ecma INTERNATIONAL

Standard ECMA-411

2nd Edition / June 2015

NFC-SEC-04: NFC-SEC Entity Authentication and Key Agreement using Symmetric Cryptography

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 an NFC Entity Authentication (NEAU) mechanism that uses the symmetric cryptographic algorithm (NEAU-S) for mutual authentication of two NFC entities.

This Standard addresses entity authentication of two NFC entities possessing a Pre-Shared Authentication Key (PSAK) during the key agreement and confirmation for the Shared Secret Service (SSE) and Secure Channel Service (SCH).

This Standard adds entity authentication to the services provided by ISO/IEC 13157-3 (ECMA-409) NFC-SEC-02.

This 2nd edition refers to the latest standards and the StarVar generation method for IV in NFC-SEC-02.

This Ecma Standard has been adopted by the General Assembly of June 2015.

NFC-SEC-04: NFC-SEC Entity Authentication and Key Agreement using Symmetric Cryptography

1 Scope

This Standard specifies the message contents and the cryptographic mechanisms for PID 04.

This Standard specifies key agreement and confirmation mechanisms providing mutual authentication, using symmetric cryptography.

NOTE This Standard adds entity authentication to the services provided by ISO/IEC 13157-3 (ECMA-409) NFC-SEC-02.

2 Conformance

Conformant implementations employ the security mechanisms specified in this NFC-SEC cryptography Standard (identified by PID 04) 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 7498-1:1994, *Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model*

ISO/IEC 9798-1:2010, *Information technology -- Security techniques -- Entity authentication -- Part 1: General*

ISO/IEC 9798-2:2008, *Information technology -- Security techniques -- Entity authentication -- Part 2: Mechanisms using symmetric encipherment algorithms*

ISO/IEC 11770-1:2010, *Information technology -- Security techniques -- Key management -- Part 1: Framework*

ISO/IEC 11770-2:2008, *Information technology -- Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques*

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 13157-3, *Information technology -- Telecommunications and information exchange between systems -- NFC Security -- Part 3: NFC-SEC Cryptography Standard using ECDH-256 and AES-GCM* (ECMA-409)

ISO/IEC 14443-3, *Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anticollision*

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 18092, *Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1)* (ECMA-340)

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*

4 Terms and definitions

Clause 4 of ISO/IEC 13157-3 (ECMA-409) applies. Additionally, the following terms and definitions apply.

4.1
entity authentication
corroboration that an entity is the one claimed

[ISO/IEC 9798-1: 2010]

4.2
n-entity-title
a name that is used to identify unambiguously an n-entity

[ISO/IEC 7498-1: 1994]

4.3
symmetric cryptography (symmetric cryptographic technique)
cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation

[ISO/IEC 9798-1: 2010]

5 Conventions and notations

Clause 5 of ISO/IEC 13157-3 (ECMA-409) applies. Additionally, the following conversions and notations following apply.

$\oplus$ exclusive OR

For any message field “F”, F denotes the value placed in the field upon sending, F’ the value upon receipt.

6 Acronyms

Clause 6 of ISO/IEC 13157-3 (ECMA-409) applies. Additionally, the following acronyms apply.

KEIA	Encryption and Integrity Key in Authentication
MKA	Master Key in Authentication
NEAU-S	NEAU using Symmetric Cryptography
PSAK	Pre-Shared Authentication Key
TLV	Type-length-value
UID	Unique Identifier [ISO/IEC 14443-3]
ZSEED	The Seed of Z

7 General

This Standard specifies the NFC Entity Authentication using Symmetric cryptography (NEAU-S), using the key agreement and confirmation protocol in ISO/IEC 13157-1 (ECMA-385).

To enable a key agreement and confirmation mechanism providing mutual authentication between NFC entities before they start the Shared Secret Service (SSE) and the Secure Channel Service (SCH), the Pre-Shared Authentication Key (PSAK), as a credential, between these entities is used in the entity authentication. After successful NEAU-S completion, a shared secret Z that is used to establish the SSE and the SCH will be generated.

Three-pass authentication per ISO/IEC 9798-2, mechanism 4, and key establishment per ISO/IEC 11770-2, mechanism 6, are used in NEAU-S.

The relationship between NEAU-S and ISO/IEC 13157-1 (ECMA-385) is shown in Figure 1.

