INTERNATIONAL STANDARD

ISO/IEC 13157-4

First edition
2016-06-15

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

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

Technologies de l'information — Télécommunications et échange d'information entre systèmes — Sécurité NFC —
Partie 4: Authentification d'entité NFC-SEC et accord de clés utilisant une cryptographie asymétrique

Reference number
ISO/IEC 13157-4:2016(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 World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

ISO/IEC 13157-4 was prepared by Ecma International (as ECMA-410) 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 an NFC Entity Authentication (NEAU) mechanism that uses the asymmetric cryptography algorithm (NEAU-A) for mutual authentication of two NFC entities.

This International Standard addresses entity authentication of two NFC entities possessing certificates and private keys during key agreement and key confirmation for the Shared Secret Service (SSE) and Secure Channel Service (SCH).

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

This International Standard refers to the latest standards.

The holders of these patent rights have assured the ISO and IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world.

In this respect, the statements of the holders of these patent rights are registered with ISO and IEC.

Information on the declared patents may be obtained from:

Patent Holder: China IWNCOMM Co., Ltd.
Address: A201, QinFengGe, Xi'an Software Park, No. 68, Keji 2nd Road, Xi'an Hi-Tech Industrial, Development Zone, Xi'an, Shaanxi, P. R. China 710075

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

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

1 Scope

This International Standard specifies the message contents and the cryptographic mechanisms for PID 03.

This International Standard specifies key agreement and confirmation mechanisms providing mutual authentication, using asymmetric cryptography, and the transport protocol requirements for the exchange between Sender and TTP.

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

2 Conformance

Conformant NFC-SEC entities employ the security mechanisms and the transport protocol requirements specified in this NFC-SEC cryptography Standard (identified by PID 03) and conform to ISO/IEC 13157-1 (ECMA-385).

Conformant TTP implementations employ the security mechanisms and the transport protocol requirements specified in this NFC-SEC cryptography Standard (identified by PID 03).

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 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 9798-3, *Information technology -- Security techniques -- Entity authentication -- Part 3: Mechanisms using digital signature techniques*

ISO/IEC 10118-3:2004, *Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions*

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 14888-3:2006, *Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms*

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

ITU-T Recommendation X.509, ISO/IEC 9594-8, *Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks.*

4 Terms and definitions

For the purposes of this document, the terms and definitions given in Clause 4 of ISO/IEC 13157-3 (ECMA-409) and the following apply.

4.1
asymmetric cryptography (asymmetric cryptographic technique)
cryptographic technique that uses two related transformations: a public transformation (defined by the public key) and a private transformation (defined by the private key)

NOTE The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation.

[ISO/IEC 9798-1: 2010]

4.2
certificate
public key information of an entity signed by the certification authority and thereby rendered unforgeable

[ISO/IEC 9798-1: 2010]

4.3
digital signature (signature)
data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient

[ISO/IEC 9798-1: 2010]

4.4
entity authentication
corroboration that an entity is the one claimed

[ISO/IEC 9798-1: 2010]

4.5
n-entity-title
a name that is used to identify unambiguously an n-entity

[ISO/IEC 7498-1: 1994]

4.6
trusted third party
security authority or its agent, trusted by other entities with respect to security related activities

[ISO/IEC 9798-1: 2010]

NOTE In this International Standard, a trusted third party is trusted by a Sender and Recipient for the purposes of certificate validation.

5 Conventions and notations

Clause 5 of ISO/IEC 13157-3 (ECMA-409) applies.

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.

CertA	Certificate of A
CertB	Certificate of B
CertTTP	Certificate of TTP
CPA	Public Key of Certificate of A
CPB	Public Key of Certificate of B
CPTTP	Public Key of Certificate of TTP
CSA	Private Key corresponding to Certificate of A
CSB	Private Key corresponding to Certificate of B
CSTTP	Private Key corresponding to Certificate of TTP
Dual_EC_DRBG	Dual Elliptic Curve Deterministic Random Bit Generator
ECDSA	Elliptic Curve Digital Signature Algorithm
IP	Internet Protocol
k	Fresh random value in ECDSA
NEAU	NFC Entity Authentication
NEAU-A	NEAU using Asymmetric Cryptography
OCSP	Online Certificate Status Protocol
q	224-bit prime number of a divisor of the curve order in ECDSA

r, s	Digital Signature value of ECDSA
ResA	Validation result of A
ResB	Validation result of B
SHA	Secure Hash Algorithm
SigA	Digital Signature generated by A
SigB	Digital Signature generated by B
SigTTP	Digital Signature generated by TTP
TTP PolicyX	TTP policy of entity X [see 8.3]
TLV	Type-length-value
UDP	User Datagram Protocol
UID	Unique Identifier [ISO/IEC 14443-3]
TAEP	Tri-element Authentication Extensible Protocol
TAEP_REQ	TAEP Request PDU
TAEP_RES	TAEP Response PDU
TTP	Trusted Third Party involved in the authentication

7 General

This International Standard specifies the NFC Entity Authentication using Asymmetric cryptography (NEAU-A), using the key agreement and confirmation protocol of ISO/IEC 13157-1 (ECMA-385). NEAU-A specifies negotiation of authentication either involving a TTP per 6.2 of ISO/IEC 9798-3 or without TTP per 5.2.2 of ISO/IEC 9798-3.

