

BS ISO/IEC 29173-1:2012



BSI Standards Publication

Information technology — Mobile item identification and management

Part 1: Mobile RFID interrogator device
protocol for ISO/IEC 18000-63 Type C

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

National foreword

This British Standard is the UK implementation of ISO/IEC 29173-1:2012.

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 2012

Published by BSI Standards Limited 2012

ISBN 978 0 580 81264 4

ICS 35.040

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 December 2012.

Amendments issued since publication

Amd. No.	Date	Text affected
----------	------	---------------

INTERNATIONAL STANDARD

ISO/IEC 29173-1

First edition
2012-12-01

Information technology — Mobile item identification and management —

Part 1: Mobile RFID interrogator device protocol for ISO/IEC 18000-63 Type C

*Technologies de l'information — Gestion et identification d'élément
mobile —*

*Partie 1: Protocole de dispositif interrogateur RFID mobile pour
l'ISO/CEI 18000-63 Type C*



Reference number
ISO/IEC 29173-1:2012(E)

AVA Documents
Document Sharing Hub
© ISO/IEC 2012



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2012

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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	iv
Introduction.....	v
1 Scope	1
2 Normative references	1
3 Terms, definitions, symbols and abbreviated terms	1
3.1 Terms and definitions	1
3.2 Abbreviated terms	2
3.3 Notation	3
4 Overview.....	4
5 Message format of mobile RFID interrogator device protocol	4
5.1 Overview.....	4
5.2 Preamble field and end mark field	4
5.3 Header field	4
5.4 Payload field	5
5.5 Endian format and transmission order format	8
5.6 Method of describing small-size data in fixed-size field	8
5.7 Cyclic Redundancy Check (CRC) field.....	8
6 Summary and list of command, response, and notification	9
6.1 Overview.....	9
6.2 Interrogator control/management category.....	9
6.3 Tag read category.....	10
6.4 Tag write category.....	11
6.5 Tag kill/lock/erase category	12
6.6 Additional function category.....	12
6.7 Result code	12
6.8 Vendor-specific command and response	14
6.9 Notification	14
7 Details of command, response, and notification	14
7.1 Interrogator control/management category.....	14
7.2 Tag read category.....	26
7.3 Tag write category.....	31
7.4 Tag kill/lock/erase category	32
7.5 Additional function category.....	34
7.6 Appendices for command, response, and notification	36
8 Test mode.....	38
8.1 Test mode.....	38
8.2 Protocol message in test mode	38
8.3 Procedure for processing protocol message in test mode	39
8.4 Test the receive sensitivity of the interrogator	39
Annex A (informative) The scope diagram	41
Annex B (informative) Schematic of 16-bit cyclic redundancy check (CRC).....	42
Bibliography.....	43

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 29173-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

ISO/IEC 29173 consists of the following parts under the general title *Information technology — Mobile item identification and management*:

— *Part 1: Mobile RFID interrogator device protocol for ISO/IEC 18000-63 Type C*

Introduction

This International Standard provides a mobile RFID interrogator device protocol defining the interface between a mobile AIDC application platform and a mobile RFID interrogator.

Without this standard protocol, manufacturers of mobile RFID interrogators would likely develop multiple mobile RFID interrogator device drivers for different mobile AIDC application platforms. Moreover, they also would likely develop a proprietary interface protocol between the mobile AIDC application platform and the mobile RFID interrogator. On the other hand, if both the mobile AIDC application platform and the Mobile RFID interrogator developers follow this standardized mobile RFID interrogator device protocol, various independent products will be mutually interoperable without extra costs.

Previously, the ISO and EPC standards defined an interrogator protocol that supports connection of an RFID interrogator to a host through a network. Those standards are applied mainly in cases in which an RFID interrogator is connected through a network.

In mobile RFID systems, an RFID interrogator is mounted inside a mobile phone or attached to a mobile phone in a dongle configuration. Such RFID systems require a protocol that enables a main control unit of the mobile phone to control the RFID interrogator. Therefore, the Mobile RFID system requires a new interface protocol between the mobile AIDC application platform and the mobile RFID interrogator to meet the new requirements.

