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 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).

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.

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.

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 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

EBV	Extensible bit vector
ECC	Elliptic curve cryptography
ECDH	Elliptic curve Diffie-Hellman
ECDHP	ECDH parameter
ECDSA	Elliptic curve digital signature algorithm
FN	Fragmentation number
IAK	Integrity authentication key
IID	IDentifier of interrogator
MIC	Message integrity check code
MAC	Message authentication code
MAM	Mutual authenticate message
MK	Master key
MTU	Maximum transmission unit
RFU	Reserved for future use
RN	Random number
RFID	Radio frequency identification
SEK	Session encryption key
SIK	Session integrity check key
TID	IDentifier of tag
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

5 Conformance

5.1 Claiming conformance

To claim conformance with this document, an Interrogator or a Tag shall comply with all relevant clauses of this document except those marked as “optional”.

Relevant conformance test methods are provided in ISO/IEC 19823-16[1].

5.2 Interrogator conformance and obligations

To conform to this document, an Interrogator shall implement the mandatory messages and responses format defined in this document, and conform to the relevant part of the ISO/IEC 18000 series.

To conform to this document, an Interrogator may implement any subset of the optional parameters for message and response format defined in this document.

To conform to this document, the Interrogator shall not

— implement any messages and responses format that conflicts with this document, or

— require the use of an optional, proprietary, or custom parameters for message and response format to meet the requirements of this document.

5.3 Tag conformance and obligations

To conform to this document, a Tag shall implement the mandatory message and response formatting defined in this document for the supported types, and conform to the relevant part of the ISO/IEC 18000 series.

To conform to this document, a Tag may implement any subset of the optional parameters in the message and response formatting defined in this document.

To conform to this document, a Tag shall not

— implement any message and response formatting that conflicts with this document, or

— require the use of an optional, proprietary, or custom parameter in the message and response formatting to meet the requirements of this document.

6 Cipher introduction

The ECDSA is a variant of the DSA which uses ECC. ECDSA supports mutual authentication and has been specified in ISO/IEC 14888-3. The cipher descriptions of Annex C shall apply.

ECDH is an anonymous key agreement protocol that allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel. This shared secret shall be directly used as a key, or better yet, to derive another key which shall then be used to encrypt subsequent communications using a symmetric key cipher. It is a variant of the Diffie-Hellman protocol using ECC. ECDH protocol specified in ISO/IEC 11770-3 shall apply.

ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Compared to the RSA algorithm, ECC offers equivalent security with smaller key sizes which result in savings for power, memory, bandwidth, and computational resources that make ECC especially attractive for RFID system.

7 Parameter definitions

7.1 Parameter definitions

Table 1 contains the parameters definitions of the crypto suite.

Table 1 — Descriptions of parameters

Parameter	Description
FN[7:0]	The number of fragmentations.
AuthType[1:0]	This shows the authentication type in the authentication procedure. The values are as following: — 00: mutual authentication; — 01: reserved for the use of interrogator authentication; — 10: reserved for the tag authentication; — 11: Other (as defined by the CSI).
AuthStep[2:0]	This shows the step number in the authentication procedure. The values are as following: — 000: Step 1 of Authenticate command; — 001: Step 2 of Authenticate command; — 010-111: All other values are RFU.
ECDHP[255:0]	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) 01h: 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.
Certx[Variable]	The digital certificate of x. x can be tag, interrogator or TTP. See 7.2.
RNt[63:0]	64-bit random number generated by the tag.
X t[391:0]	Temporary private key generated by tag and used for ECDH exchange.
TPKt[391:0]	Temporary public key generated by tag and used for ECDH exchange, the procedure of generation is as follows: the tag generates a temporary private key which is used for ECDH exchange, and temporary public key TPKt=Xt•P.
TTPID[Variable]	Specifying whether or not the TTP is to be involved and the identifier of the TTP.
Sigt[383:0]	Digital signature generated by the tag.
RNi[63:0]	64-bit random number generated by the interrogator.
Xi[391:0]	Temporary private key generated by interrogator and used for ECDH exchange.
TPKi[391:0]	Temporary public key generated by interrogator and used for ECDH exchange, the procedure of generation is as follows: the interrogator generates a temporary private key which is used for ECDH exchange, the temporary public key TPKi=Xi•P.
MICi[255:0]	Message integrity code generated by the interrogator.
Sigi[383:0]	Digital signature generated by the interrogator.
MICt[255:0]	Message integrity code generated by the tag.
MK[127:0]	Master key.
AuthRes[Variable]	Authentication result generated by the TTP and contains the value of RESt, RESi and Sigttp.

