

**OEM UHF Series
OEM RFID Module
Communication Protocol**

iDTRONIC GmbH
Ludwig-Reichling-Straße 4
67059 Ludwigshafen
Germany/Deutschland

Phone: +49 621 6690094-0
Fax: +49 621 6690094-9
E-Mail: info@idtronic.de
Web: idtronic.de

Issue 2.1
– 21. July 2022 –

Subject to alteration without prior notice.
© Copyright iDTRONIC GmbH 2022
Printed in Germany

Contents

1	Info on the MCU	6
2	Command Frames	7
2.1	Command Frame Format	7
2.2	Command Type	7
2.3	Baudrate Settings	7
3	Command Code Overview	8
4	Command Descriptions	9
4.1	Read firmware information	9
4.1.1	Command Frame	9
4.1.2	Response Frame.....	9
4.2	Single Inventory Command	9
4.2.1	Command Frame	10
4.2.2	Notification Frame Definition	10
4.2.3	Response Frame.....	10
4.3	Multiple Inventory Command	10
4.3.1	Command Frame	10
4.3.2	Notification Frame Definition	11
4.3.3	Response Frame Notification.....	11
4.4	Stop Multiple Inventory Command	11
4.4.1	Command Frame	11
4.4.2	Response Frame.....	12
4.5	Set Select Parameter Command	12
4.5.1	Command Frame	12
4.5.2	Response Frame.....	13
4.6	Set Select Mode	13
4.6.1	Command Frame	13
4.6.2	Response Frame.....	13
4.7	Read Memory Bank	14
4.7.1	Command Frame	14
4.7.2	Response Frame.....	14
4.8	Write Data to Memory Bank	16
4.8.1	Command Frame	16
4.8.2	Response Frame.....	16
4.9	Lock Memory Bank	18
4.9.1	Command Frame	18
4.9.2	Response Frame.....	19
4.10	Kill the Tag.....	20
4.10.1	Command Frame	20
4.10.2	Response Frame.....	20
4.11	Get Query Parameter	21
4.11.1	Command Frame	21
4.11.2	Response Frame.....	22
4.12	Set Query Parameter	22
4.12.1	Command Frame	22
4.12.2	Response Frame.....	23
4.13	Set Region	23

4.13.1	Command Frame	23
4.13.2	Response Frame	23
4.14	Get Region	24
4.14.1	Command Frame	24
4.14.2	Response Frame	24
4.15	Set Working Channel	24
4.15.1	Command Frame	24
4.15.2	Response Frame	25
4.16	Get Working Channel	25
4.16.1	Command Frame	25
4.16.2	Response Frame	25
4.17	Set Auto Frequency Hopping	25
4.17.1	Command Frame	25
4.17.2	Response Frame	26
4.18	Get the Transmitted Power	26
4.18.1	Command Frame	26
4.18.2	Response Frame	26
4.19	Set the Transmitted Power	26
4.19.1	Command Frame	26
4.19.2	Response Frame	27
4.20	Set Continuous Carrier	27
4.20.1	Command Frame	27
4.20.2	Response Frame	27
4.21	Get Receiver Demodulator Parameters	27
4.21.1	Command Frame	27
4.21.2	Response Frame	28
4.22	Set Receiver Demodulator Parameters	28
4.22.1	Command Frame	28
4.22.2	Response Frame	29
4.23	Scan Jammer	30
4.23.1	Command Frame	30
4.23.2	Response Frame	30
4.24	Scan Channel (LBT)	30
4.24.1	Command Frame	30
4.24.2	Response Frame	31
4.25	GPIO Control	31
4.25.1	Command Frame	31
4.25.2	Response Frame	32
4.26	Module Sleep	32
4.26.1	Command Frame	32
4.26.2	Response Frame	32
4.27	Set Module Idle Time	33
4.27.1	Command Frame	33
4.27.2	Response Frame	33
4.28	NXP Read Protect/Reset Read Protect	33
4.28.1	Command Frame	33
4.28.2	Response Frame	34
4.29	NXP Change EAS	35
4.29.1	Command Frame	35
4.29.2	Response Frame	35

4.30	NXP EAS_Alarm	36
4.30.1	Command Frame	36
4.30.2	Response Frame.....	37
4.31	NXP ChangeConfig.....	37
4.31.1	Command Frame	37
4.31.2	Response Frame.....	37
4.32	Impinj Monza QT	39
4.32.1	Command Frame	39
4.32.2	Response Frame.....	39
5	Error Frames.....	41
5.1	Error Codes.....	41
5.2	EPC Gen2 protocol specified error code.....	41
5.3	Specific Error Codes of NXP G2X Tag.....	42
5.4	Specific Error Codes of Impinj Monza QT Tag	42
6	Revision History	43

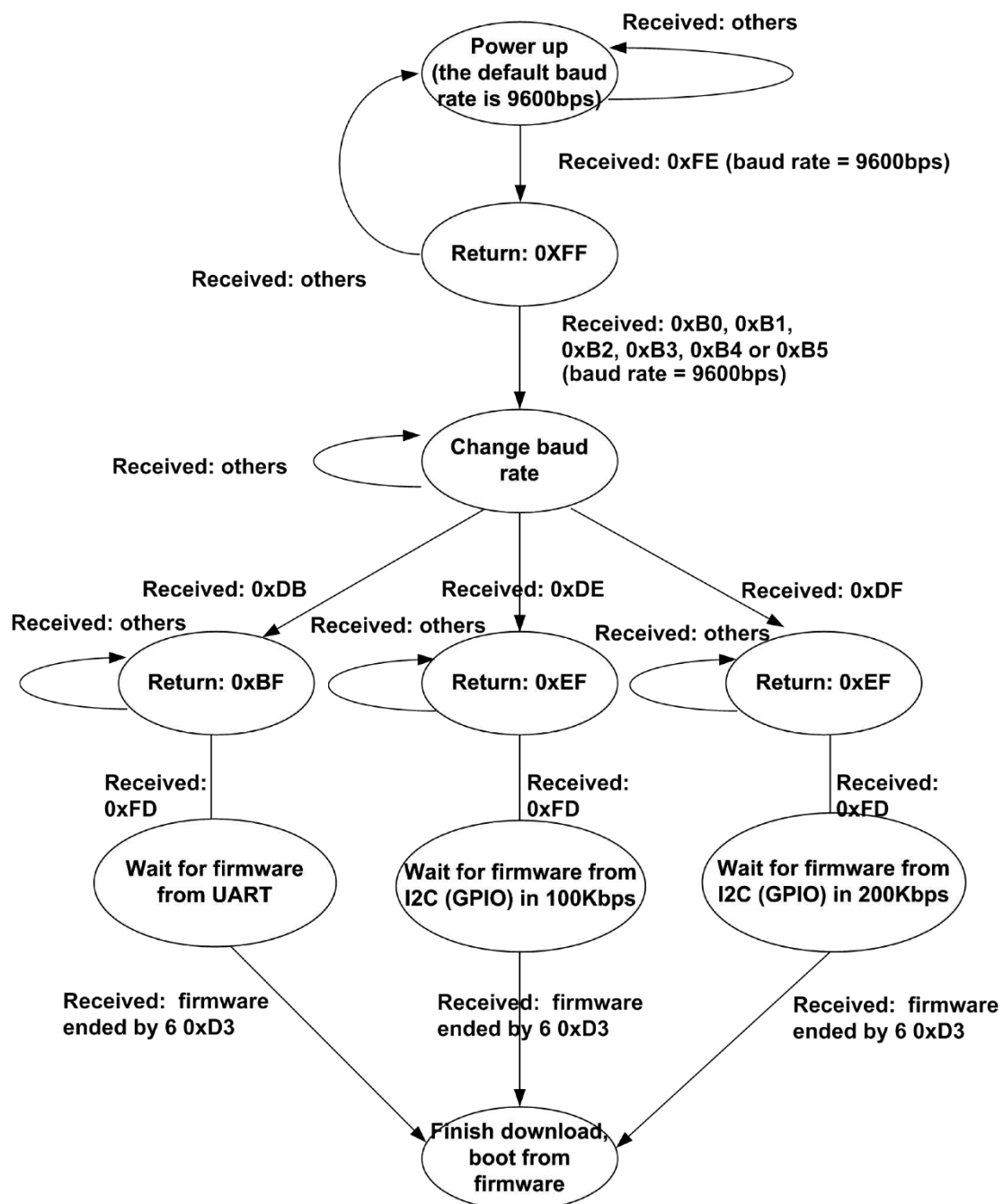
1 Info on the MCU

M100 has an internal 8bit 8051 MCU, which has 256Byte RAM, 16Kbyte program ROM and 3 timer (In the firmware, the timer2 is used for baud rate control, the timer0 is used for frequency hopping control and the timer1 is reserved for user). And there is 8Kbyte data RAM which can be used by the 8051 MCU and the MODEM. In the receiving phase, the data RAM can NOT be accessed by MCU.