There are alternative techniques to meet the use case addressed by this International Standard, and one is the use of EPC and ONS. Those interested in this technique are encouraged to contact GS1 for further information.

Information technology — Mobile item identification and management —

Part 1: Mobile RFID interrogator device protocol for ISO/IEC 18000-63 Type C

1 Scope

This part of ISO/IEC 29173 defines an interface protocol between a device driver of a mobile AIDC application platform and a mobile RFID interrogator within a mobile AIDC terminal. It is intended that this part of ISO/IEC 29173 be implemented in both the device driver of a mobile AIDC application platform and the mobile RFID interrogator.

In accordance with the ISO/IEC 18000-63 type C RFID air interface, this part of ISO/IEC 29173 includes:

- types of command/response/notification protocol messages and their usages,
- protocol message format, and
- protocol message exchange procedures.

2 Normative references

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

ISO/IEC 18000-63, *Information technology — Radio frequency identification for item management: — Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C*

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

ISO/IEC 29143, *Information technology — Mobile item identification and management — Air interface specification for Mobile RFID interrogators*

ISO/IEC TR 29172, *Information technology — Mobile item identification and management — Reference architecture for Mobile AIDC services*

3 Terms, definitions, symbols and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762, ISO/IEC 18000-63, ISO/IEC TR 29172 and the following apply.

3.1.1

mobile AIDC application platform

set of computer instructions as the place to launch a mobile AIDC application in a mobile AIDC terminal

[ISO/IEC TR 29172]

3.1.2

mobile AIDC terminal

electronic device equipped with one or more mobile AIDC device(s) to support the functions of Mobile Item Identification and Management (MIIM) technologies

[ISO/IEC TR 29172]

3.1.3

mobile RFID

AIDC technique supporting the Mobile Item Identification and Management (MIIM) technologies of radio frequency identification (RFID)

[ISO/IEC TR 29172]

3.1.4

mobile RFID interrogator

electronic equipment that retrieves information from radio frequency tags by transmitting and receiving radio frequency signals to and from the tags

3.1.5

mobile RFID MIIM content name

description of the object associated with MIIM services, such as brand name, company name, food name, movie title, building name, etc.

3.2 Abbreviated terms

AFID	Application Family ID
A/I	Air Interface
AM	tag memory Access Mode
AP	Access Password
Arg	Argument
BM	Byte Mask
CRC	Cyclic Redundancy Check
DR	TRcal Divide Ratio
EAC	Embedded Application Code
EnMAC	Enable MAC
H/W	Hardware
KP	Kill Password
LD	Lock Data
MB	Tag Memory Bank
MB01EC	UII Memory Bank (01) data except the CRC

MB01ECL	MB01EC Length
MD	Memory Data of TID or content name
MDL	Memory Data Length
MI	Modulation Index
MII	Mobile Item Identifier
MSA	Memory Start Address
MT	Message Type
MTIME	Maximum elapsed Time to tagging
NUMT	Number of Maximum Tag to read
PL	Payload Length
PNTR	Pointer
RC	Repeat Cycle for inventory
RFU	Reserved for Future Use
RSV	Reserved
SDF	Storage Data Format
SeKey	Security Key
SelFM	Select Frequency Mode
SelSeM	Select Security Mode
S/N	Serial Number
TID	Tag Identifier
TN	Tag Number
TR	TRcal (Tag-to-interrogator Calibration symbol)
UID	Unique Identifier
UII	Unique Item Identifier
URI	Uniform Resource Identifier
WD	Write Data
WDL	Write Data Length
b	bit

3.3 Notation

This document uses the following notational conventions:

0bNNNN	binary notation
0xNNNN	hexadecimal notation

4 Overview

This part of ISO/IEC 29173 is organized as follows: Clause 5 describes the message format of a mobile RFID interrogator device protocol. Clause 6 summarizes and lists all commands, responses and notifications defined in this part of ISO/IEC 29173. Clause 7 describes the details of each command, response, and notification. Clause 8 describes the test mode protocol used for testing a mobile RFID interrogator. The role of this part of ISO/IEC 29173 in mobile RFID is described in ISO/IEC TR 29172.

