

---

# 摩亨电助力智能锁

## 网络通讯协议规范

### V1.6.6

文档作者：

日期：

审核者：

日期：

文档管理员：

日期：

技术总监：

日期：

上海摩亨网络科技有限公司

版权所有 不得复制

## 版 本 历 史

| 版本号    | 修改人 | 修改内容 | 时间         |
|--------|-----|------|------------|
| V1.6.6 |     | 加密方式 | 2017.12.01 |

DRAFT

## 目 录

|                            |    |
|----------------------------|----|
| 1. 引言 .....                | 5  |
| 1.1 目的 .....               | 5  |
| 1.2 范围 .....               | 5  |
| 1.3 目标读者 .....             | 5  |
| 1.4 概要介绍 .....             | 5  |
| 1.5 术语 .....               | 5  |
| 1.6 参考资料 .....             | 5  |
| 2. 协议格式 .....              | 6  |
| 2.1 业务交互协议格式 .....         | 6  |
| 2.2 业务流程 .....             | 6  |
| 3. 协议内容 .....              | 7  |
| 3.1 智能锁登陆 .....            | 7  |
| 3.1.1 请求数据 .....           | 7  |
| 3.1.2 应答数据 .....           | 7  |
| 3.2 远程开锁 .....             | 8  |
| 3.2.1 请求数据 .....           | 8  |
| 3.2.2 应答数据 .....           | 8  |
| 3.3 状态上报 .....             | 9  |
| 3.3.1 请求数据 .....           | 9  |
| 3.3.2 应答数据 .....           | 10 |
| 3.4 锁固件升级指令 .....          | 10 |
| 3.4.1 请求数据 .....           | 10 |
| 3.4.2 应答数据 .....           | 11 |
| 3.5 设置/获取配置参数 .....        | 11 |
| 3.5.1 请求数据 .....           | 11 |
| 3.5.2 应答数据 .....           | 12 |
| 3.6 心率包 .....              | 13 |
| 3.7 控制器读取开关锁命令(透传) .....   | 13 |
| 3.7.1 请求数据 .....           | 13 |
| 3.8 控制器状态发送命令(透传) .....    | 13 |
| 3.8.1 发送数据 .....           | 13 |
| 3.8.1 应答数据 .....           | 13 |
| 3.9 BMS 状态发送命令 (透传) .....  | 13 |
| 3.9.1 发送数据 .....           | 13 |
| 3.9.2 应答数据 .....           | 13 |
| 3.10 BMS 及蓝牙锁查询 (透传) ..... | 14 |

|                          |    |
|--------------------------|----|
| 3.10.1 发送数据.....         | 14 |
| 3.10.1 应答数据.....         | 14 |
| 3.11 控制器固件升级锁指令 .....    | 14 |
| 3.11.1 发送数据.....         | 14 |
| 3.12 控制器固件升级指令(透传).....  | 14 |
| 3.12.1 发送数据.....         | 14 |
| 3.12.1 应答数据.....         | 14 |
| 3.13 控制器指令（透传）(预留).....  | 15 |
| 3.13.1 发送数据.....         | 15 |
| 3.13.2 应答数据.....         | 15 |
| 3.14 控制器指令（透传）(预留).....  | 15 |
| 3.14.1 发送数据.....         | 15 |
| 3.14.2 应答数据.....         | 15 |
| 3.15 控制器指令（透传）(预留).....  | 15 |
| 3.15.1 发送数据.....         | 15 |
| 3.15.2 应答数据.....         | 15 |
| 3.16 网络模块（GPRS）关机指令..... | 15 |
| 3.16.1 发送数据.....         | 15 |
| 3.16.2 应答数据.....         | 16 |
| 附录:应答码定义 .....           | 16 |

