台揚科技股份有限公司
MICROELECTRONICS TECHNOLOGY INC.

ISO 9001 Certified

MTI RU-888 RFID Module

Command Reference Manual

Version 5.1

Contents

Revision History

Version Number		Description	Revision Date
USB	UART		
1.0		(1) First release of USB version document. The revision is used on firmware version 0.1.07 beta.	February 2010
1.1		(1) New add an RFID_18K6CQueryParameter command. (2) Modify command format and response packet of RFID_AntennaPortSetPowerLevel, RFID_AntennaPortSetFrequency, RFID_AntennaPortSetModulation, RFID_18K6CTagInventory, RFID_18K6CTagInventoryRSSI, and RFID_18K6CTagNXPCommand six commands. The revision is used on firmware version 0.2.05 beta.	April 2010
1.2		(1) Add region number of RFID_RadioSetRegion and response data of RFID_RadioGetRegion. (2) New add two RFID_AntennaPortTransmitPattern and RFID_EngTransmitSerialPattern commands. The revision is used on firmware version 0.3.04 beta.	May 2010
2.0	1.0	(1) Add these RFID_ERROR_GEN2_xxx status codes for performed result of ISO 18000-6C command set. (2) Add region number of RFID_RadioSetRegion and response data of RFID_RadioGetRegion. (3) Add the RFID_AntennaPortGetPowerLevel command. (4) Add the padding field in the RFID_AntennaPortSetFrequency command. (5) Add the power level field in the response packet of RFID_AntennaPortSetFrequency command. (6) Add the status field in the response packet of RFID_AntennaPortCtrlPowerState, RFID_18K6CSetQueryParameter, RFID_18K6CTagInventory, RFID_18K6CTagInventoryRSSI, RFID_18K6BTagInventory, RFID_MacGetModuleID, RFID_MacBypassReadRegister seven commands. (7) Correct the value and description of NXP command and bit status both fields in the RFID_18K6CTagNXPCommand command. (8) Add the new config word field in the response packet of RFID_18K6CTagNXPCommand command. (9) Add a use case of 6C tag writing. First release of UART version document. The revision is used on firmware version 0.5.00 beta.	August 2010
2.1	1.1	(1) Add the RFID_ERROR_CMD_INVALID_DATA_LENGTH (0x0E) status code for data length of each command checking in section 3.2. (2) Replace the GEN2 word with 18K6C in section 3.2. (3) Modify status code of 6B tag response, and correct their name from 6BTag to 18K6B in section 3.2. (4) Change value range of tag data length field of RFID_18K6CTagRead command in section 4.3. (5) Correct the description of bit status field of RFID_18K6CTagNXPCommand command in section 4.3. (6) Add three communication data tables of use cases in section 5. The revision is used on firmware version 0.5.01 beta.	August 2010
2.2	1.2	(1) Add default value information in the parameters field of RFID_RadioSetRegion, RFID_AntennaPortSetPowerLevel, RFID_AntennaPortSetOperation, RFID_AntennaPortCtrlPowerState and	August 2010

		RFID_18K6CSetQueryParameter five commands. The revision is used on firmware version 0.5.01 beta.	
2.3	1.3	(1) Correct the Status Code of "RFID_ERROR_SYS_CHANNEL_TIMEOUT" in Table 3.4; related status code is corrected also. (2) Change descriptions in table 3.4. (3) Change some field name and add more detailed description in section 4.3.1.1. (4) Corrected the range of "Mask Length" in section 4.3.1.4. (5) Modify command format of tag read in section 4.3.2.1. (6) Verify the description of write tag command & response in section 4.3.2.2. (7) Add detailed description in section 4.3.2.3. (8) Modify the description of "New Config Word" field in section 4.3.3.1. (9) Add description in "module ID" in section 4.5.1. The revision is used on firmware version 0.5.9 beta.	October 2010
2.4	1.4	(1) Add RFID_AntennaPortTransmitPulse, RFID_MacGetDebugValue, RFID_MacSoftReset and RFID_MacEnterUpdateMode four commands. (2) Add a RFID_ERROR_SYS_SECURITY_FAILURE status code in table 3.4. (3) Add a RFID_ERROR_SYS_SECURITY_FAILURE status code in the Status field of RFID_18K6CTagInventory, RFID_18K6CTagInventoryRSSI and RFID_18K6BTagInventory three commands. (4) Add Canada, Austria, New Zealand three regions and delete Japan region in the RFID_RadioSetRegion command. (5) Modify the "Dwell Time" field in the RFID_AntennaPortTransmitPattern command. (6) Delete the default value in the "Sensitivity Value" field of RFID_18K6CSetQueryParameter command and add an "Effective Sensitivity Value List Table" in the response packet. (7) Change the address range in the "OEMCfg Address" field of RFID_MacWriteOemData command. (8) Add frequency channel tables of Canada, Austria, New Zealand three regions and delete Japan region and modify South Korea region in section 7 APPENDIX B. (9) Delete related section and description of Tag-NXP command operation function. (10) Delete related section and description of ISO 18000-6B tag access function. The following modifications are only in USB version document. (11) Change the value of data length field of RFID_18K6CTagInventory, RFID_18K6CTagInventoryRSSI, RFID_18K6CTagRead, RFID_18K6BTagInventory and RFID_18K6BTagRead five commands (12) Add a maximum value for USB dongle product. (13) Modify some values in the use cases The revision is used on firmware version 0.6.5 beta.	November 2010
2.5	1.5	(1) Correct the value of data length of RFID_AntennaPortTransmitPattern command. The revision is used on firmware version 0.6.5 beta.	November 2010
3.0	2.0	(1) Add two RFID_ERROR_HWOPT_READONLY_ADDRESS and RFID_ERROR_HWOPT_UNSUPPORTED_REGION status codes in table 3.4. (2) Add a RFID_ERROR_HWOPT_UNSUPPORTED_REGION status code in the Status field of RFID_RadioSetRegion command. (3) Add a section description for specific command of NXP tag. (4) Add an OEMCfg ID parameter in the Module ID field of RFID_MacGetModuleID command to get ID information of OEMCfg area. (5) Add two new status codes in the Status field of RFID_MacWriteOemData command. The revision is used on firmware version 1.0.0.	December 2010

3.1	2.1	(1) Modify this document information in the footer. The revision is used on firmware version 1.0.0.	April 2011
3.2	2.2	(1) Add RFID_18K6CTagBlockWrite and RFID_18K6CTagNXPTriggerEASAlarm two commands. (2) Add a RFID_ERROR_18K6C_EASCODE status code in table 3.4. (3) Add an OEMCfg Update ID parameter in the Module ID field of RFID_MacGetModuleID command to get ID information of OEMCfg update. (4) Add Brazil, Hong Kong, Malaysia, Singapore, Thailand, Israel, Russia Federation, India, Saudi Arabia, Jordan, and Mexico eleven regions in the RFID_RadioSetRegion command. (5) Add frequency channel tables of Brazil, Hong Kong, Malaysia, Singapore, Thailand, Israel, Russia Federation, India, Saudi Arabia, Jordan, and Mexico eleven regions in section 7 APPENDIX B. The revision is used on firmware version 1.2.0.	May 2011
4.0	3.0	(1) Remove the API word in this document. (2) Modify frequency channel table of Brazil region in section 7 APPENDIX B. The revision is used on firmware version 1.2.1.	August 2011
4.1	3.1	(1) Modify MTI Group Proprietary Information. (2) Delete RFID_AntennaPortSetOperation command from the command sequences of RF CW on, RF modulation, RF pulse test examples, because it's useless process. (3) Change Modulation field of RFID_AntennaPortSetOperation command to RFU, because it's useless setting. (4) Correct the mistype receiver A->B, B->A in the Data I and Data Q fields of the response of RFID_AntennaPortSetFrequency command. (5) Modify description of Action field and Tag Number field of RFID_18K6CTagInventory and RFID_18K6CTagInventoryRSSI command. (6) Correct the value of EPC Length field of RFID_18K6CTagInventory and RFID_18K6CTagInventoryRSSI response. (7) Correct the value of Data Length and Mask Length fields of RFID_18K6CTagSelect command. (8) Correct the value of Memory Address field of RFID_18K6CTagRead command. (9) Correct the value of Memory Address field of RFID_18K6CTagWrite command. (10) Correct the value of Data Length, Memory Address, Tag Data Length and Written Number fields of RFID_18K6CTagBlockWrite command and response. (11) Modify description and caution of NXP Command, Bit Status, Access Password, Toggled Config-Word and Config-Word fields of RFID_18K6CTagNXPCommand command and response. (12) Correct the Step5 of Command and Response Sequences of use case 5.1, 5.3. (13) Add use case of changing Config-Word of the specific NXP tag. The revision is used on firmware version 1.2.1 or higher.	July 2012
5.0		(1) Merge two documents (USB and UART version) into one. (2) Add RIFD_18K6CSetQuickAccessMode, RIFD_18K6CGetQuickAccessMode two commands. (3) Add caution about confirming the host interface before entering the firmware update mode for RFID_MacEnterUpdateMode command. (4) Add Appendix D to highlight the difference between USB and UART interface. The revision is used on firmware version 2.1.1 or higher.	July 2012
5.1		(1) Delete un-support SL session of Session Value field of RFID_18K6CSetQueryParameter command and response. (2) Correct the description of RFID_18K6CTagWrite and RFID_18K6CTagBlockWrite command. (3) Delete ISO 18000-6B words.	May 2013

	The revision is used on firmware version 2.1.1 or higher.	

1 Introduction

The *MTI RU-888 RFID Module Command Reference Manual* provides detailed information for configuring, controlling, and accessing the MTI RU-888 RFID module. Each command and its parameters are then described in detail.

The intended audience for this document includes the following:

- RFID middleware software developers who will be creating software for configuring, controlling, and accessing the MTI RU-888 RFID module.
- RFID reader manufacturers who will need to understand how to configure, control, and access the MTI RU-888 RFID module during development and testing phases.

1.1 Terminology

Table 1.1 - Terminology

Term	Description
CRC	Cyclic Redundancy Check
EPC	Electronic Product Code
GPIO	General Purpose I/O
ISO	International Standards Organization
OEM	Original Equipment Manufacturer
RFID	Radio Frequency Identification
RX	Receiver
TID	Tag Identifier
TX	Transmitter
UART	Universal Asynchronous Receiver/Transmitter
USB	Universal Serial Bus
HID	Human Interface Device

2 System Development Overview

2.1 MTI RU-888 RFID Module Application Overview

Figure 2.1 illustrates a typical MTI RU-888 RFID module application. The MTI RU-888 RFID module accesses (reads, writes, etc.) ISO 18000-6C (EPC Class 1 Generation 2) RFID tags and passes the digital data stream via the USB or UART to a host processor. The host processor connects to and controls the MTI RU-888 RFID module via USB or UART interface.

For USB interface:
After connecting the MTI RU-888 RFID module to the computer it is automatically installed as a HID (Human Interface Device). The host processor uses the USB VID and PID combination to find the MTI RU-888 RFID module. The USB VID and PID both numbers are as follows,

USB Vendor ID: 0x1325 / Product ID: 0xC029

For UART interface:
The UART configuration between host processor and MTI RU-888 RFID module are as follows,

115200 bps baud rate / 8 bits data / No parity / 1 stop bit / No flow control.

NOTICE: MTI RU-888 RFID module supports USB or UART interface, depending on the OEM configuration. The host processor can change the host interface and related setting. Refer to the *MTI RU-888 RFID Module OEM Configuration Guide* for detailed information.

Connection to the external RFID network infrastructure is achieved via an application layer. This application layer is depended on the embedded processor. The detailed description of this functionality is outside the scope of this document.

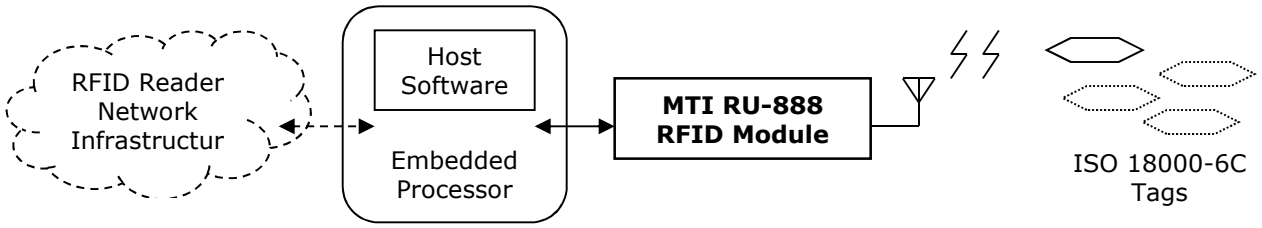


Figure 2.1 - Typical MTI RU-888 RFID Module Application Architecture

2.2 Theory of Operation

The command set provides many programming commands for controlling ISO 18000-6C compatible MTI RU-888 RFID module. The host can configure the MTI RU-888 RFID module for operation and tag protocol operations can be issued.

The host initiates transactions with ISO 18000-6C tags or tag populations by executing ISO 18000-6C tag-protocol operations. The command set exposes direct access to the following ISO 18000-6C tag-protocol operations:

- Inventory
- Read
- Write

- Kill
- Lock

After inventory operation, first the host should send a select operation in case there are several tags found, and then perform the tag-protocol operation.

The MTI MAC firmware provides some response packets for presenting tag-protocol operation response data to the host. Tag-protocol operation results include EPC values returned by the Inventory operation, read data returned by the Read operation, and operation status returned by the Write, Kill, and Lock operations.

The command set supports the operation of the antenna port on the RFID module.

