INTERNATIONAL STANDARD

ISO/IEC 13157-3

First edition
2016-04-01

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

Part 3: NFC-SEC cryptography standard using ECDH-256 and AES-GCM

Technologies de l'information — Téléinformatique — Sécurité NFC —

Partie 3: Norme de cryptographie NFC-SEC utilisant ECDH-256 et AES-GCM

Reference number
ISO/IEC 13157-3:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

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 13157-3 was prepared by Ecma International (as ECMA-409) 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.

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

— Part 3: NFC-SEC cryptography standard using ECDH-256 and AES-GCM

— Part 4: NFC-SEC entity authentication and key agreement using asymmetric cryptography

— Part 5: NFC-SEC entity authentication and key agreement using symmetric cryptography.

Introduction

The NFC Security series of standards comprise a common services and protocol Standard and NFC-SEC cryptography standards.

This NFC-SEC cryptography Standard specifies cryptographic mechanisms that use the Elliptic Curves Diffie-Hellman (ECDH-256) protocol for key agreement and the AES algorithm in GCM mode to provide data authenticated encryption.

This International Standard addresses secure communication of two NFC devices that do not share any common secret data ("keys") before they start communicating which each other. It is based on ISO/IEC 13157-2 (ECMA-386) with some adaptations to address actual cryptography standards.

This International Standard refers to the latest standards and updates the generation method for StartVar in compliance with ISO/IEC 19772:2009/Cor.1:2014 which also complies with NIST SP 800-38B.

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

Part 3: NFC-SEC cryptography standard using ECDH-256 and AES-GCM

1 Scope

This International Standard specifies the message contents and the cryptographic methods for PID 02.

This International Standard specifies cryptographic mechanisms that use the Elliptic Curves Diffie-Hellman (ECDH) protocol with a key length of 256 bits for key agreement and the AES algorithm in GCM mode to provide data authenticated encryption.

2 Conformance

Conformant implementations employ the security mechanisms specified in this NFC-SEC cryptography Standard (identified by PID 02) and conform to ISO/IEC 13157-1 (ECMA-385).

The NFC-SEC security services shall be established through the protocol specified in ISO/IEC 13157-1 (ECMA-385) and the mechanisms specified in this International Standard.

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 9797-1:2011, *Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher*

ISO/IEC 11770-3, *Information technology -- Security techniques -- Key management -- Part 3: Mechanisms using asymmetric techniques*

ISO/IEC 13157-1, *Information technology -- Telecommunications and information exchange between systems -- NFC Security -- Part 1: NFC-SEC NFCIP-1 security services and protocol* (ECMA-385)

ISO/IEC 13157-2, *Information technology -- Telecommunications and information exchange between systems -- NFC Security -- Part 2: NFC-SEC cryptography standard using ECDH and AES* (ECMA-386)

ISO/IEC 18031:2011, *Information technology -- Security techniques -- Random bit generation*

ISO/IEC 18031:2011/Cor.1:2014, *Information technology -- Security techniques -- Random bit generation -- Technical Corrigendum 1*

ISO/IEC 18033-3:2010, *Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers*

ISO/IEC 19772:2009*, Information technology -- Security techniques -- Authenticated encryption*

ISO/IEC 19772:2009/Cor.1:2014*, Information technology -- Security techniques -- Authenticated encryption -- Technical Corrigendum 1*

FIPS 186-4, *Digital Signature Standard (DSS)*

4 Terms and definitions

Clause 4 of ISO/IEC 13157-2 (ECMA-386) applies.

5 Conventions and notations

Clause 5 of ISO/IEC 13157-2 (ECMA-386) applies.

6 Acronyms

Clause 6 of ISO/IEC 13157-2 (ECMA-386) applies. Additionally, the following acronyms apply.

AAD	Additional Authenticated Data
GCM	Galois Counter Mode
CMAC	Cipher-based MAC

7 General

Clause 7 of ISO/IEC 13157-2 (ECMA-386) applies.

8 Protocol Identifier (PID)

This International Standard shall use the one octet protocol identifier PID with value 2.

9 Primitives

This Clause specifies cryptographic primitives. Clauses 11 and 12 specify the actual use of these primitives.

Table 1 summarizes the features.