There is no internal flash in M100. The firmware of MCU could be download by UART or I2C (GPIO emulated: P1.0, P1.1) interface.

UART interface frame has 8bit data and 1bit stop, no parity.

The handshake protocol for firmware download at power up or reset is as below:



2 Command Frames

2.1 Command Frame Format

Every command includes Header, Command Type, Command Code, Parameter Length (PL), Checksum, End.

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	00	07	00	01	01	09	7E

Header: 0xBB
 Type: 0x00
 Command: 0x07
 Parameter Length: 0x0001
 Parameter: 0x01
 Checksum: 0x09
 End: 0x7E

Checksum calculation: Sum from Type to Parameter. And take the least significant Byte of the sum.

2.2 Command Type

Type	Description
0x00	Command Frame: Sent from PC/PLC to RFID device
0x01	Response Frame: Sent from RFID device to PC/PLC
0x02	Notification Frame: Sent from RFID device to PC/PLC

Each command contains the related response frame, which indicates if the command is executed.

Single Inventory command and repeatedly Inventory command also have related notification frame. Numbers of notification frames are decided by MCU and send automatically to upper computer. For example, one notification for when one tag is read, multiple notification frames when multiple tags are read.

2.3 Baudrate Settings

Type	Baud Rate(bps)
0xB0	9600
0xB1	19200
0xB2	28800
0xB3	38400
0xB4	57600
0xB5	115200

115'200 Baud is factory preset.

3 Command Code Overview

Code	Description
0x03	Get Module Information
0x07	Set Region
0x08	Get Region
0x0C	Set Select Parameters
0x0D	Get Query Parameters
0x0E	Set Query Parameters
0x12	Setting up to send Select instructions
0x17	Module Sleep
0x1A	GPIO Control
0x1D	Set Module Idle Time
0x22	Single polling instruction
0x27	Multiple polling instructions
0x28	Stop multiple polling instructions
0x39	Read
0x49	Write
0x65	Kill
0x82	Lock
0xAA	Get Channel
0xAB	Set Channel
0xAD	Frequency Hopping
0xB0	Continuous Wave
0xB6	Set TX Power
0xB7	Get TX Power
0xE0	NXP Change Configuration
0xE1	NXP Read Protect / Reset Read Protect
0xE3	NXP Change EAS
0xE4	NXP EAS-Alarm
0xE5	Impinj Monza 4 QT
0xF0	Set Modem Parameters
0xF1	Get Modem Parameters
0xF2	Scan Jammer
0xF3	Scan Channel

4 Command Descriptions

4.1 Read firmware information

This command can get the information of modules such as hardware version, software version and manufacturer information.

4.1.1 Command Frame

Type: 0x00
Command Code: 0x03

Parameters (Info Type)

Hardware Version: 0x00
Software Version: 0x01
Manufacturer: 0x02

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	00	03	00	01	00	04	7E

Type: 0x00
Command: 0x03
Parameter Length: 0x0001
Parameter: 0x00 (hardware version)
Checksum: 0x04

4.1.2 Response Frame

Type: 0x01
Command: 0x03
Data: Variable (ASCII)

The response data first byte is the information type, followed by the detailed message in ASCII codes. The response of getting hardware version is as below:

Header	Type	Command	PL(MSB)	PL(LSB)	Info Type	Info	
BB	01	03	00	0B	00	4D ('M')	31 ('1')
30 ('0')	30 ('0')	20 (' ')	56 ('V')	31 ('1')	2E ('.')	30 ('0')	30 ('0')
Checksum	End						
22	7E						

Type: 0x01
Command: 0x03
Parameter Length: 0x000B
Hardware Info Type: 0x00 (hardware version)
Software Info: 4D 31 30 30 20 56 31 2E 30 30 ("M100 V1.00" in ASCII)
Checksum: 0x22

4.2 Single Inventory Command

When received this command, the reader chip will do the inventory once. The power amplifier will be opened at the beginning of the inventory and be closed after the inventory. Select parameter settings please refer to section 4.4. Query parameter settings please refer to section 4.11.

4.2.1 Command Frame

Header	Type	Command	PL(MSB)	PL(LSB)	Checksum	End
BB	00	22	00	00	22	7E

Type: 0x00
 Command: 0x22
 PL: 0x0000
 Checksum: 0x22

4.2.2 Notification Frame Definition

After the firmware received a single inventory command, and successfully read a tag (CRC check passed), a notice frame including RSSI, PC, EPC and CRC will be sent. If multiple tags are read in one inventory, notice frames of the same number of successfully read tag will be sent.

Header	Type	Command	PL(MSB)	PL(LSB)	RSSI	PC(MSB)	PC(LSB)
BB	02	22	00	11	C9	34	00
EPC(MSB)							
30	75	1F	EB	70	5C	59	04
			EPC(LSB)	CRC(MSB)	CRC(LSB)	Checksum	End
E3	D5	0D	70	3A	76	EF	7E

Type: 0x02
 Command: 0x22
 PL: 0x0011
 RSSI: 0xC9
 PC: 0x3400
 EPC: 0x30751FEB705C5904E3D50D70
 CRC (of EPC): 0x3A76
 Checksum: 0xEF

RSSI is a received signal strength indicator at the RF input port of the reader chip. It's a complementally coded signed hex in the unit of dBm. E.g. an RSSI of 0xC9 means the tag returned signal power at the input port of the reader chip is -55dBm.

4.2.3 Response Frame

Error code of 0x15 would be returned when receiving no tag data or CRC verification failed

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	FF	00	01	15	16	7E

Type: 0x01
 Command: 0xFF
 PL: 0x01
 Parameter: 0x15
 Checksum: 0x16

4.3 Multiple Inventory Command

4.3.1 Command Frame

This command would require MCU to carry out multiple Inventory operation, between numbers of 0~65535. For example, if we set the numbers as 10000. The command would be like follows:

Header	Type	Command	PL(MSB)	PL(LSB)	Reserved	CNT(MSB)	CNT(LSB)
BB	00	27	00	03	22	27	10
Checksum	End						
83	7E						

Type: 0x00
 Command: 0x27
 PL: 0x0003
 Reserved: 0x22
 CNT: 0x2710
 Checksum: 0x83

4.3.2 Notification Frame Definition

The notice frame of multiple inventory is the same as single inventory.

Header	Type	Command	PL(MSB)	PL(LSB)	RSSI	PC(MSB)	PC(LSB)
BB	02	22	00	11	C9	34	00
EPC(MSB)							
30	75	1F	EB	70	5C	59	04
			EPC(LSB)	CRC(MSB)	CRC(LSB)	Checksum	End
E3	D5	0D	70	3A	76	EF	7E

Type: 0x02
 Command: 0x27
 PL: 0x0011
 RSSI: 0xC9
 PC: 0x3400
 EPC: 0x30751FEB705C5904E3D50D70
 CRC (of EPC): 0x3A76
 Checksum: 0xEF

4.3.3 Response Frame Notification

Error code of 0x15 would be returned when receiving no tag data or CRC verification failed:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	FF	00	01	15	16	7E

Type: 0x01
 Command: 0xFF
 PL: 0x01
 Parameter: 0x15
 Checksum: 0x16

4.4 Stop Multiple Inventory Command

The multiple inventory command can be stopped (not pause) immediately by this command.

4.4.1 Command Frame

Header	Type	Command	PL(MSB)	PL(LSB)	Checksum	End
BB	00	28	00	00	28	7E

Type: 0x00
 Command: 0x28
 Parameter Length: 0x0000

Checksum: 0x28

4.4.2 Response Frame

If the multiple inventory is stopped successfully, a response frame will be return:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	28	00	01	00	2A	7E

Type: 0x01
 Command: 0x28
 Parameter Length: 0x0001
 Parameter: 0x00
 Checksum: 0x2A

4.5 Set Select Parameter Command

4.5.1 Command Frame

This command will set select parameters and set Select Mode to 0x02. And the select will be send before inventory by default. Example (select tags which has the same code from bit 0x20 to bit 0x80):

Header	Type	Command	PL(MSB)	PL(LSB)	SelParam	Ptr(MSB)	
BB	00	0C	00	13	01	00	00
	Ptr(LSB)	MaskLen	Truncate	Mask(MSB)			
00	20	60	00	30	75	1F	EB
							Mask(LSB)
70	5C	59	04	E3	D5	0D	70
Checksum	End						
AD	7E						

Type: 0x00
 Command: 0x0C
 Parameter Length: 0x0013
 SelParam: 0x01 (Target: 3'b000, Action: 3'b000, MemBank: 2'b01)
 Ptr: 0x00000020 (unit of bit, non-word), starts from EPC bank memory bit
 MaskLen: 0x60 (6x word, 96bits)
 Truncate: 0x00 (0x00 as Disable truncation, 0x80 as Enable truncation)
 Mask: 0x30 75 1F EB 70 5C 59 04 E3 D5 0D 70
 Checksum: 0xAD

SelParam is a one byte parameter which contains 3-bits Target, 3-bits Action and 2-bits MemBank.

