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

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)*

4 Terms and definitions

For the purposes of this International Standard, the following terms and definitions apply.

4.1
digital certificate (certificate)
public key information of an entity signed by the certification authority and thereby rendered unforgeable

[SOURCE: ISO/IEC 9798-1]

4.2
name
the names of basic elements for test case, e.g. specific fields that are written with a capital initial letter

4.3
recipient
NFC-SEC entity that receives ACT_REQ

[SOURCE: ISO/IEC 13157-1]

4.4
sender
NFC-SEC entity that sends ACT_REQ

[SOURCE: ISO/IEC 13157-1]

4.5
test report
report for the test, that includes amongst other information: supplier, device ID, test suite, test name, test result, the number of passed tests versus the total number of tests, the number of different samples and the date of the tests, see Annexes A and B

5 Conventions and notations

Clause 5 of ISO/IEC 13157-2 (ECMA-386) applies.

6 Acronyms

For the purposes of this International Standard, the following acronyms following apply.

A106	Active communication mode at 106 kbps
A212	Active communication mode at 212 kbps
A424	Active communication mode at 424 kbps
IUT	Implementation Under Test
I/O	Input and Output
LT	Lower Tester
NEAU	NFC Entity Authentication
NEAU-A	NEAU using Asymmetric Cryptography
NEAU-S	NEAU using Symmetric Cryptography

NFC-SEC	NFC Security
NFC-SEC-TEST	NFC-SEC Test
P_{xx}	DEP_REQ or DEP_RES PDU coded as Protected PDU and PNI set to xx.
P106	Passive communication mode at 106 kbps
P212	Passive communication mode at 212 kbps
P424	Passive communication mode at 424 kbps
RTO	Response Timeout
SCH	Secure Channel Service
SEP	Secure Exchange Protocol
SSE	Shared Secret Service
TB-PDU	Transmission Block – Protocol Data Unit
TM-SDU	Test Management – Service Data Unit
UT	Upper Tester

7 NFC-SEC-TEST apparatus

7.1 General

The concepts and abstract model of ISO/IEC 9646 are used to verify that the operation of an Implementation Under Test (IUT) is compliant to any standard of the ISO/IEC 13157 series of NFC-SEC standards.

The NFC-SEC-TEST apparatus consists of an Upper Tester (UT) and a Lower Tester (LT) as illustrated in Figure 1.

To communicate with the IUT, e.g. to establish the shared secret on the IUT, the UT and IUT exchange TM-SDUs. The SDU definition and the interface between UT and IUT are out of scope of this International Standard.

The NFC-SEC-TEST apparatus shall provide different test modes. Each test mode is capable to emulate a conformant implementation by sending and receiving respectively interpreting the specified PDUs of any of ISO/IEC 13157-2 (NFC-SEC-01), ISO/IEC 13157-3 (NFC-SEC-02), ISO/IEC 13157-4 (NFC-SEC-03) and ISO/IEC 13157-5 (NFC-SEC-04).

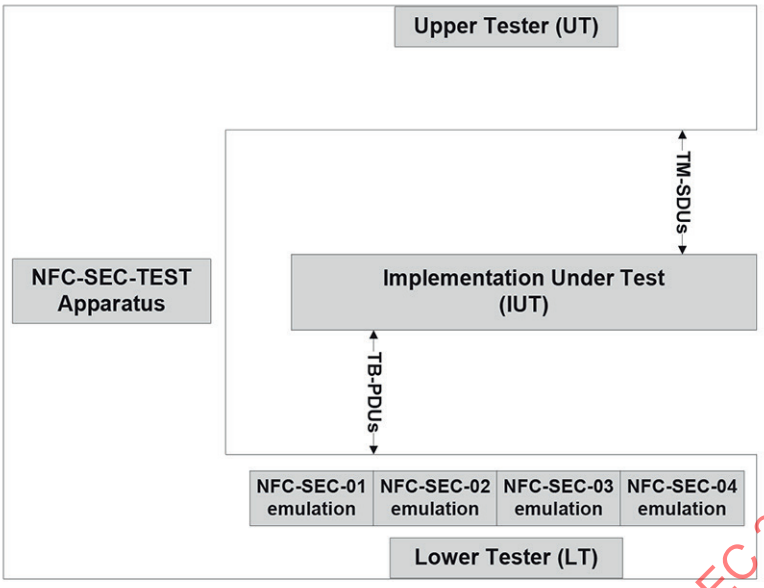


Figure 1 — NFC-SEC-TEST apparatus

7.2 Apparatus for testing the Sender

The NFC-SEC-TEST apparatus tests the IUT when operating as a Sender by emulating a Recipient.

