



DPC: 16 / 30322561 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 08 September 2016

Origin: International

Latest date for receipt of comments: 29 October 2016

Project No. 2015/00721

Responsible committee: IST/34 Automatic identification and data capture techniques

Interested committees:

Title: Draft BS ISO/IEC 19823-10 Information technology - Conformance test methods for security service crypto suites

Part 10: Crypto suite AES-128

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 29 October 2016**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: **Ms Sophie Erskine (BSI)**
Direct tel: **7254**
E-mail: sophie.erskine@bsigroup.com

Introduction

This draft standard is based on international discussions in which the UK has taken an active part. Your comments on this draft are welcome and will assist in the preparation of the consequent standard. There is a high probability that this text could be adopted by CENELEC as a reference document for harmonization or as a European Standard. Recipients of this draft are requested to comment on the text bearing in mind this possibility.

UK Vote

Please indicate whether you consider the UK should submit a negative (with reasons) or positive vote on this draft.

BSI Committee Responsibilities

Whether or not the standard is published in its original (international) form, or as a formal British Standard Implementation the BSI committee's responsibilities are to:

- aid enquirers to understand the text;
- present to the responsible international committee any enquiries on interpretation, or proposals for change, and keep UK interests informed;
- monitor related International and European developments and promulgate them in the UK.

Submission of Comments

- The guidance given below is intended to ensure that all comments receive efficient and appropriate attention by the responsible BSI committee. **Annotated drafts are not acceptable and will be rejected.**
- All comments must be submitted, preferably electronically, to the Responsible Committee Secretary at the address given on the front cover. Comments should be compatible with version 6.0 or version 97 of Microsoft Word for Windows, if possible; otherwise comments in ASCII text format are acceptable. **Any comments not submitted electronically should still adhere to these format requirements.**
- All comments submitted should be presented as given in the example below. Further information on submitting comments and how to obtain a blank electronic version of a comment form are available from the BSI website at:
<http://drafts.bsigroup.com/>

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	(7)
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/ Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 19823-10

ISO/IEC JTC 1/SC 31

Secretariat: ANSI

Voting begins on:
2016-09-07

Voting terminates on:
2016-11-29

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

Part 10: Crypto suite AES-128

Technologies de l'information — [Conformance test methods for security service crypto suites] — Partie 10: [Crypto suite AES-128]

ICS: 35.040

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.



Reference number
ISO/IEC DIS 19823-10:2016(E)
Documents
AVA Document Sharing Hub
© ISO/IEC 2016



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, 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	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms, definitions, symbols and abbreviated terms	2
3.1 Terms and definitions.....	2
3.2 Symbols.....	2
3.3 Abbreviated terms.....	2
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	3
5.1 Test requirements for ISO/IEC 18000-3 interrogators and tags.....	3
5.2 Test requirements for ISO/IEC 18000-63 interrogators and tags.....	3
6 Test methods in respect to the ISO/IEC 29167-10 interrogators and tags	3
6.1 Test map for optional features.....	3
6.2 Additional parameters required as input for the test.....	4
6.3 Crypto suite requirements.....	4
6.3.1 Crypto suite requirements of ISO/IEC 29167-10 in clauses 1 - 6	4
6.3.2 Crypto suite requirements of ISO/IEC 29167-10 in clauses 7 - 12.....	4
6.3.3 Crypto suite requirements of ISO/IEC 29167-10 in Annex A.....	15
6.3.4 Crypto suite requirements of ISO/IEC 29167-10 in Annex E.....	16
6.4 Test patterns.....	18
6.4.1 Test patterns for ISO/IEC 18000-3 mode 1.....	18
6.4.2 Test patterns for ISO/IEC 18000-3 mode 3.....	19
6.4.3 Test patterns for ISO/IEC 18000-63.....	19
Bibliography	22

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 19823-10 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

This second/third/... edition cancels and replaces the first/second/... edition (), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised.

ISO/IEC 19823 consists of the following parts, under the general title *Information technology — Conformance test methods for security service crypto suites*:

- *Part 1: General requirements*
- *Part 10: Crypto suite AES-128 security services for air interface communications*
- *Part 11: Crypto suite PRESENT-80 security services for air interface communications*
- *Part 12: Crypto suite ECC-DH security services for air interface communications*
- *Part 13: Crypto suite Grain-128A security services for air interface communications*
- *Part 17: Crypto suite cryptoGPS security services for air interface communications*

Introduction

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

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

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 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 part of ISO/IEC 19823 describes the test methods for the AES-128 crypto suite as standardized in ISO/IEC 29167-10

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

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

Part 10: Crypto suite AES-128

1 Scope

This part of ISO/IEC 19823 describes test methods for determining the conformance of security crypto suites defined in ISO/IEC 29167-10.

This part of ISO/IEC 19823 contains conformance tests for all mandatory and applicable optional functions.

The conformance parameters are the following:

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

Unless otherwise specified, the tests in this part of ISO/IEC 19823 are to be applied exclusively related to RFID tags and interrogators defined in the ISO/IEC 18000- series using ISO/IEC 29167-10.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendment s) applies.

ISO/IEC 19762 (all parts), *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

ISO/IEC 18000-3, *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 960 MHz Type C*

ISO/IEC 18047-3, *Information technology — Radio frequency identification device conformance test methods — Part 3: Test methods for air interface communications at 13,56 MHz*

ISO/IEC 18047-6, *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 29167-10, *Information technology — Automatic identification and data capture techniques — Part 10: Crypto suite AES-128 security services for air interface communications*