INTERNATIONAL STANDARD

ISO/IEC 29167-11

First edition
2014-08-01

Information technology — Automatic identification and data capture techniques —

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

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

Partie 11: Services de sécurité par suite cryptographique PRESENT-80 pour communications par interface radio

© ISO/IEC 2014

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:*

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

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

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

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

— *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 cryptoGPS*

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

Introduction

This part of ISO/IEC 29167 specifies the security services for Tag authentication of a PRESENT crypto suite that is based on a lightweight block cipher with a block size of 64 bits. While PRESENT supports both 80 and 128 bits, the version specified in this crypto suite uses only 80-bit keys.

This part of ISO/IEC 29167 only defines procedures for Tag authentication using PRESENT-80.

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.

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:

Impinj, Inc.
701 N 34th Street, Suite 300
Seattle, WA 98103
USA

The latest information on IP that can be applicable to this document can be found at www.iso.org/patents.

Information technology — Automatic identification and data capture techniques —

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

1 Scope

This part of ISO/IEC 29167 defines the crypto suite for PRESENT-80 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 can be referred by ISO committees for air interface standards and application standards. PRESENT-80 is a symmetric block cipher that can process data blocks of 64 bits, using a key length of 80 bits.

This part of ISO/IEC 29167 specifies a crypto suite for PRESENT-80 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 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 the relevant part of ISO/IEC 18000.

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

— 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 the relevant part of ISO/IEC 18000.

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

— 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*

ISO/IEC 29192-2:2011,*(E) — Information technology — Security techniques — Lightweight cryptography — Part 2: Block ciphers.*