The NFC-SEC-TEST apparatus shall execute the SEP and perform data exchange commands.

The NFC-SEC-TEST apparatus for testing the IUT when operating as the Sender consists of two parts.

— The UT configures the Sender and instructs the Sender to send commands. This Standard does not specify how the UT controls the IUT.

— The LT emulates the Recipient protocol, and occasionally uses incorrect messages to perform negative tests.

7.3 Apparatus for testing the Recipient

The NFC-SEC-TEST apparatus tests the IUT when operating as a Recipient by emulating a Sender.

The NFC-SEC-TEST apparatus shall execute the SEP activation and perform data exchange commands and occasionally uses incorrect messages to perform negative tests.

7.4 NFC-SEC-01 emulation

LT using NFC-SEC-01 Emulation to interact with the IUT If the PID in NFC-SEC-PDU equals to 01.

7.5 NFC-SEC-02 emulation

LT using NFC-SEC-02 Emulation to interact with the IUT If the PID in NFC-SEC-PDU equals to 02.

7.6 NFC-SEC-03 emulation

LT using NFC-SEC-03 Emulation to interact with the IUT If the PID in NFC-SEC-PDU equals to 03.

7.7 NFC-SEC-04 emulation

LT using NFC-SEC-04 Emulation to interact with the IUT If the PID in NFC-SEC-PDU equals to 04.

8 Test rules

8.1 General test rules

An IUT when operating as a Sender sends an ACT_REQ as the first message and the LT sends an ACT_RES.

An IUT when operating as a Sender sends a VFY_REQ and the LT sends a VFY_RES.

An IUT when operating as a Sender sends ENC and the LT receives and analyses it.

An IUT when operating as a Sender sends TMN and the LT receives and analyses it.

An IUT when operating as a Sender sends ERROR and the LT receives and analyses it.

An IUT when operating as a Recipient sends an ACT_RES after the LT sent the ACT_REQ.

An IUT when operating as a Recipient sends a VFY_RES after the LT sent the VFY_REQ.

NOTE Testing the format of DEP_REQ and DEP_RES Protected PDUs as specified in ECMA-340 is outside the scope of this International Standard.

8.2 Test scenario and report

Testing the IUT requires test scenarios to be executed. Each test scenario specifies a sequence of PDUs to be exchanged between the Sender and the Recipient.

The result of the test scenario should be documented in a test report as defined in Annexes A and B.

8.3 RFU bits

A test shall fail in case an RFU field is not set to its default value.

8.4 Test scenarios

The IUT shall answer/request as specified in the scenarios, optionally inserting one or more RTO PDUs before responding with the PDU as specified in the scenarios.

Scenario R 1 — DEP_REQ Protected PDU, correct transaction, Recipient test

NFC-SEC-TEST Apparatus		IUT
P_{00}	→	
	←	P_{01}

Scenario R 2 — DEP_REQ Protected PDU, erroneous transaction, Recipient test

NFC-SEC-TEST Apparatus		IUT
P_{00}	→	
	←	Mute
P_{00}	→	
	←	P_{01}

Scenario R 3 — DEP_REQ Protected PDU, extended transaction, Recipient test

NFC-SEC-TEST Apparatus		IUT
P_{00}	→	
	←	P_{01}
P_{02}	→	
	←	P_{03}

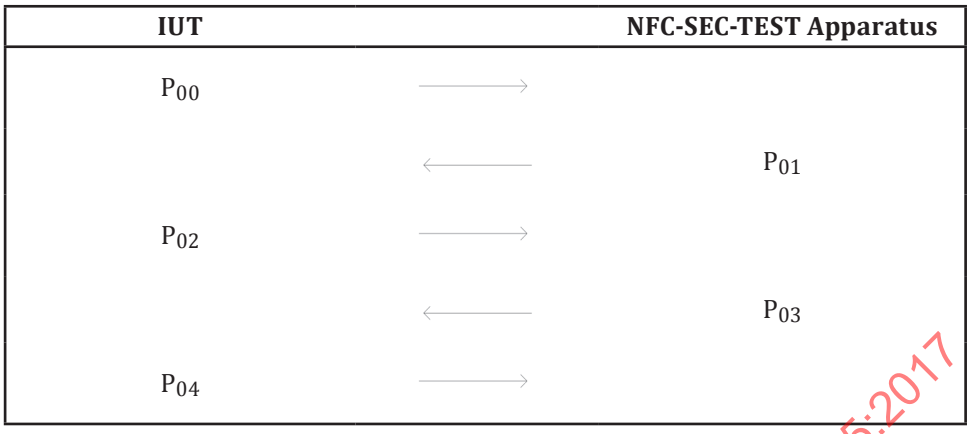
Scenario R 4 — DEP_REQ Protected PDU, correct transaction, Sender test

IUT		NFC-SEC-TEST Apparatus
P_{00}	→	
	←	P_{01}

Scenario R 5 — DEP_REQ Protected PDU, extended transaction, Sender test

IUT		NFC-SEC-TEST Apparatus
P_{00}	→	
	←	P_{01}
P_{02}	→	
	←	P_{03}

Scenario R 6 — DEP_REQ Protected PDU, extended transaction, TMN and ENC test



9 Test methods for NFC-SEC-01

9.1 Recipient test methods

This subclause lists all the required protocol test methods for recipients.