The meaning of MemBank is:

MemBank

2'b00: RFU
 2'b01: EPC
 2'b10: TID
 2'b11: User

When length of Select Mask is larger than 80 bits (5 words), all the tags would be set as Inventoried Flag A when sending Select command, and SL Flag with status of ~SL, then would Action would work. When length of Select Mask is less than 80 bits (5 words), these settings would be set.

The meanings of Target and Action please refer to EPC UHF Class 1 Gen 2 Standard Protocol.

4.5.2 Response Frame

When select parameters are set successfully, a response frame will be returned:

Header	Type	Command	PL(MSB)	PL(LSB)	Data	Checksum	End
BB	01	0C	00	01	00	0E	7E

Type: 0x01
 Command: 0x0C
 Parameter Length: 0x0001
 Data: 0x00
 Checksum: 0x0E

4.6 Set Select Mode

4.6.1 Command Frame

After set select parameters, the select command could be set to send or not send before inventory or other operation.

Example (not to send select before inventory):

Header	Type	Command	PL(MSB)	PL(LSB)	Mode	Checksum	End
BB	00	12	00	01	01	14	7E

Type: 0x00
 Command: 0x12
 Parameter Length: 0x0001
 SelectMode: 0x01
 Checksum: 0x14

Select Mode Explanation

0x00: Send Select command to the tag before any operation to select the specific tag
 0x01: Cancel Select command
 0x02: . Send select before all tag operation except Inventory (Single Inventory and Multiple Inventory).
 E.g. select a certain tag before Read, Write, Lock, and Kill.

4.6.2 Response Frame

When Select command is cancelled or sent successfully, the firmware would return the following data:

Header	Type	Command	PL(MSB)	PL(LSB)	Data	Checksum	End
BB	01	0C	00	01	00	0E	7E

Type: 0x01
 Command: 0x0C
 PL: 0x0001
 Data: 0x00 (Success)
 Checksum: 0x0E

4.7 Read Memory Bank

4.7.1 Command Frame

Read the memory bank of tag from the given address and by the given length. The unit for segment address (SA) and data length (DL) is word. Before this command, a set select parameter command should be sent first to select a single tag. The access command will not be send if the access password is all zero.

Header	Type	Command	PL(MSB)	PL(LSB)	AP(MSB)		
BB	00	39	00	09	00	00	FF
AP(LSB)	MemBank	SA(MSB)	SA(LSB)	DL(MSB)	DL(LSB)	Checksum	End
FF	03	00	00	00	02	45	7E

Type: 0x00
 Command: 0x39
 Parameter Length: 0x0009
 Access Password: 0x0000FFFF
 MemBank: 0x03 (User Memory Bank)
 SA: 0x0000
 DL: 0x0002
 Checksum: 0x45

4.7.2 Response Frame

When memory bank of specified tag is read successfully and CRC verification also works, returned data would be as follows:

Header	Type	Command	PL(MSB)	PL(LSB)	UL	PC(MSB)	PC(LSB)
BB	01	39	00	13	0E	34	00
EPC(MSB)							
30	75	1F	EB	70	5C	59	04
			EPC(LSB)	Data(MSB)			Data(LSB)
E3	D5	0D	70	12	34	56	78
Checksum	End						
B0	7E						

Type: 0x01
 Command: 0x39
 Parameter Length: 0x0013
 PC+ EPC Length UL: 0x0E
 PC: 0x3400
 EPC: 0x30751FEB705C5904E3D50D70
 Data: 0x12345678
 Checksum: 0xB0

Error code of 0x09 would be returned when the tag is not within the reading distance or when the specific EPC is incorrect, details as follows:

Header	Type	Command	PL(MSB)	PL(LSB)	Error Code	Checksum	End
BB	01	FF	00	01	09	0A	7E

Type: 0x01
 Command: 0xFF
 Parameter Length: 0x0001
 Error Code: 0x09
 Checksum: 0x0A

If Access password is incorrect, error code of 0x16 would be returned, together with PC+EPC of the tag, details as follows:

Header	Type	Command	PL(MSB)	PL(LSB)	Error Code	UL	PC(MSB)
BB	01	FF	00	10	16	0E	34
PC(LSB)	EPC(MSB)						
00	30	75	1F	EB	70	5C	59
				EPC(LSB)	Checksum	End	
04	E3	D5	0D	70	75	7E	

Type: 0x01
 Command: 0xFF
 Parameter Length: 0x0010
 Error Code: 0x16
 PC+ EPC Length UL: 0x0E
 PC: 0x3400
 EPC: 0x30751FEB705C5904E3D50D70
 Checksum: 0x75

If there are errors in SA or DL (e.g. the reading address is exceed the data memory bound), an error code of 0xA3 will be returned, and the tag's PC + EPC will be sent back:

Header	Type	Command	PL(MSB)	PL(LSB)	Error Code	UL	PC(MSB)
BB	01	FF	00	10	A3	0E	34
PC(LSB)	EPC(MSB)						
00	30	75	1F	EB	70	5C	59
				EPC(LSB)	Checksum	End	
04	E3	D5	0D	70	02	7E	

Type: 0x01
 Command: 0xFF
 Parameter Length: 0x0010
 Error Code: 0xA3
 PC+ EPC Length UL: 0x0E
 PC: 0x3400
 EPC: 0x30751FEB705C5904E3D50D70
 Checksum: 0x02

4.8 Write Data to Memory Bank

Write the memory bank of tag from the given address and by the given length. The unit for segment address (SA) and data length (DL) is word. Before this command, a set select parameter command should be sent first to select a single tag. The access command will not be sent if the access password is all zero. The data length to be written cannot exceed 32 words (64 bytes).

4.8.1 Command Frame

Header	Type	Command	PL(MSB)	PL(LSB)	AP(MSB)		
BB	00	49	00	0D	00	00	FF
AP(LSB)	MemBank	SA(MSB)	SA(LSB)	DL(MSB)	DL(LSB)	DT(MSB)	
FF	03	00	00	00	02	12	34
	DT(LSB)	Checksum	End				
56	78	6D	7E				

Type: 0x00
 Command: 0x39
 PL: 0x000D
 Access Password: 0x0000FFFF
 MemBank: 0x03
 SA: 0x0000
 DL: 0x0002
 DT: 0x12345678
 Checksum: 0x6D

4.8.2 Response Frame

Response frame would be as follows when data is written to the memory bank successfully and the module receives the correct data from the tag:

Header	Type	Command	PL(MSB)	PL(LSB)	UL	PC(MSB)	PC(LSB)
BB	01	49	00	10	0E	34	00
EPC(MSB)							
30	75	1F	EB	70	5C	59	04
			EPC(LSB)	Parameter	Checksum	End	
E3	D5	0D	70	00	A9	7E	

Type: 0x01
 Command: 0x49
 Parameter Length: 0x0010
 PC+ EPC Length UL: 0x0E
 PC: 0x3400
 EPC: 0x30751FEB705C5904E3D50D70
 Parameter: 0x00(Success)
 Checksum: 0xA9

Error code of 0x10 would be returned if the tags is not within the reading distance or the specified EPC is incorrect, details as follows:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	FF	00	01	10	0A	7E

Type: 0x01
 Command: 0xFF
 PL: 0x0001

Parameter: 0x10
Checksum: 0x0A

Error code of 0x16 would be returned when Access Password is incorrect, and PC + EPC of the tag would also be returned, details as follows:

Header	Type	Command	PL(MSB)	PL(LSB)	Error Code	UL	PC(MSB)
BB	01	FF	00	10	16	0E	34
PC(LSB)	EPC(MSB)						
00	30	75	1F	EB	70	5C	59
				EPC(LSB)	Checksum	End	
04	E3	D5	0D	70	75	7E	

Type: 0x01
Command: 0xFF
PL: 0x0016
Error Code: 0x16
PC+EPC: 0x0E
PC: 0x3400
EPC: 0x30751FEB705C5904E3D50D70
Checksum: 0x75

If there is an error code according to EPC Gen2 Protocol occurs (e.g. the address exceeds the data memory bound, an error code of 0xB3 will be returned), the error code bitwise OR 0xB0 will be returned, and the tag's PC + EPC will be sent back:

Header	Type	Command	PL(MSB)	PL(LSB)	Error Code	UL	PC(MSB)
BB	01	FF	00	10	B3	0E	34
PC(LSB)	EPC(MSB)						
00	30	75	1F	EB	70	5C	59
				EPC(LSB)	Checksum	End	
04	E3	D5	0D	70	12	7E	

Type: 0x01
Command: 0xFF
PL: 0x0010
Error Code: 0xB3
PC+EPC: 0x0E
PC: 0x3400
EPC: 0x30751FEB705C5904E3D50D70
Checksum: 0x12

Tag Error Codes:

0xB0: Other Error
0xB3: Memory Overrun
0xB4: Memory Locked
0xBB: Insufficient Power

4.9 Lock Memory Bank

Lock or unlock the tag memory bank by access password. Before this command, a set select parameter command should be sent first to select a single tag.

