INTERNATIONAL STANDARD

ISO/IEC 13157-1

First edition
2010-05-01

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 13157-1:2010(E)

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 13157-1 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.

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*

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.

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 1 NFC-SEC is exclusively designed for the data exchange protocol of ISO/IEC 18092.

NOTE 2 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 employ the security mechanisms in the NFC-SEC cryptography part that defines the selected PID using one or more of the services specified in this International Standard.

Conformant implementations that use the NFCIP-1 protocol shall also conform to the requirements in Annex B.

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 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 18092:2004, *Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1) (also published by Ecma as Standard ECMA-340)*