9.1.1 List of protocol test methods

To test Recipients supporting SSE and SCH, the test methods listed in Table 1 shall be executed.

Table 1 — NFC-SEC-PDUs

Test method		Corresponding requirement	
Clause	Name	Base standard	Clause(s)
9.1.2	NFC-SEC PDU format	ECMA-385	11

For all Recipients, the test methods listed in Table 2 shall be executed.

Table 2 — Logical operation of the Transport Protocol

Test method		Corresponding requirement	
Clause	Name	Base standard	Clause(s)
9.1.3.1	Handling of ACT_REQ PDUs	ECMA-386	11.2.2
9.1.3.2	Handling of VFY_REQ PDUs	ECMA-386	11.4.2

9.1.2 NFC-SEC-PDU format

The purpose of this test is to determine if the PDU formats of NFC-SEC-PDUs are correct (see ECMA-385 Clause 11).

NOTE The PDU format is correct when it contains all mandatory and any of the allowed field values and RFU bits are set to default value.

9.1.2.1 Procedure

Repeat steps a) to d) for the SSE transformation.

a) Place the IUT into the operating volume.

b) Generate an RF-field between the limits Hmin and Hmax and verify that the field strength does not influence the test results.

c) Execute scenario R 1, receive the ACT_REQ PDU in DEP_REQ and send ACT_RES PDU in DEP_RES.

d) Execute scenario R 2, receive the VFY_REQ PDU in DEP_REQ in the first PDU exchange and receive the ACT_REQ PDU in DEP_REQ and send ACT_RES PDU in DEP_RES in the second PDU exchange.

9.1.2.2 Test report

The test report shall indicate whether the IUT behaves correctly for SSE and shall include results for the following characteristics:

Characteristic	Expected result for P_{01} in R 1
SEP	Conforming to ECMA-385, 11.1
PID	Conforming to ECMA-385, 11.2
NFC-SEC Payload	Conforming to ECMA-385, 11.3
	Expected result for P_{01} in R 2
SEP	Conforming to ECMA-385, 11.1
PID	Conforming to ECMA-385, 11.2
NFC-SEC Payload	Conforming to ECMA-385, 11.3

9.1.3 Logical operation of the Transport Protocol

9.1.3.1 Handling of ACT_REQ PDUs

The purpose of this test is to determine the correct handling of the ACT_REQ of the IUT.

9.1.3.1.1 Procedure

Repeat steps a) to d) for the SSE transformation for each bit rate.

a) Place the IUT into the operating volume.

b) Generate an RF-field between the limits Hmin and Hmax and verify that the field strength does not influence the test results.

c) Apply the test scenario R 1, receive the ACT_REQ PDU in DEP_REQ and send ACT_RES PDU in DEP_RES.

d) Analyse if the ACT_RES from the IUT is according to scenario R 1.

9.1.3.1.2 Report

The test report shall indicate whether the IUT behaves correctly for SSE and shall include results for the following characteristics for each bit rate:

Characteristic	Expected result
SEP	11000001
PID	Ignored
NFC-SEC Payload	QB||NB, see ECMA-386, 11.2.2, step 4

9.1.3.2 Handling of VFY_REQ PDUs

The purpose of this test is to determine the correct handling of the VFY_REQ of the IUT.

9.1.3.2.1 Procedure

Repeat steps a) to d) for the SSE transformation for each bit rate.

a) Place the IUT into the operating volume.

b) Generate an RF-field between the limits Hmin and Hmax and verify that the field strength does not influence the test results.

c) Apply the test scenario R 3.

   1) Receive the ACT_REQ PDU in DEP_REQ and send the ACT_RES PDU in DEP_RES.

   2) Receive the VFY_REQ PDU in DEP_REQ and send the VFY_RES PDU in DEP_RES.

d) Analyse if VFY_RES from the IUT is correct.

9.1.3.2.2 Report

The test report shall indicate whether the IUT behaves correctly for SSE and shall include results for the following characteristics for each bit rate:

Characteristic	Expected result
SEP	11000011
PID	Ignored
NFC-SEC Payload	MacTagB, see ECMA-386, 11.4.2, step 4

9.1.3.3 ERROR PDUs

The purpose of this test is to determine the correct format and content of ERROR PDUs from the IUT.

