INTERNATIONAL STANDARD

ISO/IEC 13157-3

First edition
2016-04-01

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

Part 3: NFC-SEC cryptography standard using ECDH-256 and AES-GCM

Technologies de l'information — Téléinformatique — Sécurité NFC —

Partie 3: Norme de cryptographie NFC-SEC utilisant ECDH-256 et AES-GCM

Reference number
ISO/IEC 13157-3:2016(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 2
5 Conventions and notations 2
6 Acronyms 2
7 General 2
8 Protocol Identifier (PID) 2
9 Primitives 2
9.1 Key agreement 3
9.1.1 Curve P- 256 3
9.1.2 EC Key Pair Generation Primitive 3
9.1.3 EC Public key validation 3
9.1.4 ECDH secret value derivation Primitive 3
9.1.5 Random nonces 3
9.2 Key Derivation Functions 3
9.2.1 KDF for the SSE 4
9.2.2 KDF for the SCH 4
9.3 Key Usage 4
9.4 Key Confirmation 4
9.4.1 Key confirmation tag generation 5
9.4.2 Key confirmation tag verification 5
9.5 Data Authenticated Encryption 5
9.5.1 Starting Variable (StartVar) 5
9.5.2 Additional Authenticated Data (AAD) 5
9.5.3 Generation-Encryption 5
9.5.4 Decryption-Verification 5
9.6 Data Integrity 6
9.7 Message Sequence Integrity 6
10 Data Conversions 6
11 SSE and SCH service invocation 6
12 SCH data exchange 6
12.1 Preparation 6
12.2 Data Exchange 7
12.2.1 Send 7
12.2.2 Receive 7
Annex A (normative) Fields sizes 8

© 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 13157-3 was prepared by Ecma International (as ECMA-409) 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 cryptographic mechanisms that use the Elliptic Curves Diffie-Hellman (ECDH-256) protocol for key agreement and the AES algorithm in GCM mode to provide data authenticated encryption.

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. It is based on ISO/IEC 13157-2 (ECMA-386) with some adaptations to address actual cryptography standards.

This International Standard refers to the latest standards and updates the generation method for StartVar in compliance with ISO/IEC 19772:2009/Cor.1:2014 which also complies with NIST SP 800-38B.

© ISO/IEC 2016 — All rights reserved

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

Part 3: NFC-SEC cryptography standard using ECDH-256 and AES-GCM

1 Scope

This International Standard specifies the message contents and the cryptographic methods for PID 02.

This International Standard specifies cryptographic mechanisms that use the Elliptic Curves Diffie-Hellman (ECDH) protocol with a key length of 256 bits for key agreement and the AES algorithm in GCM mode to provide data authenticated encryption.

2 Conformance

Conformant implementations employ the security mechanisms specified in this NFC-SEC cryptography Standard (identified by PID 02) 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 9797-1:2011, *Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a 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 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 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 2016 — All rights reserved

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*

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

4 Terms and definitions

Clause 4 of ISO/IEC 13157-2 (ECMA-386) applies.

5 Conventions and notations

Clause 5 of ISO/IEC 13157-2 (ECMA-386) applies.

6 Acronyms

Clause 6 of ISO/IEC 13157-2 (ECMA-386) applies. Additionally, the following acronyms apply.

AAD	Additional Authenticated Data
GCM	Galois Counter Mode
CMAC	Cipher-based MAC

7 General

Clause 7 of ISO/IEC 13157-2 (ECMA-386) applies.

8 Protocol Identifier (PID)

This International Standard shall use the one octet protocol identifier PID with value 2.

9 Primitives

This Clause specifies cryptographic primitives. Clauses 11 and 12 specify the actual use of these primitives.

Table 1 summarizes the features.

© ISO/IEC 2016 — All rights reserved