重庆高速蓝牙车载单元

技术要求建议稿

Ver1.07

北京泰德渥特科技有限公司

2019年09月

**目录**

[第1章 **概述** 3](#_Toc9968163)

[1.1 项目背景 3](#_Toc9968164)

[1.2 编写目的 3](#_Toc9968165)

[1.3 参考文献 3](#_Toc9968166)

[1.4 缩略语 3](#_Toc9968167)

[第2章 总体要求 5](#_Toc9968168)

[2.1 蓝牙车载单元应用体系总体结构 5](#_Toc9968169)

[2.2 系统构成和技术要求 5](#_Toc9968170)

[2.3 蓝牙通信模型和协议 6](#_Toc9968171)

[**2.3.1** 数据传输帧格式 8](#_Toc9968172)

[**2.3.2** 应用层数据定义 9](#_Toc9968173)

[**2.3.3** 应用数据类型定义应符合下列规定: 9](#_Toc9968174)

[**2.3.4** 应用数据域定义应符合下列规定: 10](#_Toc9968175)

[2.4 兼容第三方蓝牙协议策略 19](#_Toc9968176)

[2.5 安全要求 19](#_Toc9968177)

[**2.5.1** 车路通信安全保障 19](#_Toc9968178)

[**2.5.2** 互联网通行安全保障 20](#_Toc9968179)

# **概述**

## 项目背景

随着国家有关全国高速公路拆除省界站项目的推进，对于ETC用户的发行量将会出现大规模增长，为满足这一变化，采用蓝牙车载单元（OBU）、配合重庆高速的推广团队工作，形成线上线下和推广合力，能对相关的工作起到巨大的推动作用。为了满足重庆地区对于蓝牙车载标签的特定应用场景，规范各厂家供应车载OBU的到货品质,参照交通部《公路电子不停车收费技术标准》制定本规范。

## 编写目的

本文的编写目的在于，为重庆高速通渝公司发行的蓝牙BOBU产品提供对外接口及使用方法的约定，规范为重庆高速通渝公司供货的各BOBU厂家的通讯协议、调用方式和调用流程。

