



International
Standard

ISO/IEC 29167-11

**Information technology —
Automatic identification and data
capture techniques —**

**Part 11:
Crypto suite PRESENT-80
security services for air interface
communications**

*Technologies de l'information — Identification et capture
automatique de données —*

*Partie 11: Services de sécurité par suite cryptographique
PRESENT-80 pour communications par interface radio*

**Third edition
2025-09**

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

ISO/IEC 29167-11:2025

<https://standards.iteh.ai/catalog/standards/iso/44c4eec1-7973-4910-bc0f-67570be4c423/iso-iec-29167-11-2025>



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	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	2
3.3 Abbreviated terms	3
4 Conformance	3
4.1 Air interface protocol specific information	3
4.2 Interrogator conformance and requirements	3
4.3 Tag conformance and requirements	3
5 Introduction of the PRESENT-80 cryptographic suite	4
6 Parameter and variable definitions	4
7 Crypto suite state diagram	4
8 Initialization and resetting	5
9 Authentication	5
9.1 Introduction	5
9.2 Message and response formatting	5
9.3 Tag authentication: AuthMethod “00”	6
9.3.1 General	6
9.3.2 TAM1 message	6
9.3.3 Intermediate Tag processing	7
9.3.4 TAM1 response	8
9.3.5 Final Interrogator processing	8
9.4 Interrogator authentication: AuthMethod “01”	8
9.4.1 General	8
9.4.2 IAM1 message	9
9.4.3 Intermediate Tag processing #1	9
9.4.4 IAM1 response	9
9.4.5 Intermediate Interrogator processing	10
9.4.6 IAM2 message	10
9.4.7 Intermediate Tag processing #2	10
9.4.8 IAM2 response	11
9.4.9 Final Interrogator processing	11
9.5 Mutual authentication: AuthMethod “10”	11
9.5.1 General	11
9.5.2 MAM1 message	11
9.5.3 Intermediate Tag processing #1	12
9.5.4 MAM1 response	12
9.5.5 Intermediate Interrogator processing	12
9.5.6 MAM2 message	13
9.5.7 Intermediate Tag processing #2	13
9.5.8 MAM2 response	13
9.5.9 Final Interrogator processing	14
10 Communication	14
11 Key table and Key update	14
Annex A (normative) Crypto suite state transition table	15
Annex B (normative) Errors and error handling	16
Annex C (informative) Description of PRESENT	17

Annex D (informative) Test vectors	22
Annex E (normative) Protocol specific information	24
Bibliography	27

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

[ISO/IEC 29167-11:2025](https://standards.iteh.ai/catalog/standards/iso/44c4eec1-7973-4910-bc0f-67570be4c423/iso-iec-29167-11-2025)

<https://standards.iteh.ai/catalog/standards/iso/44c4eec1-7973-4910-bc0f-67570be4c423/iso-iec-29167-11-2025>

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 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 third edition cancels and replaces the second edition (ISO/IEC 29167-11:2023), which has been technically revised.

The main change is as follows: [Annex E](#) has been updated to reflect changes to the over-the-air protocol.

A list of all parts in the ISO/IEC 29167 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.