INTERNATIONAL STANDARD

ISO/IEC 13157-1

Second edition
2014-08-15

Corrected version
2014-11-15

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

Part 1: NFC-SEC NFCIP-1 security services and protocol

Technologies de l'information — Téléinformatique — Sécurité NFC — Partie 1: Services de sécurité et protocole NFC-SEC NFCIP-1

Reference number
ISO/IEC 13157-1:2014(E)

COPYRIGHT PROTECTED DOCUMENT

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.

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 13157-1 was prepared by Ecma International (as ECMA-385) 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 13157-1:2010), 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.*

This corrected version of ISO 13157-1:2014 incorporates the following corrections:

5.1, last list item: the underlined part has been added:

— In octets the lsb is bit number 1, the msb <u>is</u> bit number 8; <u>in n-length bit strings the lsb is bit number 1 and the msb is bit number n.</u>

Introduction

This International Standard specifies common NFC Security services and a protocol. This International Standard is a part of the NFC Security series of standards. The NFC-SEC cryptography standards of the series complement and use the services and protocol specified in this International Standard. This second edition has removed Annex B because it has been included in ISO/IEC 18092:2013 and it allows implementation on generic NFC connections.

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

Part 1:
NFC-SEC NFCIP-1 security services and protocol

1 Scope

This International Standard specifies the NFC-SEC secure channel and shared secret services for NFCIP-1 and the PDUs and protocol for those services.

NOTE This International Standard does not address application specific security mechanisms (as typically needed for smart card related use cases and standardized in the ISO/IEC 7816 series). NFC-SEC may complement application specific security mechanisms of ISO/IEC 7816.

2 Conformance

Conformant implementations implement one or more of the services specified in this International Standard, using the security mechanisms from the NFC-SEC cryptography part identified by the selected Protocol Identifier.

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 7498-1:1994, *Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*

ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

ISO/IEC 10731:1994, *Information technology — Open Systems Interconnection — Basic Reference Model — Conventions for the definition of OSI services*

ISO/IEC 11770-1:1996, *Information technology — Security techniques — Key management — Part 1: Framework*

ISO/IEC 13157-2:2010, *Information technology — Telecommunications and information exchange between systems — NFC Security — Part 2: NFC-SEC cryptography standard using ECDH and AES* (also published by Ecma as Standard ECMA-386)

ISO/IEC 18092:2013, *Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1)* (also published by Ecma as Standard ECMA-340)