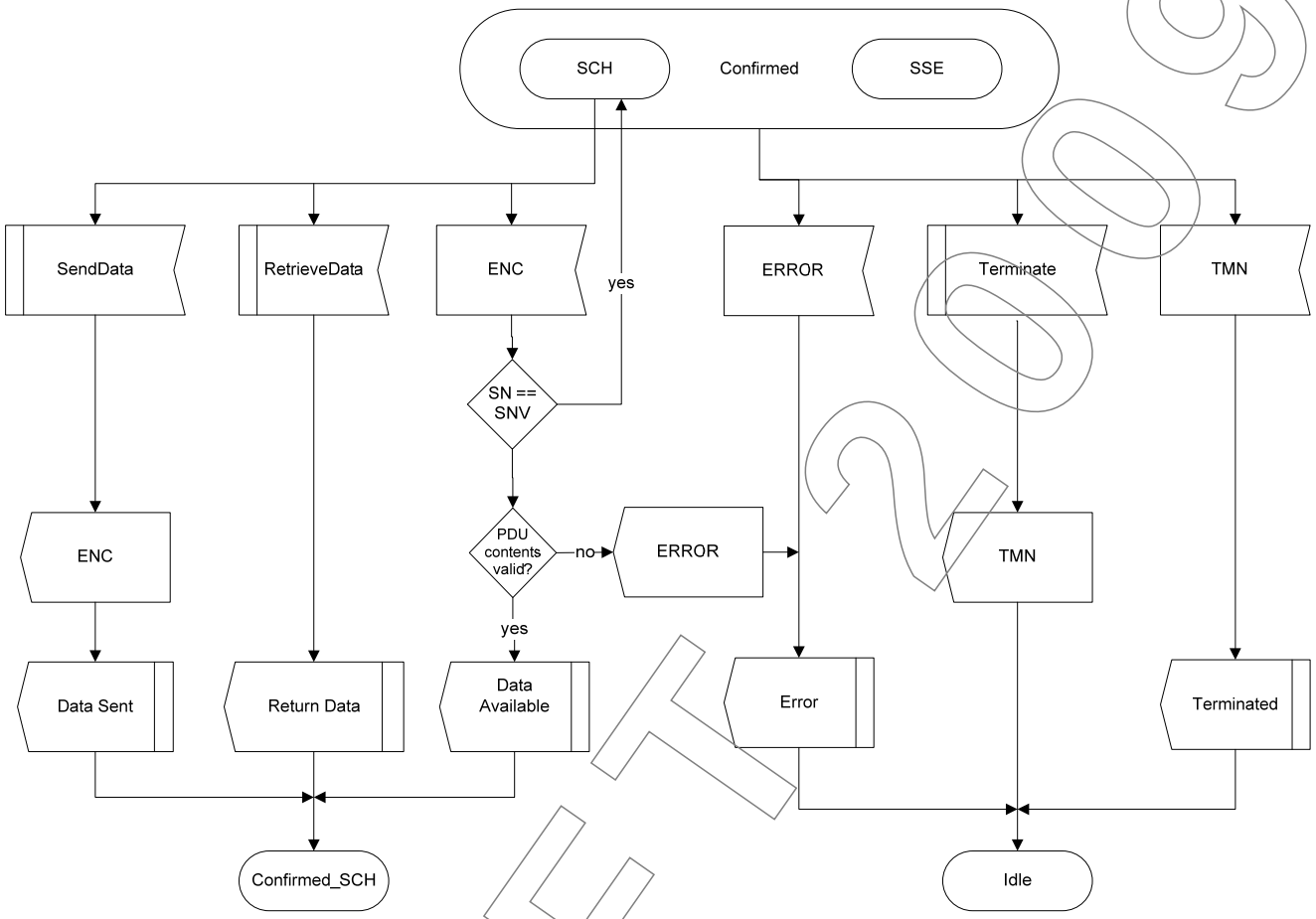


DRAFT 2009

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.4.4 Confirmed State



DRAFT 2009

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B
(normative)

Additional requirements for ECMA-340 (NFCIP-1)

When using this Standard for ECMA-340 implementations, the following additional requirements for ECMA-340:2004 shall apply until they are fully integrated into a new edition of the standard.

These additional requirements are stated in B.4 by amendments to ECMA-340:2004 and relate to the following functions:

B.1 The method by which NFCIP-1 devices indicate their support of NFC-SEC

An initiator indicates its support of NFC-SEC with the SECi field in the ATR_REQ.

A target indicates its support of NFC-SEC with the SECt field in the ATR_RES.

For the definitions of the SECi and SECt fields, see B.4.

B.2 Introduction of Protected PDU

Additional Protected PDUs are used in the data exchange protocol as specified in B.4.

B.3 Extension of PDU numbering rules for Protected PDU

Protected PDUs are included in the rules for numbering PDUs as specified in B.4.

B.4 NFCIP-1 amendments

The following amendments to ECMA-340:2004 shall apply:

Replace in 12.5.1.1.1 the definition of Byte 13: PPi, Figure 29 and Table 20 by the following:

"Byte13: PPi

The PPi byte specifies optional parameters used by Initiator device. The coding of bits is specified in Figure B.1.

