Type	
Date	
Version	02.01
Department	Engineering

Share Bike Bluetooth Smart Lock(Hardware) Air interface Protocol

Revision history:

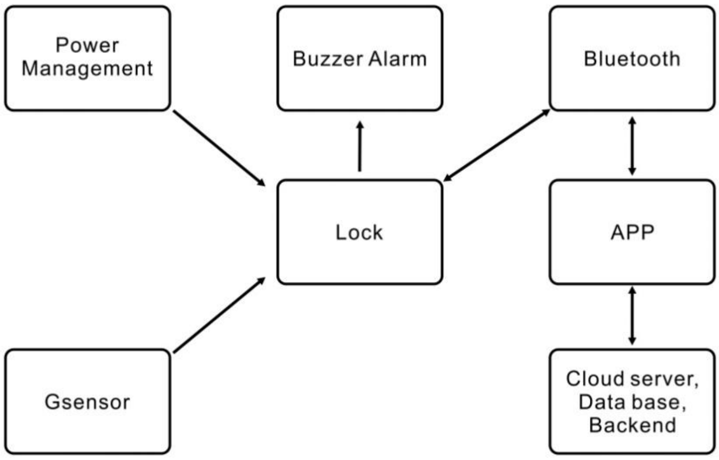
Version	Date	Revision description	Drafted by

Content

1.1 Purpose

This document is a illustration about the communication protocol between smart bike lock and Server or APP designed and manufactured by Omni。

1.2 Items Functions Framework



1.3 Communication package format

Byte	Item	Instructions
0	STX	Data header/frame header, fixed value：0xFE
1	NUM	Random Number, is generated only when data sending， for encrypting Data
2	ID	User's ID from APP, this ID is allotted by Server when registering
3		
4		
5		
6	KEY	Communicate secret key， generated randomly by bike lock， APP receives the KEY by（0x11）command
7	CMD	Command byte
8	LEN	Data length
9	DATA	Data
10+LEN	CRC	CRC16 checking value, the Data before CRC after being encrypted
11+LEN		

1.4 Data encryption processing

Encryption consistent：random num, KEY.
Encryption processing:

1、Generate random NUM
2、Generate random variant NUM_1 = NUM + 0x32
3、Fill NUM_1 into the First byte of Data
4、Use NUM or after NUM， before CRC plaintext data, and fill the results corresponding
5、Take the data before CRC to do CRC16 Checking， checking value files into CRC position.

For example -> unlock command(random NUM is 0x88 ; KEY is 0x88) **RED** part are CRC value.

plaintext	0xFE,0x88,0x11,0x11,0x11,0x11,0x88,0x21,0x00
ciphertext	0xFE,0xBA,0x99,0x99,0x99,0x99,0x00,0xA9,0x88,**0xE9,0x91**

1.5 Communications process between APP and bike lock

1.APP is connecting to bike lock by bluetooth.
2.APP is sending command（0x11）to bike lock for getting communication secret key.
3.Bike Lock returns to communication secret KEY, APP needs to save KEY for next communication
4.APP is building communication to bike lock.

Note： KEY is only regenerated when APP is building communication to bike lock， communication is kept from now on.

1.6 Command list

1 , Getting unlock KEY command(0x11)
2 , Unlock command(0x21)
3 , lock command(0x22)
4, Checking bike lock status(0x31)
5, Getting un-uploaded Data(0x51)
6, Erase un-uploaded Data (0x52)
7, Popping up battery of bike lock(0x81)

1.7 Command illustration &Sample

1.7.1 Getting unlock KEY command(0x11)

1.7.1.1 APP->Bike Lock

Byte	Item	Instruction
0	STX	Data header/frame header, fixed value：0xFE
1	NUM	Random Number
2	ID	APP user' ID Number
3		
4		
5		
6	KEY	0x00
7	CMD	0x11

8	LEN	0x00
9	CRC	CRC16 checking value, the Data before CRC after being encrypted
10		

e.g： user ID(11H,11H,11H,11H) random number（88H）

plaintext	0xFE,0x88,0x11,0x11,0x11,0x11,0x00,0x11,0x00
ciphertext	0xFE,0xBA,0x99,0x99,0x99,0x99,0x88,0x99,0x88,**0xC3,0x05**

1.7.1.2 Bike Lock->APP

Byte	Items	Instructions
0	STX	Data header/frame header, fixed value： 0xFE
1	NUM	Random Number
2	ID	APP user' ID Number
3		
4		
5		
6	KEY	communication secret key
7	CMD	0x11
8	LEN	0x01
9	DATA	Secret KEY
10	CRC	CRC16 checking value, the Data before CRC after being encrypted
11		

e.g： user ID(11H,11H,11H,11H) random number（88H）,KEY(80H) **RED** part are CRC value

plaintext	0xFE,0x88,0x11,0x11,0x11,0x11,0x80,0x11,0x01,0x80
ciphertext	0xFE,0xBA,0x99,0x99,0x99,0x99,0x08,0x99,0x89,0x08,**0x95,0x2A**