4.9.1 Command Frame

Details are as follows when locking Access Password:

Header	Type	Command	PL(MSB)	PL(LSB)	AP(MSB)		
BB	00	82	00	07	00	00	FF
AP(LSB)	LD(MSB)		LD(LSB)	Checksum	End		
FF	02	00	80	09	7E		

Type: 0x00
 Command: 0x82
 PL: 0x0007
 Access Password: 0x0000FFFF
 LD: 0x020080
 Checksum: 0x09

The 4bits MSB of the lock payload (LD) is reserved. And the next 20 bits is for lock mask (10 bits) and lock action (10 bits) accordingly.

The detailed lock payload, masks and action field should refer to EPCTM Radio-Frequency Identity Protocols from EPC global.

Lock-Command Payload

19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Kill Mask		Access Mask		EPC Mask		TID Mask		User Mask		Kill Action		Access Action		EPC Action		TID Action		User Action	

Masks and Associated Action Fields

	Kill pwd		Access pwd		EPC memory		TID memory		User memory	
	19	18	17	16	15	14	13	12	11	10
Mask	skip/write	skip/write	skip/write	skip/write	skip/write	skip/write	skip/write	skip/write	skip/write	skip/write
Action	9	8	7	6	5	4	3	2	1	0
	pwd read/write	perma lock	pwd read/write	perma lock	pwd write	perma lock	pwd write	perma lock	pwd write	perma lock

pwd-write	permalock	Description
0	0	Associated memory bank is writeable from either the open or secured states.
0	1	Associated memory bank is permanently writeable from either the open or secured states and may never be locked.
1	0	Associated memory bank is writeable from the secured state but not from the open state.
1	1	Associated memory bank is not writeable from any state.
pwd-read/write	permalock	Description
0	0	Associated password location is readable and writeable from either the open or secured states.
0	1	Associated password location is permanently readable and writeable from either the open or secured states and may never be locked.
1	0	Associated password location is readable and writeable from the secured state but not from the open state.
1	1	Associated password location is not readable or writeable from any state.

4.9.2 Response Frame

If lock command works and detailed response frame is as follows:

Header	Type	Command	PL(MSB)	PL(LSB)	UL	PC(MSB)	PC(LSB)
BB	01	82	00	10	0E	34	00
EPC(MSB)							
30	75	1F	EB	70	5C	59	04
			EPC(LSB)	Parameter	Checksum	End	
E3	D5	0D	70	00	E2	7E	

Type: 0x01
 Command: 0x82
 PL: 0x0010
 PC+EPC: 0x0E
 PC: 0x3400
 EPC: 0x30751FEB705C5904E3D50D70
 Parameter: 0x00 (successful command execution)
 Checksum: 0xE2

If there is no tag response, an error code of 0x13 will be returned:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	FF	00	01	13	14	7E

Type: 0x01
 Command: 0xFF
 PL: 0x0001
 Parameter: 0x13
 Checksum: 0x14

If the access password is not correct, an error code of 0x16 will be returned, and the tag's PC + EPC will be sent back:

Header	Type	Command	PL(MSB)	PL(LSB)	Error Code	UL	PC(MSB)
BB	01	FF	00	10	16	0E	34
PC(LSB)	EPC(MSB)						
00	30	75	1F	EB	70	5C	59
			EPC(LSB)	Checksum	End		
04	E3	D5	0D	70	75	7E	

Type: 0x01
 Command: 0xFF
 PL: 0x0016
 Error Code: 0x16
 PC+EPC: 0x0E
 PC: 0x3400
 EPC: 0x30751FEB705C5904E3D50D70
 Checksum: 0x75

If there is an error code according to EPC Gen2 Protocol occurs (e.g. the Memory Bank has been permalocked, an error code of 0xC4 will be returned), the error code bitwise OR 0xC0 will be returned, and the tag's PC + EPC will be sent back:

Header	Type	Command	PL(MSB)	PL(LSB)	Error Code	UL	PC(MSB)
BB	01	FF	00	10	C4	0E	34
PC(LSB)	EPC(MSB)						
00	30	75	1F	EB	70	5C	59
				EPC(LSB)	Checksum	End	
04	E3	D5	0D	70	23	7E	

Type: 0x01
 Command: 0xFF
 PL: 0x0010
 Error Code: 0xC4
 PC+EPC: 0x0E
 PC: 0x3400
 EPC: 0x30751FEB705C5904E3D50D70
 Checksum: 0x23

Tag Error Codes

0xC0: Other Error
 0xC3: Memory Overrun
 0xC4: Memory Locked
 0xCB: Insufficient Power

4.10 Kill the Tag

Before this command, a set select parameter command should be sent first to select a single tag.

The kill command is as follow:

4.10.1 Command Frame

Set Select command before this command:

Header	Type	Command	PL(MSB)	PL(LSB)	KP(MSB)		
BB	00	65	00	04	00	00	FF
KP(LSB)	Checksum	End					
FF	67	7E					

Type: 0x00
 Command: 0x65
 PL: 0x0012
 Kill Password: 0x0000FFFF
 Checksum: 0x67

Note

A tag with all zero Kill Password cannot be killed!

4.10.2 Response Frame

Response Frame would be as follows when Kill command works:

Header	Type	Command	PL(MSB)	PL(LSB)	UL	PC(MSB)	PC(LSB)
BB	01	65	00	10	0E	34	00
EPC(MSB)							
30	75	1F	EB	70	5C	59	04

			EPC(LSB)	Parameter	Checksum	End	
E3	D5	0D	70	00	C5	7E	

Type: 0x01
 Command: 0x65
 PL: 0x0010
 PC+EPC: 0x0E
 PC: 0x3400
 EPC: 0x30751FEB705C5904E3D50D70
 Parameter: 0x00(Success)
 Checksum: 0xC5

Error code of 0x12 would be returned when the tag is not within the reading distance or the specified EPC is incorrect, details as follows:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	FF	00	01	12	13	7E

Type: 0x01
 Command: 0xFF
 PL: 0x0001
 Parameter: 0x12
 Checksum: 0x13

If there is an error code according to EPC Gen2 Protocol occurs (e.g. the tag has no kill password, an error code of 0xD0 will be returned), the error code bitwise OR 0xD0 will be returned, and the tag's PC + EPC will be sent back:

Header	Type	Command	PL(MSB)	PL(LSB)	Error Code	UL	PC(MSB)
BB	01	FF	00	10	D0	0E	34
PC(LSB)	EPC(MSB)						
00	30	75	1F	EB	70	5C	59
				EPC(LSB)	Checksum	End	
04	E3	D5	0D	70	2F	7E	

Type: 0x01
 Command: 0xFF
 PL: 0x0010
 Error Code: 0xD0
 PC+EPC: 0x0E
 PC: 0x3400
 EPC: 0x30751FEB705C5904E3D50D70
 Checksum: 0x2F

4.11 Get Query Parameter

4.11.1 Command Frame

Header	Type	Command	PL(MSB)	PL(LSB)	Checksum	End	
BB	00	0D	00	00	0D	7E	

Type: 0x00
 Command: 0x0D
 PL: 0x0000
 Checksum: 0x0D

4.11.2 Response Frame

Response Frame would be as follows when Query command is executed successfully, details as follows:

Header	Type	Command	PL(MSB)	PL(LSB)	Para(MSB)	Para(LSB)	Checksum
BB	01	0D	00	02	10	20	40
End							
7E							

Type: 0x01
 Command: 0x0D
 PL: 0x0002
 Query Parameter: 0x1020
 Checksum: 0x40

Parameter of it is 2 Bytes, which contains the following parts:

- DR = 8
- M = 1
- TRext = Use pilot tone
- Sel = 00
- Session = 00
- Target = A, Q = 4

