ICS 03.220.20;33.060.99
R07

T/ITS

中国智能交通产业联盟标准

T/ITS 0055—2017

电子收费（ETC）设备蓝牙应用接口规范

Bluetooth application interface specification for ETC equipment

2017-12-10 发布　　2018-03-01 实施

中国智能交通产业联盟　发布

目　　次

前　言

本标准定义了电子收费蓝牙设备的一般规定、蓝牙通信模型和协议、应用层、安全要求等内容。

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国智能交通产业联盟提出并归口。

本标准于2017年12月首次发布，本次为首次发布。

本标准起草单位：北京速通科技有限公司、交通运输部公路科学研究院、广东联合电子服务股份有限公司、深圳成谷科技有限公司、广州市埃特斯通讯设备有限公司、深圳市金溢科技股份有限公司、广州优路加信息科技有限公司、北京聚利科技股份有限公司、北京万集科技股份有限公司、天津中兴智联科技有限公司、江南天安科技有限公司、重庆云途交通科技有限公司、北京握奇智能科技有限公司、浙江创泰科技有限公司、深圳熹刷科技有限公司、丰田汽车研发中心（中国）有限公司、金陵科技学院

本标准主要起草人：张北海、刘鸿伟、逯静辉、陈丙勋、李全发、王刚、陈喆、于海、卢立阳、薛金银、高文宝、武潇、何山、于海、尤鑫、彭海勇、陈仰华、段作义、李智辉、李阳龙、赵昱阳、马涛、赵云辉、祖晖、贾安州、李振华、胡振、钱烨、辛宇、时旭、魏星、杨琼

引　言

为使电子收费（ETC）设备的蓝牙应用接口能够按统一的标准进行说明和描述，特制定本标准。

为了保持标准的适用性与可操作性，各使用者在采标过程中，及时将对本标准规范的意见及建议函告北京速通科技有限公司，以便修订时研用。

地址：北京市丰台区六里桥南里甲 9 号首发大厦 C 座，邮编：100161，邮箱：lujinghui@ktetc.com。）

电子收费(ETC)设备蓝牙应用接口规范

1 范围

本标准规定了电子收费（ETC）蓝牙设备的一般规定、蓝牙通信模型和协议、应用层、安全要求等内容。

本标准适用于采用电子收费（ETC）专用短程通信（DSRC）技术的蓝牙车载单元（B-OBU）设备，也可以供应用于电子收费CPU用户卡充值的蓝牙读卡设备参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

交通运输部2011年第13号公告 《收费公路联网电子不停车收费技术要求》

GB/T 20851.1-2007 电子收费 专用短程通信 第1部分：物理层

GB/T 20851.2-2007 电子收费 专用短程通信 第2部分：数据链路层

GB/T 20851.3-2007 电子收费 专用短程通信 第3部分：应用层

GB/T 20851.4-2007 电子收费 专用短程通信 第4部分：设备应用

GB/T 20851.5-2007 电子收费 专用短程通信 第5部分：物理层主要参数测试方法

Bluetooth Core Specification Version 4.x 蓝牙4.x规范

JR/T 0025-2005 中国金融集成电路（IC）卡规范

ISO/IEC 14443 识别卡-非接触式集成电路卡

3 术语、定义和缩略语

下列术语和缩略语适用于本文件。

3.1 术语

3.1.1

电子收费 electronic toll collection

在不停车条件下，应用无线电射频识别及计算机等技术自动完成对通过车辆的识别、收费操作、车道设备控制和收费数据处理的收费方式。

3.1.2

路侧单元 roadside unit

安装在收费车道门架上或收费岛立柱上的用于同过往车辆上的车载单元进行通信的天线及相应的控制设备。

3.1.3

车载单元 on-board unit

安装在车辆内部（风挡玻璃或仪表台上）并且支持利用专用短程通信与路侧单元进行信息交换的设备。

3.1.4

蓝牙车载单元 bluetooth on-board unit

具备蓝牙通讯模块的车载单元。

3.1.5

蓝牙4.0协议

一种支持设备短距离通信的无线电技术，由蓝牙技术联盟（Bluetooth Special Interest Group，简称Bluetooth SIG）管理。当前包括经典蓝牙、高速蓝牙和蓝牙低功耗（Bluetooth Low Energy，简称BLE）协议。本规范采用BLE模式。

3.1.6

APP

指应用程序（APP为Application缩写），本规范中特指为智能移动终端的第三方应用程序。

3.1.7

SM2算法 SM2 Algorithm

一种椭圆曲线密码算法，密钥长度为256比特。

3.1.8

SM3算法SM3 Algorithm

一种密码杂凑算法，其输出为 256 比特。

3.1.9

SM4算法 SM4 Algorithm

一种分组密钥算法，分组长度为128比特，密钥长度为128比特。

3.2 缩略语

3DES：三重数据加密标准（Triple Data Encryption Standard）

APDU：应用协议数据单元（Application Protocol Data Unit）

B-OBU：蓝牙车载单元（Bluetooth On-Board Unit）

BLE：蓝牙低功耗（Bluetooth Low Energy）

CA：证书认证机构（Certification Authority）

CLA：命令类别（Chip Card Payment Service）

COS：卡片操作系统（Chip Operating System）

CPU：中央处理单元（Central Process Unit）

CRC：循环冗余校验(Cyclic Redundancy Check)

