INTERNATIONAL STANDARD

ISO/IEC 15963

Second edition
2009-09-01

Information technology — Radio frequency identification for item management — Unique identification for RF tags

Technologies de l'information — Identification par radiofréquence pour la gestion des objets — Identification unique des tags RF

Reference number
ISO/IEC 15963:2009(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.

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 15963:2009 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 15963:2004), which has been technically revised.

Introduction

ISO/IEC 15963 is one of a series of International Standards and Technical Reports developed by ISO/IEC JTC 1/SC 31 for the identification of items (Item Management) using radio frequency identification (RFID) technology.

ISO/IEC 15963 describes numbering systems for the unique identification of RF tags.

It is intended for use in conjunction with other International Standards developed by SC 31 for "RFID for item management" and “Real time locating systems” such as ISO/IEC 18000 and ISO/IEC 24730.

Information technology — Radio frequency identification for item management — Unique identification for RF tags

1 Scope

This International Standard describes numbering systems that are available for the identification of RF tags.

The unique ID can be used

— for the traceability of the integrated circuit itself for quality control in its manufacturing process,

— for the traceability of the RF tag during its manufacturing process and along its lifetime,

— for the completion of the reading in a multi-antenna configuration,

— by the anti-collision mechanism to inventory multiple tags in the reader's field of view, and

— for the traceability of the item to which the RF tag is attached.

2 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 19762-1, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary — Part 1: General terms relating to AIDC*

ISO/IEC 19762-3, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary — Part 3: Radio frequency identification (RFID)*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762-1, ISO/IEC 19762-3 and the following apply.

3.1
RF tag
automatic identification and data capture device carrying data that can be queried by means of suitably modulated inductive or radiating electromagnetic carriers from an interrogator so as to transfer information to an information system

NOTE RF tags include both RFID and RTLS transponders.

3.2
RF tag unique identifier
number that uniquely identifies an RF tag

3.3
RF tag issuer
company or organization that allocates the RF tags to the items they identify

3.4
IC manufacturer
company that manufactures the RF tag integrated circuit

3.5
RF tag manufacturer
company that manufactures the RF tag in a ready-to-use configuration

3.6
allocation class
8-bit value used to classify companies or organizations allowed to allocate unique tag identification

3.7
IC manufacturer registration number
number allocated to IC manufacturers according to ISO/IEC 7816-6 or ANSI ASC INCITS T6

3.8
RF tag issuer registration number
number allocated to RF tag issuers according to ISO 6346, ISO/TS 14816, GS1, or ANSI ASC INCITS T6

3.9
chip ID
CID
unique permanent ID of the integrated circuit in an RF tag

NOTE The term unique identifier (UID) is deprecated. See **tag ID**, **unique item identifier** and **object identifier**.

3.10
tag ID
TID
unique permanent ID of the actual RF tag

NOTE 1 May or may not be the same as the Chip ID.

NOTE 2 There may be multiple chips within a tag.

NOTE 3 The tag ID may identify the manufacturer of a completed tag device and constituent parts of that tag

NOTE 4 The term unique identifier (UID) is deprecated. See **chip ID**, **unique item identifier** and **object identifier**.

3.11
unique item identifier
UII
identification that uniquely identifies a specific entity during its life

NOTE 1 An item ID may not change though the data carrier may be used to identify a different item. In that case, the Item ID within the data carrier would change.

NOTE 2 A DoD Unique Identifier “UID” and an “EPC” are both forms of Item ID. A GS1 SSCC is an example of a time limited Item ID (IID). A GS1 GRAI is an example of an Item ID (IID) assigned to a returnable asset. A GS1 sGTIN is an example of an Item ID (IID) assigned to a commercial product.

NOTE 3 The term unique identifier (UID) is deprecated. See **chip ID**, **tag ID** and **object identifier**.

3.12
object identifier
OID
unambiguous identifier for an “Informational Object” that can identify a product, an organization, a person, a standard, a drawing, a (computer) file, etc.

NOTE 1 In general an Object Identifier is associated with a type of object, and is used to label information on an instance of that type as such.

NOTE 2 The term unique identifier (UID) is deprecated. See **chip ID**, **tag ID** and **unique item identifier**.

4 Abbreviated terms

AC	Allocation Class
AID	Application Identifier
ANS	American National Standard
ANSI	American National Standards Institute
ASC	Accredited Standards Committee
CID	Chip Identifier
GS1	a set of standards administered by GS1
IC	Integrated Circuit
ID	Identifier
INCITS	InterNational Committee for Information Technology Standards
LSB	Least Significant Bit
MSB	Most Significant Bit
OID	Object Identifier
RFU	Reserved for Future Use
RTLS	Real-Time Locating System
TID	Unique Tag Identifier
UID	Unique Identifier (as defined by the U.S. Department of Defense)
UII	Unique Item Identifier

5 Unique identifiers

There are several types of identifiers associated with an RF tag. The most basic form is a chip ID (CID), which is assigned by the integrated circuit (I.C.) manufacturer to a specific semiconductor device at the time of manufacture in a manner that prevents it from being changed. Multiple semiconductor devices may be associated with a single RF tag, though one I.C. per tag is common. In such a case, the identity of the RF tag (TID) might simply assume the CID as its identity or it may assign an identifier distinct from the I.C. In many cases, and as a recommendation of this standard, the TID is assigned at the time of RF tag manufacture in a manner that prevents the TID from being changed.

