International Standard

ISO/IEC 29167-13

Second edition
2026-03

Information technology — Automatic identification and data capture techniques —

Part 13: Crypto suite Grain-128A security services for air interface communications

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

Partie 13: Services de sécurité par suite cryptographique Grain-128A pour communications par interface radio

Reference number
ISO/IEC 29167-13:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
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 ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Symbols and abbreviated terms ... **1**
4.1 Symbols ... 1
4.2 Abbreviated terms ... 2
5 Conformance ... **2**
5.1 Air interface protocol specific information ... 2
5.2 Interrogator conformance and obligations ... 2
5.3 Tag conformance and obligations ... 2
6 Overview of the Grain-128A crypto suite ... **3**
7 Parameter description ... **3**
8 Crypto suite state diagram ... **4**
9 Initialization and resetting ... **6**
10 Authentication ... **7**
10.1 General ... 7
10.2 Tag authentication ... 8
10.2.1 General ... 8
10.2.2 CryptoAuthCmd(TA.1 Payload for Tag CS) ... 8
10.2.3 CryptoAuthResp(TA.1 Payload for Interrogator CS) ... 9
10.2.4 Final interrogator processing ... 9
10.3 Interrogator authentication ... 9
10.3.1 General ... 9
10.3.2 CryptoAuthCmd(IA.1 Payload for Tag CS) ... 9
10.3.3 CryptoAuthResp(IA.1 Payload for Interrogator CS) ... 10
10.3.4 CryptoAuthCmd(IA.2 Payload for Tag CS) ... 10
10.3.5 CryptoAuthResp(IA.2 Payload for Interrogator CS) ... 10
10.4 Mutual authentication ... 11
10.4.1 General ... 11
10.4.2 CryptoAuthCmd (MA.1 Payload for Tag CS) ... 11
10.4.3 CryptoAuthResp(MA.1 Payload for Interrogator CS) ... 11
10.4.4 CryptoAuthCmd(MA.2 Payload for Tag CS) ... 11
10.4.5 CryptoAuthResp(MA.2 Payload for Interrogator CS) ... 12
10.4.6 Final interrogator processing ... 12
11 Communication ... **12**
11.1 General ... 12
11.2 Authenticated communication ... 13
11.3 Secure authenticated communication ... 14
12 Key table and key update ... **15**
Annex A (normative) **State transitions** ... **16**
Annex B (normative) **Error conditions and error handling** ... **20**
Annex C (normative) **Cipher description** ... **21**
Annex D (informative) **Test vectors** ... **24**
Annex E (normative) **Protocol specific information** ... **31**
Bibliography ... **39**

© ISO/IEC 2026 – All rights reserved

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 second edition cancels and replaces the first edition (ISO/IEC 29167-13:2015), which has been technically revised.

The main change is as follows: requirements in Annex E 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.

© ISO/IEC 2026 – All rights reserved

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 lightweight stream cipher Grain-128A.

It is important to know that all security services are optional. Every manufacturer has the liberty to choose which services will be implemented on a Tag (e.g. Tag-only authentication).

© ISO/IEC 2026 – All rights reserved

Information technology — Automatic identification and data capture techniques —

Part 13: Crypto suite Grain-128A security services for air interface communications

1 Scope

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

This document specifies various authentication methods and methods of use for the cipher.

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

3 Terms and definitions

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

4 Symbols and abbreviated terms

4.1 Symbols

$xxxx_b$	binary notation
$xxxx_h$	hexadecimal notation
||	concatenation of syntax elements in the order written

© ISO/IEC 2026 – All rights reserved