INTERNATIONAL STANDARD

ISO/IEC 18000-4

Fourth edition
2018-08

Information technology — Radio frequency identification for item management —

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

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

Partie 4: Paramètres de communications d'une interface d'air à 2,45 GHz

Reference number
ISO/IEC 18000-4:2018(E)

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

Published in Switzerland

Contents

Page

Foreword ... **vi**
Introduction ... **vii**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **2**
4 Symbols and abbreviated terms ... **4**
5 General items on 2,45 GHz RFID protocols that support this document ... **7**
5.1 Protocols ... 7
5.2 Frequency ... 7
5.2.1 General ... 7
5.2.2 Interface definitions ... 7
5.3 Tag identification number ... 8
5.4 Potential interference ... 8
6 MODE 1: Passive backscatter RFID system ... **8**
6.1 MODE 1: General ... 8
6.2 Physical layer and data coding ... 9
6.2.1 Interrogator power-up waveform ... 9
6.2.2 Interrogator power-down ... 10
6.2.3 Frequency hopping carrier rise and fall times ... 10
6.2.4 Forward link ... 11
6.2.5 FM0 return link ... 13
6.2.6 Cyclic redundancy check (CRC) ... 14
6.2.7 Protocol concept ... 15
6.2.8 Command format ... 16
6.2.9 Response format ... 17
6.2.10 WAIT ... 17
6.2.11 Communication sequences at packet level ... 18
6.3 Protocol and collision arbitration ... 19
6.3.1 Definition of data elements, bit and byte ordering ... 19
6.3.2 Tag memory organization ... 20
6.3.3 Block security status ... 20
6.3.4 Overall protocol description ... 20
6.3.5 Collision arbitration ... 25
6.3.6 Commands ... 26
6.3.7 Transmission errors ... 46
7 MODE 2: Long range high data rate RFID system ... **46**
7.1 MODE 2: General ... 46
7.2 Modulation and coding ... 46
7.2.1 Forward link (only for R/W-tag) ... 46
7.2.2 Return link for notification (for both types of the tag) ... 47
7.2.3 Return link for communication (only for R/W-tag) ... 47
7.3 General system description ... 48
7.4 Frame structure ... 49
7.4.1 Hierarchical structure ... 49
7.4.2 Logical channels ... 50
7.4.3 Physical channels ... 56
7.5 Channel coding and sequences ... 71
7.5.1 Synchronization and CRC patterns ... 71
7.6 Command set for the command slot channel: CS-CH (only for R/W-tag) ... 73
7.6.1 Command types ... 73
7.6.2 Command set ... 74
7.6.3 Command codes ... 75

8 MODE 3: Active RFID ITF network 76
8.1 General 76
8.2 Operational requirements 77
8.3 Network Physical Layer description 77
8.4 Network description 78
8.4.1 General 78
8.4.2 Network topology 78
8.5 Star topology 80
8.5.1 General 80
8.5.2 Star topology data flow 81
8.6 Trunk topology 81
8.6.1 Trunk coordinator requirements 81
8.6.2 Data flow in a trunk topology 81
8.7 Peer-to-peer topology 82
8.8 Mesh topology 82
8.8.1 Establishing a mesh network 83
8.9 Message types 86
8.9.1 Network discovery beacon (NDB) 87
8.9.2 Network status message (NSM) 92
8.9.3 Acknowledgement message 96
8.9.4 Command message 98
8.9.5 Data message 99
8.9.6 Mesh request 100
8.9.7 Mesh data 101
8.10 Network discovery 102
8.10.1 Methods of network discovery 102
8.10.2 Transmitting network discovery beacons 103
8.10.3 Connectionless network 103
8.10.4 Associated network connection (ANC) 105
8.11 Link encryption methods 107