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
SECi	RFU	LRi	LRi	RFU	RFU	Gi	NAD

Figure B.1 – Coding of the PPi byte

– bit 7: SECi. The initiator shall set SECi to ONE if it supports NFC-SEC; ZERO indicates no support

– bit6: RFU. The Initiator shall set it to ZERO. The Target shall ignore it.

– bit 5 and bit 4: Length Reduction value.

DRAFT 2009

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table B.1 – Definition of LRi

LRi	LEN_{MAX}
00	Transport data field max length is 64
01	Transport data field max length is 128
10	Transport data field max length is 192
11	Transport data field max length is 254

– bit 3 and bit 2: RFU. The Initiator shall set it to ZERO. The Target shall ignore it.

– bit 1: If bit is set to ONE then it indicates General bytes are available.

– bit 0: If bit is set to ONE then it indicates the Initiator uses NAD."

Replace in 12.5.1.2.1 the defnition of Byte 14: PPt, Figure 34 and Table 21 by the following:

"The PPt byte specifies optional parameters used by Target device. The coding of bits shall be as follows:

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
SECt	RFU	LRt	LRt	RFU	RFU	Gt	NAD

Figure B.2 – Coding of the PPt byte

– bit 7 SECt The target shall set SECt to ONE if it supports NFC-SEC; ZERO indicates no support

– bit 6: RFU. The Initiator shall set it to ZERO. The Target shall ignore it.

– bit 5 and bit 4: Length Reduction value.

Table B.2 – Definition of LRt

LRt	LEN_{MAX}
00	Transport data field max length is 64
01	Transport data field max length is 128
10	Transport data field max length is 192
11	Transport data field max length is 254

– bit 3 and bit 2: RFU. The Initiator shall set it to ZERO. The Target shall ignore it.

– bit 1: If bit is set to ONE then it indicates General bytes available.

– bit 0: If bit is set to ONE then it indicates the Target uses NAD."

Replace in 12.6.1.1.1 the defnition of Byte 0:PFB, Table 24 by the following

"Byte 0: PFB

The PFB byte shall contain bits to control the data transmission and error recovery. The PFB byte is used to convey the information required controlling the transmission. The data exchange protocol defines these fundamental types of PDU's:

– Information PDU's to convey information for the application layer.

– Protected PDU's to convey protected information

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

– Acknowledge PDU's to convey positive or negative acknowledgements. An Acknowledge PDU never contains a data field. The acknowledgement relates to the last received block.

– Supervisory PDU's to exchange control information between the Initiator and the Target. Two types of supervisory PDU's are defined.

  – Timeout extensions containing a 1 byte long data field.

  – Attention containing no data field.

The coding of PFB depends on its type and is defined in Table B.3.

Table B.3 – Coding of the PFB bits 7 to 5

bit 7	bit 6	bit 5	PFB
0	0	0	Information PDU
0	0	1	Protected PDU
0	1	0	Acknowledge PDU
1	0	0	Supervisory PDU
Other settings are RFU			

"

Add in 12.6.1.1.1 the defnition of a Protected PDU and add Figure B.3 as follows:

"Definition of the Protected PDU:

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
RFU	RFU	ONE	MI	NAD	DID	PNI	PNI

Figure B.3 – Coding of the Protected PDU

– bit 7 to bit 6: RFU. The Initiator shall set it to ZERO. The Target shall ignore it.

– Bit 5: Shall be set to ONE

– bit 4: If bit set to ONE then it indicates Multiple Information chaining activated.

– bit 3: If bit set to ONE then it indicates NAD available.

– bit 2: If bit set to ONE then it indicates DID available.

– bit 1 and bit 0: PNI packet number information.

The Packet Number Information (PNI) counts the number of packet send by the Initiator to the Target and vice versa starting by 0. These bytes are used for error detection during the protocol handling."

Replace 12.6.1.2 by the following:

"12.6.1.2 Handling of PDU number information

12.6.1.2.1 Initiator rules

The PNI of the Initiator shall be initialized for each Target with all ZEROs.

When an Information, Protected or Acknowledge PDU with an equal PNI is received, the Initiator shall increment the current PNI for that Target before optionally sending a new frame.

12.6.1.2.2 Target rules

The PNI of the Target shall be initialized with all ZEROs.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

When an Information, Protected or Acknowledge PDU with an equal PNI was received the Target shall send its response with this PNI and shall increment the PNI afterwards."

Replace 12.6.1.3.1 by the following:

"12.6.1.3.1 General rules

The first PDU shall be sent by the Initiator.

When an Information or Protected PDU indicating more information is received the PDU shall be acknowledged by an Acknowledge PDU (ACK) .

Supervisory PDUs are only used in pairs. A Supervisory Request shall always be followed by a Supervisory Response."

Replace 12.6.1.3.3 by the following:

"12.6.1.3.3 Target rules

The Target is allowed to send a Supervisory PDU (RTO) instead of an Information PDU.

When an Information or Protected PDU not containing chaining is received it shall be acknowledged by an Information or Protected PDU.

When an Acknowledge PDU (NACK) is received, if the PNI is equal to the PNI of the previous sent PDU, the previous block shall be re-transmitted.

When an erroneous PDU is received the Target shall not answer but stay in same State.

When a Supervisory PDU (Attention) is received, the Target shall respond sending a Supervisory PDU (Attention) response."

DRAFT 2009

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale