INTERNATIONAL STANDARD

ISO/IEC 18000-63

Second edition
2015-10-15

Information technology — Radio frequency identification for item management —

Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C

Technologies de l'information — Identification par radiofréquence (RFID) pour la gestion d'objets —

Partie 63: Paramètres de communications d'une interface radio entre 860 MHz et 960 MHz, Type C

Reference number
ISO/IEC 18000-63:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Conformance **1**
2.1 Claiming conformance 1
2.2 General conformance requirements 2
2.2.1 Interrogators 2
2.2.2 Tags 2
2.3 Command structure and extensibility 3
2.3.1 Mandatory commands 3
2.3.2 Optional commands 3
2.3.3 Proprietary commands 3
2.3.4 Custom commands 3
2.4 Reserved for Future Use (RFU) 3
2.5 Cryptographic Suite Indicators 3

3 Normative references **4**

4 Terms and definitions **4**

5 Symbols, abbreviated terms and notation **11**
5.1 Symbols 12
5.2 Abbreviated terms 13
5.3 Notation 16

6 Protocol requirements - Type C **16**
6.1 Protocol overview 16
6.1.1 Physical layer 16
6.1.2 Tag-identification layer 17
6.2 Protocol parameters 17
6.2.1 Signaling – Physical and media access control parameters 17
6.2.2 Logical – Operating procedure parameters 20
6.3 Description of operating procedure 21
6.3.1 Physical interface 21
6.3.2 Logical interface 43

7 Battery Assisted Passive (BAP) Interrogator Talks First Type C systems (optional) **117**
7.1 Applicability 117
7.2 General overview, definitions, and requirements of BAP 117
7.3 Battery Assisted Passive inventoried flag and state machine behaviour modifications 119
7.3.1 Modification to ready state and power-down support for BAP Tags 119
7.3.2 Signal loss tolerance via timer (mandatory) 119
7.3.3 Modified persistence of BAP PIE inventory flags (optional) 122
7.4 Battery Assisted Passive PIE (optional) 124
7.4.1 Flex_Query command (optional) 124
7.4.2 BAP PIE detailed operation including optional Battery Saver Mode 126
7.5 Manchester mode Battery Assisted operation protocol extensions 132
7.5.1 Introduction 132
7.5.2 Physical layer 133
7.5.3 Manchester Activation 138
7.5.4 Commands summary 153
7.6 Extended Protocol Control 167

8 Sensor support **168**
8.1 Applicability 168
8.2 Overview 168
8.3 Real Time Clock (RTC) 169

8.3.1 General ... 169
8.3.2 Setting the RTC ... 169
8.3.3 BroadcastSync command (optional) ... 170
8.3.4 Time synchronisation ... 170
8.4 HandleSensor command (optional) ... 171
8.5 Simple Sensor ... 172
8.5.1 Type C and Simple Sensor ... 173
8.6 Sensor Directory System and Full Function Sensors ... 175
8.6.1 Sensor Access – General Approach ... 175
Annex A (normative) **Extensible bit vectors (EBV)** ... **181**
Annex B (normative) **State-transition tables** ... **182**
Annex C (normative) **Command-Response Tables** ... **233**
Annex D (informative) **Example slot-count (*Q*) selection algorithm** ... **261**
Annex E (informative) **Example Tag inventory and access** ... **262**
Annex F (informative) **Calculation of 5-bit and 16-bit cyclic redundancy checks** ... **263**
Annex G (normative) **Multiple- and dense-Interrogator channelized signaling** ... **265**
Annex H (informative) **Interrogator-to-Tag link modulation** ... **268**
Annex I (normative) **Error codes** ... **270**
Annex J (normative) **Slot counter** ... **272**
Annex K (informative) **Example data-flow exchange** ... **273**
Annex L (informative) **Optional Tag Features** ... **276**
Annex M (informative) **Cryptographic-Suite Checklist** ... **279**
Annex N (informative) **Battery Assisted Tag to Interrogator synchronization** ... **280**
Annex O (normative) **Simple Sensors Data Block** ... **283**
Annex P (normative) **Record structures and commands for Ported Simple Sensors** ... **295**
Annex Q (informative) **BAP PIE and Manchester mode tutorial guide** ... **310**
Annex R (informative) **Manchester mode RF power control** ... **320**
Bibliography ... **325**

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 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 18000-63:2013), which has been technically revised.