9 MODE 4: Configurable data rate active RFID system 108
9.1 General 108
9.2 Cryptographic suite indicators 108
9.3 Physical layer 109
9.3.1 Operating frequency 109
9.3.2 Emission spectrum density mask 109
9.3.3 Modulation and spectrum spread 109
9.3.4 TX/RX switch time 113
9.3.5 EVM 113
9.4 Data link layer 113
9.4.1 General 113
9.4.2 Preamble 113
9.4.3 Synchronous code 113
9.4.4 Data length 113
9.4.5 Frame option 114
9.4.6 Message data 114
9.4.7 CRC 118
9.5 Tag memory structure 118
9.5.1 Overview 118
9.5.2 Data organization of security section 118
9.5.3 Data organization of user section 119
9.5.4 File definitions of user section 123
9.6 Tag state transition 126
9.6.1 Overview 126
9.6.2 Figure of tag state transition 126
9.6.3 Sense state 127
9.6.4 Ready state 128
9.6.5 Operation state 128

9.6.6 Sleep state 129
9.6.7 Killing state 129
9.7 Interrogator commands and tag responses 129
9.7.1 Command types 129
9.7.2 Command codes list 129
9.7.3 Ready and sleep commands 132
9.7.4 Access commands 135
9.7.5 Collection commands 138
9.7.6 File access commands 141
9.7.7 Monitor commands 149
9.7.8 Security protocol commands 152
9.7.9 Other commands 155
9.8 Protocol operation mode 158
9.8.1 Overview 158
9.8.2 Operation process 158
9.8.3 Operation mode 161
9.9 Anti-collision method 162
9.9.1 Overview 162
9.9.2 Anti-collision process 162
9.9.3 Binary tree algorithm 162
9.10 Parameters for air interface 163
9.10.1 Parameters of physical and data link layer 163
9.10.2 Protocol parameters 165

10 Table of characteristic differences between the modes specified in this document 166

Annex A (informative) **Mode 1: Memory map 167**

Annex B (informative) **Mode 1: CRC 173**

Annex C (normative) **Mode 2: Memory map 176**

Annex D (informative) **Mode 2: CRC 179**

Annex E (normative) **Mode 4: Tag state transition tables 181**

Annex F (informative) **Mode 4: Inventory process example 195**

Annex G (informative) **Mode 4: Wake-up mechanism 196**

Annex H (informative) **Mode 4: Typical parameters of anti-collision algorithm 199**

Bibliography 200

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 ISO documents 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 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 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by 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 18000-4:2015), which has been technically revised. The main changes compared to the previous edition are as follows:

— Mode 4, described in Clause 9 as "MODE 4: Configurable data rate active RFID system", has been added.

A list of all parts in the ISO 18000 series can be found on the ISO website.

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.

Introduction

This document 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.

This document defines four 2,45 GHz protocols. Each of the specific physical/data link configuration is defined in a separate subclause. The configuration descriptions include a physical layer and a data link layer.

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 given in all parts of this document.

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

The holders of these patent rights have assured the 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 may be obtained from the following companies.

	Contact details
Patent holder:	
Legal name	iControl Inc.
Contact for licence application:	
Name and department	George Cavage
Address	3235 Kifer Road, Suite 260, Santa Clara, CA 94109, USA
Tel.	+1 408 730 5364
Fax	
E-mail	gcavage@icontrol-inc.com
URL (optional)	www.icontrol-inc.com
Patent holder:	
Legal name	Impinj, Inc.
Contact for licence application:	
Name and department	Stacy Jones, Impinj, Inc.
Address	701 N 34th Street, Suite 300, Seattle, WA 98103, USA
Tel.	+1 206 834 1032
Fax	+1 206 517 5262
E-mail	stacy.jones@impinj.com
URL (optional)	www.impinj.com

