INTERNATIONAL STANDARD

ISO/IEC 29176

First edition
2011-10-15

Information technology — Mobile item identification and management — Consumer privacy-protection protocol for Mobile RFID services

Technologies de l'information — Gestion et identification d'élément mobile — Protocole de protection de la vie privée de l'utilisateur pour les services RFID mobiles

Reference number
ISO/IEC 29176:2011(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 29176 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology,* Subcommittee SC 31, *Automatic identification and data capture techniques*.

Introduction

There are many possible concerns regarding the authenticity and integrity of mobile radio frequency identification (Mobile RFID) systems. For example, an unauthorized interrogator can easily read a UII (Unique Item Identifier), TID (Tag Identifier), and the User memory banks of ISO/IEC 18000-6 Type C tags and ISO/IEC 18000-3 MODE 3 tags because there is no read-protection for these memory banks. In this case, the unauthorized interrogator could gather the product information by analysing the UII coding rules. Therefore, a privacy protection function needs to be included in a Mobile RFID system utilizing those tags.

This International Standard is intended to address consumer privacy-protection for Mobile RFID services. It focuses on technical solutions for protecting the privacy of Mobile RFID consumers. Its scope is limited to consumer privacy-protection suitable for tags and interrogators conforming to ISO/IEC 18000-6 Type C and ISO/IEC 18000-3 MODE 3 RFID interfaces. Cases for other ISO/IEC 18000-X protocols are not included. In addition, this International Standard will be coordinated with ISO/IEC 29167-X without conflict.

Consumer privacy-protection issues may be a critical barrier to deploying Mobile RFID services in a commercial field. Unless the Mobile RFID system is properly designed in aspects of privacy protection, there may be unexpected effects for Mobile RFID consumers. This International Standard is not required for tags attached to some items. But, it is useful for providing a technique for protecting the consumer's information if the tags are attached to private possessions such as purchased jewels and medicines.

Information technology — Mobile item identification and management — Consumer privacy-protection protocol for Mobile RFID services

1 Scope

This International Standard specifies a consumer privacy-protection protocol for Mobile RFID services. It provides a technical solution for addressing privacy concerns with tagged items for consumers.

This International Standard focuses on tag-to-interrogator communications for providing a consumer privacy-protection solution. Interrogator-to-host and host (back-end enterprise) system security issues are not within the scope of this International Standard, but are covered by a variety of other best-practice documents.

2 Conformance

This International Standard is intended for use in conjunction with the other standards related to Mobile RFID services. It can be applied to tags and interrogators conforming to ISO/IEC 18000-6 Type C and ISO/IEC 18000-3 MODE 3 RFID air interfaces and can, wherever appropriate and practicable, also be applied to tags and interrogators other than those covered by ISO/IEC 18000-6 Type C and ISO/IEC 18000-3 MODE 3 RFID air interfaces.

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 18000-3, *Information technology — Radio frequency identification for item management — Part 3: Parameters for air interface communications at 13,56 MHz*

ISO/IEC 18000-6, *Information technology — Radio frequency identification for item management — Part 6: Parameters for air interface communications at 860 MHz to 960 MHz*

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

ISO/IEC 29172, *Information technology — Mobile item identification and management — Reference architecture for Mobile AIDC services*

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762 (all parts), ISO/IEC 18000-6, ISO/IEC 29172, and the following apply.

4.1
cover-coding
method by which an Interrogator obscures information that it is transmitting to a tag by requesting a random number from the tag, then performing a bit-wise EXOR of the data or password with the received random number, and, finally, transmitting the cover-coded (also called ciphertext) string to the tag, which uncovers the data or password by performing a bit-wise EXOR of the received cover-coded string with the original random number

[ISO/IEC 18000-6]

NOTE To cover-code an EMII (Encoded Mobile Item Identification), an interrogator performs a bit-wise XOR of the EMII with input information, and the interrogator uncovers the EMII by performing the bit-wise XOR of the cover-coded EMII with the same input information.

4.2
Mobile RFID terminal
electronic device equipped with one or more Mobile RFID interrogator(s) to support the functions of Mobile Item Identification and Management (MIIM) technologies

5 Background

5.1 Reference model for consumer privacy-protection

This International Standard considers consumer's actions such as the purchase of some tagged items as the reference model. Figure 1 illustrates an example of reading the information from a consumer's low-cost tag. In this reference model using ISO/IEC 18000-6 Type C or ISO/IEC 18000-3 MODE 3 tags, UII memory, TID memory, and User memory are easily disclosed to Mobile RFID terminals conforming to this International Standard. Note that the TID remain unchanged.

