INTERNATIONAL STANDARD

ISO/IEC 29167-1

Second edition
2014-08-15

Information technology — Automatic identification and data capture techniques —

Part 1: Security services for RFID air interfaces

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

Partie 1: Services de sécurité pour les interfaces radio RFID

Reference number
ISO/IEC 29167-1:2014(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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 ISO documents 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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is 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 29167-1:2012) which has been technically revised.

ISO/IEC 29167 consists of the following parts, under the general title *Information technology — Automatic identification and data capture techniques*:

— *Part 1: Security services for RFID air interfaces*

— *Part 10: Crypto suite AES-128 security services for air interface communications*

— *Part 11: Air interface for security services — Crypto suite PRESENT-80*

— *Part 12: Crypto suite ECC-DH security services for air interface communication*

— *Part 13: Air interface for security services — Crypto suite Grain-128A*

— *Part 14: Air interface for security services — Crypto suite AES OFB*

— *Part 15: Air interface for security services — Crypto suite XOR*

— *Part 16: Air interface for security services crypto suite ECDSA-ECDH*

— *Part 17: Air interface for security services crypto suite cryptoGPS*

— *Part 19: Air interface for security services crypto suite RAMON*

Introduction

ISO/IEC 29167 describes security as applicable for ISO/IEC 18000. ISO/IEC 29167 is an optional extension to the ISO/IEC 18000 air interfaces.

The ISO/IEC 18000 series of International Standards on radio frequency identification (RFID) for item management does not offer strong security of the tag and interrogator data and identity. For example, the unique item identifiers (UII) of tags are typically transmitted to every other device in the RF field and can thus be easily tracked. Additionally, sensitive data such as passwords are typically transmitted over RF without encryption and can easily be intercepted. Moreover, utilized passwords may be short in length. ISO/IEC 29167 fulfills the need for applications requiring effective security in the handling of sensitive information including the unauthorized interception and tracking of data and devices.

ISO/IEC 29167 covers the crypto suites for interrogators and tags that have security mechanisms on board. ISO/IEC 29167 only applies to tags that perform the computations that are required for the security mechanisms. Tag-to-tag communication is not excluded.

ISO/IEC 29167 covers a number of cryptographic suites designed for protecting application information transmitted across the RFID air interface, product authentication, and protecting access to resources on the tag. Suite implementations relative to specific ISO/IEC 18000 series RFID air interface standards, where relevant, are described in the Annexes of each cryptographic suite. Users should be aware that they must assess their own risk management needs for their application (e.g. amount of necessary security features, management of keys, etc.) in order to determine the appropriate suite for implementation.

This part of ISO/IEC 29167 describes a framework to implement security mechanisms used in an RFID system. The other parts of ISO/IEC 29167 specify individual crypto suites.

Information technology — Automatic identification and data capture techniques —

Part 1:
Security services for RFID air interfaces

1 Scope

This part of ISO/IEC 29167 defines the architecture for security services for the ISO/IEC 18000 air interfaces standards for radio frequency identification (RFID) devices. Its purpose is to provide a common technical specification for optional security services for RFID devices that may be used by ISO committees developing RFID application standards.

This part of ISO/IEC 29167 defines various security features called security mechanisms that can be implemented by a tag depending on the application. A tag may support one, a subset, or all of the specified security mechanisms. For an interrogator, it is possible to get information about the security mechanisms that are actually implemented and supported by a tag. Moreover, it has been considered that adding new security mechanisms remains possible. Besides signalling the presence of certain security services, further details of the mechanisms such as utilized encryption algorithm and key length also need to be specified and accessible.

This part of ISO/IEC 29167 defines the requirements for crypto suites defined in further parts of this International Standard and, furthermore, defines how crypto suites identifiers are assigned to the various parts of this International Standard.

2 Conformance

In general, it is assumed that all requirements defined in this part of ISO/IEC 29167 shall be fulfilled.

A tag is compliant to this part of ISO/IEC 29167 if it supports one or more of the security mechanisms as defined in this part of ISO/IEC 29167.

An interrogator is compliant to this part of ISO/IEC 29167 if it supports one or more of the security mechanisms as defined in this part of ISO/IEC 29167.

The discovery mechanisms are mandatory for interoperability.

3 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

4 Terms and definitions, symbols, and abbreviated terms

4.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762 (all parts) and the following apply.