## 参考文献

《公路电子不停车收费技术标准》

## 缩略语

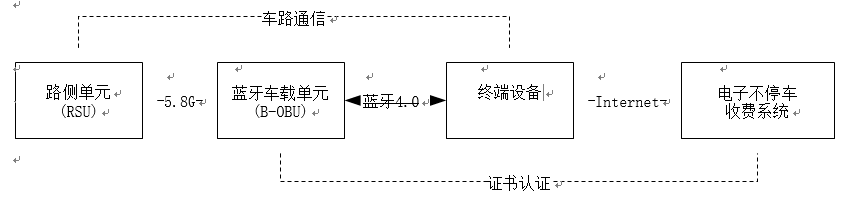
OBU – 车载单元

B-OBU – 蓝牙车载单元

# BOBU基本要求

## 蓝牙车载单元应用体系总体结构

蓝牙OBU应用体系的总体结构如下图所示：



B-OBU 应符合下列规定：

1. 应符合《电子收费 专用短程通信》GB/T 20851-2007 系列标准规定的 A 类上下行链路的各项要求。

2. 应支持蓝牙无线通信功能，支持蓝牙 BLE通信、5.8G 通信之间的数据 转发功能。

## 系统构成和技术要求

B-OBU 应在具备传统 OBU 的模块基础上，还应具备蓝牙模块和 SE 模块。

B-OBU 除支持 5.8G 电子收费 DSRC 接口外，应支持以下接口：

1. 蓝牙接口应符合本规范规定的内容。

2. 应支持数字证书的申请、发放、吊销等证书业务管理接口。

B-OBU 的蓝牙物理层基本参数应在符合 BLE 蓝牙相关规范要求外， 还应符合表 1 的规定。

**表1 蓝牙技术要求**

|  |  |
| --- | --- |
| 指标名称 | 指标 |
| 广播间隔 | ≤1S |
| 接入方式 | 移动终端APP发起 |

## BOBO设备的蓝牙特征要求

B-OBU 的主要参数应包括其 UUID 及属性，并符合表 2 的规定：

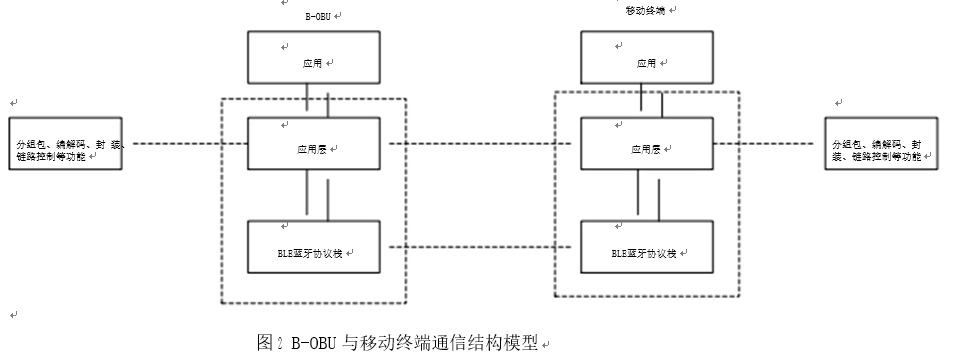
|  |  |
| --- | --- |
| 名称 | 值 |
| Service UUID | 0xfee7 |
| Write Characteristics UUID | 0xfec7 |
| Indicate Characteristics UUID | 0xfec8 |
| Read Characteristics UUID | 0xfec9 |
| Notify Characteristics UUID | - |

表2 主要参数

所有蓝牙设备的名称统一为: “CQOBU”+表面印刷号后7位

# BOBU的通讯协议

## 蓝牙通信模型和协议

移动终端与 B-OBU 通过 BLE 蓝牙通信协议进行无线通信的通信模型 见图图2。

B-OBU 的蓝牙协议应符合下列规定：

1. 通信协议应符合 BLE 蓝牙协议。
2. 应支持 Indication数据传输方式进行数据传输。

BOBU

在 B-OBU 与移动终端 APP 的通信基本流程，应符合图 3 的规定。

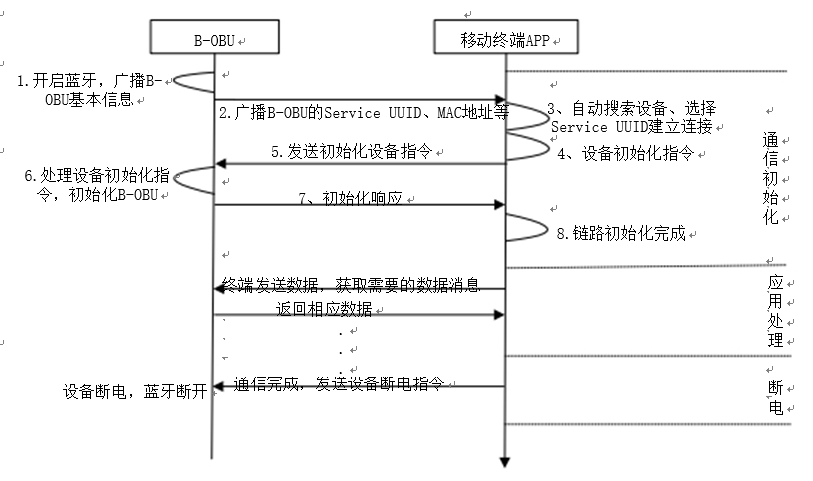


图3 基本会话流程

### 数据传输帧格式

数据传输的数据帧格式应符合表 3 的规定，数据帧中 各数据域的说明见表 4

表3数据帧格式

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ST(1byte) | CTL（2byte） | LEN(2byte) | DATA | BCC(1byte) |