Table 1 — Summary of features

Supported services	SSE (see ISO/IEC 13157-1 (ECMA-385)) SCH (see ISO/IEC 13157-1 (ECMA-385))
Key agreement	ECDH P-256
KDF	AES-CMAC-PRF-128
Key confirmation	AES-CMAC-96
Data authenticated encryption	AES128-GCM
Sequence integrity	SN (see ISO/IEC 13157-1 (ECMA-385))
Encryption order	Authenticated encryption (MAC then encrypt)

9.1 Key agreement

Clause 9.1 of ISO/IEC 13157-2 (ECMA-386) applies.

9.1.1 Curve P- 256

Curve P-256 as specified in *D.1.2.3 Curve P-256* of FIPS 186-4 shall be used.

9.1.2 EC Key Pair Generation Primitive

Clause 9.1.2 of ISO/IEC 13157-2 (ECMA-386) applies.

9.1.3 EC Public key validation

Clause 9.1.3 of ISO/IEC 13157-2 (ECMA-386) applies.

9.1.4 ECDH secret value derivation Primitive

Clause 9.1.4 of ISO/IEC 13157-2 (ECMA-386) applies.

9.1.5 Random nonces

Each peer NFC-SEC entity shall send fresh random nonces with the EC public key of the entity.

The entity shall guarantee that the nonces it generates have 128 bits of entropy valid for the duration of the protocol. The nonces used in an NFC-SEC transaction shall be cryptographically uncorrelated with the nonces from a previous transaction, see also ISO/IEC 18031.

9.2 Key Derivation Functions

Two Key Derivation Functions (KDF) are specified; one for the SSE and one for the SCH.

The PRF shall be AES in CMAC mode as specified in MAC algorithm 5 of ISO/IEC 9797-1, used with 128 bits output length, denoted AES-CMAC-PRF-128.

For the following sections PRF is:

PRF (K, S) = AES-CMAC-PRF-128K (S)

The random source (nonces and the SharedSecret z obtained from 9.1.4) used for the SCH shall be different from the random source used for the SSE.

9.2.1 KDF for the SSE

The KDF for the SSE is:

$$\mathrm{MK_{SSE}} = \text{KDF-SSE}\ (\mathrm{Nonce_S}, \mathrm{Nonce_R}, \mathrm{ID_S}, \mathrm{ID_R}, \mathrm{SharedSecret})$$

Detail of the KDF-SSE function:

$$\mathrm{Seed} = (\mathrm{Nonce_S}\ [1..64]\ ||\ \mathrm{Nonce_R}\ [1..64])$$

$$\mathrm{SKEYSEED} = \mathrm{PRF}\ (\mathrm{Seed}, \mathrm{SharedSecret})$$

$$\mathrm{MK_{SSE}} = \mathrm{PRF}\ (\mathrm{SKEYSEED}, \mathrm{Seed}\ ||\ \mathrm{ID_S}\ ||\ \mathrm{ID_R}\ ||\ (01))$$

9.2.2 KDF for the SCH

The KDF for the SCH is:

$$\{\mathrm{MK_{SCH}}, \mathrm{K_{SCH}}\} = \text{KDF-SCH}\ (\mathrm{Nonce_S}, \mathrm{Nonce_R}, \mathrm{ID_S}, \mathrm{ID_R}, \mathrm{SharedSecret})$$

Detail of the KDF-SCH function:

$$\mathrm{Seed} = (\mathrm{Nonce_S}\ [1..64]\ ||\mathrm{Nonce_R}\ [1..64])$$

$$\mathrm{SKEYSEED} = \mathrm{PRF}\ (\mathrm{Seed}, \mathrm{SharedSecret})$$

$$\mathrm{MK_{SCH}} = \mathrm{PRF}\ (\mathrm{SKEYSEED}, \mathrm{Seed}\ ||\ \mathrm{ID_S}\ ||\ \mathrm{ID_R}\ ||\ (01))$$

$$\mathrm{K_{SCH}} = \mathrm{PRF}\ (\mathrm{SKEYSEED}, \mathrm{MK_{SCH}}\ ||\ \mathrm{Seed}\ ||\ \mathrm{ID_S}\ ||\ \mathrm{ID_R}\ ||\ (02))$$

9.3 Key Usage

Each derived key $\mathrm{MK_{SCH}}$, $\mathrm{K_{SCH}}$ and $\mathrm{MK_{SSE}}$ shall be used only for the purpose specified in Table 2.

The Keys $\mathrm{MK_{SCH}}$, $\mathrm{K_{SCH}}$, and $\mathrm{MK_{SSE}}$ shall be different for each NFC-SEC transaction.