4.1.1
crypto suite
module for secure data handling that can be utilized by multiple air interfaces due to its modularity

4.2 Symbols and abbreviated terms

PRNG pseudo random generator

TRNG true random generator

5 Safeguarding personal privacy and data

5.1 Motivation

RFID technology enables the processing of data without physical contact or visible interaction between the interrogator and the tag. Application of the technology can deliver numerous economic and societal benefits.

RFID applications hold the potential to transfer data relating to an identified or identifiable person who is being identified directly or indirectly. Furthermore, the potential exists for this technology to be used to monitor an individual through his/her possession of one or more items that contain a unique RFID item number. This interaction can happen without the individual concerned being aware of it.

The functionality offered by ISO/IEC 29167 allows RFID applications to provide privacy, integrity, authenticity and confidentiality of the data on the tag. This functionality includes organization of data and access control.

ISO/IEC 29167, in combination with ISO/IEC 18000, addresses issues of privacy and security related to the use of RFID for Item Management. This part of ISO/IEC 29167 provides an overview, while details will be described in the specific parts of ISO/IEC 29167 in combination with the corresponding parts of ISO/IEC 18000.

ISO/IEC 29167 extends ISO/IEC 18000 with the following features:

— untraceability;

— authenticity;

— secure access to data and functions,

— encryption.

5.2 Features of this International Standard

The tag features and air interface commands in ISO/IEC 29167 enable the implementation of the following features in an RFID system:

— Untraceability: by putting the tag in a special mode (called untraceability mode) where the RFID tag hides all or part of its identity.

— Certify authenticity: by using one or more air interface commands a tag can produce a certificate of authenticity. Verification of this certificate may require additional features such as key management to be implemented in the RFID system.

— Secure access to tag data and functions: data can be organized in files, access to these files and tag functions can be configured and transmission of the data can be secured.

In addition to these features, the tag also provides the necessary information about the features and air interface commands it supports.

5.3 Safeguarding personal privacy and data on the tag

Privacy and information security features should be built into the RFID applications before their widespread use.[1)] ISO/IEC 29167 is intended to assist RFID application operators in taking reasonable measures to achieve 'security and privacy-by-design'. The main properties that need to be protected are:

a) Identity of the tag The identity of the tag can be protected by the untraceability feature. Untraceability prevents unauthorized tracking of a tag. Untraceability prevents associating the tag to an identified or identifiable person.

b) Data on the tag Access to the data (and other features of the tag) may be protected by verification of the authenticity of the interrogator. The data on the tag may be organized in files. Access rights may be associated to each individual file.

c) Communication between the tag and the interrogator The data that needs to be exchanged between the tag and the interrogator can be overheard by somebody who intercepts this communication. The integrity and confidentiality of the data may be protected by cryptographic methods.

5.4 Implications of security

5.4.1 Key management

Use of cryptography requires the management of secrets, sometimes including keys. Management of secrets increases system complexity.

For example:

— The secrets should be communicated and stored securely.

— Complexity increases with multiple custodians of secrets in the system.

— Mechanisms to recover from compromised secrets increases complexity of the system.

CAUTION — Inadequate management of secrets can compromise the security and effectiveness of the entire supply chain.

5.4.2 Increased resource requirements for RFID components

Implementation of cryptography requires additional resources on the interrogator and/or on the tag.

5.4.3 Performance

Application of cryptography impacts power consumption and processing time for the RFID components and may degrade system performance.

1) For further information, see related document of the European Commission: Reference [11], [12], [13], [14], [15], [16], [17], [18].

5.4.4 Random number generation

Most cryptography depends on random numbers. Such random numbers are usually generated by pseudo random generators (PRNG) or true random generators (TRNG). Details about random number generation are described in ISO/IEC 18031.

Users of crypto suite enabled RFID products should be aware of issues surrounding the random number generation.

CAUTION — Lack of entropy in random numbers can defeat security services provided by cryptographic suites

6 Security mechanisms

6.1 General

This part of ISO/IEC 29167 describes a framework to implement security mechanisms used in an RFID system. The other parts of ISO/IEC 29167 specify individual crypto suites. Implementations of commands for various different frequencies remain in the respective ISO/IEC 18000 part.

The tag shall allow access control by security mechanisms as will be specified in other parts of ISO/IEC 29167. The mechanisms specify how data and resources on the tag can be accessed and retrieved in a secure manner and how the data-communication channel between the interrogator and the tag can be protected against attacks (tracking, cloning, relaying etc.).

6.2 Untraceability

Untraceability is the property that controls if and how the tag can be identified. Untraceability ranges from uniquely identifiable (no untraceability) to completely untraceable when a tag does not emit any (identifiable) information.

