INTERNATIONAL STANDARD

ISO/IEC 29167-16

First edition
2015-11-15

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 par suite cryptographique ECDSA-ECDH pour communications d'interface radio

Reference number
ISO/IEC 29167-16:2015(E)

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

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

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).

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 JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

ISO/IEC 29167 consists of the following parts, under the general title *Information technology — Automatic identification and data capture techniques*:

— *Part 1: Air Interface for security services and file management for RFID architecture*

— *Part 10: Air Interface for security services crypto suite AES128*

— *Part 11: Air Interface for security services crypto suite PRESENT-80*

— *Part 12: Air Interface for security services crypto suite ECC-DH*

— *Part 13: Air Interface for security services crypto suite Grain-128A*

— *Part 14: Air Interface for security services crypto suite AES-OFB*

— *Part 15: Air Interface for security services crypto suite XOR*

— *Part 16: Air Interface for security services crypto suite ECDSA-ECDH*

— *Part 17: Air Interface for security services crypto suite Crypto GPS*

— *Part 19: Air Interface for security services crypto suite RAMON*

Introduction

This international standard describes a crypto suite based on Elliptic Curve Cryptography (ECC) for the ISO/IEC 18000- series of standards protocol. In particular, it 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 international standard defines only mutual authentication for the ECDSA-ECDH cipher. An Interrogator or a Tag authentication is not supported in this international standard.

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

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning radio-frequency identification technology given in the clauses identified below.

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent rights have ensured 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 statements of the holders of these patent rights are registered with ISO and IEC.

Information on the declared patents may be obtained from:

NXP B.V. **411 East Plumeria, San José, CA 95134-1924 USA**
China IWNCOMM Co., LTD. **A201, QinFeng Ge, Xi'an Software Park, No.68 Keji 2nd Road, Xi'an Hi-tech Industrial Development Zone, Shaanxi, P. R. China 710075**
Impinj, Inc. **701 N 34th Street, Suite 300, Seattle, WA 98103 USA**

The latest information on IP that may be applicable to this part of ISO/IEC 29167 can be found at www.iso.org/patents.

Information technology — Automatic identification and data capture techniques —

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

1 Scope

This international standard describes a crypto suite based on Elliptic Curve Cryptography (ECC) for the ISO/IEC 18000- series of standards protocol. In particular, it 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 international standard 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 international standard defines a mutual authentication method and methods of use for the cipher. A Tag and an Interrogator may support one, a subset, or all of the specified options, clearly stating what is supported. Key update is not supported in this international standard.

2 Conformance

2.1 Claiming conformance

To claim conformance with this part of ISO/IEC 29167, an Interrogator or a Tag shall comply with all relevant clauses of this part of ISO/IEC 29167, except those marked as “optional”.

2.2 Interrogator conformance and obligations

To conform to this part of ISO/IEC 29167, an Interrogator shall

— implement the mandatory messages and responses format defined in this part of ISO/IEC 29167, and conform to the relevant part of ISO/IEC 18000

To conform to this part of ISO/IEC 29167, an Interrogator may

— implement any subset of the optional parameters for message and response format defined in this part of ISO/IEC 29167

To conform to this part of ISO/IEC 29167, the Interrogator shall not

— implement any messages and responses format that conflicts with this part of ISO/IEC 29167, or

— require the use of an optional, proprietary, or custom parameters for message and response format to meet the requirements of this part of ISO/IEC 29167.

2.3 Tag conformance and obligations

To conform to this part of ISO/IEC 29167, a Tag shall

— implement the mandatory message and response formatting defined in this part of ISO/IEC 29167 for the supported types, and conform to the relevant part of ISO/IEC 18000

To conform to this part of ISO/IEC 29167, a Tag may

— implement any subset of the optional parameters in the message and response formatting defined in this part of ISO/IEC 29167

To conform to this part of ISO/IEC 29167, a Tag shall not

— implement any message and response formatting that conflicts with this part of ISO/IEC 29167, or

— require the use of an optional, proprietary, or custom parameter in the message and response formatting to meet the requirements of this part of ISO/IEC 29167.

