

# 摩亨电助力智能锁蓝牙通信协议

## V3. 4

文档名称	
编号	
关键字	项目
编制	
日期	
保密等级	内部

## 目录

1. 协议格式.....	1
1.1 基本格式.....	1
1.2 蓝牙服务.....	1
1.3 约定.....	1
1.4 示例.....	1
2. 协议内容.....	2
0x81 请求租车.....	2
0x82 开锁.....	2
0x86 获取/删除交易记录.....	3
0x89 重启设备.....	3
0x8D 蜂鸣器长叫.....	3
0x90 租还状态查询/通知（连接后发送查询指令）.....	4
0x93 查询硬件信息（维护 app 使用）.....	4
0x94 控制器透传命令(20171118 保留暂不使用).....	5
0x99 激活网络（GPRS） 功能.....	5
0x9C 控制器透传命令 控制器读取工作模式命令.....	5
0x9D 控制器透传命令 读取控制状态命令.....	6
0x9E 控制器透传命令 读取 BMS 状态命令.....	6
0x9F 控制器透传命令 读取 BMS 序列号命令.....	6
0xA0 锁的生产 APP 获取硬件初始数据.....	6
0xA1 控制器透传命令 预留（20171120）.....	7
0xA2 控制器透传命令 预留（20171120）.....	8
0xA3 控制器透传命令 预留（20171120）.....	8
0xA4 关闭网络模块（GPRS） 功能.....	8
3. 应答码.....	9
4. 补充内容（for Nordic）.....	9

## 修订表

[illegible]

# 审批记录

版本	审批人	审批意见	审批日期
V3.4		修改 A0 指令	2017.12.01

## 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 0x51 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 0x12+ 软件版本号 0x67, 起始版本 0x1166, 每改动一个版本+1
锁状态	1	0: 锁关闭 1: 锁打开
租车序列号	16	加密之前的原文, 传长度为 16 的随机字符串
电池电压	2	整型, 330 即 3.30v, 低位在前
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---63 (秘钥长度-16-1)

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	网络传输秘钥索引=实际秘钥索引+128
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	锁位置纬度
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

设备软件重启---维护 app 使用, 重启成功蜂鸣器会响一下, 电机能动。

app->lock, 指令码: 0x89

字段	长度	描述
约定字符	1	0xf0

## 0x8D 蜂鸣器长叫

使蜂鸣器长叫, 响 10s 自动停止。

app->lock, 指令码: 0x8D

字段	长度	描述
随机数	4	无
约定字符	1	0xf2

lock-&gt;app, 指令码: 0x5D

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-&gt;lock, 指令码: 0x90

字段	长度	描述
无	0	无

lock-&gt;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-&gt;lock, 指令码: 0x93

字段	长度	描述
无	0	无

lock-&gt;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(20171118 保留暂不使用)**

app-&gt;lock, 指令码: 0x94

字段	长度	描述
校准状态	1	

lock-&gt;app, 指令码: 0x54

字段	长度	描述
校准状态	1	0x00: 陀螺仪校准完成 0x01: 陀螺仪校准未完成

**0x99 激活网络（GPRS） 功能**

（维护 APP 指令，锁 GPRS 关机的情况下，通过此指令开机或激活上网功能（某些运营商 SIM 卡过测试期后第一次上网开始计费））

app-&gt;lock, 指令码: 0x99

字段	长度	描述
无	0	无

lock-&gt;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

**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-&gt;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-&gt;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

**0xA0 锁的生产 APP 获取硬件初始数据**

(锁生产 APP 使用, 20171113 更新)

app->lock, 指令码: 0xA0

字段	长度	描述

lock->app, 指令码: 0x60 (必须在收到 0x81 指令后再收到 0xA0 指令才会返回)

返回加密秘钥: 原始秘钥异或一个固定的 value 值(value 根据不同的厂商定不同)得到加密后的秘钥, 传给后台。

目前 value = "mintbike"

返回加密 CheckInKey : CheckInKey 和固定的 value 异或加密后得到的值, 传给后台。

举例:

原始秘钥: "12345678 90123456 78901234 56789012 34567890 12345678 90123456 78901234 56789012 34567890"

Value: "20171201"

加密秘钥 = { "12345678 " ^ "20171201"  
 "90123456 " ^ "20171201"  
 "78901234 " ^ "20171201"  
 "56789012 " ^ "20171201"  
 "34567890 " ^ "20171201"  
 "12345678 " ^ "20171201"  
 "90123456 " ^ "20171201"  
 "78901234 " ^ "20171201"  
 "56789012 " ^ "20171201"  
 "34567890 " ^ "20171201" }

原始 CheckInKey : "12345678"

Value: "20171201"

加密 CheckInKey = { "12345678 " ^ "20171201" }

字段	长度	描述
加密秘钥	80	返回原始 80 个字符的字符串秘钥异或 value 后的值
Mac 地址	6	6byte 唯一物理地址
加密 CheckInKey	8	锁在 80 位秘钥内随机生成的 8 个字符的字符串异或 value 后的值

0xA1 控制器透传命令 预留 (20171120)

app->lock, 指令码: 0XA1

字段	长度	描述
蓝牙返回		蓝牙返回控制原始数据 预留

lock-&gt;app, 指令码: 0x61

字段	长度	描述
控制器发送		控制器发送原始数据 预留

0xA2 控制器透传命令 预留 (20171120)

app-&gt;lock, 指令码: 0xA2

字段	长度	描述
蓝牙返回		蓝牙返回控制原始数据 预留

lock-&gt;app, 指令码: 0x62

字段	长度	描述
控制器发送		控制器发送原始数据 预留

0xA3 控制器透传命令 预留 (20171120)

app-&gt;lock, 指令码: 0xA3

字段	长度	描述
蓝牙返回		蓝牙返回控制原始数据 预留

lock-&gt;app, 指令码: 0x63

字段	长度	描述
控制器发送		控制器发送原始数据 预留

0xA4 关闭网络模块 (GPRS) 功能

(锁生产或维护 APP 指令, 锁 GPRS 开机的情况下, 通过此指令关机 (锁生产时测试完毕可用 APP 通过此指令或后台批量关机))

app-&gt;lock, 指令码: 0x99

字段	长度	描述
无	0	无

lock-&gt;app, 指令码: 0x64

字段	长度	描述
激活状态	1	0x00: 关机成功 0x01: 已关机 0x02: 关机失败

### 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 个字节 0x00，一共 20 个字节），所有 app 连接成功后都要发送这个指令。  
所有控制器数据，手机 APP 网络以及蓝牙通道正常的情况下，**优先走蓝牙通道**。