INTERNATIONAL STANDARD

ISO/IEC 29167-11

Second edition
2023-02

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: Interface radio pour services sécurité – Suite cryptographique PRESENT-80 security services for air interface communications

Reference number
ISO/IEC 29167-11:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

SO (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.

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 or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 29167-11:2014), which has been technically revised.

The main changes are as follows:

— the Interrogator authentication and Tag-Interrogator mutual authentication has been added;

— the variant of PRESENT that uses a 128-bit key has been added.

A list of all parts in the ISO/IEC 29167 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of a patent.

ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured ISO and IEC that he/she is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from the patent database available at www.iso.org/patents or https://patents.iec.ch.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those in the patent database. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Information technology — Automatic identification and data capture techniques —

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

1 Scope

This document defines the crypto suite for PRESENT-80 for the ISO/IEC 18000 series of air interfaces standards for radio frequency identification (RFID) devices. This document provides a common crypto suite for security for RFID devices for air interface standards and application standards. The crypto suite is defined in alignment with existing air interfaces.

This document specifies basic security services that are use the lightweight block cipher PRESENT-80. The variant of PRESENT that takes 128-bit keys is also considered in this document.

This document defines various 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 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. 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 (all parts), *Information technology — Radio frequency identification for item management*

ISO/IEC 19762, *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*

3 Terms, definitions, symbols and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1.1
bit string
ordered sequence of 0's and 1's

3.1.2
block cipher
family of permutations parameterized by a *cryptographic key* (3.1.3); permutations map bit strings of a fixed length given by the block size to bit strings of the same length

3.1.3
cryptographic key
string of bits of a specified length that is used by the *block cipher* (3.1.2) to transform a *data block* (3.1.4)

3.1.4
data block
string of bits whose length is given by the block size (3.1.3) of the *block cipher* (3.1.2)

3.1.5
PRESENT-*k*-ENC(key, data)
PRESENT encryption of **data**, a 64-bit *data block* (3.1.4), using **key**, a *k*-bit *cryptographic key* (3.1.3)

3.1.6
PRESENT-*k*-DEC(key, data)
PRESENT decryption of **data**, a 64-bit *data block* (3.1.4), using **key**, a *k*-bit *cryptographic key* (3.1.3)

3.1.7
salt
string of bits, typically randomly generated, that is used to diversify a cryptographic computation

3.2 Symbols

$XXXX_2$ Binary notation

$XXXX_h$ Hexadecimal notation

|| Concatenation of syntax elements, transmitted in the order written

Ø Empty string, typically used to indicate a deliberately empty input or omitted field

|A| Bit-wise length of the string A expressed as an integer

EXAMPLE 1 $|0000_2| = 4$

EXAMPLE 2 $|0000_h| = 16$

EXAMPLE 3 |Ø| = 0

Field [a:b] Selection of bits from a string of bits denoted Field

The selection ranges from bit "a" through to, and including, bit "b" where Field [0] represents the least significant or rightmost bit.

EXAMPLE 1 Field [2:0] represents the selection of the three least significant bits of Field.

EXAMPLE 2 Field, without a specified range, indicates the entirety of Field.

EXAMPLE 3 Field [-1:0] is an alternative representation of the empty string Ø.

Field [~] Non-empty string constructed from a string of bits denoted Field

Key.KeyID Cryptographic key identified and indexed by the numerical value KeyID

3.3 Abbreviated terms

CS	Crypto Suite
CSI	Crypto Suite Indicator
IA	Interrogator authentication
IChallenge	Interrogator challenge
MA	Mutual Authentication
RFU	Reserved for future use
RFID	Radio frequency identification
TA	Tag authentication
TID	Tag Identification number

4 Conformance

4.1 Air interface protocol specific information

An Interrogator or Tag shall comply with all relevant clauses of this document, except those marked as "optional".

Relevant conformance test methods are provided in ISO/IEC 19823-11[1].

4.2 Interrogator conformance and requirements

The Interrogator shall implement the mandatory commands defined in this document and conform to the relevant part of the ISO/IEC 18000 series.

The Interrogator can implement any subset of the optional commands defined in this document.

