



BSI Standards Publication

Information technology — Radio frequency identification for item management

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

National foreword

This British Standard is the UK implementation of ISO/IEC 18000-4:2018. It supersedes BS ISO/IEC 18000-4:2015, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/34, Automatic identification and data capture techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018

Published by BSI Standards Limited 2018

ISBN 978 0 580 94435 2

ICS 35.040.50

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 August 2018.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

**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)

AVA Documents
Document Sharing Hub
© ISO/IEC 2018



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	74

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

86-21-61613339

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
Cl _t	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

QPSK	quad-phased shift keying
RFID	radio frequency identification
RID	interrogator identifier
RNr	random number generated by interrogators
RNt	random number generated by tags
RN16	16-bit random number
RN8	8-bit random number
RTLS	real time locating system
SN _{slot}	serial number of time-slot
SN _{success}	serial number of successful access
Tbmf	Manchester fall time
Tbmr	Manchester rise time
Tcf	carrier fall time
Tcr	carrier rise time
Tcs	carrier steady time
TDMA	time division multiple access
Tf	fall time
Tfhf	carrier FHSS fall time
Tfhr	carrier FHSS rise time
Tfhs	carrier FHSS steady time
Tflb	forward link bit time
Tr	rise time
Trlb	return link bit time
TID	tag identifier
TTL	tag talk last
UII	unique item identifier
Wslot	width of time-slot
⊕	bitwise XOR
	series connection
•	point multiplication
+	binary addition

5 General items on 2,45 GHz RFID protocols that support this document

5.1 Protocols

This clause describes the general items of the ISO/IEC 18000-4 2,45 GHz RFID command/data level communication protocols. These protocols facilitate communication between compliant tag and compliant interrogator. The timing parameters and signal characteristics for the protocols are defined in the physical link specifications in each mode. Details of the Modes of various protocols are described in [Clauses 6, 7, 8 and 9](#).

5.2 Frequency

5.2.1 General

This document is intended to address RFID devices operating in the 2 450 MHz Industrial, Scientific and Medical (ISM) frequency band.

5.2.2 Interface definitions

This document supports standard parameters and standard air interface implementations for wireless, non-contact information system equipment for Item Management applications. Typical applications operate at ranges greater than 1 m.

5.2.2.1 RFID system definition

The radio frequency identification (RFID) system shall include a host system and RFID equipment (interrogator and tags). The host system runs an application program, which controls interfaces with the RFID. The RFID equipment shall be composed of two principal components: tags and interrogators. The tag is intended for attachment to an item, which a user wishes to manage. It is capable of storing a tag ID number and other data regarding the tag or item and of communicating this information to the interrogator. The interrogator is a device, which communicates to tags in its field of view. Additionally, the interrogator can use its transmitted RF carrier to power the tag. Systems, which rely on the transmitted interrogator carrier for powering the tag, are typically referred to as passive tag systems. The interrogator controls the protocol, reads information from the tag, directs the tag to store data in some cases, and ensures message delivery and validity.

5.2.2.2 Minimum features

RFID systems defined by this document provide the following minimum features:

- identify tag in range;
- read data;
- write data or handle read-only systems gracefully;
- selection by group or address;
- graceful handling of multiple tags in the field of view;
- error detection.

5.2.2.3 Conformance

To claim conformance with this document, an RFID system shall comply with one of the physical/data link implementations described in [Clauses 6, 7, 8 and 9](#).

The rules for RFID device conformity evaluation are given in ISO/IEC 18047-4.

5.3 Tag identification number

A tag identification number shall be included in commands directed to a specific tag unless the protocol provides other means like Tag Talks First (TTF) protocols. This document mandates that each tag shall include a manufacturer's tag identification number as defined in [Annex A](#) for mode 1, in [Annex C](#) for mode 2, in [8.5.1](#) for mode 3 and in [9.4.6.1](#) for mode 4.

A separate User Tag Identification is not mandatory, but is an option. When a UserTagID is used, it shall consist of the number of bytes required by the user application. This number and other application data shall be accessed as user data fields on the tag. These fields can be accessed via the API using the driver's field name resolution mechanism. The UserTagID is a user-defined tag identifier and is not necessarily unique.

5.4 Potential interference

Standards developers have a duty to ensure that no "significant interference" exists between Standardized modes. "Significant Interference" exists if a system of one Standardized mode (working within the most widespread regulated power emissions) is likely to impede the successful operation of a system of another Standardized mode (working within the most widespread regulated power emissions), *in likely expected operating situations*.

Marginal measurable interference that does not impede operation *in likely expected operating situations*, or that could be avoided by simple and inexpensive design improvement, shall not be considered cause to reject a mode.

- Therefore, TTF modes are clearly identified as such in this document.
- Therefore, installers of RFID systems are advised that they should make best efforts to be a good neighbour in installing any systems, bearing in mind that there may be other systems sharing the same bandwidth, and are advised to take precautions to minimize interference to other systems. Installers are equally advised to be prepared to handle interference within the bandwidth from other users up to transmission powers permitted by local regulations.

6 MODE 1: Passive backscatter RFID system

6.1 MODE 1: General

The FHSS backscatter option or the narrow band operation RFID system shall include an interrogator that runs the FHSS backscatter option 1 RFID protocol or in narrow band operation, as well as one or more tags within the interrogation zone.

When placed in the RF field of an interrogator, the tag shall begin to power up. If the field is adequate, the tag shall execute a power-on reset and shall be ready to receive commands. Each command shall begin with a preamble and start delimiters that, taken together, enable the tag to perform clock and data recovery on the incoming signal. Data to and from the tag are checked for errors using a Cyclic Redundancy Code (CRC). Therefore, CRC fields are present in all interrogator interrogations and in all tag responses. Additional data protection is provided by Manchester encoding on the forward (interrogator to tag) link and FM0 encoding on the return (tag to interrogator) link.

By using the FHSS backscatter option 1 RFID command set or in narrow band operation, the interrogator can execute a number of functions on tags in its field. For example, the interrogator can send a command sequence, which allows it to identify multiple tags simultaneously in its RF field. Alternately, it can select a subset of the tags in the field based on tag memory contents. It can also read data stored on a tag in its field, as well as write or lock data to such a tag.

The description of the RFID tag command set in the following clause shall provide detail regarding the command field and return data/acknowledgement fields, if any. In addition, it shall cover additional high-level elements of the FHSS backscatter option RFID protocol, including how the multiple item

identification algorithm works and byte ordering requirements. The more general aspects of the protocol (preambles, CRC-16, etc.) are covered in detail in [6.2.7](#).

This portion of this document describes a passive backscatter RFID system that supports the following system capabilities:

System protocol

- Identify and communicate with multiple tags in the field
- Select a subgroup of tags to identify or communicate with based on information that the user has stored in the tag
- Read from and write or rewrite data many times to individual tags
- User controlled permanent lock memory

Data integrity protection

- Manchester bit-wise encoding and CRC-16 packet-level protection are applied to the forward link (interrogator-to-tag) data.
- FM0 bit-wise encoding and CRC-16 packet-level protection are applied to the return link (tag-to-interrogator) data.

In this RFID system, interrogators both power and communicate with the tags that are within their range. Tags receive data as on-off key amplitude modulation of the power/data signal from the interrogator. During the time that the tag communicates back to the interrogator, the interrogator broadcasts a steady radio frequency power level, and the tag modulates the impedance of its radio frequency load attached to the tag antenna terminals. The interrogator then receives the data back from the tag as a variation in reflection of its transmitted power.

6.2 Physical layer and data coding

6.2.1 Interrogator power-up waveform

The interrogator power-up waveform shall comply with the mask specified in [Figure 1](#) and [Table 1](#).

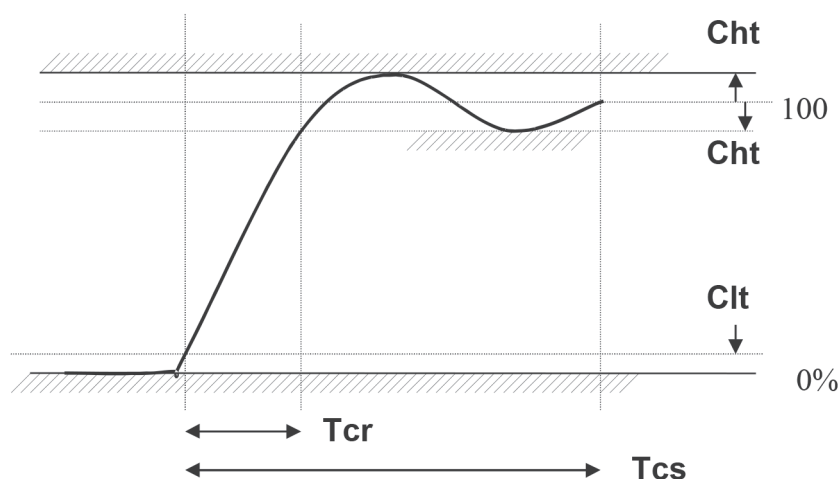


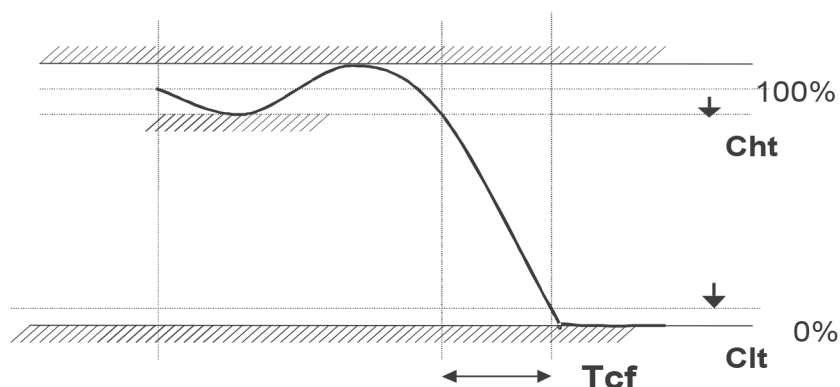
Figure 1 — Interrogator power-up waveform

Table 1 — Interrogator power-up waveform parameter values

Parameter	Min	Max
Tcs		400 μ s
Tcr	0 μ s	30 μ s
Cht		3 %
Clf		1 %

6.2.2 Interrogator power-down

Once the carrier level has dropped below the ripple limit Cht, power down shall be monotonic and of duration Tcf, as specified in [Figure 2](#) and [Table 2](#).

