INTERNATIONAL STANDARD

ISO/IEC 13157-2

Second edition
2016-04-01

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

Part 2: NFC-SEC cryptography standard using ECDH and AES

Technologies de l'information — Téléinformatique — Sécurité NFC — Partie 2: Norme de cryptographie NFC-SEC utilisant ECDH et AES

Reference number
ISO/IEC 13157-2:2016(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 2
5 Conventions and notations 2
5.1 Concatenation 2
5.2 Hexadecimal numbers 2
6 Acronyms 2
7 General 3
8 Protocol Identifier (PID) 3
9 Primitives 3
9.1 Key agreement 4
9.1.1 Curve P-192 4
9.1.2 EC Key Pair Generation Primitive 4
9.1.3 EC Public key validation 4
9.1.4 ECDH secret value derivation Primitive 4
9.1.5 Random nonces 4
9.2 Key Derivation Functions 5
9.2.1 KDF for the SSE 5
9.2.2 KDF for the SCH 5
9.3 Key Usage 5
9.4 Key Confirmation 6
9.4.1 Key confirmation tag generation 6
9.4.2 Key confirmation tag verification 6
9.5 Data Encryption 6
9.5.1 Initial value of counter (IV) 6
9.5.2 Encryption 6
9.5.3 Decryption 7
9.6 Data Integrity 7
9.6.1 Protect data integrity 7
9.6.2 Check data integrity 7
9.7 Message Sequence Integrity 7
10 Data Conversions 7
10.1 Integer-to-Octet-String Conversion 7
10.2 Octet-String-to-Integer Conversion 7
10.3 Point-to-Octet-String Conversion 8
10.4 Octet-String-to-Point Conversion 8
11 SSE and SCH service invocation 8
11.1 Pre-requisites 9
11.2 Key Agreement 10
11.2.1 Sender (A) Transformation 10
11.2.2 Recipient (B) Transformation 10
11.3 Key Derivation 11
11.3.1 Sender (A) Transformation 11

© ISO/IEC 2016 — All rights reserved

11.3.2 Recipient (B) Transformation 11
11.4 Key Confirmation 11
11.4.1 Sender (A) Transformation 11
11.4.2 Recipient (B) Transformation 12

12 SCH data exchange 12
12.1 Preparation 13
12.2 Data Exchange 13
12.2.1 Send 13
12.2.2 Receive 13

Annex A (normative) AES-XCBC-PRF-128 and AES-XCBC-MAC-96 algorithms 15
A.1 AES-XCBC-PRF-128 15
A.2 AES-XCBC-MAC-96 15

Annex B (normative) Fields sizes 16

Annex C (informative) Informative references 17

 © 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 WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

ISO/IEC 13157-2 was prepared by Ecma International (as ECMA-386) 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.

This second edition cancels and replaces the first edition (ISO/IEC 13157-2:2010) which has been technically revised.

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*[1]

— *Part 4: NFC-SEC entity authentication and key agreement using asymmetric cryptography*[1]

— *Part 5: NFC-SEC entity authentication and key agreement using symmetric cryptography*[1]

[1] To be published.

© 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 cryptographic mechanisms that use the Elliptic Curves Diffie-Hellman (ECDH) protocol for key agreement and the AES algorithm for data encryption and integrity.

This International Standard addresses secure communication of two NFC devices that do not share any common secret data ("keys") before they start communicating which each other.

This edition ensures to use the latest references to cryptographic standards.

© ISO/IEC 2016 — All rights reserved

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

Part 2: NFC-SEC cryptography standard using ECDH and AES

1 Scope

This International Standard specifies the message contents and the cryptographic methods for PID 01.

This International Standard specifies cryptographic mechanisms that use the Elliptic Curves Diffie-Hellman (ECDH) protocol for key agreement and the AES algorithm for data encryption and integrity.

2 Conformance

Conformant implementations employ the security mechanisms specified in this NFC-SEC cryptography Standard (identified by PID 01) 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 documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 10116, *Information technology -- Security techniques -- Modes of operation for an n-bit block cipher*

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 15946-1, *Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 1: General*

ISO/IEC 18031, *Information technology -- Security techniques -- Random bit generation*

ISO/IEC 18033-3, *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)

IEEE 1363, *IEEE Standard Specifications for Public-Key Cryptography*

© ISO/IEC 2016 — All rights reserved

FIPS 186-4, *Digital Signature Standard (DSS)*

4 Terms and definitions

For the purposes of this International Standard, all terms and definitions from ISO/IEC 13157-1 (ECMA-385) apply.

5 Conventions and notations

The conventions and notations of ISO/IEC 13157-1 (ECMA-385) as well as the following apply in this document unless otherwise stated.

5.1 Concatenation

A || B represents the concatenation of the fields A and B: content of A followed by content of B.

5.2 Hexadecimal numbers

(XY) denotes a hexadecimal number XY (i.e. with the Radix of 16) and each pair of characters is encoded in one octet.

6 Acronyms

For the purposes of this International Standard, all acronyms from ISO/IEC 13157-1 (ECMA-385) apply. Additionally, the following acronyms apply.

A	Sender, as specified in ISO/IEC 13157-1 (ECMA-385)
AES	Advanced Encryption Standard
B	Receiver, as specified in ISO/IEC 13157-1 (ECMA-385)
d_A	Sender's private EC key
d_B	Recipient's private EC key
DataLen	Length of the UserData
EC	Elliptic Curve
ECDH	Elliptic Curve Diffie-Hellman
EncData	Encrypted data
G	The base point on EC
ID_A	Sender nfcid3
ID_B	Recipient nfcid3
ID_R	Any Recipient identification number (e.g. ID_B)
ID_S	Any Sender identification number (e.g. ID_A)
IV	Initial Value
K	Key
KDF	Key Derivation Function
KE	Encryption Key
KI	Integrity Key

© ISO/IEC 2016 — All rights reserved