INTERNATIONAL STANDARD

ISO/IEC 29167-12

First edition
2015-05-15

Information technology — Automatic identification and data capture techniques —

Part 12: Crypto suite ECC-DH security services for air interface communication

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

Partie 12: Services de sécurité par suite cryptographique ECC-DH pour communications par interface radio

Reference number
ISO/IEC 29167-12:2015(E)

© ISO/IEC 2015



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
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 ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Conformance **1**
2.1 Claiming conformance 1
2.2 Interrogator conformance and obligations 1
2.3 Tag conformance and obligations 2

3 Normative references **2**

4 Terms and definitions **2**

5 Symbols and abbreviated terms **3**
5.1 Symbols 3
5.2 Abbreviated terms 4

6 Introduction of the ECC-DH crypto suite **5**
6.1 Core functionality 5
6.2 Design principles of the crypto suite 6

7 Parameter definitions **6**
7.1 Elliptic curve parameters 6
7.2 Parameters of the EPIF Format 7
7.3 Random number generation 7

8 Crypto suite state diagram **7**

9 Initialization and resetting **8**

10 Tag Authentication **8**
10.1 Introduction 8
10.2 Message and Response formatting 9
10.2.1 Concept 9
10.2.2 Description of Message and Response concept 9
10.2.3 Transmission order of the data 9
10.2.4 Parsing the Message 9
10.3 TAM1.0 10
10.3.1 TAM1.0 Message — write certificate data 10
10.3.2 TAM1.0 Response ..... status of write operation 11
10.3.3 Protection of certificate record 11
10.4 TAM1.1 11
10.4.1 TAM1.1 Message ..... request certificate data 11
10.4.2 TAM1.1 Response ..... certificate data 11
10.5 TAM1.2 12
10.5.1 TAM1.2: Message ..... send Interrogator challenge 12
10.5.2 TAM1.2 Response ..... authentication result 12
10.6 TAM1.3 13
10.6.1 TAM1.3: Message ..... request certificate data and send challenge 13
10.6.2 TAM1.3 Response ..... certificate data and authentication result 13

11 Certificate memory **13**
11.1 Concept 13

© ISO/IEC 2015 – All rights reserved

11.2 Certificate memory structure 14
11.3 Certificate record 15
11.4 Compressed X.509 certificate 15
11.5 X.509 certificate 17
11.6 Custom certificates 17

12 Tag authentication procedure 17
12.1 Processing steps 17
12.2 IChallenge generation and formatting 17
12.3 IChallenge examination 18
12.4 TResponse generation and formatting 18
12.5 TResponse examination 19

13 Communication 19

14 Key table and key update 20

Annex A (normative) **Cryptographic suite State transition table 21**

Annex B (normative) **Error conditions and error handling 22**

Annex C (normative) **Cipher description 23**

Annex D (informative) **Examples ECC cryptographic protocol 25**

Annex E (normative) **Air Interface Protocol specific information 27**

Annex F (normative) **Reconstruction of X.509 Certificate 30**

Bibliography 39

 © ISO/IEC 2015 – 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. 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*.

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

— *Part 1: Security services for RFID air interfaces*

— *Part 10: Crypto suite AES-128 security services for air interface communications*

— *Part 11: Crypto suite PRESENT-80 security services for air interface communications*

— *Part 12: Crypto suite ECC-DH security services for air interface communication*

— *Part 13: Crypto suite Grain-128A security services for air interface communications*

— *Part 14: Crypto suite AES OFB security services for air interface communications*

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

— *Part 17: Crypto suite cryptoGPS security services for air interface communications*

— *Part 19: Crypto suite RAMON security services for air interface communications*

The following parts are under preparation:

— *Part 15: Crypto suite XOR security services for air interface communications*

© ISO/IEC 2015 – All rights reserved

Introduction

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly-known base point is computationally infeasible. The size of the elliptic curve determines the difficulty of the problem.

This part of ISO/IEC 29167 specifies the security services for an RFID Tag with an ECC-DH crypto suite based on the Diffie-Hellman key exchange algorithm. It specifies the details of a protocol and interface format for application with RFID Tags which provide unilateral authentication capability, based on the use of ECC. Although such Tags can operate in any frequency band legitimate for such applications, the main focus of this part of ISO/IEC 29167 is on externally-powered (also called "passive") Tags designed for the HF/UHF frequency bands, where the demands on low silicon footprint and power consumption are most stringent.

This part of ISO/IEC 29167 defines only Tag authentication for the ECC-DH cipher.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this part of ISO/IEC 29167 may involve the use of patents concerning radio-frequency identification and cryptographic technologies 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 licenses 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:

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.

© ISO/IEC 2015 – All rights reserved

Information technology — Automatic identification and data capture techniques —

Part 12: Crypto suite ECC-DH security services for air interface communication

1 Scope

This part of ISO/IEC 29167 defines the crypto suite for ECC-DH for the ISO/IEC 18000 air interfaces standards for radio frequency identification (RFID) devices. Its purpose is to provide a common crypto suite with Diffie-Hellmann-based authentication using ECC (elliptic curve cryptography) over binary fields for security for RFID devices that may be referred by ISO committees for air interface standards and application standards.

This part of ISO/IEC 29167 specifies a crypto suite for ECC-DH for air interface for RFID systems. The crypto suite is defined in alignment with existing air interfaces.

This part of ISO/IEC 29167 defines various authentication methods 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.

2 Conformance

2.1 Claiming conformance

To claim conformance with this part of ISO/IEC 29167, an Interrogator or 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 commands 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 commands defined in this part of ISO/IEC 29167.

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

— implement any command that conflicts with this part of ISO/IEC 29167, or

— require the use of an optional, proprietary, or custom command to meet the requirements of this part of ISO/IEC 29167.

© ISO/IEC 2015 – All rights reserved

2.3 Tag conformance and obligations

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

— implement the mandatory commands 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 commands defined in this part of ISO/IEC 29167.

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

— implement any command that conflicts with this part of ISO/IEC 29167, or

— require the use of an optional, proprietary, or custom command 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 18000-63, *Information technology — Radio frequency identification for item management — Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C*

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*

FIPS PUB 186-4, *Digital Signature Standard (DSS)*[1)]

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
Certificate
digitally signed statement binding a Public Key to an Identity

Note 1 to entry: The term “Certificate” is also known as “Public Key Certificate”.

4.3
double-word
bit string comprised of 32 bits

4.4
entropy
randomness collected by an operating system or application for use in cryptography or other uses that require random data

1) http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

© ISO/IEC 2015 – All rights reserved