DRAFT INTERNATIONAL STANDARD ISO/IEC 13157-2

Attributed to ISO/IEC JTC 1 by the Central Secretariat

Voting begins on
2015-09-14

Voting terminates on
2015-12-14

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОММИСИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

FAST-TRACK PROCEDURE

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

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

Titre manque

Partie 2:

ICS 35.110

This draft International Standard is submitted for JTC 1 national body vote under the "fast-track" procedure.

In accordance with Resolution 30 of the JTC 1 Berlin Plenary 1993, the proposer of this document recommends assignment of ISO/IEC 13157-2 to JTC 1/SC 6.

The procedures used to develop this document are described in the ISO/IEC Directives, Part 1 - Consolidated JTC 1 Supplement.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

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.

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 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.

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 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 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*

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

MAC	Message Authentication Code
Mac_A /Mac_B	Integrity protection value of Sender/ Recipient
MacTag_A	Key confirmation tag from Sender
MacTag_B	Key confirmation tag from Recipient
MK	Master Key
NA / NB	Nonce generated by Sender/Recipient
NAA / NBB	Nonce generated by the pair of NFC-SEC entities
Nonce_S	Sender's nonce
Nonce_R	Recipient's nonce
PK	Public Key
PK_R	Recipient's Public Key
PK_S	Sender's Public Key
PRNG	Pseudo Random Number Generator
QA / QB	Compressed EC public key of Sender / Recipient
Q_A / Q_B	Decompressed EC public key of Sender / Recipient
RNG	Random Number Generator
SharedSecret	Shared secret
UserData	NFC-SEC User data
z	Unsigned integer representation of the Shared Secret
Z	Octet string representation of z

The acronyms used in Clauses 9 and 10 not listed above are formal parameters.

7 General

This International Standard specifies mechanisms for the Shared Secret Service (SSE) and the Secure Channel Service (SCH) in ISO/IEC 13157-1 (ECMA-385).

To enable secure communication between NFC devices that do not share any common secret data ("keys") before they start communicating with each other, public key cryptography is used to establish a shared secret between these devices, and more specifically the Elliptic Curve Diffie-Hellman key exchange scheme. This shared secret is used to establish the SSE and the SCH.

8 Protocol Identifier (PID)

This International Standard shall use the one octet protocol identifier PID with value 1.

9 Primitives

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

Table 1 summarizes the features.