DES：数据加密标准(Data Encryption Standard)

DSRC：专用短程通信（Dedicated Short Range Communication）

EF：基本文件（Elementary File）

ETC：电子（不停车）收费（Electronic Toll Collection）

IC：集成电路(Integrated Circuit)

ICC：集成电路卡（Integrate Circuit Card）

ID：身份标识号码（Identity）

INS：命令报文的指令字节（Instruction Byte of Command Message）

Lc：终端发出的命令数据的实际长度（Exact Length of Data Sent）

Le：响应数据中的最大期望长度（Maximum Length of Data Expected）

MAC：报文鉴别码（Message Authentication Code）

MF：主控文件（Master File）

OBE：车载设备（On Board Equipment）

OBU：车载单元（On Board Unit）

P1：参数1（Parameter 1）

P2：参数2（Parameter 2）

RFU：保留为将来所用（Reserved for Future Use）

RSU：路侧单元（Roadside Unit）

SAM：安全存取模块(Secure Access Module)

SE：安全单元（Security Embedded Secure Access Module）

UUID：通用唯一识别码（Universally Unique Identifier）

4 一般规定

B-OBU应符合下列规定：

a）应符合《电子收费 专用短程通信》（GB/T 20851）规定的 A 类上下行链路的要求。

b）应支持蓝牙通信，蓝牙物理层基本参数除应符合 BLE 的规定外，还应符合表 1 的规定。为降低使用蓝牙功能的功耗，表 1 中定义了广播超时定时器和通信链路存活定时器。广播超时定时器定义了 B-OBU 的蓝牙模块激活后广播信息尝试建立通信链接，若移动终端 APP 在规定的时

间内无响应，B-OBU 应停止广播。通信链路存活定时器是 B-OBU 与移动终端 APP 建立链路后，在规定时间内无数据交互，B-OBU 应释放链路并将蓝牙模块置于休眠状态。

c) 当 B-OBU 的蓝牙接口和 5.8GHz 接口同时有数据收发时，应优先处理 5.8GHz 接口数据。

d) 应能同时广播多个 Service UUID，除移动终端 APP 要求的 Service UUID 外，还应包含表 2 的 Service UUID。

e) B-OBU 同时广播多个 Service UUID，是为了兼容第三方蓝牙协议策略，如微信蓝牙协议。为兼容未来对通讯协议特殊需求，支持多种 APP 的通讯要求，可添加自定义通讯协议，但新增的通信协议必须是在本规范应用层的基础上打包数据。

f) 应采用基于国产密码算法的 SE 模块，SE 模块应符合附录 B 的规定。

g) 应支持数字证书业务相关接口。

h) 应能实现车路通信应用和互联网应用，见图 1。

表1 蓝牙技术要求

指标名称	指标
广播间隔	≤1s
广播超时定时器	90s
通信链路存活定时器	90s
接入方式	移动终端APP发起

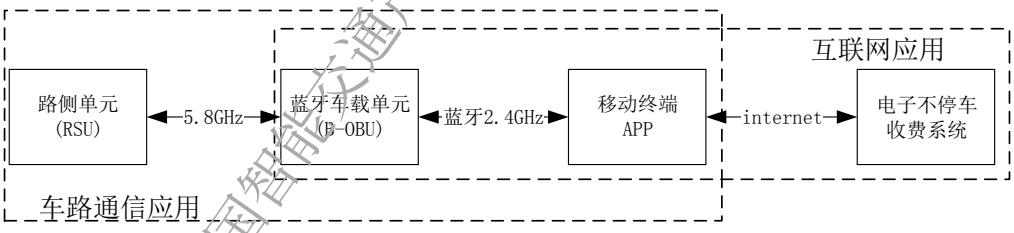

图1 B-OBU 支持的应用场景示意图

5 蓝牙通信模型和协议

5.1 蓝牙通信模型

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 2。B-OBU 的蓝牙通讯模型分二层，第一层为原生 BLE 标准协议，第二层应用层在 BLE 标准协议基础上，定义了通讯数据帧结构和应用数据类型，对应用提供的数据按照应用层帧结构进行封帧、分包、组包、

