INTERNATIONAL STANDARD

ISO/IEC 29167-1

First edition
2012-03-01

Information technology — Automatic identification and data capture techniques —

Part 1: Air interface for security services and file management for RFID architecture

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

Partie 1: Interface d'air pour services de sécurité et gestion des fichiers pour architecture RFID

Reference number
ISO/IEC 29167-1:2012(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

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 29167-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

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

— *Part 1: Air interface for security services and file management for RFID architecture*

Introduction

ISO/IEC 29167 describes file management and 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 fulfils 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 air interface for interrogators and tags that have security mechanisms and/or file management on board. ISO/IEC 29167 only applies to tags that perform the computations that are required for the security and file management mechanisms. Tag to tag communication is not excluded.

Information technology — Automatic identification and data capture techniques —

Part 1:
Air interface for security services and file management for RFID architecture

1 Scope

This part of ISO/IEC 29167 defines the architecture for security and file management for the ISO/IEC 18000 air interface standards for radio frequency identification (RFID) devices. It provides a common technical specification for security and file management for RFID devices that can be used by ISO committees developing RFID application standards.

This part of ISO/IEC 29167 specifies architecture for

— untraceability,

— security services, and

— file management

as a further optional extension of the air interface. Both security and file management are defined in alignment with existing air interfaces and this part of ISO/IEC 29167 only covers extensions on security and file management beyond the scope of the ISO/IEC 18000 air interfaces.

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 can 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 signaling 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.

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 or file management mechanisms as defined in this part of ISO/IEC 29167.

The discovery services are mandatory for interoperability.

3 Normative references

The following referenced documents are indispensable for the application 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 15962, *Information technology — Radio frequency identification (RFID) for item management — Data protocol: data encoding rules and logical memory functions*

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

4 Terms and definitions

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

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. The technology can deliver numerous economic and societal benefits.

RFID applications hold the potential to process 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 ensure 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.

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:

1) 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.

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

3) 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 render an entire supply chain ineffective.

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 and time consumption for the RFID components and may degrade system performance.

1) For further information see related document of the European Commission: [9], [10], [11], [12], [13], [14], [15] and [16].

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 will specify detailed implementation requirements for the corresponding frequencies and define the command set.

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 18000-6 type C 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:

— the same for all tags, or

— undistinguishable from random.

Examples in which information 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 will define the detailed behavior 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 behavior 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 will be specified in the other parts of ISO/IEC 29167.

8 File management mechanisms

These 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).

8.1 File access

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.