The command set provides the host with access to (i.e. read and write) the OEM configuration data area on the RFID module. The host can use the OEM configuration data area to store and retrieve the specific hardware configuration and capabilities of the RFID module. The host can read a RFID module's OEM configuration data area immediately after gaining exclusive control of the RFID module and use that data to configure and control low-level parameters of the RFID module. For detailed information, refer to the *MTI RU-888 RFID Module OEM Configuration Guide* document.

The command set also supports low-level control of the RFID module's MAC firmware. For hardware register access, the relative command provides the host a means for reading and writing the RFID module's hardware register to control hardware function of low level.

3 Command Set

3.1 Command Set Summary

Table 3.1 - Command Set Summary

CMD ID	Command Name	Simple Description	Diff. b/w Interface
RFID Module Configuration			
0xA8	RFID_RadioSetRegion	Setting the RFID Module's Region of Operation	
0xAA	RFID_RadioGetRgion	Retrieving the RFID Module's Region of Operation	
Antenna Port Operation			
0xC0	RFID_AntennaPortSetPowerLevel	Setting Antenna-Port Power Level	
0xC2	RFID_AntennaPortGetPowerLevel	Retrieving Antenna-Port Power Level	
0x41	RFID_AntennaPortSetFrequency	Setting Antenna-Port Frequency	
0xE4	RFID_AntennaPortSetOperation	Setting Antenna-Port Operation	
0x18	RFID_AntennaPortCtrlPowerState	Controlling Antenna-Port Power State	
0xE6	RFID_AntennaPortTransmitPattern	Transmitting the Fixed Data via Antenna Port	
0xEA	RFID_AntennaPortTransmitPulse	Transmitting the Fixed Pulse via Antenna Port	
ISO 18000-6C Tag Access			
0x59	RFID_18K6CSetQueryParameter	Setting the Configuration Parameters of Query	
0x5B	RFID_18K6CSetQuickAccessMode	Setting the Quick Access Mode	
0x5D	RFID_18K6CGetQuickAccessMode	Retrieving the Quick Access Mode	
0x31	RFID_18K6CTagInventory	6C Tag Inventory Operation	*
0x43	RFID_18K6CTagInventoryRSSI	6C Tag Inventory Operation with RSSI	*
0x33	RFID_18K6CTagSelect	6C Tag Select Operation	
0x37	RFID_18K6CTagRead	6C Tag Read Operation	*
0x35	RFID_18K6CTagWrite	6C Tag Write Operation	*
0x3D	RFID_18K6CTagKill	6C Tag Kill Operation	
0x3B	RFID_18K6CTagLock	6C Tag Lock Operation	
0x70	RFID_18K6CTagBlockWrite	6C Tag Block Write Operation	
0x45	RFID_18K6CTagNXPCommand	6C Tag NXP Command Set Operation	
0x72	RFID_18K6CTagNXPTriggerEASAlarm	6C Tag NXP Trigger EAS Alarm Operation	
RFID Module Firmware Access			
0x10	RFID_MacGetModuleID	Retrieving the RFID Module's MAC Firmware and Hardware Version Information	
0xA2	RFID_MacGetDebugValue	Retrieving the RFID Module's MAC Firmware Debug Value	
0x1A	RFID_MacBypassWriteRegister	Writing to an RFID Module Hardware Register	
0x1C	RFID_MacBypassReadRegister	Reading from an RFID Module Hardware Register	
0xA4	RFID_MacWriteOemData	Writing MAC Firmware OEM Configuration Data	
0xA6	RFID_MacReadOemData	Reading MAC Firmware OEM Configuration Data	
0xA0	RFID_MacSoftReset	Performing a Software Reset	
0xD0	RFID_MacEnterUpdateMode	Entering Firmware Update Mode	

3.2 Packet Format Specification

3.2.1 Command Packet Format

The length of the command packet is variable. In command packet, bold italic text is applied to the value in the both Byte Offset and Name columns of the common fields to indicate they are Command Data.

For USB interface:

Table 3.2 – USB Command Format Fields

Byte Offset	Name	Description
0	***Command ID***	See Table 3.1 - Command Set Summary.
1	***Data Length***	The Data Length is byte number over the Command ID field to the Parameters field.
n:2	***Parameters***	Effective parameters size of each command is different. The length of this field is variable byte number.

For UART interface:

Table 3.3 – UART Command Format Fields

Byte Offset	Name	Description
3:0	Header	Four ASCII codes are 'M', 'T', 'I' and 'C'. (Hexadecimal values are 0x4D/0x54/0x49/0x43) [0] = 'M', [1] = 'T', [2] = 'I', [3] = 'C'.
4	Device ID	Module's device identification number. Default factory setting value is 0x00. General device ID number is 0xFF for broadcasting.
5	***Command ID***	See Table 3.1 - Command Set Summary.
6	***Data Length***	The Data Length is byte number over the Command ID field to the Parameters field.
n:7	***Parameters***	Effective parameters size of each command is different. The length of this field is variable byte number.
n+2: n+1	Checksum	The Checksum is CRC-16 calculated over the Header field to the Parameters field. Consult Section 8: Calculation of CRC-16. [n+1] = Checksum[15:8], [n+2] = Checksum[7:0]

3.2.2 Response Packet Format

The length of the response packet is variable. In response packet, italic text is applied to the value in the both Byte Offset and Name columns of the common fields to indicate they are Response Data. If the incorrect command packet was sent, then reply nothing to host.

For USB interface:

Table 3.4 – USB Response Format Fields

Byte Offset	Name	Description
0	***Response ID***	The value is equal to Command ID number plus 1. See response packet of each command section of chapter 4.
1	***Data Length***	The Data Length is byte number over the Response ID field to the Returned Data field.
n:2	***Returned Data***	Effective returned data size of each response is different. The length of this field is variable byte number. Comprise status, detail see Table 3.6 - Status Message Define.

For UART interface:

Table 3.5 - UART Response Format Fields

Byte Offset	Name	Description
3:0	Header	Four ASCII codes are 'M', 'T', 'I' and 'R'. (Hexadecimal values are 0x4D/0x54/0x49/0x52) [0] = 'M', [1] = 'T', [2] = 'I', [3] = 'R'.
4	Device ID	Module's device identification number. Default factory setting value is 0x00.
5	***Response ID***	The value is equal to Command ID number plus 1. See response packet of each command section of chapter 4.
6	***Data Length***	The Data Length is byte number over the Response ID field to the Returned Data field.
n:7	***Returned Data***	Effective returned data size of each response is different. The length of this field is variable byte number. Comprise status, detail see Table 3.6 - Status Message Define.
n+2: n+1	Checksum	The Checksum is CRC-16 calculated over the Header field to the Returned Data field. Consult Section 8: Calculation of CRC-16. [n+1] = Checksum[15:8], [n+2] = Checksum[7:0]

Table 3.6 - Status Message Define

Status Code	Name	Description
0x00	RFID_STATUS_OK	Performed result of command is success or tags have been found.
0x0E	RFID_ERROR_CMD_ INVALID_DATA_LENGTH	The value range in the data length field of command is invalid.
0x0F	RFID_ERROR_CMD_ INVALID_PARAMETER	One of the function parameters of command is invalid.
0x0A	RFID_ERROR_SYS_ CHANNEL_TIMEOUT	Occupational time of operational channel is overtime.
0xA0	RFID_ERROR_HWOPT_ READONLY_ADDRESS	The OEMCfg address is read only.
0xA1	RFID_ERROR_HWOPT_ UNSUPPORTED_REGION	The region selection is unsupported.
0xFE	RFID_ERROR_SYS_ SECURITY_FAILURE	Checking security protection of product is failed.
0xFF	RFID_ERROR_SYS_ MODULE_FAILURE	The underlying module encountered an error. The RFID module indicated a failure. For tag operation, the RFID module did not get any reply from tag.
0x01	RFID_ERROR_18K6C_ REQRN	Requesting allowance to access tag is failed.
0x02	RFID_ERROR_18K6C_ ACCESS	Requesting is not permitted; or no tags response to reader.
0x03	RFID_ERROR_18K6C_ KILL	Killing a tag is failed.
0x04	RFID_ERROR_18K6C_ NOREPLY	Tag does not reply to Read/Write/Lock/Kill command. Completeness of command is not guaranteed.
0x05	RFID_ERROR_18K6C_ LOCK	Locking a certain tag memory bank is failed.
0x06	RFID_ERROR_18K6C_ BLOCKWRITE	Writing blocks of words to tag memory bank is failed.
0x07	RFID_ERROR_18K6C_ BLOCKERASE	Erasing blocks of words of tag memory bank is failed.
0x08	RFID_ERROR_18K6C_	Reading tag memory is failed; reader does not get response from tag.

	READ	
0x09	RFID_ERROR_18K6C_ SELECT	Trying to find certain tag is failed.
0x20	RFID_ERROR_18K6C_ EASCODE	EAS Code is not valid.
0x80	RFID_ERROR_6CTAG_ OTHER_ERROR	Catch-all for errors not covered by other codes.
0x83	RFID_ERROR_6CTAG_ MEMORY_OVERRUN	The specified memory location does not exist or the PC value is not supported by the tag.
0x84	RFID_ERROR_6CTAG_ MEMORY_LOCKED	The specified memory location is locked unless access password is applied; or it is "Always Not Accessible" and is either not writeable or not readable permanently.
0x8B	RFID_ERROR_6CTAG_ INSUFFICIENT_POWER	The tag has insufficient power to perform the memory-write operation.
0x8F	RFID_ERROR_6CTAG_ NONSPECIFIC_ERROR	The tag does not support error-specific codes.

4 Command Introduction

4.1 RFID Module Configuration

4.1.1 Regulatory Region of Operation

The RFID module supports operating in different geographical regions. The parameters that are affected by different geographical region support include, but are not limited to, the number of unique and the frequencies of the channels used, the amount of time spent upon a particular channel, etc.
The RFID module exposes two functions that allow a host to set and retrieve the region of operation.

4.1.1.1 Setting the Module's Region of Operation

Description: Configures the RFID module's region of operation as specified.

Command: **RFID_RadioSetRegion**

Byte Offset	Name	Value	Description
0	Command ID	0xA8	Command ID number of RFID_RadioSetRegion.
1	Data Length	0x03	Byte number of command data length.
2	Region	0 ~ 17	The new region of operation for the RFID module. 00 = United States / Canada (US) / (CA) 01 = Europe (EU) (ETSI EN 302 208) 02 = Taiwan (TW) 03 = China (CN) 04 = South Korea (KR) 05 = Australia / New Zealand (AU) / (NZ) 06 = Europe 2 (EU2) (ETSI EN 300 220) 07 = Brazil (BR) 08 = Hong Kong (HK) 09 = Malaysia (MY) 10 = Singapore (SG) 11 = Thailand (TH) 12 = Israel (IL) 13 = Russia Federation (RU) 14 = India (IN) 15 = Saudi Arabia (SA) 16 = Jordan (JO) 17 = Mexico (MX) Default value depends on the OEMCfg's REGION_SEL setting.

Response:

Byte Offset	Name	Value	Description
0	Response ID	0xA9	Response ID number of RFID_RadioSetRegion.
1	Data Length	0x03	Byte number of response data length.
2	Status	0x00/0E/0F/A1/FF	Performed result of command.

4.1.1.2 Retrieving the Module's Region of Operation

Description: Retrieves the region of operation for which the RFID module is configured.

Command: **RFID_RadioGetRegion**

Byte Offset	Name	Value	Description
0	Command ID	0xAA	Command ID number of RFID_RadioGetRegion.
1	Data Length	0x02	Byte number of command data length.

Response:

Byte Offset	Name	Value	Description
0	Response ID	0xAB	Response ID number of RFID_RadioGetRegion.
1	Data Length	0x04	Byte number of response data length.
2	Status	0x00/0E/FF	Performed result of command.
3	Region	0 ~ 17/ 0xFF	Receives the current region of operation. 00 = United States / Canada (US) / (CA) 01 = Europe (EU) (ETSI EN 302 208) 02 = Taiwan (TW) 03 = China (CN) 04 = South Korea (KR) 05 = Australia / New Zealand (AU) / (NZ) 06 = Europe 2 (EU2) (ETSI EN 300 220) 07 = Brazil (BR) 08 = Hong Kong (HK) 09 = Malaysia (MY) 10 = Singapore (SG) 11 = Thailand (TH) 12 = Israel (IL) 13 = Russia Federation (RU) 14 = India (IN) 15 = Saudi Arabia (SA) 16 = Jordan (JO) 17 = Mexico (MX) 0xFF = Unknown

4.2 Antenna Port Operation

The RFID module supports active use of one physical antenna port. The command set supports the operation of the antenna port on the RFID module.

4.2.1 Antenna-Port State with Regulatory Region

Allow a host to specify whether or not the power level of RFID module's physical antenna port is configured for subsequent tag operations. Moreover, the frequencies of the channels used are selected automatically with the module's region of operation.
The RFID module exposes two functions that allow a host to set and retrieve the current power level of physical antenna port.

4.2.1.1 Setting Antenna-Port Power Level

Description: Configures the power level of RFID module's physical antenna port.

Command: **RFID_AntennaPortSetPowerLevel**

Byte Offset	Name	Value	Description
0	Command ID	0xC0	Command ID number of RFID_AntennaPortSetPowerLevel.
1	Data Length	0x03	Byte number of command data length.
2	Power Level	5 ~ 18/24	The power level for the physical antenna port, unit is dBm. For USB dongle product, the maximum value is 18 dBm. For RFID module product, the maximum value is 24 dBm. Default value is 5 dBm.

Response:

Byte Offset	Name	Value	Description
0	Response ID	0xC1	Response ID number of RFID_AntennaPortSetPowerLevel.
1	Data Length	0x03	Byte number of response data length.
2	Status	0x00/0E/0F/FF	Performed result of command.

4.2.1.2 Retrieving Antenna-Port Power Level

Description: Retrieves the power level of RFID module's physical antenna port.