**Figure 2 — Interrogator power-down waveform****Table 2 — Interrogator power-down timings**

Parameter	Min	Max
Tcf	1 μ s	500 μ s
Cht		3 %
Clf		1 %

6.2.3 Frequency hopping carrier rise and fall times

When the interrogator operates in the frequency hopping spread spectrum (FHSS) mode, the carrier rise and fall times shall conform to the characteristics specified in [Figure 3](#) and [Table 3](#).

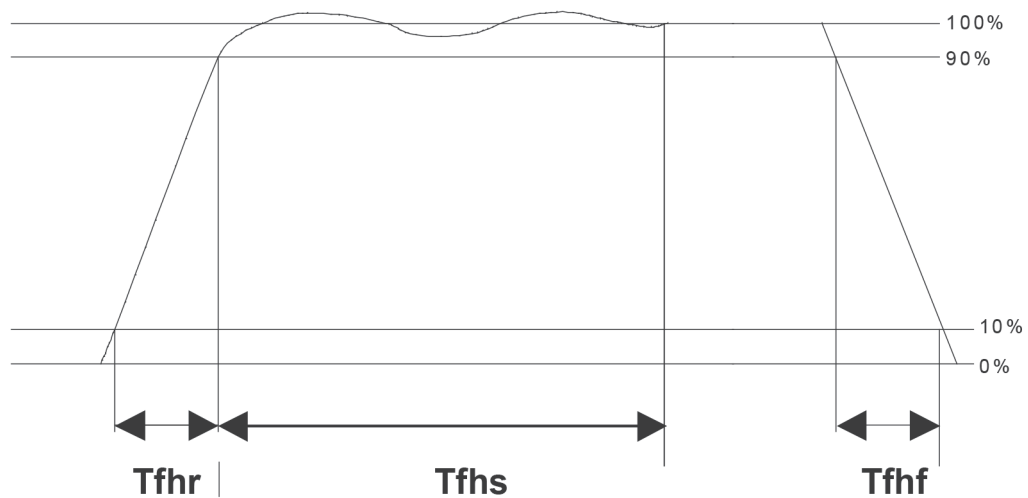


Figure 3 — FHSS carrier rise and fall characteristics

Table 3 — FHSS carrier rise and fall parameters

Parameter	Min	Max
Tfhr		15 μ s
Tfhs	400 μ s	
Tfhf		15 μ s

NOTE The numbers in [Table 3](#) are an example for current FCC regulations only.

6.2.4 Forward link

6.2.4.1 Carrier modulation

The data transmission from the interrogator to the tag is achieved by modulation of the carrier (ASK). The data coding is performed by generating pulses that create a Manchester coding.

The example of 40 kbit/s signal of Manchester coding as per [Figure 4](#).

The parameter for 99 % Modulation of Manchester coding is specified in [Table 4](#).

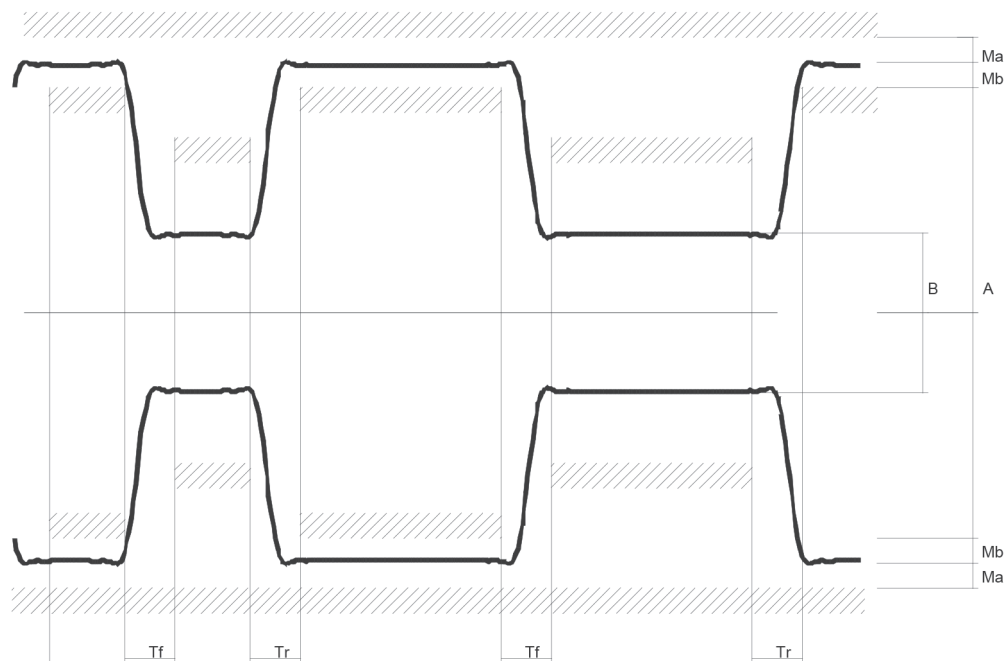


Figure 4 — Example of 40 kbit/s signal

Table 4 — Parameter for 99 % Modulation

Parameter	Minimum	Nominal	Maximum
$M = (A - B)/(A + B)$	90	99	100
Ma	0		0,03 (A - B)
Mb	0		0,03 (A - B)
Tr	0 μ s	1,8 μ s	0,1/f _{bitrate}
Tf	0 μ s	1,8 μ s	0,1/f _{bitrate}

6.2.4.2 Bit coding of forward link fields

Data are Manchester encoded as per [Figure 5](#).

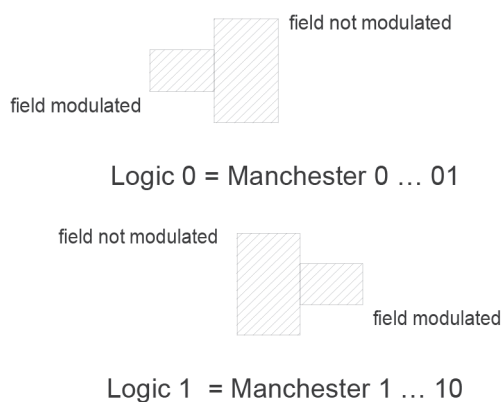


Figure 5 — Forward link bit coding

6.2.5 FM0 return link

6.2.5.1 General

The tag transmits information to the interrogator by modulating the incident energy and reflecting it back to the interrogator (backscatter).

6.2.5.2 Modulation

The tag switches its reflectivity between two states. The “space” state is the normal condition in which the tag is powered by the interrogator and is able to receive and decode the forward link. The “mark” state is the alternative condition created by changing the antenna configuration or termination.

6.2.5.3 Data rate

The return link data rate is derived from the forward link data rate and is typically 40 kbit/s. For details, see [Table 5](#).

6.2.5.4 Data coding

Data are coded using the FM0 technique, also known as Bi-Phase Space.

One symbol period $Trlb$ is allocated to each bit to be sent. In FM0 encoding, data transitions occur at all bit boundaries. In addition, data transitions occur at the mid-bit of logic 0 being sent.

Table 5 — Return link parameters

Data rate	$Trlb$	Tolerance
30 kbit/s to 40 kbit/s	25 μ s to 33 μ s	± 15 %

Coding of data is MSB first. [Figure 6](#) illustrates the coding for the 8 bits of 'B1'.

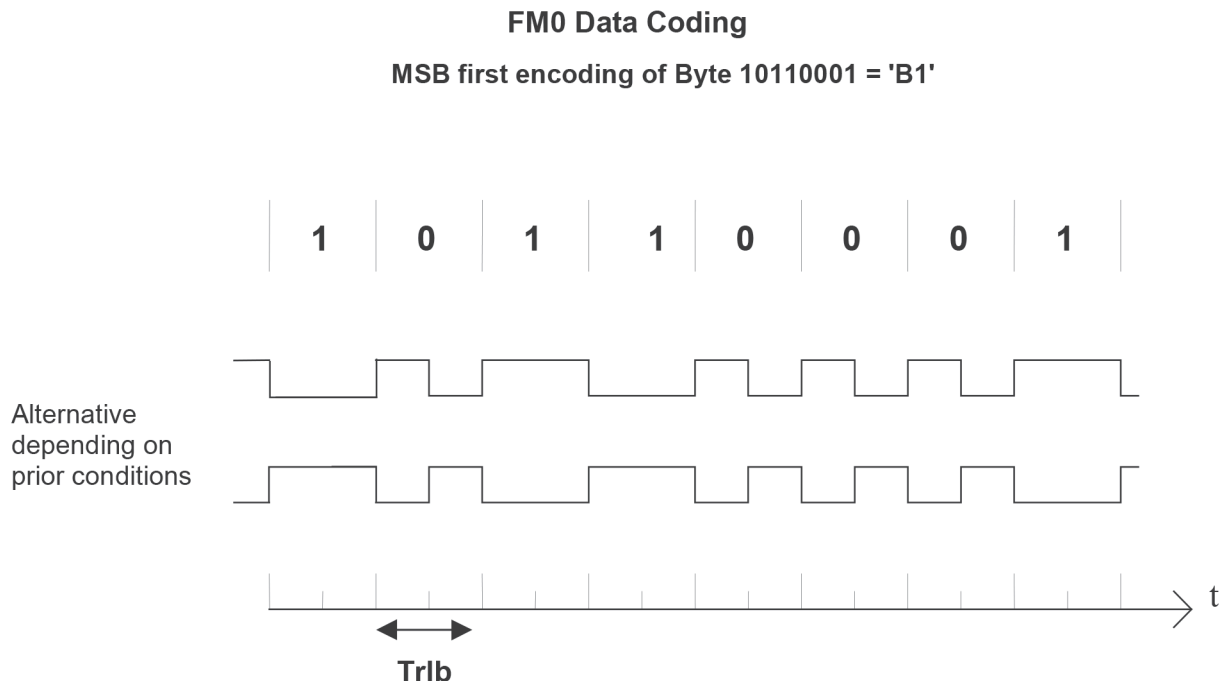


Figure 6 — Tag to interrogator data coding

6.2.5.5 Message format

A Return Link Message consists of n data bits preceded by the Preamble and followed by the tag data. The data bits are sent MSB first.

