BS ISO/IEC 19823-22:2019

BSI Standards Publication

Information technology — Conformance test methods for security service crypto suites

Part 22: Crypto suite SPECK

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 19823-22:2019

National foreword

This British Standard is the UK implementation of ISO/IEC 19823-22:2019.

The UK participation in its preparation was entrusted to Technical Committee IST/34, Automatic identification and data capture techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2019
Published by BSI Standards Limited 2019

ISBN 978 0 580 99262 9

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 May 2019.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 19823-22:2019

INTERNATIONAL STANDARD

ISO/IEC 19823-22

First edition
2019-05

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

Part 22: Crypto suite SPECK

Technologies de l'information — Méthodes d'essai de conformité pour les suites cryptographiques des services de sécurité —

Partie 22: Suite cryptographique SPECK

Reference number
ISO/IEC 19823-22:2019(E)

Documents
Document Sharing Hub
© ISO/IEC 2019

Full document details: BS ISO/IEC 19823-22:2019

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2019

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

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 19823-22:2019

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 requirements for ISO/IEC 18000-63 interrogators and tags ... **2**
6 Test methods with respect to ISO/IEC 29167-22 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 29167-22:2018, Clauses 1 to 8 and Annexes A to C ... 3
6.2.3 Crypto suite requirements of ISO/IEC 29167-22:2018, Clauses 9 to 12 and Annex E ... 3
6.3 Test patterns ... 13
6.3.1 General ... 13
6.3.2 Test_Pattern 1 ... 14
6.3.3 Test_Pattern 2 ... 14
6.3.4 Test_Pattern 3 ... 15
6.3.5 Test_Pattern 4 ... 15
6.3.6 Test_Pattern 5 ... 16
6.3.7 Test_Pattern 6 ... 16
6.3.8 Test_Pattern 7 ... 17
6.3.9 Test_Pattern 8 ... 17
6.3.10 Test_Pattern 9 ... 18
6.3.11 Test_Pattern 10 ... 18
6.3.12 Test_Pattern 11 ... 19
Bibliography ... **20**

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19823-22:2019

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).

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) or the IEC list of patent declarations received (see http://patents.iec.ch).

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.

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.

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.

© ISO/IEC 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19823-22:2019

Introduction

The ISO/IEC 29167 series describes security services as applicable for the ISO/IEC 18000 series. 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 describes the conformance test methods for security service crypto suites. It 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, 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 SPECK crypto suite as standardized in ISO/IEC 29167-22.

NOTE 2 Test methods for interrogator and tag performance are covered by ISO/IEC 18046 (all parts).

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19823-22:2019

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 19823-22:2019

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

Part 22:
Crypto suite SPECK

1 Scope

This document describes methods for determining conformance to the security crypto suite defined in ISO/IEC 29167-22.

This document contains conformance tests for all mandatory 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 document are intended to be applied exclusively to RFID tags and interrogators defined in the ISO/IEC 18000- series using ISO/IEC 29167-22.

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 18000-63, *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 18047-6:2017, *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 19762, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

ISO/IEC 29167-22:2018, *Information technology — Automatic identification and data capture techniques — Part 22: Crypto suite SPECK security services for air interface communications*

3 Terms, definitions, symbols and abbreviated terms

For the purposes of this document, the terms, definitions, symbols and abbreviated terms given in ISO/IEC 19762 and ISO/IEC 29167-22 apply.

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

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19823-22:2019