INTERNATIONAL STANDARD

ISO/IEC 18000-7

Fourth edition
2014-09-01

Information technology — Radio frequency identification for item management —

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

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

Partie 7: Paramètres de communications actives d'une interface radio à 433 MHz

Reference number
ISO/IEC 18000-7:2014(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

This fourth edition cancels and replaces the third edition (ISO/IEC 18000-7:2009), which has been technically revised and extended.

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

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

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

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

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

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

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

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

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

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

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

Introduction

This part of ISO/IEC 18000 is intended to address radio frequency identification (RFID) devices operating in the 433 MHz frequency band, providing an air interface implementation for wireless, non-contact information system equipment for item management applications. Typical applications operate at ranges greater than one metre.

The RFID system includes a host system and RFID equipment (interrogator and tags). The host system runs an application program, which controls interfaces with the RFID equipment. The RFID equipment is 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 serial 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 RF communication range. 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. This system uses an active tag.

RFID systems defined by this part of ISO/IEC 18000 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.

This part of ISO/IEC 18000 consists of two modes, Base and Extended. The following simplified differences should be drawn between the two modes:

— Base Mode defined in clause 6 is backwards compatible and includes all features described in the last revision of this part of ISO/IEC 18000 (ISO/IEC 18000-7:2009) with the addition of security features as described in clause 6.7.

— Extended Mode defined in clause 7 is new to this part of ISO/IEC 18000. Extended Mode presents a new communication protocol stack (PHY, MAC and Application layers) and provides an extended feature set that addresses more complex user and deployment requirements.

Substantive differences exist between Base Mode and Extended Mode across all layers of the communication protocol (PHY, MAC and Application). However, both modes may co-exist in any given physical environment.

All parties are directed to consider carefully their use model before determining the most appropriate mode.

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

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

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

Information on the declared patents may be obtained from:

Patent Holder: Legal Name CISC Semiconductor GmbH Contact for license application: Name & Department Markus Pistauer, CEO Address Lakeside B07 Address 9020 Klagenfurt, Austria Tel. +43(463) 508 808 Fax +43(463) 508 808-18 E-mail m.pistauer@cisc.at URL (optional) www.cisc.at
Patent Holder: Legal Name Impinj, Inc. Contact for license application: Name & Department Stacy Jones Address 701 N 34th Street, Suite 300 Address 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

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

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

Information technology — Radio frequency identification for item management —

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

1 Scope

This part of ISO/IEC 18000 defines the air interface for radio frequency identification (RFID) devices operating as an active RF tag in the 433 MHz band used in item management applications. It provides a common technical specification for RFID devices that can be used by ISO technical committees developing RFID application standards. This part of ISO/IEC 18000 is intended to allow for compatibility and to encourage inter-operability of products for the growing RFID market in the international marketplace. This part of ISO/IEC 18000 defines the forward and return link parameters for technical attributes including, but not limited to, operating frequency, operating channel accuracy, occupied channel bandwidth, maximum power, 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 part of ISO/IEC 18000 further defines the communications protocol used in the air interface.

2 Conformance

The rules for evaluation of RFID device conformity to this part of ISO/IEC 18000 are defined in ISO/IEC TR 18047-7.

2.1 RF emissions general population

Device manufacturers claiming conformance to this part of ISO/IEC 18000 shall declare on their own responsibility that RF emissions do not exceed the maximum permitted exposure limits recommended by either IEEE C95.1:2005 or ICNIRP according to IEC 62369-1. If a device manufacturer is unsure which recommendation is to be cited for compliance, the manufacturer shall declare on their own responsibility to ICNIRP limits.

2.2 RF emissions and susceptibility health care setting

Device manufacturers claiming conformance to this part of ISO/IEC 18000 shall declare on their own responsibility that RF emissions and susceptibility comply with IEC 60601-1-2.

2.3 Command structure and extensibility

This part of ISO/IEC 18000 includes a definition of the structure of command codes between an interrogator and a tag and indicates how many positions are available for future extensions.

Command specification clauses provide a full definition of the command and its presentation.

Each command is labelled as being “mandatory” or “optional”.

The clauses of this part of ISO/IEC 18000 make provisions for “custom” and “proprietary” commands.