ISO/IEC 18000 consists of the following parts, under the general title *Information technology — Radio frequency identification for item management*:

— *Part 1: Reference architecture and definition of parameters to be standardized*

— *Part 2: Parameters for air interface communications below 135 kHz*

— *Part 3: Parameters for air interface communications at 13,56 MHz*

— *Part 4: Parameters for air interface communications at 2,45 GHz*

— *Part 6: Parameters for air interface communications at 860 MHz to 960 MHz General*

— *Part 61: Parameters for air interface communications at 860 MHz to 960 MHz Type A*

— *Part 62: Parameters for air interface communications at 860 MHz to 960 MHz Type B*

— *Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C*

— *Part 64: Parameters for air interface communications at 860 MHz to 960 MHz Type D*

— *Part 7: Parameters for active air interface communications at 433 MHz*

Introduction

This part of ISO/IEC 18000 defines the physical and logical requirements for a passive-backscatter, Interrogator-talks-first (ITF), radio-frequency identification (RFID) system operating in the 860 MHz – 960 MHz frequency range. The system comprises Interrogators, also known as Readers, and Tags, also known as Labels or Transponders.

An Interrogator transmits information to a Tag by modulating an RF signal in the 860 MHz – 960 MHz frequency range. The Tag receives both information and operating energy from this RF signal. Tags are passive, meaning that they receive all of their operating energy from the Interrogator's RF signal.

An Interrogator receives information from a Tag by transmitting a continuous-wave (CW) RF signal to the Tag; the Tag responds by modulating the reflection coefficient of its antenna, thereby backscattering an information signal to the Interrogator. The system is ITF, meaning that a Tag modulates its antenna reflection coefficient with an information signal only after being directed to do so by an Interrogator.

Interrogators and Tags are not required to talk simultaneously; rather, communications are half-duplex, meaning that Interrogators talk and Tags listen, or vice versa.

The described backscatter radio frequency identification (RFID) system that supports the following system capabilities:

— identification and communication with multiple tags in the field;

— selection of a subgroup of tags for identification or with which to communicate;

— reading from and writing to or rewriting data many times to individual tags;

— user-controlled permanently lockable memory;

— data integrity protection;

— Interrogator-to-tag communications link with error detection;

— tag-to-Interrogator communications link with error detection;

— support for both passive back-scatter tags with or without batteries.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning radio frequency identification technology.

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent rights have assured ISO and IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with ISO and IEC.

Information on the declared patents may be obtained from:

Contact details
Patent Holder: Legal Name Atmel Automotive GmbH **Contact for license application:** Name & Department Leo Merken, Legal Department, ATMEL Corporation Address 2325 Orchard Parkway Address San Jose, CA 95131 USA Tel. +1 408 436 4251 Fax +1 408 487 2615 E-mail leo.merken@atmel.com URL (optional)
Patent Holder: Legal Name CISC Semiconductor Design+Consulting GmbH **Contact for license application:** Name & Department Markus Pistauer, CEO Address Lakeside B07 Address 9020 Klagenfurt, Austria Tel. +43(463) 508 808 Fax +43(463) 508 808-18 E-mail m.pistauer@cisc.at URL (optional) www.cisc.at
Patent holder: ETRI (Electronics Telecommunication Reseach Institute) **Contact for license application:** Name & Department: Min-Sheo Choi, Intellectual Property Management Team Address: 138 Gajeongno, Yuseong-gu Address: Daejeon, 305-700, Korea Tel. +82-42-860-0756 Fax +82-42-860-3831 E-mail choims@etri.re.kr URL (optional) www.etri.re.kr