Contact details

Patent holder:	
Legal name	Zebra Technologies Corporation
Contact for licence application:	
Name and department	James O'Hagan, Director of Patents & Technology
Address	475 Half Day Road, Suite 500, Lincolnshire, IL 60069, USA
Tel.	+1 (847) 793-6798
Fax	+1 (847) 955-4514
E-mail	johagan@zebra.com
URL (optional)	
Patent holder:	
Legal name	Chengdu West Valley Digital Technologies, Inc.
Contact for licence application:	
Name and department	Jason Y. Liao
Address	Room 305 Building #9, #88 Tian Chen West High-Tech Zone, Chengdu, China
Tel.	86-28-66767921
Fax	
E-mail	
URL (optional)	www.westv.cn
Patent holder:	
Legal name	Nationz Technologies Inc.
Contact for licence application:	
Name and department	Yang, Xianwei and Mobile Payment and RCC Department
Address	China Technology Exchange Building, 66 North 4th Ring Road West, Haidian District, Beijing
Tel.	86-10-82868162
Fax	
E-mail	
URL (optional)	www.nationz.com.cn
Patent holder:	
Legal name	Shenzhen ZTE Top sky Information Technology Co., Ltd.
Contact for licence application:	
Name and department	Min Zhu
Address	Room B, 10/F, No.3 China Academy of Science-Tech Development Building, Gaoxin 1st Road South, High-Tech Industrial Park, Nanshan District, Shenzhen, China
Tel.	86-0755-86079364
Fax	
E-mail	
URL (optional)	www.zte-v.com.cn

Contact details

Patent holder:	
Legal name	Xidian University
Contact for licence application:	
Name and department	Changxing Pei
Address	No.2, South Taibai Road, Xi'an, Shanxi, China
Tel.	86-29-88204486
Fax	
E-mail	
URL (optional)	www.xidian.edu.cn
Patent holder:	
Legal name	CEC Huada Electronic Design Co., Ltd.
Contact for licence application:	
Name and department	Lan Tian
Address	Floor 5, Building A, Wangjing Science and Technology Park, No.2, Lizezhonger Rd., Chaoyang District, 100102, Beijing, China
Tel.	86-10-64365577
Fax	
E-mail	
URL (optional)	www.hed.com.cn
Patent holder:	
Legal name	China Electronics Standardization Institute (Corresponding corporation)
	CEC Huada Electronic Design Co., Ltd.
Contact for licence application:	
Name and department	Wang Wenfeng
Address	No.1 Andingmen East Street, Beijing
Tel.	86-10-84042998
Fax	
E-mail	
URL (optional)	www.cesi.cn
Patent holder:	
Legal name	Shanghai Super Electronics Technology Co., Ltd.
Contact for licence application:	
Name and department	Qin Zhong
Address	6/F Building 52, 1089 North Qinzhou Rd., Shanghai, China
Tel.	86-21-61613336
Fax	86-21-6161339
E-mail	qinzhong@superrfid.net
URL (optional)	www.superrfid.net

Information technology — Radio frequency identification for item management —

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

1 Scope

This document defines the air interface for radio frequency identification (RFID) devices operating in the 2,45 GHz industrial, scientific, and medical (ISM) band used in item management applications. This document provides a common technical specification for RFID devices that can be used by ISO committees developing RFID application standards. This document is intended to allow for compatibility and to encourage inter-operability of products for the growing RFID market in the international marketplace. This document defines the forward and return link parameters for technical attributes including, but not limited to, operating frequency, operating channel accuracy, occupied channel bandwidth, maximum equivalent isotropically 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 defines the communications protocol used in the air interface.

This document contains four modes. Mode 1 is an interrogator talks first with passive tag. Mode 2 is a tag talks first with battery-assisted passive tag. Mode 3 is a globally available, ubiquitous network supporting (but not limited to) the logistics and transportation industry; agnostic to any device, commercial or otherwise, requiring global availability. Mode 4 is a configurable data rate active RFID system. It provides the functions of long range objects identification and environmental sense, and it is intended to realize the low cost device and low power consumption, long range identification, fast and reliable tags access. The detailed technical differences between the modes are shown in the parameter tables.

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 646, *Information technology — ISO 7-bit coded character set for information interchange*

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

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

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

ISO/IEC/TR 18047-4, *Information technology — Radio frequency identification device conformance test methods — Part 4: Test methods for air interface communications at 2,45 GHz*

ISO/IEC/IEEE 8802-15-4:2018, *Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 15-4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs)*

IEEE 802.15.4:2006, *Information technology — Local and metropolitan area networks — Specific requirements — Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs)*

3 Terms and definitions

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

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

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

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

3.1
associated
successful negotiation of a bi-directional wireless link with a coordinator

Note 1 to entry: Associated networks require communication be maintained and monitored for a period of time.

