

共享单车锁 808 通讯协议

V0. 1

深圳奇新智能技术有限公司

二〇一七年八月

目录

一、	范围	5
二、	规范性引用文件.....	5
三、	术语和定义、缩略语	5
3.1	术语和定义.....	5
3.1.1	数据通信链路异常	5
3.1.2	注册	5
3.1.3	鉴权	5
3.1.4	位置汇报策略.....	5
3.1.5	警报	5
3.2	缩略语	6
四、	协议基础.....	6
4.1	通信方式.....	6
4.2	数据类型.....	6
4.3	传输规则.....	7
4.4	消息的组成	7
4.4.1	消息结构.....	7
4.4.2	标识位.....	7
4.4.3	消息头.....	7
4.4.4	校验码.....	8
五、	通信连接	8
5.1	连接的建立.....	8
5.2	连接的维持.....	8
5.3	连接的断开.....	8
六、	消息处理	9
6.1	平台主发的消息.....	9
6.2	终端主发的消息.....	9
6.1.1	数据通信链路正常	9
6.1.2	数据通信链路异常	9

七、	协议分类.....	10
7.1	概述.....	10
7.2	终端管理类协议.....	10
7.2.1	终端注册.....	10
7.2.2	终端鉴权.....	10
7.2.3	设置/查询终端参数.....	10
7.2.4	终端控制.....	10
7.3	位置、报警类协议.....	10
7.3.1	位置信息汇报.....	10
7.3.2	位置信息查询.....	10
7.3.3	终端报警.....	10
7.3	车辆控制类协议.....	11
7.4	加密类协议.....	11
八、	数据格式.....	11
8.1	终端通用应答.....	11
8.2	平台通用应答.....	11
8.3	终端心跳.....	12
8.4	终端注册.....	12
8.5	终端注册应答.....	13
8.6	终端鉴权.....	13
8.7	终端鉴权应答.....	13
8.8	设置终端参数.....	14
8.9	查询终端参数.....	14
8.10	查询终端参数应答.....	14
8.11	终端控制.....	15
8.12	查询终端属性.....	15
8.13	查询终端属性应答.....	15
8.14	下发终端升级包.....	16
8.15	终端升级结果通知.....	16
8.16	位置信息汇报.....	16

8.17 位置信息查询.....	18
8.18 位置信息查询应答.....	18
8.19 车辆控制	19
8.20 车辆控制应答.....	19
8.21 平台 RSA 公钥.....	20
8.22 终端 RSA 公钥.....	20
附 录.....	21

一、 范围

本协议规定了共享单车锁终端（以下简称终端）与服务器平台（以下简称平台）之间的通讯协议与数据格式，包括协议基础、通讯连接、消息处理、协议分类与说明及数据格式。

本协议适用于共享单车锁 808 协议终端和平台之间的通讯。

二、 规范性引用文件

《道路运输车辆卫星定位系统北斗兼容车载终端通讯协议技术规范》

三、 术语和定义、缩略语

3.1 术语和定义

3.1.1 数据通信链路异常

abnormal data communication link

无线通信链路断开

3.1.2 注册

register

终端向平台发送消息告知当前终端的所有硬件信息。

3.1.3 鉴权

Authentication

终端连接上平台时向平台发送消息以使平台验证自己身份，即请求长连接。

3.1.4 位置汇报策略

location reporting strategy

定时上报、开关锁位置汇报。

3.1.5 警报

Warning

警报分为低电量警报、移动警报、撞击警报、故障警报。

3.2 缩略语

GSM-- Global System for Mobile Communication（全球移动通信系统）

GPRS --- General Packet Radio Service（通用分组无线服务技术）

SOCKET --- 套接字

GPS --- Global Positioning System（全球定位系统）

AGPS --- Assisted Global Positioning System（辅助全球卫星定位系统）

LBS --- 基于基站信息的位置服务

GSENSOR --- Gravity-sensor（重力传感器）

APN --- access point name (接入点名称)

RSA --- 一种非对称密码算法（由 Ron Rivest、Adi Shamir、Len Adleman 开发，取名来自三者的名字）

TCP/IP --- 传输控制协议(transmission control protocol)