5 Message format of mobile RFID interrogator device protocol

5.1 Overview

A mobile RFID interrogator device protocol includes a preamble, a header, a payload, and an end mark. Fig. 1 illustrates a message format of a mobile RFID interrogator device protocol.

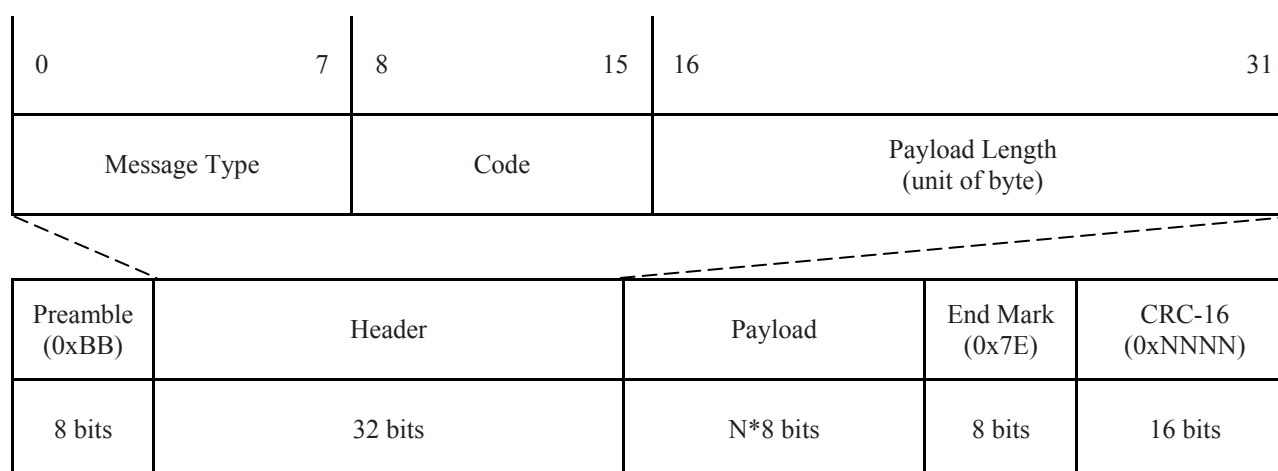


Figure 1 — Message format

5.2 Preamble field and end mark field

A preamble includes information for indicating the start of a protocol message, which is used to discern protocol messages. For example, the preamble may be configured in 8 bits and may have a value of 0xBB. A header includes information for indicating the message type, a corresponding code, and a payload length. That is, the payload length information is stored in the header and the information received from the RFID tag is stored in the payload. An end mark includes information for indicating the end of a protocol message, which is used to discern the protocol messages together with the preamble. For example, the end mark may be configured in 8 bits and may have a value of 0x7E.

5.3 Header field

5.3.1 General

The header includes three fields describing: 1) an RFID tag type, 2) command/response/notification type and code, and 3) the payload length. The message type field is used to discern a command that is transmitted from the processor to the interrogator and a response and notification transmitted from the interrogator to the processor. The code field is used to discern a variety of types of commands, responses or notifications. The code field includes information about the success or failure of commands in response and notification. The payload length field includes information indicating the length, in bytes, of the payload.

5.3.2 Message type field

The message type field associates commands, responses and notifications with the corresponding code value represented in 8 bits. The message type (e.g., command, response and notification) can be discerned using the values shown in Table 1 below.

Table 1 — Command/Response/Notification type and corresponding code value

Command/Response/Notification type	Corresponding code value (Hexadecimal)
Command	0x00
Response	0x01
Notification	0x02
Test mode	0x03
Reserved	0x04-0xFF

As shown in Table 1, a code value indicating a command is 0x00, a code value indicating a response is 0x01, a code value indicating a notification is 0x02, a code value indicating a test mode is 0x03, and code values indicating "Reserved" are 0x04 ~ 0xFF. The command, the response, the notification, and the test mode shown in Table 1 will be described later in detail.

