INTERNATIONAL STANDARD

ISO/IEC 19823-16

First edition
2020-10

Information technology — Conformance test methods for security service crypto suites —

Part 16:
Crypto suite ECDSA-ECDH security services for air interface communications

© ISO/IEC 2020

iTeh STANDARD PREVIEW
(standards.iteh.ai)

COPYRIGHT PROTECTED DOCUMENT

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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 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 of 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 www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

A list of all parts in the ISO/IEC 19823 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The ISO/IEC 29167 series describes security services as applicable for the ISO/IEC 18000 series. The various parts of ISO/IEC 29167 describe crypto suites that are optional extensions to the ISO/IEC 18000 series air interfaces.

The ISO/IEC 19823 series describes the conformance test methods for security service crypto suites. It is related to the ISO/IEC 18047 series, which describes the radio frequency identification device conformance test methods, in the same way as the ISO/IEC 29167 series is related to the ISO/IEC 18000 series.

These relations mean that for a product that is claimed to conform to a pair of ISO/IEC 18000 and ISO/IEC 29167 documents, then the test methods of the ISO/IEC 18047 and ISO/IEC 19823 documents apply. If a product supports more than one part of ISO/IEC 18000 or ISO/IEC 29167, all related parts of ISO/IEC 18047 and ISO/IEC 19823 apply.

This part of ISO/IEC 19823 describes the test methods for the ECDSA-ECDH crypto suite as standardized in ISO/IEC 29167-16.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent concerning radio-frequency identification security technology given in Clause 6.

ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the ISO and IEC that they are willing to negotiate licences 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 ISO and IEC.

Information may be obtained from:

Patent holder: China IWNCOMM Co., Ltd.

Address: A201, QinFeng Ge, Xi'an Software Park, No.68 KeJi 2nd Road, Xi'an Hi-tech Industrial Development Zone, Xi'an, Shaanxi, P.R.China 710075

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. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

NOTE   Test methods for interrogator and tag performance are covered by the ISO/IEC 18046 series.

Information technology — Conformance test methods for security service crypto suites —

Part 16:
Crypto suite ECDSA-ECDH security services for air interface communications

1 Scope

This document describes test methods for determining the conformance of security crypto suites defined in ISO/IEC 29167-16.

This document contains conformance tests for all mandatory and applicable optional functions.

The conformance parameters are the following:

— parameters that apply directly affecting system functionality and inter-operability;

— protocol including commands and replies;

— nominal values and tolerances.

Unless otherwise specified, the tests in this document are to be applied exclusively to RFID tags and interrogators defined in the ISO/IEC 18000 series using ISO/IEC 29167-16.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 19762 (all parts), *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

ISO/IEC 18000-4:2018, *Information technology — Radio frequency identification for item management — Part 4: Parameters for air interface communications at 2.45 GHz*

ISO/IEC 29167-16:2015, *Information technology — Automatic identification and data capture techniques — Part 16: Crypto suite ECDSA-ECDH security services for air interface communications*

3 Terms, definitions, symbols and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762 and ISO/IEC 29167-16 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.2 Symbols

For the purposes of this document, the symbols given in ISO/IEC 19762 apply.

3.3 Abbreviated terms

For the purposes of this document, the abbreviated terms given in ISO/IEC 19762 and the following apply.

ECDH elliptic curve diffie-hellman

ECDHP ECDH parameter

ECDSA ellipticcurvedigital signature algorithm

MAC message authentication code

MAM mutual authentication message

MIC message integrity code

RN random number

SEK session encryption key

SIK session integrity check key

TPK temporary public key

TRAIS tag and reader air interface security

TRAIS-P tag and reader air interface security based on public key cryptography

TTP trusted third party

TTPID identifier of TTP

4 Test methods

4.1 General

This document describes the general test methods for ISO/IEC 29167-16. As the parts of ISO/IEC 19823 are always tested in relation with the ISO/IEC 18047 series, a duplication of information requirements and specifications should be avoided.

Clause 5 defines elements that are assumed to be covered in the respective part of the ISO/IEC 19823 series.

Clause 6 defines elements that are not covered by the ISO/IEC 18047 series and are therefore addressed in this document.

4.2 By demonstration

"By demonstration" means laboratory testing of one or, if required for statistical reasons, multiple products, processes, or services to ensure conformance.

A test laboratory meeting the requirements of ISO/IEC 17025 shall be selected for the performance of the indicated testing to ensure conformance of the component or system.

For protocol requirements that are verified by demonstration, the test conditions are specified by this document. The detailed test plan is at the discretion of the test laboratory.

4.3 By design

"By design" means design parameters and/or theoretical analyses that ensure conformance. A vendor submitting a component or system for compliance testing shall provide the necessary technical information, in the form of a technical memorandum or similar. A test laboratory shall issue a test certificate indicating whether the technical analysis was sufficient to ensure conformance of the component or system.

For protocol requirements that are verified by design, the method of technical analysis is at the discretion of the submitting vendor and is not specified by this document. In general, the technical analysis shall have sufficient rigor and technical depth to convince a test engineer knowledgeable of the protocol that the particular requirement has been met.

5 Test methods in respect to ISO/IEC 18000-4 Mode 4

5.1 Default items applicable to the test methods

The following requirements and applicable optional requirements shall be fulfilled.

5.1.1 Test environment

Unless otherwise specified, testing shall take place in an environment of temperature 23 °C ± 3 °C (73 °F ± 5 °F) and relative humidity of 40 % to 60 %.

5.1.2 Pre-conditioning

Where pre-conditioning is required by the test method, the tags and interrogators to be tested shall be conditioned to the test environment for an appropriate period of time before testing.