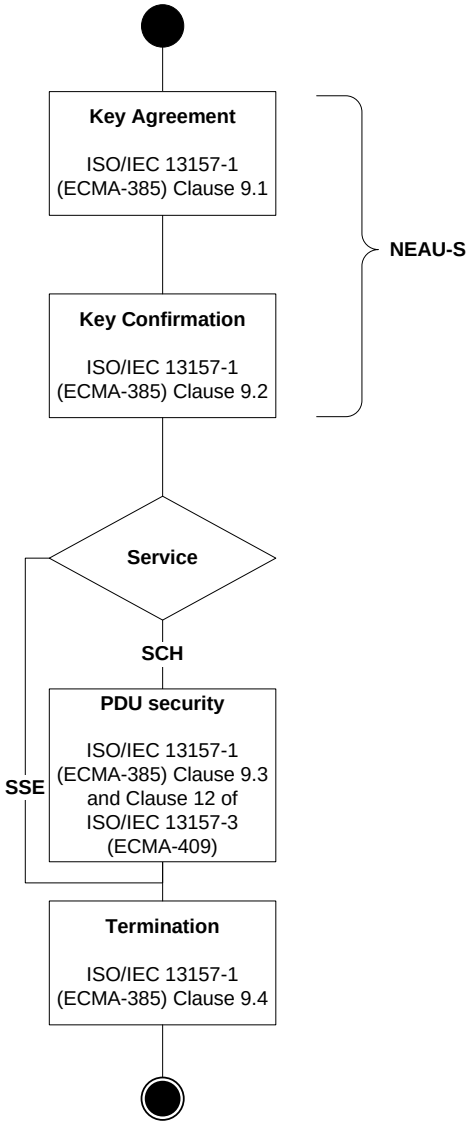

Figure 1 — The use of the NFC-SEC protocol by NEAU-S

8 Fields and PDUs for NEAU-S

8.1 Protocol Identifier (PID)

This Standard shall use the one octet protocol identifier PID with value 4.

8.2 NFC-SEC-PDUs

The peer NFC-SEC entities shall establish a shared secret Z using ACT_REQ, ACT_RES, VFY_REQ and VFY_RES according to the NEAU-S mechanism.

8.3 Entity identifiers

The n-entity-title of the Sender's and Recipient's n-entity shall be used as ID_S and ID_R, respectively. Figure 2 specifies the encoding of ID_S and ID_R in the TLV format.

	Type	Length	Value
Octets:	1	2	variable

Figure 2 — ID format

1. The Type subfield specifies the type of the ID and shall be 1 octet in length. The values are:

   a) 1: Value subfield contains Sender (A) identification number, ID_S;

   b) 2: Value subfield contains Recipient (B) identification number, ID_R;

   c) All other values are RFU.

2. The 2-octet Length subfield contains the length in number of octets of the Value subfield, in the range of 1 to 65535.

9 Primitives

9.1 General requirements

Clause 9 specifies cryptographic primitives of NEAU-S. Clause 10 specifies the actual use of these primitives. Table 1 specifies the size and description of parameters.

Table 1 — NEAU-S parameters

Parameter	Field Size	Description
PSAK	Variable	Pre-Shared authentication key available to the Sender (A) and the Recipient (B).
MKA	128 bits	Master key used in the entity authentication and derived from the PSAK.
KEIA	128 bits	Encryption and integrity key used in the entity authentication and derived from the MKA.
MAC	96 bits	Message authentication code.
ID_S	Variable	The Sender (A) identification number.
ID_R	Variable	The Recipient (B) identification number.
NA	128 bits	See Clause 6 of ISO/IEC 13157-2 (ECMA-386).
NB	128 bits	See Clause 6 of ISO/IEC 13157-2 (ECMA-386).
Z	256 bits	See Clause 6 of ISO/IEC 13157-2 (ECMA-386).
$ZSEED_S$	256 bits	The Sender's seed for the derivation of the shared secret Z.
$ZSEED_R$	256 bits	The Recipient's seed for the derivation of the shared secret Z.
MK	128 bits	See Clause 6 of ISO/IEC 13157-2 (ECMA-386).
K	128 bits	See Clause 6 of ISO/IEC 13157-2 (ECMA-386).
IV	96 bits	Initial value of counter.

ISO/IEC 18031 shall be used to generate the random nonces and keys, with the exception of Dual_EC_DRBG.

9.2 Entity authentication

9.2.1 Mechanism

Peer NFC-SEC entities achieve mutual authentication per ISO/IEC 9798-2, mechanism 4 by use of the PSAK which shall be known to them prior to the commencement of the NEAU-S mechanism.

9.2.2 AES

AES per 5.1 of ISO/IEC 18033-3 shall be used for encryption, decryption and MACing during the entity authentication.