The Preamble enables the interrogator to lock to the tag data clock and begin decoding of the message. It consists of 16 bits as shown in Table 6. There are multiple code violations (sequence not conforming to FM0 rules) that act as a frame marker for the transition from Preamble to Data.

6.2.5.6 Return preamble

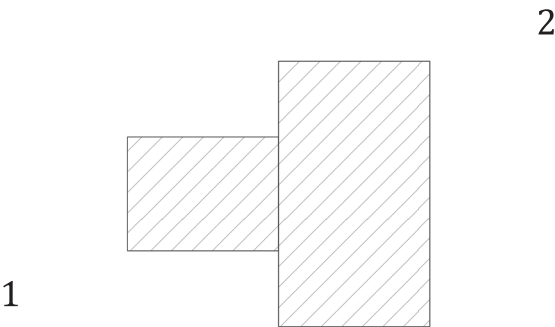
The return preamble is a sequence of backscatter modulation specified in Table 6.

Table 6 — Return preamble

00 00 01 01 01 01 01 01 01 01 00 01 10 11 00 01

Data ‘0’ is represented by the tag’s modulator being in the high impedance state, Data ‘1’ is represented by the tag’s modulator switching to the low impedance state, thereby causing a change in the incident energy to be back-scattered.

The tag shall execute backscatter, a half-bit 1 and half-bit 0 sent by the tag defined as follows in Figure 7.



NOTE 1 = low impedance (backscatter), 0 = high impedance (no backscatter).

Figure 7 — Return link preamble

6.2.6 Cyclic redundancy check (CRC)

When sending a command to the tag, the interrogator shall attach an inverted CRC to the message packet. On receiving a command from the interrogator, the tag shall verify that the checksum or the CRC value is valid. If it is invalid, it shall discard the frame, shall not respond and shall not take any other action.

The 16-bit CRC applies for both communication directions: from interrogator to tag and from tag to interrogator.

The polynomial used to calculate the CRC is $X^{16} + X^{12} + X^5 + 1$. The 16-bit register shall be preloaded with ‘FFFF’. The resulting CRC value shall be inverted, attached to the end of the packet and transmitted.

The most significant byte shall be transmitted first. The most significant bit of each byte shall be transmitted first.

At the tag, the incoming CRC bits are inverted and then clocked into the register. After the LSB bit is clocked into the tag, the 16-bit CRC register should contain all zeroes.

The 16-bit CRC shall be calculated on all data bits up to, but not including, the first CRC bit.

On receiving of a response from the tag, it is recommended that the interrogator verifies that the CRC value is valid. If it is invalid, appropriate remedial action is the responsibility of the interrogator designer.

The CRC 16 bits and bytes transmission rules is specified in [Table 7](#).

Table 7 — CRC 16 bits and bytes transmission rules

MSByte				LSByte			
MSB		LSB		MSB		LSB	
CRC 16 (8 bits)				CRC 16 (8 bits)			
↑ first transmitted bit of the inverted CRC							

6.2.7 Protocol concept

Data are encoded and presented in slightly different ways in the constituent fields. For interrogator-to-tag communication (forward link), data are sent using an on-off key format. The radio frequency field being on corresponds to 1, while the radio frequency field being off corresponds to 0. The on-off ratio specification is defined in [6.2.4](#). In the case of Manchester coding, a Manchester 1 is a 1 to 0 transition, while a Manchester 0 is a 0 to 1 transition.

For tag-to-interrogator communication (return link), data are sent using backscatter techniques. This requires that the interrogator provide steady power to the tag during the return link. While the interrogator powers the tag, the tag shall change alternately the effective impedance of the tag front end and thus changing the overall radio frequency reflectivity of the tag as seen by the interrogator. During this time, the interrogator shall not modulate the carrier. During the WAIT field (when tags write data into their memory), the interrogator shall also provide steady power to the tag and shall not modulate the carrier. The transmission protocol defines the mechanism to exchange instructions and data between the interrogator and the tag, in both directions.

It is based on the concept of "interrogator talks first".

This means that any tag shall not start transmitting (modulating) unless it has received and properly decoded an instruction sent by the interrogator.

The protocol is based on an exchange of a command from the interrogator to the tag and a response from the tag(s) to the interrogator.

The conditions under which the tag sends a response are defined in [6.3.6](#).

Each command and each response are contained in a frame. The frame is specified in [6.2.7](#).

Each command consists of the following fields:

- Preamble
- Delimiter
- Command code
- Parameter fields, depending on the command
- Application data fields, depending on the command
- CRC

Each response consists of the following fields:

- Return preamble
- Application data fields

CRC

The protocol is bit-oriented. The number of bits transmitted in a frame is a multiple of eight (8), i.e. an integer number of bytes. However, the frame itself is not based on an integer number of bytes.

In all byte fields, the MSB shall be transmitted first, proceeding to the LSB. In all word (8-byte) data fields, the MSB shall be transmitted first.

The MSB shall be the byte at the specified address. The LSB shall be the byte at the specified address plus 7 (i.e. bytes are transmitted in incrementing address order).

The byte significance is relevant to data transmission and to the GROUP_SELECT and GROUP_UNSELECT greater than and less than comparisons.

The MSB of the byte mask shall correspond to the most significant data byte, the byte at the specified address.

Word (8-byte) addresses are not required to be on an 8-word boundary and may be on any byte boundary.

RFU bits and bytes shall be set to zero (0).

6.2.8 Command format

6.2.8.1 General

The command consists of the following fields:

- Preamble
- Delimiter
- Command
- Parameter and data files
- CRC

The general command format is specified in [Table 8](#).

Table 8 — General command format

Preamble detect	Preamble	Delimiter	Command	Parameter	Data	CRC
-----------------	----------	-----------	---------	-----------	------	-----

6.2.8.2 Preamble detect field

The preamble detect field consists of a steady carrier (no modulation) during a time of at least 400 µs. This corresponds to 16 bits for a communication rate of 40 kbit/s.

6.2.8.3 Preamble

The preamble is equivalent to 9 bits of Manchester 0.

0101010101010101

6.2.8.4 Delimiter

6.2.8.4.1 Start delimiter 1

In NRZ format; includes Manchester errors; spaces ignored

11 00 11 10 10 Delimiter 1

6.2.8.5 CRC

See [6.2.6](#) and [Annex B](#).

6.2.9 Response format

6.2.9.1 General

The response consists of the following fields:

- Quiet
- Return preamble
- Data fields
- CRC

The general response format is specified in [Table 9](#).

Table 9 — General response format

Quiet	Return preamble	Data	CRC
-------	-----------------	------	-----

The tag shall use a backscatter technique to communicate data to the interrogator. The interrogator shall be steadily powering the tag as well as listening to the tag response throughout the tag-to-interrogator (backscatter) communication. This applies to all fields in the return link.

6.2.9.2 QUIET

The tag shall not backscatter for $16 \times \text{Trlb} - 0,75 \times \text{Tflb}$. The duration of the quiet time is determined by the communication speed of the forward and return link.

6.2.9.3 CRC

See [6.2.6](#) and [Annex B](#).

6.2.10 WAIT

During the WAIT field, the interrogator provides steady power to the tag for the duration of at least 15 ms. No on-off key data may be sent during the write operation.

When a tag receives a write command, it shall execute a write operation. (The details of the conditions under which a write will occur are described in [6.3.6.2.5.4](#).) If a write operation is executed, the final field in the overall field sequence shall always be WAIT.

During the WAIT field, when the tag is writing data into the EEPROM, the interrogator shall steadily power the tag. On-off key data shall not be sent during this time.

Details are shown in [Figure 8](#) and in [Figure 9](#).

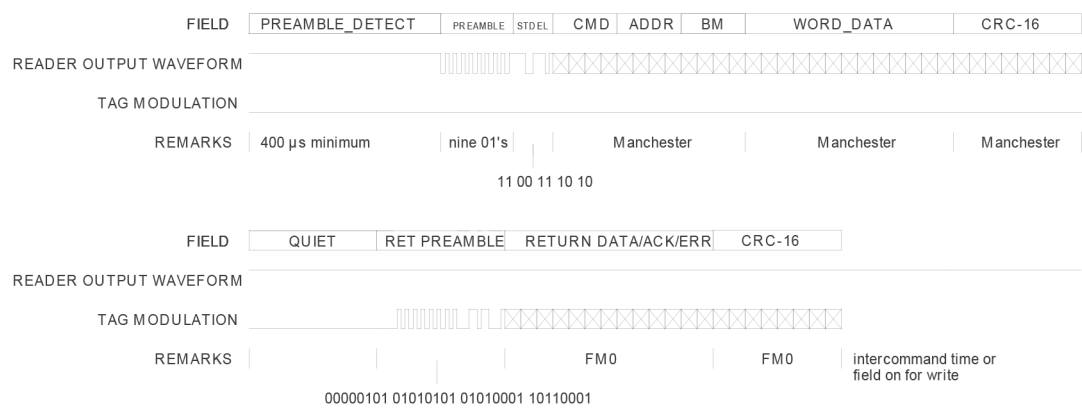


Figure 8 — Sample command/response packets for GROUP_SELECT (40 kbit/s on forward and return link)