3.2
association
service used to establish membership for a device communicating within the wireless network described in this document

3.3
authentication
ATH
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 document are Tag authentication, Interrogator authentication, and Tag-Interrogator mutual authentication. For data authentication, see *authenticated communications* (3.4).

3.4
authenticated communications
communications in which message integrity is protected

3.5
block cipher
cryptographic function that operates on strings of fixed size

3.6
chip
smallest unit of signal after spectrum spreading

Note 1 to entry: In the spreading process, an information bit is usually represented by a number of coded signals, wherein a coded signal is called a chip.

3.7
coordinator
full-function device (FFD) capable of relaying messages

Note 1 to entry: If a coordinator is the principal controller of a personal area network (PAN), it is called the PAN coordinator.

3.8
data server
device data termination point

3.9
device
any entity that meets the ISO/IEC/IEEE 8802-15-4 medium access control (MAC), physical interface to the wireless medium, and this document

Note 1 to entry: A device may be a reduced-function device (RFD) or a full-function device (FFD).

3.10
encryption
transformation of a message into a new representation so that privileged information is required to recover the original representation

3.11
full-function device
FFD
device capable of operating as a coordinator

3.12
group key
key that is known only to a set of devices

3.13
hailing channel
ISO/IEC/IEEE 8802-15-4 radio channel used to broadcast the NDB

3.14
key
privileged information that may be used, for example, to protect information from disclosure to, and/or undetectable modification by, parties that do not have access to this privileged information

3.15
keyID
numerical designator for a single key

3.16
link key
secret key that is shared between precisely two devices

3.17
mesh networking
type of network where an FFD serves as a relay for other devices

3.18
message authentication code
MAC1
code, computed over bits in a message, that an Interrogator or a Tag may use to verify the integrity of the message

3.19
message integrity code
MIC
data whereby an entity receiving a message corroborates evidence about the true source of the information in the message and, thereby, evidence that the message has not been modified in transit

3.20
network channel
primary ISO/IEC/IEEE 8802-15-4 radio channel between a coordinator and remote devices

3.21
packet
formatted, aggregated bits that are transmitted together in time across the physical medium

3.22
password
information that is used to verify identities in the *tag access* (3.29) process

3.23
payload data
contents of a data message that is being transmitted

3.24
reduced-function device
RFD
device that is not capable of operating as a coordinator

3.25
secure communications
communications in which message confidentiality is protected

3.26
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.

3.27
server connected coordinator
SCC
network coordinator that terminates the wireless protocol described in this document and is connected to control servers

3.28
tag
any device type associated with the device and capable of joining the network

3.29
tag access
process in which tags establish communication links with interrogators according to certain communication protocols

4 Symbols and abbreviated terms

ACK	acknowledgement
ALW	always
CCITT	Comité Consultatif International Téléphonique et Télégraphique
Cht	Carrier high level tolerance
Clt	Carrier low level tolerance
CRC	cyclical redundancy check
CSI	cryptographic suite identifier
CSMA	carrier sense multiple access
DBPSK	differential binary phase shift keying
DF	dedicated file

DSSS	direct sequence spread spectrum
EBV	extensible bit vectors
EF	element file
EIRP	equivalent isotropic radiated power
EVM	error vector magnitude
$f_{bitrate}$	base frequency of the bit rate of Manchester code without bit changes
f_c	frequency of operating field (carrier frequency)
FCF	frame control field
FCS	frame check sequence
FHSS	frequency hopping spread spectrum
LSB	least significant bit
M	Modulation
Ma	Modulation overshoot
MAC	medium access control
Mb	Modulation undershoot
MF	main directory file
MIC	message integrity code
MIN	Manufacturing Identification Number
Mlt	Modulation lower tolerance
MSB	most significant bit
Mut	Modulation upper tolerance
N	total number of time-slots in access frame
NAK	no-acknowledgement
NDB	network discovery beacon
NEV	never
NSM	network status message
OID	object identifier
O-QPSK	offset quadrature phase shift keying
ppm	parts per million
PWD	password
Q	parameter that controls tag access number