Command: **RFID_AntennaPortGetPowerLevel**

Byte Offset	Name	Value	Description
0	Command ID	0xC2	Command ID number of RFID_AntennaPortGetPowerLevel.
1	Data Length	0x02	Byte number of command data length.

Response:

Byte Offset	Name	Value	Description
0	Response ID	0xC3	Response ID number of RFID_AntennaPortGetPowerLevel.
1	Data Length	0x04	Byte number of response data length.
2	Status	0x00/0E/FF	Performed result of command.
3	Power Level	5 ~ 24	Receives the current power level of physical antenna port, unit is dBm.

4.2.2 Antenna-Port Configuration with Fixed Channel

The RFID module provides some functions that allow a host to configure the frequency channel, FHSS or LBT operation, and power state of RFID module's physical antenna port. The command of frequency channel configuration should be executed first, then perform antenna-port power state controlling or antenna-port pattern transmitting operation with fixed frequency channel. The frequency channel of manual selecting is limited; it must be comprised in the Module's region of operation. These commands must be operated together for special purpose, such as continuous wave and modulation test with fixed frequency channel.

These command sequences of RF CW on test example are listed below:

a. RFID_AntennaPortSetFrequency (0x41) [Mask = 0x08][Frequency value][RSSI value]
b. RFID_AntennaPortCtrlPowerState (0x18) [State = 0xFF]
c. Waiting for Test.
d. RFID_AntennaPortCtrlPowerState (0x18) [State = 0x00]

These command sequences of RF modulation test example are listed below:

a. RFID_AntennaPortSetFrequency (0x41) [Mask = 0x08][Frequency value][RSSI value]
b. RFID_AntennaPortTransmitPattern (0xE6) [Dwell Time value]

These command sequences of RF pulse test example are listed below:

a. RFID_AntennaPortSetFrequency (0x41) [Mask = 0x08][Frequency value][RSSI value]
b. RFID_AntennaPortTransmitPulse (0xEA) [Dwell Time value]

IMPORTANT: When these functional tests of special purpose are done, a host must perform the RFID_RadioSetRegion command before perform any tag access operation.

4.2.2.1 Setting Antenna-Port Frequency

Description: Configures the RFID module's frequency within region of operation and gets the reflected power or the RSSI value of the channel.

Command: **RFID_AntennaPortSetFrequency**

Byte Offset	Name	Value	Description
0	Command ID	0x41	Command ID number of RFID_AntennaPortSetFrequency.
1	Data Length	0x09	Byte number of command data length.
2	Mask	0x00/01/02 /08	It is possible to select either the RSSI value that is scanned with no carrier (LBT) or the reflected power that is received with activated carrier. 0x00 = no specific value (measurement skipped no valid dates) 0x01 = RSSI scanning 0x02 = reflected power scanning 0x08 = clear the channel list and turn hop mode off
3	Frequency Low	0x00 ~ 0xFF	The frequency is transmitted in KHz that means 914250 means 914.25 MHz. 914.25 MHz = 914250 KHz = 0x0D F3 4A The value of this field is equal to 0x4A.
4	Frequency Mid	0x00 ~ 0xFF	As above 914.25 MHz, the value of this field is equal to 0xF3.
5	Frequency High	0x00 ~ 0xFF	As above 914.25 MHz, the value of this field is equal to 0x0D.
6	RSSI Level	-128 ~ 127	Defines the LBT border which is used in the hop mode, unit is dBm. Default value is -84 dBm.
8:7	PADDING	0x00 ~ 0xFF	Pad any value added to end of returned data field to force this command data to stuff 9 bytes length. Suggested value is 0x00.

Byte Offset	Name	Value	Description
0	Command ID	0x41	Command ID number of RFID_AntennaPortSetFrequency.
1	Data Length	0x09	Byte number of command data length.
2	Mask	0x10	Defines these time parameters of LBT for frequency hopping. 0x10 = set LBT parameters.
3	Listening Time Low	0x00 ~ 0xFF	Sets the listening time, unit is ms.
4	Listening Time High	0x00 ~ 0xFF	Sets the listening time, unit is ms.
5	Max Sending Time Low	0x00 ~ 0xFF	Sets the maximum sending time, unit is ms.
6	Max Sending Time High	0x00 ~ 0xFF	Sets the maximum sending time, unit is ms.
7	Idle Time Low	0x00 ~ 0xFF	Sets the idle time, unit is ms.
8	Idle Time High	0x00 ~ 0xFF	Sets the idle time, unit is ms.

Response:

Byte Offset	Name	Value	Description
0	Response ID	0x42	Response ID number of RFID_AntennaPortSetFrequency.
1	Data Length	0x06	Byte number of response data length.
2	Status	0x00/0E/0F/FF	Performed result of command.
3	Data I	0x00 ~ 0xFF	Mask = 0x00, fixed value = 0xFF Mask = 0x01, RSSI value of I channel Mask = 0x02, mixer DC value of receiver A Mask = 0x08, fixed value = 0xFE Mask = 0x10, Maximum sending time >= 50 ms, value = 0xFE Maximum sending time < 50 ms, value = 0xFF
4	Data Q	0x00 ~ 0xFF	Mask = 0x00, fixed value = 0xFF Mask = 0x01, RSSI value of Q channel Mask = 0x02, mixer DC value of receiver B Mask = 0x08, fixed value = 0xFF Mask = 0x10, fixed value = 0xFF
5	Power Level	-128 ~ 127	Mask = 0x01, Power level of RSSI, unit is dBm Mask = other, fixed value = 0x00

4.2.2.2 Setting Antenna-Port Operation

Description: Configures the operation of RFID module's physical antenna port.

Command: **RFID_AntennaPortSetOperation**

Byte Offset	Name	Value	Description
0	Command ID	0xE4	Command ID number of RFID_AntennaPortSetOperation.
1	Data Length	0x04	Byte number of command data length.
2	RFU	0x00/01	Reserved for future use.
3	Operation	0x00/01	The state of FHSS or LBT operation for the physical transmit antenna. If the Operation value = 0x00, perform the tag access operation with the first frequency of channel list. 0x00 = disabled 0x01 = enabled

			Default value is 0x01 (enabled).

Response:

Byte Offset	Name	Value	Description
0	Response ID	0xE5	Response ID number of RFID_AntennaPortSetOperation.
1	Data Length	0x03	Byte number of response data length.
2	Status	0x00/0E/0F/FF	Performed result of command.

4.2.2.3 Controlling Antenna-Port Power State

Description: Controls the power state of RFID module's physical antenna port with the first frequency of channel list.

Command: **RFID_AntennaPortCtrlPowerState**

Byte Offset	Name	Value	Description
0	Command ID	0x18	Command ID number of RFID_AntennaPortCtrlPowerState.
1	Data Length	0x03	Byte number of command data length.
2	State	0x00/FF	The power state of the physical antenna port. 0x00 = power off 0xFF = power on Default value is 0x00 (power off).

Response:

Byte Offset	Name	Value	Description
0	Response ID	0x19	Response ID number of RFID_AntennaPortCtrlPowerState.
1	Data Length	0x03	Byte number of response data length.
2	Status	0x00/0E/0F/FF	Performed result of command.

4.2.2.4 Transmitting Antenna-Port Pattern

Description: Transmits the fixed data pattern via RFID module's physical antenna port.

Command: **RFID_AntennaPortTransmitPattern**

Byte Offset	Name	Value	Description
0	Command ID	0xE6	Command ID number of RFID_AntennaPortTransmitPattern.
1	Data Length	0x04	Byte number of command data length.
3:2	Dwell Time	1 ~ 3600	Sets the performed time, unit is second. [2] = dwell time[15:8] [3] = dwell time[7:0] Example: Dwell time value = 3600 = 0x0E 10 [2] = dwell time[15:8] = 0x0E [3] = dwell time[7:0] = 0x10

Response:

Byte Offset	Name	Value	Description
0	Response ID	0xE7	Response ID number of RFID_AntennaPortTransmitPattern.
1	Data Length	0x03	Byte number of response data length.
2	Status	0x00/0E/0F/FF	Performed result of command.

4.2.2.5 Transmitting Antenna-Port Pulse

Description: Transmits the fixed data pulse via RFID module's physical antenna port.
This command can support successive transmit pulses test of ETSI EN 302 208-1 V1.3.1.

Command: **RFID_AntennaPortTransmitPulse**

Byte Offset	Name	Value	Description
0	Command ID	0xEA	Command ID number of RFID_AntennaPortTransmitPulse.
1	Data Length	0x04	Byte number of command data length.
3:2	Dwell Time	1 ~ 3600	Sets the performed time, unit is second. [2] = dwell time[15:8] [3] = dwell time[7:0] Example: Dwell time value = 3600 = 0x0E 10 [2] = dwell time[15:8] = 0x0E [3] = dwell time[7:0] = 0x10

Response:

Byte Offset	Name	Value	Description
0	Response ID	0xEB	Response ID number of RFID_AntennaPortTransmitPulse.
1	Data Length	0x03	Byte number of response data length.
2	Status	0x00/0E/0F/FF	Performed result of command.

4.3 ISO 18000-6C Tag Access

This section describes the functions through which a host can access ISO 18000-6C tags.

A host has control of several configuration parameters that control the operation of the inventory commands. The RFID module allows the host to explicitly issue the following ISO 18000-6C access commands: read, write, kill, and lock. Tag access operation results include EPC values returned by the Inventory operation, read data returned by the Read operation, and operation status returned by the Write, Kill, and Lock operations.
Therefore the power state of the physical antenna port must be enabled and there must be at least one tag in the field.

4.3.1 Tag Inventory and Select Operation Functions

An inventory operation allows the host to gather the EPCs for all tags of interest. Then a select operation allows the host to select a unique tag for tag-protocol operation.

4.3.1.1 Setting the Configuration Parameters of Query

Description: Configures several configuration parameters that control the operation of the inventory commands. When filling "don't change" (0x00) in any "Set" field (ex: "Link Frequency Set" "Miller Set"), it not only remains but also reads back current settings. In other words, it performs "Get" function at the same time.
MTI only uses these default values of Link Frequency, Miller and TRext three fields to perform regulatory test for multi-regions.

Command: **RFID_18K6CSetQueryParameter**

Byte Offset	Name	Value	Description
0	Command ID	0x59	Command ID number of RFID_18K6CQueryParameter.
1	Data Length	0x0E	Byte number of command data length.
2	Link Frequency Set	0x00/01	This field is changed if the subsequent field should be set. 0x00 = don't change other = change
3	Link Frequency Value	0x00/06/08 /09/0C/0F	Sets the T=>R link frequency. 0x00 = 40 kHz 0x06 = 160 kHz 0x08 = 213 kHz 0x09 = 256 kHz 0x0C = 320 kHz 0x0F = 640 kHz Default value is 0x06 (160 kHz).
4	Miller Set	0x00/01	This field is changed if the subsequent field should be set. 0x00 = don't change other = change
5	Miller Value	0x00/01/02 /03	Sets the T=>R data rate and modulation format. 0x00 = FM0 baseband 0x01 = Miller-2 subcarrier 0x02 = Miller-4 subcarrier 0x03 = Miller-8 subcarrier Default value is 0x01 (miller-2 subcarrier).
6	Session Set	0x00/01	This field is changed if the subsequent field should be set. 0x00 = don't change other = change
7	Session Value	0x00/01/02	Chooses a session or the selected flag for the inventory round.

		/03	0x00 = S0 session 0x01 = S1 session 0x02 = S2 session 0x03 = S3 session Default value is 0x00 (S0 session).
8	TRext Set	0x00/01	This field is changed if the subsequent field should be set. 0x00 = don't change other = change
9	TRext Value	0x00/01	Chooses whether the T=>R preamble is pre-pended with a pilot tone. 0x00 = No pilot tone 0x01 = Use pilot tone Default is 0x01 (use pilot tone).
10	Q Begin Set	0x00/01	This field is changed if the subsequent field should be set. 0x00 = don't change other = change
11	Q Begin Value	0x00 ~ 0x0F	Starts a value for Q when doing inventory rounds. The first round will have 2^Q slots. Default value is 4.
12	Sensitivity Set	0x00/01	This field is changed if the subsequent field should be set. 0x00 = don't change other = change
13	Sensitivity Value	-128 ~ 127	Sets the sensitivity value for channel access, unit is dBm.

Response:

Byte Offset	Name	Value	Description
0	Response ID	0x5A	Response ID number of RFID_18K6CQueryParameter.
1	Data Length	0x0F	Byte number of response data length.
2	Status	0x00/0E/0F/FF	Performed result of command.
3	Link Frequency Set	0x00	This field is set to zero.
4	Link Frequency Value	0x00/06/08/09/0C/0F	Receives the T=>R link frequency. 0x00 = 40 kHz 0x06 = 160 kHz 0x08 = 213 kHz 0x09 = 256 kHz 0x0C = 320 kHz 0x0F = 640 kHz
5	Miller Set	0x00	This field is set to zero.
6	Miller Value	0x00/01/02/03	Receives the T=>R data rate and modulation format. 0x00 = FM0 baseband 0x01 = Miller-2 subcarrier 0x02 = Miller-4 subcarrier 0x03 = Miller-8 subcarrier
7	Session Set	0x00	This field is set to zero.
8	Session Value	0x00/01/02/03	Receives a session or the selected flag for the inventory round. 0x00 = S0 session 0x01 = S1 session 0x02 = S2 session

			0x03 = S3 session
9	TRext Set	0x00	This field is set to zero.
10	TRext Value	0x00/01	Receives whether the T=>R preamble is pre-pended with a pilot tone. 0x00 = No pilot tone 0x01 = Use pilot tone
11	Q Begin Set	0x00	This field is set to zero.
12	Q Begin Value	0x00 ~ 0x0F	Receives a value for Q when doing inventory rounds. The first round will have 2^Q slots.
13	Sensitivity Set	0x00	This field is set to zero.
14	Sensitivity Value	-128 ~ 127	Receives the sensitivity value for channel access, unit is dBm.

