INTERNATIONAL STANDARD

ISO/IEC 21277

First edition
2018-02

Information technology — Radio frequency identification device performance test methods — Crypto suite

Technologies de l'information — Méthodes de test de performance des systèmes d'identification par radiofréquence (RFID) — Suites cryptographiques

Reference number
ISO/IEC 21277:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
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 Symbols and abbreviated terms **2**
5 Measurement context **2**
6 Setup of test equipment **2**
7 System parameters **3**
7.1 General 3
7.2 Crypto performance 3
7.3 Interrogator-system architecture 3
8 Measurements in scope **3**
9 Test method **4**
Annex A (informative) **Interrogator crypto suite implementation** **7**
Annex B (informative) **Security suite application considerations** **8**
Bibliography **9**

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

Introduction

ISO/IEC 18000 defines the air interfaces for radio frequency identification (RFID) devices used in item management applications. ISO/IEC 18000-63 defines the air interface for these devices operating at frequencies from 860 MHz to 960 MHz Type C.

ISO/IEC 29167 defines crypto suite air interfaces for ISO/IEC 18000-63 utilising on tag cryptography functions.

This document provides test methods for performance measurement of the ISO/IEC 29167 devices.

NOTE This specification is a system measurement of tag and interrogator performance.

Information technology — Radio frequency identification device performance test methods — Crypto suite

1 Scope

This document defines test methods to measure the performance of crypto suites of radio frequency identification (RFID) devices (tags and interrogators) for item management as specified in ISO/IEC 18000-63 and ISO/IEC 29167 (all parts).

These test methods measure the crypto suite system performance (tags and interrogators) against the crypto suite outcomes as required by the desired set of use case requirements for a specific application/service. These test methods are used as an extension of ISO/IEC 18046-1 but can be used in a standalone manner.

Crypto suite performance can vary substantially between crypto suites, implementations of a crypto suite for tags and interrogators and crypto suite outcomes in specific interrogation scenarios. Tag crypto functions require time and energy to complete successfully. The desired crypto strength and method influence the time and energy required. "Crypto suite performance" is therefore defined in this document as "the shortest time to complete a crypto outcome at a given read distance in relation to the RF power available". This document provides guidelines in the evaluation of the measurement results.

The test methods do not measure crypto capabilities which include crypto strength, suitability and robustness. They neither measure random generator performance nor deal with key management.

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 18046-1, *Information technology — Radio frequency identification device performance test methods — Part 1: Test methods for system performance*

ISO/IEC 19762, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762 and ISO/IEC 18000-63 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/

4 Symbols and abbreviated terms

4.1 Symbols

For the purposes of this document, symbols given in ISO/IEC 19762 and ISO/IEC 18000-63 apply.

4.2 Abbreviated terms

For the purposes of this document, the abbreviated terms given in ISO/IEC 19762 and ISO/IEC 18000-63 apply.

5 Measurement context

The combination of ISO/IEC 18000-63 and ISO/IEC 29167 provides a set of security outcomes by utilising on-chip cryptography functions. The set of potential crypto functions are as follows:

1) Authentication – this method may be used where the physical interrogation environment ensures that the risk of over the air splicing or message confusion is countered within the scope of the overall security risk.

   a) Tag – the interrogator trusts the tag.

   b) Interrogator – the tag trusts the interrogator.

   c) Mutual – the tag and the interrogator trust each other.

2) Communication

   a) Authenticated communication – This counters over the air splicing or message confusion.

   Tag => Interrogator – the interrogator trusts the message from the authenticated tag.

   Interrogator => Tag – the tag trusts the message from the authenticated interrogator.

   Interrogator <=> Tag – the tag and interrogator trust each other's messages.

   b) Encrypted communication – This counters eavesdropping.

   Tag => Interrogator – messages from the tag can only be recovered by the interrogator.

   Interrogator => Tag – messages from the interrogator can only be recovered by the tag.

   Interrogator <=> Tag – messages can only be recovered by the two participants.

   c) Authenticated and encrypted communication (a and b).

   Tag => Interrogator

   Interrogator => Tag

   Interrogator <=> Tag

3) Untraceability may be achieved by ensuring that the tag cannot be uniquely recognised by the messages between the tag and the interrogator.

6 Setup of test equipment

Test equipment shall be setup in accordance with ISO/IEC 18046-1.

Duration may be measured by programming the interrogator to perform interrogation duration measurement or by using a spectrum analyser. Whichever is used shall be noted on the test report.

7 System parameters

7.1 General

These system parameters, while not addressed by the specification, should be considered by users.

7.2 Crypto performance

Crypto performance normally refers to crypto strength, suitability and robustness, which is associated with key length, crypto algorithms, hash function, time to process, energy required to process, to name a few.

The applicability of the crypto method of a crypto suite should be performed by inspection which needs to consider the following:

1) The system (which uses the crypto suites) implementation needs to address the risk profile of the system use.

2) Random generator performance of both the tag and the interrogator.

3) Crypto strength.

4) Key management.

5) Revocation of compromised tags or sets of tags because of a compromised key.

6) Roll-over to news keys sets, maintaining operability of deployed tags and future proving data structure changes.

NOTE 1 The following specifications (of many more) can assist in evaluating points 1 and 2:

— FIPS 140-2;

— NIST/SP 800-22, Rev. 1a.

NOTE 2 Items 3) to 6) are complex issues which extend beyond key lengths and key configures within the digital domain. See NIST/SP 800-57-1, Rev. 4 and NIST/SP 800-131A, Rev. 1.

