Deleted: PRF

# Information technology — Conformance test methods for security service crypto suites — Part 21: Crypto suite SIMON

*Technologies de l'information — Méthodes d'essai de conformité pour les suites cryptographiques des services de sécurité— Partie 21: Suite cryptographique SIMON*

Deleted: PRF

## 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.

Deleted: PRF

## 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 the ISO/IEC 18047 series, 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 SIMON crypto suite as standardized in ISO/IEC 29167-21.

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

Deleted: PRF

# Information technology — Conformance test methods for security service crypto suites — Part 21: Crypto suite SIMON

## 1 Scope

This document describes methods for determining conformance to the security crypto suite defined in ISO/IEC 29167-21.

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 29167-21.



## 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 29167-21:2018, *Information technology — Automatic identification and data capture techniques — Part 21: Crypto suite SIMON 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 in ISO/IEC 29167-21 apply.

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

Deleted: PRF

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

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

# 4 Test methods

## 4.1 General

This document describes test methods for ISO/IEC 29167-21. As parts of ISO/IEC 19823 are always tested in relation to ISO/IEC 18047, duplication of information requirements and specifications is meant to be avoided.

Clause 5 defines elements that are covered in the respective part of ISO/IEC 18047.

Clause 6 defines elements that are not covered by ISO/IEC 18047 and are therefore addressed in this document.

## 4.2 By demonstration

If tests are labelled "**by demonstration**" then laboratory testing of one or (if required for statistical reasons) multiple products, processes or services is required to ensure conformance. A test laboratory that meets the requirements of ISO/IEC 17025 shall perform the indicated testing to ensure conformance of the component or system.

For protocol requirements that are verified **by demonstration**, the test conditions are specified in this document. The detailed test plan is left to the discretion of the test laboratory.

## 4.3 By design

If tests are labelled "**by design**" then verification of design parameters and/or theoretical analysis is used to ensure conformance. A vendor submitting a component or system for conformance testing shall provide the necessary technical information, in the form of a technical memorandum or similar. A test laboratory shall issue a test report indicating whether the technical analysis was sufficient to ensure conformance of the component or system.

For protocol requirements that are verified **by design**, the method of technical analysis is at the discretion of the submitting vendor and is not specified by this document. In general, the technical analysis shall have sufficient rigor and technical depth to convince a test engineer knowledgeable of the protocol that the particular requirement has been met.

# 5 Test requirements for ISO/IEC 18000-63 interrogators and tags

The mandatory requirements and applicable optional requirements of ISO/IEC 18047-6:2017, Clauses 4 and 5 shall be fulfilled.

Before a DUT is tested according to this document, it shall successfully pass ISO/IEC 18047-6:2017, Clause 7.

# 6 Test methods with respect to ISO/IEC 29167-21 interrogators and tags

## 6.1 Test map for optional features

Table 1 lists all optional features of this crypto suite and shall be used as a template to report the test results. Furthermore, it is used to refer to the test requirements in 6.2.

Deleted: PRF

**Table 1 — Test map for optional features**

| # | Feature | Additional requirement | To be tested for supplied product? | Test results |
|---|---|---|---|---|
| 1 | TA | Shall be tested with the Authenticate command of ISO/IEC 18000-63 | | |
| 2 | IA | Shall be tested with the Authenticate command of ISO/IEC 18000-63 | | |
| 3 | MA | Shall be tested with the Authenticate command of ISO/IEC 18000-63 | | |
| 4 | Secure Communication | Shall be tested with the SecureComm command of ISO/IEC 18000-63 | | |

## 6.2 Crypto suite requirements

### 6.2.1 General

This clause refers to the requirements of ISO/IEC 29167-21.

### 6.2.2 Crypto suite requirements of ISO/IEC 29167-21:2018, Clauses 1 to 8 and Annexes A to C

All the requirements of ISO/IEC 29167-21:2018, Clauses 1 to 8 and Annexes A to C shall be met and conformance shall be verified by design only.

### 6.2.3 Crypto suite requirements of ISO/IEC 29167-21:2018, Clauses 9 to 12 and Annex E

The requirements of ISO/IEC 29167-21:2018, Clauses 9 to 12 and Annex E listed in Table 2 shall be met. This document shall be read in conjunction with ISO/IEC 29167-21 to provide a full explanation of the terms used.