9.1.3.3.1 Procedure

Repeat steps a) to d) for the SSE or SCH transformation for each bit rate.

a) Place the IUT into the operating volume.

b) Generate an RF-field between the limits Hmin and Hmax and verify that the field strength does not influence the test results.

c) Apply the test scenario R 1, and insert a wrong PID into ACT_REQ.

d) Analyse if ERROR from the IUT is correct.

9.1.3.3.2 Report

The test report shall indicate whether the IUT behaves correctly for the following characteristics:

Characteristic	Expected result
SEP	00xx1111
PID	Ignored
NFC-SEC Payload	Zero-terminated octet string

9.2 Sender test methods

This subclause lists all the required protocol test methods for senders.

9.2.1 List of protocol test methods

To test Senders supporting SSE and SCH, the test methods listed in Table 3 shall be executed.

Table 3 — NFC-SEC-PDUs

Test method		Corresponding requirement	
Clause	Name	Base standard	Clause(s)
9.2.2	PDU format	ECMA-385	11

For all Senders, the test methods listed in Table 4 shall be executed.

Table 4 — Logical operation of the Transport Protocol

Test method		Corresponding requirement	
Clause	Name	Base standard	Clause(s)
9.2.3.1	ACT_REQ PDUs	ECMA-386	11.2.1
9.2.3.2	VFY_REQ PDUs	ECMA-386	11.4.1
9.2.3.3	ENC PDUs	ECMA-386	12.2.1
9.2.3.4	TMN PDUs	ECMA-385	11.4

9.2.2 NFC-SEC-PDU format

The purpose of this test is to determine the PDU formats of NFC-SEC-PDUs are correct (see ECMA-385 Clause 11).

NOTE The PDU format is correct when it contains all mandatory and any of the allowed field values and RFU bits are set to default value.

9.2.2.1 Procedure

Repeat steps a) to c) for the SSE transformation.

a) Place the IUT into the operating volume.

b) Generate an RF-field between the limits Hmin and Hmax and verify that the field strength does not influence the test results.

c) Execute scenario R 4, send the ACT_REQ PDU in DEP_REQ and Receive ACT_RES PDU in DEP_RES.

9.2.2.2 Test report

The test report shall indicate whether the IUT behaves correctly for SSE and shall include results for the following characteristics:

Characteristic	Expected result for P_{00} in R4
SEP	Conforming to ECMA-385, 11.1
PID	Conforming to ECMA-385, 11.2
NFC-SEC Payload	Conforming to ECMA-385, 11.3

9.2.3 Logical operation of the Transport Protocol

9.2.3.1 ACT_REQ PDUs

The purpose of this test is to determine the correct format and content of ACT_REQ PDUs from the IUT.

9.2.3.1.1 Procedure

Repeat steps a) to d) for the SSE transformation for each bit rate.

a) Place the IUT into the operating volume.

b) Generate an RF-field between the limits Hmin and Hmax and verify that the field strength does not influence the test results.

c) Apply the test scenario R 4, send ACT_REQ PDU in DEP_REQ.

d) Analyse if ACT_REQ from the IUT is correct.

9.2.3.1.2 Report

The test report shall indicate whether the IUT behaves correctly for SSE and shall include results for the following characteristics for each bit rate:

Characteristic	Expected result
SEP	00000000
PID	1
NFC-SEC Payload	QA||NA, see ECMA-386, 11.2.1, step 3

9.2.3.2 VFY_REQ PDUs

The purpose of this test is to determine the correct format and content of VFY_REQ PDUs of the IUT.

9.2.3.2.1 Procedure

Repeat steps a) to d) for the SSE transformation for each bit rate.

a) Place the IUT into the operating volume.

b) Generate an RF-field between the limits Hmin and Hmax and verify that the field strength does not influence the test results.

c) Apply the test scenario R 5.

   1) Send the ACT_REQ PDU in DEP_REQ and receive the response ACT_RES in DEP_RES.

   2) Send the VFY_REQ PDU in DEP_REQ.

d) Analyse if VFY_REQ from the IUT is correct.

9.2.3.2.2 Report

The test report shall indicate whether the IUT behaves correctly for SSE and shall include results for the following characteristics:

Characteristic	Expected result
SEP	00000010
PID	Ignored
NFC-SEC Payload	MacTagA, see ECMA-386, 11.4.1, step 2

9.2.3.3 ENC PDUs

The purpose of this test is to determine the correct format and content of ENC PDUs from the IUT.