表4数据帧格式说明

|  |  |  |
| --- | --- | --- |
| 字段 | 长度（字节） | 描述 |
| ST | 1 | 帧头控制字，0x50 |
| CTL | 2 | 最高位[bit:15]为1时，表示起始包，[bit:14～bit:0]表示总包数n 最高位[bit:15]为0时，表示延续包，[bit:14 ～bit:0]表示当前包序号，采用升序的方式，从2升到n，当前包序号为n时表示最后一个包 |
| LEN | 2 | 发送的数据长度（网络字节序，即 0x00,0x02 表示长度为2） |
| DATA | 由LEN计算获得 | 发送的数据 |
| BCC | 1 | BCC校验，从ST开始到DATA |

### 应用层数据定义

应用层数据包对应数据帧中的 DATA 域，其格式应符合表5规定：

表5 应用层数据帧格式

|  |  |
| --- | --- |
| Type(1Bytes) | Content(N字节) |

注：1. Type：应用数据类型，1 字节。

2. Content：应用数据域内容。

### 应用数据类型定义应符合下列规定:

APP 发送到 OBU 的指令与响应见表6 的规定。

表6 APP 到 OBU 指令

|  |  |  |
| --- | --- | --- |
| 应用数据类型 | 代码(Type) | 功能说明 |
| 设备初始化指令 | 0x80 | 设备初始化 |
| 设备通道指令 | 0x81 | 对B-OBU设备操作 |
| COS通道指令 | 0x82 | 对CPU用户卡/OBE-SAM/SE等COS通道的操作 |
| 获取记录 | 0x83 | 获取CPU用户卡密文通信时的记录 |
| 认证通道指令 | 0x84 | 设备认证（包括更新终端证书）操作 |
| 透传通道指令 | 0x85 | 数据透传操作 |
| 数据传输回应 | 0x86 | 对B-OBU发给APP的数据的回应 |
| 厂商通道指令 | 0x8F | 厂商自定义功能 |

OBU 发送到 APP 的响应与指令见表 7 的规定。

表 7 OBU 到 APP 指令

|  |  |  |
| --- | --- | --- |
| 应用数据类型 | 代码(Type) | 功能说明 |
| 设备初始化回应 | 0x90 | 返回数据帧分包最大字节，B-OBU的版本信息，以及保留的  文本状态等。 |
| 设备通道回应 | 0x91 | 返回设备通道操作结果 |
| COS通道回应 | 0x92 | 返回CPU用户卡/OBE-SAM/SE等通道的COS操作结果 |
| 获取记录回应 | 0x93 | 返回CPU用户卡密文通信时的记录 |
| 认证通道回应 | 0x94 | 返回认证通道操作结果 |
| 透传通道回应 | 0x95 | 返回透传通道操作结果 |
| 数据传输指令 | 0x96 | B-OBU传输数据到APP |
| 厂商通道回应 | 0x9F | 返回厂商通道操作结果 |

### 应用数据域定义应符合下列规定:

设备初始化指令与响应见表8 规定。

表 8 设备初始化指令与响应

|  |  |  |  |
| --- | --- | --- | --- |
| 位置 | 字节数 | 数据元 | 数据内容 |
| 发送指令 | | | |
| 0 | 1 | Type | 指令代码，此处取值0x80 |
| 指令响应 | | | |
| 0 | 1 | Type | 指令代码，此处取值0x90 |
| 1 | 1 | Status | 0x00表示正常返回；其他表示错误，具体参考附录G.2，  此时不存在下面的数据元 |
| 2 | 2 | 返回长度 | 初始化指令数据的长度（网络字节序，即 0x00,0x02 表示长度为2） |
| 4 | 2 | 返回数据 | 标识数据帧分包最大字节数。 |
| 6 | 2 | OBU状态信息 | OBU状态信息（参见GB/T20851.3 规定的ObuStatus） |
| 8 | 27 | OBU系统信息 | OBE-SAM系统信息文件前27字节 |
| 35 | 43 | OBU版本号 | OBU软件版本信息，格式：Vx.y+空格+2位省份编号+空  格+厂商编码＋空格＋厂商自定义信息（32字节文本，不足部分用空格代替） |
| 78 | 4 | OBU MAC | OBUMAC |