解析，并规定了应用层的数据传输的链路控制协议。

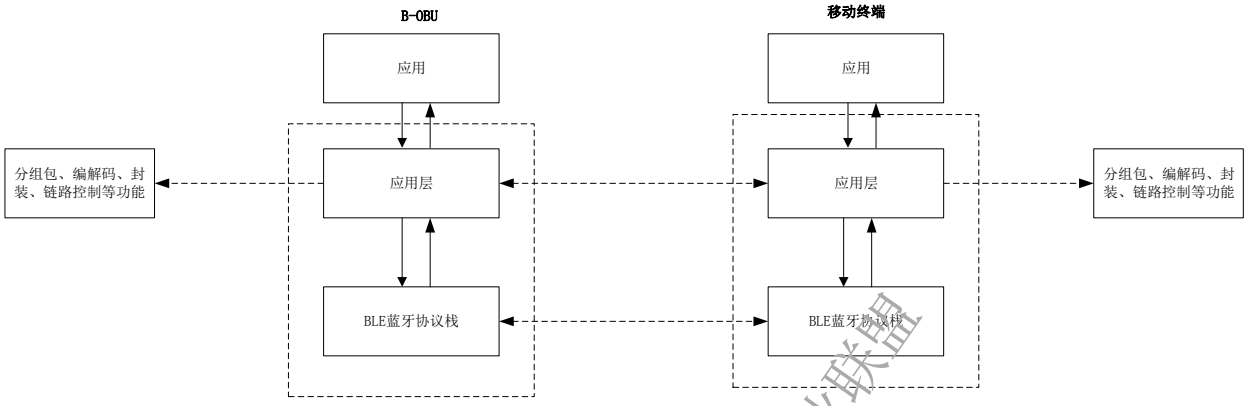

图2　B-OBU 与移动终端通信结构模型

5.2　蓝牙协议规定

B-OBU 的蓝牙协议应符合下列规定：

a) 通信协议应符合 BLE 蓝牙协议。每次收发数据长度应遵守 BLE 蓝牙协议规范要求。

b) 应支持 Indication 和 Notification 数据传输方式，由主机端应用选择传输方式。Indication 数据传输为蓝牙应答传输方式，数据传输顺序及可靠传输由 BLE 蓝牙协议栈保障，Notification 数据传输方式为蓝牙无应答传输方式，由于 BLE 蓝牙协议栈不能保障数据可靠传输，应由应用层设计链路控制机制来保证数据发送成功。经过测试验证，Notification 通信模式比 Indication 通信模式传输速率要快，在对传输速率较高的应用场景宜选用 Notification 通信模式，对可靠性要求较高的应用场景，两种模式均可。

c)采用 Indication 数据传输方式时，应用层封装成帧的数据帧长度超过 BLE 蓝牙协议规范要求长度时，应用将其分割为相应长度的小数据包依次发送。考虑到不同厂家 B-OBU 性能差异，数据帧的最大长度可由厂商自定义。

1） 移动设备 APP 可通过设备初始化命令获得 B-OBU 的支持最大数据帧长度。

2） 若数据包超过 B-OBU 支持的最大数据帧长度，则需要多帧发送，若不是最后一个数据帧，数据长度必须为支持的最大数据帧长度。

3） 采用小端模式传输。

d) 采用 Notification 数据传输方式时，应用层封装成帧的数据帧长度应不大于 BLE 蓝牙协议规范要求长度，例如 BLE4.0 规定的 20 字节。当应用数据长度超过 BLE 蓝牙协议规范要求长度

时，发送端应采用先分包后封装成帧后发送给蓝牙协议栈，接收端应采用按帧解析后依据帧序号组包。采用小端模式传输。

5.3 蓝牙主要参数

B-OBU 的主要参数应包括其 UUID 及属性，并符合表 2 的规定：

表2 主要参数

名称	值
Service UUID	0xXXXX
Write Characteristics UUID	0xXXXX
Indicate Characteristics UUID	0xXXXX
Read Characteristics UUID	0xXXXX
Notify Characteristics UUID	0xXXXX

6 应用层

6.1 通信初始化流程

B-OBU 与移动终端的通信中，移动终端作为主机，B-OBU 作为从机，会话流程分为会话初始化、应用处理、会话结束断电三个基本步骤。B-OBU 与移动终端 APP 的通信初始化流程，应符合图 3 的规定。B-OBU 打开蓝牙并广播基本信息尝试建立蓝牙通信链接可以有多种方式，以适应不同的应用场景：蓝牙通信链路长连接模式，适用于 B-OBU 车辆前装通过车载取电场景下，长连接模式下为防止未经认证的移动终端 APP 与 B-OBU 建立连接；外部触发激活蓝牙模块信息并尝试建立蓝牙通信链路，包括 B-OBU 收到 RSU 转发给移动终端 APP 的指令、B-OBU 开关按钮、插卡等信号触发。

