摩亭智能锁蓝牙通信协议

文档名称	
编号	
关键字	项目
编制	
日期	
保密等级	内部

目录

修订表

审批记录

版本	审批人	审批意见	审批日期

1. 协议格式

1.1 基本格式

SOF	LEN	CMD	DATA	CHK
2 bytes	1 byte	1 byte	n bytes	1 byte

SOF: 帧头，规定两个字节 0x67 0x74
LEN: 负载字段长度
CMD: 指令码

位	描述
Bit 7	数据传输方向 0: 锁->app 1: app->锁
Bit 6	数据类型 0: 请求数据 1: 应答数据
Bit 0~5	指令编码

Bit 7: 0: 锁->app 1: app->锁
Bit 6: 0: 主发 1: 应答
Bit 0~5: 指令编码
DATA: 负载数据
CHK: 校验位，从 CMD 到 DATA 最后一字节异或产生的值

1.2 蓝牙服务

- 使用服务 UUID: FFF0
- 使用写入设备特征值 UUID: FFF5
- 使用读取设备特征值 UUID: FFF6
- 单个蓝牙数据包最大长度 20 字节

1.3 约定

整型数据统一使用大端字节序，高位在前。

1.4 示例

App 发送:
0x67 0x74 0x00 0x90 0x90 查询锁是否在租车状态
锁返回:
0x67 0x74
0x00 0x50 0x01 51 表示在租车状态

2. 协议内容

0x81 请求租车

蓝牙开锁前要先发送请求租车，获取车辆状态

app->lock，指令码: 0x81

字段	长度	描述
经度	10/0	手机定位经度，没有定位到不填写
纬度	9/0	手机定位纬度，没有定位到不填写

lock->app，指令码: 0x41

字段	长度	描述
应答码	1	见应答码定义
版本信息	2	硬件版本号+软件版本号 0x1166
锁状态	1	0: 锁关闭 1: 锁打开
租车序列号	4	用做开锁时的加密源 mac 4byte （1100f6ff）
电池电压	2	整型, 330 即 3.30v
短信条数	1	Sim 卡中短信数量(未使用)

0x82 开锁

加密说明:

算法: AES(ECB) 128 位（现在是源码字符串+mac）

秘钥:每把锁有唯一 80 字符串秘钥，(随机字符串生成 68 字符串+ mac 地址 12 字符串)

秘钥索引: 范围 0----64（80-16）

加密源: 从索引值开始的 16 位字符串和 KEY 进行加密

app->lock，指令码: 0x82

字段	长度	描述
秘钥索引	1	实际秘钥索引
用户 ID	7	用户手机号
时间戳	4	用于锁同步时间(作为骑行开始时间)。由后台生成
AES 加密数据	16	从索引值开始的 16 位字符串和 KEY 进行加密

lock->app，指令码: 0x42

字段	长度	描述

应答码	1	见定义

0x86 获取/删除交易记录

获取/删除最新记录

app->lock，指令码: 0x86

字段	长度	描述
交易序列号	13/0	当字段长度为 0 是会获取锁的最新记录，当字段传入 13 个字节交易序列号时删除最近获取的记录，返回下一条记录

lock->app，指令码: 0x46

字段	长度	描述
用户 ID	6	开锁时传入的用户 ID（手机号）
交易序列号	13	4 字节时间戳 + 9 字节车号（ascii 的 16 进制）
交易时间	4	整型时间戳（低位在前）
交易记录类型	1	租车 00 /还车 01
纬度	12	锁位置维度
经度	12	锁位置经度
Aes 加密数据	16	AES 加密数据
秘钥索引	1	实际索引
电池电量	3	电量百分比
电池电压	2	整型, 330 即 3.30v（低位在前）

