INTERNATIONAL STANDARD

ISO/IEC 29167-17

First edition
2015-06-01

Information technology — Automatic identification and data capture techniques —

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

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

Partie 17: Services de sécurité par suite cryptographique cryptoGPS pour communications d'interface radio

Reference number
ISO/IEC 29167-17:2015(E)

COPYRIGHT PROTECTED DOCUMENT

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*, 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: 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 communications*
- *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 part is under preparation:

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

Introduction

cryptoGPS is a lightweight asymmetric identification scheme that is suitable for RFID Tag authentication. While there are many types of such scheme, the computational costs for the Tag when using cryptoGPS are relatively low. This is particularly the case since cryptoGPS is well-suited to an implementation strategy using what is referred to as “coupons”. These are the results given by a modest off-line pre-computation, with coupons being used by the prover at each invocation of the cryptoGPS scheme. The resultant scheme offers very useful performance trade-offs.

This part of ISO/IEC 29167 specifies the security services of the cryptoGPS cryptographic suite that provides Tag authentication.

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 might 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 assured 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 can be obtained from:

Orange
38-40, rue du General Leclerc
F-92794 Issy Les Moulineaux CEDEX 9

The latest information on IP that might 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 17: Crypto suite cryptoGPS security services for air interface communications

1 Scope

This part of ISO/IEC 29167 defines the cryptoGPS cryptographic suite for the ISO/IEC 18000 air interfaces standards for radio frequency identification (RFID) devices. Its purpose is to provide a common crypto suite for security for RFID devices that might be referred by ISO committees for air interface standards and application standards.

This part of ISO/IEC 29167 defines a lightweight mechanism using asymmetric techniques and providing a unilateral authentication mechanism whose security is related to the difficulty of taking discrete logarithms on elliptic curves.

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 message and response formatting 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 might

— implement any subset of the parameters for message and response formatting 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.

2.3 Tag conformance and obligations

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

— implement the 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 might

— implement any subset of the parameters for 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 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 9798-5:2010, *Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero-knowledge techniques*

ISO/IEC 15946-1, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General*

ISO/IEC 18000-3, *Information technology — Radio frequency identification for item management — Part 3: Parameters for air interface communications at 13,56 MHz*

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*

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
asymmetric cryptographic technique
cryptographic technique that uses two related operations: a public operation defined by a public data item, and a private operation defined by a private data item

Note 1 to entry: The two operations have the property that, given the public operation, it is computationally infeasible to derive the private operation.

[SOURCE: ISO/IEC 9798-5:2009, 2.3]

4.2
asymmetric pair
two related data items where the private data item defines a private operation and the public data item defines a public operation

[SOURCE: ISO/IEC 9798-5:2009, 2.5]