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

Reference number
ISO/IEC 29167-11:2014(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

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.*

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
bit string
ordered sequence of 0's and 1's

4.2
block cipher
family of permutations and their inverse that is parameterized by a cryptographic key; permutations map bit strings of a fixed length to bit strings of the same length

4.3
block size
number of bits in an input (or output) block of the block cipher

4.4
cryptographic key
string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa

4.5
command (Message)
data that Interrogator sends to Tag with "Message" as parameter

4.6
data block (Block)
sequence of bits whose length is the block size of the block cipher

4.7
input block
data that is an input to either the forward cipher function or the inverse cipher function of the block cipher algorithm

4.8
message
part of the command that is defined by the crypto suite

4.9
output block
data that is an output of either the forward cipher function or the inverse cipher function of the block cipher algorithm

4.10
PRESENT-80-ENC (key, data)
single block PRESENT encryption with 80 bit cryptographic key "key" of input data "data"

4.11
PRESENT-80-DEC (key, data)
single block PRESENT decryption with 80 bit cryptographic key 'key' of input data 'data'

4.12
reply (Response)
data that Tag returns to the Interrogator with "Response" as parameter

4.13
response
part of the reply (stored or sent) that is defined by the crypto suite

5 Symbols and abbreviated terms

5.1 Symbols

$xxxx_2$	binary notation
$xxxx_h$	hexadecimal notation
||	concatenation of syntax elements, transmitted in the order written
Field[a:b]	selection from a string of bits in Field Selection ranges from bit "a" till and including bit "b" from the bits of the string in Field, whereby Field[0] represents the least significant bit. For example Field[2:0] represents the selection of the three least significant bits of Field.

5.2 Abbreviated terms

RFU	Reserved for future use
SPN	Substitution Permutation Network

6 Introduction of the PRESENT-80 crypto suite

PRESENT is a Substitution Permutation Network (SPN) block cipher that is suitable for extremely constrained environments such as RFID Tags. The references for understanding the operation of the PRESENT cipher are listed in Annex C and it is standardised in ISO/IEC 29192-2:2011.

The background for the development of PRESENT-80 and its design principles are described in ISO/IEC 29192-2:2011.

7 Parameter definitions

Table 1 describes all the parameters that are used in this part of ISO/IEC 29167.

Table 1 — Definition of PRESENT-80 crypto suite parameters

Parameter	Description
IChallenge[41:0]	42-bit challenge of Interrogator for challenge-response protocol
TRnd[19:0]	20-bit random value generated by Tag
C_TAM1[1:0]	2-bit predefined constant with value “00_b”
TAM-key[79:0]	80-bit key that is stored in the Tag and will be used for TAM1

8 Crypto Suite State diagram

After power-up and after a reset the crypto suite transitions into the **Initial** state.

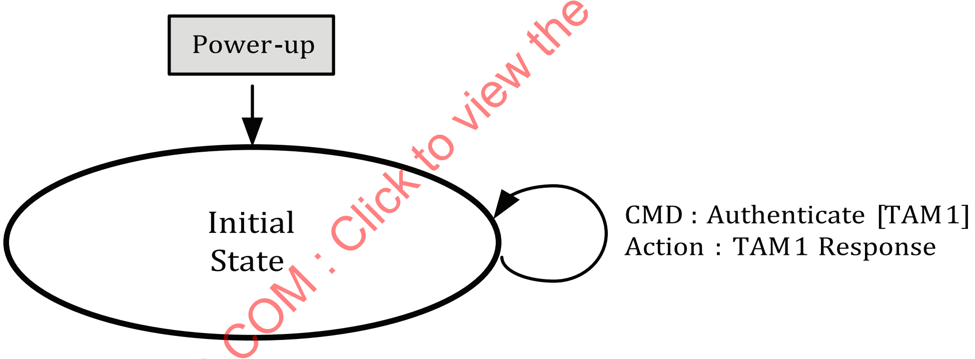

Figure 1 — Crypto Suite state diagram.