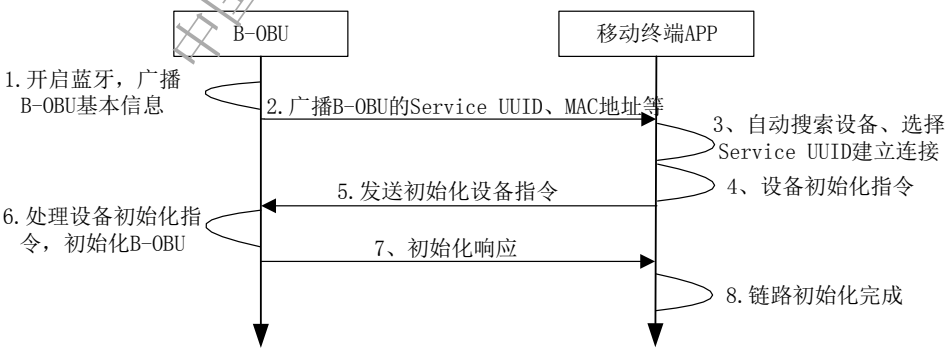

图3 B-OBU 与移动终端 APP 的通信初始化流程

6.2 数据帧格式

1 Indication 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 Indication 数据传输方式的数据帧格式

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

表4 数据帧数据域说明

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，表示开始包，[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	1	发送的数据长度
DATA	由LEN计算获得	发送的数据
BCC	1	BCC校验，从ST开始到DATA

2 Notification 数据传输的数据帧格式应符合表 5 的规定，数据帧中各数据域的说明见表 6。

表5 Notification 数据传输方式的数据帧格式

ST(1byte)	CTL(2Bytes)	LEN(1byte)	DATA	BCC(1byte)

表6 数据帧中数据域的说明

字段	长度	描述
ST	1	帧头控制字：0x50-表示数据帧；0xA0-表示控制帧。
CTL	2	最高位[bit:15]为1时，表示开始包，[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	1	发送的数据长度
DATA	由LEN计算取得	发送的数据
BCC	1	BCC校验，从ST开始到DATA

3 应用层数据包对应数据帧中的 DATA 域，其格式应符合表 7 规定：

表7 DATA 域格式

Type(1byte)	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。

3） 蓝牙每一条指令的 Type 应固定，当同一指令的数据进行分帧发送时，第一帧的数据含有 Type，其它帧没有 Type。

6.3 应用数据类型定义

1 APP 发送到 OBU 的指令与响应见表 8 的规定。

表8 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

注：1）在 Indication 数据传输方式下，为适应各个厂商 B-OBU 性能，设备初始化（0x80）指令需要完成的功能由厂商自定义，APP 只需要在操作设备之前发送 0x80 指令即可（指令内容为空）。

2）采用 Indication 数据传输方式时，帧封装数据长度通过设备初始化命令确定，若应用数据长度超过一帧最大长度，则需要多帧发送。

2 OBU 发送到 APP 的响应与指令见表 9 的规定。

表9 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

6.4 应用数据域定义

1 设备初始化指令与响应见表 10 规定。

表10　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A.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
4	1	返回数据	第1字节标识数据帧分包最大字节数。
5	2	OBU状态信息	OBU状态信息（参见GB/T20851.3 规定的ObuStatus）
7	27	OBU系统信息	OBE-SAM系统信息文件前27字节
34	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）

2　设备通道指令与响应见表 11 规定，设备通道指令与响应中的数据说明见表 12 的规定。

表11　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A.2，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12　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

表 12 设备通道指令与响应数据（续）

1	C2	获取设备的电池电量百分比
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
2	C6+时长	设置蓝牙在指定时间内保持激活状态，如果处于CPU卡操作过程中应保持CPU用户卡不断电。时长占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+电池电量百分比	电池电量百分比（1byte）
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

3 COS 通道指令与响应见表 13 的规定。

表13 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A.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A.2，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A.2）

4 获取记录的指令与响应见表 14 的规定，获取记录指令与响应中数据说明见表 15 的规定。

表14　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A.2，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15　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A.2） 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

5　认证通道的指令与响应见表16的规定，认证通道指令与响应中的数据说明见表17的规定。

表16　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			

表 16　认证通道指令与响应(续)

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A.2，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17　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+时间戳（4字节）	设备认证步骤1
N	C1+工作密钥密文+工作密钥校验值（8字节）+MAC密钥密文+MAC密钥校验值（8字节）+Rnd2（16字节）+会话ID d1+S2	设备认证步骤2 S2:服务器私钥签名，签名数据见7.2 注：设备端由SE完成验签、密钥校验、密钥解密操作
1	C2	更新终端证书步骤1：初始化
1	C3	更新终端证书步骤2：获取终端公钥
N	C4+终端证书	更新终端证书步骤3：更新证书
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+SE芯片编号+Rnd1+A1 +时间戳T1	SE芯片编号(8bytes)从SE中获取 Rnd1(16bytes)，随机数 A1(1 bytes)，算法标识，国密SM2设置为0x82 时间戳T1经移动终端APP从处理中心获得
1	C1	无
1	C2	无
N	C3+终端表面号+终端公钥	终端表面号（设备表面号，16bytes）， ASCII码 终端公钥：不同算法的公钥长度不同
1	C4	无