Authentication credentials shall be Public Key Certificates conforming to ISO/IEC 9594-8 / ITU X.509.

NOTE It is outside the scope of this International Standard how the certificates and the related private keys are issued and established.

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

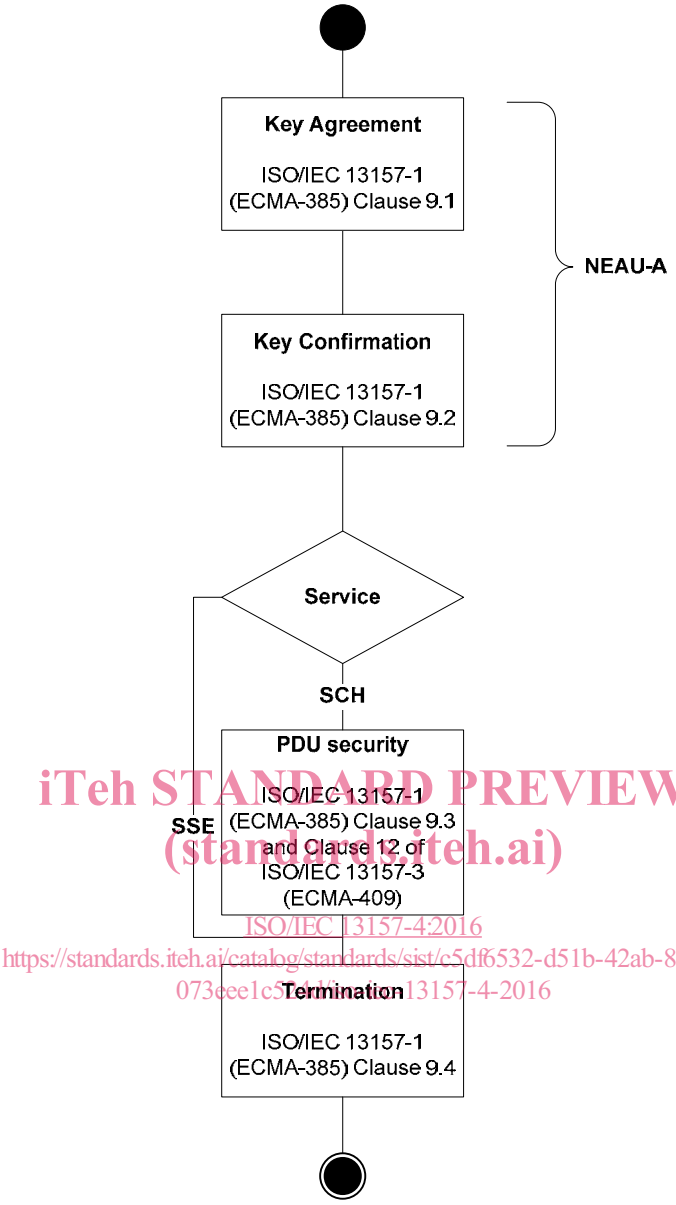

Figure 1 — The use of the NFC-SEC protocol by NEAU-A

8 Fields and PDUs for NEAU-A

8.1 Protocol Identifier (PID)

This International Standard shall use the one octet protocol identifier PID with value 3.

8.2 NFC-SEC-PDUs

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

8.3 TTP involving

8.3.1 TTP policy and field

TTP $Policy_X$ specifies the entity policy regarding the involvement of the TTP in NEAU-A. The payload of ACT_REQ and ACT_RES shall contain the 1-octect TTP field encoding the TTP $Policy_X$ as follows:

a) 0: TTP to be involved;

b) 1: TTP not to be involved;

c) 2: No preference;

d) All other values are RFU.

8.3.2 TTP policy negotiation

The NEAU-A mechanism provides a method for TTP policy negotiation. Peer NFC-SEC entities shall negotiate whether or not to involve the TTP, in accordance with their TTP $Policy_X$.

The Sender (A) shall include a TTP field in the ACT_REQ with the value (0, 1 or 2) according to its TTP $Policy_A$. If the TTP is unavailable (see 10.1.2) then the values 0 and 2 are prohibited. The value 2 shall be replaced by 1, and if the value is 0 then 'PDU content valid' shall be set to false.

Upon receiving the ACT-REQ, the Recipient (B) shall perform policy negotiation as specified in Table 1; if the Result is False then the Recipient shall set 'PDU content valid' to false, for the Result of 0 or 1, the Recipient (B) shall set the TTP field in the ACT-RES to the Result and shall continue with step 3 of 10.1.4 or step 4 of 10.2.4 respectively.

The Sender (A) shall validate the TTP field in the ACT-RES:

- If it equals 2, then set 'PDU content valid' to false;

Otherwise, evaluate Table 1; if the Result is False then set 'PDU content valid' to false, for the Result of 0 or 1 continue with step 6 of 10.1.3 or 10.2.3 respectively.

Table 1 — Results of the TTP policy negotiation

TTP Field	TTP Policy	Result
0	TTP to be involved	0
0	TTP not to be involved	False
0	No preference	0
1	TTP to be involved	False
1	TTP not to be involved	1
1	No preference	1
2	TTP to be involved	0
2	TTP not to be involved	1
2	No preference	0