Consumer privacy problems caused by this disclosed memory data are analysed as follows in ITU-T X.1171 (Refer to the chapter 9 of ITU-T X.1171 for more detail):

1) leakage of information associated with the identifier;

2) leakage of the historical context data.

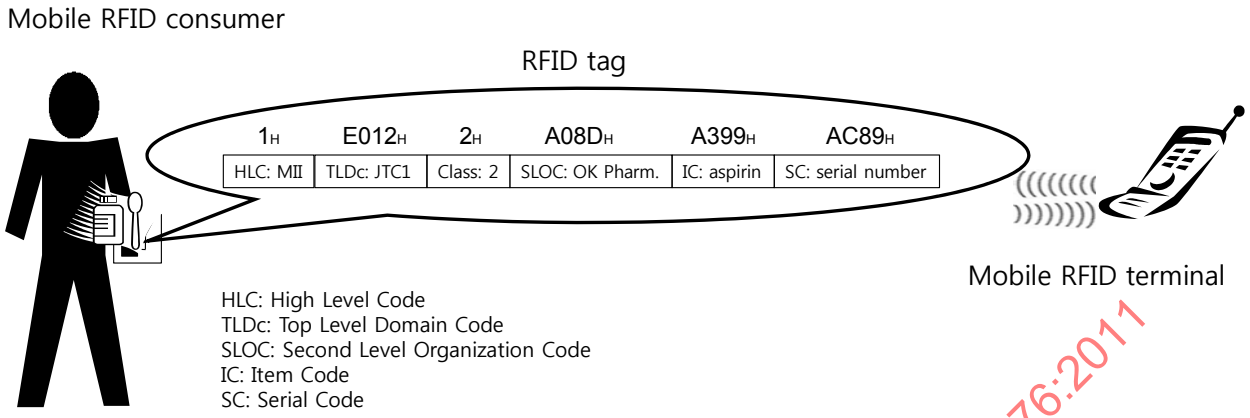

Figure 1 — Reference model for consumer privacy-protection

5.2 Prerequisites

The following conditions are prerequisites for defining the consumer privacy-protection protocol of this International Standard.

1) The tag shall support the *Access* command of ISO/IEC 18000-6 Type C and ISO/IEC 18000-3 MODE 3.

   - If a tag is not able to support the *Access* command, the tag shall not be used to execute the consumer privacy-protection protocol of this International Standard.

2) The tag shall support a nonzero-valued access password.

   - If a tag is not able to support a nonzero-valued access password, the tag shall not be used to execute the consumer privacy-protection protocol of this International Standard.

3) The consumer privacy-protection protocol does not preclude other methods of securing an RFID tag.

6 Consumer privacy-protection protocol

6.1 Goal

The goal of the consumer privacy-protection protocol is to conceal the original EMII (Encoded Mobile Item Identifier). The consumer privacy-protection protocol consists of five phases: 1) transition to a **secured** state, 2) acquisition of the original access password, 3) generation of the consumer's access password and cover-coding the EMII, 4) updating the memory banks, and 5) locking the memory banks.

6.2 Phase 1. Transition to secured state

The first phase is related to an action immediately after purchasing a tagged item. The purpose of this phase is to transit the tag to the **secured** state. This International Standard considers two cases regarding the access password of the tag. The first is an all zero-values access password at purchase and the other is a nonzero-valued access password at purchase.

In the case of the all zero-valued access password, the tag in the **acknowledged** state can transition to the **secured** state after receiving a valid *Req_RN* command. Therefore, the consumer's Mobile RFID terminal can write a new access password on the Access Passwd field of the Reserved memory bank of the tag (Refer to

9.3.2.1 Tag memory of ISO/IEC 18000-6:2010). In this case, the second phase, acquisition of the original access password, may be skipped because the all zero-valued access password is the default value of this International Standard.

In the case of the nonzero-valued access password, the tag shall use the *Access* command with a valid access password in order to transition to the **secured** state. Therefore, the consumer's Mobile RFID terminal shall go to the next phase to acquire the original access password.

6.3 Phase 2. Acquisition of the original access password

The second phase is to acquire the original access password of the tag. The transfer mechanism of the access password from a host computer or a key management server is out of the scope of this International Standard.

This International Standard presumes that the access password of the tag is securely transferred to the consumer's Mobile RFID terminal.