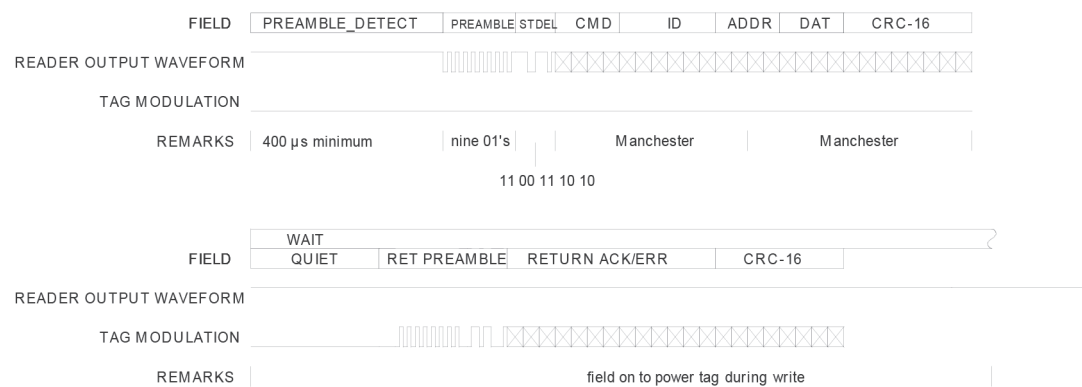


Figure 9 — Sample command/response packets for WRITE (40 kbit/s on forward and return link)

6.2.11 Communication sequences at packet level

Figure 10 and Figure 11 show several examples of communication sequences at the packet level. Figure 10 depicts a packet sequence that includes a write command. The sequence includes a wait for write time, which provides the necessary time for the chip to complete its write operation. In addition, following the wait for write time, the interrogator issues a tag resync signal. This signal is composed of 10 consecutive 01 signals. The purpose of the tag resync signal is to initialize the tag data recovery circuitry. It is required after a write because the interrogator may output spurious edges during the wait for write time. Without the tag resync, tags may miscalibrate as a result of the spurious signals that may be generated.

Figure 11 depicts a packet sequence in which a frequency hop between commands is included. The tag resync signal is again required after the hop because spurious signals may be generated during the hop time.

In order to ensure that tags do not get confused, frequency hops between command and response should be avoided.

Action		COMMAND	RESPONSE	WAIT FOR WRITE	TAG RESYNC	COMMAND	RESPONSE
Component action	execution	Interrogator	Tag	Interrogator	Interrogator	Interrogator	Tag
Notes		---	---	15 ms minimum	ten 01's	---	---

Figure 10 — Command sequence (including a write) with no hopping

Action		COMMAND	RESPONSE	HOP	TAG RESYNC	COMMAND	RESPONSE
Component action	execution	Interrogator	Tag	Interrogator	Interrogator	Interrogator	Tag
Notes		---	---	< 26 μ s	ten 01's	---	---

Figure 11 — Command sequence with a hop between response and next command

6.3 Protocol and collision arbitration

6.3.1 Definition of data elements, bit and byte ordering

6.3.1.1 Unique ID

See [A.2](#).

6.3.1.2 CRC

See [6.2.6](#) and [Annex B](#).

6.3.1.3 FLAGS

The tag shall support a field of eight flags. This field is called FLAGS.

The FLAGS is specified in [Table 10](#).

Table 10 — FLAGS

Bit	Name
FLAG1 (LSB)	DE_SB (Data_Exchange Status Bit)
FLAG2	WRITE_OK
FLAG3	BATTERY_POWERED
FLAG4	BATTERY_OK
FLAG5	0 (RFU)

Table 10 (continued)

Bit	Name
FLAG6	0 (RFU)
FLAG7	0 (RFU)
FLAG8 (MSB)	0 (RFU)

6.3.1.3.1 Data Exchange Status Bit (DE_SB)

The tag shall set this bit when the tag goes into the DATA_EXCHANGE state and keep it set unless it moves into the POWER-OFF state.

When the DE_SB is set and the tag comes into the POWER-OFF state, then the tag shall trigger a timer that will reset the DE_SB bit after t_{DE_SB} .

t_{DE_SB} shall be at least 2 s in the temperature range 30 °C to 60 °C.

t_{DE_SB} shall be at least 4 s in the temperature range 0 °C to 50 °C.

When the tag receives the INITIALIZE command, then it shall reset the DE_SB immediately.

6.3.1.3.2 WRITE_OK

The WRITE_OK bit shall be set after a successful write access to the memory (e.g. WRITE, LOCK).

The WRITE_OK bit is cleared after execution of the command following the write command.

6.3.1.3.3 BATTERY_POWERED

The BATTERY_POWERED bit shall be set when the tag should have a battery. It shall be cleared for passive tags.

6.3.1.3.4 BATTERY_OK

The BATTERY_OK bit shall be set when the battery has enough power to support the tag. It shall be cleared for passive tags.

6.3.2 Tag memory organization

The functional memory shall be organized in blocks of one byte.

Up to 256 blocks of one byte can be addressed.

This leads to a maximum memory capacity of up to 2 kbit.

NOTE This structure allows future extensions of the maximum memory capacity.

6.3.3 Block security status

Each byte shall have a corresponding lock bit. The lock bits may be locked by use of the LOCK command. The status of the lock bit may be read by the QUERY_LOCK command. The tag shall not be allowed to reset any lock bit after leaving the final production site. In most cases, this is the production site that defines the unique ID.

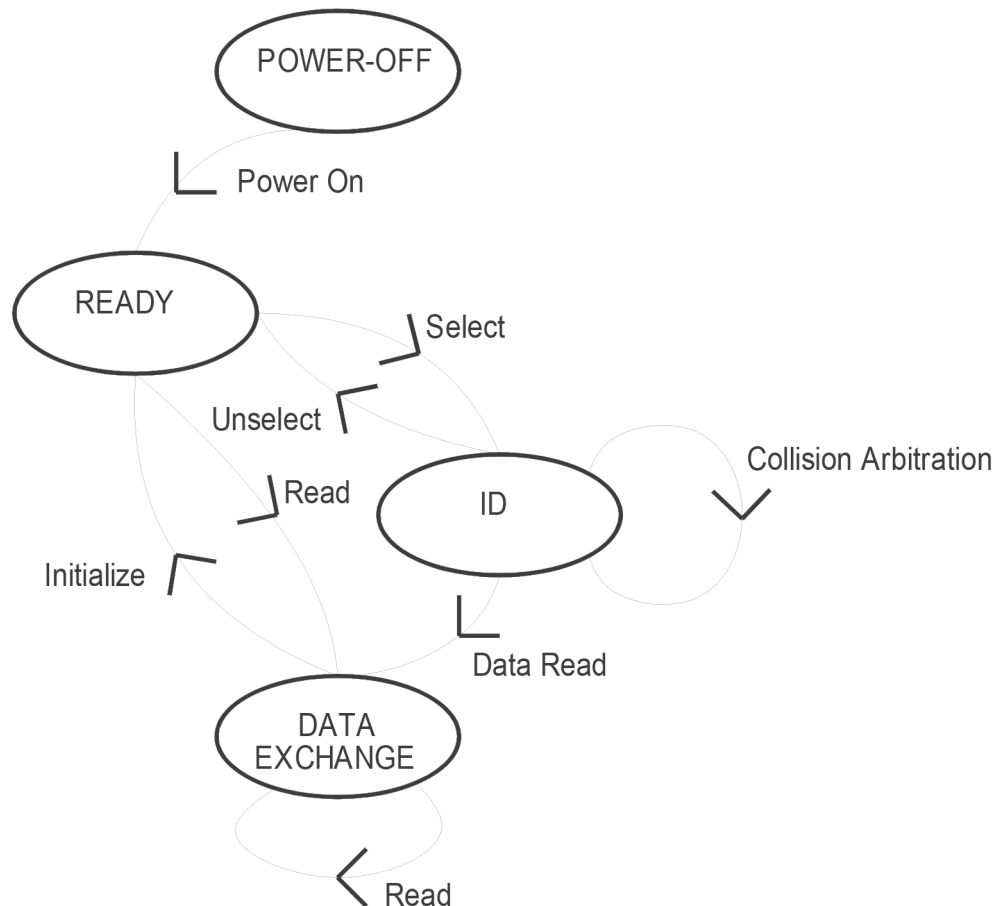
6.3.4 Overall protocol description

6.3.4.1 Tag states

The tag has four major states:

POWER-OFF	The tag is in the POWER-OFF state when the interrogator cannot activate it. (For battery-assisted tags, it means that the level of RF excitation is insufficient to turn on the tag circuits.)
READY	The tag is in the READY state when the interrogator first powers it up.
ID	The tag is in the ID state when it is trying to identify itself to the interrogator.
DATA_EXCHANGE	The tag is in the DATA_EXCHANGE state when it is known to the interrogator and was selected.

The state diagram as per [Figure 12](#).



NOTE This diagram does not show that the tag goes into POWER-OFF from all states in the case that the interrogator field is permanently turned off.

Figure 12 — State diagram

The state diagram only shows an overview of the possible transition. Details are specified in [Table 12](#).

Power-On:

State change when interrogator field is turned on.

Select

State change due to selection of tag by GROUP_SELECT or READ commands.

Unselect

State change due to deselection of tag by GROUP_UNSELECT commands or INITIALIZE command.

Collision Arbitration

No state change during collision arbitration until single tag is identified.

Data_Read

State change due to first read access in collision arbitration process.

Read

State change due to read access independent of collision arbitration process.

Initialize

State change due to deselection of tag by INITIALIZE command.

The detailed command processing is specified in [Table 11](#).

The transition between these states is specified in [Table 12](#).

6.3.4.2 Detailed command processing

Commands shall be active in states marked with “X” and neither causes a state change nor cause a response in the other states.

