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*