DR (1 bit): DR = 8 (1'b0), DR = 64/3 (1'b1). Supports the mode of DR = 8 only
 M (2 bit): M = 1 (2'b00), M = 2 (2'b01), M = 4 (2'b10), M = 8 (2'b11). Supports the mode of M = 1 only
 TRext (1 bit): No pilot tone (1'b0), Use pilot tone (1'b1). Supports the mode of Use pilot tone (1'b1) only
 Sel (2 bit): ALL (2'b00/2'b01), ~SL (2'b10), SL (2'b11)
 Session (2 bit): S0 (2'b00), S1 (2'b01), S2 (2'b10), S3 (2'b11)
 Target (1 bit): A (1'b0), B (1'b1)
 Q (4 bit): 4'b0000-4'b1111

4.12 Set Query Parameter

4.12.1 Command Frame

DR (1 bit): DR = 8 (1'b0), DR = 64/3 (1'b1). Supports the mode of DR = 8 only
 M (2 bit): M = 1 (2'b00), M = 2 (2'b01), M = 4 (2'b10), M = 8 (2'b11). Supports the mode of M = 1 only
 TRext (1 bit): No pilot tone (1'b0), Use pilot tone (1'b1). Supports the mode of Use pilot tone (1'b1) only
 Sel (2 bit): ALL (2'b00/2'b01), ~SL (2'b10), SL (2'b11)
 Session (2 bit): S0 (2'b00), S1 (2'b01), S2 (2'b10), S3 (2'b11)
 Target (1 bit): A (1'b0), B (1'b1)
 Q (4 bit): 4'b0000-4'b1111

If DR=8, M=1, TRext=Use pilot tone, Sel=00, Session=00, Target=A, Q=4, detailed setting commands are as follows:

Header	Type	Command	PL(MSB)	PL(LSB)	Para(MSB)	Para(LSB)	Checksum
BB	00	0E	00	02	10	20	40
End							
7E							

Type: 0x00
 Command: 0x0E
 PL: 0x0002
 Query Parameter: 0x1020

Checksum: 0xC6

4.12.2 Response Frame

If set query parameters successfully, a response frame will be returned:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	0E	00	01	00	10	7E

Type: 0x01
 Command: 0x0E
 PL: 0x0001
 Parameter: 0x00
 Checksum: 0x10

4.13 Set Region

4.13.1 Command Frame

Set region for radio frequency regulation. Example (China band):

Header	Type	Command	PL(MSB)	PL(LSB)	Region	Checksum	End
BB	00	07	00	01	01	09	7E

Type: 0x00
 Command: 0x07
 PL: 0x0001
 Region: 0x01
 Checksum: 0x09

Codes of different regions are as follows:

Region	Parameter
China 900MHz	01
China 800MHz	04
USA	02
Europe	03
Korea	06

4.13.2 Response Frame

If region is set successfully, a response frame will be returned:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	07	00	01	00	09	7E

Type: 0x01
 Command: 0x07
 PL: 0x0001
 Parameter: 0x00
 Checksum: 0x09

4.14 Get Region

Get current region setting from RFID device.

4.14.1 Command Frame

Set region for radio frequency regulation. Example (China band):

Header	Type	Command	PL(MSB)	PL(LSB)	Checksum	End
BB	00	08	00	00	08	7E

Type: 0x00
 Command: 0x08
 PL: 0x0000
 Checksum: 0x08

4.14.2 Response Frame

A response frame includes current working region (in this example, region is China 900 MHz) will be returned:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	08	00	01	01	0B	7E

Type: 0x01
 Command: 0x08
 PL: 0x0001
 Parameter: 0x01
 Checksum: 0x0B

4.15 Set Working Channel

4.15.1 Command Frame

Set the current working channel. Example (In China band, set the working channel to 920.125 MHz):

Header	Type	Command	PL(MSB)	PL(LSB)	CH Index	Checksum	End
BB	00	AB	00	01	01	AC	7E

Type: 0x00
 Command: 0xAB
 PL: 0x0001
 Channel Index: 0x01
 Checksum: 0xAC

Calculate Channel Index

Calculate channel index from channel central frequency (Freq_CH is the channel central frequency):

China 900MHz channel: $CH_Index = (Freq_CH - 920.125M) / 0.25M$
 China 800MHz channel: $CH_Index = (Freq_CH - 840.125M) / 0.25M$
 USA channel: $CH_Index = (Freq_CH - 902.25M) / 0.5M$
 Europe channel: $CH_Index = (Freq_CH - 865.1M) / 0.2M$
 Korea channel: $CH_Index = (Freq_CH - 917.1M) / 0.2M$

4.15.2 Response Frame

If set channel successfully, a response frame will be returned:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	AB	00	01	00	AD	7E

Type: 0x01
 Command: 0xAB
 PL: 0x0001
 Parameter: 0x00
 Checksum: 0xAD

4.16 Get Working Channel

4.16.1 Command Frame

Get the working channel under current working region, details as follows:

Header	Type	Command	PL(MSB)	PL(LSB)	Checksum	End
BB	00	AA	00	00	AA	7E

Type: 0x00
 Command: 0xAA
 PL: 0x0000
 Checksum: 0xAA

4.16.2 Response Frame

Response frame as follows when getting working current works:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	AA	00	01	00	AC	7E

Type: 0x01
 Command: 0xAA
 PL: 0x0001
 Parameter: 0x00 (Channel_Index 0x00)
 Checksum: 0xAC

Calculate Channel Frequency

China 900MHz channel: $\text{Freq_CH} = \text{CH_Index} * 0.25\text{M} + 920.125\text{M}$
 China 800MHz channel: $\text{Freq_CH} = \text{CH_Index} * 0.25\text{M} + 840.125\text{M}$
 USA channel: $\text{Freq_CH} = \text{CH_Index} * 0.5\text{M} + 902.25\text{M}$
 Europe channel: $\text{Freq_CH} = \text{CH_Index} * 0.2\text{M} + 865.1\text{M}$
 Korea channel: $\text{Freq_CH} = \text{CH_Index} * 0.2\text{M} + 917.1\text{M}$

4.17 Set Auto Frequency Hopping

Enable/Disable frequency hopping.

4.17.1 Command Frame

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	00	AD	00	01	FF	AD	7E

Type: 0x00
 Command: 0xAD

PL: 0x0001
 Parameter: 0xFF (0xFF = auto frequency hopping, 0x00 = cancelling auto frequency hopping)
 Checksum: 0xAD

4.17.2 Response Frame

If frequency hopping is set successfully, a response frame will be returned:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	AD	00	01	00	AF	7E

Type: 0x01
 Command: 0xAD
 PL: 0x0001
 Parameter: 0x00
 Checksum: 0xAF

4.18 Get the Transmitted Power

Get the current TX power.

4.18.1 Command Frame

Header	Type	Command	PL(MSB)	PL(LSB)	Checksum	End
BB	00	B7	00	00	B7	7E

Type: 0x00
 Command: 0xB7
 PL: 0x0000
 Checksum: 0xB7

4.18.2 Response Frame

Response frame as follows when the above command works:

Header	Type	Command	PL(MSB)	PL(LSB)	Pow(MSB)	Pow(LSB)	Checksum
BB	01	B7	00	02	07	D0	91
End							
7E							

Type: 0x01
 Command: 0xB7
 PL: 0x0002
 Power: 0x07D0 (current power of decimal 2000, that is 20dBm)
 Checksum: 0x91

4.19 Set the Transmitted Power

4.19.1 Command Frame

Header	Type	Command	PL(MSB)	PL(LSB)	Pow(MSB)	Pow(LSB)	Checksum
BB	00	B6	00	02	07	D0	8F
End							
7E							

Type: 0x00
 Command: 0xB6

PL: 0x0002
 Power: 0x07D0 (current power of decimal 2000, that is +20 dBm)
 Checksum: 0x8F

4.19.2 Response Frame

Response frame as follows when the above command works:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	B6	00	01	00	B8	7E

Type: 0x01
 Command: 0xB6
 PL: 0x0001
 Parameter: 0x00
 Checksum: 0xB8

4.20 Set Continuous Carrier

4.20.1 Command Frame

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	00	B0	00	01	FF	B0	7E

Type: 0x00
 Command: 0xB0
 PL: 0x0001
 Parameter: 0xFF(0xFF as opening continuous carrier, 0x00 as closing)
 Checksum: 0xB0

4.20.2 Response Frame

Response frame as follows when the above command works:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	B0	00	01	00	B2	7E

Type: 0x01
 Command: 0xB0
 PL: 0x0001
 Parameter: 0x00
 Checksum: 0xB2

4.21 Get Receiver Demodulator Parameters

To get the current key modem parameters that includes: the mixer gain, the intermediate frequency (baseband) amplifier gain and the threshold for demodulation (the tag returned signal with RSSI higher than threshold will be demodulated).