For most practical applications the highest level of untraceability will correspond to that of a tag that is detectable and for which the physical communication properties can be determined: e.g. ISO/IEC 18000-63 physical layer. This untraceability level could be realized by, for instance, ensuring that all untraceable tags of the same family reply to identical queries with a response that is formatted identically and that all the fields of this reply are either:

— are either all the same for all tags or for groups of tags, or

— undistinguishable from random.

Examples regarding the amount of information that is revealed include:

— no information (ultimate untraceability),

— presence and tag family (highest practical untraceability)

— cryptographic suite parameters (e.g. information about authentication required to change the untraceability settings),

— partial identity (e.g. manufacturer info), and

— full identity (e.g. serial number).

The other parts of ISO/IEC 29167 may define the detailed behaviour of the untraceability mode for particular ISO/IEC 18000 compatible tags. Those parts will also specify how the untraceability mode is enabled and disabled.

6.3 Physical mechanisms

Physical security mechanisms are security functions based on physical properties, such as communication distance reduction, or physical interaction such as a push button.

The other parts of ISO/IEC 29167 will define the detailed behaviour of the physical mechanisms for particular ISO/IEC 18000 compatible tags.

6.4 Cryptographic mechanisms

Cryptographic mechanisms are based on cryptographic algorithms. The cryptographic mechanisms provided by this framework include mechanisms to:

— Verify the genuineness of tag.

— Prove the authenticity of the data, tag and/or interrogator.

— Control access to tag data and functions.

— Secure communications.

6.5 Cryptographic suites

A cryptographic suite is a set of functions that specify how to apply a cryptographic algorithm on input data to produce output data. A cryptographic suite defines the sequence in which to apply these functions and the data to be retained in order to implement basic security protocols. Details of the cryptographic suites will be defined in the other parts of ISO/IEC 29167.

ISO/IEC 29167 allows the definition of multiple interoperable cryptographic suites. Parts of ISO/IEC 29167 may support more than one cryptographic suite to be supported on a tag.

The flexibility and choice of cryptographic suites allows for a large number of possible configurations.

7 Discovery mechanisms

The discovery mechanisms allow getting the identity of an untraceable tag and obtaining more information on supported security and file management mechanisms and the current state of the tag.

— Get status of the untraceability mode of a tag. When the untraceability mode is active then data sent from the tag does not show its identity (or only a configurable part of it) and the interrogator shall act accordingly (e.g. ignore the data or retrieve the identity of the tag).

— Get features supported by the tag: this mechanism allows an interrogator to read information about the security mechanisms, cryptographic suites and file management that are implemented on the tag.

— Get identity of an untraceable tag: this mechanism allows authorized interrogators only to uniquely identify an untraceable tag.

The specific implementation details are specified in the various parts of ISO/IEC 18000.

8 File management mechanisms

File management mechanisms enable protection and selective access to data on the tag.

File management allows for partitioning of a tag's physical memory into a set of logical memories, each of which can be viewed as a file, so that different files on a tag can be addressed independently, and governed by different access privileges (such as Read and Write permissions).

Some or all of a tag's files may define access privileges that require security mechanisms. The resulting access conditions shall be defined in terms of which security mechanisms grant access to each privilege.

Other than files, a tag may further implement standardized or manufacturer-defined memory locations that can be – either exclusively or additionally – directly accessed through specific Crypto Suite commands.

If a tag supports hidden (or untraceable) memory that is not accessible to interrogators by means of non-cryptographic commands defined in the tag's respective air interface standard (e.g. as a means of privacy or confidentiality protection), then the Crypto Suite shall specify if and how the hidden memory portions can be accessed by means of the cryptographic mechanisms it defines.

The various parts of ISO/IEC 18000 may define file management mechanisms such that each file, once selected by the interrogator, uses the same standard address space and air interface commands used by a tag that does not support file management.

9 Assignment of Crypto Suite Indicators (CSI)

9.1 Relation of CSI and part number

ISO/IEC 29167 supports 8 bits (CSI7- CSI0) to number Crypto Suites. Crypto Suites are defined in other parts of ISO/IEC 29167 starting with part number 10. Part numbers smaller than 10 are not assigned for Crypto Suites, as they have been previously used for air interface specific assignments.

Table 1 defines the assignment of the leading bits of the CSI.

