INTERNATIONAL STANDARD

ISO/IEC 22425

First edition
2017-11

Information technology — Telecommunications and information exchange between systems — NFC-SEC Test Methods

Technologies de l'information — Télécommunications et échange d'informations entre systèmes — Méthodes d'essai NFC-SEC

Reference number
ISO/IEC 22425:2017(E)

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 v
Introduction vi
1 Scope 1
2 Conformance 1
3 Normative references 1
4 Terms and definitions 2
5 Conventions and notations 2
6 Acronyms 2
7 NFC-SEC-TEST apparatus 3
7.1 General 3
7.2 Apparatus for testing the Sender 4
7.3 Apparatus for testing the Recipient 4
7.4 NFC-SEC-01 emulation 4
7.5 NFC-SEC-02 emulation 4
7.6 NFC-SEC-03 emulation 4
7.7 NFC-SEC-04 emulation 5
8 Test rules 5
8.1 General test rules 5
8.2 Test scenario and report 5
8.3 RFU bits 5
8.4 Test scenarios 5
9 Test methods for NFC-SEC-01 7
9.1 Recipient test methods 7
9.1.1 List of protocol test methods 7
9.1.2 NFC-SEC-PDU format 7
9.1.3 Logical operation of the Transport Protocol 8
9.2 Sender test methods 9
9.2.1 List of protocol test methods 10
9.2.2 NFC-SEC-PDU format 10
9.2.3 Logical operation of the Transport Protocol 10
10 Test methods for NFC-SEC-02 12
10.1 Recipient test methods 12
10.2 Sender test methods 13
10.2.1 ACT_REQ PDUs 13
10.2.2 ENC PDUs 13
11 Test methods for NFC-SEC-03 14
11.1 Recipient test methods 14
11.1.1 List of protocol test methods 14
11.1.2 NFC-SEC-PDU format 14
11.1.3 Logical operation of the Transport Protocol 14
11.2 Sender test methods 16
11.2.1 List of protocol test methods 16
11.2.2 NFC-SEC-PDU format 16
11.2.3 Logical operation of the Transport Protocol 16
11.2.4 Logical operation of the TTP Transport Protocol 18
12 Test methods for NFC-SEC-04 18
12.1 Recipient test methods 18
12.1.1 List of protocol test methods 19
12.1.2 Logical operation of the Transport Protocol 19

12.2 Sender test methods 20

12.2.1 List of protocol test methods 20

12.2.2 Logical operation of the Transport Protocol 20

Annex A (informative) **Test report template for Recipient tests** **22**

Annex B (informative) **Test report template for Sender tests** **25**

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 voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

ISO/IEC 22425 was prepared by Ecma International (as ECMA-415) 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.

Introduction

The NFC Security Test (NFC-SEC-TEST) standard specifies the definitions, rules and methods for the NFC-SEC-TEST standard and the necessary test apparatus. It corresponds to ISO/IEC 13157 series (ECMA-385, ECMA-386, ECMA-409, ECMA-410 and ECMA-411) of NFC-SEC standards which specify:

— NFC-SEC secure channel and shared secret services and protocol for NFCIP-1, and

— mechanisms for those services.

ISO/IEC 13157 series of NFC-SEC consist of the following standards:

— 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* (NFC-SEC-01, ECMA-386)

— ISO/IEC 13157-3: *Information technology — Telecommunications and information exchange between systems — NFC Security — Part 3: NFC-SEC cryptography standard using ECDH-256 and AES-GCM* (NFC-SEC-02, ECMA-409)

— ISO/IEC 13157-4: *Information technology — Telecommunications and information exchange between systems — NFC Security — Part 4: NFC-SEC entity authentication and key agreement using asymmetric cryptography* (NFC-SEC-03, ECMA-410)

— ISO/IEC 13157-5: *Information technology — Telecommunications and information exchange between systems — NFC Security — Part 5: NFC-SEC entity authentication and key agreement using symmetric cryptography* (NFC-SEC-04, ECMA-411)

Compliance with this International Standard may involve the use of a patent. Ecma International takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured Ecma International that he/she is willing to negotiate licences either free of charge or under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with Ecma International. Information may be obtained from: http://www.ecma-international.org/publications/files/ECMA-ST/EcmaPATENT/EcmaListofPatentStatements.htm

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. Ecma International shall not be held responsible for identifying any or all such patent rights.

Information technology — Telecommunications and information exchange between systems — NFC-SEC Test Methods

1 Scope

This International Standard specifies the definitions, rules and methods for the NFC-SEC-TEST standard and the necessary test apparatus. The test report templates are provided in Annexes A and B.

2 Conformance

In addition to conforming to ISO/IEC 22536 (ECMA-356) and ISO/IEC 23917 (ECMA-362), conforming implementations of ECMA-386, ECMA-409, ECMA-410 and ECMA-411 shall pass all respective normative test cases and requirements specified herein using the test apparatus and rules of this International Standard. Test results should be recorded using Annex A and Annex B of 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 9646 (all parts), *Information technology — Open Systems Interconnection — Conformance Testing Methodology and Framework*

ISO/IEC 9798-1:2010, *Information technology — Security techniques — Entity authentication — Part 1: General*

ISO/IEC 13157-1:2014, *Information technology — Telecommunications and information exchange between systems — NFC Security — Part 1: NFC-SEC NFCIP-1 security services and protocol (ECMA-385)*

ISO/IEC 13157-2:2016, *Information technology — Telecommunications and information exchange between systems — NFC Security — Part 2: NFC-SEC cryptography standard using ECDH and AES (ECMA-386)*

ISO/IEC 13157-3:2016, *Information technology — Telecommunications and information exchange between systems — NFC Security — Part 3: NFC-SEC cryptography standard using ECDH-256 and AES-GCM (ECMA-409)*

ISO/IEC 13157-4:2016, *Information technology — Telecommunications and information exchange between systems — NFC Security — Part 4: NFC-SEC entity authentication and key agreement using asymmetric cryptography (ECMA-410)*

ISO/IEC 13157-5:2016, *Information technology — Telecommunications and information exchange between systems — NFC Security — Part 5: NFC-SEC entity authentication and key agreement using symmetric cryptography (ECMA-411)*

ISO/IEC 18092, *Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1) (ECMA-340)*

ISO/IEC 22536, *Information technology — Telecommunications and information exchange between systems — Near Field Communication Interface and Protocol (NFCIP-1) — RF Interface Test Methods (ECMA-356)*

ISO/IEC 23917, *Information technology — Telecommunications and information exchange between systems — NFCIP-1 — Protocol Test Methods (ECMA-362)*