



**International
Standard**

ISO/IEC 29167-21

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

Part 21:

**Crypto suite SIMON security
services for air interface
communications**

*Technologies de l'information — Techniques automatiques
d'identification et de capture de données —*

*Partie 21: Services de sécurité par suite cryptographique SIMON
pour communications par interface radio*

**Second edition
2026-03**

This document is a preview generated by AI



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

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
Introduction	vi
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 obligations	3
4.3 Tag conformance and obligations	4
5 Overview of the SIMON crypto suite	4
6 Parameter and variable descriptions	4
7 Crypto suite state diagram	5
8 Initialization and resetting	6
9 Authentication	6
9.1 General	6
9.2 Message and response formatting	7
9.3 Tag authentication (AuthMethod “00”)	7
9.3.1 General	7
9.3.2 TAM1 message	7
9.3.3 Intermediate Tag processing	8
9.3.4 TAM1 response	8
9.3.5 Final Interrogator processing	8
9.4 Interrogator authentication (AuthMethod “01”)	9
9.4.1 General	9
9.4.2 IAM1 message	9
9.4.3 Intermediate Tag processing #1	10
9.4.4 IAM1 response	10
9.4.5 Intermediate Interrogator processing	10
9.4.6 IAM2 message	10
9.4.7 Intermediate Tag processing #2	11
9.4.8 IAM2 response	11
9.4.9 Final Interrogator processing	11
9.5 Mutual authentication (AuthMethod “10”)	12
9.5.1 General	12
9.5.2 MAM1 message	12
9.5.3 Intermediate Tag processing #1	13
9.5.4 MAM1 response	13
9.5.5 Intermediate Interrogator processing	14
9.5.6 MAM2 message	14
9.5.7 Intermediate Tag processing #2	14
9.5.8 MAM2 response	15
9.5.9 Final Interrogator processing	15
10 Communication	16
10.1 General	16
10.2 Message and response formatting	16
10.3 Transforming a payload prior to encapsulation	17
10.3.1 General	17
10.3.2 Encapsulating an Interrogator command	18

10.3.3	Cryptographically protecting a Tag reply.....	19
10.4	Processing an encapsulated or cryptographically-protected reply	20
10.4.1	General	20
10.4.2	Recovering an encapsulated Interrogator command.....	21
10.4.3	Recovering a cryptographically-protected Tag response.....	22
11	Key table and key update.....	22
Annex A	(normative) Crypto suite state transitions	23
Annex B	(normative) Errors and error handling.....	24
Annex C	(normative) Description of SIMON and SILC v3	25
Annex D	(informative) Test vectors	29
Annex E	(normative) Protocol specific information.....	40
Bibliography		43

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 second edition cancels and replaces the first edition (ISO/IEC 29167-21:2018), 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.

Introduction

This document provides a common crypto suite for security for radio frequency identification (RFID) devices. The crypto suite is defined in alignment with existing air interfaces and specifies a variety of security services provided by the lightweight block cipher SIMON.

This document is a preview generated by EVS

Information technology — Automatic identification and data capture techniques —

Part 21:

Crypto suite SIMON security services for air interface communications

1 Scope

This document specifies the crypto suite for SIMON for the ISO/IEC 18000 air interface standards for radio frequency identification (RFID) devices.

SIMON is a symmetric block cipher that is parameterized in both its block length and key length. The block/key length options supported in this crypto suite (in bits) are 64/96, 96/96, 64/128, 128/128 and 128/256.

In this document, a Tag and an Interrogator can support one, a subset or all of the specified options, clearly stating what is supported.

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 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 19762, *Information technology — Automatic identification and data capture (AIDC) techniques — Vocabulary*

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 and the following apply.

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

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1.1

bit string

ordered sequence of 0s and 1s

3.1.2

block cipher

family of permutations that is parameterized by a *cryptographic key* (3.1.4) and, optionally, the *block size* (3.1.3)