**Table 2 — Crypto suite requirements for ISO/IEC 29167-21**

| Item | Protocol subclause[a] | Requirement[a] | MO [b] | Applies to | How verified |
|---|---|---|---|---|---|
| 1 | 9.3.2 | The Interrogator shall generate a random Interrogator challenge (IChallenge-*b*/*k*) that is carried in the TAM1 message. | M | Interrogator | By design |
| 2 | 9.3.3 | The Tag shall accept the TAM1 message at any time (unless occupied by internal processing and not capable of receiving messages), i.e. upon receipt of the message with valid parameters, the Tag shall abort any cryptographic protocol that has not yet been completed and shall remain in the **Initial** state. | M | Tag | By design |
| 3 | 9.3.3 | The Tag shall check if the Step is "$00_2$". If the value of Step is different, the Tag shall return a "Not Supported" error. | M | Tag | Test_Pattern 2 |
| 4 | 9.3.3 | The Tag shall check if the RFU is "$00_2$". If the value of RFU is different, the Tag shall return a "Not Supported" error. | M | Tag | Test_Pattern 2 |
| 5 | 9.3.3 | The Tag shall check whether the values of BlockSize and KeySize are supported by the Tag. | M | Tag | By design |

Deleted: PRF

| | | | | | |
|---|---|---|---|---|---|
| | | If at least one of these checks is failed, the Tag shall return a "Not Supported" error. | | | |
| 6 | 9.3.3 | The Tag shall check whether the values of BlockSize and KeySize are supported by Key.KeyID and that Key.KeyID is authorized for use in Tag authentication. If either or both of these checks is failed, the Tag shall return a "Not Supported" error. | M | Tag | By design |
| 7 | 9.3.3 | The Tag shall check whether the parameter set PS is supported. If the parameter set PS is not supported, the Tag shall return a "Not Supported" error. | M | Tag | Test_Pattern 2 |
| 8 | 9.3.3 | Assuming that the TAM1 message is successfully parsed by the Tag, the Tag shall prepare the TAM1 response. | M | Tag | By design |
| 9 | 9.3.4 | The Tag shall generate a random salt TRnd-$b/k$ of length $r$ bits were $r$ is given for the parameter set in Table 4. | M | Tag | By design |
| 10 | 9.3.4 | The Tag shall use Key.KeyID and SIMON encryption to form a $b$-bit string TResponse such that<br>TResponse = SIMON-b/k-ENC ( Key.KeyID, C_TAM-$b/k$ \|\| TRnd-$b/k$ \|\| IChallenge-$b/k$ ) | M | Tag | Test_Pattern 1 |
| 11 | 9.3.4 | The Tag shall return TResponse to the Interrogator. | M | Tag | By design |
| 12 | 9.3.5 | After receiving TAM1 response, the Interrogator shall use Key.KeyID to compute the $b$-bit string S where:<br>S = SIMON-$b/k$-DEC ( Key.KeyID, TResponse ).<br>The Interrogator shall check that S[$t$-1:0] = IChallenge-$b/k$. | M | Interrogator | By design |
| 13 | 9.4.2 | The Interrogator shall send an initial message IAM1 to the Tag prompting the Tag to start a challenge-response exchange.<br>The Interrogator shall also indicate the variant of SIMON to be used. | O | Interrogator | By design |
| 14 | 9.4.3 | The Tag shall accept this message at any time (unless occupied by internal processing and not capable of receiving messages), i.e. upon receipt of the message with valid parameters, the Tag shall abort any cryptographic protocol that has not yet been completed and shall remain in the **Initial** state. | O | Tag | By design |
| 15 | 9.4.3 | If Interrogator authentication is not supported on the Tag, i.e. if "$01_2$" is not a valid value for AuthMethod, then the Tag shall return a "Not Supported" error condition. | O | Tag | By design |
| 16 | 9.4.3 | The Tag shall check if the Step is "$00_2$". If the value of Step is different, the Tag shall return a "Not Supported" error. | O | Tag | Test_Pattern 3 |