6　透传通道指令与响应见表 18 的规定。

表18　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:数据类型（0:明文数据；1:加密数据） bit1:是否回应（0:回应；1:不回应） bit2～3:保留（设置为0） bit4～7:目标索引（1:传输到蓝牙通道；2:传输到5.8GHz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A.2，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	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

7　数据传输指令与响应见表 19 的规定。

表19　数据传输指令与响应

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	Data Type	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

表 19　数据传输指令与响应(续)

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

8　厂商通道的指令与响应见表 20 规定。

表20　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0x9F
1	1	Status	0x00表示正常返回；其他表示错误，具体参考附录A.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）

6.5　协议规程

6.5.1　Indication 数据传输的协议规程

应用层 Indication 数据传输的协议规程见图 4，流程如下:

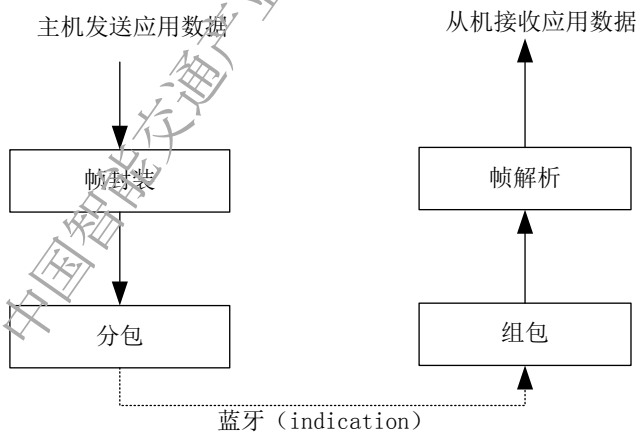

图4　Indication 模式下应用层协议

1　帧封装

将应用数据依据6.2所规定的格式封装。

2　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。

3　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。

4　帧解析

依据6.2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。

6.5.2　Notification 数据传输的协议规程

应用层 Notification 数据传输的协议规程见图 5，流程如下：

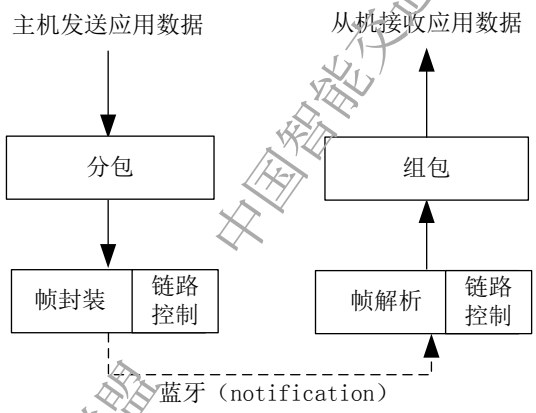

图5　Notification 模式下应用层协议

1　分包

将应用传输的数据依据10.3.3所规定的格式能封装的最大数据进行分包。

2　帧封装

将分包依据10.3.3所规定的格式封装成帧并采用蓝牙Notification传输方式依次传输数据。

3　帧解析

依据10.3.3所规定的格式解析数据帧。

4　组包

依据数据包的帧头、包号、长度信息，按序组包，并将数据包发送给从机应用。

6.5.2.1　链路控制协议

采用Notification数据传输方式时，蓝牙协议栈不能保证数据成功发送，需要在应用层增加链路控制协议来保障数据是否成功发送，发送端和接收端之间的数据通信应遵循其协议流程，确保

