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/IEC 2016



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 v
Introduction vi
1 Scope 1
2 Conformance 1
3 Normative references 1
4 Terms and definitions 1
5 Conventions and notations 3
6 Acronyms 3
7 General 4
8 Fields and PDUs for NEAU-A 5
8.1 Protocol Identifier (PID) 5
8.2 NFC-SEC-PDUs 5
8.3 TTP involving 6
8.3.1 TTP policy and field 6
8.3.2 TTP policy negotiation 6
8.4 Entity identifiers 7
8.5 Cert field 7
8.6 Res field 7
9 Primitives 8
9.1 General requirements 8
9.2 Entity authentication 9
9.2.1 Mechanisms 9
9.2.2 EC curve 10
9.2.3 ECDSA 10
9.2.4 Certificate validation 12
9.3 Key agreement 13
9.4 Key confirmation 13
9.5 Key Derivation Function (KDF) 13
10 NEAU-A mechanism 13
10.1 Entity authentication involving a TTP 13
10.1.1 Protocol overview 13
10.1.2 Preparation 14
10.1.3 Sender (A) transformation 14
10.1.4 Recipient (B) transformation 16
10.1.5 TTP transformation 17
10.2 Entity authentication without involving a TTP 17
10.2.1 Protocol overview 17
10.2.2 Preparation 17
10.2.3 Sender (A) transformation 18
10.2.4 Recipient (B) transformation 19
10.3 Key derivation 20
10.3.1 Sender (A) 20
10.3.2 Recipient (B) 20
11 Data Authenticated Encryption in SCH 20
Annex A (normative) UDP Port 5111 and TAEP 21
A.1 UDP and port 5111 21

© ISO/IEC 2016 — All rights reserved

A.1.1 UDP 21
A.1.2 Port 5111 21
A.2 TAEP 22
A.2.1 TAEP packet format 22
A.2.2 TAEP_REQ and TAEP_RES format 22
Annex B (informative) ECDSA test vectors 24
Bibliography 27

 © ISO/IEC 2016 — All rights reserved

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.

© ISO/IEC 2016 — All rights reserved

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

© ISO/IEC 2016 — All rights reserved

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 2016 — All rights reserved

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]

© ISO/IEC 2016 — All rights reserved

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

© ISO/IEC 2016 — All rights reserved