四、 协议基础

4.1 通信方式

通信协议采用 TCP 作为唯一控制协议，使用 socket 封装内容，走 GPRS 链路通讯，平台作为服务器端，终端作为客户端。

4.2 数据类型

协议消息中使用的数据类型见 表 1：

数据类型	描述及要求
BYTE	无符号单字节整型（字节，8 位）
WORD	无符号双字节整型（字，16 位）
DWORD	无符号四字节整型（双字，32 位）
BYTE[n]	n 字节
BCD[n]	8421 码，n 字节
STRING	GBK 编码，若无数据，置空

表 1 数据类型

4.3 传输规则

协议采用大端模式的网络字节序来传递字和双字。

约定如下：

- 字节(BYTE)的传输约定：按照字节流的方式传输；
- 字(WORD)的传输约定：先传递高八位，再传递低八位；
- 双字(DWORD)的传输约定：先传递高 24 位，然后传递高 16 位，再传递高 8 位，最后传递低 8 位。

4.4 消息的组成

4.4.1 消息结构

每条消息由标识位、消息头、消息体和校验码组成，消息结构如表 1 所示：

标识位	消息头	消息体	校验码	标识位
-----	-----	-----	-----	-----

表 1 消息结构

4.4.2 标识位

采用 0x7e 表示，若校验码、消息头以及消息体中出现 0x7e，则要进行转义处理，转义规则定义如下：

0x7e <-----> 0x7d 后紧跟一个 0x02；

0x7d <-----> 0x7d 后紧跟一个 0x01。

转义处理过程如下：

发送消息时：消息封装——>计算并填充校验码——>转义；

接收消息时：转义还原——>验证校验码——>解析消息。

示例：

发送一包内容为 0x30 0x7e 0x08 0x7d 0x55 的数据包，则经过封装如下：

0x7e 0x30 0x7d 0x02 0x08 0x7d 0x01 0x55 0x7e

4.4.3 消息头

消息头内容详见 表 2：

起始字节	字段	数据类型	描述及要求
0	消息 ID	WORD	
2	消息体属性	WORD	消息体属性格式结构图见表 3

4	终端 ID	BCD[6]	单车锁编号
10	消息流水号	WORD	按发送顺序从 0 开始循环累加

表 2 消息头内容

消息体属性格式结构如表 3 所示：

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
保留			数据加密方式			消息体长度									

表 3 消息体属性格式结构

数据加密方式：

- bit10~bit12 为数据加密标识位；
- 当此三位都为 0，表示消息体不加密；
- 当第 10 位为 1，表示消息体经过 RSA 算法加密；

4.4.4 校验码

校验码指从消息头开始，同后一字节异或，直到校验码前一个字节，占用一个字节。

五、通信连接

5.1 连接的建立

终端与平台的数据日常连接采用 TCP 方式，终端复位后应尽快与平台建立连接，连接建立后立即向平台发送终端鉴权消息进行鉴权，鉴权成功即终端与平台建立起了长连接。

5.2 连接的维持

连接建立和终端鉴权成功后，在没有正常数据包传输的情况下，终端应周期性向平台发送终端心跳消息，平台收到后向终端发送平台通用应答消息，发送周期由终端参数指定。

5.3 连接的断开

平台和终端均可根据 TCP 协议主动断开连接，双方都应主动判断 TCP 连接是否断开。

平台判断 TCP 连接断开的方法：

- 根据 TCP 协议判断出终端主动断开；
- 相同身份的终端建立新连接，表明原连接已断开；
- 在一定的时间内未收到终端发出的消息，如终端心跳。

终端判断 TCP 连接断开的方法：

- 根据 TCP 协议判断出平台主动断开；
- 数据通信链路断开；
- 数据通信链路正常，达到重传次数后仍未收到应答。

六、 消息处理

6.1 平台主发的消息

所有平台主发的消息均要求终端应答，应答分为通用应答和专门应答，由各具体功能协议决定。发送方等待应答超时后，应对消息进行重发。应答超时时间和重传次数由平台参数指定，每次重传后的应答超时时间的计算公式见式(1)：

$$T_{N+1}=T_N \times (N+1) \dots\dots\dots (1)$$

式中：

T_{N+1} ——每次重传后的应答超时时间；

T_N ——前一次的应答超时时间；

N ——重传次数。

6.2 终端主发的消息

6.1.1 数据通信链路正常

数据通信链路正常时，所有终端主发的消息均要求平台应答，应答分为通用应答和专门应答，由各具体功能协议决定。终端等待应答超时后，应对消息进行重发。应答超时时间和重传次数由终端参数指定，每次重传后的应答超时时间按式（1）进行计算。对于终端发送的关键报警消息，若达到重传次数后仍未收到应答，则应对其进行保存。以后在发送其它消息前要先发送保存的关键报警消息。