6.4 Phase 3. Generation of the consumer's access password and cover-coding the EMII

In the third phase, the consumer's Mobile RFID terminal generates its own access password and cover-codes the EMII. This International Standard provides for three generation methods of the access password.

One of the methods is to use the Mobile RFID terminal number and the mobile device identifier of the terminal. The typical Mobile RFID terminal number is the ITU-T E.164 telephone number and the typical mobile device identifiers are ESN (Electronic Serial Number), MEID (Mobile Equipment Identifier), and IMEI (International Mobile Equipment Identity). In the case of a 2G CDMA mobile phone, a telephone number of 01012345678 can be an example of the terminal number and an ESN of B0000000 can be an example of the mobile device identifier.

Figure 2 shows the generation method of the consumer's access password. The main feature of this method is that the access password is automatically derived without the consumer's intervention. The Mobile RFID start program performs the SHA1 (Secure Hash Algorithm 1) and selects the MSB (Most Significant Bits) 32 bits as the access password. The Mobile RFID start program is a special application that an end-user of the terminal meets initially when using Mobile RFID services. When an end-user presses a dedicated button or selects a menu icon, the Mobile RFID start program is executed.

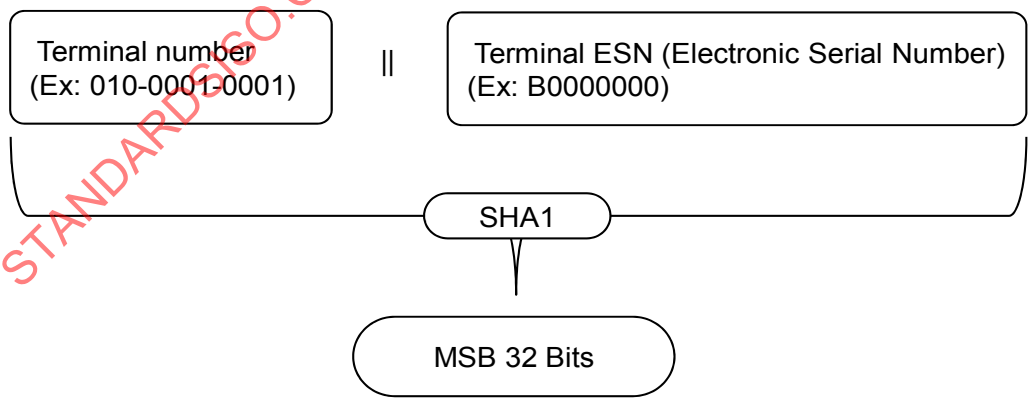

Figure 2 — Generation of the access password without consumer's intervention

The second method uses input information from the consumer, as well as the Mobile RFID terminal number and the mobile device identifier of the terminal. Figure 3 shows the access password generation method using consumer information. The main feature of this method is that the access password is differently derived

according to the consumer's input. For example, if the Mobile RFID terminal number is 01000010001, the ESN of the terminal is B0000000, and the consumer's input from the keypad of the terminal is 1234, the Mobile RFID start program performs the SHA1 after concatenating these values and selects the MSB 32 bits as the access password. This method has the advantage that the consumer can also manage product information by category. That is, if the consumer assigns the number “1000” to medical products and the number “2000” clothing, those numbers can play the role of a group index.

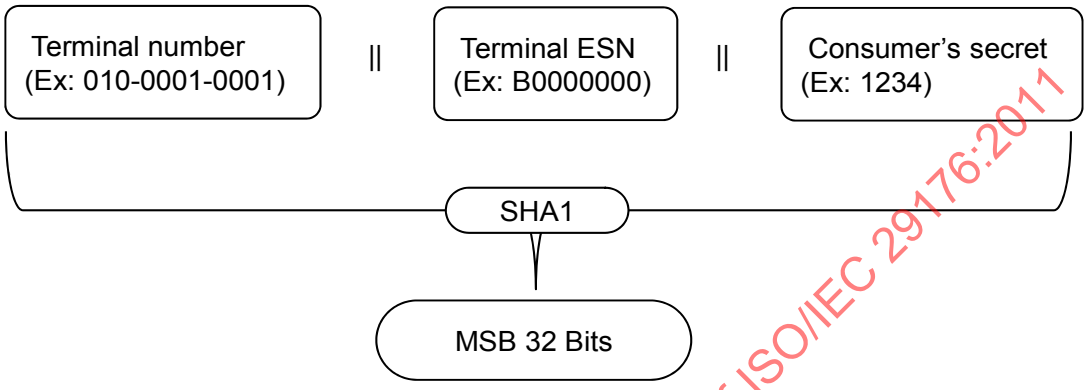

Figure 3 — Generation of the access password using consumer input and terminal information

