International Standard

ISO/IEC 19823-16

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

Part 16: Crypto suite ECDSA-ECDH

Technologies de l'information — Méthodes d'essai de conformité pour les suites cryptographiques des services de sécurité —

Partie 16: Suite cryptographique ECDSA-ECDH

Second edition
2026-03

Reference number
ISO/IEC 19823-16:2026(en)

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

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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

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

This second edition cancels and replaces the first edition (ISO/IEC 19823-16:2020), which has been technically revised.

The main changes are as follows:

— command codes have been technically revised, “01h” revised to “80h” in 6.3;

— normative references have updated – ISO/IEC 29167-16:2015 has been updated and ISO/IEC 29167-15:2022 has been removed.

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

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 and www.iec.ch/national-committees.

Introduction

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

The ISO/IEC 19823 series describes conformance test methods for security service crypto suites. The ISO/IEC 19823 series 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 be compliant to a pair of ISO/IEC 18000-n and ISO/IEC 29167-m, the test methods of ISO/IEC 18047-n and ISO/IEC 19823-m apply. If a product supports more than one part of the ISO/IEC 18000 series or the ISO/IEC 29167 series, all related parts of the ISO/IEC 18047 series and the ISO/IEC 19823 series apply.

This document describes the test methods for the elliptic curve digital signature algorithm-elliptic curve Diffie-Hellman (ECDSA-ECDH) crypto suite as defined in ISO/IEC 29167-16.

The conformance parameters are:

- parameters that apply directly affecting system functionality and inter-operability;
- protocol including commands and replies;
- nominal values and tolerances.

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

Part 16: Crypto suite ECDSA-ECDH

1 Scope

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

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

Unless otherwise specified, the tests in this document are only applicable to radio frequency identification (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 17025, *General requirements for the competence of testing and calibration laboratories*

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 19762, *Information technology — Automatic identification and data capture (AIDC) techniques — Vocabulary*

ISO/IEC 29167-16:2022, *Information technology — Automatic identification and data capture techniques — Part 16: Crypto suite ECDSA-ECDH security services for air interface communications*

Bibliography

[1] ISO/IEC 18000 (all parts), *Information technology — Radio frequency identification for item management*

[2] ISO/IEC 18047 (all parts), *Information technology — Radio frequency identification device conformance test methods*

[3] ISO/IEC 19823 (all parts), *Information technology — Conformance test methods for security service crypto suites*

[4] ISO/IEC 29167 (all parts), *Information technology — Automatic identification and data capture techniques*

[5] ISO Guide to the Expression of Uncertainty in Measurement, ISBN 92-67-10188-9, 1993.