The Interrogator shall not:

— implement any command that conflicts with this document; or

— require the use of an optional, proprietary or custom command to meet the requirements of this document.

4.3 Tag conformance and requirements

The Tag shall implement the mandatory commands defined in this document for the supported types and conform to the relevant part of the ISO/IEC 18000 series.

The Tag can implement any subset of the optional commands defined in this document.

The Tag shall not:

— implement any command that conflicts with this document; or

— require the use of an optional, proprietary or custom command to meet the requirements of this document.

5 Introduction of the PRESENT-80 cryptographic suite

PRESENT-80 is a block cipher that uses an 80-bit key and is designed to be suitable for extremely constrained environments such as RFID Tags.

The details of the operation of the PRESENT-80 cipher are provided in Annex C. The background to the development of PRESENT-80 and its design principles are described in Reference [3].

A variant of PRESENT-80, denoted PRESENT-128, supports keys of length 128 bits.

Guidance on the appropriate variant to use in a given application lies outside the scope of this document. A thorough security and risk assessment is advised before deployment. Errors and error-handling for this cryptographic suite shall be in accordance with Annex B.

Test vectors for parts of this document are provided in Annex D.

Over-the-air protocol commands that use this cryptographic suite shall be in accordance with Annex E.

6 Parameter and variable definitions

Table 1 lists the variables and constants that are used in this document.

Table 1 — PRESENT-80 cryptographic suite variables and constants

Parameter	Description
IChallenge	A random challenge generated by the Interrogator
TChallenge	A random challenge generated by the Tag
TRnd	A random salt value generated by the Tag
IRnd	A random salt value generated by the Interrogator
CTAM	A pre-defined constant set to the two-bit value 00_2
CIAM	A pre-defined constant set to the two-bit value 01_2
CMAM1	A pre-defined constant set to the two-bit value 10_2
CMAM2	A pre-defined constant set to the two-bit value 11_2
PurposeIAM	Purpose bits for Interrogator authentication If PurposeIAM[3:3] = 0_2, the bits [2:0] are RFU with value 000_2. If PurposeIAM[3:3] = 1_2, the bits [2:0] are manufacturer defined.
PurposeMAM	Purpose bits for Mutual authentication If PurposeMAM[3:3] = 0_2, the bits [2:0] are RFU with value 000_2. If PurposeMAM[3:3] = 1_2, the bits [2:0] are manufacturer defined.
Key.0 ... Key.15	A set of up to 16 keys Key.0 through to Key.15 Not all key values need to be specified. However, Key.j shall not be specified when there remains an unspecified Key.i with i<j. If there is only one key on the Tag, it shall be identified as Key.0.

7 Crypto suite state diagram

After power-up and after a reset, the cryptographic engine transitions into the **Initial** state. The cryptographic engine shall follow the state transition in Table A.1. The state progressions defined by the state transition table in Annex A is illustrated in Figure 1.