6.1.2 数据通信链路异常

数据通信链路异常时，终端应对需发送的位置信息汇报消息进行保存。在数据通信链路恢复正常后，立即发送保存的消息。

七、协议分类

7.1 概述

以下按功能分类对协议进行描述。均采用 TCP 通信方式。协议中消息名称与消息 ID 的消息对照表见附录。

7.2 终端管理类协议

7.2.1 终端注册

终端在未注册状态下，应首先进行注册，注册成功后终端将获得鉴权码并进行保存，鉴权码在终端登录时使用。

7.2.2 终端鉴权

终端注册后每次在与平台建立连接后，应立即进行鉴权。鉴权成功前终端不得发送其它消息。终端通过发送终端鉴权消息进行鉴权，平台回复鉴权结果，其中附带当前时间信息，终端进行时间校准。

7.2.3 设置/查询终端参数

平台通过发送设置终端参数消息设置终端参数，终端回复终端通用应答消息。平台通过发送查询终端参数消息查询终端参数，终端回复查询终端参数应答消息。不同网络制式下的终端应支持各自网络的一些特有参数。

7.2.4 终端控制

平台通过发送终端控制消息对终端进行控制，终端回复终端通用应答消息。

7.3 位置、报警类协议

7.3.1 位置信息汇报

终端根据参数设定周期性发送位置信息汇报消息。

7.3.2 位置信息查询

平台通过发送位置信息查询消息，查询指定车载终端当时位置信息，终端回复位置信息查询应答消息。

7.3.3 终端报警

终端判断满足报警条件时发送位置信息汇报消息，在位置汇报消息中设置相应的报警标志，平台可通过回复平台通用应答消息进行报警处理。

各报警类型见位置信息汇报消息体中的描述。

7.3 车辆控制类协议

平台通过发送车辆控制消息，要求终端按指定的操作对车辆进行控制。终端收到后立即回复终端通用应答消息。之后终端对车辆进行控制，根据结果再回复车辆控制应答消息。控制协议中附带时间信息，终端需要根据此时间来判断控制指令的时效性。

7.4 加密类协议

平台与终端之间若需加密通信，可采用 RSA 公钥密码系统。平台通过发送平台 RSA 公钥消息向终端告知自己的 RSA 公钥，终端回复终端 RSA 公钥消息，反之亦然。

八、数据格式

8.1 终端通用应答

消息 ID: **0x0001**

终端通用应答消息体数据格式见 表 4。

起始字节	字段	数据类型	描述及要求
0	应答流水号	WORD	对应的平台消息的流水号
2	应答 ID	WORD	对应的平台消息的 ID
4	结果	BYTE	0: 成功/确认; 1: 失败; 2: 消息有误; 3: 不支持

表 4 终端通用应答消息体数据格式

8.2 平台通用应答

消息 ID: **0x8001**

平台通用应答消息体数据格式见 表 5。

起始字节	字段	数据类型	描述及要求
0	应答流水号	WORD	对应的终端消息的流水号
2	应答 ID	WORD	对应的终端消息的 ID
4	结果	BYTE	0: 成功/确认; 1: 失败; 2: 消息有误; 3: 不支持; 4: 报警处理确认;