2.4 Mandatory commands

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

2.5 Optional commands

Optional commands are commands that are specified as such within this part of ISO/IEC 18000. Interrogators shall be technically capable of performing all optional commands that are specified in this part of ISO/IEC 18000 (although they 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 this part of ISO/IEC 18000.

2.6 Custom commands

Custom commands may be permitted by those applying this part of ISO/IEC 18000, but they are not specified in this part of ISO/IEC 18000.

A custom command shall not solely duplicate the functionality of any mandatory or optional command defined in this part of ISO/IEC 18000 by a different method. An interrogator shall use a custom command only in accordance with the specifications of the tag manufacturer.

2.7 Proprietary commands

Proprietary commands may be permitted by those applying this part of ISO/IEC 18000, but they are not specified in this part of ISO/IEC 18000.

A proprietary command shall not solely duplicate the functionality of any mandatory or optional command defined in this part of ISO/IEC 18000 by a different method. All proprietary commands shall be disabled before the tag leaves the tag manufacturer. Proprietary commands are intended for manufacturing purposes and shall not be used in field-deployed RFID systems.

3 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 8859-1, *Information technology — 8-bit single-byte coded graphic character sets — Part 1: Latin alphabet No. 1*

ISO/IEC 15459 (all parts), *Information technology — Unique identifiers*

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

ISO/IEC TR 18047-7, *Information technology — Radio frequency identification device conformance test methods — Part 7: Test methods for active air interface communications at 433 MHz*

ISO/IEC 19762-1, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary — Part 1: General terms relating to AIDC*

ISO/IEC 19762-3, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary — Part 3: Radio frequency identification (RFID)*

IEC 62369-1, *Ed. 1.0, Evaluation of human exposure to electromagnetic fields from short range devices (SRDs) in various applications over the frequency range 0 GHz to 300 GHz — Part 1: Fields produced by devices used for electronic article surveillance, radio frequency identification and similar systems*

IEC 60601-1-2, *Medical electrical equipment — Part 1-2: General requirements for basic safety and essential performance — Collateral standard: Electromagnetic compatibility — Requirements and tests*

ICNIRP Guidelines, *Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields (up to 300 GHz), International Commission on Non-Ionizing Radiation Protection*

IEEE C95.1:2005, *IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz*

IEEE Std 802.15.4, *IEEE Standard for Local and metropolitan area networks Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762-1 and ISO/IEC 19762-3 apply.

5 Symbols and abbreviated terms

For the purposes of this document, all symbols and abbreviated terms given in ISO/IEC 19762-1 and ISO/IEC 19762-3 shall apply.

AES	Advanced Encryption Standard
AES-CBC	Advanced Encryption Standard – Cipher Block Chaining
HMAC	Hash-based Message Authentication Code
LR-WPAN	Low-Rate Wireless Personal Area Network
PKI	Public Key Infrastructure
PMK	Pairwise Master Key
PSK	Pre-shared Key
SHA-1	Secure Hash Algorithm – 1
HB2-128	Hummingbird2 128-bit key cipher

6 433,92 MHz active narrowband specification

6.1 Physical layer

The RF communication link between interrogator and tag shall utilize a narrow band UHF frequency with the following nominal characteristics:

Carrier Frequency	433,92 MHz
Modulation Type	FSK
Frequency Deviation	+/- 50 kHz
Symbol LOW	fc +50 kHz
Symbol HIGH	fc -50 kHz

Data Modulation Rate	27,7 kHz
Wake up Signal	Modulation with 31,25 kHz square wave signal followed by modulation with 10 kHz square wave signal

For detailed physical layer specifications, see section 6.6.

The Wake Up Signal shall be transmitted by the interrogator for a minimum of 2,45 seconds to wake up all tags within communication range. The Wake Up Signal shall consist of a 2,35 to 4,8-second 31,25 kHz square wave modulated signal called the "Wake Up Header" immediately followed by a 0,1-second 10 kHz square wave modulated signal called the "Co-Header." Upon detection and by completion of the Wake Up Signal all tags shall enter into the Ready state awaiting a command from the interrogator. See Figure 1. A tag has two states, awake/ready and asleep. During the ready state, the tags will accept the valid commands from interrogators and respond accordingly. When the tag is asleep, it will ignore all commands.

