International Standard

ISO/IEC 29167-10

Information technology — Automatic identification and data capture techniques —

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

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

Partie 10: Services de sécurité par suite cryptographique AES-128 pour communications par interface radio

Third edition
2026-03

Reference number
ISO/IEC 29167-10:2026(en)

COPYRIGHT PROTECTED DOCUMENT

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

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.

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).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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 third edition cancels and replaces the second edition (ISO/IEC 29167-10:2017), which has been technically revised.

The main change is as follows: requirements in Clause E.4 have been updated to reflect changes to the corresponding over-the-air protocol.

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

This document provides a common crypto suite for security for radio frequency identification (RFID) devices. The crypto suite is defined in alignment with existing air interfaces and specifies a variety of security services provided by the symmetric block cipher AES-128.

A crypto suite only supports the encryption on the Tag and use the encryption for “encrypting” messages sent from the Tag to the Interrogator and “decrypting” messages received from the Interrogator.

Information technology — Automatic identification and data capture techniques —

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

1 Scope

This document specifies the crypto suite for AES-128 for the ISO/IEC 18000 air interface standards for radio frequency identification (RFID) devices.

This document specifies the security services of an AES-128 crypto suite. AES has a fixed block size of 128 bits and a key size of 128 bits, 192 bits or 256 bits. This document uses AES with a fixed key size of 128 bits and is referred to as AES-128.

This document specifies procedures for the authentication of a Tag and or an Interrogator using AES-128 and provides the following features:

— Tag authentication;

— Tag authentication allowing authenticated and encrypted reading of part of the Tag's memory;

— Interrogator authentication;

— Interrogator authentication allowing authenticated and encrypted writing of part of the Tag's memory;

— Mutual authentication.

In this document, 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 18000-3:2010, *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 930 MHz Type C*

ISO/IEC 19762, *Information technology — Automatic identification and data capture (AIDC) techniques — Vocabulary*

ISO/IEC 29167-1, *Information technology — Automatic identification and data capture techniques — Part 1: Security services for RFID air interfaces*

Bibliography

[1] ISO/IEC 9797-1, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

[2] ISO/IEC 15693-3, *Cards and security devices for personal identification — Contactless vicinity objects — Part 3: Anticollision and transmission protocol*

[3] ISO/IEC 18000 (all parts), *Information technology — Radio frequency identification for item management*

[4] ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

[5] ISO/IEC 29167 (all parts), *Information technology — Automatic identification and data capture techniques*

[6] EPC™ Radio-Frequency Identity Protocols, UHF RFID Generation-2 Version 2.0.1, Specification for RFID Air Interface Protocol for Communications at 860 MHz – 960 MHz; GS1 EPCglobal™ Inc.

[7] ERC REC 70-03, Relating to the Use of Short Range Devices (SRD), Annex 1, Band e; European Radio-communications Committee (ERC)

[8] NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication

[9] NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques

[10] NIST FIPS 197, Advanced Encryption Standard, May 9 2023.

[11] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[12] https://csrc.nist.gov/archive/aes/rijndael/rijndael-vals.zip

[13] http://testprotect.com/appendix/AEScalc