



Nederlandse norm

NEN-ISO/IEC 19823-13

(en)

Information technology - Conformance test methods for security service crypto suites - Part 13: Cryptographic Suite Grain-128A (ISO/IEC 19823-13:2018, IDT)

ICS 35.030
mei 2018

Als Nederlandse norm is aanvaard:

- ISO/IEC 19823-13:2018, IDT

Normcommissie 381043 'Automatische identificatie'



THIS PUBLICATION IS COPYRIGHT/PROTECTED

DEZE PUBLICATIE IS AUTEURSRECHTELIJK BESCHERMD

Apart from exceptions provided by the law, nothing from this publication may be duplicated and/or published by means of photocopy, microfilm, storage in computer files or otherwise, which also applies to full or partial processing, without the written consent of the Royal Netherlands Standardization Institute.

The Royal Netherlands Standardization Institute shall, with the exclusion of any other beneficiary, collect payments owed by third parties for duplication and/or act in and out of law, where this authority is not transferred or falls by right to the Reproduction Rights Foundation.

Auteursrecht voorbehouden. Behoudens uitzondering door de wet gesteld mag zonder schriftelijke toestemming van het Koninklijk Nederlands Normalisatie-instituut niets uit deze uitgave worden verveelvoudigd en/of openbaar gemaakt door middel van fotokopie, microfilm, opslag in computerbestanden of anderszins, hetgeen ook van toepassing is op gehele of gedeeltelijke bewerking.

Het Koninklijk Nederlands Normalisatie-instituut is met uitsluiting van ieder ander gerechtigd de door derden verschuldigde vergoedingen voor verveelvoudiging te innen en/of daartoe in en buiten rechte op te treden, voor zover deze bevoegdheid niet is overgedragen c.q. rechtens toekomt aan de Stichting Reprorecht.

Although the utmost care has been taken with this publication, errors and omissions cannot be entirely excluded. The Royal Netherlands Standardization Institute and/or the members of the committees therefore accept no liability, not even for direct or indirect damage, occurring due to or in relation with the application of publications issued by the Royal Netherlands Standardization Institute.

Hoewel bij deze uitgave de uiterste zorg is nagestreefd, kunnen fouten en onvolledigheden niet geheel worden uitgesloten. Het Koninklijk Nederlands Normalisatie-instituut en/of de leden van de commissies aanvaarden derhalve geen enkele aansprakelijkheid, ook niet voor directe of indirecte schade, ontstaan door of verband houdend met toepassing van door het Koninklijk Nederlands Normalisatie-instituut gepubliceerde uitgaven.

Preview

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

**Part 13:
Cryptographic Suite Grain-128A**

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

Partie 13: Suite cryptographique Grain-128A



Copyright
Preview



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

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
Fax: +41 22 749 09 47
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
4 Test methods	2
4.1 General.....	2
4.2 By demonstration.....	2
4.3 By design.....	2
5 Test methods in respect to the ISO/IEC 18000 parts	2
5.1 Test requirements for ISO/IEC 18000-62 interrogators and tags.....	2
6 Test methods in respect to the ISO/IEC 29167-13 interrogators and tags	3
6.1 Test map for optional features.....	3
6.2 Crypto suite requirements.....	3
6.3 Test patterns.....	14
Bibliography	21

Copyright
 Preview

ISO/IEC 19823-13:2018(E)**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 Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

A list of all parts in the ISO/IEC 19823 series can be found on the ISO website.

Introduction

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

The ISO/IEC 19823 series of standards describes the conformance test methods for security service crypto suites. The ISO/IEC 19823 series is related to the ISO/IEC 18047 series of standards, which describes the radio frequency identification device conformance test methods, in the same way as ISO/IEC 29167 series is related to the ISO/IEC 18000 series.

These relations mean that for a product that is claimed to be compliant to a pair of ISO/IEC 18000-n and ISO/IEC 29167-m then the test methods of ISO/IEC 18047-n and ISO/IEC 19823-m apply. If a product supports more than one part of ISO/IEC 18000 or ISO/IEC 29167, all related parts of ISO/IEC 18047 and ISO/IEC 19823 apply.

NOTE 1 The conformance test requirements of ISO/IEC 18000-6, ISO/IEC 18000-61, ISO/IEC 18000-62, ISO/IEC 18000-63, ISO/IEC 18000-64 are currently all in ISO/IEC 18047-6.

This document describes the test methods for the Grain-128A crypto suite as standardized in ISO/IEC 29167-13.

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

Voorbeld
Preview

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

Part 13: Cryptographic Suite Grain-128A

1 Scope

This document describes test methods for determining the conformance of security crypto suites with the specifications given in ISO/IEC 29167-13.

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

The conformance parameters are the following:

- parameters that apply directly affecting system functionality and inter-operability;
- protocol including commands and replies; and
- nominal values and tolerances

Unless otherwise specified, the tests in this document are applied exclusively to 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 19762 (all parts), *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

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 18047-6:2017, *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 29167-13:2015, *Information technology — Automatic identification and data capture techniques — Part 13: Crypto suite Grain-128A security services for air interface communications*

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

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 (all parts) and ISO/IEC 29167-13 apply.

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

- IEC Electropedia: available at <https://www.electropedia.org/>

ALTIJD DE ACTUELE NORM IN UW BEZIT HEBBEN?

Nooit meer zoeken in de systemen en uzelf de vraag stellen:
“Is NEN-ISO/IEC 19823-13:2018 en de laatste versie?”™

Via het digitale platform NEN Connect heeft u altijd toegang tot de meest actuele versie van deze norm. Vervallen versies blijven ook beschikbaar. **U en uw collega's** kunnen de norm via NEN Connect makkelijk raadplagen, online en offline.

Kies voor slimmer werken en bekijk onze mogelijkheden op www.nenconnect.nl.

Heeft u vragen?

Onze Klantenservice is bereikbaar maandag tot en met vrijdag, van 8.30 tot 17.00 uur.

Telefoon: 015 2 690 391

E-mail: klantenservice@nen.nl

