International Standard

ISO/IEC 18000-63

# Information technology — Radio frequency identification for item management —

## Part 63: Parameters for air interface communications at 860 MHz to 930 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 930 MHz, Type C*

Fourth edition
2026-10

Reference number
ISO/IEC 18000-63:2026(en)

© ISO/IEC 2026



## COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved.

This ISO publication is protected by copyright and is owned by ISO and/or its licensors.

The content of this ISO publication is provided under licence, not sold. Use is subject to the applicable licence terms issued by ISO, an ISO member body, or an authorized third-party distributor.

Except as required for implementation or expressly permitted by a separate licence, no part of this ISO publication may be reproduced, distributed, modified, used, or made available in any form or by any means – electronic or mechanical, including photocopying, scanning, recording, or posting on internal or external digital platforms.

Any use beyond the scope of the granted rights is prohibited and may result in legal action.

ISO copyright office
CP 401 • CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

# Contents

Page

**Foreword** ..... **v**
**Introduction** ..... **vi**
**1 Scope** ..... **1**
**2 Normative references** ..... **1**
**3 Terms and definitions** ..... **2**
**4 Symbols, abbreviated terms and notations** ..... **6**
4.1 Symbols ..... 6
4.2 Abbreviated terms ..... 8
4.3 Notations ..... 9
**5 Conformance** ..... **10**
5.1 Claiming conformance ..... 10
5.2 General conformance requirements ..... 11
5.2.1 Interrogators ..... 11
5.2.2 Tags ..... 11
5.3 Command structure and extensibility ..... 12
5.3.1 General ..... 12
5.3.2 Mandatory commands ..... 12
5.3.3 Optional commands ..... 12
5.3.4 Proprietary commands ..... 12
5.3.5 Custom commands ..... 12
5.4 Reserved for Future Use (RFU) ..... 12
5.5 Cryptographic Suite Indicators ..... 13
**6 Protocol requirements** ..... **13**
6.1 Protocol overview ..... 13
6.1.1 Physical layer ..... 13
6.1.2 Tag-identification layer ..... 13
6.2 Protocol parameters ..... 14
6.2.1 Signaling — Physical and media access control parameters ..... 14
6.2.2 Logical — Operating procedure parameters ..... 16
6.3 Description of operating procedure ..... 17
6.3.1 Physical interface ..... 17
6.3.2 Logical interface ..... 43
**7 Battery assisted passive (BAP) Interrogator Talks First systems (optional)** ..... **139**
7.1 Applicability ..... 139
7.2 General overview, descriptions and requirements of BAP ..... 139
7.3 BAP inventoried flag and state machine behaviour modifications ..... 141
7.3.1 Modification to ready state and power-down support for BAP Tags ..... 141
7.3.2 Signal loss tolerance via timer (mandatory) ..... 142
7.3.3 Modified persistence of BAP PIE inventory flags (optional) ..... 144
7.4 BAP PIE (optional) ..... 146
7.4.1 Flex_Query command (optional) ..... 146
7.4.2 BAP PIE detailed operation including optional Battery Saver Mode ..... 150
7.5 Manchester mode battery assisted operation protocol extensions ..... 156
7.5.1 General ..... 156
7.5.2 Physical layer ..... 156
7.5.3 Manchester activation ..... 163
7.5.4 Commands summary ..... 177
**8 Sensor support (optional)** ..... **191**
8.1 Applicability ..... 191
8.2 Overview ..... 191
8.3 Real Time Clock ..... 193
8.3.1 General ..... 193