9.2.3.3.1 Procedure

Repeat steps a) to d) for the SCH transformation for each bit rate.

a) Place the IUT into the operating volume.

b) Generate an RF-field between the limits Hmin and Hmax and verify that the field strength does not influence the test results.

c) Apply the test scenario R 6, send ENC PDU in DEP_REQ of P_{04}.

d) Analyse if ENC from the IUT is correct.

9.2.3.3.2 Report

The test report shall indicate whether the IUT behaves correctly for SCH and shall include results for the following characteristics for each bit rate:

Characteristic	Expected result
SEP	00010100
PID	Ignored
NFC-SEC Payload	SNV||DataLen||EncData||Mac, see ECMA-386, 12.2.1, step 6.

9.2.3.4 TMN PDUs

The purpose of this test is to determine the correct format and content of TMN PDUs from the IUT.

9.2.3.4.1 Procedure

Repeat steps a) to d) for the SSE of SCH transformation for each bit rate.

a) Place the IUT into the operating volume.

b) Generate an RF-field between the limits Hmin and Hmax and verify that the field strength does not influence the test results.

c) Apply the test scenario R 6, send TMN PDU in DEP_REQ in P_{04}.

d) Analyse if the TMN from the IUT is correct.

9.2.3.4.2 Report

The test report shall indicate whether the IUT behaves correctly for the following characteristics:

Characteristic	Expected result
SEP	00xx0110
PID	Ignored
NFC-SEC Payload	Ignored

10 Test methods for NFC-SEC-02

10.1 Recipient test methods

9.1 of this International Standard applies.

10.2 Sender test methods

9.2 of this International Standard applies when the contents of ACT_REQ PDUs and ENC PDUs are replaced as specified in this subclause.

10.2.1 ACT_REQ PDUs

The purpose of this test is to determine the correct format and content of ACT_REQ PDUs from the IUT.

10.2.1.1 Procedure

Repeat steps a) to d) for the SSE transformation for each bit rate.

a) Place the IUT into the operating volume.

b) Generate an RF-field between the limits Hmin and Hmax and verify that the field strength does not influence the test results.

c) Apply the test scenario R 4, send ACT_REQ PDU in DEP_REQ.

d) Analyse if ACT_REQ from the IUT is correct.

10.2.1.2 Report

The test report shall indicate whether the IUT behaves correctly for SSE and shall include results for the following characteristics for each bit rate:

Characteristic	Expected result
SEP	00000000
PID	2
NFC-SEC Payload	See ECMA-409 Clause 11

10.2.2 ENC PDUs

The purpose of this test is to determine the correct format and content of ENC PDUs from the IUT.

10.2.2.1 Procedure

Repeat steps a) to d) for the SCH transformation for each bit rate.

a) Place the IUT into the operating volume.

b) Generate an RF-field between the limits Hmin and Hmax and verify that the field strength does not influence the test results.

c) Apply the test scenario R 6, send ENC PDU in DEP_REQ of P_{04}.

d) Analyse if ENC from the IUT is correct.

10.2.2.2 Report

The test report shall indicate whether the IUT behaves correctly for SCH and shall include results for the following characteristics for each bit rate:

Characteristic	Expected result
SEP	00010100
PID	Ignored
NFC-SEC Payload	S3 || S2 || S1 || AuthEncData, see ECMA-409, 12.2.1, step 7.

11 Test methods for NFC-SEC-03

11.1 Recipient test methods

This subclause lists all the required protocol test methods for recipients.

11.1.1 List of protocol test methods

To test Recipients supporting SSE and SCH, the test methods listed in Table 5 shall be executed.

Table 5 — NFC-SEC-PDUs

Test method		Corresponding requirement	
Clause	Name	Base standard	Clause(s)
11.1.2	NFC-SEC PDU format	ECMA-385	11

For all Recipients, the test methods listed in Table 6 shall be executed.

Table 6 — Logical operation of the Transport Protocol

Test method		Corresponding requirement	
Clause	Name	Base standard	Clause(s)
11.1.3.1	Handling of ACT_REQ PDUs	ECMA-410	10.1.4 10.2.4
11.1.3.2	Handling of VFY_REQ PDUs	ECMA-410	10.1.4 10.2.4
11.1.3.3	ERROR PDUs	ECMA-385	11.5

11.1.2 NFC-SEC-PDU format

9.1.2 of this International Standard applies.

11.1.3 Logical operation of the Transport Protocol

11.1.3.1 Handling of ACT_REQ PDUs

The purpose of this test is to determine the correct handling of the ACT_REQ of the IUT.

