Standard ECMA-409

1st Edition / December 2014

NFC-SEC-02: NFC-SEC Cryptography Standard using ECDH-256 and AES-GCM

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

Contents

Page

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 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 Ecma Standard has been adopted by the General Assembly of December 2014.

NFC-SEC-02: NFC-SEC Cryptography Standard using ECDH-256 and AES-GCM

1 Scope

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

This 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 Standard.

3 Normative references

The following referenced documents are indispensable for the application 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 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 18031:2005, *Information technology -- Security techniques -- Random bit generation*

ISO/IEC 18033-3:2005, *Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers*

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

FIPS 186-3, *Digital Signature Standard (DSS)*

NIST SP 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*

RFC 4494, *The AES-CMAC-96 Algorithm and Its Use with IPsec*

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 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 186-3 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 CMAC as specified in NIST SP 800-38B, used with 128 bits output length. It will be denoted AES-CMAC-PRF-128.

For the following sections PRF is:

$$\text{PRF (K, S)} = \text{AES-CMAC-PRF-128K (S)}$$

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:

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

Detail of the KDF-SSE function:

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

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

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

9.2.2 KDF for the SCH

The KDF for the SCH is:

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

Detail of the KDF-SCH function:

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

$$SKEYSEED = PRF\ (Seed, SharedSecret)$$

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

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

9.3 Key Usage

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

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

Table 2 — Key usage

Key	Key description	Key usage
MK_{SCH}	Master Key for SCH	Key Verification for the Secure Channel Keys
K_{SCH}	Authenticated Encryption Key for SCH	Authenticated Encryption of data packets sent through SCH
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.

The MAC used for Key Confirmation (MacTag) shall be AES in CMAC-96 mode as specified in RFC 4494.

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
$\text{AES-CMAC-96}_K\ (MsgID\ ||\ ID_S\ ||\ ID_R\ ||\ PK_S\ ||\ PK_R)$, specified in RFC 4494, 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 from the SNV, defined in 9.7, in the following way:

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

The StartVal shall equal the 96 bit string: S1 || S2 || S3 || S2 || S3 || S1 || S3 || S1 || S2 || S3 || S2 || S1.

9.5.2 Additional Authenticated Data (AAD)

This data is only authenticated, but not encrypted.

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

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.

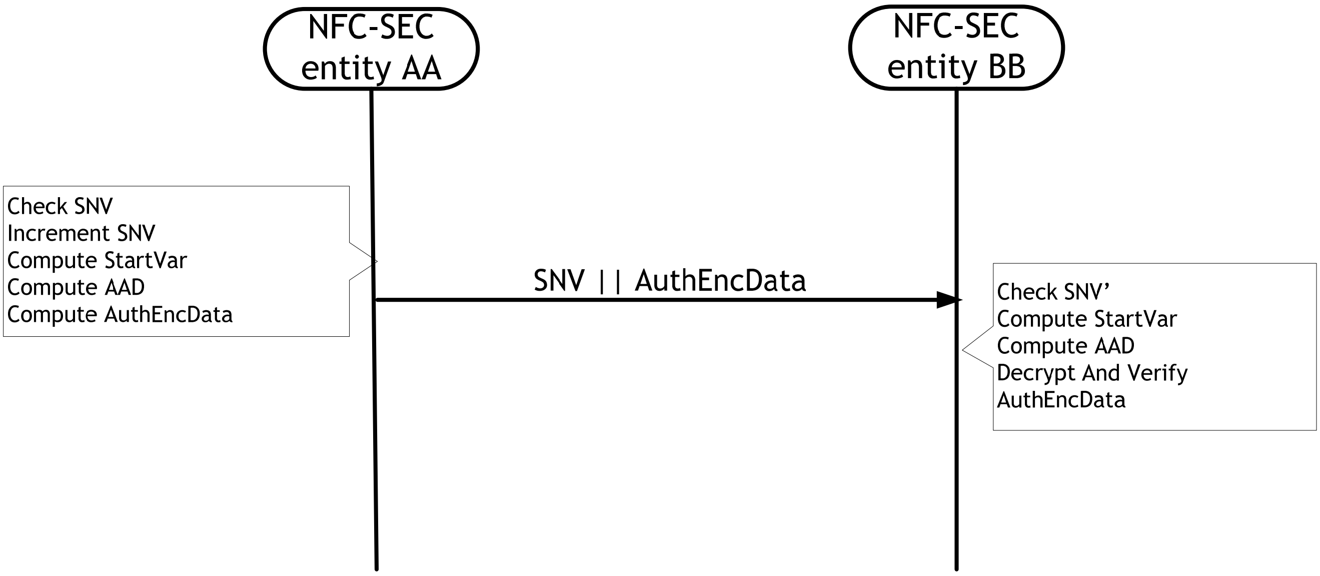

Figure 1 — SCH: protocol overview

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$_{KSCH}$ (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$_{KSCH}$ (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