Table 11 — Detailed command processing

COMMAND	States		
	READY	ID	DATA EXCHANGE
GROUP_SELECT_EQ	X	X	
GROUP_SELECT_NE	X	X	
GROUP_SELECT_GT	X	X	
GROUP_SELECT_LT	X	X	
GROUP_SELECT_EQ_FLAGS	X	X	
GROUP_SELECT_NE_FLAGS	X	X	
GROUP_UNSELECT_EQ		X	
GROUP_UNSELECT_NE		X	
GROUP_UNSELECT_GT		X	
GROUP_UNSELECT_LT		X	
GROUP_UNSELECT_EQ_FLAGS		X	
GROUP_UNSELECT_NE_FLAGS		X	
MULTIPLE_UNSELECT		X	
FAIL		X	
SUCCESS		X	
RESEND		X	
INITIALIZE	X	X	X
READ	X	X	X

Table 11 (continued)

COMMAND	States		
	READY	ID	DATA EXCHANGE
DATA_READ		X	X
READ_VERIFY	X	X	X
READ_VERIFY4BYTE	X	X	X
WRITE	X	X	X
WRITE4BYTE	X	X	X
WRITE4BYTE_MULTIPLE		X	X
WRITE_MULTIPLE		X	X
LOCK			X
QUERY_LOCK	X	X	X

Table 12 — State transition table

Current state	Command	Condition	New state
POWER-OFF	ANY COMMAND		POWER OFF
POWER-OFF	"Power up"		READY
READY	GROUP_SELECT_EQ	≠	READY
READY	GROUP_SELECT_NE	=	READY
READY	GROUP_SELECT_GT	≤	READY
READY	GROUP_SELECT_EQ_FLAGS	flag not set	READY
READY	GROUP_SELECT_NE_FLAGS	flag set	READY
READY	GROUP_SELECT_LT	≥	READY
READY	GROUP_SELECT_EQ	=	ID
READY	GROUP_SELECT_NE	≠	ID
READY	GROUP_SELECT_GT	>	ID
READY	GROUP_SELECT_LT	<	ID
READY	GROUP_SELECT_EQ_FLAGS	flag set	ID
READY	GROUP_SELECT_NE_FLAGS	flag not set	ID
READY	INITIALIZE		READY
READY	READ	ID no match	READY
READY	READ	ID match	DATA_EXCHANGE
READY	READ_VERIFY	ID no match or not WRITE_OK	READY
READY	READ_VERIFY	ID match and WRITE_OK	DATA_EXCHANGE
READY	READ_VERIFY4BYTE	ID no match or not WRITE_OK	READY
READY	READ_VERIFY4BYTE	ID match and WRITE_OK	DATA_EXCHANGE
READY	WRITE	ID no match	READY
READY	WRITE	ID match	DATA_EXCHANGE
READY	WRITE4BYTE	ID no match	READY
READY	WRITE4BYTE	ID match	DATA_EXCHANGE
READY	QUERY_LOCK	ID no match	READY
READY	QUERY_LOCK	ID match	DATA_EXCHANGE
ID	GROUP_UNSELECT_EQ	≠	ID

Table 12 (continued)

Current state	Command	Condition	New state
ID	GROUP_UNSELECT_NE	=	ID
ID	GROUP_UNSELECT_GT	≤	ID
ID	GROUP_UNSELECT_LT	≥	ID
ID	GROUP_UNSELECT_EQ_FLAGS	flag not set	ID
ID	GROUP_UNSELECT_NE_FLAGS	flag set	ID
ID	GROUP_UNSELECT_EQ	=	READY
ID	GROUP_UNSELECT_NE	≠	READY
ID	GROUP_UNSELECT_GT	>	READY
ID	GROUP_UNSELECT_LT	<	READY
ID	GROUP_UNSELECT_EQ_FLAGS	flag set	READY
ID	GROUP_UNSELECT_NE_FLAGS	flag not set	READY
ID	MULTIPLE_UNSELECT	≠ or not WRITE_OK	ID
ID	MULTIPLE_UNSELECT	= and WRITE_OK	READY
ID	GROUP_SELECT_EQ		ID
ID	GROUP_SELECT_NE		ID
ID	GROUP_SELECT_GT		ID
ID	GROUP_SELECT_LT		ID
ID	GROUP_SELECT_EQ_FLAGS		ID
ID	GROUP_SELECT_NE_FLAGS		ID
ID	FAIL		ID
ID	SUCCESS		ID
ID	RESEND		ID
ID	INITIALIZE		READY
ID	READ	ID no match	ID
ID	READ	ID match	DATA_EXCHANGE
ID	DATA_READ	ID no match	ID
ID	DATA_READ	ID match	DATA_EXCHANGE
ID	READ_VERIFY	ID no match or not WRITE_OK	ID
ID	READ_VERIFY	ID match and WRITE_OK	DATA_EXCHANGE
ID	READ_VERIFY4BYTE	ID no match or not WRITE_OK	ID
ID	READ_VERIFY4BYTE	ID match and WRITE_OK	DATA_EXCHANGE
ID	WRITE	ID no match	ID
ID	WRITE	ID match	DATA_EXCHANGE
ID	WRITE4BYTE	ID no match	ID
ID	WRITE4BYTE	ID match	DATA_EXCHANGE
ID	WRITE_MULTIPLE		ID
ID	WRITE4BYTE_MULTIPLE		ID
ID	QUERY_LOCK	ID no match	ID
ID	QUERY_LOCK	ID match	DATA_EXCHANGE
DATA_EXCHANGE	INITIALIZE		READY
DATA_EXCHANGE	READ		DATA_EXCHANGE
DATA_EXCHANGE	DATA_READ		DATA_EXCHANGE

Table 12 (continued)

Current state	Command	Condition	New state
DATA_EXCHANGE	READ_VERIFY		DATA_EXCHANGE
DATA_EXCHANGE	READ_VERIFY4BYTE		DATA_EXCHANGE
DATA_EXCHANGE	WRITE		DATA_EXCHANGE
DATA_EXCHANGE	WRITE4BYTE		DATA_EXCHANGE
DATA_EXCHANGE	WRITE4BYTE_MULTIPLE		DATA_EXCHANGE
DATA_EXCHANGE	WRITE_MULTIPLE		DATA_EXCHANGE
DATA_EXCHANGE	LOCK		DATA_EXCHANGE
DATA_EXCHANGE	QUERY_LOCK		DATA_EXCHANGE

6.3.5 Collision arbitration

The interrogator may use the GROUP_SELECT and GROUP_UNSELECT commands to define all or a subset of tags in the field to participate in the collision arbitration. It then may use the identification commands to run the collision arbitration algorithm.

For the collision arbitration, the tag shall support two pieces of hardware on the tag:

- an 8-bit counter COUNT;
- a random 1 or 0 generator.

In the beginning, a group of tags is moved to the ID state by GROUP_SELECT commands and shall set their internal counters to 0. Subsets of the group may be unselected by GROUP_UNSELECT commands back to the READY state. Other groups can be selected before the identification process begins. Simulation results show no advantage in identifying one large group or a few smaller groups.

After the above described selection, the following loop should be performed:

- a) All tags in the ID state with the counter COUNT at 0 shall transmit their ID. This set initially includes all the selected tags.
- b) If more than one tag transmitted, the interrogator receives an erroneous response. The FAIL command shall be sent.
- c) All tags receiving a FAIL command with COUNT not equal to 0 shall to increment COUNT. That is, they move further away from being able to transmit.

All tags receiving FAIL a count of 0 (those that just transmitted) shall generate a random number. Those that roll a 1 shall increment COUNT and shall not transmit. Those that roll a 0 shall keep COUNT at 0 and shall send their UID again.

One of four possibilities now occurs:

- d) If more than one tag transmits the FAIL command, step b) repeats (Possibility 1).
- e) If all tags roll a 1, none transmits. The interrogator receives nothing. It sends the SUCCESS command. All the counters decrement, and the tags with a count of 0 transmit. Typically, this returns to step b) (Possibility 2).
- f) If only one tag transmits and the ID is received correctly, the interrogator shall send the DATA_READ command with the ID. If the DATA_READ command is received correctly, that tag shall move to the DATA_EXCHANGE state and shall transmit its data.

The interrogator shall send SUCCESS. All tags in the ID state shall decrement COUNT.

- g) If only one tag has a count of 1 and transmits, step e) or f) is repeated. If more than one tag transmits, step b) is repeated (Possibility 3).

- h) If only one tag transmits and the ID is received with an error, the interrogator shall send the RESEND command. If the ID is received correctly, step e) is repeated. If the ID is received again some variable number of times (this number can be set based on the level of error handling desired for the system), it is assumed that more than one tag is transmitting and step b) is repeated (Possibility 4).

6.3.6 Commands

Commands are divided into four functional groups:

- selection commands;
- identification commands;
- data transfer commands;
- multiple commands.

Further, commands have one of the following types:

- mandatory;
- optional;
- custom;
- proprietary.

6.3.6.1 Command types

All tags with the same IC manufacturer code and the same IC version number shall behave the same.

6.3.6.1.1 Mandatory

The command codes range from '00' to '0A', '0C', '15', '1E', '1F' and '20' to '3F'.

A mandatory command shall be supported by all tags that claim to be compliant. Interrogators which claim compliance shall support all mandatory commands.

6.3.6.1.2 Optional

The command codes range from '0B', '0D' to '0F', '11' to '13', '17' to '1C', '1D' and from '40' to '9F'.

Optional commands are commands that are specified within the International Standard. Interrogators shall be technically capable of performing all optional commands that are specified in the International Standard (although need not be set up to do so). Tags may or may not support optional commands. If an optional command is used, it shall be implemented in the manner specified in the International Standard.

If the tag does not support an optional command, it shall remain silent.

NOTE The commands whose code ranges from '17' to '1C' are optional and not essential to operate the tag. However, their support by the tag is recommended for appropriate performance. To reflect this, they are reported as "recommended" in [Table 13](#).

6.3.6.1.3 Custom

The command codes range from 'A0' to 'DF'.