5.3.3 Code field

A code field is used to discern the types of command, response, and notification. There may be various commands to be processed by a mobile RFID interrogator, various responses to the commands and various notifications to be sent by the interrogator. Therefore, when a code is assigned to a command, response or notification, the interrogator can accurately distinguish them by referring to the message type field and the code field. For example, when a value 0x00 and a value 0x01 are respectively assigned to a message type field and a code field for a power control command, the interrogator can recognize the received command as the power control command by the assigned values.

5.3.4 Payload length field

A payload length field indicates the length of the payload field, which occurs immediately after a header field. For example, the payload length field may be composed of 16 bits. Here, the unit of length is byte. When a payload length is represented in byte using 16 bits, the maximum length that can be represented becomes 65,536 bytes. This means that the maximum length of a payload cannot exceed 65,536 bytes.

5.4 Payload field

A payload field stores various types of data. The payload field may include arguments related to a command transmitted from the processor to the RFID interrogator, as well as various data contained in a response transmitted from the RFID interrogator to the processor. There may be various types of payloads suitable for respective commands and responses, such as the payloads illustrated in Figs. 2 and 3 that illustrate payload type A through payload type Q.

Each of the payloads illustrated in Figs. 2 and 3 includes a specific field. The use of the specific field and the method thereof will be described later in detail. The generation and configuration of each payload type will now be described in detail. The number of bits and the order mentioned in the following payload configurations are presented as examples and do not limit this part of ISO/IEC 29173.