## 1. 引言

### 1.1 目的

本文档主要针对后台开发人员，让后台开发人员了解智能锁的基本工作原理，实现智能锁的打开，获取开锁、上锁信息，锁的电量，车辆位置信息等。

### 1.2 范围

GPRS 智能锁与服务器间通信

### 1.3 目标读者

GPRS 智能锁嵌入式开发和服务器端开发人员

### 1.4 概要介绍

### 1.5 术语

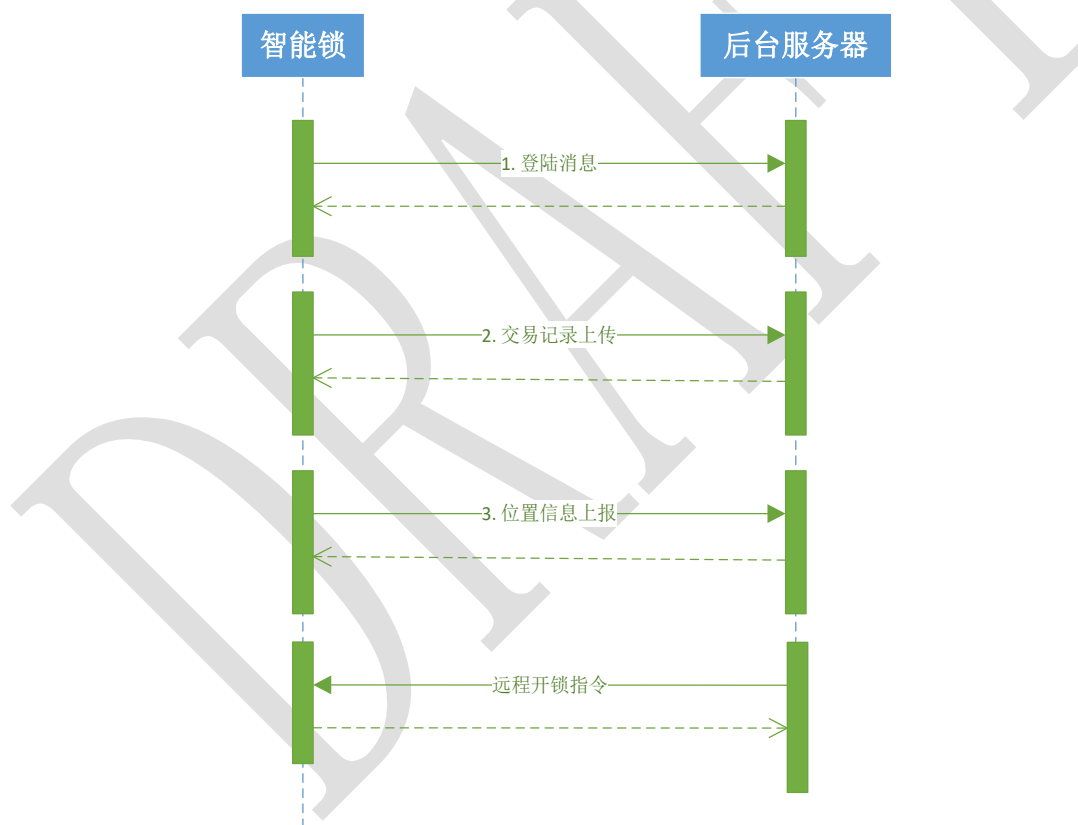
### 1.6 参考资料

## 2. 协议格式

### 2.1 业务交互协议格式

- ◆ 原始业务数据采用文本格式，每条业务数据分两行：  
    第一行： 业务类型 + 消息 ID  
    第二行： 业务数据
- ◆ 采用请求-应答形式通信,应答消息 ID 需要和请求消息 ID 一致,每次请求-应答使用唯一的消息 ID
- ◆ 秘钥生成规则:前 6 位 MAC 地址+68 位随机(大写字母+小写字母+数字)字符+后 6 位 MAC 地址

### 2.2 业务流程



### 3. 协议内容

#### 3.1 智能锁登陆

##### 3.1.1 请求数据

◆ 格式

LOGIN <MsgId>\r\n  
<DeviceId> <EncryptData> <Index> <IMEI> <控制器序列> <BMS 序列号>  
<VerionCode>  
\r\n