9.2.3 Modes of operation

In the NEAU-S mechanism, the data authenticated encryption mode shall be GCM mode per *11 Authenticated encryption mechanism 6 (GCM)* of ISO/IEC 19772.

9.2.4 Message Authentication Code (MAC)

MACing shall be used for integrity protection of the payload of ACT_RES, VFY_REQ and VFY_RES.

9.3 Key agreement

The shared secret Z shall be established using key establishment from ISO/IEC 11770-2, mechanism 6, which requires both entities to contribute their seeds.

9.4 Key confirmation

9.4.1 Overview

The MK shall be derived using the KDF per 9.2 of ISO/IEC 13157-3 (ECMA-409). This key confirmation mechanism is according to Clause 9 of ISO/IEC 11770-3. The MAC used for Key Confirmation (MacTag) shall be AES in CMAC-96 mode per ISO/IEC 13157-3 (ECMA-409).

9.4.2 Key confirmation tag generation

The $MacTag_A$ in VFY_REQ shall be:

$$MacTag_A = AES\text{-}CMAC\text{-}96_{MK}(MK, (02) \,||\, ID_S \,||\, ID_R \,||\, NA \,||\, NB),$$

using $AES\text{-}CMAC\text{-}96_{MK}$ per ISO/IEC 13157-3 (ECMA-409), with key MK.

The $MacTag_B$ in VFY_RES shall be:

$$MacTag_B = AES\text{-}CMAC\text{-}96_{MK}(MK, (03) \,||\, ID_R \,||\, ID_S \,||\, NB \,||\, NA),$$

using $AES\text{-}CMAC\text{-}96_{MK}$ per ISO/IEC 13157-3 (ECMA-409), with key MK.

9.4.3 Key confirmation tag verification

The $MacTag_A$ shall be checked by evaluating the equation:

$$MacTag_A' = AES\text{-}CMAC\text{-}96_{MK}(MK, (02) \,||\, ID_S \,||\, ID_R \,||\, NA' \,||\, NB)$$

The $MacTag_B$ shall be checked by evaluating the equation:

$$MacTag_B' = AES\text{-}CMAC\text{-}96_{MK} (MK, (03) || ID_R || ID_S || NB' || NA)$$

9.5 Key Derivation Function (KDF)

9.5.1 Overview

Four KDFs are specified in NEAU-S for generating:

- MKA and KEIA;
- the shared secret Z;
- key of SSE and
- key of SCH.

9.5.2 KDF for MKA and KEIA

The PRF shall be CMAC per 9.2 of ISO/IEC 13157-3 (ECMA-409), used with 128 bits output length. It will be denoted AES-CMAC-PRF-128. For the following sections PRF is:

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

The KDF for the MKA and KEIA shall be:

$$\{MKA, KEIA\} = KDF\text{-}MKA\text{-} KEIA (NA, NB, ID_S, ID_R, PSAK)$$

Detail of the KDF-MKA- KEIA function:

$$Seed = (NA [1..64] || NB [1..64])$$

$$SKEYSEED = PRF(Seed, PSAK)$$

$$MKA = PRF (SKEYSEED, Seed || ID_S || ID_R || (01))$$

$$KEIA = PRF (SKEYSEED, MKA || Seed || ID_S || ID_R || (02))$$

The keys MKA and KEIA shall be different for each NEAU-S invocation.

9.5.3 KDF for the shared secret Z

The value of the shared secret Z shall be generated per a) of Annex C of ISO/IEC 11770-2:

$$Z = ZSEED_S \oplus ZSEED_R$$

9.5.4 KDF for the SSE and SCH

9.2.1 and 9.2.2 of ISO/IEC 13157-3 (ECMA-409) apply.

9.6 Data authenticated encryption during authentication

9.6.1 Initial values (IV)

Both entities shall calculate AES-CMAC-PRF-128$_{MK}$ per 9.5.1 of per ISO/IEC 13157-3 (ECMA-409), where MK equals MKA.

Both entities shall set their IV for AuthEncData$_R$ to AES-CMAC-PRF-128$_{MK}$[1..96], their IV for SCH to AES-CMAC-PRF-128$_{MK}$[17..112] and their IV for AuthEncData$_S$ to AES-CMAC-PRF-128$_{MK}$[33..128].

9.6.2 Additional Authenticated Data (AAD)

This data is only authenticated, but not encrypted.