11.1.3.1.1 Procedure

Repeat steps a) to d) for the SSE transformation with and without involving TTP and for each bit rate.

a) Place the IUT into the operating volume.

b) Generate an RF-field between the limits Hmin and Hmax and verify that the field strength does not influence the test results.

c) Apply the test scenario R 1, receive the ACT_REQ PDU in DEP_REQ and send ACT_RES PDU in DEP_RES.

d) Analyse if the ACT_RES from the IUT is correct.

11.1.3.1.2 Report

For NEAU-A mechanism involving a TTP, the test report shall indicate whether the IUT behaves correctly for SSE and shall include results for the following characteristics for each bit rate:

Characteristic	Expected result
SEP	11000001
PID	Ignored
NFC-SEC Payload	TTP||NB||NA'||CertB||QB||SigB, see ECMA-410, 10.1.4, step 6

For NEAU-A mechanism without involving a TTP, the test report shall indicate whether the IUT behaves correctly for SSE and shall include results for the following characteristics for each bit rate:

Characteristic	Expected result
SEP	11000001
PID	Ignored
NFC-SEC Payload	TTP||NB||NA'||CertB||QB||SigB, see ECMA-410, 10.2.4, step 7

11.1.3.2 Handling of VFY_REQ PDUs

The purpose of this test is to determine the correct handling of the VFY_REQ of the IUT.

11.1.3.2.1 Procedure

Repeat steps a) to d) for the SSE transformation for each bit rate.

a) Place the IUT into the operating volume.

b) Generate an RF-field between the limits Hmin and Hmax and verify that the field strength does not influence the test results.

c) Apply the test scenario R 3.

   1) Receive the ACT_REQ PDU in DEP_REQ and send the ACT_RES PDU in DEP_RES.

   2) Receive the VFY_REQ PDU in DEP_REQ and send the VFY_RES PDU in DEP_RES.

   NOTE When involving a TTP, the validity of the certificates of Sender A and Recipient B should be checked, (refer to 10.1 of ECMA-410) by the TTP following c).1) and before c).2).

d) Analyse if VFY_RES from the IUT is correct.

11.1.3.2.2 Report

For NEAU-A mechanism involving a TTP, the test report shall indicate whether the IUT behaves correctly for SSE and shall include results for the following characteristics for each bit rate:

Characteristic	Expected result
SEP	11000011
PID	Ignored
NFC-SEC Payload	$MacTag_B$, see ECMA-410, 10.1.4, step 15

For NEAU-A mechanism without involving a TTP, the test report shall indicate whether the IUT behaves correctly for SSE and shall include results for the following characteristics for each bit rate:

Characteristic	Expected result
SEP	11000011
PID	Ignored
NFC-SEC Payload	$MacTag_B$, see ECMA-410, 10.2.4, step 16

11.1.3.3 ERROR PDUs

9.1.3.3 of this International Standard applies.

11.2 Sender test methods

This subclause lists all required protocol test methods for senders.

11.2.1 List of protocol test methods

To test Senders supporting SSE and SCH the test methods listed in Table 7 shall be executed.

Table 7 — NFC-SEC-PDUs

Test method		Corresponding requirement	
Clause	Name	Base standard	Clause(s)
11.2.2	PDU format	ECMA-385	11

For all Senders, the test methods listed in Table 8 shall be executed.

Table 8 — Logical operation of the Transport Protocol

Test method		Corresponding requirement	
Clause	Name	Base standard	Clause(s)
11.2.3.1	ACT_REQ PDUs	ECMA-410	10.1.3 10.2.3
11.2.3.2	VFY_REQ PDUs	ECMA-410	10.1.3 10.2.3
11.2.3.3	ENC PDUs	ECMA-409	12.2.1
11.2.3.4	TMN PDUs	ECMA-385	11.4
11.2.4.1	TAEP_REQ PDU	ECMA-410	10.1.5

11.2.2 NFC-SEC-PDU format

9.2.2 of this International Standard applies.

11.2.3 Logical operation of the Transport Protocol

11.2.3.1 ACT_REQ PDUs

The purpose of this test is to determine the correct format and content of ACT_REQ PDUs from the IUT.

11.2.3.1.1 Procedure

Repeat steps a) to d) for the SSE transformation for each bit rate.

a) Place the IUT into the operating volume.

b) Generate an RF-field between the limits Hmin and Hmax and verify that the field strength does not influence the test results.

c) Apply the test scenario R 4, send ACT_REQ PDU in DEP_REQ.

d) Analyse if ACT_REQ from the IUT is correct.