© ISO/IEC 2026 – All rights reserved

8.3.2 Setting the RTC ... 193
8.3.3 BroadcastSync command (optional) ... 193
8.3.4 Time synchronisation ... 194
8.4 HandleSensor command (optional) ... 195
8.5 Simple Sensors ... 196
8.5.1 General ... 196
8.5.2 Simple Sensor implementation ... 196
8.6 Full Function Sensors and Sensor Directory System ... 198
8.6.1 General ... 198
8.6.2 Sensor Access — General approach ... 198
8.7 Snapshot Sensors ... 203
8.7.1 General ... 203
8.7.2 Initiating Snapshot Sensor measurements ... 205
8.7.3 Reporting Snapshot Sensor Information ... 206

**Annex A** (normative) **Extensible bit vectors** ... **208**

**Annex B** (normative) **State-transition tables** ... **210**

**Annex C** (normative) **Command-response tables** ... **272**

**Annex D** (informative) **Example of a slot-count parameter, *Q*, selection algorithm** ... **300**

**Annex E** (informative) **Example of Tag inventory and access** ... **301**

**Annex F** (informative) **Calculation of 5-bit and 16-bit cyclic redundancy checks** ... **302**

**Annex G** (normative) **Multiple- and dense-Interrogator channelized signaling** ... **305**

**Annex H** (informative) **Interrogator-to-Tag link modulation — Baseband waveforms, modulated RF, and detected waveforms** ... **307**

**Annex I** (normative) **Tag error codes and their usage** ... **309**

**Annex J** (normative) **Slot counter operation** ... **310**

**Annex K** (informative) **Example data-flow exchange** ... **311**

**Annex L** (informative) **Optional Tag features** ... **314**

**Annex M** (informative) **Cryptographic suite checklist** ... **317**

**Annex N** (informative) **Battery assisted Tag to Interrogator synchronization** ... **318**

**Annex O** (normative) **Simple Sensors Data Block** ... **321**

**Annex P** (normative) **Record structures and commands for Ported Simple Sensors** ... **335**

**Annex Q** (informative) **BAP PIE and Manchester mode tutorial guide** ... **349**

**Annex R** (informative) **Manchester mode RF power control** ... **359**

**Annex S** (informative) **Additional information about RAIN** ... **364**

**Bibliography** ... **365**

© ISO/IEC 2026 – All rights reserved

# 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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

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

This fourth edition cancels and replaces the third edition (ISO/IEC 18000-63:2021), which has been technically revised.

The main changes are as follows:

— tag selection process has been improved;

— a method to ensure tags are sufficiently energized before selection and communication has been added;

— a method for tag data reading has been provided;

— QueryX and QueryY has been added to make the selection process more topics useful and robust;

— ReadVar and Read-User-Memory-bit (RUM) automate the access to item attributes and the Tag Identifier (TID);

— ResponseBuffer has been made optional.

A list of all parts in the ISO/IEC 18000 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2026 – All rights reserved

# Introduction

A radio frequency identification (RFID) system comprises:

— Interrogators, also known as radio identification (RAIN) Readers, and

— RAIN Tags, also known as RAIN Labels or RAIN Transponders.

This document is also referred as RAIN Air Interface. For more information on RAIN, see Annex S.

A RAIN Interrogator transmits information to a RAIN Tag by modulating an RF signal in the 860 MHz to 930 MHz frequency range. The Tag receives both information and operating energy from this RF signal. Tags are passive, which means that they receive all of their operating energy from the Interrogator's RF signal.

A RAIN Interrogator receives information from a RAIN 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 Interrogator-talks-first (ITF), which means 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, i.e. Interrogators talk and Tags listen, or vice versa.

The backscatter RFID system described in this document 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.

© ISO/IEC 2026 – All rights reserved

# Information technology — Radio frequency identification for item management —

# Part 63:
# Parameters for air interface communications at 860 MHz to 930 MHz Type C

## 1 Scope

This document establishes the air interface for radio frequency identification (RFID) devices operating in the 860 MHz to 930 MHz industrial, scientific and medical (ISM) band used in item management applications.

This document specifies a common technical specification for RFID devices that can be used to develop standards for applications using this radio identification (RAIN) air interface. This document is intended to improve compatibility and encourage inter-operability of products for the growing RFID market in the international marketplace.