9 Initialization and resetting

After power-up and after a reset the crypto suite transitions into the **Initial** state.

Implementations of this suite shall assure that all memory used for intermediate results is cleared after each operation (message-response pair) and after reset.

10 Authentication

10.1 Introduction

This part of ISO/IEC 29167 supports Tag authentication, to be referred to as Method “00”.

This section describes the details of the messages and responses that are exchanged between the Interrogator and the Tag.

10.2 Message and Response formatting

Message and Response are part of the security commands that are described in the air interface specification. The following sections of this document describe the formatting of Message and Response for a Tag authentication method.

10.3 Tag authentication (Method “00” = TAM1)

Tag authentication uses a challenge-response protocol.

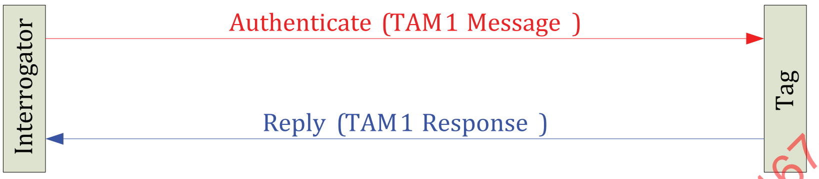

Figure 2 — Tag authentication.

10.3.1 Authenticate (TAM1 Message)

The Interrogator shall generate a 42-bit random Interrogator challenge (IChallenge) that is carried in the TAM1 message. There are no additional options during the authentication protocol.

Table 2 — TAM1 Message format

	AuthMethod	**RFU**	**IChallenge**
# of bits	2	4	42
description	00_b	0000_b	IChallenge

The Tag shall accept this message at any time (unless occupied by internal processing and not capable of receiving messages); i.e. upon receipt of the message with valid parameters the Tag shall abort any cryptographic protocol that has not yet been completed and shall remain in the **Initial** state.

The Tag shall check if AuthMethod is “00_b”. If the value of AuthMethod is different the Tag shall return a “Not Supported” error condition.

The Tag shall check if the RFU is “0000_b”. If the value of RFU is different the Tag shall return a “Not Supported” error condition.

10.3.2 TAM1 Response

Assuming the TAM1 message is successfully parsed by the Tag, the Tag calculates its response and answers accordingly.

The Tag encrypts the challenge IChallenge (42 bits) of the Interrogator after first prefixing the constant C_TAM1 together with a randomly generated TRnd (20 bits). The Tag shall use a preconfigured key (TAM_key) for this encryption. The key TAM_key shall only be used for tag authentication.

NOTE only one input block (64 bits) is encrypted and so only one invocation of PRESENT-80 is required.

Table 3 — TAM1 Response

	TResponse
# of bits	64
description	PRESENT-80-ENC (TAM_key, C_TAM1[1:0] || TRnd[19:0] || IChallenge[41:0])

10.3.3 Final Interrogator Processing

The Interrogator decrypts the TAM1 Response [TResponse] with the key TAM_key and verifies that both C_TAM1 and IChallenge have the correct value. The Interrogator accepts the Tag as valid if these fields have the correct value.

Note How the correct value for TAM_key is determined by the Interrogator is a matter of key management and falls outside of the scope of this part of ISO/IEC 29167.

10.3.4 Communication

This crypto suite does not support secure communication.

11 Key table and key update

This crypto suite does not support updating the key.

Annex A
(normative)

Crypto Suite State transition table

Table A.1 — Crypto Suite State transition table

Start State	Transition	End State	Result
Initial	TAM1	**Initial**	not applicable

Annex B
(normative)

Error conditions and error handling

A Tag that encounters an error during the execution of a crypto suite operation might send an error reply to the Interrogator. The details of these error replies are defined in the respective air interface standards.