3 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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, *Information technology — Radio frequency identification for item management — Part 4: Parameters for air interface communications at 2,45 GHz*

ISO/IEC 19762 (all parts), *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 14888-3:2006, *Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms*

ISO/IEC 11770-3:2008, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

ISO/IEC 9798-3:1998/Amd.1:2010, *Information technology — Security techniques — Entity authentication — Part 3: Mechanisms using digital signature techniques / Amendment 1: .*

ISO/IEC 18031:2011, *Information technology — Security techniques — Random bit generation*

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

RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

4 Terms and definitions

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

4.1
command (message)
command that Interrogator sends to Tag with “Message” as parameter

4.2
message
part of the Command that is defined by the CS

4.3
reply (response)
reply that Tag returns to the Interrogator with “Response” as parameter

4.4
response
part of the Reply (stored or sent) that is defined by the CS

5 Symbols and abbreviated

5.1 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

5.2 Abbreviated terms

CRC	Cyclic Redundancy Check
CS	Crypto Suite
CSI	Cryptographic Suite Identifier
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
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

6 Cipher introduction

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a variant of the Digital Signature Algorithm (DSA) which uses Elliptic Curve Cryptography (ECC). ECDSA supports mutual authentication and has been specified in ISO/IEC 14888-3.

Elliptic curve Diffie–Hellman (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 has been specified in ISO/IEC 11770-3.

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 — Definition 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)

Table 1 *(continued)*

Parameter	Description
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) 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.
$Cert_x$[Variable]	The digital certificate of x. x can be tag, interrogator or TTP. See 7.2.
RN_t[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.
TPK_t[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 $TPK_t = X_t \bullet P$.
TTPID[Variable]	Specifying whether or not the TTP is to be involved and the identifier of the TTP
Sig_t[383:0]	Digital signature generated by the tag.
RN_i[63:0]	64-bit random number generated by the interrogator.
X_i[391:0]	Temporary private key generated by interrogator and used for ECDH exchange.
TPK_i[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 $TPK_i = X_i \bullet P$.
MIC_i[255:0]	Message integrity code generated by the interrogator.
Sig_i[383:0]	Digital signature generated by the interrogator.
MIC_t[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 RES_t, RES_i and Sig_{ttp}.

7.2 Certiticate 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

1. 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.

2. 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. See Annex A.

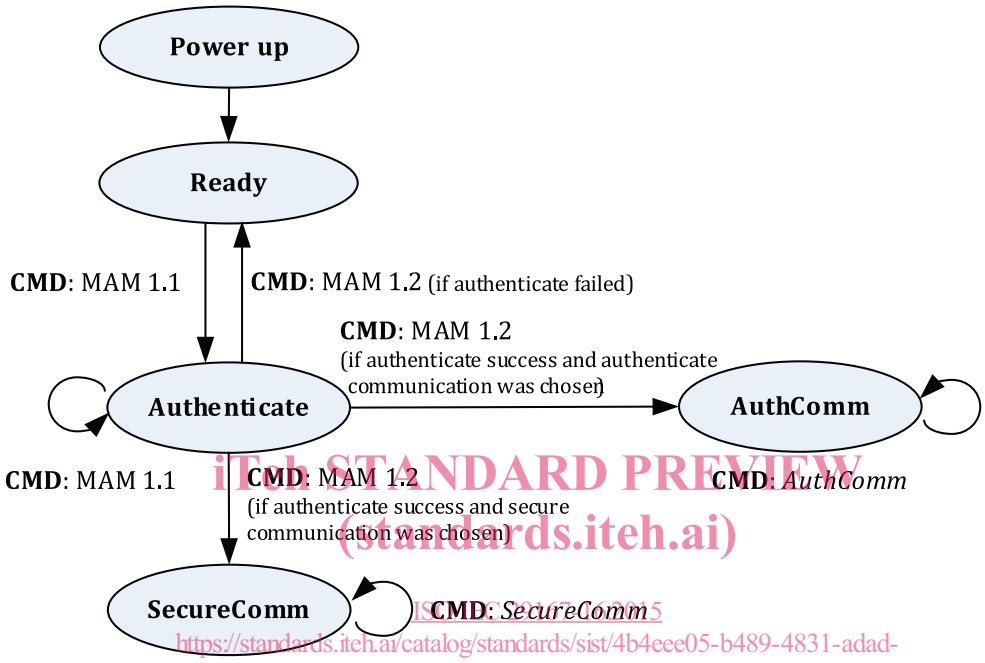

Figure 2 — State diagram

9 Initialization and resetting

This part of ISO/IEC 29167 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 ensure that all memory used for intermediate results is cleared after each operation (message-response pair) and after reset.

10 Authentication

10.1 General

This part of the standard describes additions to the ISO/IEC 18000 series of standards protocol to support the tag and reader air interface security (TRAIS) based on public key cryptography (TRAIS-P). Especially, it defines

1. the use of ECC certificates and Elliptic Curve Digital Signature Algorithm (ECDSA) for mutual authentication of an interrogator and a tag, and

2. the use of the Elliptic Curve Diffie-Hellman (ECDH) key agreement scheme with keys to establish the secure channel, and