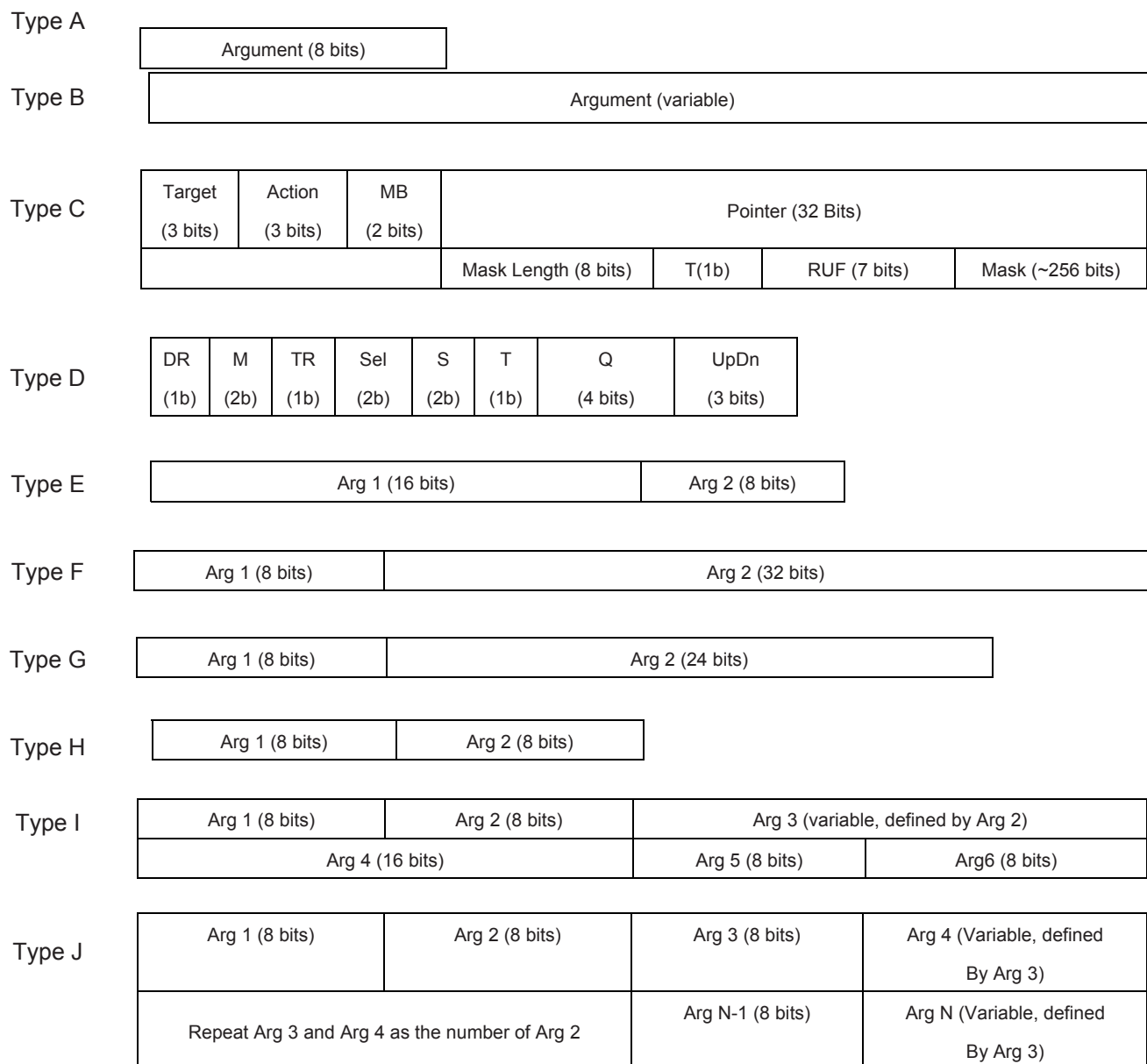


Figure 2 — Payload type A to payload type J

Type K	Arg 1 (8 bits)		Arg 2 (8 bits)		Arg 3 (8 bits)		RSV (5 bits)	DT (2 bits)	AM (1 bit)
	Arg 7 (32 bits)								
	Arg 8 (16 bits)				Arg 9 (8 bits)				

Type L	Arg 1 (8 bits)	Arg 2 (8 bits)	Arg 3 (8 bits)	Arg 4 (Variable, defined By Arg N-3)	Arg 5 (8 bits)	Arg 6 (Variable, defined By Arg 5)
	Repeat from Arg 4 to Arg 6 as the number of Arg 2					
	Arg N-3 (8 bits)	Arg N-2 (Variable, defined By Arg N-3)		Arg N-1 (8 bits)	Arg N (Variable, defined By Arg N-1)	

Type M	Arg 1 (32 bits)					
	Arg 2 (8 bits)		Arg 3 (8 bits)		Arg 4 (Variable, defined by Arg 3)	
	Arg 5 (16 bits)			Arg 6 (8 bits)		Arg 7 (Variable, defined By Arg 6)

Type P	Arg 1 (32 bits)				
	Arg 2 (32 bits)				
	Arg 3 (8 bits)		Arg 4 (Variable, defined by Arg 3)		Arg 5 (8 bits)

Type N	Arg 1 (32 bits)				
	Arg 2 (8 bits)		Arg 3 (Variable, defined by Arg 2)		
	Arg 4 (8 bits)		Arg 5 (20 bits)		

Type Q	Arg 1 (32 bits)				
	Arg 2 (8 bits)		Arg 3 (Variable, defined by Arg 2)		
	Arg 4 (8 bits)		Arg 5 (16 bits)		Arg 6 (8 bits)

Type O	Arg 1 (32 bits)				
--------	-----------------	--	--	--	--

Figure 3 — Payload type K to payload type Q

The description of the preceding payload types, the use of each field, and the use method thereof will be described later in detail.

5.5 Endian format and transmission order format

All of the fields used in constructing the mobile RFID interrogator device protocol format follow the big-Endian format. According to the big-Endian format, the most significant byte value is written first followed by the least significant byte value. A preamble field, a header field, a payload field, and an end mark field are transmitted in the order named. In the header field, a message type field, a code field, and a payload length field are transmitted in the order named. In the payload field, a target field, an argument type field, a payload data length field, and a payload data and pending field are transmitted in the order named. In each field, the most significant byte is transmitted first.