◆ 字段说明

<MsgId>

请求消息 ID, 标识一次请求应答

<DeviceId>

设备唯一 ID,6 个字节 mac 地址转化的 12 个字节字符串;

设备 ID 为 D43639B816C8 则 mac 地址为 D4:36:39:B8:16:C8;

<EncryptData>

原始数据使用 AES(ECB 模式)加密后产生的加密数据;

原始数据为 12 个字节设备 ID 加上 4 个字节的字符 0 组成的 16 字节字符串, 比如设备 ID 是 D43639B816C8 加密原始数据为 D43639B816C8000

<Index>

密钥索引

<IMEI>

设备中 SIM 卡的唯一身份码

版本号

<控制器序列>

<BMS 序列号>

<VerionCode>

◆ 示例

LOGIN 0  
D43639B816C8 400A442135D1F2723A7E841AEC92A02D 16 866873020454024  
99999999999999999999999999999999 77777777777777777777777777777777 9

注意:字段之间使用一个空格分离

##### 3.1.2 应答数据

◆ 格式

LOGIN <MsgId>\r\n

<ResCode> OK\r\n

◆ 字段说明

<MsgId>

应答消息 ID,需要和请求消息 ID 一致

<ResCode>

应答码, 见应答码定义

◆ 示例

LOGIN 0

0 OK

## 3.2 远程开锁

### 3.2.1 请求数据

◆ 格式

OPEN <MsgId>\r\n

<Date>,<UserID>,<TradeNo>,<EncryptData>,< IndexKey>\r\n

◆ 字段说明

<MsgId>

请求消息 ID, 标识一次请求应答

<Date>

交易记录产生时间, 10 位时间戳 (20 秒不开锁待定)

<UserID>

用户 ID

<TradeNo>

交易序列号

<EncryptData>

原始数据和秘钥索引指向的秘钥 AES(ECB)加密产生的加密数据;

原始数据为 6 字节 mac 地址+8 字节 CheckInKey+2 字节字符 0;

设备秘钥信息和 CheckInKey 在设备出厂时配置;

<IndexKey>

设备秘钥索引

### 3.2.2 应答数据

◆ 格式

OPEN <MsgId>\r\n

<ResCode> OK\r\n

◆ 字段说明

<MsgId>

应答消息 ID, 需要和请求消息 ID 一致



<ResCode>

应答码，见应答码定义

### 3.3 状态上报

#### 3.3.1 请求数据

##### ◆ 格式

REPORT <MsgId>\r\n

<TradeDate>,<UserId>,<TradeNo>,<TradeType>,<EncryptData>,<IndexKey>,<Longitude>,<Latitude>,<LocationType>,<Vibrate>\r\n