The last method uses only consumer input information. Figure 4 shows the access password generation method using only consumer input. The main feature of this method is that the consumer can read the EMII of the tag attached to the purchased item using other Mobile RFID terminals. Since the above two methods use the specific terminal information, only the consumer's Mobile RFID terminal can regenerate the access password. On the other hand, in this method, other Mobile RFID terminals can regenerate the access password if provided the consumer input.

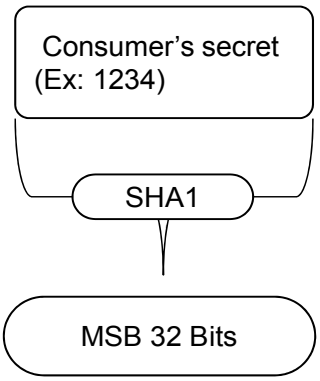

Figure 4 — Generation of the access password using only consumer input

Using the generated SHA1 output, the EMII is cover-coded. The default cover-coding algorithm is the bit-wise XOR (eXclusive OR). The EMII shall be cover-coded with MSBs of the SHA1 output. The size of the used MSBs is the same length as the EMII. If the length of the EMII is larger than 160 which is the size of the SHA1 output, the MSBs enough for cover-coding the EMII are used repeatedly. In addition, the CRC-16 (Cyclic Redundancy Check) shall be computed over the PC (Protocol Control) word and the new EMII.

6.5 Phase 4. Updating memory banks

The fourth phase is the tag memory update. Objects of this phase are the UII field of the UII memory bank and the Access Passwd field of the Reserved memory bank.

In general, the identification of the tagged item can be disclosed by the EMII. Therefore, it is necessary to update the EMII after the consumer purchases the tagged item.

The EMII can be updated with the new EMII which is the cover-coded value of the original EMII. In addition, the CRC-16 field of the UII memory bank can be updated with a new CRC-16.

In addition, the access password is updated with the new access password generated in phase 3.

These update operations are performed in the **secured** state and by using the *Write* command or the *BlockWrite* command.

6.6 Phase 5. Locking memory banks

The fifth phase is to lock tag memory banks. Objects for locking are the UII memory bank and the Access Passwd field of the Reserved memory bank.

After phase 4, the tag remains in the **secured** state and has the cover-coded EMII and the updated access password. Therefore, it is necessary to lock the related memory banks so other interrogators cannot update the memory.

The locking operations are performed by using the *Lock* command. Table 1 shows the payload format of the *Lock* command and the mandatory value for Mask bits and Action bits. (Refer to **9.3.2.11.3.5 Lock** of ISO/IEC 18000-6:2010).

Table 1 — Lock payload and usage in the phase 4

		Masks and associated action fields									
		Kill pwd		Access pwd		UII memory		TID memory		User memory	
Mask	Bit	19	18	17	16	15	14	13	12	11	10
	Meaning	skip/ write	skip/ write	skip/ write	skip/ write	skip/ write	skip/ write	skip/ write	skip/ write	skip/ write	skip/ write
	Value	x	x	1	x	1	x	x	x	x	x
Action	Bit	9	8	7	6	5	4	3	2	1	0
	Meaning	pwd read/ write	pwd read/ write	pwd read/ write	pwd read/ write	pwd read/ write	pwd read/ write	pwd read/ write	pwd read/ write	pwd read/ write	pwd read/ write
	Value	x	x	1	x	1	x	x	x	x	x

x: don't care

7 Operation scenarios

7.1 Valid consumer's Mobile RFID terminal

This International Standard can be applied to any tag conforming to ISO/IEC 18000-6 Type C and ISO/IEC 18000-3 MODE 3. Therefore, the consumer's Mobile RFID terminal should play an important role in protecting consumer-privacy.

The following scenario is related to behaviors of the valid consumer's Mobile RFID terminal conforming to this International Standard at the time of purchase.

1) (Consumer) Purchases tagged items

2) (Mobile RFID terminal) Inventories tags and transitions tags to **secured** state

   - If the access password of a tag is the all zero-valued access password, the tag transitions to the **secured** state without an additional key acquisition action.

