FINAL DRAFT International Standard

ISO/IEC FDIS 19823-11

ISO/IEC JTC **1**/SC **31**

Secretariat: **ANSI**

Voting begins on:
2025-06-27

Voting terminates on:
2025-08-22

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

Part 11: Crypto suite PRESENT-80

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

Partie 11: Suite cryptographique PRESENT-80

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/IEC FDIS 19823-11
https://standards.iteh.ai/catalog/standards/iso/1bf03747-7732-4792-8b4a-f648f6c33c95/iso-iec-fdis-19823-11

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.

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.

Reference number
ISO/IEC FDIS 19823-11:2025(en)

© ISO/IEC 2025

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/IEC FDIS 19823-11
https://standards.iteh.ai/catalog/standards/iso/1bf03747-7732-4792-8b4a-f648f6c33c95/iso-iec-fdis-19823-11

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

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 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 29167-11 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 29167-11, Clauses 1 to 8 and Annexes A – C ... 3
6.2.3 Crypto suite requirements of ISO/IEC 29167-11, Clauses 9 to 11 and Annex E ... 3
6.3 Test patterns ... 7
6.3.1 General ... 7
6.3.2 Test Pattern 1 ... 8
6.3.3 Test Pattern 2 ... 8
6.3.4 Test Pattern 3 ... 8
6.3.5 Test pattern 4 ... 9
Bibliography ... **10**

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/IEC FDIS 19823-11
https://standards.iteh.ai/catalog/standards/iso/1bf03747-7732-4792-8b4a-f648f6c33c95/iso-iec-fdis-19823-11

© ISO/IEC 2025 – All rights reserved