Table 2 — Key usage

Key	**Key description**	**Key usage**
$\mathrm{MK_{SCH}}$	Master Key for SCH	Key Verification for the Secure Channel Keys
$\mathrm{K_{SCH}}$	Authenticated Encryption Key for SCH	Authenticated Encryption of data packets sent through SCH
$\mathrm{MK_{SSE}}$	Master Key for SSE	Master Key for SSE used as Shared secret to be passed to the upper layer and as Key Verification

9.4 Key Confirmation

When a key is derived using one of the KDF processes specified in 9.2 both NFC-SEC entities check that they indeed have the same key. Each entity shall generate a key confirmation tag as specified in 9.4.1 and shall send it to the peer entity. Entities shall verify the key confirmation tag upon reception as specified in 9.4.2.

This key confirmation mechanism is according to *9, Key Confirmation,* of ISO/IEC 11770-3*.*

9.4.1 Key confirmation tag generation

MacTag, the Key confirmation tag, equals

MAC-KC (K, MsgID, IDS, IDR, PKS, PKR) and shall be calculated using
AES-CMAC-96$_K$ (MsgID || ID$_S$ || ID$_R$ || PK$_S$ || PK$_R$), specified in MAC algorithm 5 of ISO/IEC 9797-1 with 96-bit truncated output in msb-first order, with key K.

The MsgID field is specified at each invocation of MAC-KC.

9.4.2 Key confirmation tag verification

Clause 9.4.2 of ISO/IEC 13157-2 (ECMA-386) applies.

9.5 Data Authenticated Encryption

The underlying block cipher used is AES as specified in *5.1 AES* of ISO/IEC 18033-3 with a block size of 128 bits.

The data authenticated encryption mode shall be GCM mode as specified in *11 Authenticated encryption mechanism 6 (GCM)* of ISO/IEC 19772.

9.5.1 Starting Variable (StartVar)

To ensure that Starting Variable StartVar is distinct for every message to be protected, it shall be generated by both entities from the nonces in the following way:

StartVal shall be generated using bit [17..112] of AES-CMAC-PRF-128$_{MK}$ (MK, K$_{SCH}$ || NA || NB || (03)), with the key MK.

9.5.2 Additional Authenticated Data (AAD)

This data is only authenticated, but not encrypted.

AAD = SEP || PID || S3 || S2 || S1

The 3-octect value of SNV equals S3 || S2 || S1 where S1 is the LSB and S3 is the MSB.

For the NFC-SEC-PDUs where PID is prohibited (see *Table 2 – NFC-SEC-PDU Fields* of ISO/IEC 13157-1 (ECMA-385), PID is replaced by one byte (00).

9.5.3 Generation-Encryption

The data shall be authenticated and encrypted using the Secure Channel Key K$_{SCH}$ as specified in *11.6 Encryption procedure* of ISO/IEC 19772 with t = 96:

AuthEncData = GEN-ENC$_{KSCH}$ (AAD, StartVar, Data)

9.5.4 Decryption-Verification

The authenticated and encrypted data shall be decrypted and verified using the Secure Channel Key K$_{SCH}$ as specified in *11.7 Decryption procedure* of ISO/IEC 19772 with t = 96:

DEC-VER$_{KSCH}$ (AAD, StartVar, AuthEncData) shall return Data' if valid

INVALID otherwise

9.6 Data Integrity

The requirements in 9.5.3 and 9.5.4 provide data integrity.

9.7 Message Sequence Integrity

Clause 9.7 of ISO/IEC 13157-2 (ECMA-386) applies.

10 Data Conversions

Clause 10 of ISO/IEC 13157-2 (ECMA-386) applies.

11 SSE and SCH service invocation

Clause 11 of ISO/IEC 13157-2 (ECMA-386) applies.

12 SCH data exchange

After invocation of the SCH as specified in 11, the data exchange between two NFC-SEC entities uses the protocol specified in ISO/IEC 13157-1 (ECMA-385) as illustrated in Figure 1 and further specified in this Clause.