Effective Sensitivity Value List Table (dBm)					
-84	-81	-80	-77	-74	-71
-68	-65	-63	-60	-57	-54

4.3.1.2 Setting Quick Access Mode

MTI RFID module provides a special Quick Access Mode to simplify the process for the single tag application. After enable Quick Access Mode, the host can omit the inventory operation and select operation, just perform tag-protocol operation directly when only one tag in the field.
If there are multiple tags in the field, the host must disable the Quick Access Mode and follow the original process. Refer to section 4.3.2, 4.3.3 Tag-Protocol Operation Function for detailed information.

Description: Configures Quick Access Mode.

Command: **RFID_18K6CSetQuickAccessMode**

Byte Offset	Name	Value	Description
0	Command ID	0x5B	Command ID number of RFID_18K6CSetQuickAccessMode.
1	Data Length	0x03	Byte number of command data length.
2	Quick Access Mode	0x00/0x01	Setting Quick Access Mode. 0x00 = disabled 0x01 = enabled Default value is 0x00.

Response:

Byte Offset	Name	Value	Description
0	Response ID	0x5C	Response ID number of RFID_18K6CSetQuickAccessMode.
1	Data Length	0x03	Byte number of response data length.
2	Status	0x00/0E/0F/FF	Performed result of command.

4.3.1.3 Retrieving Quick Access Mode

Description: Retrieves the current setting of Quick Access Mode.

Command: **RFID_18K6CGetQuickAccessMode**

Byte Offset	Name	Value	Description
0	Command ID	0x5D	Command ID number of RFID_18K6CGetQuickAccessMode.
1	Data Length	0x02	Byte number of command data length.

Response:

Byte Offset	Name	Value	Description
0	Response ID	0x5E	Response ID number of RFID_18K6CGetQuickAccessMode.
1	Data Length	0x04	Byte number of response data length.
2	Status	0x00/0E/FF	Performed result of command.
3	Quick Access Mode	0x00/0x01	Receives the current setting of Quick Access Mode. 0x00 = disabled 0x01 = enabled

4.3.1.4 6C Tag Inventory Operation

Description: Executes a tag inventory for all tags of interest. Starts an inventory round to find new tags and gets tag information of all found tags.

The response data length of this command is different between USB and UART interface.
For USB interface it is fixed, the RFID module will pad zero value added to end of EPC Data field to force this packet to stuff 64 bytes length in order to fit a variety of USB development platform.
For UART interface it is variable.

Command: **RFID_18K6CTagInventory**

Byte Offset	Name	Value	Description
0	Command ID	0x31	Command ID number of RFID_18K6CTagInventory.
1	Data Length	0x03	Byte number of command data length.
2	Action	0x01/02/03	The host can select whether it wants to start a new inventory round, then RFID module will store the found tags information in the tag list buffer or if it wants to get information of the leftover tags from the tag list buffer. Start a new inventory round or perform any other 18K6C tag access command will reset the tag list buffer. 0x01 = start a new inventory round and get the first tag information 0x02 = get next tag information 0x03 = get all leftover tags information

Response (USB):

Byte Offset	Name	Value	Description
0	Response ID	0x32	Response ID number of RFID_18K6CTagInventory.
1	Data Length	0x40	Byte number of response data length.
2	Status	0x00/0E/0F/ 0A/FE/FF	Performed result of command.
3	Tag Number	0 ~ 30	Number of the tags in the tag buffer in this inventory round. Every time the host get the tag information from the tag list buffer, this value will minus 1. Example: 1: means this is the last tag in the tag buffer 0: means there is no tag in the tag buffer
4	EPC Length	0 ~ 58	Byte number of EPC Data field length.
n:5	EPC Data	0x00 ~ 0xFF	EPC data information. When the value of EPC Length field is more than 1, this field is valid. EPC Data = PC (2 bytes) + EPC Byte offset n = value of EPC Length field + 4

63:n+1	PADDING	0x00	Pad zero value added to end of returned data field to force this packet to stuff 64 bytes length.

Response (UART):

Byte Offset	Name	Value	Description
0	Response ID	0x32	Response ID number of RFID_18K6CTagInventory.
1	Data Length	0x05 ~ 0x3F	Byte number of response data length is variable.
2	Status	0x00/0E/0F/ 0A/FE/FF	Performed result of command.
3	Tag Number	0 ~ 30	Number of the tags in the tag buffer in this inventory round. Every time the host get the tag information from the tag list buffer, this value will minus 1. Example: 1: means this is the last tag in the tag buffer. 0: means there is no tag in the tag buffer.
4	EPC Length	0 ~ 58	Byte number of EPC Data field length.
n:5	EPC Data	0x00 ~ 0xFF	EPC data information. When the value of EPC Length field is more than 1, this field is valid. EPC Data = PC (2 bytes) + EPC Byte offset n = value of EPC Length field + 4

4.3.1.5 6C Tag Inventory Operation with RSSI

Description: Executes a tag inventory for all tags of interest. Starts an inventory round to find new tags and gets tag information of all found tags.

The response data length of this command is different between USB and UART interface.
For USB interface it is fixed, the RFID module will pad zero value added to end of EPC Data field to force this packet to stuff 64 bytes length in order to fit a variety of USB development platform.
For UART interface it is variable.

Command: **RFID_18K6CTagInventoryRSSI**

Byte Offset	Name	Value	Description
0	Command ID	0x43	Command ID number of RFID_18K6CTagInventoryRSSI.
1	Data Length	0x03	Byte number of command data length.
2	Action	0x01/02/03	The host can select whether it wants to start a new inventory round, then RFID module will store the found tags information in the tag list buffer or if it wants to get information of the leftover tags from the tag list buffer. Start a new inventory round or perform any other 18K6C tag access command will reset the tag list buffer. 0x01 = start a new inventory round and get the first tag information 0x02 = get next tag information 0x03 = get all leftover tags information

Response (USB):

Byte Offset	Name	Value	Description
0	Response ID	0x44	Response ID number of RFID_18K6CTagInventoryRSSI.
1	Data Length	0x40	Byte number of response data length.
2	Status	0x00/0E/0F/ 0A/FE/FF	Performed result of command.
3	Tag Number	0 ~ 30	Number of the tags in the tag buffer in this inventory round.

			Every time the host get the tag information from the tag list buffer, this value will minus 1. Example: 1: means this is the last tag in the tag buffer. 0: means there is no tag in the tag buffer.
4	RSSI	-128 ~ 127	RSSI value, unit is dBm.
7:5	Frequency	0x00 ~ 0xFF	Frequency value of operational channel. [5] = Frequency[7:0] = Frequency Low [6] = Frequency[15:8] = Frequency Mid [7] = Frequency[23:16] = Frequency High
8	EPC Length	0 ~ 54	Byte number of EPC Data field length.
n:9	EPC Data	0x00 ~ 0xFF	EPC data information. When the value of EPC Length field is more than 1, this field is valid. EPC Data = PC (2 bytes) + EPC Byte offset n = value of EPC Length field + 8
63:n+1	PADDING	0x00	Pad zero value added to end of returned data field to force this packet to stuff 64 bytes length.

Response (UART):

Byte Offset	Name	Value	Description
0	Response ID	0x44	Response ID number of RFID_18K6CTagInventoryRSSI.
1	Data Length	0x09 ~ 0x3F	Byte number of response data length is variable.
2	Status	0x00/0E/0F/ 0A/FE/FF	Performed result of command.
3	Tag Number	0 ~ 30	Number of the tags in the tag buffer in this inventory round. Every time the host get the tag information from the tag list buffer, this value will minus 1. Example: 1: means this is the last tag in the tag buffer. 0: means there is no tag in the tag buffer.
4	RSSI	-128 ~ 127	RSSI value, unit is dBm.
7:5	Frequency	0x00 ~ 0xFF	Frequency value of operational channel. [5] = Frequency[7:0] = Frequency Low [6] = Frequency[15:8] = Frequency Mid [7] = Frequency[23:16] = Frequency High
8	EPC Length	0 ~ 54	Byte number of EPC Data field length.
n:9	EPC Data	0x00 ~ 0xFF	EPC data information. When the value of EPC Length field is more than 1, this field is valid. EPC Data = PC (2 bytes) + EPC Byte offset n = value of EPC Length field + 8

4.3.1.6 6C Tag Select Operation

Description: To communicate with one tag the host must isolate one of the found tags. The host needs to send always all EPC bytes to the RFID module regardless how long the EPC mask is specified.

The data length of this command is not fixed value. Maybe for differential USB development platform, the application needs to send fixed size of packet. For this command, the application can pad zero value added to end of Mask Data field to force this packet to stuff 64 bytes length.

Command: **RFID_18K6CTagSelect**

Byte	Name	Value	Description

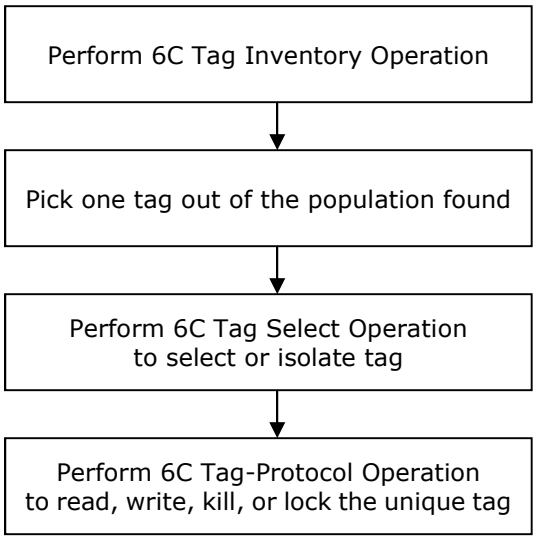
Offset			
0	Command ID	0x33	Command ID number of RFID_18K6CTagSelect.
1	Data Length	0x03 ~ 0x22	Byte number of command data length.
2	Mask Length	0 ~ 31	Length of EPC mask data in bytes.
n:3	Mask Data	0x00 ~ 0xFF	EPC mask data. When the value of EPC Length field is more than 1, this field is valid. Byte offset n = value of Mask Length field + 2 [3] = mask data 0 [4] = mask data 1 … Example: EPC value = 0x01 02 03 04 05 06 07 08 09 0A 0B 0C Mask Length = 0x0C (mask all EPC value, 12 bytes) [3] = mask data 0 = 0x01 [4] = mask data 1 = 0x02 [5] = mask data 2 = 0x03 [6] = mask data 3 = 0x04 [7] = mask data 4 = 0x05 [8] = mask data 5 = 0x06 [9] = mask data 6 = 0x07 [10] = mask data 7 = 0x08 [11] = mask data 8 = 0x09 [12] = mask data 9 = 0x0A [13] = mask data 10 = 0x0B [14] = mask data 11 = 0x0C

Response:

Byte Offset	Name	Value	Description
0	Response ID	0x34	Response ID number of RFID_18K6CTagSelect.
1	Data Length	0x03	Byte number of response data length.
2	Status	0x00/09/0E /0A/FF	Performed result of command. 0x00 = tag found 0x09 = tag not found

4.3.2 Tag-Protocol Operation Functions

After inventory operation, first the host should send a select operation in case there are several tags found, and then perform the tag-protocol operation. After a tag-protocol operation was performed, the host should re-send a select operation except write EPC memory bank. After the EPC memory bank was written, the host should re-send an inventory operation. The correct sequences to operate these commands are shown below:



4.3.2.1 6C Tag Read Operation

Description: A read operation can be used to read one or more 16-bit words from any of a tag's memory banks. Reads may only be performed on 16-bit word boundaries and for multiples of 16-bit words. If one or more of the memory words specified by the Address/Length combination do not exist or are read-locked, the read from the tag fails and this failure is reported through the operation response packet.

The response data length of this command is different between USB and UART interface.
For USB interface it is fixed, the RFID module will pad zero value added to end of EPC Data field to force this packet to stuff 64 bytes length in order to fit a variety of USB development platform.
For UART interface it is variable.

Command: **RFID_18K6CTagRead**

Byte Offset	Name	Value	Description
0	Command ID	0x37	Command ID number of RFID_18K6CTagRead.
1	Data Length	0x09	Byte number of command data length.
2	Memory Bank	0x00 ~ 0x03	The memory bank from which to read. Valid values are: 0x00 = Reserved memory 0x01 = EPC memory 0x02 = TID memory 0x03 = User memory
3	Memory Address	0x00 ~ 0x7F	The address of the first 16-bit word, where zero is the first 16-bit word in the memory bank, to read from the specified memory bank.
7:4	Access Password	0x00 ~ 0xFF	The access password for the tags. A value of zero indicates no access password. [4] = Access Password[31:24] [5] = Access Password[23:16] [6] = Access Password[15:8] [7] = Access Password[7:0]

8	Tag Data Length	1 ~ 30	The number of 16-bit words to be read.

Response (USB):

Byte Offset	Name	Value	Description
0	Response ID	0x38	Response ID number of RFID_18K6CTagRead.
1	Data Length	0x40	Byte number of response data length.
2	Status	0x00 ~ 0xFF	Performed result of command.
3	Tag Data Length	0 ~ 30	Length of tag data in words.
n:4	Tag Data	0x00 ~ 0xFF	Tag data information in words. When the value of Tag Data Length field is >= 1, this field is valid. Byte offset n = 2 * value of Tag Data Length field + 3
63:n+1	PADDING	0x00	Pad zero value added to end of returned data field to force this packet to stuff 64 bytes length.