数据有序可靠的传输。

（一）应用层 Notification 数据传输时的链路控制协议的基本流程见图 6，具体流程如下：

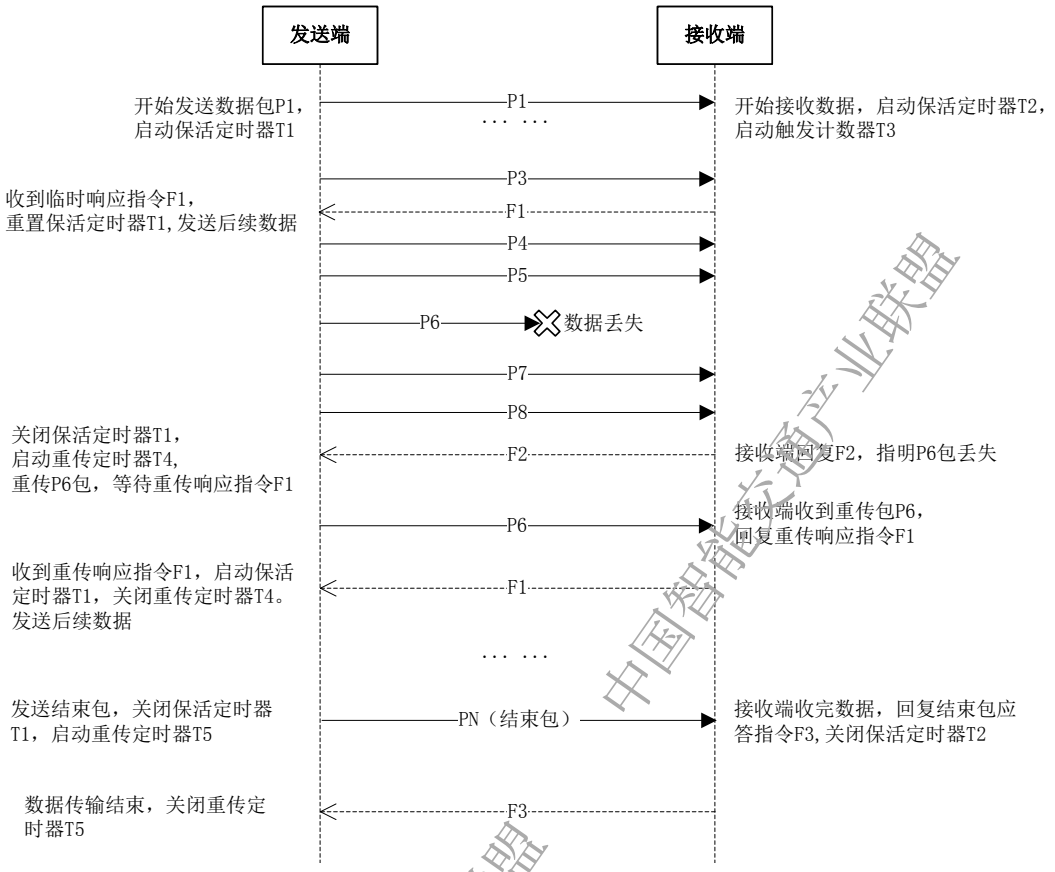

图6　Notification 数据传输方式下的链路控制协议的基本流程

1　发送端开始发送数据 P1，同时启动保活定时器 T1。

注: 1）P1 为第 1 个数据包，Pn 为第 n 个数据包。

2）T1 的作用是让发送端确认数据链路处于正常通信状态，当 T1 超时，则发送端认为通信链路断开。

2　接收端收到 P1 后启动保活定时器 T2，每收到新的数据包则重置保活定时器 T2。若 T2 超时，则接收端判定数据接收失败，接收状态复位，中断此次数据传输。

3　接收端收到 P1 后启动触发计数器 T3，连续成功接收指定数量的数据包后应回复一个临时响应指令 F1。

注:具体接收端收到多少个数据包回复 F1 自行决定，但每接收到 30 个数据包至少回复一次 F1。

4　发送端收到临时响应指令 F1 后重置保活定时器 T1。

5　接收端可依据数据包的包序号判断数据是否存在丢包，若存在丢包则回复丢包响应指令 F2。

6　发送端收到丢包响应指令 F2 后关闭保活定时器 T1，并启动重传定时器 T4。发送端根据 F2 中包含的丢包信息对丢失的数据包进行重传，重传后等待重传响应指令 F1。

7　接收端收到重传数据包后回复重传响应指令 F1。

注：若丢失的数据包正好是需要临时响应的数据包，则接收端收到重传数据包后只回复重传响应指令，无需回复临时响应指令。

8　发送端收到重传响应指令 F1 后应判断该 F1 是否为丢失数据包的重传响应，若是，则继续发送后续包，并启动保活定时器 T1，关闭重传定时器 T4。若发送端未收到指定的重传响应指令，则 T4 超时后继续重发。发送端有三次重发机会，若三次重发失败，则判定数据传输失败。

9　考虑到接收端回复重传响应指令可能存在延时，这段时间内发送端会继续发送后续数据包，对于丢失数据包的后续包，接收端可以选择接收，也可以选择不接收，协议不作强制规定。