This document establishes 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. This document further specifies the communications protocol used in the air interface.

This document describes the physical and logical requirements for a passive backscatter, Interrogator-talks-first (ITF), radio frequency identification system operating in the 860 MHz to 930 MHz frequency range.

This document 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 29167-1:2014 [1].

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 15961-1, *Information technology — Data protocol for radio frequency identification (RFID) for item management — Part 1: Application interface*

ISO/IEC 15961-2, *Information technology — Data protocol for radio frequency identification (RFID) for item management — Part 2: Registration of RFID data constructs*

ISO/IEC 15961-3, *Information technology — Data protocol for radio frequency identification (RFID) for item management — Part 3: RFID data constructs*

© ISO/IEC 2026 – All rights reserved

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

ISO/IEC 15963-1, *Information technology — Radio frequency identification for item management — Part 1: Unique identification for RF tags numbering systems*

ISO/IEC 18047-63, *Information technology — Radio frequency identification device conformance test methods — Part 63: Test methods for air interface communications at 860 MHz to 960 MHz*

ISO/IEC 19762:2025, *Information technology — Automatic identification and data capture (AIDC) techniques — Vocabulary*

ISO/IEC 29143, *Information technology — Automatic identification and data capture techniques — Air interface specification for Mobile RFID interrogators*

GS1 EPC Tag Data Standard (TDS), available at: https://www.gs1.org/standards/epc-rfid/tds

ISO/IEC 18000-61, *Information technology — Radio frequency identification for item management — Part 61: Parameters for air interface communications at 860 MHz to 960 MHz Type A*

ISO/IEC 18000-62, *Information technology — Radio frequency identification for item management — Part 62: Parameters for air interface communications at 860 MHz to 960 MHz Type B*

ISO/IEC 18000-64, *Information technology — Radio frequency identification for item management — Part 64: Parameters for air interface communications at 860 MHz to 960 MHz Type D*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762:2025 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

**3.1**
**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

**3.2**
**authenticated communication**
communication in which message integrity is protected

**3.3**
**backscatter link frequency**
frequency at which a Tag modulates the backscattered signal

**3.4**
**battery assisted mode**
working mode of battery assisted tags with non-empty battery

**3.5**
**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 bitwise exclusive OR (XOR) 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 bitwise XOR of the received cover-coded string with the original random number.

© ISO/IEC 2026 – All rights reserved

**3.6**
**Extended Tag identifier**
XTID
memory construct that defines a Tag's capabilities and which can include a Tag serial number

Note 1 to entry: More information on XTID is provided in Reference [2].

**3.7**
**extended temperature range**
temperature range that is from –40 °C to +65 °C

**3.8**
**file type**
8-bit string that specifies a file's designated type

**3.9**
**file superuser**
access password or key with a $0011_2$ **secured**-state file privilege value

**3.10**
**full-duplex communication**
communication channel that carries data in both directions at once

Note 1 to entry: See *half-duplex communications* (3.12) for another option for bidirectional communication.

**3.11**
**GS1 application**
application whose usage denotes an acceptance of GS1 EPCglobal® standards and policies

Note 1 to entry: Reference [3] contains more details on GS1 application.

Note 2 to entry: See *ISO application* (3.17) for an alternative application option.

**3.12**
**half-duplex communication**
communication channel that carries data in one direction at a time rather than in both directions at once

Note 1 to entry: See *full-duplex communications* (3.10) for another option for bidirectional communication.

**3.13**
**handle**
16-bit tag identifier

**3.14**
**hibernate**
state of energy saving when the device is not required to be used

**3.15**
**interrogator authentication**
means for a Tag to determine, via cryptographic means, that an Interrogator's identity is as claimed

**3.16**
**inventory round**
period initiated by a Query command or a QueryX command and terminated by either a subsequent Query command, a subsequent QueryX command, a Select command or a Challenge command

**3.17**
**ISO application**
application whose usage denotes an acceptance of ISO standards and policies

Note 1 to entry: See *GS1 application* (3.11) for an alternative application option.