Response (UART):

Byte Offset	Name	Value	Description
0	Response ID	0x38	Response ID number of RFID_18K6CTagRead.
1	Data Length	0x04 ~ 0x40	Byte number of response data length is variable. Tag Data Length = 0, this field = 0x04 Tag Data Length > 0, this field = 2*value of Tag Data Length field+4
2	Status	0x00 ~ 0xFF	Performed result of command.
3	Tag Data Length	0 ~ 30	Length of tag data in words.
n:4	Tag Data	0x00 ~ 0xFF	Tag data information in words. When the value of Tag Data Length field is >= 1, this field is valid. Byte offset n = 2 * value of Tag Data Length field + 3

4.3.2.2 6C Tag Write Operation

Description: A write operation allows a host to write one or more 16-bit word to the specified memory bank of the ISO 18000-6C tags of interest. Writes may only be performed on 16-bit word boundaries. If one memory word specified by the Address/Length does not exist or is write-locked, the write to the tag fails and this failure is reported through the operation response packet.

The data length of this command is not fixed value. Maybe for differential USB development platform, the application needs to send fixed size of packet. For this command, the application can pad zero value added to end of Tag Data field to force this packet to stuff 63 bytes length.

Command: **RFID_18K6CTagWrite**

Byte Offset	Name	Value	Description
0	Command ID	0x35	Command ID number of RFID_18K6CTagWrite.
1	Data Length	0x0B ~ 0x3F	Byte number of command data length.
2	Memory Bank	0x00 ~ 0x03	The memory bank in which to write. Valid values are: 0x00 = Reserved memory 0x01 = EPC memory 0x02 = TID memory 0x03 = User memory
3	Memory Address	0x00 ~ 0x7F	The address of the first 16-bit word, where zero is the first 16-bit word in the memory bank, to write in the specified memory bank.

7:4	Access Password	0x00 ~ 0xFF	The access password for the tags. A value of zero indicates no access password. [4] = Access Password[31:24] [5] = Access Password[23:16] [6] = Access Password[15:8] [7] = Access Password[7:0]
8	Tag Data Length	1 ~ 27	The number of 16-bit words to be writes.
n:9	Tag Data	0x00 ~ 0xFF	The 16-bit word value to be written to the tag's specified memory bank. When the value of Tag Data Length field is >= 1, this field is valid. Byte offset n = 2 * value of Tag Data Length field + 8

Response:

Byte Offset	Name	Value	Description
0	Response ID	0x36	Response ID number of RFID_18K6CTagWrite.
1	Data Length	0x04	Byte number of response data length.
2	Status	0x00 ~ 0xFF	Performed result of command.
3	Written Number	0 ~ 27	Number of words written. Number of data written into tag (in unit of words). CAUTION: It contains valid information even if "Status" is replied error instead of RFID_STATUS_OK (Success). For example, when RFID_ERROR_6CTAG_MEMORY_OVERRUN (memory address do not exist) is reported, it may implies some words had been written into tag memory, but remain words can not due to memory address exceeded

4.3.2.3 6C Tag Kill Operation

Description: A kill operation allows a host to kill (i.e. render inoperable) a set of tags of interest. Tag's whose kill password value is zero do not execute a kill operation; if such a tag receives an RFID_18K6CTagKill it ignores this command and backscatters an error code.

Command: **RFID_18K6CTagKill**

Byte Offset	Name	Value	Description
0	Command ID	0x3D	Command ID number of RFID_18K6CTagKill.
1	Data Length	0x06	Byte number of command data length.
5:2	Kill Password	0x00 ~ 0xFF	The kill password for the tags. [2] = Kill Password[31:24] [3] = Kill Password[23:16] [4] = Kill Password[15:8] [5] = Kill Password[7:0]

Response:

Byte Offset	Name	Value	Description
0	Response ID	0x3E	Response ID number of RFID_18K6CTagKill.
1	Data Length	0x03	Byte number of response data length.
2	Status	0x00 ~ 0xFF	Performed result of command.

4.3.2.4 6C Tag Lock Operation

A tag-permission command (tag lock) allows the host to set the access permissions of a tag. These include the following:

- Set whether or not an access password is required to write to the EPC, TID, or user memory banks.
- Set whether or not the above memory-write permission is permanently set. Once the memory-write permission has been permanently set, attempts to change the permission or turn off the permanent setting fail.
- Set a memory bank to be read-only.
- Set whether or not the individual passwords (i.e. access and kill) may be accessed (i.e. read and written) and, if they are accessible, whether or not an access password is required to read the individual passwords (i.e. access and kill).
- Set whether or not the above password-access permission is permanently set. Once the password-access permission has been permanently set, attempts to change the permission or turn off the permanent setting fail.
- Set the individual passwords to be inaccessible (i.e. unable to be read or written).

For a tag, there are five access permissions that may be set: access permissions for the EPC, TID, and user memory banks and access permissions for the access and kill passwords.

There are several scenarios in which attempting to set a tag's access permissions may fail:

- Attempting to change the access permission for a non-existent memory bank or password.
- Attempting to change an access permission that has been previously set as permanent.
- Attempting to change the permanent status of an access permission that has been previously set as permanent.
- Attempting to lock a password or memory bank that is not lockable.
- Attempting to unlock a password or memory bank that is not un-lockable.

Description: A lock operation allows a host to execute a tag lock (setting a tag's access permissions) for all tags of interest.

Command: **RFID_18K6CTagLock**

Byte Offset	Name	Value	Description
0	Command ID	0x3B	Command ID number of RFID_18K6CTagLock.
1	Data Length	0x08	Byte number of command data length.
2	Lock Action	0x00 ~ 0x03	Lock actions. The access permissions for the kill/access two passwords of tag. 0x00 = Accessible: The password can be read and written when the tag is in either the open or secured states. 0x01 = Always Accessible: The password can be read and written when the tag is in either the open or secured states and this access permission should be set permanently. 0x02 = Password Accessible: The password can be read or written only when the tag is in the secured state. 0x03 = Always Not Accessible: The password can not be read or written and this access permission should be set permanently. The access permissions for the EPC/TID/User three memory banks of tag. 0x00 = Writeable: The memory bank is writeable when the tag is in either the open or secured states.

			0x01 = Always Writeable: The memory bank is writeable when the tag is in either the open or secured states and this access permission should be set permanently. 0x02 = Password Writeable: The memory bank is writeable only when the tag is in the secured state. 0x03 = Always Not Writeable: The memory bank is not writeable and this access permission should be set permanently.
3	Memory Space	0x00 ~ 0x04	Select the memory space, which should be locked. 0x00 = Kill Password in Reserved memory bank 0x01 = Access Password in Reserved memory bank 0x02 = EPC memory bank 0x03 = TID memory bank 0x04 = User memory bank
7:4	Access Password	0x00 ~ 0xFF	The access password for the tags. [4] = Access Password[31:24] [5] = Access Password[23:16] [6] = Access Password[15:8] [7] = Access Password[7:0]

Response:

Byte Offset	Name	Value	Description
0	Response ID	0x3C	Response ID number of RFID_18K6CTagLock.
1	Data Length	0x03	Byte number of response data length.
2	Status	0x00 ~ 0xFF	Performed result of command.

4.3.2.5 6C Tag Block Write Operation

Description: Tags implemented BlockWrite (optional command in the ISO 18000-6C standard) allow an interrogator to write multiple words in tag's memory (reserved, EPC, TID or user memory bank) using a single command. Command/Response and user scenario of BlockWrite are the same as Write command.

The data length of this command is not fixed value. Maybe for differential USB development platform, the application needs to send fixed size of packet. For this command, the application can pad zero value added to end of Tag Data field to force this packet to stuff 63 bytes length.

Command: **RFID_18K6CTagBlockWrite**

Byte Offset	Name	Value	Description
0	Command ID	0x70	Command ID number of RFID_18K6CTagBlockWrite.
1	Data Length	0x0B ~ 0x13	Byte number of command data length.
2	Memory Bank	0x00 ~ 0x03	The memory bank in which to write. Valid values are: 0x00 = Reserved memory 0x01 = EPC memory 0x02 = TID memory 0x03 = User memory
3	Memory Address	0x00 ~ 0x7F	The address of the first 16-bit word, where zero is the first 16-bit word in the memory bank, to write in the specified memory bank.
7:4	Access Password	0x00 ~ 0xFF	The access password for the tags. A value of zero indicates no access password.

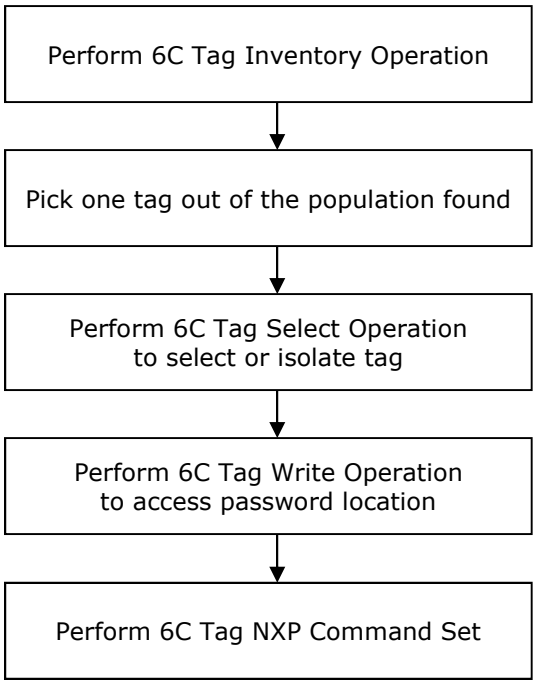
			[4] = Access Password[31:24] [5] = Access Password[23:16] [6] = Access Password[15:8] [7] = Access Password[7:0]
8	Tag Data Length	1 ~ 5	The number of 16-bit words to be written.
n:9	Tag Data	0x00 ~ 0xFF	The data (16-bits words) to be written to the tag's specified memory bank. When the value of Tag Data Length field is >= 1, this field is valid. Byte offset n = 2 * value of Tag Data Length field + 8

Response:

Byte Offset	Name	Value	Description
0	Response ID	0x71	Response ID number of RFID_18K6CTagBlockWrite.
1	Data Length	0x04	Byte number of response data length.
2	Status	0x00 ~ 0xFF	Performed result of command.
3	Written Number	0 ~ 5	Number of words (=2 Bytes) written to tag. Unlike Write Command, it shall be either zero or Tag Data Length.

4.3.3 Tag-NXP Command Operation Function

After inventory operation, first the host should send a select operation in case there are several tags found, and then perform the write operation and the NXP command set. After a NXP command was performed, the host should re-send a select operation. The correct sequences to operate these commands are shown below:



The NXP tag which Protect EPC bit in Config-Word has been set to '1' by Change Read Protect Status (set) or Change Config command, its EPC data in the EPC memory will return '0' and can't be selected. If the host wants to access the NXP tag which has been read protected, need to enable Quick Access Mode and omit select operation to perform tag-protocol operation directly. Refer to section 4.3.1.2 for detailed information.

4.3.3.1 6C Tag NXP Command Set Operation

Description: Performs NXP custom command set for special NXP tags of interest.

Command: **RFID_18K6CTagNXPCommand**

Byte Offset	Name	Value	Description
0	Command ID	0x45	Command ID number of RFID_18K6CTagNXPCommand.
1	Data Length	0x0A	Byte number of command data length.
2	NXP Command	0x01/02/09	NXP custom command set. 0x01 = Change EAS Status 0x02 = Change Read Protect Status 0x09 = Change Config
3	Bit Status	0x00/0x01	Bit status information. NXP Command = 0x01, 0x00 = reset / 0x01 = set NXP Command = 0x02, 0x00 = reset / 0x01 = set NXP Command = 0x09, this field is invalid This field set or reset the appropriate Bit of Change EAS and Read protect command. It's no function for Change Config command.
7:4	Access Password	0x00 ~ 0xFF	The access password for the tags. [4] = Access Password[31:24] [5] = Access Password[23:16]

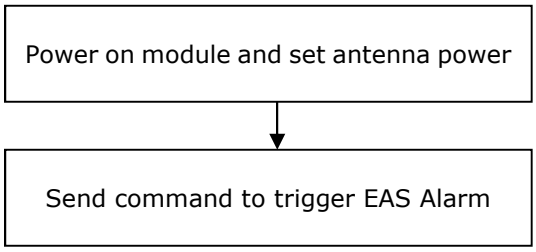
			[6] = Access Password[15:8] [7] = Access Password[7:0] CAUTION: If Access Password is zero or tags do not have Access Password, perform Change EAS Status / Change ReadProtect Status (set) command will be ignored by tag or perform Change Config command, tag won't modify Config-Word but backscatter the current Config-Word.
9:8	Toggled Config-Word	0x00 ~ 0xFF	The bits of Config-Word which the host wants to toggle (0->1, 1->0) set to 1. [8] = Toggled Config-Word[0:7] [9] = Toggled Config-Word[8:15] Example: If the original value of the PSF Alarm bit is 0. Set 0x0001 first time will activate the PSF Alarm bit (=1). Set 0x0001 again will deactivate the PSF Alarm bit (=0). Invalid toggling on indicator or RFU bits of Config-Word are ignored. This field is only valid when NXP Command field is 0x09.

Response:

Byte Offset	Name	Value	Description
0	Response ID	0x46	Response ID number of RFID_18K6CTagNXPCommand.
1	Data Length	0x05	Byte number of response data length.
2	Status	0x00 ~ 0xFF	Performed result of command.
4:3	Config-Word	0x00 ~ 0xFF	Current Config-Word backscattered by tag. [3] = Config-Word[0:7] [4] = Config-Word[8:15] This field is valid when the value of NXP Command field in the command is 0x09 and the value of Status field is 0x00.