设备通道指令与响应见表9 规定，设备通道指令与响应中的数据说明见表10 的规定。

表 9 设备通道指令与响应

|  |  |  |  |
| --- | --- | --- | --- |
| 位置 | 字节数 | 数据元 | 数据内容 |
| 发送指令 | | | |
| 0 | 1 | Type | 指令代码，此处取值0x81 |
| 1 | 2 | 指令长度 | 设备控制指令数据的长度 |
| 3 | N | 指令数据 | 设备控制指令数据，参见：设备通道指令与响应中的数据说明 |
| 指令响应 | | | |
| 0 | 1 | Type | 指令代码，此处取值0x91 |
| 1 | 1 | Status | 0x00表示正常返回；其他表示错误，具体参考附录B，  此时不存在下面的数据元 |
| 2 | 2 | 返回长度 | 设备通道指令返回数据的长度 |
| 4 | N | 返回数据 | 设备通道指令返回数据，参见：设备通道指令与响应  中的数据说明 |

表 10 设备通道指令与响应数据

|  |  |  |
| --- | --- | --- |
| 设备通道指令数据发送说明 | | |
| 指令长度 | 指令数据 | 指令描述 |
| 1 | C0 | 获取设备的设备表面号 |
| 1 | C1 | 获取设备的版本号 |
| 1 | C2 | 获取设备的电池电量 |
| 1 | C3 | 强制断开蓝牙连接 |
| 1 | C4 | 对设备复位 |
| 1 | C5 | 获取设备的蓝牙MAC |
| 1 | C6+时长 | 设置蓝牙在指定时间内保持激活状态，并且保持CPU用户卡不  断电，时长1字节，单位为秒 |
| 1 | CC | 获取设备信息：ASCII码，最长100字节 |
| 回应长度 | 回应数据 | 回应描述 |
| 17 | C0+设备表面号 | 设备表面号（16bytes），ASCII码 |
| 3 | C1+版本号 | 版本号（2bytes），例，V2.0.1表示为0x02 0x01 |
| 2 | C2+电池电量 | 电池电量（1byte），电量百分比（0–没电，非0–有电） |
| 1 | C3 | 无 |
| 1 | C4 | 无 |
| 7 | C5+蓝牙MAC | 设备的蓝牙MAC：6bytes |
| 2 | C6+实际执行的不下电  时长 | B-OBU根据自身电量情况，回应实际执行的激活时间。宜与APP  要求相同。 |
| <=100 | CC+设备信息 | 设备信息，ASCII码，内容厂家自定义 |

COS 通道指令与响应见表11 的规定。

表 11 COS 通道指令与响应

|  |  |  |  |
| --- | --- | --- | --- |
| 位置 | 字节数 | 数据元 | 数据内容 |
| 发送指令 | | | |
| 0 | 1 | Type | 指令代码，此处取值0x82 |
| 1 | 1 | Data Type | bit0:数据类型（ 0-明文数据，1-加密数据）  bit1~3:保留（设置为0）  bit4~7:目标索引（1-CPU用户卡；2-OBE-SAM；3-SE；其他值-保留） |
| 2 | 2 | 指令长度 | COS指令数据的长度（不超过384） |
| 4 | N | 指令数据 | COS指令数据（TLV格式，见附录G.2） |
| 指令响应 | | | |
| 0 | 1 | Type | 指令代码，此处取值0x92 |
| 1 | 1 | Status | 0x00表示正常返回；其他表示错误，具体参考附录B，此时不存在下面的数据元 |
| 2 | 1 | Data Type | bit0:数据类型（ 0-明文数据，1-加密数据）  bit1~3:保留（设置为0）  bit4~7:目标索引（和指令的值相同） |
| 3 | 2 | 返回长度 | COS指令返回数据的长度（不超过384） |
| 5 | N | 返回数据 | COS指令返回数据（TLV格式，见附录G.2） |