Custom commands may be enabled by an International Standard, but they shall not be specified in that International Standard. A custom command shall not solely duplicate the functionality of any mandatory or optional command defined in the International Standard by a different method.

The only fields that can be customized are the parameters and the data fields.

Any custom command contains as its first parameter the IC manufacturer code. This allows IC manufacturers to implement custom commands without risking duplication of command codes and thus misinterpretation.

If the tag does not support a custom command, it shall remain silent.

6.3.6.1.4 Proprietary

The command codes are '10', '14', '16' and they range from 'E0' to 'FF'.

Proprietary commands may be enabled by an International Standard, but they shall not be specified in that International Standard. A proprietary command shall not solely duplicate the functionality of any mandatory or optional command defined in the International Standard by a different method.

These commands are used by IC and tag manufacturers for various purposes such as tests, programming of system information, etc. The IC manufacturer may at its option document them or not. It is allowed that these commands are disabled after IC and/or tag manufacturing.

6.3.6.2 Command codes and format

Table 13 — Command codes and format

Command code	Type	Command name	Parameters		
'00'	Mandatory	GROUP_SELECT_EQ	ADDRESS	BYTE_MASK	WORD_DATA
'01'	Mandatory	GROUP_SELECT_NE	ADDRESS	BYTE_MASK	WORD_DATA
'02'	Mandatory	GROUP_SELECT_GT	ADDRESS	BYTE_MASK	WORD_DATA
'03'	Mandatory	GROUP_SELECT_LT	ADDRESS	BYTE_MASK	WORD_DATA
'04'	Mandatory	GROUP_UNSELECT_EQ	ADDRESS	BYTE_MASK	WORD_DATA
'05'	Mandatory	GROUP_UNSELECT_NE	ADDRESS	BYTE_MASK	WORD_DATA
'06'	Mandatory	GROUP_UNSELECT_GT	ADDRESS	BYTE_MASK	WORD_DATA
'07'	Mandatory	GROUP_UNSELECT_LT	ADDRESS	BYTE_MASK	WORD_DATA
'08'	Mandatory	FAIL	None	None	None
'09'	Mandatory	SUCCESS	None	None	None
'0A'	Mandatory	INITIALIZE	None	None	None
'0B'	Optional	DATA_READ	ID	ADDRESS	None
'0C'	Mandatory	READ	ID	ADDRESS	None
'0D'	Recommended	WRITE	ID	ADDRESS	BYTE_DATA
'0E'	Recommended	WRITE_MULTIPLE	None	ADDRESS	BYTE_DATA
'0F'	Recommended	LOCK	ID	ADDRESS	None
'10'	Proprietary	IC manufacturer dependent			
'11'	Recommended	QUERY_LOCK	ID	ADDRESS	None
'12'	Recommended	READ_VERIFY	ID	ADDRESS	None
'13'	Recommended	MULTIPLE_UNSELECT	ADDRESS	BYTE_DATA	None
'14'	Proprietary	IC manufacturer dependent			
'15'	Mandatory	RESEND	None	None	None
'16'	Proprietary	IC manufacturer dependent			

Table 13 (continued)

Command code	Type	Command name	Parameters		
'17'	Recommended	GROUP_SELECT_EQ_FLAGS	None	BYTE_MASK	BYTE_DATA
'18'	Recommended	GROUP_SELECT_NE_FLAGS	None	BYTE_MASK	BYTE_DATA
'19'	Recommended	GROUP_UNSELECT_EQ_FLAGS	None	BYTE_MASK	BYTE_DATA
'1A'	Recommended	GROUP_UNSELECT_NE_FLAGS	None	BYTE_MASK	BYTE_DATA
'1B'	Recommended	WRITE4BYTE	ID	ADDRESS	BYTE_MASK
'1C'	Recommended	WRITE4BYTE_MULTIPLE	BYTE_MASK	ADDRESS	4BYTE_DATA
'1D'	Recommended	READ_VERIFY4BYTE	ID	ADDRESS	
'1E' to '1F'	Mandatory	RFU			
'20' to '3F'	Mandatory	RFU			
'40' to '9F'	Optional	RFU			
'A0' to 'DF'	Custom	IC manufacturer dependent			
'E0' to 'FF'	Proprietary	IC manufacturer dependent			

6.3.6.2.1 Command fields

The command fields are specified in [Table 14](#).

Table 14 — Command fields

Field name	Field size
COMMAND	1 byte
ADDRESS	1 byte
BYTE_MASK	1 byte
ID	8 bytes
WORD_DATA	8 bytes
BYTE_DATA	1 byte
4BYTE_DATA	4 bytes

6.3.6.2.2 Tag responses

The tag responses are specified in [Table 15](#).

Table 15 — Tag responses

Response code	Response name	Response size
'00'	ACKNOWLEDGE	1 byte
	ACKNOWLEDGE_NOK	1 byte
'01'	ACKNOWLEDGE_OK	1 byte
'FE'	ERROR_NOK	1 byte
'FF'	ERROR	1 byte
	ERROR_OK	1 byte

Table 15 (continued)

Response code	Response name	Response size
Not applicable	WORD_DATA	8 bytes
Not applicable	BYTE_DATA	1 byte
'02' to 'FD'	RFU	

6.3.6.2.3 Selection commands

Selection commands define a subset of tags in the field to be identified or written to and may be used as part of the collision arbitration.

6.3.6.2.3.1 Data comparison for selection command on memory

Each select command of the commands GROUP_SELECT_EQ, GROUP_SELECT_NE, GROUP_SELECT_GT, GROUP_SELECT_LT, GROUP_UNSELECT_EQ, GROUP_UNSELECT_NE, GROUP_UNSELECT_GT, GROUP_UNSELECT_LT has three arguments (parameter and data):

ADDRESS

BYTE_MASK

WORD_DATA

and the tag shall make one of four possible comparisons:

EQ M EQUAL D
 NE M NOT EQUAL D
 GT M GREATER THAN D
 LT M LOWER THAN D

The arguments of the comparison are

M7 MSB	M6	M5	M4	M3	M2	M1	M0 LSB
Tag memory content at ADDRESS+0	Tag memory content at ADDRESS+1	Tag memory content at ADDRESS+2	Tag memory content at ADDRESS+3	Tag memory content at ADDRESS+4	Tag memory content at ADDRESS+5	Tag memory content at ADDRESS+6	Tag memory content at ADDRESS+7

$$M = M0 + M1 \times 2^8 + M2 \times 2^{16} + M3 \times 2^{24} + M4 \times 2^{32} + M5 \times 2^{40} + M6 \times 2^{48} + M7 \times 2^{56}$$

and the argument of the command

D7 MSB	D6	D5	D4	D3	D2	D1	D0 LSB
First byte after command							Last byte after command

$$D = D0 + D1 \times 2^8 + D2 \times 2^{16} + D3 \times 2^{24} + D4 \times 2^{32} + D5 \times 2^{40} + D6 \times 2^{48} + D7 \times 2^{56}$$

The argument BYTE_MASK defines what bytes to be considered for comparison.

The data masking for Group Select and Group Unselect commands are specified in [Table 16](#).

Table 16 — Data masking for Group_Select and Group_Unselect commands

BYTE_MASK	WORD_DATA
Bit 7 (MSB) is set	Consider D7 and M7 for comparison
Bit 6 is set	Consider D6 and M6 for comparison
Bit 5 is set	Consider D5 and M5 for comparison
Bit 4 is set	Consider D4 and M4 for comparison
Bit 3 is set	Consider D3 and M3 for comparison
Bit 2 is set	Consider D2 and M2 for comparison
Bit 1 is set	Consider D1 and M1 for comparison
Bit 0 (LSB) is set	Consider D0 and M0 for comparison
Bit 7 (MSB) is cleared	Ignore D7 and M7 for comparison
Bit 6 is cleared	Ignore D6 and M6 for comparison
Bit 5 is cleared	Ignore D5 and M5 for comparison
Bit 4 is cleared	Ignore D4 and M4 for comparison
Bit 3 is cleared	Ignore D3 and M3 for comparison
Bit 2 is cleared	Ignore D2 and M2 for comparison
Bit 1 is cleared	Ignore D1 and M1 for comparison
Bit 0 (LSB) is cleared	Ignore D0 and M0 for comparison

6.3.6.2.3.2 Data comparison for selection command on flags

Each select command of the commands GROUP_SELECT_EQ_FLAGS, GROUP_SELECT_NE_FLAGS, GROUP_UNSELECT_EQ_FLAGS, GROUP_UNSELECT_NE_FLAGS has two arguments (parameter and data):

BYTE_MASK

BYTE_DATA

and the tag shall make of two possible comparisons:

EQ FLAGS EQUAL D

NE FLAGS NOT EQUAL D

The arguments of the comparison are FLAGS, as defined in [6.3.1.3](#), and the argument of the command D, consisting of the bits D7 (MSB) to D0 (LSB).

The argument BYTE_MASK defines what bits to be considered for comparison.

The data masking for Group_Select_Flags and Group_Unselect_Flags are specified in [Table 17](#).