   - If the access password of a tag is the nonzero-valued access password, the tag transitions to the **secured** state using the *Access* command after acquisition of the valid access password.

3) (Mobile RFID terminal) Generates the consumer's access password

   - If the consumer input is used, a Mobile RFID start program will provide the interface to receive the input.

4) (Mobile RFID terminal) Cover-codes the EMII

   - The EMII is cover-coded with MSBs of the SHA1 output generated in the previous phase.

   - The CRC-16 is computed over the PC word and the cover-coded EMII.

5) (Mobile RFID terminal) Updates memory banks

   - The UII field of the UII memory bank is updated with the new EMII which is a cover-coded value of the original EMII.

   - The CRC-16 field of the UII memory bank is updated with the new CRC-16 which is computed in the previous phase.

   - The Access Passwd field of the Reserved memory bank is updated with the consumer's access password.

6) (Mobile RFID terminal) Locks the updated memory banks

   - The pwd-write field for the UII memory bank is set to 1.

   - The pwd-read/write field for the Access Passwd field of the Reserved memory bank is set to 1.

After possession of the tagged items, the consumer performs the following procedure to use the Mobile RFID service.

1) (Mobile RFID terminal) Takes an inventory of the tags attached to the consumer's possessions

   - If the information from the consumer's Mobile RFID terminal is used, only that terminal can uncover the cover-coded EMII.

- If the consumer input is used, a Mobile RFID start program will provide the interface to receive the input.

2) (Mobile RFID terminal) Uncovers the cover-coded EMII

- The consumer's tags respond to the *ACK* command with the cover-coded EMII which is a different value from the original EMII. The cover-coded EMII can be uncovered by the only consumer's Mobile RFID terminal. Figure 6 shows an example of the consumer's tag inventory procedure.

3) (Consumer) Enjoys a Mobile RFID service using the EMII after uncovering.

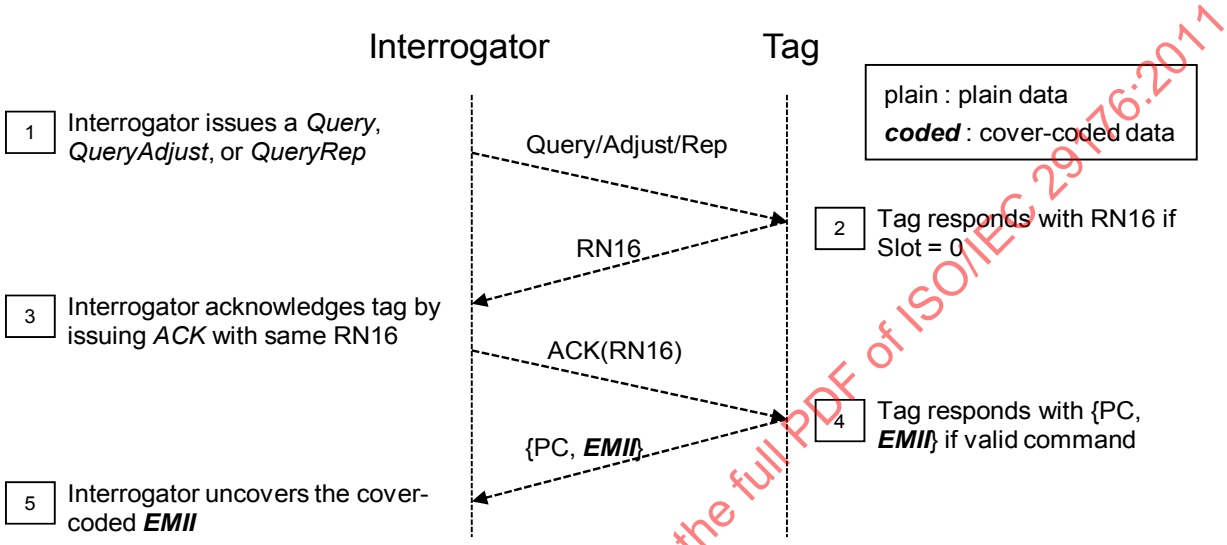

Figure 5 — Consumer's tag inventory

7.2 Invalid consumer's Mobile RFID terminal

In the case of a procedure between an invalid consumer's Mobile RFID terminal which does not know the access password and a tag which is updated with a cover-coded EMII, the Mobile RFID terminal identifies the cover-coded EMII as the original EMII. Therefore, a person who is not able to generate the correct access password cannot infer the item information from the identified EMII.