INTERNATIONAL STANDARD

ISO/IEC 29167-14

First edition
2015-10-15

Information technology — Automatic identification and data capture techniques —

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

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

Partie 14: Services de sécurité par suite cryptographique AES-OFB pour communications d'interface radio

Reference number
ISO/IEC 29167-14:2015(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: 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 parts are under preparation:

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

— *Part 20: Air interface for security services — Cryptographic Suite Algebraic Eraser*

Introduction

This part of ISO/IEC 29167 describes a cryptographic suite that is applicable to the ISO/IEC 18000 standard. The ISO/IEC 18000 series of standards on RFID for item management do not contain any strong cryptographic security. The unique item identifier (UII) of tags is transmitted during the identification/singulation process to every reader that is able to communicate according to the standard. Sensitive data that are communicated from the interrogator, such as passwords and certain data written to memory, could be cover-coded with a one-time pad obtained from the tag. The tag sends this one-time pad over the air in plain text allowing an attacker to easily intercept all communications. Additionally, passwords are limited in length, providing limited security for the system. This part of ISO/IEC 29167 will fill this security gap for applications requiring a high level of security. Furthermore, it is applicable to applications requiring a large amount of data to be communicated between interrogators and tags.

This part of ISO/IEC 29167 covers the air interface for RFID tags that have a security module on board and its corresponding interrogators. Any other means of security is not addressed in this part of ISO/IEC 29167. A security module according to this part of ISO/IEC 29167 is either a means to provide read or write access limitations, password protection or a crypto engine. The use of a crypto engine is the typical case and all others are less likely.

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 can 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 may be obtained from:

Contact details	
Patent holder:	
Electronics Telecommunication Reseach Institute	
Contact for license application:	
Name & Department:	Ickchan, Lee, Intellectual Property Management Team
Address:	138 Gajeongno, Yuseong-gu
Address:	Daejeon, 305-700, Korea
Tel.	+82-42-860-6904
Fax	+82-42-860-3831
E-mail	ickchanlee@etri.re.kr
URL (optional)	www.etri.re.kr
Patent Holder:	
Legal Name	Impinj, Inc.
Contact for license application:	
Name & Department	Stacy Jones
Address	701 N. 34th Street, Suite 300
Address	Seattle, WA 98103, USA
Tel.	+1.206 834 1032
Fax	+1.206 517 5262

E-mail	stacy.jones@impinj.com
URL (optional)	www.impinj.com

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

1 Scope

This part of ISO/IEC 29167 defines the cryptographic suite for AES using OFB mode (AES OFB) for the ISO/IEC 18000-63 air interface standard for radio frequency identification (RFID) devices. Its purpose is to provide a common cryptographic suite for security for RFID devices that can be referenced by ISO committees for air interface standards and application standards.

This part of ISO/IEC 29167 specifies a cryptographic suite for AES OFB for air interface for RFID systems. The cryptographic 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 can 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 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.

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 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*