表 5 平台通用应答消息体数据格式

8.3 终端心跳

消息 ID: **0x0002**

终端心跳数据消息体为空。

8.4 终端注册

消息 ID: **0x0100**

终端注册消息体数据格式见表 6。

起始字节	字段	数据类型	描述及要求
0	制造商 ID	BYTE[10]	10 个字节，终端制造商编码
10	终端型号	BYTE[10]	10 个字节，此终端型号由制造商自行定义，位数不足时，后补“0X00”。
20	终端 ID	BCD[10]	10 个字节的 BCD 码，此终端 ID 由制造商自行定义，位数不足时，后补“0X00”。
30	蓝牙 MAC 地址	BYTE[6]	蓝牙的物理地址（如：0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF）
36	ICCID	BCD[10]	SIM 卡的 ICCID 码，（如：0x89, 0x85, 0x20, 0x30, 0x01, 0x00, 0x78, 0x82, 0x54, 0x8f）
46	GNSS 模块属性	BYTE	bit0, 0: 不支持 GPS 定位, 1: 支持 GPS 定位; bit1, 0: 不支持北斗定位, 1: 支持北斗定位; bit2, 0: 不支持 GLONASS 定位, 1: 支持 GLONASS 定位; bit3, 0: 不支持 Galileo 定位, 1: 支持 Galileo 定位。
47	通信模块属性	BYTE	bit0, 0: 不支持 GPRS 通信, 1: 支持 GPRS 通信; bit1, 0: 不支持 CDMA 通信, 1: 支持 CDMA 通信; bit2, 0: 不支持 TD-SCDMA 通信, 1: 支持 TD-SCDMA 通信; bit3, 0: 不支持 WCDMA 通信, 1: 支持 WCDMA 通信; bit4, 0: 不支持 CDMA2000 通信, 1: 支持 CDMA2000 通信。 bit5, 0: 不支持 TD-LTE 通信, 1: 支持 TD-LTE 通信; bit7, 0: 不支持其他通信方式, 1: 支持其他通信方式。
48	终端硬件版本号	BYTE[n]	第 1 位表示长度，后面 n-1 位是实际字符串数据（如：HW_V0.1 = 0x07 , 0x48, 0x57, 0x5F, 0x56, 0x30, 0x2E, 0x31）
48+n	终端 GSM 固件版本号	BYTE[n]	同上
48+n+n	终端蓝牙固件版本号	BYTE[n]	同上

表 6 终端注册消息体数据格式

8.5 终端注册应答

消息 ID: **0x8100**

终端注册应答消息体数据格式见表 7。

起始字节	字段	数据类型	描述及要求
0	应答流水号	WORD	对应的终端注册消息的流水号
2	结果	BYTE	0: 成功; 1: 车辆已被注册; 2: 数据库中无该车辆; 3: 终端已被注册; 4: 数据库中无该终端
3	鉴权码	STRING	只有在成功后才有该字段

表 7 终端注册应答消息体数据格式

8.6 终端鉴权

消息 ID: **0x0102**

终端鉴权消息体数据格式见表 8。

起始字节	字段	数据类型	描述及要求
0	鉴权码	STRING	终端重连后上报鉴权码

表 8 终端鉴权消息体数据格式

8.7 终端鉴权应答

消息 ID: **0x8102**

终端鉴权结果消息体数据格式见表 9。

起始字节	字段	数据类型	描述及要求
0	应答流水号	WORD	对应的终端消息的流水号
2	应答 ID	WORD	对应的终端消息的 ID
4	结果	BYTE	0: 成功/确认; 1: 失败; 2: 禁止鉴权;
5	时间	BCD[6]	YY-MM-DD-hh-mm-ss
11	时区	STRING	+0800 (+为东经, -为西经, 08 为小时, 00 为分钟) (国内默认为 GMT+8 时间, 本标准中之后涉及的时间均采用此时区)

表 9 终端鉴权应答消息体数据格式

注: 当终端收到结果为“禁止鉴权”时, 应当停止后续鉴权操作。

8.8 设置终端参数

消息 ID: **0x8103**

设置终端参数消息体数据格式见表 10。

起始字节	字段	数据类型	描述及要求
0	参数总数	BYTE	
1	参数项列表		参数项格式见 表 11

表 10 终端参数消息体数据格式

字段	数据类型	描述及要求
参数 ID	WORD	参数 ID 定义及说明见 表 12
参数长度	BYTE	
参数值		

表 11 终端参数项数据格式

参数 ID	数据类型	描述及要求
0x0001	DWORD	终端心跳发送间隔, 单位为秒 (S)
0x0003	DWORD	消息重传次数
0x0013	STRING	主服务器地址, IP 或域名
0x0018	DWORD	服务器端口
0x0029	DWORD	缺省时间汇报间隔, 单位为秒 (S), >0

表 12 终端参数设置各参数项定义及说明

8.9 查询终端参数

消息 ID: **0x8104**

查询终端参数消息体为空。

8.10 查询终端参数应答

消息 ID: **0x0104**

查询终端参数应答消息体数据格式见表 13。

起始字节	字段	数据类型	描述及要求
0	应答流水号	WORD	对应的终端参数查询消息的流水号
2	应答参数个数	BYTE	
3	参数项列表		参数项格式和定义见表 11

