INTERNATIONAL STANDARD

ISO/IEC 29167-16

Second edition
2022-11

Information technology — Automatic identification and data capture techniques —

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

Technologies de l'information — Techniques automatiques d'identification et de capture de données —

Partie 16: Services de sécurité de la suite cryptographique ECDSA-ECDH pour les communications d'interfaces aériennes



Reference number
ISO/IEC 29167-16:2022(E)

© ISO/IEC 2022



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

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

© ISO/IEC 2022 – All rights reserved

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **2**

4 Symbols and abbreviated terms ... **2**
4.1 Symbols ... 2
4.2 Abbreviated terms ... 2

5 Conformance ... **3**
5.1 Claiming conformance ... 3
5.2 Interrogator conformance and obligations ... 4
5.3 Tag conformance and obligations ... 4

6 Cipher introduction ... **4**

7 Parameter definitions ... **4**
7.1 Parameter definitions ... 4
7.2 Certiticate format ... 5

8 State diagram ... **6**

9 Initialization and resetting ... **6**

10 Authentication ... **7**
10.1 General ... 7
10.2 Authenticate message ... 7
10.2.1 Message in Authenticate command and reply ... 7
10.2.2 Authenticate(MAM1.1 Message) ... 8
10.2.3 MAM1.1 Response ... 9
10.2.4 Authenticate(MAM1.2 Message) ... 9
10.2.5 MAM1.2 Response ... 10
10.3 Authentication procedure ... 11
10.3.1 Protocol requirements ... 11
10.3.2 Procedure ... 11

11 Communication ... **13**
11.1 Authenticate communication ... 13
11.2 Secure communication ... 13

Annex A (normative) **State transition table** ... **15**

Annex B (normative) **Error codes and error handling** ... **16**

Annex C (normative) **Cipher description** ... **17**

Annex D (informative) **Test vectors** ... **18**

Annex E (normative) **Protocol specific operation** ... **23**

Annex F (normative) **Protocol message's fragmentation and defragmentation** ... **27**

Annex G (informative) **Examples of ECC parameters** ... **28**

Annex H (normative) **TTP involving** ... **29**

Bibliography ... **31**

© ISO/IEC 2022 – All rights reserved

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).

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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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 29167-16:2015), which has been technically revised.

The main changes are as follows:

— certain normative references have been updated;

— editorial and technical revisions have been made to maintain conformance with ISO/IEC 18000-4:2018.

A list of all parts in the ISO/IEC 29167 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.

© ISO/IEC 2022 – All rights reserved

Introduction

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of a patent.

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

The holder of this patent right has assured ISO and IEC that he/she is 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 the patent database available at www.iso.org/patents or https://patents.iec.ch.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those in the patent database. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

© ISO/IEC 2022 – All rights reserved

Information technology — Automatic identification and data capture techniques —

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

1 Scope

This document describes a crypto suite based on elliptic curve cryptography (ECC) for the ISO/IEC 18000 series of standards protocol. In particular, this document specifies the use of elliptic curve Diffie-Hellman (ECDH) key agreement in a secure channel establishment and the use of elliptic curve digital signature algorithm (ECDSA) in an authentication mechanism.

This document specifies a crypto suite for ECDSA-ECDH for air interface for RFID systems. The crypto suite is defined in alignment with existing air interfaces.

This document defines a mutual authentication method and methods of use for the cipher. A Tag and an Interrogator can support one, a subset, or all of the specified options, clearly stating what is supported. Key update is not supported in this document.

ECDSA-ECDH cipher is a high-weight security protocol especially for active RFID system, aiming at meeting those scenarios with high level security requirement.

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 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 — Harmonized vocabulary*

ISO/IEC 29167-1, *Information technology — Automatic identification and data capture techniques — Part 1: Security services for RFID air interfaces*

ISO/IEC 14888-3, *IT Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms*

ISO/IEC 11770-3, *Information security — Key management — Part 3: Mechanisms using asymmetric techniques*

ISO/IEC 9797-3, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 3: Mechanisms using a universal hash-function*

ISO/IEC 9798-3, *IT Security techniques — Entity authentication — Part 3: Mechanisms using digital signature techniques*

ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

© ISO/IEC 2022 – All rights reserved

ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

ISO/IEC 11770-6, *Information technology — Security techniques — Key management — Part 6: Key derivation*

3 Terms and definitions

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

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

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

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

3.1
command
message that interrogator sends to tag with "Message" as parameter

3.2
Message
part of the *command* (3.1) that is defined by the crypto suite

3.3
reply
response that tag returns to the interrogator with "Response" as parameter

3.4
Response
part of the *reply* (stored or sent) (3.3) that is defined by the crypto suite

4 Symbols and abbreviated terms

4.1 Symbols

$xxxx_2$	Binary notation
$xxxx_h$	Hexadecimal notation
||	Concatenation of syntax elements, transmitted in the order written
$()_{abscissa}$	Refers to that element of an ordered pair which is plotted on the horizontal axis of a two-dimensional cartesian coordinate system
•	Point multiply

4.2 Abbreviated terms

CRC	Cyclic redundancy check
CS	Crypto suite
CSI	Cryptographic suite identifier
DSA	Digital signature algorithm

© ISO/IEC 2022 – All rights reserved