获取记录的指令与响应见表 12 的规定，获取记录指令与响应中数据说明见表 13 的规定。

表12 获取记录指令与响应

|  |  |  |  |
| --- | --- | --- | --- |
| 位置 | 字节数 | 数据元 | 数据内容 |
| 发送指令 | | | |
| 0 | 1 | Type | 指令代码，此处取值0x83 |
| 1 | 2 | 指令长度 | 获取记录指令数据的长度 |
| 3 | N | 指令数据 | 获取记录指令数据，参见：获取记录指令与响应中的  数据说明 |
| 指令响应 | | | |
| 0 | 1 | Type | 指令代码，此处取值0x93 |
| 1 | 1 | Status | 0x00表示正常返回；其他表示错误，具体参考附录B，  此时不存在下面的数据元 |
| 2 | 2 | 返回长度 | 获取记录返回数据的长度 |
| 4 | N | 返回数据 | 获取记录返回数据，参见：获取记录指令与响应中的  数据说明 |

表 13 获取记录指令与响应

|  |  |  |
| --- | --- | --- |
| 获取记录指令数据发送说明 | | |
| 指令长度 | 指令数据 | 指令描述 |
| 2 | C0+记录索引 | 获取IC卡COS通道指令记录  索引（1bytes）:记录索引号，循环记录，最新的记录号为01，上一次的为02，依次类推…… |
| 获取记录指令返回数据说明 | | |
| 回应长度 | 回应数据 | 回应描述 |
| N | C0+记录 | 记录：TLV格式，（TLV格式，见附录B）  例：记录索引号+len+'E'+len(密文命令)+密文命令  +'C'+len(明文命令)+明文命令+'R'+len(回应)+回应。 |

注：循环记录，记录总数量为 9，不存在的记录长度为 0

认证通道的指令与响应见表 14的规定，认证通道指令与响应中的数据说明见表 15 的规定。

表 14 认证通道指令与响应

|  |  |  |  |
| --- | --- | --- | --- |
| 位置 | 字节数 | 数据元 | 数据内容 |
| 发送指令 | | | |
| 0 | 1 | Type | 指令代码，此处取值0x84 |
| 1 | 2 | 指令长度 | 认证通道指令数据的长度 |
| 3 | N | 指令数据 | 认证通道指令数据，参见：认证通道指令与响应中的  数据说明 |
| 指令响应 | | | |
| 0 | 1 | Type | 指令代码，此处取值0x94 |
| 1 | 1 | Status | 0x00表示正常返回；其他表示错误，具体参考附录B，  此时不存在下面的数据元 |
| 2 | 2 | 返回长度 | 认证返回信息的长度 |
| 4 | N | 返回数据 | 认证返回信息，参见：认证通道指令与响应中的数据  说明 |

表 15认证通道指令与响应

|  |  |  |
| --- | --- | --- |
| 认证通道指令数据发送说明 | | |
| 指令长度 | 指令数据 | 指令描述 |
| 1 | C0+认证端发来的随机数[8BYTES] | 认证计算结果（随机数 + 8Bytes0x00）的结果，由认证密钥进行SM4/3DES加密，得到的计算结果 |
| 1 | C1+SM4/3DES认证密钥+MAC | 认证密钥更新（SM4/3DES）  MAC + 原密钥签名值（4BYTES）  注：1、C1指令的MAC计算方法为BOBU内原认证密钥对初始值(SM4为16字节“0x00”/3DES为8字节“0x00”) 进行**解密运算**的前4字节。  2、如厂家生产流程中不采用蓝牙接口灌注认证密钥，可不提供此接口 |
| 认证通道指令返回数据说明 | | |
| 回应长度 | 回应数据 | 回应描述 |
| n | C0+认证结果[8BYTES] | 认证计算结果（随机数 + 8Bytes0x00）的结果，由认证密钥进行SM4/3DES加密，得到的计算结果 |
| 1 | C1 | 无 |