4.21.1 Command Frame

Header	Type	Command	PL(MSB)	PL(LSB)	Checksum	End
BB	00	F1	00	00	F1	7E

Type: 0x00
 Command: 0xF1
 PL: 0x0000
 Checksum: 0xF1

4.21.2 Response Frame

Response frame as follows when the above command works:

Header	Type	Command	PL(MSB)	PL(LSB)	Mixer_G	IF_G	Thrd(MSB)
BB	01	F1	00	04	03	06	01
Thrd(LSB)	Checksum	End					
B0	B0	7E					

Type: 0x01
 Command: 0xF1
 PL: 0x0004
 Mixer_G: 0x03 (Mixer gain of 9 dB, range: 0–9)
 IF_G: 0x06 (IF AMP gain of 36 dB)
 Threshold: 0x01B0 (recommend value of 0x01B0, max value of 0x0360)
 Checksum: 0xB0

Notes on the Threshold

The smaller the threshold is, the weaker tag returned signal could be received, but with the higher package error rate. So small threshold is for short communication, like inventory, to get longer reading distance. And large threshold is recommended for long communication, like read/write, to increase the success rate. 0x01B0 is a typical small threshold

Mixer Gain

Type	Mixer_G(dB)
0x00	0
0x01	3
0x02	6
0x03	9
0x04	12
0x05	15
0x06	16

IF AMP Gain

Type	IF_G(dB)
0x00	12
0x01	18
0x02	21
0x03	24
0x04	27
0x05	30
0x06	36
0x07	40

4.22 Set Receiver Demodulator Parameters

To set the key modem parameters which includes: the mixer gain, the IF amplifier gain and the threshold for demodulation.

4.22.1 Command Frame

Header	Type	Command	PL(MSB)	PL(LSB)	Mixer_G	IF_G	Thrd(MSB)
BB	00	F0	00	04	03	06	01

Thrd(LSB)	Checksum	End					
B0	AE	7E					

Type: 0x01
 Command: 0xF1
 PL: 0x0004
 Mixer_G: 0x03 (Mixer gain of 9 dB, range 0-9)
 IF_G: 0x06 (IF AMP gain of 36 dB)
 Threshold: 0x01B0 (recommend value of 0x01B0, max value of 0x0360)
 Checksum: 0xAE

Notes on the Threshold

The smaller the threshold is, the weaker tag returned signal could be received, but with the higher package error rate. So small threshold is for short communication, like inventory, to get longer reading distance. And large threshold is recommended for long communication, like read/write, to increase the success rate. 0x01B0 is a typical small threshold.

Mixer Gain

Type	Mixer_G(dB)
0x00	0
0x01	3
0x02	6
0x03	9
0x04	12
0x05	15
0x06	16

IF AMP Gain

Type	IF_G(dB)
0x00	12
0x01	18
0x02	21
0x03	24
0x04	27
0x05	30
0x06	36
0x07	40

4.22.2 Response Frame

If set modem parameters successfully, a response frame will be returned:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	F0	00	01	00	F2	7E

Type: 0x01
 Command: 0xF0
 PL: 0x0001
 Parameter: 0x00
 Checksum: 0xF1

4.23 Scan Jammer

To scan the jammer signal strength at the RF input port of the reader chip (a continuous wave will be transmitted at the current set power when doing the scan). The channel to be scan is determined by the current frequency band setting.

4.23.1 Command Frame

Header	Type	Command	PL(MSB)	PL(LSB)	Checksum	End
BB	00	F2	00	00	F2	7E

Type: 0x00
 Command: 0xF2
 PL: 0x0000
 Checksum: 0xF2

4.23.2 Response Frame

The scan jammer result will be returned by a response frame. E.g. in China 900 MHz band, there are 20 channels. If the scan jammer is executed successfully, a response frame will be returned.

Header	Type	Command	PL(MSB)	PL(LSB)	CH_L	CH_H	JMR(MSB)
BB	01	F2	00	16	00	13	F2
F1	F0	EF	EC	EA	E8	EA	EC
EE	F0	F1	F5	F5	F5	F6	F5
F5	F5	JMR(LSB)	Checksum	End			
		F5	DD	7E			

Type: 0x01
 Command: 0xF2
 PL: 0x0016
 Testing starting channel CH_L: 0x00 (starting value, Index as 0)
 Testing ending channel CH_H: 0x13 (ending value, Index as 19)
 JMR: 0xF2F1F0EFECEAE8EAECF0F1F5F5F5F6F5F5F5 (0xF2 as -14 dBm)
 Checksum: 0xDD

4.24 Scan Channel (LBT)

Listen Before Talk: Scan the channel power at the RF input power of the reader chip.

4.24.1 Command Frame

Header	Type	Command	PL(MSB)	PL(LSB)	Checksum	End
BB	00	F3	00	00	F3	7E

Type: 0x00
 Command: 0xF3
 PL: 0x0000
 Checksum: 0xF3

4.25.2 Response Frame

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter0	Parameter1	Parameter2
BB	01	1A	00	03	00	04	01
Checksum	End						
23	7E						

Type: 0x01
 Command: 0x1A
 PL: 0x0003
 Parameter: 0x00 0x04 0x01
 Checksum: 0x23

Item	Description	Length	State																								
0	Parameter 0	1 byte	Operation Type Select: 0x00: Set IO Direction ; 0x01: Set IO Level ; 0x02: Read IO Level. Current IO is defined by parameter 1																								
1	Parameter 1	1 byte	Range 0x01~0x04 selects port number of IO1~IO4																								
2	Parameter 2	1 byte	<table><tr><td colspan="3">0x00 or 0x01</td></tr><tr><th>Parameter0</th><th>Parameter2</th><th>State</th></tr><tr><td>0x00</td><td>0x00</td><td>Set IO direction fail</td></tr><tr><td>0x00</td><td>0x01</td><td>Set IO direction success</td></tr><tr><td>0x01</td><td>0x00</td><td>Set IO status fail</td></tr><tr><td>0x01</td><td>0x01</td><td>Set IO status success</td></tr><tr><td>0x02</td><td>0x00</td><td>IO status is low</td></tr><tr><td>0x02</td><td>0x01</td><td>IO status is high</td></tr></table>	0x00 or 0x01			Parameter0	Parameter2	State	0x00	0x00	Set IO direction fail	0x00	0x01	Set IO direction success	0x01	0x00	Set IO status fail	0x01	0x01	Set IO status success	0x02	0x00	IO status is low	0x02	0x01	IO status is high
0x00 or 0x01																											
Parameter0	Parameter2	State																									
0x00	0x00	Set IO direction fail																									
0x00	0x01	Set IO direction success																									
0x01	0x00	Set IO status fail																									
0x01	0x01	Set IO status success																									
0x02	0x00	IO status is low																									
0x02	0x01	IO status is high																									

4.26 Module Sleep

The Module Sleep command can make the module stay a low power status. Any byte sent by UART can wake up the module and the byte will be discarded. This command will also reset the M100/QM100 chip. The firmware will be downloaded to M100/QM100 chip after waking up. Some parameters might be reset.

4.26.1 Command Frame

Header	Type	Command	PL(MSB)	PL(LSB)	Checksum	End
BB	00	17	00	00	17	7E

Type: 0x00
 Command: 0x17
 PL: 0x0000
 Checksum: 0x17

4.26.2 Response Frame

The response frame is defined as below:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	17	00	01	00	19	7E

Type: 0x01
 Command: 0x17
 PL: 0x0001

Parameter: 0x00
Checksum: 0x19

4.27 Set Module Idle Time

This command can set how many minutes the module stays idle before it enters into sleep mode automatically.

4.27.1 Command Frame

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	00	1D	00	00	02	20	7E

Type: 0x00
Command: 0x17
PL: 0x0001
Parameter: 0x02 (leep after 2 minutes no operation, range 1...9minutes, 0x00 means no automatic sleep)
Checksum: 0x20

4.27.2 Response Frame

The response frame is defined as below:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	1D	00	01	02	21	7E

Type: 0x01
Command: 0x1D
PL: 0x0001
Parameter: 0x02 (Idle Time in Minutes)
Checksum: 0x21

4.28 NXP Read Protect/Reset Read Protect

NXP G2X tags support ReadProtect/Reset ReadProtect commands. The tag's ProtectEPC and ProtectTID bits will be set to '1' after executing ReadProtect successfully, and the tag will be in data protection status. A Reset ReadProtect command should be executed if a user wants the tag return to normal status. Before this command, a set select parameter command should be sent first to select a single tag.