Table 17 — Data masking for Group_Select_Flags and Group_Unselect_Flags

BYTE_MASK	BYTE_DATA
Bit 7 (MSB) is set	Consider D7 and FLAG7 for comparison
Bit 6 is set	Consider D6 and FLAG6 for comparison
Bit 5 is set	Consider D5 and FLAG5 for comparison
Bit 4 is set	Consider D4 and FLAG4 for comparison
Bit 3 is set	Consider D3 and FLAG3 for comparison
Bit 2 is set	Consider D2 and FLAG2 for comparison
Bit 1 is set	Consider D1 and FLAG1 for comparison
Bit 0 (LSB) is set	Consider D0 and FLAG0 for comparison

Table 17 (continued)

BYTE_MASK	BYTE_DATA
Bit 7 (MSB) is cleared	Ignore D7 and FLAG7 for comparison
Bit 6 is cleared	Ignore D6 and FLAG6 for comparison
Bit 5 is cleared	Ignore D5 and FLAG5 for comparison
Bit 4 is cleared	Ignore D4 and FLAG4 for comparison
Bit 3 is cleared	Ignore D3 and FLAG3 for comparison
Bit 2 is cleared	Ignore D2 and FLAG2 for comparison
Bit 1 is cleared	Ignore D1 and FLAG1 for comparison
Bit 0 (LSB) is cleared	Ignore D0 and FLAG0 for comparison

Formula describing the EQUAL function:

The EQUAL comparison passes if $(!B7 + (D7 = FLAG7)) * (!B6 + (D6 = FLAG6)) * (!B5 + (D5 = FLAG5)) * (!B4 + (D4 = FLAG4)) * (!B3 + (D3 = FLAG3)) * (!B2 + (D2 = FLAG2)) * (!B1 + (D1 = FLAG1)) * (!B0 + (D0 = FLAG0))$ is true.

Formula describing the UNEQUAL function:

The UNEQUAL comparison passes if $B7 * (D7 \neq FLAG7) + B6 * (D6 \neq FLAG6) + B5 * (D5 \neq FLAG5) + B4 * (D4 \neq FLAG4) + B3 * (D3 \neq FLAG3) + B2 * (D2 \neq FLAG2) + B1 * (D1 \neq FLAG1) + B0 * (D0 \neq FLAG0)$ is true.

6.3.6.2.3.3 GROUP_SELECT_EQ

Command code = '00'

On receiving a GROUP_SELECT_EQ command, a tag which is in the READY state shall read the 8-byte memory content beginning at the specified address and compare it with the WORD_DATA sent by the interrogator. In the case that the memory content is equal to the WORD_DATA, the tag shall set its internal counter COUNT to 0, read its UID and send back the UID, and go into the state ID.

On receiving a GROUP_SELECT_EQ command, a tag which is in the ID state shall set its internal counter COUNT to 0, read its UID and send back the UID, and stay in the ID state.

In all other cases, the tag shall not send a reply.

The GROUP_SELECT_EQ command is specified in [Table 18](#).

The GROUP_SELECT_EQ response in the case of NO error is specified in [Table 19](#).

Table 18 — GROUP_SELECT_EQ command

Preamble	Delimiter	COMMAND	ADDRESS	MASK	WORD_DATA	CRC
		8 bits	8 bits	8 bits	64 bits	16 bits

Table 19 — GROUP_SELECT_EQ response in the case of NO error

Preamble	ID	CRC
	64 bits	16 bits

NOTE If the byte mask is zero, GROUP_SELECT_EQ selects all tags.

6.3.6.2.3.4 GROUP_SELECT_NE

Command code = '01'

On receiving a GROUP_SELECT_NE command, a tag which is in the READY state shall read the 8-byte memory content beginning at the specified address and compare it with the WORD_DATA sent by the interrogator. In the case that the memory content is not equal to the WORD_DATA, the tag shall set its internal counter COUNT to 0, read its UID and send back the UID, and go into the state ID.

On receiving a GROUP_SELECT_NE command, a tag which is in the ID state shall set its internal counter COUNT to 0, read its UID and send back the UID, and stay in the ID state.

In all other cases, the tag shall not send a reply.

The GROUP_SELECT_NE command is specified in [Table 20](#).

The GROUP_SELECT_NE response in the case of NO error is specified in [Table 21](#).

Table 20 — GROUP_SELECT_NE command

Preamble	Delimiter	COMMAND	ADDRESS	BYTE_MASK	WORD_DATA	CRC
		8 bits	8 bits	8 bits	64 bits	16 bits

Table 21 — GROUP_SELECT_NE response in the case of NO error

Preamble	ID	CRC
	64 bits	16 bits

6.3.6.2.3.5 GROUP_SELECT_GT

Command code = '02'

On receiving a GROUP_SELECT_GT command, a tag which is in the READY state shall read the 8-byte memory content beginning at the specified address and compare it with the WORD_DATA sent by the interrogator. In the case that the memory content is greater than the WORD_DATA, the tag shall set its internal counter COUNT to 0, read its UID and send back the UID, and go into the state ID.

On receiving a GROUP_SELECT_GT command, a tag which is in the ID state shall set its internal counter COUNT to 0, read its UID and send back the UID, and stay in the ID state.

In all other cases, the tag shall not send a reply.

The GROUP_SELECT_GT command is specified in [Table 22](#).

The GROUP_SELECT_GT response in the case of NO error is specified in [Table 23](#).

Table 22 — GROUP_SELECT_GT command

Preamble	Delimiter	COMMAND	ADDRESS	MASK	WORD_DATA	CRC
		8 bits	8 bits	8 bits	64 bits	16 bits

Table 23 — GROUP_SELECT_GT response in the case of NO error

Preamble	ID	CRC
	64 bits	16 bits

6.3.6.2.3.6 GROUP_SELECT_LT

Command code = '03'

On receiving a GROUP_SELECT_LT command, a tag which is in the READY state shall read the 8-byte memory content beginning at the specified address and compare it with the WORD_DATA sent by the interrogator. In the case that the memory content is lower than the WORD_DATA, the tag shall set its

internal counter COUNT to 0, read its UID and send back the UID and go into the state ID, and stay in the ID state.

On receiving a GROUP_SELECT_LT command, a tag which is in the ID state shall set its internal counter COUNT to 0, read its UID and send back the UID, and stay in the ID state.

In all other cases, the tag shall not send a reply.

The GROUP_SELECT_LT command is specified in [Table 24](#).

The GROUP_SELECT_LT response is specified in [Table 25](#).

Table 24 — GROUP_SELECT_LT command

Preamble	Delimiter	COMMAND	ADDRESS	BYTE_MASK	WORD_DATA	CRC
		8 bits	8 bits	8 bits	64 bits	16 bits

Table 25 — GROUP_SELECT_LT response

Preamble	ID	CRC
	64 bits	16 bits

6.3.6.2.3.7 GROUP_UNSELECT_EQ

Command code = '04'

On receiving a GROUP_UNSELECT_EQ command, a tag which is in the ID state shall read the 8-byte memory content beginning at the specified address and compare it with the WORD_DATA sent by the interrogator. In the case that the memory content is equal to the WORD_DATA, the tag shall go into the state READY and not send any reply. In the case that the comparison fails, the tag shall set its internal counter COUNT to 0, read its UID and send back the UID, and shall stay in the ID state.

In all other cases, the tag shall not send a reply.

The GROUP_UNSELECT_EQ command is specified in [Table 26](#).

The GROUP_UNSELECT_EQ response is specified in [Table 27](#).

Table 26 — GROUP_UNSELECT_EQ command

Preamble	Delimiter	COMMAND	ADDRESS	BYTE_MASK	WORD_DATA	CRC
		8 bits	8 bits	8 bits	64 bits	16 bits

Table 27 — GROUP_UNSELECT_EQ response

Preamble	ID	CRC
	64 bits	16 bits

NOTE If the byte mask is zero, GROUP_UNSELECT_EQ unselects all tags.

6.3.6.2.3.8 GROUP_UNSELECT_NE

Command code = '05'

On receiving a GROUP_UNSELECT_NE command, a tag which is in the ID state shall read the 8-byte memory content beginning at the specified address and compare it with the WORD_DATA sent by the interrogator. In the case that the memory content is not equal to the WORD_DATA, the tag shall go into the state READY and not send any reply. In the case the comparison fails, the tag shall set its internal counter COUNT to 0, read its UID and send back the UID, and shall stay in the ID state.

In all other cases, the tag shall not send a reply.

The GROUP_UNSELECT_NE command is specified in [Table 28](#).

The GROUP_UNSELECT_NE response is specified in [Table 29](#).

Table 28 — GROUP_UNSELECT_NE command

Preamble	Delimiter	COMMAND	ADDRESS	BYTE_MASK	WORD_DATA	CRC
		8 bits	8 bits	8 bits	64 bits	16 bits

Table 29 — GROUP_UNSELECT_NE response

Preamble	ID	CRC
	64 bits	16 bits

6.3.6.2.3.9 GROUP_UNSELECT_GT

Command code = '06'

On receiving a GROUP_UNSELECT_GT command, a tag which is in the ID state shall read the 8-byte memory content beginning at the specified address and compare it with the WORD_DATA sent by the interrogator. In the case that the memory content is greater than the WORD_DATA, the tag shall go into the state READY and not send any reply. In the case that the comparison fails, the tag shall set its internal counter COUNT to 0, read its UID and send back the UID, and shall stay in the ID state.

In all other cases, the tag shall not send a reply.

The GROUP_UNSELECT_GT response is specified in [Table 30](#).

The GROUP_UNSELECT_GT response in the case of NO error and comparison fails is specified in [Table 31](#).

Table 30 — GROUP_UNSELECT_GT command

Preamble	Delimiter	COMMAND	ADDRESS	BYTE_MASK	WORD_DATA	CRC
		8 bits	8 bits	8 bits	64 bits	16 bits

Table 31 — GROUP_UNSELECT_GT response in the case of NO error and comparison fails

Preamble	ID	CRC
	64 bits	16 bits

6.3.6.2.3.10 GROUP_UNSELECT_LT

Command code = '07'

On receiving a GROUP_UNSELECT_LT command, a tag which is in the ID state shall read the 8-byte memory content beginning at the specified address and compare it with the WORD_DATA sent by the interrogator. In the case that the memory content is lower than the WORD_DATA, the tag shall go into the state READY and not send any reply. In the case that the comparison fails, the tag shall set its internal counter COUNT to 0, read its UID and send back the UID, and shall stay in the ID state.

In all other cases, the tag shall not send a reply.

The GROUP_UNSELECT_LT command is specified in [Table 32](#).

The GROUP_UNSELECT_LT response is specified in [Table 33](#).