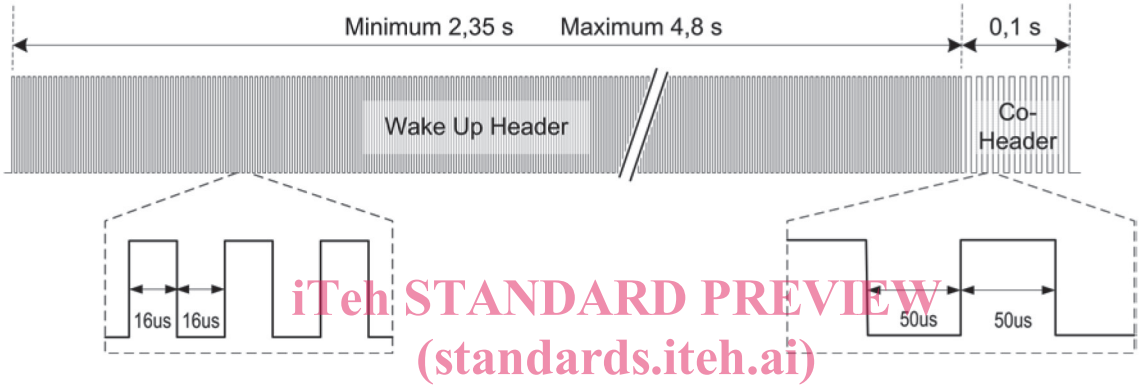


Figure 1 — Wake Up Signal

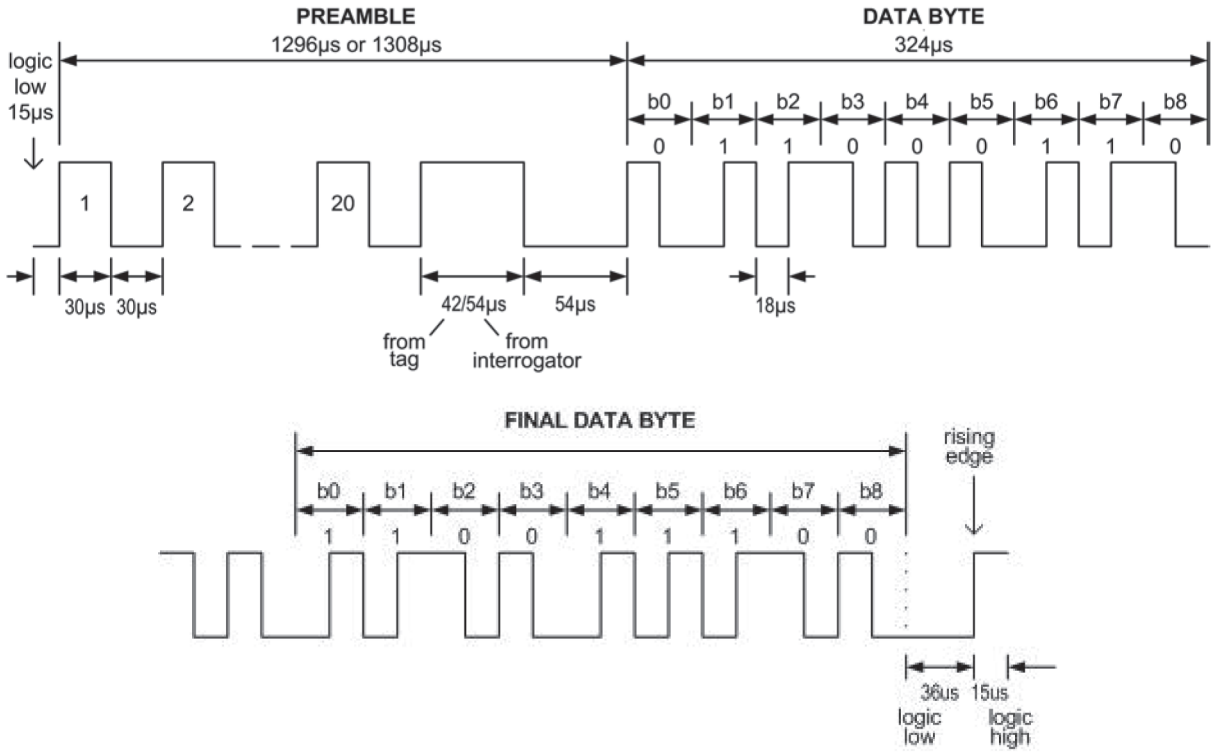
Once awoken, the tag shall stay awake for a minimum of 30 seconds after receipt of the last well-formed message packet consisting of a valid Protocol ID, command code, and CRC values, unless the interrogator otherwise commands the tag to sleep. If no well-formed command message is received within the 30 seconds, the tag will transition to the sleep state and SHALL no longer respond to command messages from Interrogators.