Deleted: PRF

| | | | | | |
|---|---|---|---|---|---|
| 17 | 9.4.3 | The Tag shall check if the RFU is "$00_2$". If the value of RFU is different, the Tag shall return a "Not Supported" error. | O | Tag | Test_Pattern 3 |
| 18 | 9.4.3 | The Tag shall check whether the values of BlockSize and KeySize are supported by the Tag. If at least one of these checks is failed, the Tag shall return a "Not Supported" error. | O | Tag | By design |
| 19 | 9.4.3 | The Tag shall check whether the values of BlockSize and KeySize are supported by Key.KeyID and that Key.KeyID is authorized for use in Interrogator authentication. If at least one of these checks is failed, the Tag shall return a "Not Supported" error. | O | Tag | By design |
| 20 | 9.4.3 | The Tag shall check whether the value of parameter set PS is supported by the Tag. If not, the Tag shall return a "Not Supported" error. | O | Tag | Test_Pattern 3 |
| 21 | 9.4.3 | If the IAM1 message is successfully parsed by the Tag, the Tag shall calculate the IAM1 response. | O | Tag | By design |
| 22 | 9.4.4 | The Tag shall generate a random challenge TChallenge-$b/k$ of length $t$ bits, where $t$ is determined by the parameter set, and shall send this to the Interrogator. | O | Tag | By design |
| 23 | 9.4.5 | The Interrogator shall construct the IAM2 message. | O | Interrogator | By design |
| 24 | 9.4.6 | The Interrogator shall form a $b$-bit string IResponse such that<br>IResponse = SIMON-$b/k$-DEC ( Key.KeyID, C_IAM-$b/k$ \|\| IRnd-$b/k$ \|\| TChallenge-$b/k$ ).<br>The Interrogator shall send IResponse to the Tag as part of the IAM2 message; see Table 10. | O | Interrogator | Test_Pattern 4 |
| 25 | 9.4.7 | The Tag shall only accept the IAM2 message when the cryptographic engine is in state **PA1**. | O | Tag | By design |
| 26 | 9.4.7 | If Interrogator authentication is not supported on the Tag, i.e. if "$01_2$" is not a valid value for AuthMethod, then the Tag shall return a "Not Supported" error condition. | O | Tag | By design |
| 27 | 9.4.7 | The Tag shall check if the Step is "$01_2$". If the value of Step is different, the Tag shall return a "Not Supported" error. | O | Tag | Test_Pattern 5 |
| 28 | 9.4.7 | The Tag shall check if the RFU is "$0000_2$". If the value of RFU is different, the Tag shall return a "Not Supported" error. | O | Tag | Test_Pattern 5 |
| 29 | 9.4.7 | The Tag shall use Key.KeyID to compute the $b$-bit string S where<br>S = SIMON-$b/k$-ENC ( Key.KeyID, IResponse ). | O | Tag | By design |
| 30 | 9.4.7 | The Tag shall check that S[$t$-1:0] = TChallenge-$b/k$. | O | Tag | By design |
| 31 | 9.4.7 | The Tag shall prepare IAM2 response. | O | Tag | By design |

Deleted: PRF

| | | | | | |
|---|---|---|---|---|---|
| 32 | 9.4.8 | The Tag shall return the value of TStatus to the Interrogator. | O | Tag | Test_Pattern 6 |
| 33 | 9.4.9 | If, under conditions laid out in the over-the-air protocol, there is no response from the Tag or if the returned value of TStatus is $0_2$, then the Interrogator shall abandon the cryptographic protocol. | O | Interrogator | By design |
| 34 | 9.5.2 | The Interrogator shall generate a random Interrogator challenge (IChallenge-*b*/*k*) that is carried in the MAM1 message. | O | Interrogator | By design |
| 35 | 9.5.2 | The Interrogator shall indicate the variant of SIMON to be used. | O | Interrogator | By design |
| 36 | 9.5.3 | The Tag shall accept MAM1 message at any time (unless occupied by internal processing and not capable of receiving messages), i.e. upon receipt of the message with valid parameters, the Tag shall abort any cryptographic protocol that has not yet been completed and shall remain in the **Initial** state. | O | Tag | By design |
| 37 | 9.5.3 | If Mutual authentication is not supported on the Tag, i.e. if "$10_2$" is not a valid value for AuthMethod, then the Tag shall return a "Not Supported" error condition. | O | Tag | By design |
| 38 | 9.5.3 | The Tag shall check if the Step is "$00_2$". If the value of Step is different, the Tag shall return a "Not Supported" error. | O | Tag | Test_Pattern 7 |
| 39 | 9.5.3 | The Tag shall check if the RFU is "$00_2$". If the value of RFU is different, the Tag shall return a "Not Supported" error. | O | Tag | Test_Pattern 7 |
| 40 | 9.5.3 | The Tag shall check whether the values of BlockSize and KeySize are supported by the Tag. If at least one of these checks is failed, the Tag shall return a "Not Supported" error. | O | Tag | By design |
| 41 | 9.5.3 | The Tag shall check whether the values of BlockSize and KeySize are supported by Key.KeyID and that Key.KeyID is authorized for use in Interrogator-Tag mutual authentication. If at least one of these checks is failed, the Tag shall return a "Not Supported" error. | O | Tag | By design |
| 42 | 9.5.3 | The Tag shall check whether the value of parameter set PS is supported by the Tag. If not, the Tag shall return a "Not Supported" error. | O | Tag | By design |
| 43 | 9.5.3 | The Tag shall generate a random challenge TChallenge-b/k. | O | Tag | By design |
| 44 | 9.5.3 | The Tag shall construct a *b*-bit string by concatenating C_MAM-*b*/*k* with the (*b*-*t*-*c*) most significant bits of TChallenge-*b*/*k* and the entirety of IChallenge-*b*/*k*. | O | Tag | By design |
| 45 | 9.5.3 | The Tag shall use Key.KeyID to compute the b-bit string S where<br>S = SIMON-*b*/*k*-ENC ( Key.KeyID, C_MAM-*b*/*k* \|\| | O | Tag | Test_Pattern 8 |