表 13 查询终端参数应答消息体数据格式

8.11 终端控制

消息 ID: **0x8105**

终端控制消息体数据格式见表 14。

起始字节	字段	数据类型	描述及要求
0	命令字	BYTE	终端控制命令字说明见表 15
1	命令参数	BYTE	见表 14

表 14 终端控制消息体数据格式

命令字	命令参数	描述及要求
3	0	终端关机
4	0	终端复位
5	0	终端恢复出厂设置
6	0	关闭数据通信
7	0	0:退出运输模式。1: 进入运输模式（锁在关锁状态下，会自动开锁，并进入运输模式。手动关锁后自动退出运输模式）

表 15 终端控制命令字说明

8.12 查询终端属性

消息 ID: **0x8107**

查询终端属性消息体为空。

8.13 查询终端属性应答

消息 ID: **0x0107**

查询终端属性应答消息体数据格式见表 16。

起始字节	字段	数据类型	描述及要求
------	----	------	-------

0	应答流水号	WORD	对应的终端属性查询消息的流水号
2	终端属性消息		终端属性同注册消息，见表 6

表 16 查询终端属性应答消息体数据格式

8.14 下发终端升级包

消息 ID: **0x8108**

下发终端升级包消息体数据格式见表 17。对该命令终端使用通用应答确认是否正确收到升级包数据。

起始字节	字段	数据类型	描述及要求
0	升级类型	BYTE	0: GSM 通讯终端, 1: 蓝牙终端
1	制造商 ID	BYTE[10]	制造商编号
11	版本号长度	BYTE	n
12	版本号	STRING	

表 17 下发终端升级包消息体数据格式

注：这里仅做通知终端升级的指令，终端收到指令后需要自行到相应的下载地址寻找指定版本号的升级包。

8.15 终端升级结果通知

消息 ID: **0x0108**

终端在升级完成并重新连接后使用该命令通知监控中心。终端升级结果通知消息体数据格式见表 18。

起始字节	字段	数据类型	描述及要求
0	升级类型	BYTE	0: GSM 通讯终端, 1: 蓝牙终端
1	升级结果	BYTE	0: 成功, 1: 失败, 2: 取消
2	版本号长度	BYTE	n
3	版本号	STRING	当前终端中的版本号

表 18 终端升级结果通知消息体数据格式

8.16 位置信息汇报

消息 ID: **0x0200**

位置信息汇报消息体由位置基本信息和位置附加信息项列表组成，消息结构图如表 19 所示：

位置基本信息(表 20)	位置附加信息项列表（表 23）
--------------	-----------------

表 19 位置汇报消息结构图

位置附加信息项列表由各位置附加信息项组合，也可没有，根据消息头中的长度字段确定。

位置基本信息数据格式见表 20。

起始字节	字段	数据类型	描述及要求
0	报警标志	WORD	报警标志位定义见表 21
2	状态	WORD	状态位定义见表 22
4	纬度	DWORD	以度为单位的纬度值乘以 10 的 6 次方，精确到百万分之一度
8	经度	DWORD	以度为单位的经度值乘以 10 的 6 次方，精确到百万分之一度
12	速度	WORD	km/h
14	方向	WORD	0-359，正北为 0，顺时针
16	时间	BCD[6]	YY-MM-DD-hh-mm-ss

表 20 位置基本信息数据格式

位	定义	说明
0	1: 低电量报警	终端电量低于 10%
1	1: 移动报警	终端在关锁状态下发生非正常移动
2	1: 撞击报警	终端在关锁状态下发生激烈撞击
3	1: 侧翻报警	终端在关锁状态下发生侧翻
4	1: 非法开锁	终端在没接收到任何开锁指令情况下发生开锁
5	1: 终端故障	终端无法开锁、关锁等
6-15	保留	

表 21 报警标志位定义

位	状态
0	0: 未定位；1: 定位
1	0: 北纬；1: 南纬
2	0: 东经；1: 西经
3	0: 正常状态；1: 运输状态
4	1: 定时上报

5	1: 开锁上报
6	1: 关锁上报
7	0: 放电; 1: 充电
8	0: 在停车区; 1: 离开停车区
9-15	保留

表 22 状态位定义

字段	数据类型	描述及要求
附加信息 ID	BYTE	1-255
附加信息长度	BYTE	
附加信息		附加信息定义见 表 24

表 23 位置附加信息项格式

附加信息 ID	附加信息长度	描述及要求
0x30	1	BYTE, 无线通信网络信号强度 (CSQ)
0x31	1	BYTE, 可用定位卫星个数
0xE1	1	BYTE, 电池电量百分比 (0x00-0x64)
0xE2	2	WORD, 电池电量*1000 (如电压为 4.20V, 则值为 0x1068)
0xE3	2	WORD, 充电电压*1000 (如电压为 5V, 则值为 0x1388)
0xE4	根据实际情况	基站编码的格式为: MCC+MNC+LAC+CI+ 信号强度+ (LAC CI 信号强度)+ (LAC CI 信号强度) +... 其中MCC为2个字节国家编码, MNC为2个字节网络编码, LAC为2个字节地区编码, CI为2个字节蜂窝ID, 信号强度一个字节。后面有0到3组临近小区信息。