4.3.3.2 6C Tag NXP Trigger EAS Alarm Operation

Due to the uniqueness of "triggering" EAS Alarm (not set/reset); it is divided from NXP commands. Tags with EAS Alarm is set (refer to NXP Command: Change EAS Status) shall response to EAS Alarm code immediately without any delay caused by Select/Query. 64-bits EAS Alarm code backscattered from tags is expected. The alarm code is fixed numbers but may be various depend on different types of tag in the future. For G2iL+ and G2iM tags, whether EAS Alarm is set can be check by reading 15th bit of Config-Word. It is also known as "PSF Alarm". Enable EAS Alarm in previous is necessary for triggering EAS Alarm. The host may enable this feature by writing to Config-Word directly, or using NXP commands.



After receive EAS Code, the RFID module do correctness check and newly defined response stats RFID_ERROR_18K6C_EASCODE will be replied if EAS Code do not match known valid EAS Code stored in OEM configuration data area.

Command: **RFID_18K6CTagNXPTriggerEASAlarm**

Byte Offset	Name	Value	Description
0	Command ID	0x72	Command ID number of RFID_18K6CTagNXPTriggerEASAlarm.
1	Data Length	0x02	Byte number of command data length.

Response:

Byte Offset	Name	Value	Description
0	Response ID	0x73	Response ID number of RFID_18K6CTagNXPTriggerEASAlarm.
1	Data Length	0x0B	Byte number of response data length.
2	Status	0x00 ~ 0xFF	Performed result of command.
10:3	EAS Code	See Description	64-bits EAS Code backscattered from tags. EAS Code is fixed hex number: 690A EC7C D215 D8F9 for G2iL+, G2iM and G2X series. This field reports received EAS Code or all zero value depends on different value of Status field: Status = RFID_STATUS_OK: EAS Code is received and considered valid. Received EAS Code is replied. Status = RFID_ERROR_18K6C_EASCODE: EAS Code is received, but considered invalid. Received EAS Code is still replied anyway. Other Status: No EAS Code is received. 8 bytes zeroes should be reported.

4.4 RFID Module Firmware Access

4.4.1 Retrieving the RFID Module's MAC Firmware and Hardware Version Information

Description: Retrieves the version number and information of the RFID module's MAC firmware, hardware and OEMCfg.

Command: **RFID_MacGetModuleID**

Byte Offset	Name	Value	Description
0	Command ID	0x10	Command ID number of RFID_MacGetModuleID.
1	Data Length	0x03	Byte number of command data length.
2	Module ID	0x00/01/02/03	ID information of firmware, hardware or OEMCfg. 0x00 = Firmware ID 0x01 = Hardware ID 0x02 = OEMCfg ID 0x03 = OEMCfg Update ID

Response:

Byte Offset	Name	Value	Description
0	Response ID	0x11	Response ID number of RFID_MacGetModuleID.
1	Data Length	0x30	Byte number of response data length.
2	Status	0x00/0E/0F/FF	Performed result of command.
47:3	ID Information	0x00 ~ 0xFF	The RFID module's ID information. Four leading characters are [AP]; indicate the module is in the application state.

4.4.2 Retrieving the RFID Module's MAC Firmware Debug Value

Description: Retrieves the fixed MAC firmware debug value for test purpose only.

Command: **RFID_MacGetDebugValue**

Byte Offset	Name	Value	Description
0	Command ID	0xA2	Command ID number of RFID_MacGetDebugValue.
1	Data Length	0x02	Byte number of command data length.

Response:

Byte Offset	Name	Value	Description
0	Response ID	0xA3	Response ID number of RFID_MacGetDebugValue.
1	Data Length	0x05	Byte number of response data length.
2	Status	0x00/0E/FF	Performed result of command.
3	Debug Value 1	0xA5	Fixed number, 0xA5.
4	Debug Value 2	0x5A	Fixed number, 0x5A.

4.4.3 Accessing RFID Module Hardware Registers

4.4.3.1 Writing to an RFID Module Hardware Register

The MAC firmware supports a mode, called MAC firmware bypass, which allows a host to write directly to the RFID module's hardware registers. Generally, applications do not need to perform any direct accessing of RFID module registers. For those applications that require direct access to the underlying RFID module's hardware registers, great care must be taken as inadvertently writing RFID module registers may render the RFID module inoperable.

Description: Writes directly to a RFID module hardware register.

Command: **RFID_MacBypassWriteRegister**

Byte Offset	Name	Value	Description
0	Command ID	0x1A	Command ID number of RFID_MacBypassWriteRegister.
1	Data Length	0x06	Byte number of command data length.
2	Register Address	0x00 ~ 0xFF	The address of hardware registers.
5:3	Register Data	0x00 ~ 0xFF	The data of hardware registers. Byte 4 and 5 are optional data. If data is longer than one byte, the data is written into one of the 3 bytes deep register. [3] = Hardware register data[7:0] [4] = Hardware register data[15:8] [5] = Hardware register data[23:16]

Response:

Byte Offset	Name	Value	Description
0	Response ID	0x1B	Response ID number of RFID_MacBypassWriteRegister.
1	Data Length	0x03	Byte number of response data length.
2	Status	0x00/0E/FF	Performed result of command.

4.4.3.2 Reading from an RFID Module Hardware Register

The MAC firmware supports a mode, called bypass, which allows a host to read the RFID module's hardware registers.

Description: Reads directly from a RFID module hardware register.

Command: **RFID_MacBypassReadRegister**

Byte Offset	Name	Value	Description
0	Command ID	0x1C	Command ID number of RFID_MacBypassReadRegister.
1	Data Length	0x03	Byte number of command data length.
2	Register Address	0x00 ~ 0xFF	The address of hardware registers.

Response:

Byte Offset	Name	Value	Description
0	Response ID	0x1D	Response ID number of R RFID_MacBypassReadRegister.
1	Data Length	0x06	Byte number of response data length.
2	Status	0x00/0E/FF	Performed result of command.
5:3	Register Data	0x00 ~ 0xFF	The data of hardware registers. Byte 4 and 5 are optional data. If one of the 3 bytes deep registers is selected the RFID module sends back 3 bytes data.

			[3] = Hardware register data[7:0] [4] = Hardware register data[15:8] [5] = Hardware register data[23:16]

4.4.4 Accessing MAC Firmware-Resident OEM Configuration Data

The MAC firmware manages a portion of non-volatile memory that contains OEM configuration data. A host can access (i.e. read and write) this memory. The MAC firmware treats the OEM configuration data as a sequence of byte values. The MAC firmware accepts and returns the OEM configuration data values in the MAC's native format.
For detailed information, refer to the *MTI RU-888 RFID Module OEM Configuration Guide* document.

4.4.4.1 Writing MAC Firmware OEM Configuration Data

Description: Writes one byte value to the MAC firmware's OEM configuration data area.

Command: **RFID_MacWriteOemData**

Byte Offset	Name	Value	Description
0	Command ID	0xA4	Command ID number of RFID_MacWriteOemData.
1	Data Length	0x05	Byte number of command data length.
3:2	OEMCfg Address	0x00 80 ~ 0x07 FF	The address of OEM configuration data.
4	OEMCfg Data	0x00 ~ 0xFF	The data of OEM configuration data.

Response:

Byte Offset	Name	Value	Description
0	Response ID	0xA5	Response ID number of RFID_MacWriteOemData.
1	Data Length	0x03	Byte number of response data length.
2	Status	0x00/0E/0F/ A0/A1/FF	Performed result of command.

4.4.4.2 Reading MAC Firmware OEM Configuration Data

Description: Reads one byte value from the MAC firmware's OEM configuration data area.

Command: **RFID_MacReadOemData**

Byte Offset	Name	Value	Description
0	Command ID	0xA6	Command ID number of RFID_MacReadOemData.
1	Data Length	0x04	Byte number of command data length.
3:2	OEMCfg Address	0x00 00 ~ 0x1F FF	The address of OEM configuration data.

Response:

Byte Offset	Name	Value	Description
0	Response ID	0xA7	Response ID number of RFID_MacReadOemData.
1	Data Length	0x04	Byte number of response data length.
2	Status	0x00/0E/0F/ FF	Performed result of command.
3	OEMCfg Data	0x00 ~ 0xFF	The data of OEM configuration data.

4.4.5 Performing a Software Reset

Description: Causes the MAC firmware to perform the specified reset. The MAC firmware runs built in self test and reinitialize all board hardware. The RFID module is placed in an idle state.

Command: **RFID_MacSoftReset**

Byte Offset	Name	Value	Description
0	Command ID	0xA0	Command ID number of RFID_MacSoftReset.
1	Data Length	0x02	Byte number of command data length.

Response:

Byte Offset	Name	Value	Description
0	Response ID	0xA1	Response ID number of RFID_MacSoftReset.
1	Data Length	0x03	Byte number of response data length.
2	Status	0x00/0E/FF	Performed result of command.

4.4.6 Entering the Firmware Update Mode

Description: The RFID module enters firmware update mode.

CAUTION: MTI RFID module supports firmware update via the USB or UART interface, depending on the OEM configuration. The host processor must confirm that the interface setting of OEM configuration is needed before entering the firmware update mode. Refer to the *MTI RU-888 RFID Module OEM Configuration Guide* document for detailed information.

Command: **RFID_MacEnterUpdateMode**

Byte Offset	Name	Value	Description
0	Command ID	0xD0	Command ID number of RFID_MacEnterUpdateMode.
1	Data Length	0x02	Byte number of command data length.

Response:

Byte Offset	Name	Value	Description
0	Response ID	0xD1	Response ID number of RFID_MacEnterUpdateMode.
1	Data Length	0x03	Byte number of response data length.
2	Status	0x00/0E/FF	Performed result of command.

5 Use Cases

5.1 Read the EPC Value from EPC Memory Bank of a 6C Tag

[Step 1]
Purpose: Configures the RF power level of physical antenna port to 18 dBm.
Command: RFID_AntennaPortSetPowerLevel (ID: 0xC0)

[Step 2]
Purpose: Executes a tag inventory for all tags and get the first tag data.
Command: RFID_18K6CTagInventory (ID: 0x31)

[Step 3]
Purpose: Gets the second tag data.
Command: RFID_18K6CTagInventory (ID: 0x31)

[Step 4]
Purpose: Selects one of the found tags.
Command: RFID_18K6CTagSelect (ID: 0x33)

[Step 5]
Purpose: Reads the EPC value from EPC memory bank of the 6C tag.
Command: RFID_18K6CTagRead (ID: 0x37)

Table 5.1.1 – USB Command and Response Sequences of Use Case 5.1

Step	Data Flow	Command / Response Packet
1t	Host => Module	C0 03 12
1r	Host <= Module	C1 03 00
2t	Host => Module	31 03 01
2r	Host <= Module	32 40 00 02 0E 30 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3t	Host => Module	31 03 02
3r	Host <= Module	32 40 00 01 0E 30 00 11 22 33 44 55 66 77 88 99 AA BB CC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
4t	Host => Module	33 0F 0C 01 02 03 04 05 06 07 08 09 0A 0B 0C
4r	Host <= Module	34 03 00
5t	Host => Module	37 09 01 02 00 00 00 00 06
5r	Host <= Module	38 40 00 06 01 02 03 04 05 06 07 08 09 0A 0B 0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Table 5.1.2 - UART Command and Response Sequences of Use Case 5.1

Step	Data Flow	Command / Response Packet
1t	Host => Module	4D 54 49 43 FF **C0 03 12** 92 18
1r	Host <= Module	4D 54 49 52 00 **C1 03 00** 72 F3
2t	Host => Module	4D 54 49 43 FF **31 03 01** 64 28
2r	Host <= Module	4D 54 49 52 00 **32 13 00 02 0E 30 00 01 02 03 04 05 06 07 08 09 0A 0B 0C** 9F 01
3t	Host => Module	4D 54 49 43 FF **31 03 02** 54 4B

3r	Host <= Module	4D 54 49 52 00 **32 13 00 01 0E 30 00 11 22 33 44 55 66 77 88 99 AA BB CC** BB 54
4t	Host => Module	4D 54 49 43 FF **33 0F 0C 01 02 03 04 05 06 07 08 09 0A 0B 0C** 59 94
4r	Host <= Module	4D 54 49 52 00 **34 03 00** 7A 51
5t	Host => Module	4D 54 49 43 FF **37 09 01 02 00 00 00 00 06** 82 BD
5r	Host <= Module	4D 54 49 52 00 **38 10 00 06 01 02 03 04 05 06 07 08 09 0A 0B 0C** E9 44

5.2 Write the EPC Value to EPC Memory Bank of a 6C Tag

[Step 1]
Purpose: Configures the RF power level of physical antenna port to 18 dBm.
Command: RFID_AntennaPortSetPowerLevel (ID: 0xC0)

[Step 2]
Purpose: Executes a tag inventory for all tags and get the first tag data.
Command: RFID_18K6CTagInventory (ID: 0x31)

[Step 3]
Purpose: Gets the second tag data.
Command: RFID_18K6CTagInventory (ID: 0x31)

[Step 4]
Purpose: Selects one of the found tags.
Command: RFID_18K6CTagSelect (ID: 0x33)

[Step 5]
Purpose: Writes the EPC value to EPC memory bank of the 6C tag.
Command: RFID_18K6CTagWrite (ID: 0x35)

Table 5.2.1 - USB Command and Response Sequences of Use Case 5.2

Step	Data Flow	Command / Response Packet
1t	Host => Module	C0 03 12
1r	Host <= Module	C1 03 00
2t	Host => Module	31 03 01
2r	Host <= Module	32 40 00 02 0E 30 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3t	Host => Module	31 03 02
3r	Host <= Module	32 40 00 01 0E 30 00 11 22 33 44 55 66 77 88 99 AA BB CC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
4t	Host => Module	33 0F 0C 01 02 03 04 05 06 07 08 09 0A 0B 0C
4r	Host <= Module	34 03 00
5t	Host => Module	35 15 01 02 00 00 00 00 06 F1 F2 F3 F4 F5 F6 F7 F8 F9 FA FB FC
5r	Host <= Module	36 04 00 06