Table 1 — CSI assignment of leading bits

CSI7	CSI6	CSI5	CSI4	CSI3	CSI2	CSI1	CSI0	CSI ASSIGNMENT BY
0	0	X	X	X	X	X	X	ISO/IEC 29167
0	1	X	X	X	X	X	X	RFU
1	0	X	X	X	X	X	X	RFU
1	1	0	0	X	X	X	X	RFU
1	1	0	1	X	X	X	X	Tag manufacturer
1	1	1	0	X	X	X	X	GS1
1	1	1	1	X	X	X	X	Reserved for future extension (providing 12 bits for CSI out of 16 bits in total)

When CSI7 and CSI6 are both zero (corresponding to the first row of Table 1), then (CSI5-CSI0) for each part are defined by the part number itself by subtracting the value of 10 from the part number. In order to ensure that there is no misunderstanding details are shown in Table 2.

Table 2 — CSI5-CSI0 bit assignment

CSI5	CSI4	CSI3	CSI2	CSI1	CSI0	PART
0	0	0	0	0	0	ISO/IEC 29167-10
0	0	0	0	0	1	ISO/IEC 29167-11
0	0	0	0	1	0	ISO/IEC 29167-12
0	0	0	0	1	1	ISO/IEC 29167-13
0	0	0	1	0	0	ISO/IEC 29167-14
0	0	0	1	0	1	ISO/IEC 29167-15
0	0	0	1	1	0	ISO/IEC 29167-16
0	0	0	1	1	1	ISO/IEC 29167-17

Table 2 *(continued)*

CSI5	CSI4	CSI3	CSI2	CSI1	CSI0	PART
0	0	1	0	0	0	ISO/IEC 29167-18
0	0	1	0	0	1	ISO/IEC 29167-19
0	0	1	0	1	0	ISO/IEC 29167-20
…	…	…	…	…	…	
1	1	1	1	1	0	ISO/IEC 29167-72
1	1	1	1	1	1	ISO/IEC 29167-73

For all rows of Table 1, except for the final "extension" row, the numerical value of the CSI is equal to the decimal equivalent of the binary value shown. For example, the highest-possible CSI-assigned CSI is "11101111" representing a CSI with the decimal value 239. Therefore, the first "extension CSI" ("1111" followed by 12 zero bits) will be assigned a decimal value of 240.

9.2 Example for CSI of an ISO/IEC 29167-n

The below example shall be used in each part of ISO/IEC 29167-n, whereas it is shown for the example of ISO/IEC 29167-12:

This part of ISO/IEC 29167 is part 12 and shall be used with CSI = 2 as shown in Table 3.

Table 3 — CSI7-CSI0 assignment for ISO/IEC 29167-12

CSI7	CSI6	CSI5	CSI4	CSI3	CSI2	CSI1	CSI0	PART
0	0	0	0	0	0	1	0	ISO/IEC 29167-12

9.3 Example for CSI of ISO/IEC 18000-63

ISO/IEC 180000-63 supports an 8 bit CSI field as shown in Table 4.

Table 4 — CSI7-CSI0 assignment in ISO/IEC 18000-63 for ISO/IEC 29167-12

CSI7	CSI6	CSI5	CSI4	CSI3	CSI2	CSI1	CSI0	PART
0	0	0	0	0	0	1	0	ISO/IEC 29167-12

In ISO/IEC 18000-63 all CSI with CSI7 = 0 and CSI6 = 0 are according ISO/IEC 29167.

9.4 Sources for Crypto Suite Indicators

9.4.1 General

If a new Crypto Suite shall be considered for any part of ISO/IEC 18000 then this may be done by multiple ways. In case the new Crypto Suite shall become a part of ISO/IEC 29167 then clause 9.4.2 shall apply. Otherwise clause 9.4.3 or other any higher numbered clause in 9.4 shall apply.

9.4.2 ISO/IEC 29167

For the ISO/IEC 18000 series (where CSI7-CSI6 = 00), ISO/IEC 29167 applies and a NWIP shall be filed for a new part of ISO/IEC 29167. If the NWIP is approved then the ISO CS assigns a new part number for this submission. As ISO CS ensures that there are no duplications in numbers for standards it is also ensured that CSI5-CSI0 are unique.

9.4.3 Others

In case of any other content of CSI7-CSI6 than 00 the respective organization has to be approached.

9.5 Increase number of CSIs for ISO/IEC 29167

If all numbers for CSI5-CSI0 are used up then ISO/IEC 29167 will be revised in order to assign another content for CSI7-CSI6 for ISO/IEC 29167. This will require some rewording in respect to how CSI5-CSI0 are derived from the part number in ISO/IEC 29167-1.

10 Crypto suite template

SD 3 (Standing Document 3) should be used as template for a crypto suite.