Table 32 — GROUP_UNSELECT_LT command

Preamble	Delimiter	COMMAND	ADDRESS	BYTE_MASK	WORD_DATA	CRC
		8 bits	8 bits	8 bits	64 bits	16 bits

Table 33 — GROUP_UNSELECT_LT response

Preamble	ID	CRC
	64 bits	16 bits

6.3.6.2.3.11 MULTIPLE_UNSELECT

Command code = '13'

On receiving a MULTIPLE_UNSELECT command, a tag which is in the ID state shall read the 1-byte memory content beginning at the specified address and compare it with the BYTE_DATA sent by the interrogator. In the case that the memory content is equal to the BYTE_DATA and the flag WRITE_OK is set, then the tag shall go into the state READY and not send any reply. In the case that the comparison fails, the tag shall set its internal counter COUNT to 0, read its UID and send back the UID, and shall stay in the ID state.

In all other cases, the tag shall not send a reply.

The MULTIPLE_UNSELECT command is specified in [Table 34](#).

The MULTIPLE_UNSELECT response is specified in [Table 35](#).

Table 34 — MULTIPLE_UNSELECT command

Preamble	Delimiter	COMMAND	ADDRESS	BYTE_DATA	CRC
		8 bits	8 bits	8 bits	16 bits

Table 35 — MULTIPLE_UNSELECT response

Preamble	ID	CRC
	64 bits	16 bits

This command may be used to unselect all tags that had a successful write, while tags that had a weak write or write problems stay selected.

6.3.6.2.3.12 GROUP_SELECT_EQ_FLAGS

Command code = '17'

On receiving a GROUP_SELECT_EQ_FLAGS command, a tag which is in the READY state shall compare the FLAGS with the BYTE_DATA sent by the interrogator. In the case that the FLAGS are equal to the BYTE_DATA, the tag shall set its internal counter COUNT to 0, read its UID and send back the UID, and go into the state ID.

On receiving a GROUP_SELECT_EQ_FLAGS command, a tag which is in the ID state shall set its internal counter COUNT to 0, read its UID and send back the UID, and stay in the ID state.

In all other cases, the tag shall not send a reply.

The GROUP_SELECT_EQ_FLAGS command is specified in [Table 36](#).

The GROUP_SELECT_EQ_FLAGS response is specified in [Table 37](#).

Table 36 — GROUP_SELECT_EQ_FLAGS command

Preamble	Delimiter	COMMAND	BYTE_MASK	BYTE_DATA	CRC
		8 bits	8 bits	8 bits	16 bits

Table 37 — GROUP_SELECT_EQ_FLAGS response

Preamble	ID	CRC
	64 bits	16 bits

NOTE If the byte mask is zero, GROUP_SELECT_EQ_FLAGS selects all tags.

6.3.6.2.3.13 GROUP_SELECT_NE_FLAGS

Command code = '18'

On receiving a GROUP_SELECT_NE_FLAGS command, a tag which is in the READY state shall compare the FLAGS with the BYTE_DATA sent by the interrogator. In the case that the FLAGS are not equal to the BYTE_DATA, the tag shall set its internal counter COUNT to 0, read its UID and send back the UID, and go into the state ID.

On receiving a GROUP_SELECT_NE_FLAGS command, a tag which is in the ID state shall set its internal counter COUNT to 0, read its UID and send back the UID, and stay in the ID state.

In all other cases, the tag shall not send a reply.

The GROUP_SELECT_NE_FLAGS command is specified in [Table 38](#).

The GROUP_SELECT_NE_FLAGS response is specified in [Table 39](#).

Table 38 — GROUP_SELECT_NE_FLAGS command

Preamble	Delimiter	COMMAND	BYTE_MASK	BYTE_DATA	CRC
		8 bits	8 bits	8 bits	16 bits

Table 39 — GROUP_SELECT_NE_FLAGS response

Preamble	ID	CRC
	64 bits	16 bits

6.3.6.2.3.14 GROUP_UNSELECT_EQ_FLAGS

Command code = '19'

On receiving a GROUP_UNSELECT_EQ_FLAGS command, a tag which is in the ID state shall compare the FLAGS with the BYTE_DATA sent by the interrogator. In the case that the FLAGS are equal to the BYTE_DATA, the tag shall go into the state READY and not send any reply. In the case that the comparison fails, the tag shall set its internal counter COUNT to 0, read its UID and send back the UID, and shall stay in the ID state.

In all other cases, the tag shall not send a reply.

The GROUP_UNSELECT_EQ_FLAGS command is specified in [Table 40](#).

The GROUP_UNSELECT_EQ_FLAGS response is specified in [Table 41](#).

Table 40 — GROUP_UNSELECT_EQ_FLAGS command

Preamble	Delimiter	COMMAND	BYTE_MASK	BYTE_DATA	CRC
		8 bits	8 bits	8 bits	16 bits

Table 41 — GROUP_UNSELECT_EQ_FLAGS response

Preamble	ID	CRC
	64 bits	16 bits

NOTE If the byte mask is zero, GROUP_UNSELECT_EQ_FLAGS unselects all tags.

6.3.6.2.3.15 GROUP_UNSELECT_NE_FLAGS

Command code = '1A'

On receiving a GROUP_UNSELECT_NE_FLAGS command, a tag which is in the ID state shall compare the FLAGS with the BYTE_DATA sent by the interrogator. In the case that the FLAGS are not equal to the BYTE_DATA, the tag shall go into the state READY and not send any reply. In the case that the comparison fails, the tag shall set its internal counter COUNT to 0, read its UID and send back the UID, and shall stay in the ID state.

In all other cases, the tag shall not send a reply.

The GROUP_UNSELECT_NE_FLAGS command is specified in [Table 42](#).

The GROUP_UNSELECT_NE_FLAGS response is specified in [Table 43](#).

Table 42 — GROUP_UNSELECT_NE_FLAGS command

Preamble	Delimiter	COMMAND	BYTE_MASK	BYTE_DATA	CRC
		8 bits	8 bits	8 bits	16 bits

Table 43 — GROUP_UNSELECT_NE_FLAGS response

Preamble	ID	CRC
	64 bits	16 bits

6.3.6.2.4 Identification commands

Identification commands are used to perform to run the multiple tag identification protocol.

6.3.6.2.4.1 FAIL

Command code = '08'

The identification algorithm uses FAIL when more than one tag tried to identify itself at the same time. Some tags back off and some tags retransmit.

A tag shall only accept a FAIL command if it is in the ID state. In the case that its internal counter COUNT is not zero or the random generator result is 1, then COUNT shall be increased by 1, unless it is FF.

If the resulting COUNT value is 0, then the tag shall read its UID and send it back in the response.

The FAIL command is specified in [Table 44](#).

The FAIL response is specified in [Table 45](#).

Table 44 — FAIL command

Preamble	Delimiter	COMMAND	CRC
		8 bits	16 bits

Table 45 — FAIL response

Preamble	ID	CRC
	64 bits	16 bits

6.3.6.2.4.2 SUCCESS

Command code = '09'

SUCCESS initiates identification of the next set of tags. It is used in two cases:

- When all tags receiving FAIL backed off and did not transmit, SUCCESS causes those same tags to transmit again.
- After, for example, a DATA_READ moves an identified tag to DATA_EXCHANGE, SUCCESS causes the next subset of selected but unidentified tags to transmit.

A tag shall only accept a SUCCESS command if it is in the ID state. In the case that its internal counter COUNT is not zero, it shall be decreased by 1.

If the resulting COUNT value is 0, then the tag shall read its UID and send it back in the response.

The SUCCESS command is specified in [Table 46](#).

The SUCCESS response is specified in [Table 47](#).

Table 46 — SUCCESS command

Preamble	Delimiter	COMMAND	CRC
		8 bits	16 bits

Table 47 — SUCCESS response

Preamble	ID	CRC
	64 bits	16 bits

6.3.6.2.4.3 RESEND

Command code = '15'

The identification algorithm uses RESEND when only one tag transmitted but the UID was received in error. The tag that transmitted resends its UID.

A tag shall only accept a RESEND command if it is in the ID state. If the COUNT value is 0, then the tag shall read its UID and send it back in the response.

The RESEND command is specified in [Table 48](#).

The RESEND response is specified in [Table 49](#).

Table 48 — RESEND command

Preamble	Delimiter	COMMAND	CRC
		8 bits	16 bits

Table 49 — RESEND response

Preamble	ID	CRC
	64 bits	16 bits

6.3.6.2.4.4 INITIALIZE

Command code = '0A'

On receiving an INITIALIZE command, a tag shall go into the READY state and reset the Data_Exchange_Status_Bit.

It shall not send any response.

The INITIALIZE command is specified in [Table 50](#).

Table 50 — INITIALIZE command

Preamble	Delimiter	COMMAND	CRC
		8 bits	16 bits

6.3.6.2.5 Data Transfer commands

Data Transfer commands are used to read or write data from or to the tag memory.

For memory lock functionality, a tag shall provide the opportunity to mark an address lockable. An ADDRESS is marked lockable by commands as described in this clause. No ADDRESS shall be marked lockable after the tag has been in the POWER-OFF state. A tag shall not support more than one ADDRESS to be marked lockable at the same time.

6.3.6.2.5.1 READ

Command code = '0C'

On receiving the READ command, the tag shall compare the sent ID with its UID. In the case that the ID is equal to the UID, the tag shall from any state move to the DATA_EXCHANGE state, read the 8-byte memory content beginning at the specified address and send back its content in the response. In the case that the ID is not equal to the UID or any other error, the tag shall not send a reply. Further, the tag makes the byte of ADDRESS lockable.

The address is numbered from '00' to 'FF' (0 to 255).

The Read command is specified in [Table 51](#).

The Read response is specified in [Table 52](#).

Table 51 — Read command

Preamble	Delimiter	COMMAND	ID	ADDRESS	CRC
		8 bits	64 bits	8 bits	16 bits

Table 52 — Read response

Preamble	WORD_DATA	CRC
	64 bits	16 bits

6.3.6.2.5.2 DATA_READ

Command code = '0B'