Table 5.2.2 - UART Command and Response Sequences of Use Case 5.2

Step	Data Flow	Command / Response Packet
1t	Host => Module	4D 54 49 43 FF **C0 03 12** 92 18
1r	Host <= Module	4D 54 49 52 00 **C1 03 00** 72 F3
2t	Host => Module	4D 54 49 43 FF **31 03 01** 64 28
2r	Host <= Module	4D 54 49 52 00 **32 13 00 02 0E 30 00 01 02 03 04 05 06 07 08 09 0A 0B 0C** 9F 01
3t	Host => Module	4D 54 49 43 FF **31 03 02** 54 4B
3r	Host <= Module	4D 54 49 52 00 **32 13 00 01 0E 30 00 11 22 33 44 55 66 77 88 99 AA BB CC** BB 54
4t	Host => Module	4D 54 49 43 FF **33 0F 0C 01 02 03 04 05 06 07 08 09 0A 0B 0C** 59 94
4r	Host <= Module	4D 54 49 52 00 **34 03 00** 7A 51
5t	Host => Module	4D 54 49 43 FF **35 15 01 02 00 00 00 00 06 F1 F2 F3 F4 F5 F6 F7 F8 F9 FA FB FC** CA D1

5r	Host <= Module	4D 54 49 52 00 **36 04 00 06** 98 EC

5.3 Kill a Specific 6C Tag

[Step 1]
Purpose: Configures the RF power level of physical antenna port to 18 dBm.
Command: RFID_AntennaPortSetPowerLevel (ID: 0xC0)

[Step 2]
Purpose: Executes a tag inventory for all tags and get the first tag data.
Command: RFID_18K6CTagInventory (ID: 0x31)

[Step 3]
Purpose: Gets the second tag data.
Command: RFID_18K6CTagInventory (ID: 0x31)

[Step 4]
Purpose: Selects one of the found tags.
Command: RFID_18K6CTagSelect (ID: 0x33)

[Step 5]
Purpose: Reads the kill password value from RESERVED memory bank of the 6C tag.
Command: RFID_18K6CTagRead (ID: 0x37)

Tag's whose kill password value is zero do not execute a kill operation; if such a tag receives an RFID_18K6CTagKill it ignores this command and backscatters an error code.
If the tag's kill password is zero, perform step 6 to change the kill password to nonzero.
If the tag's kill password is nonzero, skip step 6 to perform the kill operation directly.

[Step 6]
Purpose: Writes the nonzero value to Kill Password location of RESERVED memory bank of the 6C tag when the tag's kill password is zero
Command: RFID_18K6CTagWrite (ID: 0x35)

[Step 7]
Purpose: Kills the specific 6C tag with valid nonzero kill password.
Command: RFID_18K6CTagKill (ID: 0x3D)

Table 5.3.1 - USB Command and Response Sequences of Use Case 5.3

Step	Data Flow	Command / Response Packet
1t	Host => Module	C0 03 12
1r	Host <= Module	C1 03 00
2t	Host => Module	31 03 01
2r	Host <= Module	32 40 00 02 0E 30 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3t	Host => Module	31 03 02
3r	Host <= Module	32 40 00 01 0E 30 00 11 22 33 44 55 66 77 88 99 AA BB CC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
4t	Host => Module	33 0F 0C 01 02 03 04 05 06 07 08 09 0A 0B 0C
4r	Host <= Module	34 03 00
5t	Host => Module	37 09 00 00 00 00 00 00 02
5r	Host <= Module	38 40 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
6t	Host => Module	35 0D 00 00 00 00 00 00 02 DE AD C0 DE
6r	Host <= Module	36 04 00 02

7t	Host => Module	3D 06 DE AD C0 DE
7r	Host <= Module	3E 03 00

Table 5.3.2 - UART Command and Response Sequences of Use Case 5.3

Step	Data Flow	Command / Response Packet
1t	Host => Module	4D 54 49 43 FF **C0 03 12** 92 18
1r	Host <= Module	4D 54 49 52 00 **C1 03 00** 72 F3
2t	Host => Module	4D 54 49 43 FF **31 03 01** 64 28
2r	Host <= Module	4D 54 49 52 00 **32 13 00 02 0E 30 00 01 02 03 04 05 06 07 08 09 0A 0B 0C** 9F 01
3t	Host => Module	4D 54 49 43 FF **31 03 02** 54 4B
3r	Host <= Module	4D 54 49 52 00 **32 13 00 01 0E 30 00 11 22 33 44 55 66 77 88 99 AA BB CC** BB 54
4t	Host => Module	4D 54 49 43 FF **33 0F 0C 01 02 03 04 05 06 07 08 09 0A 0B 0C** 59 94
4r	Host <= Module	4D 54 49 52 00 **34 03 00** 7A 51
5t	Host => Module	4D 54 49 43 FF **37 09 00 00 00 00 00 00 02** F1 18
5r	Host <= Module	4D 54 49 52 00 **38 08 00 02 00 00 00 00** A8 4F
6t	Host => Module	4D 54 49 43 FF **35 0D 00 00 00 00 00 00 02 DE AD C0 DE** 36 65
6r	Host <= Module	4D 54 49 52 00 **36 04 00 02** D8 68
7t	Host => Module	4D 54 49 43 FF **3D 06 DE AD C0 DE** 6C F4
7r	Host <= Module	4D 54 49 52 00 **3E 03 00** BD 90

5.4 Change Config-Word of Specific NXP Tag by NXP Command

[Step 1]
Purpose: Configures the RF power level of physical antenna port to 18 dBm.
Command: RFID_AntennaPortSetPowerLevel (ID: 0xC0)

[Step 2]
Purpose: Executes a tag inventory for all tags and get the first tag data.
Command: RFID_18K6CTagInventory (ID: 0x31)

[Step 3]
Purpose: Gets the second tag data.
Command: RFID_18K6CTagInventory (ID: 0x31)

[Step 4]
Purpose: Selects one of the found tags.
Command: RFID_18K6CTagSelect (ID: 0x33)

[Step 5]
Purpose: Reads the access password value from RESERVED memory bank of the NXP tag.
Command: RFID_18K6CTagRead (ID: 0x37)

NXP tag's whose access password value is zero won't execute change Config-Word operation, they only change Config-Word under secure state.
If the tag's access password is zero, perform step 6 to change the access password to nonzero.
If the tag's access password is nonzero, skip step 6 to perform NXP command to change Config-Word directly.

[Step 6]
Purpose: Writes nonzero access password to RESERVED memory bank of the NXP tag.
Command: RFID_18K6CTagWrite (ID: 0x35)

[Step 7]
Purpose: Read current setting of Config-Word from EPC memory bank of the NXP tag.
Command: RFID_18K6CTagRead (ID: 0x37)

[Step 8]
Purpose: If the original Config-Word is 0x0040 (Max. Backscatter Strength bit is active).
Perform NXP Command and set Toggled Config-Word as 0x0001 to activate PSF bit (0->1).
The new Config-Word 0x0041 can be found in response.
Command: RFID_18K6CTagNXPCommand (ID: 0x45)

[Step 9]
Purpose: Read back and confirm the new Config-Word.
Command: RFID_18K6CTagRead (ID: 0x37)

[Step 10]
Purpose: Perform NXP Command and set Toggled Config-Word as 0x0001 again to deactivate PSF bit (1->0). The new Config-Word 0x0040 can be found in response.
Command: RFID_18K6CTagNXPCommand (ID: 0x45)

[Step 11]
Purpose: Read back and confirm the new Config-Word.
Command: RFID_18K6CTagRead (ID: 0x37)

Table 5.4.1 - USB Command and Response Sequences of Use Case 5.4

Step	Data Flow	Command / Response Packet
1t	Host => Module	C0 03 12
1r	Host <= Module	C1 03 00
2t	Host => Module	31 03 01

2r	Host <= Module	32 40 00 02 0E 30 00 E2 00 68 06 11 11 11 11 11 11 11 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3t	Host => Module	31 03 02
3r	Host <= Module	32 40 00 01 0E 30 00 E2 00 68 06 22 22 22 22 22 22 22 22 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
4t	Host => Module	33 0F 0C E2 00 68 06 11 11 11 11 11 11 11 11
4r	Host <= Module	34 03 00
5t	Host => Module	37 09 00 02 00 00 00 00 02
5r	Host <= Module	38 40 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
6t	Host => Module	35 0D 00 02 00 00 00 00 02 AC CE C0 DE
6r	Host <= Module	36 04 00 02
7t	Host => Module	37 09 01 20 00 00 00 00 01
7r	Host <= Module	38 40 00 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
8t	Host => Module	45 0A 09 00 AC CE C0 DE 00 01
8r	Host <= Module	46 05 00 00 41
9t	Host => Module	37 09 01 20 00 00 00 00 01
9r	Host <= Module	38 40 00 01 00 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10t	Host => Module	45 0A 09 00 AC CE C0 DE 00 01
10r	Host <= Module	46 05 00 00 40
11t	Host => Module	37 09 01 20 00 00 00 00 01
11r	Host <= Module	38 40 00 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Table 5.4.2 - UART Command and Response Sequences of Use Case 5.4

Step	Data Flow	Command / Response Packet
1t	Host => Module	4D 54 49 43 FF **C0 03 12** 92 18
1r	Host <= Module	4D 54 49 52 00 **C1 03 00** 72 F3
2t	Host => Module	4D 54 49 43 FF **31 03 01** 64 28
2r	Host <= Module	4D 54 49 52 00 **32 13 00 02 0E 30 00 E2 00 68 06 11 11 11 11 11 11 11 11** 70 EF
3t	Host => Module	4D 54 49 43 FF **31 03 02** 54 4B
3r	Host <= Module	4D 54 49 52 00 **32 13 00 01 0E 30 00 E2 00 68 06 22 22 22 22 22 22 22 22** E9 62
4t	Host => Module	4D 54 49 43 FF **33 0F 0C E2 00 68 06 11 11 11 11 11 11 11 11** B6 7A
4r	Host <= Module	4D 54 49 52 00 **34 03 00** 7A 51
5t	Host => Module	4D 54 49 43 FF **37 09 00 02 00 00 00 00 02** 7A 58
5r	Host <= Module	4D 54 49 52 00 **38 08 00 02 00 00 00 00** A8 4F
6t	Host => Module	4D 54 49 43 FF **35 0D 00 02 00 00 00 00 02 AC CE C0 DE** 85 C9
6r	Host <= Module	4D 54 49 52 00 **36 04 00 02** D8 68
7t	Host => Module	4D 54 49 43 FF **37 09 01 20 00 00 00 00 01** 4C 12
7r	Host <= Module	4D 54 49 52 00 **38 06 00 01 00 40** 46 64
8t	Host => Module	4D 54 49 43 FF **45 0A 09 00 AC CE C0 DE 00 01** 21 DE

8r	Host <= Module	4D 54 49 52 00 **46 05 00 00 41** 69 CF
9t	Host => Module	4D 54 49 43 FF **37 09 01 20 00 00 00 00 01** 4C 12
9r	Host <= Module	4D 54 49 52 00 **38 06 00 01 00 41** 56 45
10t	Host => Module	4D 54 49 43 FF **45 0A 09 00 AC CE C0 DE 00 01** 21 DE
10r	Host <= Module	4D 54 49 52 00 **46 05 00 00 40** 79 EE
11t	Host => Module	4D 54 49 43 FF **37 09 01 20 00 00 00 00 01** 4C 12
11r	Host <= Module	4D 54 49 52 00 **38 06 00 01 00 40** 46 64

6 APPENDIX A - Tag Memory Map

6.1 ISO 18000-6C Tag Memory Map

Tag memory shall be logically separated into four distinct banks, each of which may comprise zero or more memory words. A logical memory map of the 6C tag is shown in Figure A.1.

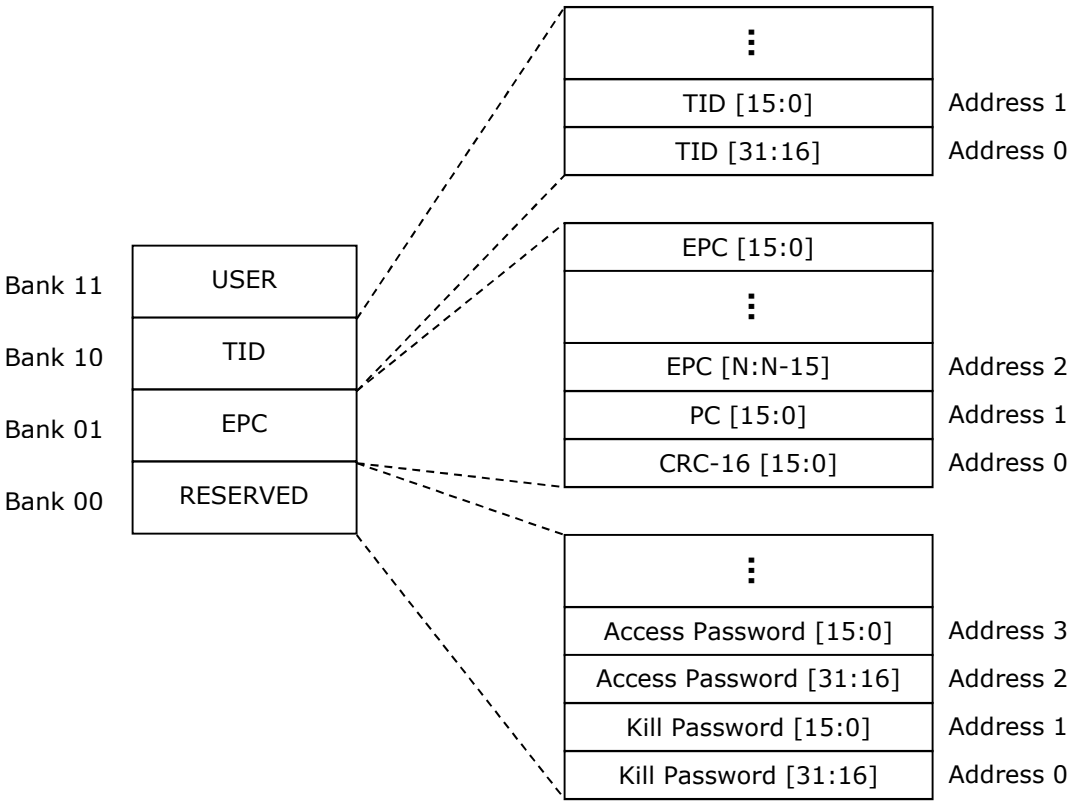


Figure A.1 - Logical Memory Map of 6C Tag

7 APPENDIX B - Frequency Channel Tables

7.1 United States/Canada Region Frequency Channel Table

The frequency range of both United States and Canada regions is from 902 to 928 MHz. A table of all 50 channels is shown in Table B.1.

