International Standard

ISO/IEC 19823-13

Information technology — Conformance test methods for security service crypto suites —

Part 13: Crypto suite Grain-128A

Technologies de l'information — Conformance test methods for security service crypto suites —

Partie 13: Suite cryptographique Grain-128A

Second edition
2026-03

Reference number
ISO/IEC 19823-13:2026(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, definitions, symbols and abbreviated terms ... **1**
3.1 Terms and definitions ... 1
3.2 Symbols and abbreviated terms ... 1

4 Test methods ... **2**
4.1 General ... 2
4.2 By demonstration ... 2
4.3 By design ... 2

5 Test requirements for ISO/IEC 18000-62 Interrogators and Tags ... **2**

6 Test methods related to the ISO/IEC 29167-13 Interrogators and Tags ... **2**
6.1 Test map for optional features ... 2
6.2 Crypto suite requirements ... 3
6.2.1 General ... 3
6.2.2 Crypto suite requirements of ISO/IEC 29167-13:2026, Clauses 5 to 8 and Annexes A to C ... 3
6.2.3 Crypto suite requirements of ISO/IEC 29167-13:2026, Clauses 9 to 12 and Annex E ... 3
6.3 Test patterns ... 12
6.3.1 General ... 12
6.3.2 Test pattern 1 ... 12
6.3.3 Test pattern 2 ... 12
6.3.4 Test pattern 3 ... 13
6.3.5 Test pattern 4 ... 13
6.3.6 Test pattern 5 ... 13
6.3.7 Test pattern 6 ... 13
6.3.8 Test pattern 7 ... 13
6.3.9 Test pattern 8 ... 14
6.3.10 Test pattern 9 ... 14
6.3.11 Test pattern 10 ... 14
6.3.12 Test pattern 11 ... 14
6.3.13 Test pattern 12 ... 15
6.3.14 Test pattern 13 ... 15
6.3.15 Test pattern 14 ... 15
6.3.16 Test pattern 15 ... 15
6.3.17 Test pattern 16 ... 16
6.3.18 Test pattern 17 ... 16
6.3.19 Test pattern 18 ... 16
6.3.20 Test pattern 19 ... 16
6.3.21 Test pattern 20 ... 17
6.3.22 Test pattern 21 ... 17
6.3.23 Test pattern 22 ... 17
6.3.24 Test pattern 23 ... 17
6.3.25 Test pattern 24 ... 18
6.3.26 Test pattern 25 ... 18

Bibliography ... **19**

© 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 not 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 19823-13:2018), which has been technically revised.

The main change is as follows: test items have been updated to reflect changes to the over-the-air protocol.

A list of all parts in the ISO/IEC 19823 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

The ISO/IEC 29167 series describes security services that are applicable for the ISO/IEC 18000 series. The various parts of the ISO/IEC 29167 series describe crypto suites that are optional extensions to the ISO/IEC 18000 air interfaces.

The ISO/IEC 19823 series describes conformance test methods for security service crypto suites. The ISO/IEC 19823 series is related to the ISO/IEC 18047 series, which describes the radio frequency identification device conformance test methods, in the same way as the ISO/IEC 29167 series is related to the ISO/IEC 18000 series. These relations mean that, for a product that is claimed to conform to a pair ISO/IEC 18000-n and ISO/IEC 29167-m, the test methods of ISO/IEC 18047-n and ISO/IEC 19823-m apply. If a product supports more than one part of the ISO/IEC 18000 series or the ISO/IEC 29167 series, all related parts of the ISO/IEC 18047 series and the ISO/IEC 19823 series apply.

The conformance parameters are:

— parameters that apply directly affecting system functionality and inter-operability;

— protocol including commands and replies;

— nominal values and tolerances.

NOTE 1 ISO/IEC 18047-6 provides the conformance test requirements of ISO/IEC 18000-6, ISO/IEC 18000-61, ISO/IEC 18000-62, ISO/IEC 18000-63 and ISO/IEC 18000-64.

NOTE 2 Test methods for interrogator and tag performance are covered by the multiple parts of the ISO/IEC 18046 series.

© ISO/IEC 2026 – All rights reserved

Information technology — Conformance test methods for security service crypto suites —

Part 13: Crypto suite Grain-128A

1 Scope

This document describes the test methods for determining conformance for the security crypto suite Grain-128A defined in ISO/IEC 29167-13.

This document contains conformance tests for all mandatory and optional functions.

Unless otherwise specified, the tests in this document are only applicable to radio frequency identification (RFID) tags and interrogators defined in the ISO/IEC 18000 series using ISO/IEC 29167-13.

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 17025, *General requirements for the competence of testing and calibration laboratories*

ISO/IEC 18000-62, *Information technology — Radio frequency identification for item management — Part 62: Parameters for air interface communications at 860 MHz to 960 MHz Type B*

ISO/IEC 18047-6:2025, *Information technology — Radio frequency identification device conformance test methods — Part 6: Test methods for air interface communications at 860 MHz to 960 MHz*

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

ISO/IEC 29167-13:2026, *Information technology — Automatic identification and data capture techniques — Part 13: Crypto suite Grain-128A security services for air interface communications*

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 ISO/IEC 29167-13 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/

3.2 Symbols and abbreviated terms

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

© ISO/IEC 2026 – All rights reserved