The RF tag is then attached to some item. In some implementations the TID might then become the unique item identifier (UII). In others, such as ISO/IEC 18000-6, Type C and ISO/IEC 18000-3, Mode 3 the UII is held in a separate part of memory and is written subsequent to being attached or associated with a specific item. The UII may either be locked or available for reprogramming.

Global uniqueness requires a central body (registration authority) to either assign manufacturer identities or to assign unique identities to various agencies that in turn assign manufacturer identities. Manufacturers then assign unique identification to the chip, tag, or item. This standard serves as the central body for assignment of unique identifiers to RF tags. This standard assigns various Allocation Classes to various agencies that issue manufacturer codes.

Some tags only have identity down to a specific lot, batch, or mask identifier. Other tags, and as recommended by this standard, are serialized so that all RF tags are globally unique from all other RF tags.

The combination of globally unique serialized tag (TID) programmed and locked at the time of manufacturer, with the unique item identifier (UII) programmed when attached or associated with a specific item and trusted trading partner communications are the cornerstones of several anti-counterfeiting techniques used within the supply chain.

For anti-collision, inventorying, reading from, and writing to an RF tag, techniques exist to utilize the TID, UII, or a randomly generated number. Neither the UII nor the randomly generated number provide life-cycle traceability for the RF tag. A TID does provide for such traceability

6 Possible ways to uniquely identify an RF tag

When a unique identification of an RF tag is required, it can be done in several ways. The following sub-clauses list and explain some of them.

6.1 Virtual ID

A virtual tag ID is a temporary ID based on tag parameters that may vary over the life of the tag. It may take several forms. A virtual ID is also known as a logical ID or a session ID. Several tags could have the same virtual ID at different times, but all tags at the same time for the same interrogator should have a different virtual ID, allowing an unambiguous identification of each tag at any time relative to any given interrogator.

The technical means to achieve and guarantee such uniqueness is outside of the scope of this International Standard. However clauses 6.1.1, 6.1.2, and 6.1.3 discuss possible approaches.

6.1.1 Data as a unique ID

Data is a possible way to implement a virtual ID where the tag contains data that when read is unique in time and location to a single tag. An example is a tag that contains date and time information. The time information can be unique to a single tag from a manufacturer, but is not guaranteed to be unique over all tags at all times. Another situation is a closed application where tag data describes only one set of information. Taken globally, the tag bit pattern might be repeated, but in a closed application the tag data uniquely identifies a single tag.

6.1.2 Time as a unique ID

Time is a possible way to implement a virtual ID where bit patterns alone do not necessarily identify a single tag unambiguously. Tag response time slot can be part of a uniquely identifying parameter set. For example, some tags use time slots to differentiate between several tags appearing to a reader at the same time. If these time slots are fixed for a single interrogation exchange, then the time slot may be used to help define a single tag at a particular time.

NOTE If the time slots are randomly defined each time a tag responds, then time slots are not suitable for determining a unique tag ID.

6.1.3 Position as a unique ID

In some applications, tag position may define a unique tag ID at a particular time. For instance, some tags have a read and write distance of only a few millimetres. In this case it is difficult to have more than one or two tags in the interrogation zone at any time. Thus any tag continually in the reading zone may be considered unique at that single time and location. A common example of this case is the tag used for fare collection on public transportation or telecommunication charges.

6.2 Permanent unique ID

When a completely and globally unique ID is required, it shall be programmed into the tag, and therefore becomes permanent.

Methods of assigning permanent unique identifiers are given in Tables A.1 to A.7.

6.2.1 Benefits of permanent unique ID versus virtual ID

The advantage of a virtual (session) ID is the reduced number of identification bits required. The disadvantage is the absence of a unique ID, independent of the reader, application, time or data configuration used. The virtual ID is unique only at a specific time and location, and is sufficient to allow the identification of a singular tag relative to time and space.

The advantage of a permanent unique ID is that it guarantees a single ID over all application, space and time situations. It is the only identification method where a completely unique ID is guaranteed in all situations.

6.2.2 Selection of the size of a permanent unique ID

Several criteria must be taken into account when selecting the size (i.e. the number of bits) of a permanent unique ID:

a) To comply and coexist with existing ISO/IEC standards, so that the uniqueness is guaranteed globally, and that the objectives of the ISO standards are met.

b) To structure it such that it's technical implementation is optimized. This results for RF tags in the selection of an "N power 2" number of bytes (1, 2, 4, 8).

c) To guarantee a number of combinations large enough to ensure that no two tags will be allocated the same ID within the maximum expected lifetime of a tag, under reasonable conditions, e.g. 10 years.

d) To ensure that individual ID assignments can be delegated to IC or tag manufacturers in an efficient manner.

e) To limit it to the absolute minimum size (i.e. number of bits) required to meet the above criteria, as its size might penalize the performance of the interrogator-to-tag communication by increasing the number of bits to transmit. As an example, a small number of bits (e.g. 32 bits) may be sufficient for applications with a small number of tags.