C0指令范例：

SM4

随机数为：EEFF112212345678

出厂密钥：FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

计算过程：出厂密钥加密-->EEFF1122123456780000000000000000==>154307EABF3CE4B07A82B6DAF1138E28

认证码为：154307EABF3CE4B0

3DES

随机数为：EEFF112212345678

出厂密钥：FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

计算过程：出厂密钥加密-->EEFF112212345678==>B80DBCDD0571F12D

认证码为：B80DBCDD0571F12D

透传通道指令与响应见表16的规定。

表 16透传通道指令与响应

|  |  |  |  |
| --- | --- | --- | --- |
| 位置 | 字节数 | 数据元 | 数据内容 |
| 发送指令 | | | |
| 0 | 1 | Type | 指令代码，此处取值0x85 |
| 1 | 1 | Data Type | bit0：是否回应（0-回应；1-不回应）  bit1~3:保留（设置为0）  bit4~7:目标索引（1-传输到蓝牙通道，2-传输到5.8G通道，3-传输到OBU自身，其他值-保留） |
| 2 | 2 | 指令长度 | 透传指令数据的长度 |
| 4 | N | 指令数据 | 透传指令数据 |
| 指令响应（若设置为需要回应） | | | |
| 0 | 1 | Type | 指令代码，此处取值0x95 |
| 1 | 1 | Status | 0x00表示正常返回；其他表示错误，具体参考附录G.2，  此时不存在下面的数据元 |
| 2 | 1 | Data Type | bit0~3:保留（设置为0）  bit4~7:目标索引（和指令的值相同） |
| 3 | 2 | 返回长度 | 透传指令返回数据的长度 |
| 5 | N | 返回数据 | 透传指令返回数据 |

数据传输指令与响应见表 18 的规定。

表 18 数据传输令

|  |  |  |  |
| --- | --- | --- | --- |
| 位置 | 字节数 | 数据元 | 数据内容 |
| 发送指令 | | | |
| 0 | 1 | FrameType | 指令代码,此处取值0x96 |
| 1 | 1 | DataType | 数据类型：  0-文本  1-二进制  2-卡片插入事件（此时无后面的Length和Content） 3-卡片拔出事件（此时无后面的Length和Content） 4-防拆弹起事件（此时无后面的Length和Content） 5-防拆按下事件（此时无后面的Length和Content）  6~255保留 |
| 2 | 1 | Reply | 应答选项  0-不需要APP应答  1-需要APP应答 |
| 3 | 2 | Length | 数据长度N |
| 4 | N | Content | 内容 |
| 响应（若设置为需要回应） | | | |
| 0 | 1 | Type | 指令代码,此处取值0x86 |
| 1 | 1 | Status | 0x00表示正常返回；其他表示错误 |

厂商通道的指令与响应见表 19 规定。

表 19 厂商通道指令与响应

|  |  |  |  |
| --- | --- | --- | --- |
| 位置 | 字节数 | 数据元 | 数据内容 |
| 发送指令 | | | |
| 0 | 1 | Type | 指令代码，此处取值0x8F |
| 1 | 2 | 指令长度 | 厂商通道指令数据的长度 |
| 3 | N | 指令数据 | 厂商通道指令数据（厂商自定义） |
| 指令响应 | | | |
| 0 | 1 | Type | 指令代码，此处取值0x9FH |
| 1 | 1 | Status | 0x00表示正常返回；其他表示错误，具体参考附录G.2，此  时不存在下面的数据元 |
| 2 | 2 | 返回长度 | 厂商通道指令返回数据的长度 |
| 4 | N | 返回数据 | 厂商通道指令返回数据（厂商自定义） |

应用层 Indication 数据传输的协议规程见图4，流程如下:

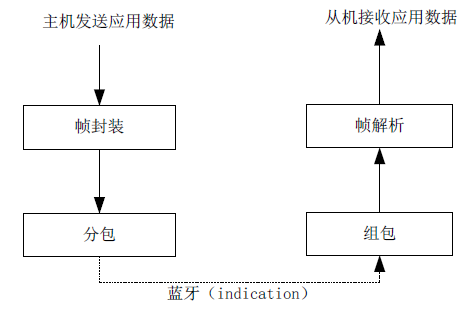


图4 Indication 模式下应用层协议

* 帧封装

将应用数据依据2.3.1所规定的格式封装。

* 分包

应用层数据帧应按BLE蓝牙协议规范要求长度分包并采用蓝牙Indication传输方式依次传输数据。

* 组包

依据接收到第一个数据包识别传输方式及传输长度，按序组包，还原数据帧。

* 帧解析

依据2.3.1所规定的格式解析数据帧，依据帧格式中CTL字段按序还原应用数据后发送给从机的应用。

## 兼容第三方蓝牙协议策略

B-OBU 可同时广播多个Service UUID，除了 APP 要求的Service UUID外，还必须包含表 2 的 Service UUID。

## 安全要求

### 车路通信安全保障

车路通信的其总体架构见图 5，车路通信逻辑通道的安全由路侧单元与 B-OBU 之间的 5.8GHz DSRC 通信的安全机制保障。

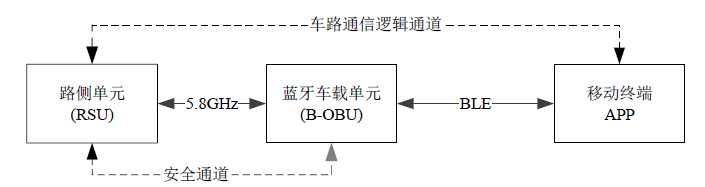


图5 车路通信安全保障

### 互联网通行安全保障

互联网通信的总体架构见图 6 ，应符合下列安全要求：

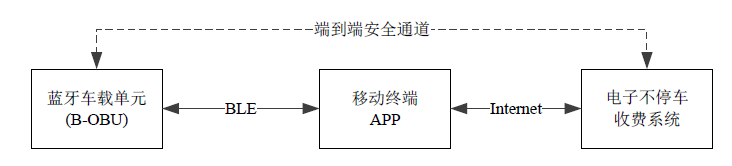


图6 互联网终端安全通道示意图

* + - 1. 当电子不停车收费系统系统业务数据在互联网上进行传输时，应对数据先加密以后再进行传输；并提供数据完整性检查的机制。
      2. 处理中心与 B-OBU 的身份应进行重庆高速通渝公司对BOBU产品的认证发行密钥的认证码运算。

### B-OBU与认证中心的握手过程和算法说明



图7 B-0BU与认证中心的握手流程

1. 由APP发起对蓝牙OBU的建立握手过程。
2. B-OBU获取ESAM上的晶片序列号（SN）；
3. B-OBU将晶片序列号通过蓝牙通道返回给APP；
4. APP向服务端发起BOBU认证请求；
5. BOBU核查数据库当中的BOBU的发行状态，产生对应的认证随机数；
6. 服务端将认证随机数返回给APP；
7. APP将认证随机数通过APP发给BOBU；
8. BOBU进行认证计算；计算方法，将认证随机数后补0x00，补足16字节，利用认证密钥进行SM4/3DES**加密**，得到认证码;
9. BOBU将认证码返回给APP；
10. APP将认证码返回给服务端；
11. 服务端利用BOBU的SN、认证根密钥等特征数据分散出B-OBU的工作认证密钥，
12. 服务端进行SM4/3DES认证运算、并将BOBU的会话至于“激活状态”，允许后续交易进行；
13. 服务端向APP发送认证成功结果。

### 认证密钥置换

为规范蓝牙OBU的认证发行，简化一次发行流程，需要在5.8G信道增加：

认证秘钥接口，如下：

根据ETC国标GBT20851.4协议，通道号暂定为ChannelID为0

TransferChannel\_rq请求

暂定指令内容为：01 16 A1 A1 + 16字节密钥 + 4字节MAC

01为指令条数，16为长度

TransferChannel\_rs响应

暂定指令内容为：01 03 B1 B1 +状态（0成功，1失败）

01为指令条数，03为长度