Contact details
Patent Holder: Legal Name Impinj, Inc. **Contact for license application:** Name & Department Chris Diorio, CTO Address 701 N. 34th Street, Suite 300 Address Seattle, WA 98103, USA Tel. +1.206 834 1115 Fax +1.206 517.5262 E-mail diorio@impinj.com URL (optional) www.impinj.com
Patent Holder: Legal Name: Magellan Technology Pty. Limited **Contact for license application:** Name & Department: Ms Jean Angus Address: 65 Johnston St Address: Annandale, NSW 2038, Australia Tel. +61 2 9562 9800 Fax +61 2 9518 7620 E-mail: license@magellan-technology.com URL (optional): www.magellan-technology.com
Patent Holder: Legal Name NXP B.V. **Contact for license application:** Name & Department Aaron Waxler – IP Licensing & Claims Address 411 East Plumeria, Address San Jose, CA 95134-1924, USA Tel. +1 914 860-4296 Fax E-mail Aaron.Waxler@nxp.com URL (optional)

Contact details
Patent Holder: Legal Name SATO VICINITY Pty. Limited **Contact for license application:** Name & Department Mr. Hiromasa Konishi, Managing Director Address 8 Guihen Street, Annandale, NSW 2038, Australia Address Tel. +61 295 629 800 Fax +61 295 187 620 E-mail hiromasa.konishi@sato-glo bal . com URL (optional) www.satovicinity.com
Patent Holder: Legal Name TAGSYS SAS **Contact for license application:** Name & Department Mr. Alain Fanet President Address 785 Voie Antiope, TI Athélia 3 Address F-13600 La Ciotat Tel. +33 332188900 Fax +33 332188900 E-mail alain.fanet@tagsysrfid.com URL (optional) www.tagsysrfid.com
Patent Holder: Legal Name Univertsity of Pittsburgh - Of the Commonwealth of Pennsylvania **Contact for license application:** Name & Department Marc S. Malandro, PhD, CLP, RTIP Address University of Pittsburgh, 200 Gardner Steel Conference Center Address Thackeray & O'Hara Streets, Pittsburgh, PA 15260 Tel. 412-624-8787 Fax 412-648-2259 E-mail mmalandro@innovation.pitt.edu URL (optional)

Contact details	
Patent Holder:	
Legal Name	Zebra Technologies Corporation
Contact for license application:	
Name & Department	Glenn Frankenberger, Sr. IP Counsel, Legal Department
Address	One Motorola Plaza
Address	Holtsville, NY 11742
Tel.	631-738-5570
Fax	631-738-4110
E-mail	glenn.frankenberger@zebra.com
URL (optional)	

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

The latest information on IP that may be applicable to this part of ISO/IEC 18000 can be found at www.iso.org/patents

Information technology — Radio frequency identification for item management —

Part 63:
Parameters for air interface communications at 860 MHz to 960 MHz Type C

1 Scope

This part of ISO/IEC 18000 defines the air interface for radio frequency identification (RFID) devices operating in the 860 MHz to 960 MHz Industrial, Scientific, and Medical (ISM) band used in item management applications. It provides a common technical specification for RFID devices that can be used by ISO committees developing RFID application standards. This part of ISO/IEC 18000 is intended to allow for compatibility and to encourage inter-operability of products for the growing RFID market in the international marketplace. It defines the forward and return link parameters for technical attributes including, but not limited to, operating frequency, operating channel accuracy, occupied channel bandwidth, maximum effective isotropic radiated power (EIRP), spurious emissions, modulation, duty cycle, data coding, bit rate, bit rate accuracy, bit transmission order, and, where appropriate, operating channels, frequency hop rate, hop sequence, spreading sequence, and chip rate. It further defines the communications protocol used in the air interface.

This part of ISO/IEC 18000 specifies the physical and logical requirements for a passive-backscatter, Interrogator-Talks-First (ITF) systems. The system comprises Interrogators, also known as readers, and tags, also known as labels. An Interrogator receives information from a tag by transmitting a continuous-wave (CW) RF signal to the tag; the tag responds by modulating the reflection coefficient of its antenna, thereby backscattering an information signal to the Interrogator. The system is ITF, meaning that a tag modulates its antenna reflection coefficient with an information signal only after being directed to do so by an Interrogator.