10　发送端发送最后一个数据包后关闭保活定时器 T1，并启动重传定时器 T5，等待结束包响应指令 F3。

11　接收端收完所有数据包后回复结束包应答指令 F3，并关闭保活定时器 T2。

12　发送端收到应答指令后对指令类型进行判断，分以下三种情况：

1）　若应答指令为 F1，发送端不做任何处理，继续等待 F3；

2）　若应答指令为 F2，则重复步骤 6；

3）　若应答指令为 F3，则数据传输结束，并关闭重传定时器 T5。

若 T5 超时未收到应答指令，则重发结束包。发送端有三次重发机会，若三次重发失败，则判定数据传输失败。

相关定时器、计数器设置参见附录 A.3。

（二）应用层 Notification 数据传输时的链路控制协议的数据传输超时处理见图 7，具体流程如下：

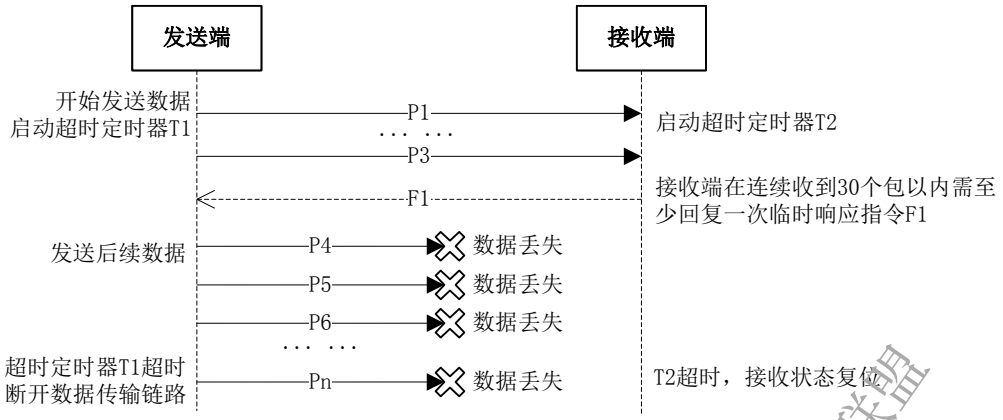

图7　Notification 数据传输方式下的链路控制协议的数据传输超时流程

1)　发送端持续发送数据，若超时未收到 F1 或 F2，则主动断开传输链路。

2)　接收端超时未收到数据，则接收状态复位。

（三）应用层 Notification 数据传输时的链路控制协议的结束包超时重发处理见图 8，具体流程如下：

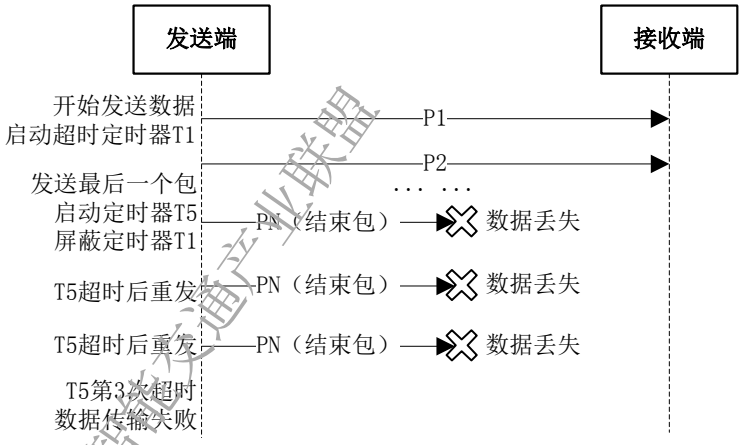

图8　Notification 数据传输方式下的链路控制协议的结束包超时重发流程

1)　发送端发送最后一个包，并启动超时定时器 T5，屏蔽定时器 T1。

2)　若 T5 超时未收到任何响应，则重发结束包，重复三次，如果没有收到任何响应，则判定数据传输失败。

6.5.2.2　控制指令说明

Notification 数据传输方式的控制指令的帧头控制字为 0xA0，控制指令规定见表 21，具体

指令规定如下：

表21　控制指令表

控制指令类型	代码(Type)	功能说明
临时响应或重传响应指令	0xF1	1. 临时响应指令:用于数据收发双方保持连接使用，接收端在连续收到30个包以内需至少回复一次临时响应指令。 2. 重传响应指令:用于收到重传数据包的响应。
数据丢包响应指令	0xF2	用于接收端反馈丢包信息。
结束包应答指令	0xF3	用于指示数据传输完成。

1　临时响应指令见表 22 规定。

表22　F1 指令

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0xF1
1	2	SN	0x0000：表示临时响应 其他：表示重传响应，该值为重传包的序号

2　数据丢包响应指令见表 23 规定。

表23　F2 指令

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0xF2
1	2	SN	丢包的序号

3　结束包应答指令见表 24 规定。

表24　F3 指令

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0xF3
1	1	SFU	备用，目前为0x00。

7　安全要求

7.1　车路通信安全要求

车路通信应用主要由 RSU 与 B-OBU 之间的 5.8GHz DSRC 通信机制保障安全。车路通信处理流程参见附录 A.1.2。

7.2　互联网通信安全要求

互联网通信业务场景是 B-OBU 通过与移动终端接入到电子不停车收费系统，移动终端 APP 依据规定的握手工作原理与处理中心建立端到端的逻辑安全通道后开展相关业务处理。互联网通信应用的总体架构见图 9，应符合下列安全要求：