5.1.3 Default tolerance

Unless otherwise specified, a default tolerance of ±5 % shall be applied to the quantity values given to specify the characteristics of the test equipment (e.g. linear dimensions) and the test method procedures (e.g. test equipment adjustments).

5.1.4 Total measurement uncertainty

The total measurement uncertainty for each quantity determined by these test methods shall be stated in the test report.

NOTE1   Basic information is given in "ISO Guide to the Expression of Uncertainty in Measurement", ISBN 92-67-10188-9, 1993.

NOTE2   The default items applicable to the test methods defined in 5.1 is given in ISO/IEC TR 18047-4.

5.2 Test setup and measurement equipment

This subclause defines the test setup and measurement equipment for verifying the operation of a tag or an interrogator according to ISO/IEC 18000-4 Mode 4.

Test results shall not be influenced by the setup method of the test.

Test setups include:

— test setup for interrogator testing (see 5.2.1),

— test setup for tag testing (see 5.2.2),

— test equipment (see 5.2.3).

These are described in the following subclauses.

5.2.1 Test setup for interrogator testing

An interrogator with integral antenna(e) shall be equipped with temporary antenna connector(s), or else coupling device(s) [i.e. sense antenna(e)] shall be used to connect to the test equipment.

A sense antenna shall not affect test results. Appropriate distances (e.g. 30 cm), antenna sizes and types (e.g. patch antenna) and antenna polarization (i.e. circular polarization) shall be used. The antenna configuration and distance shall be included in the test report.

To set up an interrogator with the appropriate test pattern and operational modes, one of two methods shall be used (combinations shall also be possible):

a) an implemented test mode,

b) a tag for initializing the appropriate operational mode.

The air interface parameter in a test mode shall behave in the same way as the air interface parameter during normal usage.

Unless otherwise stated, for all tests, the frequency of the reference carrier shall conform to ISO/IEC 18000-4:2018, 9.3.1. The output power shall be set to maximum (both carriers switched on).

5.2.2 Test setup for tag testing

A tag with integral antenna(e) shall be equipped with temporary antenna connector(s),or else suitable coupling device(s) [i.e. antenna(e)] shall be used to connect to the test equipment.

A sense antenna shall not affect test results. Appropriate distances (e.g. 30 cm), antenna sizes and types (e.g. patch antenna), as well as antenna polarization (i.e. circular polarization) shall be used. The antenna configuration and distance shall be included in the test report.

To set up a tag with the appropriate test pattern and operational modes, one of two methods shall be used (combinations shall also be possible):

a) an implemented test mode,

b) an interrogator for initializing the appropriate operational mode.

Unless otherwise stated, for all tests, the frequency of the reference carrier shall conform to ISO/IEC 18000-4:2018, 9.3.1.

5.2.3 Test equipment

All tests shall be performed using commercial test equipment. In addition to the measurement devices described in the following subclauses, appropriate devices such as power supplies, splitters, combiners and cables shall be used.

The reference point for all measurements shall be either (temporary) antenna connector(s), or appropriate coupling device(s). The reference point shall be documented in the test report.

5.2.3.1 Spectrum analyser

A spectrum analyser with the capability of digital demodulating and with vector signal analysis capability shall be used. Appropriate trigger functionality shall be either implemented in the spectrum analyser or generated externally with additional measurement devices.

5.2.3.2 Signal generator

A signal generator for the 2,45 GHz band shall be used to generate an interrogator output signal for testing tags. The signal level for the tests shall be within the operational range of the receiver input of the tag. The input level shall be specified by the tag manufacturer and shall be documented in the test report.

5.2.3.3 Logic analyser

A logic analyser shall be used for verification of the correct data. Therefore, the analyser shall be capable of storage of sequent samples in 0,5 second.

6 Test methods in respect to ISO/IEC 29167-16 interrogators and tags

6.1 Test map for optional features

Table 1 lists all optional features of the crypto suite defined by Tag and Reader Air Interface Security (TRAIS) based on Public key cryptography (TRAIS-P) and shall be used as a template for reporting the test results. Furthermore, Table 1 shall be used in reference to the test requirements in 6.2.

Table 1 — Test map for optional features

#	Feature	Additional requirement	Mark items to be tested for supplied product	Test results
1	Mutual Authentication without TTP involved	Shall be tested with the *Authenticate* command of the relevant part of ISO/IEC 18000.		
2	Mutual Authentication with TTP involved	Shall be tested with the *Authenticate* command of the relevant part of ISO/IEC 18000.		
3	Authenticate communication	Shall be tested with the *AuthComm* command of the relevant part of ISO/IEC 18000.		
4	Secure communication	Shall be tested with the *SecureComm* command of the relevant part of ISO/IEC 18000.		

Table 2 to Table 5 lists all crypto suite requirements that shall be tested in depending on the features of Table 1 as supported by the device under test. Items marked with M are mandatory and shall be tested for each device under test.

6.2 Crypto suite requirements

6.2.1 General

This subclause contains all of the requirements of ISO/IEC 29167-16.

6.2.2 Crypto suite requirements of ISO/IEC 29167-16:2015, Clauses 1 - 6

All of the requirements of ISO/IEC 29167-16:2015, Clauses 1-6 are mandatory, inherently by design only.

6.2.3 Crypto suite requirements of ISO/IEC 29167-16:2015, Clauses 7 - 11

Table 2 contains all of the requirements of ISO/IEC 29167-16:2015, Clauses 7 – 11.

The column MO (Mandatory / Optional) contains the following information:

— items marked with "M" are mandatory and shall be tested for all devices;