The communication between interrogator and tag shall be of the Master-Slave type, where the interrogator shall initiate communications and then listen for a response from a tag. Multiple response transmissions from tags shall be controlled by the collection algorithm described in 6.4.

6.2 Data Link layer

6.2.1 General

Data between interrogator and tag shall be transmitted in packet format. A packet shall be comprised of a preamble, data bytes and a final end period. The last two level changes of the preamble shall indicate the end of the preamble and beginning of the first data byte. The same two level changes of the preamble also indicate the originator of the data packet. Data bytes shall be sent in Manchester code format. Transmission order shall be most significant byte first; within a byte, the order shall be least significant bit first. Figure 2 illustrates the logic levels for the data communication timing of the preamble and the first byte of a packet.



NOTE Data byte transmitted order is most significant byte first; within each byte the order is least significant bit first. A 15 µs logic low level precedes the first preamble cycle. Byte shown is code 0xC6.

Figure 2 — Data communication timing

6.2.2 Preamble

The preamble shall be comprised of twenty (20) cycles of 60 µs period, 30 µs high and 30 µs low, followed by two final level changes which identifies the communication direction: 42 µs high, 54 µs low (tag to interrogator); or 54 µs high, 54 µs low (interrogator to tag). Refer to Figure 2 above.

6.2.3 Data bytes

Data bytes shall be in Manchester code format, each byte is comprised of 8 data bits and one stop bit. The bit period shall be 36 µs, the total byte period shall be 324 µs. A falling edge in the centre of the bit-time indicates a 0 bit, a rising edge indicates a 1 bit. The stop bit is coded as a zero bit.

6.2.4 Packet end period

A final period of 36 µs of continuous logic low, followed by a logic low to logic high transition, followed by continuous logic high for a minimum of 15 µs shall be transmitted after the last Manchester encoded bit within the packet.

6.2.5 Interrogator-to-tag message format

Tags shall recognize the interrogator-to-tag message format described in Table 1 and Table 2:

Table 1 — Interrogator-to-tag command format (broadcast)

Protocol ID	Packet Options	Packet Length	Session ID	Command Code	Command Arguments	CRC
0x40	1 byte	1 byte	2 bytes	1 byte	N bytes	2 bytes

Table 2 — Interrogator-to-tag command format (point-to-point)

Protocol ID	Packet Options	Packet Length	Tag Manufacturer ID	Tag Serial Number	Session ID	Command Code	Command Arguments	CRC
0x40	1 byte	1 byte	2 bytes	4 bytes	2 Bytes	1 byte	N bytes	2 bytes

See Annex A for other alternative application specific standards, which are identified with their respective Protocol ID.

6.2.5.1 Protocol ID

The protocol ID field allows different application standards based on this part of ISO/IEC 18000 ("derived application standards") to be developed. All derived application standards shall share the same physical layer protocols, but their command/response structure/field and command sets may vary depending on the application. The three basic commands ("Collection with Universal Data Block", "Sleep" and "Sleep All But") defined in this part of ISO/IEC 18000 shall be supported by all derived application standards. All other commands required by this part of ISO/IEC 18000 shall be supported by this part of ISO/IEC 18000 compliant products, but not necessarily by products compliant with derived application standards.

When the interrogator sends out a Wake Up Signal all tags based on the air interface of this part of ISO/IEC 18000 and derived standards shall wake up.

The interrogator may send out various commands as specified by the application. In the event that the interrogator wants to inventory all the active tags within its range, it shall send out a Collection command as defined in this part of ISO/IEC 18000. All tags adhering to this part of ISO/IEC 18000 or derived application standards shall respond to this basic Collection command. A tag shall respond with the collection response defined by the tag's own application data link layer standard (this part of ISO/IEC 18000 or derived standard). The tags shall also accept the Sleep commands ("Sleep" and "Sleep All But") defined in this part of ISO/IEC 18000. The co-existence of this part of ISO/IEC 18000 and derived standards is illustrated in Annex A.