In detail, this part of ISO/IEC 18000 contains Type C.

Type C uses PIE in the forward link and a random slotted collision-arbitration algorithm.

This part of ISO/IEC 18000 specifies

— physical interactions (the signalling layer of the communication link) between Interrogators and tags,

— logical operating procedures and commands between Interrogators and Tags.

— the collision arbitration scheme used to identify a specific tag in a multiple-tag environment.

— optional security commands that allow the use of crypto suites of ISO/IEC 29167.

2 Conformance

2.1 Claiming conformance

A device shall not claim conformance with this protocol unless the device complies with

— all clauses in this protocol (except those marked as optional), and

— the conformance document associated with this protocol, and,

— all local radio regulations.

Relevant conformance test methods are provided in ISO/IEC 18047-6.

Conformance can also require a license from the owner of any intellectual property utilized by said device.

2.2 General conformance requirements

2.2.1 Interrogators

To conform to this part of ISO/IEC 18000, an Interrogator shall:

— Meet the requirements of this part of ISO/IEC 18000,

— Implement the mandatory commands defined in this part of ISO/IEC 18000,

— Modulate/transmit and receive/demodulate a sufficient set of the electrical signals defined in the signaling layer of this protocol to communicate with conformant Tags, and

— Conform to the applicable local radio regulations.

To conform to this part of ISO/IEC 18000, an Interrogator may:

— Implement any subset of the optional commands defined in this part of ISO/IEC 18000, and

— Implement any proprietary and/or custom commands in conformance with this part of ISO/IEC 18000.

To conform to this part of ISO/IEC 18000, an Interrogator shall not:

— implement any command that conflicts with this part of ISO/IEC 18000 or any of the parts 61, 62 and 64, or

— Require using an optional, proprietary, or custom command to meet the requirements of this protocol.

2.2.2 Tags

To conform to this part of ISO/IEC 18000, a Tag shall:

— Meet the requirements of this part of ISO/IEC 18000,

— Implement the mandatory commands defined in this part of ISO/IEC 18000,

— Modulate a backscatter signal only after receiving the requisite command from an Interrogator, and

— Conform to local radio regulations.

To conform to this protocol, a Tag may:

— Implement any subset of the optional commands defined in this part of ISO/IEC 18000, and

— Implement any proprietary and/or custom commands as defined in 2.3.3 and 2.3.4, respectively.

To conform to this part of ISO/IEC 18000, a Tag shall not:

— Implement any command that conflicts with this part of ISO/IEC 18000 or any of the parts 61, 62 and 64,

— Require using an optional, proprietary, or custom command to meet the requirements of this protocol, or

— Modulate a backscatter signal unless commanded to do so by an Interrogator using the signaling layer defined in this part of ISO/IEC 18000.

2.3 Command structure and extensibility

This part of ISO/IEC 18000 allows four command types: (1) mandatory, (2) optional, (3) proprietary, and (4) custom. Subclause 6.3.2.12 and Table 6.28 define the structure of the command codes used by Interrogators and Tags for each of the four types, as well as the availability of future extensions. All commands defined by this protocol are either mandatory or optional. Proprietary or custom commands are manufacturer-defined.

2.3.1 Mandatory commands

Conforming Tags shall support all mandatory commands. Conforming Interrogators shall support all mandatory commands.

2.3.2 Optional commands

Conforming Tags may or may not support optional commands. Conforming Interrogators may or may not support optional commands. If a Tag or an Interrogator implements an optional command then it shall implement it in the manner specified in this protocol.

2.3.3 Proprietary commands

Proprietary commands may be enabled in conformance with this protocol, but are not specified herein. All proprietary commands shall be capable of being permanently disabled. Proprietary commands are intended for manufacturing purposes and shall not be used in field-deployed RFID systems.

2.3.4 Custom commands

Custom commands may be enabled in conformance with this protocol, but are not specified herein. An Interrogator shall issue a custom command only after (1) singulating a Tag, and (2) reading (or having prior knowledge of) the Tag manufacturer's identification in the Tag's TID memory. An Interrogator shall use a custom command only in accordance with the specifications of the Tag manufacturer identified in the TID. A custom command shall not solely duplicate the functionality of any mandatory or optional command defined in this protocol by a different method.