1.7.2 Unlock command (0x21)

1.7.2.1 APP->bike lock

byte	Item	Instructions
0	STX	Data header/frame header, fixed value： 0xFE
1	NUM	Random Number
2	ID	APP user' ID Number
3		
4		
5		
6	KEY	communication secret key
7	CMD	0x21
8	LEN	0x00
9	CRC	CRC16 checking value, the Data before CRC after being encrypted
10		

e.g： user ID(11H,11H,11H,11H) random number（88H）,KEY(80H) **RED** part are CRC value

plaintext	0xFE,0x88,0x11,0x11,0x11,0x11,0x80,0x21,0x00
ciphertext	0xFE,0xBA,0x99,0x99,0x99,0x99,0x08,0xA9,0x88,**0x2B,0x10**

1.7.2.2 Bike Lock->APP

Byte	Item	Instructions
0	STX	Data header/frame header, fixed value： 0xFE
1	NUM	Random Number
2	ID	APP user' ID Number
3		
4		
5		
6	KEY	communication secret key
7	CMD	0x21
8	LEN	0x01
9	DATA	Return value 0:unlock succeed 1:unlock failed
10	CRC	CRC16 checking value, the Data before CRC after being encrypted
11		

e.g： user ID(11H,11H,11H,11H) random number（88H）,KEY(80H) **RED** part are CRC value

plaintext	0xFE,0x88,0x11,0x11,0x11,0x11,0x80,0x21,0x01,0x00
ciphertext	0xFE,0xBA,0x99,0x99,0x99,0x99,0x08,0xA9,0x89,0x88,**0x3A,0x2B**

1.7.3 lock command (0x22)

1.7.3.1 Bike->APP

Item	Instructions
STX	Data header/frame header, fixed value： 0xFE
NUM	Random Number
ID	APP user' ID Number
KEY	communication secret key
CMD	0x22
LEN	0x01
DATA	0:unlock succeed 1:unlock failed
CRC	CRC16 checking value, the Data before CRC after being encrypted

e.g： user ID(11H,11H,11H,11H) random number（88H）,KEY(80H) **RED** part are CRC value

plaintext	0xFE,0x88,0x11,0x11,0x11,0x11,0x80,0x22,0x01,0x00
ciphertext	0xFE,0xBA,0x99,0x99,0x99,0x99,0x08,0xAA,0x89,0x88,**0x3A,0xDB**

1.7.3.2 APP->bike lock

Byte	Items	Instructions

0	STX	Data header/frame header, fixed value：0xFE
1	NUM	Random Number
2	ID	APP user' ID Number
3		
4		
5		
6	KEY	communication secret key
7	CMD	0x22
8	LEN	0x00
9	CRC	CRC16 checking value, the Data before CRC after being encrypted
10		

e.g： user ID(11H,11H,11H,11H) random number（88H）,KEY(80H) **RED** part are CRC value

plaintext	0xFE,0x88,0x11,0x11,0x11,0x11,0x80,0x22,0x00
ciphertext	0xFE,0xBA,0x99,0x99,0x99,0x99,0x08,0xAA,0x88,**0xDB,0x10**

1.7.4 Checking bike lock status (0x31)

1.7.4.1 APP->bike lock

Byte	Item	Instructions
0	STX	Data header/frame header, fixed value：0xFE
1	NUM	Random Number
2	ID	APP user' ID Number
3		
4		
5		
6	KEY	communication secret key
7	CMD	0x31
8	LEN	0x00
9	CRC	CRC16 checking value, the Data before CRC after being encrypted
10		

e.g： user ID(11H,11H,11H,11H) random number（88H）,KEY(80H) **RED** part are CRC value

plaintext	0xFE,0x88,0x11,0x11,0x11,0x11,0x80,0x31,0x00
ciphertext	0xFE,0xBA,0x99,0x99,0x99,0x99,0x08,0xB9,0x88,**0xEB,0x1D**

1.7.4.2 bike lock->APP

Byte	Item	Instructions
0	STX	Data header/frame header, fixed value：0xFE
1	NUM	Random Number
2	ID	APP user' ID Number
3		
4		
5		
6	KEY	communication secret key

7	CMD	0x31
8	LEN	0x03
9	DATA	bike lock status 0：unlock 1：lock
10		Battery volume e.g：37（decimalism）为 3.7V
11		Whether un-upload data 0：Yes 1：no
12	CRC	CRC16 checking value, the Data before CRC after being encrypted
13		

e.g： user ID(11H,11H,11H,11H) random number（88H）,KEY(80H) **RED** part are CRC value

plaintext	0xFE,0x88,0x11,0x11,0x11,0x11,0x80,0x31,0x03,0x00,0x25,0x01
ciphertext	0xFE,0xBA,0x99,0x99,0x99,0x99,0x08,0xB9,0x8B,0x88,0xAD,0x89,**0xAE,0xE3**

1.7.5 Getting un-uploaded Data (0x51)

Note: This is the data which un-uploaded to APP or Server, including user ID and using time for payment.