0x89 重启设备（维护 app 使用）

设备软件重启---维护 app 使用

app->lock，指令码: 0x89

字段	长度	描述
约定字符	1	0xf0

0x8D 蜂鸣器长叫（维护 app 使用）

使蜂鸣器长叫，按键停止---维护 app 使用

app->lock，指令码: 0x01

字段	长度	描述
随机数	4	无

约定字符	1	0xf2

lock->app, 指令码: 0x81

字段	长度	描述
应答码	1	

0x90 租还状态查询/通知（连接后发送查询指令）

查询设备是否租车，如果蓝牙连接状态，锁关闭，主动发送应答指令通知 app 还车

app->lock, 指令码: 0x90

字段	长度	描述
无	0	无

lock->app, 指令码: 0x50 关

字段	长度	描述	
应答码	1	0x00: 还车状态，0x01: 租车状态	
用车时间	4	从开锁到关锁的秒数	用来统计计费

0x93 查询硬件信息 （维护 app 使用）

获取硬件信息

app->lock, 指令码: 0x93

字段	长度	描述
无	0	无

lock->app, 指令码: 0x53

字段	长度	描述
设备运行时间	4	大端整型时间戳
太阳能板电压	2	大端整型（预留）
蜂鸣器运行状态	1	0x00 关闭, 0x01 运行
电机运行状态	1	0x00 关闭, 0x01 运行
交易记录个数	1	锁已保存记录个数（不用）

0x94 控制器透传命令 读取蓝牙命令(保留)

app->lock，指令码: 0x94

字段	长度	描述
蓝牙返回	9	蓝牙返回控制原始数据

lock->app，指令码: 0x54

字段	长度	描述
控制器发送	16	控制器发送原始数据

0x95 骑行模式控制 （控制器指令，old，20171118 以后废弃）

app->lock，指令码: 0x95

字段	长度	描述
是否受控	1	0x01：自动模式；0x02：后台控制
骑行模式	1	0x00：普通模式 0x01：无电模式 0x02：助力模式

lock->app，指令码: 0x55

字段	长度	描述
骑行模式	1	0x00：成功 0x01：失败

0x96 控制器状态获取 （控制器指令，old，20171118 以后废弃）

app->lock，指令码: 0x96

字段	长度	描述
无	0	无

lock->app，指令码: 0x56

字段	长度	描述
电池组电压	2	单位 ：0.1V。低字节在前，高字节在后（下同）。
电池组电流	1	有符号数，负电流代表反充电电流。单位 ：0.1A
当前整车速度	2	单位: 0.1km/h
当前踏频	1	单位: rpm
故障代码	1	0x00：无故障，0x21：电流异常， 0x24：电机霍尔故障， 0x25：刹车故障，0x26：电池欠压，0x27：IIC 通信故障
状态码	1	Bit7:陀螺仪校准状态

		0：无校准 1：校准成功 Bit[4-6]:保留 Bit[2-3]:自行车控制器运行状态是否受控; 01 ： 不受后台控制，即自行充放电运行模式 10 ： 受后台控制充放电切换运行模式 Bit[0-1]:自行车控制器运行模式; 00 ： 普通模式 01 ： 助力模式 10 ： 欠压充电模式 11 ： 超速充电模式
本次骑行实时公里数	2	单位:0.1 公里

0x97 获取 BMS 信息 （控制器指令，old，20171118 以后废弃）

app->lock，指令码: 0x97

字段	长度	描述
无	0	无

lock->app，指令码: 0x57

字段	长度	描述
电池表面温度	2	电池表面温度，单位为开尔文的温度数值，分辨率 0.1K。 转换为摄氏度的算法如下实例: 如，读取的数据为 0xb90＝2960 则，摄氏度为 2960－2731=229＝22.9 低字节在前，高字节在后（下同）。
电池剩余容量	2	单位: mAh
电池充电循环次数	2	
历史上最大的充电间隔时间，	2	单位:小时
当前充电间隔时间	2	单位:小时
电池满充容量	2	单位:mAh
荷电态	2	无单位，数值范围为 0~100
BMS 自身采集的电压	2	单位:mV
BMS 自身采集的电流	2	单位:mA