##### ◆ 字段说明

<MsgId>

请求消息 ID，标识一次请求应答

<TradeDate>

交易记录产生时间戳 10 位，开锁时传的

<UserId>

用户 ID

<TradeNo>

交易序列号

<TradeType>

0 蓝牙记录

~~1 还车记录[废弃]~~

2 刷卡租车记录

3 远程开锁租车记录

<EncryptData>

原始数据和密钥索引指向的密钥 AES(ECB)加密产生的加密数据；

原始数据为 6 字节 mac 地址+8 字节 CheckInKey+2 字节字符 0；

设备密钥信息和 CheckInKey 在设备出厂时配置

<IndexKey>

设备密钥索引

<Longitude>

经度，格式 ddd.mmmmm,如: 116.33533

<Latitude>

纬度，格式 dd.mmmmm,如: 39.20567

<LocationType>

坐标类型

1 GPS 定位坐标

2 基站辅助定位坐标

<Vibrate>

是否是震动产生的坐标

0 否 1 是

### 3.3.2 应答数据

- ◆ 格式

REPORT <MsgId>\r\n

<Type>,<ResCode> OK\r\n

- ◆ 字段说明

<MsgId>

应答消息 ID,需要和请求消息 ID 一致

<Type>

0: 控制器状态

<ResCode>

应答码, 见应答码定义

### 3.4 锁固件升级指令

#### 3.4.1 请求数据

- ◆ 格式

UPGRADE <MsgId>\r\n

<Version>,<CustomerID>,<Host>,<port>,<path>,<apn>\r\n

- ◆ 字段说明

<MsgId>

请求消息 ID, 标识一次请求

<Version>

新固件的版本号, 如 2.0.0

<CustomerID>

客户编号

<Host>

服务器 IP(或域名) 例如 api.mintbike.com

<port>

端口地址 例如 8082

<path>

升级文件路径 例如 /1152.bin

<apn>

CMNET

### 3.4.2 应答数据

#### ◆ 格式

UPGRADE <MsgId>\r\n

<ResCode> OK\r\n

#### ◆ 字段说明

<MsgId>

应答消息 ID,需要和请求消息 ID 一致

<ResCode>

应答码, 见应答码定义

### 3.5 设置/获取配置参数

#### 3.5.1 请求数据

#### ◆ 格式

CONFIG <MsgId>\r\n

<pingperiod>,<gpsperiod>,<bVibrate>,<bSMS>,<IP>,<PORT>,<EncryptData>,<IndexKey>,<reserver1>,<reserver2>,<reserver3>,<reserver4>,<reserver5>,<reserver6>\r\n

#### ◆ 字段说明

<ping period>

保活周期, 单位秒, 默认: 50

<gps period>

Gps 定位周期, 单位 h, 默认: 4h

<bVibrate>

震动检测使能, 1 启用, 0 禁用, 默认: 启用

<bSMS>

短信功能使能, 1 启用, 0 禁用, 默认: 禁用

<IP>

“IP 地址”

<PORT>

IP 端口

<alive>

是否保持长连接 1 是, 0 否

<pinlv>

传输间隔时间 小时单位 正整数

<contrlbotelv>

控制器波特率设置 eg: 9600

#### <EncryptData>

原始数据和密钥索引指向的密钥 AES(ECB)加密产生的加密数据;  
原始数据为 6 字节 mac 地址+8 字节 CheckInKey+2 字节字符 0;  
设备密钥信息和 CheckInKey 在设备出厂时配置;

#### <IndexKey>

设备密钥索引

#### <reserver1>

#### <reserver2>

#### <reserver3>

#### <reserver4>

#### <reserver5>

#### <reserver6>

预留参数, 默认为 0

### 3.5.2 应答数据

#### ◆ 格式

CONFIG <MsgId>\r\n

<pingperiod>,<gpsperiod>,<bVibrate>,<bSMS>,<IP>,<PORT>,<EncryptData>,<IndexKey>\r\n

#### ◆ 字段说明

##### <MsgId>

应答消息 ID,需要和请求消息 ID 一致

##### <ResCode>

#### ◆ 字段说明

##### <ping period>

保活周期, 单位秒, 默认: 50

##### <gps period>

Gps 定位周期, 单位 h, 默认: 4h

##### <bVibrate>

震动检测使能, 1 启用, 0 禁用, 默认: 启用

##### <bSMS>

短信功能使能, 1 启用, 0 禁用, 默认: 禁用

##### <IP>

“IP 地址”