6.2.5.2 Packet Options

Table 3 — Packet options field

Bit							
7	6	5	4	3	2	1	0
Reserved	Reserved	Reserved	Reserved	Reserved	1[a]	0= Broadcast (Tag serial number and Tag manufacturer ID not present) 1= Point to Point (Tag serial number and tag manufacturer ID present)	Reserved

[a] Bit 2 of the "packet oiptions field" has a fixed value of "1" for backwards compatibility.

The Packet Options field, described in Table 3, shall be used to indicate the presence of the Tag serial number and Tag manufacturer ID fields within the command message (packet). As indicated in Table 4, a particular command can be point-to-point or broadcast. The command type is indicated as follows:

— Point-to-point only, Packet Option field Bit 1 must be set to 1.

— Broadcast only and Packet Option field Bit 1 must be set to 0.

Reserved bits are for future use. The default value shall be “0”.

6.2.5.3 Packet Length

The packet length field shall be used to indicate the full length of the message in bytes, from the Protocol ID up to and including the CRC field.

6.2.5.4 Tag Manufacturer ID

The Tag Manufacturer ID is a unique identifier that is issued to each tag manufacturer. The Tag Manufacturer ID is a 16-bit code assigned by the Registration Authority as called out in ISO/IEC 15963. This 16-bit code is a combination of the ISO/IEC 15963 Allocation Class “0001 0001” (most significant byte) and the 8-bit Issuer UID “xxxxxxxx” (least significant byte). For example, if the Issuer UID is assigned as 00000100, the Tag Manufacturer ID would be 00010001 00000100.

The Tag Manufacturer ID format and content shall follow the requirements of unique identifiers as defined in ISO/IEC 15459-1.

The structure and allocation of the Tag Manufacturer ID is described in ISO/IEC 15963 and INCITS 256.

6.2.5.5 Tag Serial Number

The Tag Serial Number is a 32-bit integer that is uniquely assigned to each individual tag during manufacturing. This number cannot be changed and is read only. The Tag Serial Number has no structure and does not contain any information besides uniquely identifying a tag. The Tag Serial Number cannot be reused. Issuance of Tag Serial Numbers may be managed and administered by each manufacturer. The Tag Manufacturer ID and Tag Serial Number together uniquely identify a tag as defined in ISO/IEC 15963. This six-byte combination includes the two-byte Tag Manufacturer ID followed by the Tag Serial Number. An example of the combined data structure for Tag Manufacturer ID and Tag Serial Number is:

00010001 00000100 xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx

6.2.5.6 Session ID

The Session ID is a 16-bit integer value that uniquely identifies an interrogator from any other interrogator compliant with this part of ISO/IEC 18000 in the local vicinity. The Session ID of an individual interrogator may be changed without restriction, but its value shall be set to a value not in use by other interrogators compliant with this part of ISO/IEC 18000 in the local vicinity. No two interrogators compliant with this part of ISO/IEC 18000 within RF range of the same tag shall have the same Session ID. At the moment the Session ID is changed in an interrogator, any ongoing communication between that interrogator and any tag shall be terminated. An interrogator that receives a tag message containing a Session ID not equal to its own Session ID shall not transmit any packets over the UHF interface regarding the contents of the tag message. The Session ID 0x0000 is reserved and shall not be used.

6.2.5.7 Command Codes

The Command codes and their function as a Read and/or Write command shall be as listed in Table 4, below. Codes not identified are reserved.