0x98 查询控制器及 BMS 序列号 （控制器指令，old，20171118 以后废弃）

app->lock，指令码: 0x98

字段	长度	描述
无	0	无

lock->app，指令码: 0x58

字段	长度	描述
控制器序列号	32	
BMS 序列号	32	

注:字节序列号具体定义参考摩亭序列号编码规则一文

0x99 激活 GPRS 功能 （控制器指令，old，20171118 以后废弃）

app->lock，指令码: 0x99

字段	长度	描述
无	0	无

lock->app，指令码: 0x59

字段	长度	描述
激活状态	1	0x00: 激活成功 0x01: 已激活 0x02: 激活失败

0x9A 电池锁(BMS)控制指令 （控制器指令，old，20171118 以后废弃）

app->lock，指令码: 0x9A

字段	长度	描述
状态控制	1	0x00: 关锁 0x01: 开锁

lock->app，指令码: 0x5A

字段	长度	描述
电池锁当前状态	1	**开锁时只判断 bit2bit1bit0:** bit2bit1bit0=0b000 未执行开锁动作 bit2bit1bit0=0b001 执行开锁动作中 bit2bit1bit0=0b011 执行完开锁动作，且开锁成功 bit2bit1bit0=0b101 执行完开锁动作，且开锁失败 **关锁时只判断 bit6bit5bit4:**

		bit6bit5bit4=0b000 未执行关锁动作 bit6bit5bit4=0b001 执行关锁动作中 bit6bit5bit4=0b011 执行完关锁动作，且关锁成功 bit6bit5bit4=0b101 执行完关锁动作，且关锁失败

0x9B 控制器电源控制指令 （控制器指令，old，20171118 以后废弃）

app->lock，指令码: 0x9B

字段	长度	描述
是否关闭控制器	1	0x00: 不执行关动作 0x01: 执行关动作

lock->app，指令码: 0x5B

字段	长度	描述
状态返回	1	0x00: 成功

0x9C 控制器透传命令 控制器读取工作模式命令（控制器透传指令，0x10，20171118 新增）

app->lock，指令码: 0x9C

字段	长度	描述
蓝牙返回	16	蓝牙返回控制原始数据 0X10

lock->app，指令码: 0x5C

字段	长度	描述
控制器发送	9	控制器发送原始数据 0X10

0x9D 控制器透传命令 读取控制状态命令（控制器透传指令，0x11，20171118 新增）

app->lock，指令码: 0x9D

字段	长度	描述
蓝牙返回	12	蓝牙返回控制原始数据 0X11

lock->app，指令码: 0x5D

字段	长度	描述
控制器发送	28	控制器发送原始数据 0X11

0x9E 控制器透传命令 读取 BMS 状态命令（控制器透传指令，0x12，20171118 新增）

app->lock，指令码: 0x9E

字段	长度	描述
蓝牙返回	9	蓝牙返回控制原始数据 0X12

lock->app，指令码: 0x5E

字段	长度	描述
控制器发送	28	控制器发送原始数据 0X12

0x9F 控制器透传命令读取 BMS 序列号命令（控制器透传指令，0x14，20171118 新增）

app->lock，指令码: 0x9F

字段	长度	描述
蓝牙返回	12	蓝牙返回控制原始数据 0X14

lock->app，指令码: 0x5F

字段	长度	描述
控制器发送	72	控制器发送原始数据 0X14

3. 应答码

应答码	描述
0x00	正常
0x01	锁已开
0x02	电量不足
0x03	加密验证失败
0x04	内存空间不足
0x05	格式错误
0x06	没有权限
0x07	Flash 写入失败
0x08	数据空

4．补充内容（for Nordic）

蓝牙建立连接以后，APP 要主动连续发送 0x01 0x00 两个数据给锁（补齐 18 个 0，一共 20 个字节）。