INTERNATIONAL STANDARD

ISO/IEC 13157-5

First edition
2016-06-15

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

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

Technologies de l'information — Télécommunications et échange d'information entre systèmes — Sécurité NFC —

Partie 5: Authentification d'entité NFC-SEC et accord de clés utilisant une cryptographie symétrique

Reference number
ISO/IEC 13157-5:2016(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 iv
Introduction v
1 Scope 1
2 Conformance 1
3 Normative references 1
4 Terms and definitions 1
5 Conventions and notations 2
6 Acronyms 3
7 General 3
8 Fields and PDUs for NEAU-S 4
8.1 Protocol Identifier (PID) 4
8.2 NFC-SEC-PDUs 4
8.3 Entity identifiers 4
9 Primitives 5
9.1 General requirements 5
9.2 Entity authentication 6
9.2.1 Mechanism 6
9.2.2 AES 6
9.2.3 Modes of operation 6
9.2.4 Message Authentication Code (MAC) 6
9.3 Key agreement 6
9.4 Key confirmation 6
9.4.1 Overview 6
9.4.2 Key confirmation tag generation 6
9.4.3 Key confirmation tag verification 6
9.5 Key Derivation Function (KDF) 7
9.5.1 Overview 7
9.5.2 KDF for MKA and KEIA 7
9.5.3 KDF for the shared secret Z 7
9.5.4 KDF for the SSE and SCH 7
9.6 Data authenticated encryption during authentication 8
9.6.1 Initial values (IV) 8
9.6.2 Additional Authenticated Data (AAD) 8
9.6.3 NEAU-S payload encryption and MAC generation 8
9.6.4 NEAU-S payload decryption and MAC verification 8
10 NEAU-S mechanism 9
10.1 Protocol overview 9
10.2 Preparation 9
10.3 Sender (A) transformation 9
10.4 Recipient (B) transformation 10
11 Data Authenticated Encryption in SCH 11

© 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 13157-5 was prepared by Ecma International (as ECMA-411) 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 symmetric cryptographic algorithm (NEAU-S) for mutual authentication of two NFC entities.

This International 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 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 and the StarVar generation method for IV in NFC-SEC-02.

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

1 Scope

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

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

NOTE This International 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 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 9798-2, *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 2016 — All rights reserved

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

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
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.

© ISO/IEC 2016 — All rights reserved