4.28.1 Command Frame

Header	Type	Command	PL(MSB)	PL(LSB)	AP(MSB)	AP	AP
BB	00	E1	00	05	00	00	FF
AP(LSB)	Reset	Checksum	End				
FF	00	E4	7E				

Type: 0x00
Command: 0xE1
PL: 0x0005
Access Password: 0x0000FFFF
ReadProtect/
Reset ReadProtect: 0x00 (0x00 = Read Protect, 0x01 = Reset Read Protect)
Checksum: 0xE4

4.28.2 Response Frame

If a ReadProtect was executed successfully, the response frame is:

Header	Type	Command	PL(MSB)	PL(LSB)	UL	PC(MSB)	PC(LSB)
BB	01	E1	00	10	0E	30	00
EPC(MSB)	EPC	EPC	EPC	EPC	EPC	EPC	EPC
30	75	1F	EB	70	5C	59	04
EPC	EPC	EPC	EPC(LSB)	Parameter	Checksum	End	
E3	D5	0D	70	00	3E	7E	

Type: 0x01
 Command: 0xE1
 PL: 0x0010
 PC + EPC length UL: 0x0E
 PC: 0x3000
 EPC: 0x30751FEB705C5904E3D50D70
 Parameter: 0x00 (execution successful)
 Checksum: 0x3D

If a Reset ReadProtect was executed successfully, the response frame is:

Header	Type	Command	PL(MSB)	PL(LSB)	UL	PC(MSB)	PC(LSB)
BB	01	E2	00	10	0E	30	00
EPC(MSB)	EPC	EPC	EPC	EPC	EPC	EPC	EPC
30	75	1F	EB	70	5C	59	04
EPC	EPC	EPC	EPC(LSB)	Parameter	Checksum	End	
E3	D5	0D	70	00	3E	7E	

Type: 0x01
 Command: 0xE2
 PL: 0x0010
 PC + EPC length UL: 0x0E
 PC: 0x3000
 EPC: 0x30751FEB705C5904E3D50D70
 Parameter: 0x00 (execution successful)
 Checksum: 0x3E

If there is no tag response after ReadProtect (Set/Reset parameter is 0x00) command, an error code of 0x2A will be returned:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	FF	00	01	2A	2B	7E

Type: 0x01
 Command: 0xFF
 PL: 0x0001
 Parameter: 0x2A
 Checksum: 0x2B

If there is no tag response after ReadProtect (Set/Reset parameter is 0x01) command, an error code of 0x2B will be returned:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	FF	00	01	2B	2C	7E

Type: 0x01
 Command: 0xFF
 PL: 0x0001

Parameter: 0x2B
Checksum: 0x2C

If the access password is not correct, an error code of 0x16 will be returned, and the tag's PC+EPC will be sent back:

Header	Type	Command	PL(MSB)	PL(LSB)	Error Code	UL	PC(MSB)
BB	01	FF	00	10	16	0E	34
PC(LSB)	EPC(MSB)	EPC	EPC	EPC	EPC	EPC	EPC
00	30	75	1F	EB	70	5C	59
EPC	EPC	EPC	EPC	EPC(LSB)	Checksum	End	
04	E3	D5	0D	70	75	7E	

Type: 0x01
Command: 0xFF
PL: 0x0010
Error Code: 0x16
PC + EPC length UL: 0x0E
PC: 0x3400
EPC: 0x30751FEB705C5904E3D50D70
Parameter: 0x00 (execution successful)
Checksum: 0x75

4.29 NXP Change EAS

NXP G2X tags support Change EAS command. The tag's PSF bit will be set to '1' or '0' after executing Change EAS command. The tag will answer EAS_Alarm command when PSF bit is '1', otherwise the tag will not answer EAS_Alarm command when PSF bit is '0'. Before this command, a set select parameter command should be sent first to select a single tag.

4.29.1 Command Frame

Header	Type	Command	PL(MSB)	PL(LSB)	AP(MSB)	AP	AP
BB	00	E3	00	05	00	00	FF
AP(LSB)	PSF	Checksum	End				
FF	01	E7	7E				

Type: 0x00
Command: 0xE3
PL: 0x0005
Access Password: 0x0000FFFF
Set/Reset: 0x01 (0x01 = set PSF bit to '1', 0x00 = set PSF to '0')
Checksum: 0xE7

4.29.2 Response Frame

If Change EAS was executed successfully, the response frame is:

Header	Type	Command	PL(MSB)	PL(LSB)	UL	PC(MSB)	PC(LSB)
BB	01	E3	00	10	0E	30	00
EPC(MSB)	EPC	EPC	EPC	EPC	EPC	EPC	EPC
30	75	1F	EB	70	5C	59	04
EPC	EPC	EPC	EPC(LSB)	Parameter	Checksum	End	
E3	D5	0D	70	00	3F	7E	

Type: 0x01
Command: 0xE3
PL: 0x0010

PC + EPC length UL: 0x0E
 PC: 0x3000
 EPC: 0x30751FEB705C5904E3D50D70
 Parameter: 0x00 (execution successful)
 Checksum: 0x3F

If there is no tag response after Change EAS command, an error code of 0x1B will be returned:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	FF	00	01	1B	1C	7E

Type: 0x01
 Command: 0xFF
 PL: 0x0001
 Parameter: 0x1B
 Checksum: 0x1C

If the access password is not correct, an error code of 0x16 will be returned, and the tag's PC+EPC will be sent back:

Header	Type	Command	PL(MSB)	PL(LSB)	Error Code	UL	PC(MSB)
BB	01	FF	00	10	16	0E	34
PC(LSB)	EPC(MSB)	EPC	EPC	EPC	EPC	EPC	EPC
00	30	75	1F	EB	70	5C	59
EPC	EPC	EPC	EPC	EPC(LSB)	Checksum	End	
04	E3	D5	0D	70	75	7E	

Type: 0x01
 Command: 0xFF
 PL: 0x0010
 Error Code: 0x16
 PC + EPC length UL: 0x0E
 PC: 0x3400
 EPC: 0x30751FEB705C5904E3D50D70
 Parameter: 0x00 (execution successful)
 Checksum: 0x75

4.30 NXP EAS_Alarm

NXP G2X tags support EAS_Alarm command. The tag will answer 64 bits EAS-Alarm code immediately after EAS-alarm command. The tag will answer EAS-Alarm command only when PSF bit is set to '1'.

4.30.1 Command Frame

Header	Type	Command	PL(MSB)	PL(LSB)	Checksum	End
BB	00	E4	00	00	E4	7E

Type: 0x00
 Command: 0xE4
 PL: 0x0000
 Checksum: 0xE4

4.30.2 Response Frame

If EAS_Alarm command was executed successfully and the tag answers the right 64 bits EAS-Alarm code, the response frame is:

Header	Type	Command	PL(MSB)	PL(LSB)	EAS-Alarm Code (MSB)	EAS-Alarm Code	EAS-Alarm Code
BB	00	E4	00	08	69	0A	EC
EAS-Alarm Code	EAS-Alarm Code	EAS-Alarm Code	EAS-Alarm Code	EAS-Alarm Code (LSB)	Checksum	End	
7C	D2	15	D8	F9	80	7E	

Type: 0x00
 Command: 0xE4
 PL: 0x0008
 EAS-Alarm Code: 0x690AEC7CD215D8F9
 Checksum: 0x80

If there is no tag response after Change EAS command, an error code of 0x1D will be returned:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	FF	00	01	1D	1E	7E

Type: 0x01
 Command: 0xFF
 PL: 0x0001
 Parameter: 0x1D
 Checksum: 0x1E

4.31 NXP ChangeConfig

Some series of NXP G2X tags such as G2iM and G2iM+ support ChangeConfig command. This command can read or modify the 16bits Config-Word. The Config-Word is stored at address 20h of Bank 01 (EPC MemBank). It can be read or write by standard READ/WRITE command. The bits to be toggled in the configuration register need to be set to '1'. Before this command, a set select parameter command should be sent first to select a single tag.