© ISO/IEC 2026 – All rights reserved

**3.18**
**keyID**
numerical designator for a single key

**3.19**
**MAC**
**message authentication code**
code, computed over bits in a message, that an Interrogator or a Tag can use to verify the integrity of the message

**3.20**
**mutual authentication**
means for a Tag and an Interrogator to each determine, via cryptographic means, that the others' identity is as claimed

**3.21**
**nominal temperature range**
temperature range that is from –25 °C to +40 °C

Note 1 to entry: An *extended temperature range* (3.7) also exists.

**3.22**
**non-removable Tag**
Tag that a consumer cannot physically detach from an item without special equipment or without compromising the item's intended functionality

Note 1 to entry: In addition to a non-removeable tag, a *removable Tag* (3.25) also exists.

**3.23**
**password**
secret value sent by an Interrogator to a Tag to enable restricted Tag operations

Note 1 to entry: Passwords are not keys.

Note 2 to entry: The only passwords defined by the protocol defined in this document are the kill and access passwords.

**3.24**
***Q***
parameter that an Interrogator uses to regulate the probability of Tag response

Note 1 to entry: An Interrogator instructs Tags in an inventory round to load a $Q$-bit random (or pseudo-random) number into their slot counter; the Interrogator can also command Tags to decrement their slot counter. Tags reply when the value in their slot counter, i.e. their *slot* (3.30), is zero. $Q$ is an integer in the range (0 to 15); the corresponding Tag-response probabilities range from $2^0 = 1$ to $2^{-15} = 0{,}000031$.

**3.25**
**removable Tag**
Tag that a consumer can physically detach from an item without special equipment and without compromising the item's intended functionality

Note 1 to entry: In addition to a removable Tag, a *non-removable Tag* (3.22) also exists.

**3.26**
**secure communication**
communication in which message confidentiality is protected

**3.27**
**security**
degree of protection against threats identified in a *security policy*

Note 1 to entry: A system is secure if it is protected to the degree specified in the security policy.

© ISO/IEC 2026 – All rights reserved

**3.28**
**session key**
temporary key generated by one or both of Tag and Interrogator and typically used for both authenticated and secure communications

**3.29**
**Simple Sensor functionality**
functionality whereby a sensor provides a valid simple sensor data address and transmits simple sensor data subsequent to the UII as part of the reply to the *ACK* command

**3.30**
**slot**
point in an *inventory round* (3.16) at which a Tag can respond

Note 1 to entry: Slot is the value output by a Tag's slot counter; Tags reply when their slot (i.e. the value in their slot counter) is zero.

Note 2 to entry: See *Q* (3.24) for the for the maximum number of slots.

**3.31**
**snapshot sensor**
sensor that makes a measurement during power-up or on demand from an Interrogator

**3.32**
**Tag authentication**
means for an Interrogator to determine, via cryptographic means, that a Tag's identity is as claimed

**3.33**
**traceable**
not restricting the identifying information that a Tag exposes or the Tag's operating range, or both

Note 1 to entry: To view the definition of the opposite term, refer to *untraceable* (3.36).

**3.34**
**untraceable privilege**
privilege given to the access password or to a key that grants an Interrogator using the access password or key the right to access *untraceably hidden memory* (3.35) or to issue an *untraceable* (3.36) command, or both

**3.35**
**untraceably hidden memory**
memory that an untraceable Tag hides from Interrogators with a deasserted *untraceable privilege* (3.34)

**3.36**
**untraceable**
restricting the identifying information that a Tag exposes or the Tag's operating range, or both

Note 1 to entry: To view the definition of the opposite term, refer to *traceable* (3.33).

© ISO/IEC 2026 – All rights reserved