DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 19823-16

ISO/IEC JTC **1**/SC **31**	Secretariat: **ANSI**
Voting begins on: **2019-11-27**	Voting terminates on: **2020-02-19**

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

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

ICS: 35.030

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 19823-16:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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. 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. 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

The committee responsible for this document is ISO/IEC JTC1.

ISO/IEC 19823 consists of the following parts, under the general title Information technology — Conformance test methods for security service crypto suites:

— *Part 1: General requirements*

— *Part 10: Crypto suite AES-128 security services for air interface communications*

— *Part 11: Crypto suite PRESENT-80 security services for air interface communications*

— *Part 12: Crypto suite ECC-DH security services for air interface communications*

— *Part 13: Crypto suite Grain-128A security services for air interface communications*

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

— *Part 17: Crypto suite cryptoGPS security services for air interface communications*

— *Part 19: Crypto suite RAMON security services for air interface communications*

Introduction

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

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

These relations mean that for a product that is claimed to be compliant to a pair of ISO/IEC 18000-n and ISO/IEC 29167-m then the test methods of ISO/IEC 18047-n and ISO/IEC 19823-m 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 29167-16:2015.

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

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 part of ISO/IEC 19823 describes test methods for determining the conformance of security crypto suite defined in ISO/IEC 29167-16.

This part of ISO/IEC 19823 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 part of ISO/IEC 19823 are to be applied exclusively related to RFID tags and interrogators defined in the ISO/IEC 18000 series using ISO/IEC 29167-16.

2 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 amendment s) applies.

ISO/IEC 19762 (all parts), Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary

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

ISO/IEC TR 18047-4, Information technology — Radio frequency identification device conformance test methods — Part 4: Test methods for air interface communications at 2.45 GHz

ISO/IEC 29167-16, 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 apply.

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	Elliptic Curve Digital 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 test methods for ISO/IEC 29167-16. As the parts of ISO/IEC 19823 are always tested in relation with ISO/IEC 18047, a duplication of information requirements and specifications is meant to be avoided.

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

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

4.2 By demonstration

Laboratory testing of one, or (if required for statistical reasons), multiple products, processes, or services to ensure compliance. A test laboratory that meets ISO/IEC 17025 shall perform 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

Design parameters and/or theoretical analysis that ensure compliance. 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 certified test laboratory shall certify the technical analysis as being 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 the ISO/IEC 18000-4 Mode 4

5.1 Default items applicable to the test methods

The following requirements and applicable optional requirements of ISO/IEC TR 18047-4 shall be fulfilled:

- Sub-clause: 5.1 Default conditions applicable to the test methods

5.2 Test set-up and measurement equipment

This subclause defines the test set-up 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 set-up method of the test.

Test set-ups include:

- test set-up for interrogator testing (see 5.2.1),
- test set-up for tag testing (see 5.2.2),
- test equipment (see 5.2.3).

These are described in the following subclauses.

5.2.1 Test set-up for interrogator testing

An interrogator with integral antenna(s) shall be equipped with temporary antenna connector(s) or coupling device(s) [i.e. sense antenna(s)] 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 an interrogator with the appropriate test pattern and operational modes one of two methods shall be used (combinations shall also be possible):

- an implemented test mode,
- a tag for initializing the appropriate operational mode.

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

Unless otherwise stated the following frequencies shall be used for all tests.

The frequency of the reference carrier shall be conformance with Sub-clause 9.3.1 in ISO/IEC 18000-4. The output power shall be set to maximum (both carriers switched on).

5.2.2 Test set-up for tag testing

A tag with integral antenna(s) shall be equipped with temporary antenna connector(s), or suitable coupling device(s) [i.e. antenna(s)] 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 test pattern and operational modes one of two methods shall be used (combinations shall also be possible):

— an implemented test mode,

— an interrogator for initializing the appropriate operational mode.

Unless otherwise stated, all tests related frequency of the reference carrier shall be conformance with Sub-clause 9.3.1 in ISO/IEC 18000-4.

5.2.3 Test equipment

All tests shall be done with commercial test equipment. In addition to the measurement devices described below 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 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 the ISO/IEC 29167-16 interrogators and tags

6.1 Test map for optional features

Table 1 lists all optional features of this crypto suite and shall be used as template to report the test results. Furthermore, it is used to refer to the test requirements in subclause 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 declared ISO/IEC 18000 part		
2	Mutual Authentication	Shall be tested with the authenticate command of the declared ISO/IEC 18000		

	with TTP involved	part		
3	Authenticate communication	Shall be tested with the AuthComm command of the declared ISO/IEC 18000 part		
4	Secure communication	Shall be tested with the SecureComm command of the declared ISO/IEC 18000 part		

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

6.2 Crypto suite requirements

This sub-clause contains all requirements of ISO/IEC 29167-16.

6.2.1 Crypto suite requirements of ISO/IEC 29167-16 in clauses 1 - 6

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

6.2.2 Crypto suite requirements of ISO/IEC 29167-16 in clauses 7 - 11

Table 2 contains all requirements of ISO/IEC 29167-16 in clauses 7 – 11.

The column MO (Mandatory / optional) has the following content:

M mandatory
Items marked with "M" are mandatory and shall be tested for all devices.

O optional
Items marked with "O" are optional and shall be tested only for devices that support the feature that is indicated by the requirement.

Table 2 — Crypto suite requirements

Item	Protocol Subclause	Requirement	MO	Applies To	How Verified
1	7.1	ECDHP: ECDH parameter, consist of parameter ID, parameter length and parameter content three parts, where the parameter ID shall be 8 bits; parameter shall be 16 bits in length and indicates the number of bytes in the parameter content. The values of ECDH parameter: 1) 01_h: The field value shall be denoted by OIDs. The Length subfield indicates the number of octets of OIDs. The values of Content subfield are the content of OIDs. 2) Other: All other values are RFU.	M	Interrogator Tag	By design
2	7.1	MK[127:0]	M	Interrogator	By design