This annex contains a listing of the Error Conditions that can result from the operation of this crypto suite. Annex E defines how to translate this error condition into an error code for the air interface.

Table B.1 — Error conditions

Error-Condition	Description
Not Supported	The requested functionality is not supported by this crypto suite.

Annex C
(normative)

Formal Reference for PRESENT

PRESENT is a block cipher with an SPN structure. It can take both 80- and 128-bit keys and it was designed from first principles to be suitable for constrained hardware environments while offering excellent levels of security. PRESENT was originally published, along with design criteria, and standardized in ISO/IEC 29192-2:2011(E). The cipher has been widely analyzed in the cryptographic community.

Annex D
(informative)

Test vectors

Table D.1 provides test vectors for encrypting plaintext messages using the PRESENT-80 block cipher.

Table D.1 — Test vectors

Plaintext	Key	Ciphertext
$00000000_h \Vert 00000000_h$	$00000000_h \Vert 00000000_h \Vert 0000_h$	$5579C138_h$ $7B228445_h$
$00000001_h \Vert 00000001_h$	$00000000_h \Vert 00000000_h \Vert 0000_h$	$086FC044_h$ $9733895B_h$
$00000001_h \Vert 00000001_h$	$00000000_h \Vert 00000000_h \Vert 0001_h$	$65249D8F_h$ $0626D7FD_h$
$FFFFFFFF_h \Vert FFFFFFFF_h$	$00000000_h \Vert 00000000_h \Vert 0000_h$	$A112FFC7_h$ $2F68417B_h$
$00000000_h \Vert 00000000_h$	$FFFFFFFF_h \Vert FFFFFFFF_h \Vert FFFF_h$	$E72C46C0_h$ $F5945049_h$
$FFFFFFFF_h \Vert FFFFFFFF_h$	$FFFFFFFF_h \Vert FFFFFFFF_h \Vert FFFF_h$	$3333DCD3_h$ $213210D2_h$

Annex E
(normative)

Protocol specific information

E.1 General

For the implementation of this crypto suite an air interface protocol shall support security commands that allow the exchange of data between the Interrogator and the Tag. The security command contains a message with parameters for the crypto suite. The reply of the Tag contains a response with the data that is returned by the crypto suite. An example of such data exchange for this crypto suite is depicted in Figure E.1.

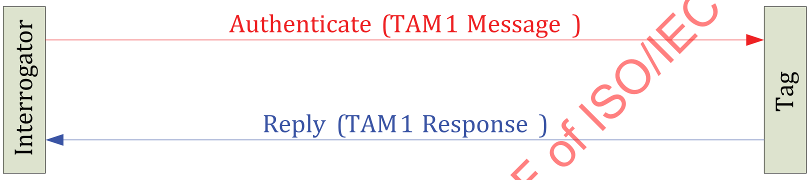

Figure E.1 — Message exchange for Tag authentication

The crypto suites that are defined by ISO/IEC 29167 can be defined by their Crypto Suite Identifier (CSI). According to ISO/IEC 29167-1 the CSI for this crypto suite shall be defined as the 6-bit value “000001_2”.

E.1.1 Supported Security Services

Table E.1 shows the security services that are supported by this crypto suite.

Table E.1 — Security Services

Security Services	Method	Mandatory, optional, prohibited, or not supported[A]
Authentication		Mandatory
Tag authentication (TA)		Mandatory
Interrogator authentication (IA)		Not supported
Mutual Authentication (MA)		Not supported
Communication		
Authenticated Tag from TA	Authenticated communication (Tag => Interrogator)	Not supported
	Secure authenticated communication (Tag => Interrogator)	Not supported
Authenticated Interrogator from IA	Authenticated communication (Interrogator => Tag)	Not supported
	Secure authenticated communication (Interrogator => Tag)	Not supported

[A] A crypto suite shall identify for each security service above and method if it is mandatory, optional, or prohibited