1.7.5.1 APP->Bike Lock

Byte	Item	Instructions
0	STX	Data header/frame header, fixed value：0xFE
1	NUM	Random Number
2	ID	APP user' ID Number
3		
4		
5		
6	KEY	communication secret key
7	CMD	0x51
8	LEN	0x00
9	CRC	CRC16 checking value, the Data before CRC after being encrypted
10		

e.g： user ID(11H,11H,11H,11H) random number（88H）,KEY(80H) **RED** part are CRC value

plaintext	0xFE,0x88,0x11,0x11,0x11,0x11,0x80,0x51,0x00
ciphertext	0xFE,0xBA,0x99,0x99,0x99,0x99,0x08,0xD9,0x88,**0xEB,0x35**

1.7.5.2 bike lock->APP

byte	item	Instructions
0	STX	Data header/frame header, fixed value：0xFE
1	NUM	Random Number
2-5	ID	APP user' ID Number
6	KEY	communication secret key
7	CMD	0x51
8	LEN	0x08
9-12	DATA	Using time unit：minute
13-16	DATA	User ID
17	CRC	CRC16 checking value, the Data before CRC after being encrypted

18		

e.g.： user ID(11H,11H,11H,11H) random number（88H）,KEY(80H) **RED** part are CRC value

plaintext	0xFE,0x88,0x11,0x11,0x11,0x11,0x80,0x51,0x08,0x00,0x00,0x00,0x01,0x00,0x00,0x00,0x02
ciphertext	0xFE,0xBA,0x99,0x99,0x99,0x99,0x08,0xD9,0x80,0x88,0x88,0x88,0x89,0x88,0x88,0x88,0x8A,**0x51,0x71**

1.7.6 Erase un-uploaded Data (0x52)

1.7.6.1 APP->Bike lock

Byte	Item	Instruction
0	STX	Data header/frame header, fixed value： 0xFE
1	NUM	Random Number
2	ID	APP user' ID Number
3		
4		
5		
6	KEY	communication secret key
7	CMD	0x52
8	LEN	0x00
9	CRC	CRC16 checking value, the Data before CRC after being encrypted
10		

e.g.： user ID(11H,11H,11H,11H) random number（88H）,KEY(80H) **RED** part are CRC value

plaintext	0xFE,0x88,0x11,0x11,0x11,0x11,0x80,0x52,0x00
ciphertext	0xFE,0xBA,0x99,0x99,0x99,0x99,0x08,0xDA,0x88,**0x1B,0x35**

1.7.6.2 Bike lock->APP

Byte	Item	Instruction
0	STX	Data header/frame header, fixed value： 0xFE
1	NUM	Random Number
2	ID	APP user' ID Number
3		
4		
5		
6	KEY	communication secret key
7	CMD	0x52
8	LEN	0x01
9	DATA	Return value： 0： succeed 1： failed
12	CRC	CRC16 checking value, the Data before CRC after being encrypted
13		

e.g.： user ID(11H,11H,11H,11H) random number（88H）,KEY(80H) **RED** part are CRC value

plaintext	0xFE,0x88,0x11,0x11,0x11,0x11,0x80,0x52,0x01,0x00

ciphertext	0xFE,0xBA,0x99,0x99,0x99,0x99,0x08,0xDA,0x89,0x88,**0xE1,0xDA**

1.7.7 Popping up battery of bike lock (0x81)

1.7.7.1 APP->bike lock

Byte	Item	Instruction
0	STX	Data header/frame header, fixed value：0xFE
1	NUM	Random Number
2	ID	APP user' ID Number
3		
4		
5		
6	KEY	communication secret key
7	CMD	0x81
8	LEN	0x00
9	CRC	CRC16 checking value, the Data before CRC after being encrypted
10		

e.g：user ID(11H,11H,11H,11H) random number（88H）,KEY(80H) **RED** part are CRC value

plaintext	0xFE,0x88,0x11,0x11,0x11,0x11,0x80,0x52,0x00
ciphertext	0xFE,0xBA,0x99,0x99,0x99,0x99,0x08,0x09,0x88,**0x2B,0x68**

1.7.7.2 Bike Lock->APP

Byte	Item	Instruction
0	STX	Data header/frame header, fixed value：0xFE
1	NUM	Random Number
2	ID	APP user' ID Number
3		
4		
5		
6	KEY	communication secret key
7	CMD	0x81
8	LEN	0x01
9	DATA	Return value：0：succeed 1：failed
12	CRC	CRC16 checking value, the Data before CRC after being encrypted
13		

e.g：user ID(11H,11H,11H,11H) random number（88H）,KEY(80H) **RED** part are CRC value

plaintext	0xFE,0x88,0x11,0x11,0x11,0x11,0x80,0x81,0x01,0x00
ciphertext	0xFE,0xBA,0x99,0x99,0x99,0x99,0x08,0x09,0x89,0x88,**0x2B,0x68**