11.2.3.1.2 Report

For NEAU-A mechanism involving a TTP, the test report shall indicate whether the IUT behaves correctly for SSE and shall include results for the following characteristics for each bit rate:

Characteristic	Expected result
SEP	00000000
PID	3
NFC-SEC Payload	TTP||NA||$Cert_A$, see ECMA-410, 10.1.3, step 3

For NEAU-A mechanism without involving a TTP, the test report shall indicate whether the IUT behaves correctly for SSE and shall include results for the following characteristics for each bit rate:

Characteristic	Expected result
SEP	00000000
PID	3
NFC-SEC Payload	TTP||NA||$Cert_A$, see ECMA-410, 10.2.3, step 3

11.2.3.2 VFY_REQ PDUs

The purpose of this test is to determine the correct format and content of VFY_REQ PDUs of the IUT.

11.2.3.2.1 Procedure

Repeat steps a) to d) for the SSE transformation for each bit rate.

a) Place the IUT into the operating volume.

b) Generate an RF-field between the limits Hmin and Hmax and verify that the field strength does not influence the test results.

c) Apply the test scenario R 5.

   1) Send the ACT_REQ PDU in DEP_REQ and receive ACT_RES in DEP_RES.

   2) Send the VFY_REQ PDU in DEP_REQ.

d) Analyse if VFY_REQ from the IUT is correct.

11.2.3.2.2 Report

For NEAU-A mechanism involving a TTP, the test report shall indicate whether the IUT behaves correctly for SSE and shall include results for the following characteristics for each bit rate:

Characteristic	Expected result
SEP	00000010
PID	Ignored
NFC-SEC Payload	NA||NB'||QA||Res_A'||Res_B'||Sig_{TTP}'||Sig_A||$MacTag_A$, see ECMA-410, 10.1.3, step 17

For NEAU-A mechanism without involving a TTP, the test report shall indicate whether the IUT behaves correctly for SSE and shall include results for the following characteristics for each bit rate:

Characteristic	Expected result
SEP	00000010
PID	Ignored
NFC-SEC Payload	NA||NB'||QA||Sig_A||$MacTag_A$, see ECMA-410, 10.2.3, step 14

11.2.3.3 ENC PDUs

10.2.2 of this International Standard applies.

11.2.3.4 TMN PDUs

9.2.3.4 of this International Standard applies.

11.2.4 Logical operation of the TTP Transport Protocol

11.2.4.1 TAEP_REQ PDUs

The purpose of this test is to determine the correct format and content of TAEP_REQ PDUs from the IUT.

11.2.4.1.1 Procedure

Perform steps a) to c) for the TTP transformation.

a) Place the IUT into the operating volume.

b) Send TAEP_REQ PDU.

c) Analyse if TAEP_REQ from the IUT is correct.

11.2.4.1.2 Report

The test report shall indicate whether the IUT behaves correctly for the following characteristics:

Characteristic	Expected result
TAEP Payload	NA'||NB'||$Cert_A$'||$Cert_B$', see ECMA-410, 10.1.5, step 1

12 Test methods for NFC-SEC-04

12.1 Recipient test methods

This subclause lists all the required protocol test methods for recipients.

12.1.1 List of protocol test methods

To test Recipients supporting SSE and SCH, the test methods listed in Table 5 shall be executed.

For all Recipients, the test methods listed in Table 9 shall be executed.

Table 9 — Logical operation of the Transport Protocol

Test method		Corresponding requirement	
Clause	Name	Base standard	Clause(s)
12.1.2.1	Handling of ACT_REQ PDUs	ECMA-411	10.4
12.1.2.2	Handling of VFY_REQ PDUs	ECMA-411	10.4
11.1.3.3	ERROR PDUs	ECMA-385	11.5

12.1.2 Logical operation of the Transport Protocol

12.1.2.1 Handling of ACT_REQ PDUs

The purpose of this test is to determine the correct handling of the ACT_REQ of the IUT.

12.1.2.1.1 Procedure

Repeat steps a) to d) for the SSE transformation for each bit rate.

a) Place the IUT into the operating volume.

b) Generate an RF-field between the limits Hmin and Hmax and verify that the field strength does not influence the test results.

c) Apply the test scenario R 1, receive the ACT_REQ PDU in DEP_REQ and send ACT_RES PDU in DEP_RES.

d) Analyse if the ACT_RES from the IUT is correct.

12.1.2.1.2 Report

The test report shall indicate whether the IUT behaves correctly for SSE and shall include results for the following characteristics for each bit rate:

Characteristic	Expected result
SEP	11000001
PID	Ignored
NFC-SEC Payload	NB||NA'||$EncData_R$||MAC_R, see ECMA-411, 10.4, step 5

12.1.2.2 Handling of VFY_REQ PDUs

The purpose of this test is to determine the correct handling of the VFY_REQ of the IUT.

12.1.2.2.1 Procedure

Repeat steps a) to d) for the SSE transformation for each bit rate.

a) Place the IUT into the operating volume.

b) Generate an RF-field between the limits Hmin and Hmax and verify that the field strength does not influence the test results.

c) Apply the test scenario R 3.