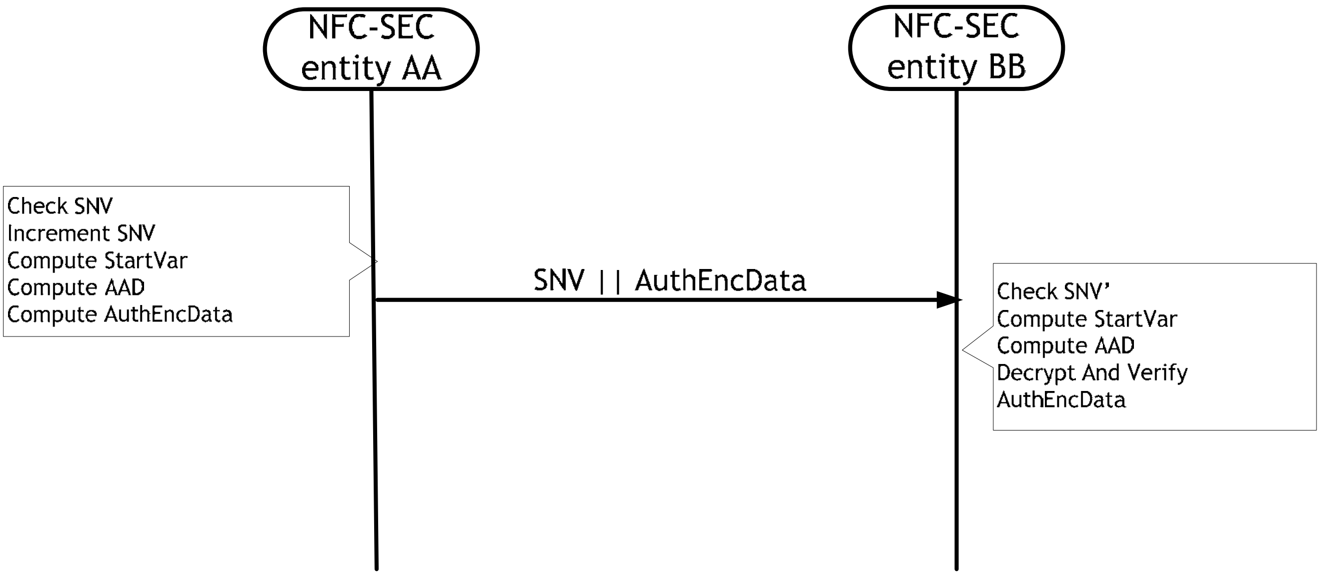

Figure 1 — SCH: protocol overview

12.1 Preparation

NFC-SEC entities A and B shall initialise the Sequence Number variable (SNV) as specified in 9.7.

NFC-SEC senders shall initialise the Starting Variable (StartVar) as specified in 9.5.1.

12.2 Data Exchange

12.2.1 Send

To send data, the sending NFC-SEC peer entity AA (A or B) shall perform the following steps:

1. Receive UserData from the SendData SDU.
2. If SNV = 2^{24}-1, then set the 'PDU content valid' to false in the Protocol Machine, otherwise proceed to the next step.
3. Increment the SNV as specified in 12.3 of ISO/IEC 13157-1 (ECMA-385).
4. Compute StartVar as specified in 9.5.1.
5. Compute AAD as specified in 9.5.3.
6. Compute AuthEncData = GEN-ENC$_{\text{KSCH}}$ (AAD, StartVar, Data) as specified in 9.5.3.
7. Send S3 || S2 || S1 || AuthEncData as the payload of the ENC PDU.

12.2.2 Receive

To receive data, the receiving NFC-SEC peer entity BB (A or B) shall perform the following steps:

1. Receive S3 || S2 || S1 || AuthEncData from the payload of the ENC PDU.
2. If SNV = 2^{24}-1, then set the 'PDU content valid' to false in the Protocol Machine, otherwise proceed to the next step.
3. Check the sequence integrity as specified in 12.3 of ISO/IEC 13157-1 (ECMA-385).
4. Compute StartVar as specified in 9.5.1.
5. Compute AAD as specified in 9.5.3.
6. Compute DEC-VER$_{\text{KSCH}}$ (AAD, StartVar, AuthEncData) as specified in 9.5.4. If it is invalid, then set the 'PDU content valid' to false in the Protocol Machine, otherwise proceed to the next step.
7. Set UserData into the DataAvailable SDU.

Annex A
(normative)

Fields sizes

Table A.1 — Fields sizes

Field	Size
NA	128 bits
NB	128 bits
d_A	256 bits
d_B	256 bits
Q_A	512 bits
Q_B	512 bits
QA	264 bits
QB	264 bits
Z	256 bits
MK	128 bits
K	128 bits
$MacTag_A$	96 bits
$MacTag_B$	96 bits
StartVar	96 bits
SN	24 bits

ICS 35.110

Price based on 8 pages