Table 4 — Command codes

Command code + Sub Command Code (R/W)	Command name	Command type	Mandatory/Optional		Description
			Interrogator	Tag	
0x1F / NA	Collection with Universal Data Block	Broadcast	Mandatory	Mandatory	Collects all Tag IDs and Universal Data Block
NA / 0x15	Sleep	Point to Point	Mandatory	Mandatory	Puts tag to sleep
NA / 0x16	Sleep All But	Broadcast	Mandatory	Mandatory	Puts all tags but one to sleep
0x13 / 0x93	User ID	Point to Point	Mandatory	Optional	Sets user assigned ID (1 – 60 bytes)
0x09 / 0x89	Routing Code	Point to point	Mandatory	Mandatory	Reads and writes routing code
0x0C / NA	Firmware Version	Point to Point	Mandatory	Optional	Retrieves manufacturer-defined tag firmware revision number
0x0E / NA	Model Number	Point to Point	Mandatory	Optional	Retrieves manufacturer-defined tag model number
0x60 / 0xE0	Read/Write Memory	Point to Point	Mandatory	Optional	Reads and writes user memory
NA / 0x95	Set Password	Point to Point	Mandatory	Optional	Sets tag password (4 bytes long)
NA / 0x97	Set Password Protect Mode	Point to Point	Mandatory	Optional	Engages/disengages password protection (see section 6.3.4)
NA/ 0x96	Unlock	Point to Point	Mandatory	Optional	Unlocks password protected tag
0x70 / NA	Read Universal Data Block	Point to Point	Mandatory	Mandatory	Reads the Universal Data Block
0x26+0x01	Table Create	Point to Point	Mandatory	Optional	Creates a database table
0x26+0x02	Table Add Records	Point to Point	Mandatory	Optional	Prepares to add new records to the specified database table
0x26+0x03	Table Update Records	Point to Point	Mandatory	Optional	Prepares to modify the specified table records
0x26+0x04	Table Update Fields	Point to Point	Mandatory	Optional	Prepares to update the specified fields of a table record
0x26+0x05	Table Delete Record	Point to Point	Mandatory	Optional	Deletes existing record from the existing database table
0x26+0x06	Table Get Data	Point to Point	Mandatory	Optional	Prepares to retrieve the specified table records
0x26+0x07	Table Get Properties	Point to Point	Mandatory	Optional	Gets total number of records and the maximum number of records the table can hold
0x26+0x08	Table Read Fragment	Point to Point	Mandatory	Optional	Retrieves a block of data from a table as initiated by the Table Get Data command

Table 4 *(continued)*

Command code + Sub Command Code (R/W)	Command name	Command type	Mandatory/Optional		Description
			Interrogator	Tag	
0x26+0x09	Table Write Fragment	Point to Point	Mandatory	Optional	Writes a block of data into a table as initiated by the Table Add Records, Table Update Records, or Table Update fields command
0x26+0x10	Table Query	Broadcast or Point to Point	Mandatory	Optional	Initiates table search based on the specified criteria
0xE1 / NA	Beep ON/OFF	Point to Point	Mandatory	Optional	Turns tag's beeper ON or OFF
0x8E	Delete Writeable Data	Point to Point	Mandatory	Optional	Deletes all allocated writeable data on a tag

The Command Type column indicates whether the command is broadcast (does not include Tag Manufacturer ID and Tag serial number in the message) or point-to-point (includes Tag Manufacturer ID and Tag Serial Number in the message).

For commands requiring a Sub Command Code, the Sub Command Code field is the first byte of the Command Arguments field that follows the Command Code.

6.2.5.8 Command Arguments

Some commands require arguments. For those commands where arguments are defined, argument data shall be supplied with the command. The contents and length of any required arguments are specific to each command. See section 6.3 for details.

6.2.5.9 CRC

A CRC checksum shall be calculated as a 16-bit value for each command message, initialized with all zeroes (0x0000), over all data bytes (excluding preamble) from the protocol ID up to and including any command arguments according to the CCITT polynomial ($x^{16} + x^{12} + x^5 + 1$). The CRC shall be appended to the data included in the command message as a two bytes field. Reference: ITU-T Recommendation V.41 (Extract from the Blue Book), Code-independent error-control system, Appendix I - *Encoding and decoding realization for cyclic code system.*

6.2.6 Tag-to-interrogator message format

The tag-to-interrogator message shall use one of two formats depending on the type of message being transmitted to the Interrogator. The tag shall always respond to a command using one of the response formats described below except in the following situations, for which the tag shall not respond:

— the command is explicitly specified in this part of ISO/IEC 18000 as requiring no response

— the CRC bytes received in the command do not match the CRC bytes that the tag has calculated for the received command packet

— receipt of a broadcast command containing an invalid command code or other error

— the tag is in the asleep state

There are two possible response formats:

— the Broadcast response message format