Deleted: PRF

| | | | | | |
|---|---|---|---|---|---|
| | | TChallenge-$b/k$ [$t$-1:2$t$-$b$+$c$] ‖<br>IChallenge-$b/k$ ). | | | |
| 46 | 9.5.5 | After receiving MAM1 Response, the Interrogator shall use Key.KeyID to compute the $b$-bit string T where:<br>T = SIMON-$b/k$-DEC ( Key.KeyID, TResponse[$b$-1:0] ).<br>1. The Interrogator shall check that T[$t$-1:0] = IChallenge-$b/k$. | O | Interrogator | By design |
| 47 | 9.5.6 | If the cryptographic protocol has not been abandoned, the Interrogator shall form a $b$-bit string IResponse depending on the parameter set PS as follows:<br>1. If PS = $00_2$ then IResponse is equal to<br>SIMON-b/k-DEC ( Key.KeyID, C_MAM-$b/k$ ‖ T[$b$-$t$-$c$-1:0] ‖ T[$b$-$c$-1:$t$] ‖<br>TResponse[$2t$+$c$-1:$b$] ).<br>2. If PS = $01_2$ then IResponse is equal to T[$b$-$c$:$t$].<br>The Interrogator shall set SecureComm = $0001_2$ if secure communications as described in Section 10 will be used after mutual authentication is completed. Otherwise, the Interrogator shall set SecureComm = $0000_2$.<br>The Interrogator shall send IResponse and the value of SecureComm to the Tag as part of the MAM2 message. | O | Interrogator | By design |
| 48 | 9.5.7 | The Tag shall only accept this message when the cryptographic engine is in the state **PA2**. | O | Tag | By design |
| 49 | 9.5.7 | If Mutual authentication is not supported on the Tag, i.e. if "$10_2$" is not a valid value for AuthMethod, then the Tag shall return a "Not Supported" error condition. | O | Tag | By design |
| 50 | 9.5.7 | The Tag shall check if the Step is "$01_2$". If the value of Step is different, the Tag shall return a "Not Supported" error. | O | Tag | Test_Pattern 9 |
| 51 | 9.5.7 | The Tag shall check if the RFU is "$0000_2$". If the value of RFU is different, the Tag shall return a "Not Supported" error. | O | Tag | Test_Pattern 9 |
| 52 | 9.5.7 | If PS = $00_2$ then the Tag computes the $b$-bit string S = SIMON-$b/k$-ENC ( Key.KeyID, IResponse ).<br>SIMON-b/k-DEC ( Key.KeyID, C_MAM-$b/k$ ‖ T[$b$-$t$-$c$-1:0] ‖ T[$b$-$c$-1:$t$] ‖<br>TResponse[$2t$+$c$-$b$-1:0] ).<br>The Tag shall check if S[$t$-1:0] = TChallenge-$b/k$. | O | Tag | Test_Pattern 10 |
| 53 | 9.5.7 | If PS = $01_2$, then the Tag shall check whether S = TChallenge-$b/k$. | O | Tag | Test_Pattern 10 |