5.6 Method of describing small-size data in fixed-size field

When a small-size data needs to be inserted into a protocol field larger than the small-sized data, the less significant bytes are filled first, then the remaining more significant bytes are filled with 0x00. In this case, the big-Endian format is also applied. For example, when a value of 12 needs to be inserted into a 16-bit length field, the less significant bytes are filled with 0x0C and the more significant bytes are filled with 0x00.

5.7 Cyclic Redundancy Check (CRC) field

5.7.1 CRC general

The commands and responses use the same CRC-16 to verify the accuracy of the message bits.

On receiving a command from a mobile AIDC application platform, the RFID interrogator shall verify that the checksum or CRC value is valid. If it is invalid, it shall discard the message and shall not respond and shall not take any other action. Otherwise it shall request the command again by sending the response with code field and result code of 0xFF. And on receiving a response from the RFID interrogator, the mobile AIDC application platform shall verify that the checksum or CRC value is valid. If it is invalid, response shall be discarded and the command shall be sent again within a limited retransmit count.

The 16-bit CRC shall be calculated on all the message bits from the message type field to the end mark field.

The polynomial used to calculate the CRC is $X^{16} + X^{12} + X^5 + 1$. The 16-bit register for the CRC calculation in a mobile AIDC application platform or an RFID interrogator shall be preloaded with 0xFFFF. The resulting CRC value shall be inverted, attached to the end of the packet (after End Mark field) and transmitted.

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

NOTE A schematic of a possible implementation is provided in Annex A.

The CRC in receiving part shall be implemented in one of two ways:

5.7.2 Inversion of incoming CRC bits by the receiving part

At the receiving part, the incoming CRC bits are inverted and then clocked into the register. After the LSB CRC bit is clocked into the register, the 16-bit CRC register should contain all zero's.

5.7.3 Non-inversion of incoming CRC bits by the receiving part

If the received CRC bits are not inverted before clocking, after the LSB CRC bit is clocked into the register, the CRC register will have the value 0x1D0F.

6 Summary and list of command, response, and notification

6.1 Overview

The protocol between the processor of a mobile terminal and an RFID interrogator can be classified into a command, a response, and a notification according to ISO/IEC 18000-63.

In this part of ISO/IEC 29173, the command and the response always exist and operate in pairs. Only after a response to a command has been received is the next command executed. Each command has a specific code, which is described in the code field of the header and represented in 8 bits. When a response is successful, the code of a corresponding command is described in the code field and a response-related content is described in the payload field. On the other hand, when a response is unsuccessful, a value of 0xFF is described in the code field and the result code is described in the payload field. The payload varies according to the commands and responses. Detailed types of payloads will be described later in detail.

The commands and responses in a mobile RFID interrogator device protocol are categorized into interrogator control/management, tag read, tag write, tag kill/lock/erase, and additional functions. Table 2 below shows an example of a command list according to this part of ISO/IEC 29173. In Table 2, the commands are classified into mandatory and optional. All of the commands have corresponding responses. Commands corresponding to a tag write category and a tag kill/lock/erase category shall be implemented carefully because these commands may change the contents of a tag. When these commands are used incorrectly, security problems may occur.

Table 2 — Overview of mandatory and optional commands

Type	Mandatory command	Optional command
Interrogator control / management category	Get type C A/I select parameters Set type C A/I select parameters Get type C A/I query-related parameters Set type C A/I query-related parameters Set security key Set frequency mode Set MAC control	Get region Set region Interrogator power control Interrogator connection control Get interrogator information Get signal strength Set signal strength Reset interrogator Get automatic read parameters Set automatic read parameters
Tag read category	Read tag once Read multiple tags Stop multiple tags	
Tag write category		Write tag
Tag kill/lock/erase category	Kill tag Lock tag	Erase tag
Additional function category		Get last result Start test mode Stop test mode Star receive test Stop receive test

6.2 Interrogator control/management category

The RFID interrogator control/management command category includes the commands shown in Table 3 below. The main commands relate to interrogator power control, interrogator connection control, get interrogator information, interrogator RF signal strength control, and interrogator filter function control. The