ECC parameters example see Annex G.

7.2 Certificate format

Figure 1 specifies the encoding of digital certificate $Cert_x$ in the TLV format.

	Cert Type	Cert Length	Value
# of bits	4	12	variable

Figure 1 — Certificate format

The Cert Type subfield specifies the type of the certificate and shall be 4 bits in length. The values are:

a) 0000: Value subfield contains X.509 certificate of Interrogator, $Cert_i$;

b) 0001: Value subfield contains X.509 certificate of Tag, $Cert_t$;

c) 0010: Value subfield contains X.509 certificate of TTP, $Cert_{ttp}$;

d) Other: All other values are RFU.

The 12-bit Cert Length subfield contains the length in number of octets of the Value subfield, in the range of 1 to 4095.

8 State diagram

The state diagram for this cryptographic suite consists of four states. The transition between these states is specified in Figure 2. The state transition table of Annex A shall apply.

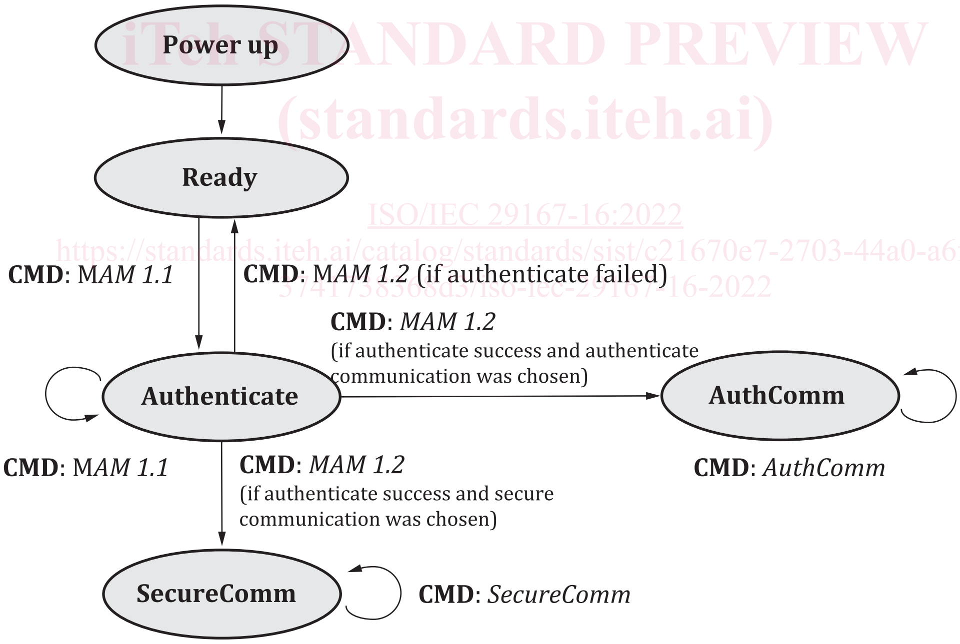

Figure 2 — State diagram

9 Initialization and resetting

This document shall implement Ready, Authenticate, AuthComm and SecureComm states.

After power-up and after a reset of the crypto suite the tag moves into the Ready state.

Implementations of this suite shall assure that all memory used for intermediate results is cleared after each operation (message-response pair) and after reset.