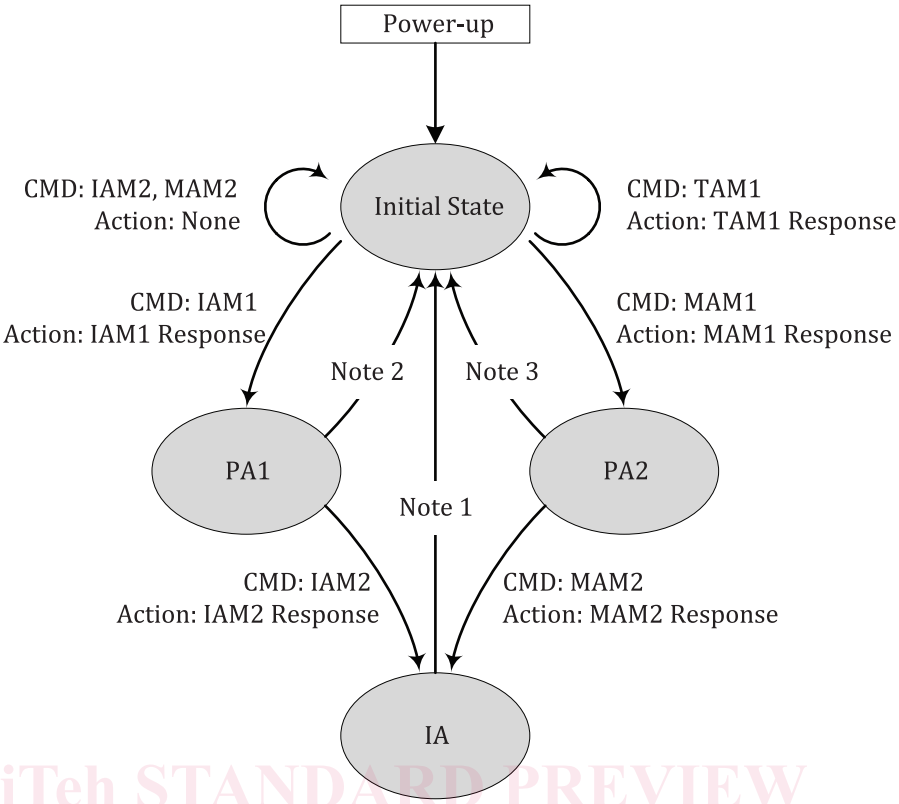

Figure 1 — Cryptographic engine state diagram

NOTE 1 For all of TAM1, IAM1, MAM1, IAM2, MAM2 and errors return to Initial State without action.

NOTE 2 For all of TAM1, IAM1, MAM1, MAM2 and errors return to Initial State without action.

NOTE 3 For all of TAM1, IAM1, MAM1, IAM2 and errors return to Initial State without action.

8 Initialization and resetting

After power-up and after a reset the cryptographic engine transitions into the **Initial** state.

Implementations of this suite shall ensure that all memory used for any intermediate results is cleared

a) after the completion of each cryptographic protocol,

b) if some cryptographic protocol is abandoned or incomplete, and

c) after reset.

9 Authentication

9.1 Introduction

This document supports Tag authentication, Interrogator authentication and Tag-Interrogator mutual authentication.

9.2 Message and response formatting

Messages and responses are part of the security commands described in the air interface specification. The following subclauses of this document describe the formatting of message and response for a

Tag authentication method, an Interrogator authentication method and a Tag-Interrogator mutual authentication method.

Different authentication methods are identified using the AuthMethod field. The values for this field are given in Table 2.

Table 2 — Values and descriptions for AuthMethod[1:0]

Value	Description
00_2	Tag authentication
01_2	Interrogator authentication
10_2	Tag-Interrogator authentication
11_2	Vendor defined

9.3 Tag authentication: AuthMethod "00"

9.3.1 General

Tag authentication uses a challenge-response protocol. This is illustrated in Figure 2.

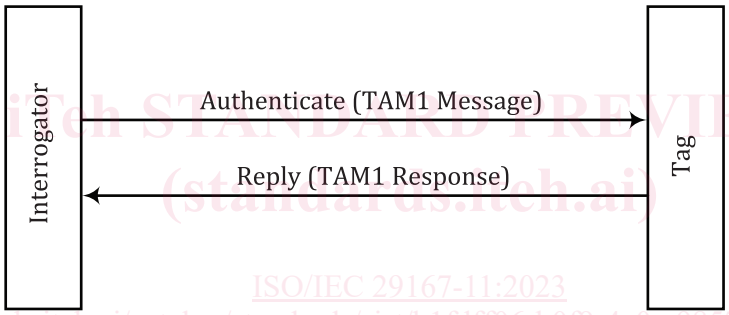

Figure 2 — Tag authentication via a challenge-response scheme

9.3.2 TAM1 message

The Interrogator shall generate a random IChallenge that is carried in the TAM1 message. The format of the TAM1 message is given in Table 3.

The Interrogator may choose optional extended functionality for the TAM1 message. The Interrogator may identify the cryptographic key Key.KeyID that should be used and, for Key.KeyID, whether it is 80 or 128 bits long.

NOTE 1 If a Tag supports anything other than a single 80-bit key, then extended functionality is required.

NOTE 2 Determining Key.KeyID is a matter of key management that lies outside the scope of this document.

NOTE 3 The variant(s) of PRESENT deployed on a device are manufacturer dependent.

NOTE 4 Appropriate mechanisms to generate IChallenge lie outside the scope of this document.