表 24 附加信息定义

8.17 位置信息查询

消息 ID: **0x8201**

位置信息查询消息体为空。

8.18 位置信息查询应答

消息 ID: **0x0201**

位置信息查询应答消息体数据格式见表 25。

起始字节	字段	数据类型	描述及要求
0	应答流水号	WORD	对应的位置信息查询消息的流水号
2	位置信息汇报		位置信息汇报见 8.16

表 25 位置信息查询应答消息体数据格式

8.19 车辆控制

消息 ID: **0x8500**

车辆控制消息体数据格式见表 26。

起始字节	字段	数据类型	描述及要求
0	控制标志	BYTE	控制指令标志位数据格式见 表 27
1	控制时间	BCD[6]	YY-MM-DD-hh-mm-ss

表 26 车辆控制消息体数据格式

位	标志
0	0: 终端关锁; 1: 终端开锁
1	0: 蜂鸣器关闭; 1: 蜂鸣器开启
2-7	保留

表 27 控制指令标志位数据格式

注: 控制时间有一定的时效性, 终端需要根据产品情况, 来配置合适的时效时间。例如, 共享单车开锁指令中的时间和单车本身的时间相差超过 20 秒 (网络延时等), 即认为此次开锁指令失效, 不再执行开锁。

8.20 车辆控制应答

消息 ID: **0x0500**

车辆控制应答消息体数据格式见表 28。

起始字节	字段	数据类型	描述及要求
0	应答流水号	WORD	对应的车辆控制消息的流水号
2	位置信息汇报消息体		根据对应的状态位判断控制成功与否

表 28 车辆控制应答消息体数据格式

8.21 平台 RSA 公钥

消息 ID: **0x8A00**

平台 RSA 公钥消息体数据格式见表 29。

起始字节	字段	数据类型	描述及要求
0	e	DWORD	平台 RSA 公钥 {e, n} 中的 e
4	n	BYTE[128]	RSA 公钥 {e, n} 中的 n

表 29 平台 RSA 公钥消息体数据格式

8.22 终端 RSA 公钥

消息 ID: **0x0A00**

终端 RSA 公钥消息体数据格式见表 30。

起始字节	字段	数据类型	描述及要求
0	e	DWORD	终端 RSA 公钥 {e, n} 中的 e
4	n	BYTE[128]	RSA 公钥 {e, n} 中的 n

表 30 终端 RSA 公钥消息体数据格式

附录

消息对照表

序号	消息体名称	消息 ID	说明
1	终端通用应答	0x0001	终端发出
2	平台通用应答	0x8001	平台发出
3	终端心跳	0x0002	终端发出，平台回 0x8001
4	终端注册	0x0100	终端发出，平台回 0x8100
5	终端注册应答	0x8100	平台发出
6	终端鉴权	0x0102	终端发出，平台回 0x8102
7	终端鉴权应答	0x8102	平台发出
8	设置终端参数	0x8103	平台发出，终端回 0x0001
9	查询终端参数	0x8104	平台发出，终端回 0x0104
10	查询终端参数应答	0x0104	终端发出
11	终端控制	0x8105	平台发出，终端回 0x0001
12	查询终端属性	0x8107	平台发出，终端回 0x0107
13	查询终端属性应答	0x0107	终端发出
14	下发终端升级包	0x8108	平台发出，终端回 0x0108
15	终端升级结果通知	0x0108	终端发出
16	位置信息汇报	0x0200	终端发出，平台回 0x8001
17	位置信息查询	0x8201	平台发出，终端回 0x0201
18	位置信息查询应答	0x0201	终端发出
19	车辆控制	0x8500	平台发出，终端先回 0x0001，再回 0x0500
20	车辆控制应答	0x0500	终端发出
21	平台 RSA 公钥	0x8A00	平台发出，终端回 0x0A00
22	终端 RSA 公钥	0x0A00	终端发出