1) Receive the ACT_REQ PDU in DEP_REQ and send the ACT_RES PDU in DEP_RES.

2) Receive the VFY_REQ PDU in DEP_REQ and send the VFY_RES PDU in DEP_RES.

d) Analyse if the VFY_RES from the IUT is correct.

12.1.2.2.2 Report

The test report shall indicate whether the IUT behaves correctly for SSE and shall include results for the following characteristics for each bit rate:

Characteristic	Expected result
SEP	11000011
PID	Ignored
NFC-SEC Payload	$MacTag_B$, see ECMA-411, 10.4, step 10

12.2 Sender test methods

This subclause lists all required protocol test methods for senders.

12.2.1 List of protocol test methods

To test Senders supporting SSE and SCH, the test methods listed in Table 7 shall be executed.

For all Senders, the test methods listed in Table 10 shall be executed.

Table 10 — Logical operation of the Transport Protocol

Test method		Corresponding requirement	
Clause	Name	Base standard	Clause(s)
12.2.2.1	ACT_REQ PDUs	ECMA-411	10.3
12.2.2.2	VFY_REQ PDUs	ECMA-411	10.3
11.2.3.3	ENC PDUs	ECMA-409	12.2.1
11.2.3.4	TMN PDUs	ECMA-385	11.4

12.2.2 Logical operation of the Transport Protocol

12.2.2.1 ACT_REQ PDUs

The purpose of this test is to determine the correct format and content of ACT_REQ PDUs from the IUT.

12.2.2.1.1 Procedure

Repeat steps a) to d) for the SSE transformation for each bit rate.

a) Place the IUT into the operating volume.

b) Generate an RF-field between the limits Hmin and Hmax and verify that the field strength does not influence the test results.

c) Apply the test scenario R 4, send ACT_REQ PDU in DEP_REQ.

d) Analyse if ACT_REQ from the IUT is correct.

12.2.2.1.2 Report

The test report shall indicate whether the IUT behaves correctly for SSE and shall include results for the following characteristics for each bit rate:

Characteristic	Expected result
SEP	00000000
PID	4
NFC-SEC Payload	NA, see ECMA-411, 10.3, step 2

12.2.2.2 VFY_REQ PDUs

The purpose of this test is to determine the correct format and content of VFY_REQ PDUs of the IUT.

12.2.2.2.1 Procedure

Repeat steps a) to d) for the SSE transformation for each bit rate.

a) Place the IUT into the operating volume.

b) Generate an RF-field between the limits Hmin and Hmax and verify that the field strength does not influence the test results.

c) Apply the test scenario R 5.

   1) Send the ACT_REQ PDU in DEP_REQ and receive ACT_RES in DEP_RES.

   2) Send the VFY_REQ PDU in DEP_REQ.

d) Analyse if VFY_REQ from the IUT is correct.

12.2.2.2.2 Report

The test report shall indicate whether the IUT behaves correctly for SSE and shall include results for the following characteristics for each bit rate:

Characteristic	Expected result
SEP	00000010
PID	Ignored
NFC-SEC Payload	NA||NB'||$EncData_S$||MAC_S||$MacTag_A$, see ECMA-411, 10.3, step 8

Annex A
(informative)

Test report template for Recipient tests

A.1 Test report template for Recipient tests of NFC-SEC-01

Supplier:

Product:

Table A.1 — Test report template for Recipient tests of NFC-SEC-01

9.1 Recipient test methods						
No	**Test name**	**Expected result**	**Reference chapter in ECMA Standards**	**Scenario number**	**Condition**	**Test results PASS/FAIL**
1	9.1.2 NFC-SEC-PDU format	The test passes if IUT behaves as described in the scenario.	ECMA-385 Clause 11	R 1, R 2	P106	
					P212	
					P424	
					A106	
					A212	
					A424	
2	9.1.3.1 Handling of ACT_REQ PDUs	The test passes if IUT behaves as described in the scenario.	ECMA-386 11.2.2	R 1	P106	
					P212	
					P424	
					A106	
					A212	
					A424	
3	9.1.3.2 Handling of VFY_REQ PDUs	The test passes if IUT behaves as described in the scenario.	ECMA-386 11.4.2	R 3	P106	
					P212	
					P424	
					A106	
					A212	
					A424	
4	9.1.3.3 Handling of ERROR PDUs	The test passes if IUT behaves as described in the scenario.	ECMA-385 11.5	R 1	P106	
					P212	
					P424	
					A106	
					A212	
					A424	

A.2 Test report template for Recipient tests of NFC-SEC-02

Clause A.1 of this International Standard applies.