4.31.1 Command Frame

Header	Type	Command	PL(MSB)	PL(LSB)	AP(MSB)	AP	AP
BB	00	E0	00	06	00	00	FF
AP(LSB)	Config(MSB)	Config(LSB)	Checksum	End			
FF	00	00	80	7E			

Type: 0x00
 Command: 0xE0
 Access Password: 0x0000FFFF
 Config-Word: 0x0000 (all 0 means response is unchanged Config-Word)
 Checksum: 0xE4

4.31.2 Response Frame

If ChangeConfig was executed successfully, the response is:

Header	Type	Command	PL(MSB)	PL(LSB)	UL	PC(MSB)	PC(LSB)
BB	01	E0	00	11	0E	30	00
EPC(MSB)	EPC	EPC	EPC	EPC	EPC	EPC	EPC
30	75	1F	EB	70	5C	59	04

EPC	EPC	EPC	EPC(LSB)	Config(MSB)	Config(LSB)	Checksum	End
E3	D5	0D	70	00	41	7E	7E

Type: 0x01
 Command: 0xE0
 PL: 0x0011
 PC + EPC length UL: 0x0E
 PC: 0x3000
 EPC: 0x30751FEB705C5904E3D50D70
 Config-Word: 0x0041
 Checksum: 0x7E

If there is no tag response after ChangeConfig command, an error code of 0x1A will be returned:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	FF	00	01	1A	1B	7E

Type: 0x01
 Command: 0xFF
 PL: 0x0001
 Parameter: 0x1A
 Checksum: 0x1B

If the access password is not correct, an error code of 0x16 will be returned, and the tag's PC+EPC will be sent back:

Header	Type	Command	PL(MSB)	PL(LSB)	Error Code	UL	PC(MSB)
BB	01	FF	00	10	16	0E	34
PC(LSB)	EPC(MSB)	EPC	EPC	EPC	EPC	EPC	EPC
00	30	75	1F	EB	70	5C	59
EPC	EPC	EPC	EPC	EPC(LSB)	Checksum	End	
04	E3	D5	0D	70	75	7E	

Type: 0x01
 Command: 0xFF
 PL: 0x0010
 Error Code: 0x16
 PC + EPC length UL: 0x0E
 PC: 0x3400
 EPC: 0x30751FEB705C5904E3D50D70
 Parameter: 0x00 (execution successful)
 Checksum: 0x75

4.32 Impinj Monza QT

Impinj Monza 4QT tags support QT command that can modify the QT Control Word. Setting the QT_SR bit can reduce the tag's operation range and modifying the QT_MEM bit can switch the tag to use Public Memory Map or Private Memory Map. Before this command, a set select parameter command should be sent first to select a single tag.

4.32.1 Command Frame

QT command is defined as blow (set QT_MEM to 1 and write it to Non-volatile memory in this example):

Header	Type	Command	PL(MSB)	PL(LSB)	AP(MSB)	AP	AP
BB	00	E3	00	05	00	00	FF
AP(LSB)	Read/Write	Persistence	Payload0	Payload1	Checksum	End	
FF	01	01	40	00	2D	7E	

Type: 0x00
 Command: 0xE5
 PL: 0x0008
 Access Password: 0x0000FFFF
 Read/Write: 0x01 (0x00 = read, 0x01 = write)
 Persistence: 0x01(0x00: write to volatile memory, 0x01: write it to Non-volatile memory, should always be 0x01)
 Payload: 0x4000(QT Control, two MSB bits is QT_SR and QT_MEM)
 Checksum: 0x2D

4.32.2 Response Frame

If the QT command was executed successfully and the Read/Write field was 0x00, the response frame is:

Header	Type	Command	PL(MSB)	PL(LSB)	UL	PC(MSB)	PC(LSB)
BB	01	E5	00	11	0E	30	00
EPC(MSB)	EPC	EPC	EPC	EPC	EPC	EPC	EPC
30	75	1F	EB	70	5C	59	04
EPC	EPC	EPC	EPC(LSB)	QT Control0	QT Control1	Checksum	End
E3	D5	0D	70	00	00	42	7E

Type: 0x01
 Command: 0xE0
 PL: 0x0011
 PC + EPC length UL: 0x0E
 PC: 0x3000
 EPC: 0x30751FEB705C5904E3D50D70
 QT Control Word: 0x0000
 Checksum: 0x42

If the QT command was executed successfully and Read/Write field was 0x01, the response frame is:

Header	Type	Command	PL(MSB)	PL(LSB)	UL	PC(MSB)	PC(LSB)
BB	01	E5	00	11	0E	30	00
EPC(MSB)	EPC	EPC	EPC	EPC	EPC	EPC	EPC
30	75	1F	EB	70	5C	59	04
EPC	EPC	EPC	EPC(LSB)	Parameter	Checksum	End	
E3	D5	0D	70	00	42	7E	

Type: 0x01
 Command: 0xE0
 PL: 0x0011
 PC + EPC length UL: 0x0E

PC: 0x3000
 EPC: 0x30751FEB705C5904E3D50D70
 Parameter: 0x00 (execution successful)
 Checksum: 0x42

If there is no tag response after QT command, an error code of 0x2E will be returned:

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	FF	00	01	2E	2F	7E

Type: 0x01
 Command: 0xFF
 PL: 0x0001
 Parameter: 0x2E
 Checksum: 0x2F

If the access password is not correct, an error code of 0x16 will be returned, and the tag's PC+EPC will be sent back:

Header	Type	Command	PL(MSB)	PL(LSB)	Error Code	UL	PC(MSB)
BB	01	FF	00	10	16	0E	34
PC(LSB)	EPC(MSB)	EPC	EPC	EPC	EPC	EPC	EPC
00	30	75	1F	EB	70	5C	59
EPC	EPC	EPC	EPC	EPC(LSB)	Checksum	End	
04	E3	D5	0D	70	75	7E	

Type: 0x01
 Command: 0xFF
 PL: 0x0010
 Error Code: 0x16
 PC + EPC length UL: 0x0E
 PC: 0x3400
 EPC: 0x30751FEB705C5904E3D50D70
 Parameter: 0x00 (execution successful)
 Checksum: 0x75

5 Error Frames

If the command frame fails to execute, the uhf-M chip sends a response frame that fails to execute to the host computer. The response frame that failed to execute shares the instruction code 0xFF. If the EPC of the tag is not obtained before the execution fails, the instruction parameter is fixed to an error code of 1 byte. If the EPC of the tag is obtained before the execution fails, the response frame parameter is an error code of 1 byte plus the tagged PC+EPC data.

For example, if the inventory command frame fails to execute, does not receive a label return or returns a data CRC check error, it will return error code 0x15, as follows

For example

Header	Type	Command	PL(MSB)	PL(LSB)	Parameter	Checksum	End
BB	01	FF	00	01	15	16	7E

FrameType: 0x01

Command: 0xFF (0xFF indicates executing failure)

Length of command parameter: 0x01

Command Parameter: 0x15 (returned error code when command executed with failure)

Checksum: 0x16

5.1 Error Codes

Type	Code	Description
Command Error	0x17	Command code error
FHSS Fail	0x20	Frequency hopping time out. All channel are occupied.
Inventory Fail	0x15	Inventory fail. No tag response or CRC error.
Access Fail	0x16	Access fail. May caused by password error.
Read Fail	0x09	Read fail. No tag response or CRC error.
Read Error	0xA0 Error code	Read error. Error code (0xA0 Error code) indication refer to Tag-error code in the next table.
Write Fail	0x10	Write fail. No tag response or CRC error.
Write Error	0xB0 Error code	Write error. Error code (0xB0 Error code) indication refer to Tag-error code in the next table.
Lock Fail	0x13	Lock fail. No tag response or CRC error.
Lock Error	0xC0 Error code	Lock error. Error code (0xC0 Error code) indication refer to Tag-error code in the next table.
Kill Fail	0x12	Kill fail. No tag response or CRC error.
Kill Error	0xD0 Error code	Kill error. Error code (0xD0 Error code) indication refer to Tag-error code in the next table.

5.2 EPC Gen2 protocol specified error code

Tag error-code

Error-code Support	Error Code	Error code Name	Error Description
Error-specific	000000002	Other error	Other errors not described in this table.
	000000112	Memory overrun	The given memory area does not exist. Or the tag does not support the given EPC length, e.g. XPC.

	000001002	Memory locked	The given memory area is locked and/or permanent locked. And the lock status is not readable or not writeable.
	000010112	Insufficient power	Tag has no enough power to write.
Non-specific	000011112	Non-specific error	Tag does not support error-code.

5.3 Specific Error Codes of NXP G2X Tag

ChangeConfig Fail	0x1A	ChangeConfig failed. No tag response or CRC error.
ReadProtect Fail	0x2A	ReadProtect failed. No tag response or CRC error.
Reset ReadProtect Fail	0x2B	Reset ReadProtect failed. No tag response or CRC error.
Change EAS Fail	0x1B	Change EAS failed. No tag response or CRC error.
EAS_Alarm Fail	0x1D	EAS_Alarm failed. No correct Alarm Code response.
Specified returned error code of NXP	0xE0 Error code	Specific commands error code. Error code (0xE0 Error code) indication refer to Tag-error code in the EPC Gen2 protocol.

5.4 Specific Error Codes of Impinj Monza QT Tag

QT Fail	0x2E	QT failed. No tag response or CRC error.
Specified returned error code of tag	0xE0 Error code	Specific commands error code. Error code (0xE0 Error code) indication refer to Tag-error code in the EPC Gen2 protocol.

6 Revision History

Date	Version	Description
2022-07-20	2.1	First version in this layout