Table B.1 - Frequency Channel Table of US/CA Band

Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)
1	902.75	2	903.25	3	903.75	4	904.25	5	904.75
6	905.25	7	905.75	8	906.25	9	906.75	10	907.25
11	907.75	12	908.25	13	908.75	14	909.25	15	909.75
16	910.25	17	910.75	18	911.25	19	911.75	20	912.25
21	912.75	22	913.25	23	913.75	24	914.25	25	914.75
26	915.25	27	915.75	28	916.25	29	916.75	30	917.25
31	917.75	32	918.25	33	918.75	34	919.25	35	919.75
36	920.25	37	920.75	38	921.25	39	921.75	40	922.25
41	922.75	42	923.25	43	923.75	44	924.25	45	924.75
46	925.25	47	925.75	48	926.25	49	926.75	50	927.25

7.2 Europe Region Frequency Channel Table (ETSI EN 302 208)

The frequency range of Europe region is from 865.6 to 867.6 MHz. A table of all 4 channels is shown in Table B.2.

Table B.2 - Frequency Channel Table of EU Band

Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)
1	865.7	2	866.3	3	866.9	4	867.5

7.3 Europe2 Region Frequency Channel Table (ETSI EN 300 220)

The frequency of Europe2 region is only 869.85 MHz. A table of 1 channel is shown in Table B.3.

Table B.3 - Frequency Channel Table of EU2 Band

Channel	Frequency (MHz)
1	869.85

7.4 Taiwan Region Frequency Channel Table

The frequency range of Taiwan region is from 922 to 928 MHz. A table of all 12 channels is shown in Table B.4.

Table B.4 - Frequency Channel Table of TW Band

Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)
1	922.25	2	922.75	3	923.25	4	923.75	5	924.25
6	924.75	7	925.25	8	925.75	9	926.25	10	926.75
11	927.25	12	927.75						

7.5 China Region Frequency Channel Table

The frequency range of China region is from 920.5 to 924.5 MHz. A table of all 16 channels is shown in Table B.5.

Table B.5 - Frequency Channel Table of CN Band

Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)
1	920.625	2	920.875	3	921.125	4	921.375	5	921.625
6	921.875	7	922.125	8	922.375	9	922.625	10	922.875
11	923.125	12	923.375	13	923.625	14	923.875	15	924.125
16	924.375								

7.6 South Korea Region Frequency Channel Table

The frequency range of South Korea is from 917 to 920.8 MHz. A table of all 6 channels is shown in Table B.6.

Table B.6 - Frequency Channel Table of KR Band

Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)
1	917.3	2	917.9	3	918.5	4	919.1	5	919.7
6	920.3								

7.7 Australia/New Zealand Region Frequency Channel Table

The frequency range of both Australia and New Zealand regions is from 920 to 926 MHz. A table of all 7 channels is shown in Table B.7.

Table B.7 - Frequency Channel Table of AU/NZ Band

Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)
1	922.25	2	922.75	3	923.25	4	923.75	5	924.25
6	924.75	7	925.25						

7.8 Brazil Region Frequency Channel Table

The frequency range of Brazil region is from 902 to 907.5 MHz and from 915 to 928 MHz. A table of all 35 channels is shown in Table B.8.

Table B.8 - Frequency Channel Table of BR Band

Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)
1	902.75	2	903.25	3	903.75	4	904.25	5	904.75
6	905.25	7	905.75	8	906.25	9	906.75	10	907.25
11	915.25	12	915.75	13	916.25	14	916.75	15	917.25
16	917.75	17	918.25	18	918.75	19	919.25	20	919.75
21	920.25	22	920.75	23	921.25	24	921.75	25	922.25
26	922.75	27	923.25	28	923.75	29	924.25	30	924.75
31	925.25	32	925.75	33	926.25	34	926.75	35	927.25

7.9 Hong Kong Region Frequency Channel Table

The frequency range of Hong Kong region is from 920 to 925 MHz. A table of all 8 channels is shown in Table B.9.

Table B.9 - Frequency Channel Table of HK Band

Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)
1	920.75	2	921.25	3	921.75	4	922.25	5	922.75
6	923.25	7	923.75	8	924.25				

7.10 Malaysia Region Frequency Channel Table

The frequency range of Malaysia region is from 919 to 923 MHz. A table of all 6 channels is shown in Table B.10.

Table B.10 - Frequency Channel Table of MY Band

Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)
1	919.75	2	920.25	3	920.75	4	921.25	5	921.75
6	922.25								

7.11 Singapore Region Frequency Channel Table

The frequency range of Singapore region is from 920 to 925 MHz. A table of all 8 channels is shown in Table B.11.

Table B.11 - Frequency Channel Table of SG Band

Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)
1	920.75	2	921.25	3	921.75	4	922.25	5	922.75
6	923.25	7	923.75	8	924.25				

7.12 Thailand Region Frequency Channel Table

The frequency range of Thailand region is from 920 to 925 MHz. A table of all 8 channels is shown in Table B.12.

Table B.12 - Frequency Channel Table of TH Band

Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)
1	920.75	2	921.25	3	921.75	4	922.25	5	922.75
6	923.25	7	923.75	8	924.25				

7.13 Israel Region Frequency Channel Table

The frequency range of Israel region is from 915 to 917 MHz. A table of all 2 channels is shown in Table B.13.

Table B.13 - Frequency Channel Table of IL Band

Channel	Frequency (MHz)	Channel	Frequency (MHz)
1	915.75	2	916.25

7.14 Russia Federation Region Frequency Channel Table

The frequency range of Russia Federation region is from 865.6 to 867.6 MHz. A table of all 2 channels is shown in Table B.14.

Table B.14 - Frequency Channel Table of RU Band

Channel	Frequency (MHz)	Channel	Frequency (MHz)
1	866.3	2	866.9

7.15 India Region Frequency Channel Table

The frequency range of India region is from 865 to 867 MHz. A table of all 2 channels is shown in Table B.15.

Table B.15 - Frequency Channel Table of IN Band

Channel	Frequency (MHz)	Channel	Frequency (MHz)
1	865.7	2	866.3

7.16 Saudi Arabia Region Frequency Channel Table

The frequency range of Saudi Arabia region is from 865.6 to 867.6 MHz. A table of all 4 channels is shown in Table B.16.

Table B.16 - Frequency Channel Table of SA Band

Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)
1	865.7	2	866.3	3	866.9	4	867.5

7.17 Jordan Region Frequency Channel Table

The frequency range of Jordan region is from 865 to 868 MHz. A table of all 4 channels is shown in Table B.17.

Table B.17 - Frequency Channel Table of JO Band

Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)
1	865.7	2	866.3	3	866.9	4	867.5

7.18 Mexico Region Frequency Channel Table

The frequency range of Mexico region is from 902 to 926 MHz. A table of all 50 channels is shown in Table B.18.

Table B.18 - Frequency Channel Table of MX Band

Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)
1	902.75	2	903.25	3	903.75	4	904.25	5	904.75
6	905.25	7	905.75	8	906.25	9	906.75	10	907.25
11	907.75	12	908.25	13	908.75	14	909.25	15	909.75
16	910.25	17	910.75	18	911.25	19	911.75	20	912.25
21	912.75	22	913.25	23	913.75	24	914.25	25	914.75
26	915.25	27	915.75	28	916.25	29	916.75	30	917.25
31	917.75	32	918.25	33	918.75	34	919.25	35	919.75
36	920.25	37	920.75	38	921.25	39	921.75	40	922.25
41	922.75	42	923.25	43	923.75	44	924.25	45	924.75
46	925.25	47	925.75	48	926.25	49	926.75	50	927.25

8 APPENDIX C - Calculation of CRC-16

8.1 CRC-16 Encoder/Decoder

An exemplary schematic diagram for a CRC-16 encoder/decoder is shown in Figure C.1, using the polynomial and preset defined in Table C.1.

To encode a CRC-16, first preload the entire CRC register (i.e. C[15:0]) with 0xFFFF, then clock the data bits to be encoded into the input labeled DATA, MSB first. After clocking in all the data bits, C[15:0] holds the ones-complement of the CRC-16 value. Finally, the CRC-16 value should be inverted, and attach the inverted CRC-16 to the end of the packet.

To decode a CRC-16, first preload the entire CRC register (C[15:0]) with 0xFFFF, then clock the received data and CRC-16 {data, CRC-16} bits into the input labeled DATA, MSB first. The CRC-16 check passes if C[15:0] = 0x1D0F.

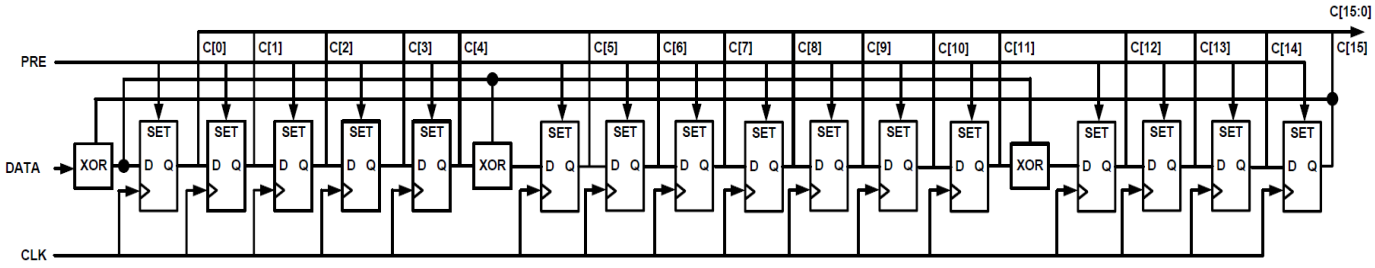


Figure C.1 - CRC-16 Circuit

Table C.1 - CRC-16 Precursor

CRC Type	Length	Polynomial	Preset	Residue
ISO/IEC 13239	16 bits	$X^{16} + X^{12} + X^5 + 1$	0xFFFF	0x1D0F

8.2 Example C Code to Generate the CRC-16 Value

```
/* CRC-16 */

#define POLY 0x1021

unsigned short crc16(unsigned char *buf, unsigned
short bit_length)
{
  unsigned short shift, data, val;
  int i;

  shift = 0xFFFF;

  for(i = 0; i < bit_length; i++)
  {
    if((i % 8) == 0)
      data = (*buf++) << 8;

    val = shift ^ data;
    shift = shift << 1;
    data = data << 1;

    if(val & 0x8000)
      shift = shift ^ POLY;
  }

  return shift;
}
```

```
void main(void)
{
  unsigned char packet[16];
  unsigned short crc, verification;

  /* Invert the resulting CRC value. */
  crc = ~crc16(packet, 14*8);

  packet[14] = crc >> 8;
  packet[15] = crc & 0xFF;

  verification = crc16(packet, 16*8);
  if(verification == 0x1D0F)
    printf("The CRC-16 checksum is correct.");
  else
    printf("The CRC-16 checksum is invalid.");
}
```

8.3 Examples for Calculated Result of CRC-16

[Example 1]

0xC1AA55	→ Calculate CRC-16 and invert	= **0xDA41**
0xC1AA55 + **0xDA41**	→ Calculate CRC-16 for checking	= 0x1D0F

[Example 2]

0x30005555555555555555555555	→ Calculate CRC-16 and invert	= **0xBCAD**
0x30005555555555555555555555 + **0xBCAD**	→ Calculate CRC-16 for checking	= 0x1D0F

[Example 3]

0x3000AAAAAAAAAAAAAAAAAAAAAA	→ Calculate CRC-16 and invert	= **0x7F8C**
0x3000AAAAAAAAAAAAAAAAAAAAAA + **0x7F8C**	→ Calculate CRC-16 for checking	= 0x1D0F

[Example 4]

0x3000A02A051012A000832A011102	→ Calculate CRC-16 and invert	= **0x33AF**
0x3000A02A051012A000832A011102 + **0x33AF**	→ Calculate CRC-16 for checking	= 0x1D0F

9 APPENDIX D - Difference Between USB and UART Interface

The following list highlights the differences of USB and UART interface in this document.

1. Configuration of the communication in section “2.1 MTI RU-888 RFID Module Application”.
2. Command and response format in section “2.2 Packet Format Specification”.
3. RFID_18K6CTagInventory command in section “4.3.1.4 6C Tag Inventory Operation”.
4. RFID_18K6CTagInventoryRSSI command in section “4.3.1.5 6C Tag Inventory Operation with RSSI”.
5. RFID_18K6CTagRead command in section “4.3.2.1 6C Tag Read Operation”.
6. All command and response sequence tables in section “5 Use Case”.