AAD = SEP || PID

9.6.3 NEAU-S payload encryption and MAC generation

The data shall be authenticated and encrypted using KEIA as specified in *11.6 Encryption procedure* of ISO/IEC 19772:

AuthEncData = ENC$_{KEIA}$ (AAD, IV, Data), with t = 96.

The AuthEncData$_R$ in ACT_RES shall be:

AuthEncData$_R$ = ENC$_{KEIA}$ (AAD, IV, NB || NA' || ID$_R$ || ID$_S$ || ZSEED$_R$).

AuthEncData$_R$ contains the encrypted data EncData$_R$ and MAC$_R$. The MAC$_R$ length is 96 bits.

The AuthEncData$_S$ in VFY_REQ shall be:

AuthEncData$_S$ = ENC$_{KEIA}$ (AAD, IV, NA || NB' || ID$_S$ || ID$_R$ || ZSEED$_S$).

AuthEncData$_S$ contains the encrypted data EncData$_S$ and MAC$_S$. The MAC$_S$ length is 96 bits.

9.6.4 NEAU-S payload decryption and MAC verification

The authenticated and encrypted data shall be decrypted and verified using KEIA as specified in *11.7 Decryption procedure* of ISO/IEC 19772:

DEC$_{KEIA}$ (AAD, IV, AuthEncData) shall return Data' if valid

INVALID otherwise

The EncData$_R$' and MAC$_R$' in ACT_RES shall be:

NB' || NA || ID$_R$' || ID$_S$' || ZSEED$_R$' || MAC$_R$' = DEC$_{KEIA}$ (AAD, IV, AuthEncData$_R$').

The EncData$_S$' and MAC$_S$' in VFY_REQ shall be:

NA' || NB || ID$_S$' || ID$_R$' || ZSEED$_S$' || MAC$_S$' = DEC$_{KEIA}$ (AAD, IV, AuthEncData$_S$').

10 NEAU-S mechanism

10.1 Protocol overview

NEAU-S mechanism is illustrated in Figure 3. During the NEAU-S, if any check fails, then 'PDU content valid' shall be set to false.

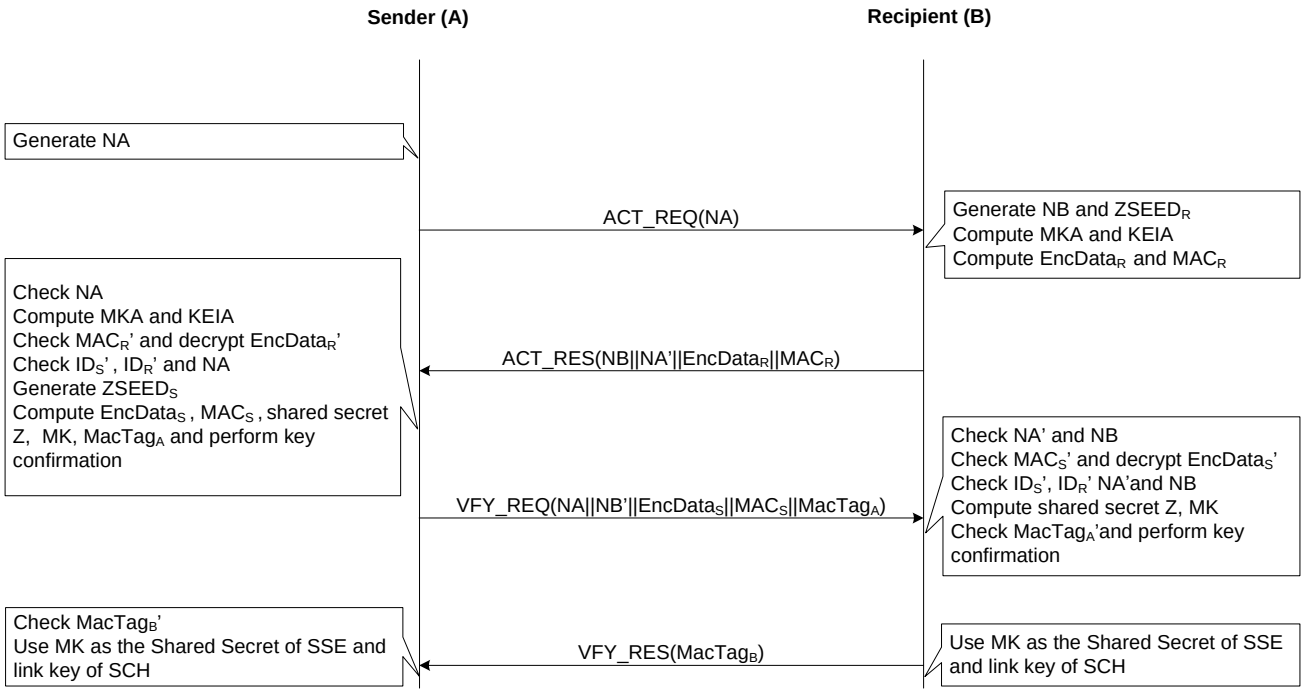

Figure 3 — NEAU-S mechanism overview

10.2 Preparation

Before starting the NEAU-S mechanism, the followings shall be available to each NFC-SEC entity:

- Its own PSAK. PSAK is a static key that is distributed to the NFC entities by a method outside the scope of this Standard. Guidance on the management of pre-shared authentication keys is provided in ISO/IEC 11770-1 and ISO/IEC 11770-2.
- Each NFC-SEC entity shall be in possession of its own and its peer's n-entity-title.

  NOTE The NFCIP-1-entity-title is the nfcid3 per ISO/IEC 18092, the 14443-3-entity-title is the UID.

10.3 Sender (A) transformation

1. Generate a nonce NA per 9.1.5 of ISO/IEC 13157-3 (ECMA-409).
2. Send NA as the payload of the ACT_REQ.
3. Receive NB' || NA || EncData$_R$' || MAC$_R$' from the payload of the ACT_RES.
4. Perform the following:

a) check if the random number NA sent to the Recipient (B) in the payload of the ACT_REQ is the same as received in the ACT_RES;

b) derive keys MKA and KEIA per 9.5.2;

c) decipher $EncData_R$' and verify the value of MAC_R' per 9.6.4, obtain the values of NB', NA, ID_R', ID_S' and $ZSEED_R$', then verify that the ID_R' and ID_S' equal the respective n-entity-title values specified in 10.2;

d) check that the random number NA sent to the Recipient (B) in the payload of the ACT_REQ and the random number NB' received from the Recipient (B) in the payload of the ACT_RES are the same as the received in the $EncData_R$'.

5. Compute the value of $EncData_S$ and MAC_S per 9.6.3, generating the nonce $ZSEED_S$ per 9.1.5 of ISO/IEC 13157-3 (ECMA-409).

6. Generate the shared secret Z per 9.5.3.

7. Compute the MK and $MacTag_A$ per 9.2 of ISO/IEC 13157-2 (ECMA-386) and 9.4.2 respectively.

8. Send NA || NB' || $EncData_S$ || MAC_S || $MacTag_A$ as the payload of the VFY_REQ.

9. Receive $MacTag_B$' from the payload of the VFY_RES.

10. Check the key confirmation tag received from Recipient (B): $MacTag_B$'(MK) per 9.4.3.

11. Set the 'PDU content valid' to true, use MK as the Shared Secret of SSE and link key of SCH respectively.

10.4 Recipient (B) transformation

1. Receive NA' from the payload of the ACT_REQ.

2. Generate a nonce NB and the seed $ZSEED_R$ per 9.1.5 of ISO/IEC 13157-3 (ECMA-409).

3. Derive keys MKA and KEIA per 9.5.2.

4. Compute the value of $EncData_R$ and MAC_R per 9.6.3.

5. Send NB || NA' || $EncData_R$ || MAC_R as the payload of the ACT_RES.

6. Receive NA' || NB || $EncData_S$' || MAC_S' || $MacTag_A$' from the payload of the VFY_REQ.

7. Perform the following:

a) check if the random numbers NA' and NB sent to the Sender (A) in the payload of the ACT_RES are the same as received in the VFY_REQ;

b) decipher $EncData_S$' and verify the value of MAC_S' per 9.6.4, obtain the values of NA', NB, ID_S', ID_R' and $ZSEED_S$', then verify that the ID_R' and ID_S' equal the respective n-entity-title values specified in 10.2;

c) check that the random numbers NA' and NB sent to the Sender (A) in the payload of the ACT_RES are the same as received in the $EncData_S$'.

8. Generate the shared secret Z per 9.5.3.

9. Compute the MK and check the key confirmation tag received from Sender (A): $MacTag_A$' (MK) per 9.2 of ISO/IEC 13157-3 (ECMA-409) and 9.4.3 respectively.

10. Compute $MacTag_B$ per 9.4.2 and send it as the payload of the VFY_RES.

11. Set the 'PDU content valid' to true, use MK as the Shared Secret of SSE and link key of SCH respectively.

11 Data Authenticated Encryption in SCH

Clause 12 of ISO/IEC 13157-3 (ECMA-409) applies.