##### <PORT>

IP 端口

### 3.6 心率包

◆ 格式

BREATH <MsgId>\r\n

### 3.7 控制器读取开关锁命令(透传)

#### 3.7.1 请求数据

◆ 格式

CONTROL1 <MsgId>\r\n

<return\_rowdata>\r\n

Rowdata: 控制器协议 0x10 蓝牙锁返回

#### 3.7.2 应答数据

◆ 格式

CONTROL1 <MsgId>\r\n

<return\_rowdata>\r\n

Rowdata: 控制器协议 0x10 控制器协议

### 3.8 控制器状态发送命令(透传)

#### 3.8.1 发送数据

◆ 格式

CONTROL2<MsgId>\r\n

<rowdata>\r\n

Rowdata: 控制器协议 0x11 蓝牙锁返回

#### 3.8.1 应答数据

◆ 格式

CONTROL2 <MsgId>\r\n

<return\_rowdata>\r\n

Rowdata: 控制器协议 0x11

### 3.9 BMS 状态发送命令 (透传)

#### 3.9.1 发送数据

CONTROL3<MsgId>\r\n

<rowdata>\r\n

Rowdata: 控制器协议 0x12 蓝牙锁返回

#### 3.9.2 应答数据

◆ 格式

CONTROL3<MsgId>\r\n  
<return\_rowdata>\r\n  
Rowdata: 控制器协议 0x12

### 3.10 BMS 及蓝牙锁查询 (透传)

#### 3.10.1 发送数据

◆ 格式

CONTROL4<MsgId>\n  
<rowdata>\r\n  
RowData: 控制器协议 0x14 蓝牙锁返回

#### 3.10.1 应答数据

◆ 格式

CONTROL4 <MsgId>\r\n  
<return\_rowdata>\r\n  
Rowdata: 控制器协议 0x14

### 3.11 控制器固件升级锁指令

#### 3.11.1 发送数据

◆ 格式

CONTROL5 <MsgId>\n  
<state>,<contrlbotelv>\r\n  
state: 1 开始升级（锁设置波特率 19200，锁给控制器断电再上电） 2 升级结束  
（锁给控制器断电，锁设置波特率为 4800）。  
Contrlbotelv,控制器波特率设置 eg: 19200 or 4800

后台要判断控制器在未使用（关锁）的情况下，并且软件版本不是最新的情况下才能下发升级指令。

### 3.12 控制器固件升级指令(透传)

#### 3.12.1 发送数据

◆ 格式

CONTROL6<MsgId>\r\n  
<rowdata>\r\n  
RowData: 控制器 OTA 升级协议，第一次 ROWdata 为空，，服务器收到 FC 后，开始执行 OTA 升级。

#### 3.12.1 应答数据

◆ 格式

CONTRL6 <MsgId>\r\n

<return\_rowdata>\r\n

Rowdata: 控制器 OTA 升级协议

### 3.13 控制器指令（透传）(预留)

#### 3.13.1 发送数据

◆ 格式

CONTROL7<MsgId>\r\n

<rowdata>\r\n

#### 3.13.2 应答数据

◆ 格式

CONTRL7 <MsgId>\r\n

<return\_rowdata>\r\n

### 3.14 控制器指令（透传）(预留)

#### 3.14.1 发送数据

◆ 格式

CONTROL8<MsgId>\r\n

<rowdata>\r\n

#### 3.14.2 应答数据

◆ 格式

CONTRL8 <MsgId>\r\n

<return\_rowdata>\r\n

### 3.15 控制器指令（透传）(预留)

#### 3.15.1 发送数据

◆ 格式

CONTROL9<MsgId>\r\n

<rowdata>\r\n

#### 3.15.2 应答数据

◆ 格式

CONTRL9 <MsgId>\r\n

<return\_rowdata>\r\n

### 3.16 网络模块（GPRS）关机指令

#### 3.16.1 发送数据

◆ 格式

POWERDOWN <MsgId>\r\n

<rowdata>\r\n

RowData: POWERDOWN

### 3.16.2 应答数据

#### ◆ 格式

POWERDOWN <MsgId>\r\n

<return\_rowdata>\r\n

Rowdata: POWERDOWN

锁先返回 Rowdata 以后再关机，服务器判断设备此时离线则默认关机成功。

## 附录:应答码定义

- |   |          |
|---|----------|
| 0 | 成功       |
| 1 | 格式错误     |
| 2 | 设备不存在    |
| 3 | 加密数据验证失败 |
| 4 | 数据空      |
| 5 | 非新固件版本   |
| 6 | 加密验证错误   |