

This is a preview of "ISO/IEC 13157-1:2014". [Click here to purchase the full version from the ANSI store.](#)

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)

© ISO/IEC 2014



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2014

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
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

This is a preview of "ISO/IEC 13157-1:2014". Click here to purchase the full version from the ANSI store.

Contents

	Page
Foreword	iv
Introduction	v
1 Scope	1
2 Conformance	1
3 Normative references	1
4 Terms and definitions	1
5 Conventions and notations	2
5.1 Representation of numbers.....	2
5.2 Names.....	3
6 Acronyms	3
7 General	4
8 Services	4
8.1 Shared Secret Service (SSE).....	4
8.2 Secure Channel Service (SCH).....	5
9 Protocol Mechanisms	5
9.1 Key agreement.....	5
9.2 Key confirmation.....	5
9.3 PDU security.....	5
9.4 Termination.....	5
10 States and Sub-states	6
11 NFC-SEC-PDUs	7
11.1 Secure Exchange Protocol (SEP).....	7
11.2 Protocol Identifier (PID).....	8
11.3 NFC-SEC Payload.....	8
11.4 Terminate (TMN).....	8
11.5 Error (ERROR).....	8
12 Protocol Rules	8
12.1 Protocol and Service Errors.....	8
12.2 Interworking Rules.....	9
12.3 Sequence Integrity.....	9
12.4 Cryptographic Processing.....	9
Annex A (normative) Protocol Machine Specification	10

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 is bit number 8; in n-length bit strings the lsb is bit number 1 and the msb is bit number n.

This is a preview of "ISO/IEC 13157-1:2014". [Click here to purchase the full version from the ANSI store.](#)

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.