7.3 Interrogator-system architecture

The overall performance of a crypto suite enable application/service/system should be analysed to determine the suitability of the crypto suite within the system. For example; data network latency and the design of the crypto suit interrogator sub-system (see Annex A) may influence crypto suite performance within a system. This analysis is beyond the scope of this document.

8 Measurements in scope

ISO/IEC 29167-1 specifies the particular outcomes achievable by a crypto suite implementation. The measurement of the desired outcomes should be evaluated in the wider context of the desired security system it enables; see Annex B.

If supported, the following crypto suite outcomes should be measured for performance:

1) Tag authentication;

2) Interrogator authentication;

3) Mutual authentication;

4) Authentic message: Tag => Interrogator;

5) Authentic message: Interrogator => Tag;

6) Authentic message: Interrogator <=> Tag;

7) Encrypted message: Tag => Interrogator;

8) Encrypted message: Interrogator => Tag;

9) Encrypted message: Interrogator <=> Tag;

10) Authentic and encrypted message: Tag => Interrogator;

11) Authentic and encrypted message: Interrogator => Tag;

12) Authentic and encrypted message: Interrogator <=> Tag;

13) Untraceability.

NOTE Crypto suites achieve some or all of the outcomes in potentially more than one manner.

The purpose of an interrogation is to either read or write data from or to the tag. The purpose of the crypto suite is to ensure the security of that interrogation within the scope of the risk profile of the service/application enabled by this interrogation. For example, items 4) to 13) shall be measured in the context of ISO/IEC 18000-63 memory access (read and write):

1) UII — in untraceability mode the open readable UII may be shortened only to reveal a common identity.

2) TID — in untraceability mode the open readable TID may be shortened only to reveal the tag chip identity. TID is read-only.

3) User memory — the bit size of the user memory and the position of the data in the memory may influence the performance parameters.

9 Test method

The measurement shall be performed in the following steps:

1) Note the crypto suite to be measured.

2) Note the tag implementation and the interrogator implementation to be measured.

3) Note the desired RF power, frequency and spectrum management method for the measurement.

4) Select a random representative set of 10 tags for the measurement.

5) Select keys based on the crypto function directives to ensure the keys are operationally representative. Note the key selection and motivation for the key selection.

6) Prepare the data to be stored on the tag. The data shall be random.

7) Measure a read distance reference point, which is the longest distance at which a reliable interrogation of the tag is achieved:

   a) Select the simplest available interrogation incorporating at least a data message of 64 bits:

   Read — this will typically be an open UII read.

   Write — this will typically be an open UII write.

   b) Measure and note the read and write sensitivity and the read distance it was achieved at; see ISO/IEC 18046-1.

c) For validity of the measurement the deviation should within 5 %. Note the worst read and write distance as the reference point.

8) For each of the measurements in Table 2:

a) Select it to be included or excluded from the measurement.

b) If included, note and describe the command sequence of each manner to achieve the measurement.

9) For each manner and each tag in the set, measure and note the duration and deviation to complete the crypto interrogation at the best distance, 50 % and 30 % of the reference point. The best distance is determined by reducing the distance from the reference distance by 5 % until the test result is consistent and reliable (repeated measurements are within 5 %).

This part of the report should use the format of Table 1.

Table 1 — Measurement report template

Test: <Test #> - <test name> **Reference distance:** <reference distance> **Command sequence:** <command sequence>				
Tag #	**Best distance**	**Duration at the following distances**		
		Best	**50 %**	**30 %**
	6,5 m[a]	80 ms[a]	72 ms[a]	70 ms[a]
[a] Example values.				

Table 2 — Crypto interrogations measurements

#	Measurement	Comment
1	Read 64 bits UII	The amount of bits may [also] be increased to 128, 256, 512… as dictated by the ability of the crypto suite and/or the application requirement.
1a	Open	No crypto
1b	Open with tag authentication	The message transfer is not encrypted and not linked with the authentication step.
1c	Open with interrogator authentication	
1d	Open with mutual authentication	
1e	Authentic message: Tag => Interrogator	The message is linked with the authentication step. The message transfer may be part of the authentication step or following the authentication step. Note the manner(s) used when both options are supported.
1f	Authentic message: Interrogator => Tag	
1g	Authentic message: Interrogator <=> Tag	
1h	Encrypted message: Tag => Interrogator	
1i	Encrypted message: Interrogator => Tag	
1j	Encrypted message: Interrogator <=> Tag	

Table 2 *(continued)*

#	Measurement	Comment
1k	Untraceability: Tag => Interrogator	There may be more than one manner to achieve untraceability. Note the manner(s) and steps used to achieve untraceability.
1l	Untraceability: Interrogator => Tag	
1m	Untraceability: Interrogator <=> Tag	
2a-m	**Write 64 bits UII**	Measurement 1 comment
3a-m	**Read TID**	Note the TID size
4a-m	**Read the first 64 bits of user memory**	Measurement 1 comment
5a-m	**Read the last 64 bits of user memory**	Measurement 1 comment
6a-m	**Read the middle 64 bits of user memory**	Measurement 1 comment
7a-m	**Write the first 64 bits of user memory**	Measurement 1 comment
8a-m	**Write the last 64 bits of user memory**	Measurement 1 comment
9a-m	**Write the middle 64 bits of user memory**	Measurement 1 comment