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

This document is a preview generated by EVS

Reference number
ISO/IEC 19823-16:2020(E)

© ISO/IEC 2020

This document is a preview generated by EVS

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms, definitions, symbols and abbreviated terms ... **1**
3.1 Terms and definitions ... 1
3.2 Symbols ... 2
3.3 Abbreviated terms ... 2
4 Test methods ... **2**
4.1 General ... 2
4.2 By demonstration ... 2
4.3 By design ... 3
5 Test methods in respect to ISO/IEC 18000-4 Mode 4 ... **3**
5.1 Default items applicable to the test methods ... 3
5.1.1 Test environment ... 3
5.1.2 Pre-conditioning ... 3
5.1.3 Default tolerance ... 3
5.1.4 Total measurement uncertainty ... 3
5.2 Test setup and measurement equipment ... 3
5.2.1 Test setup for interrogator testing ... 4
5.2.2 Test setup for tag testing ... 4
5.2.3 Test equipment ... 4
6 Test methods in respect to ISO/IEC 29167-16 interrogators and tags ... **5**
6.1 Test map for optional features ... 5
6.2 Crypto suite requirements ... 5
6.2.1 General ... 5
6.2.2 Crypto suite requirements of ISO/IEC 29167-16:2015, Clauses 1 - 6 ... 5
6.2.3 Crypto suite requirements of ISO/IEC 29167-16:2015, Clauses 7 - 11 ... 5
6.2.4 Crypto suite requirements of ISO/IEC 29167-16:2015, Annex A ... 10
6.2.5 Crypto suite requirements of ISO/IEC 29167-16: 2015 in Annex E ... 11
6.3 Test patterns for ISO/IEC 18000-4:2018, Mode 4 ... 12
6.3.1 Test pattern 1 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 12
6.3.2 Test pattern 2 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 14
6.3.3 Test pattern 3 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 14
6.3.4 Test pattern 4 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 15
6.3.5 Test pattern 5 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 15
6.3.6 Test pattern 6 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 15
6.3.7 Test pattern 7 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 15
6.3.8 Test pattern 8 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 15
6.3.9 Test pattern 9 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 16
6.3.10 Test pattern 10 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 16
Annex A (informative) **Test parameters example** ... **17**
Bibliography ... **21**

This document is a preview generated by EVS

© ISO/IEC 2020 – All rights reserved

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.

This document is a preview generated by EVS

 © ISO/IEC 2020 – All rights reserved

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.

This document is a preview generated by EVS

© ISO/IEC 2020 – All rights reserved

This document is a preview generated by EVS

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

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

This document is a preview generated by EVS

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/

© ISO/IEC 2020 – All rights reserved