2.4 Reserved for Future Use (RFU)

This part of ISO/IEC 18000 denotes some Tag memory addresses, Interrogator command codes, and bit fields within Interrogator commands as RFU.

RFU values are reserved for future extensibility. Third parties, including but not limited to solution providers and end users, shall not use these RFU values for proprietary purposes.

2.5 Cryptographic Suite Indicators

A Tag may support one or more cryptographic suites. The *Challenge* and *Authenticate* commands include a CSI field that specifies a single cryptographic suite. CSI is an 8-bit field with bit values defined below.

- Four most-significant bits: Cryptographic suite assigning authority, as follows:
  - 0000_2 – 0011_2: ISO/IEC 29167
  - 0100_2 – 1100_2: RFU
  - 1101_2: Tag manufacturer
  - 1110_2: GS1
  - 1111_2: RFU
- Four least-significant bits: One of 16 cryptographic suites that the assigning authority may assign.

Example: CSI=00000000_2 is the first and CSI=00000001_2 is the second suite that ISO/IEC 29167 may assign.

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 7816-6, *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange*

ISO/IEC 15961, *Information technology — Radio frequency identification (RFID) for item management — Data protocol: application interface*

ISO/IEC 15962, *Information technology — Radio frequency identification (RFID) for item management — Data protocol: data encoding rules and logical memory functions*

ISO/IEC 15963, *Information technology — Radio frequency identification for item management — Unique identification for RF tags*

ISO/IEC 18000-1, *Information technology — Radio frequency identification for item management — Part 1: Reference architecture and definition of parameters to be standardized*

ISO/IEC 18047-6:2012, *Information technology — Radio frequency identification device conformance test methods — Part 6: Test methods 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 29167-1: *Information technology — Automatic identification and data capture techniques — Part 1: Security services for RFID air interfaces*

GS1 EPCglobal™: *GS1 EPC™ Tag Data Standard*

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762 (all parts) and the following apply. Terms and definitions specific to this part of ISO/IEC 18000 that supersede any normative references are as follows:

4.1
air interface
complete communication link between an Interrogator and a Tag including the physical layer, collision-arbitration algorithm, command and response structure, and data-coding methodology

4.2
activation
waking up a tag from the **hibernate** state

4.3
asymmetric key pair
private key and its corresponding public key, used in conjunction with an asymmetric cryptographic suite

4.4
authentication
process of determining whether an entity or data is/are who or what, respectively, it claims to be.

Note 1 to entry: The types of entity authentication referred-to in this protocol are Tag authentication, Interrogator authentication, and Tag-Interrogator mutual authentication. For data authentication see authenticated communications.

4.5
authenticated communication
communication in which message integrity is protected

4.6
battery assistance
battery support for radio frequency communication

4.7
battery assisted mode
working mode of battery assisted tags with non-empty battery

4.8
battery saver mode
battery saving functionality based on low power threshold detection with optional duty cycling

4.9
collision arbitration loop
algorithm used to prepare for and handle a dialogue between an Interrogator and a tag

Note 1 to entry: This is also known as collision arbitration.

4.10
command set
set of commands used to inventory and interact with a Tag population

4.11
continuous wave
typically a sinusoid at a given frequency, but more generally any Interrogator waveform suitable for powering a passive Tag without amplitude and/or phase modulation of sufficient magnitude to be interpreted by a Tag as transmitted data

4.12
cover coding
method by which an Interrogator obscures information that it is transmitting to a Tag.

Note 1 to entry: To cover-code data or a password, an Interrogator first requests a random number from the Tag. The Interrogator then performs a bit-wise EXOR of the data or password with this random number, and transmits the cover-coded string to the Tag. The Tag uncovers the data or password by performing a bit-wise EXOR of the received cover-coded string with the original random number.

4.13
crypto superuser
key with an asserted CryptoSuperuser privilege

4.14
data element
low-level, indivisible data construct.

Note 1 to entry: See *file* (4.20) and *record* (4.54).