
**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*





COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms, definitions, symbols and abbreviated terms	1
4 Conformance	6
4.1 Air interface protocol specific information.....	6
4.2 Interrogator conformance and obligations.....	6
4.3 Tag conformance and obligations.....	6
5 Introduction of the AES-128 crypto suite	6
6 Parameter definitions	7
7 Crypto suite state diagram	8
8 Initialization and resetting	9
9 Authentication	9
9.1 General.....	9
9.2 Adding custom data to authentication process.....	10
9.3 Message and response formatting.....	12
9.4 Tag authentication (Method “00” = TAM).....	13
9.4.1 General.....	13
9.4.2 TAM1 Message.....	13
9.4.3 TAM1 Response.....	14
9.4.4 Final Interrogator processing TAM1.....	14
9.4.5 TAM2 Message.....	14
9.4.6 TAM2 Response.....	16
9.4.7 Final Interrogator processing TAM2.....	20
9.5 Interrogator authentication (Method “01” = IAM).....	21
9.5.1 General.....	21
9.5.2 IAM1 Message.....	21
9.5.3 IAM1 Response.....	22
9.5.4 Final Interrogator processing IAM1.....	22
9.5.5 IAM2 Message.....	22
9.5.6 IAM2 Response.....	23
9.5.7 Final Interrogator processing IAM2.....	23
9.5.8 IAM3 Message.....	23
9.5.9 IAM3 Response.....	28
9.5.10 Final Interrogator processing IAM3.....	29
9.6 Mutual authentication (Method “10” = MAM).....	29
9.6.1 General.....	29
9.6.2 MAM1 Message.....	29
9.6.3 MAM1 Response.....	30
9.6.4 Final Interrogator processing MAM1.....	30
9.6.5 MAM2 Message.....	30
9.6.6 MAM2 Response.....	31
9.6.7 Final Interrogator processing MAM2.....	31
10 Communication	31
11 Key Table and KeyUpdate	31
Annex A (normative) Crypto suite state transition table	34
Annex B (normative) Error conditions and error handling	35

Annex C (normative) Cipher description	36
Annex D (informative) Test vectors	40
Annex E (normative) Protocol specific information	41
Annex F (informative) Examples	49
Bibliography	58

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 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by 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 29167-10:2015), which has been technically revised.

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

Introduction

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 allows authenticated and encrypted reading of a part of the Tag's memory;
- Interrogator Authentication;
- Interrogator Authentication allows authenticated and encrypted writing of a part of the Tag's memory;
- Mutual Authentication.

Crypto suite only supports encryption on the Tag and uses encryption for "encrypting" messages sent from the Tag to the Interrogator and "decrypting" messages received from the Interrogator.

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 might 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 ISO and IEC that they are willing to negotiate licenses 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:

Impinj, Inc.
Chris Dorio
Chief Strategy and Technology Officer

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

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 interfaces standards for radio frequency identification (RFID) devices. Its purpose is to provide a common crypto suite for security for RFID devices that might be referred by ISO committees for air interface standards and application standards.

This document specifies a crypto suite for AES-128 for an air interface for RFID systems. The crypto suite is defined in alignment with existing air interfaces.

This document specifies various authentication methods and methods of use for the encryption algorithm. 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 9797-1, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

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, *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*