图9　互联网终端安全通道示意图

1　当电子不停车收费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 的身份应进行基于数字证书的认证方式。

3　认证基本流程工作步骤见图 10 所示，具体流程如下：

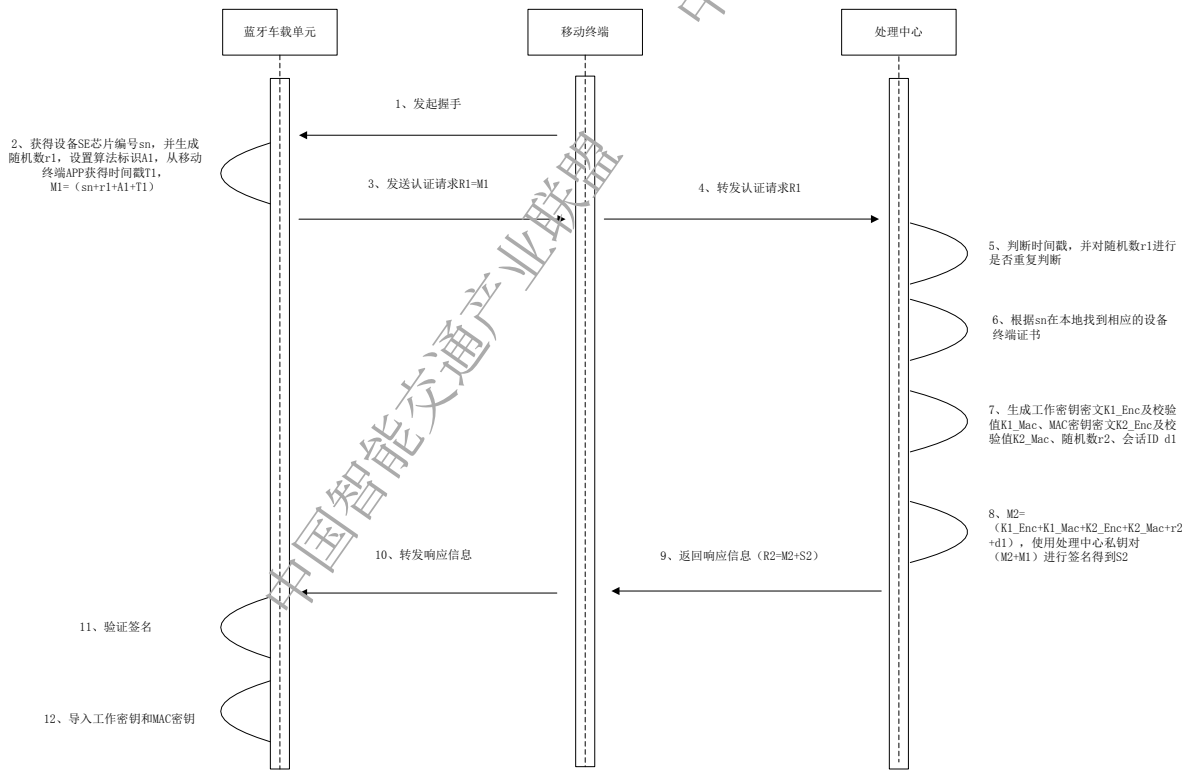

图10　B-OBU 与处理中心握手流程

1）　移动终端 APP 发起握手；

2） B-OBU 从 SE 获得 8 字节的芯片编号 sn，并生成 16 字节的随机数 r1，设置 1 字节算法标识 A1，从移动终端 APP 获得时间戳 T1，M1=(sn+r1+A1+T1)；

3） B-OBU 向移动终端 APP 发送认证请求 R1（R1=M1）；

4） 移动终端 APP 向处理中心转发认证请求 R1；

5） 处理中心判断时间戳 T1，并提取随机数 r1；然后对该随机数进行是否重复判断，如果单位窗口内该随机数已经存在，则认为存在重放攻击的风险，发送出错消息，关闭连接；

6） 处理中心根据 sn 查找终端证书，如果找不到，则发送出错消息，结束链接，找到则继续；

7） 处理中心生成工作密钥密文 K1_Enc（16 字节）及其校验值 K1_Mac（8 字节）、MAC 密钥密文 K2_Enc（16 字节）及其校验值 K2_Mac（8 字节）、随机数 r2（16 字节），会话 ID d1。K1_Enc 和 K2_Enc 都是由对应的 OBU 终端证书公钥进行 SM2 加密，密钥生成过程必须在硬件密码设备内部完成，校验值是工作密钥明文对 16 字节 0 做 SM4 加密，取前 8 字节；

8） 处理中心使用私钥对(M2+M1)进行签名，得到签名值 S2，其中 M2=（K1_Enc + K1_Mac + K2_Enc + K1_Mac + r2 +d1)；

9） 处理中心发送响应 R2（R2=M2+S2）给移动终端 APP；

10） 移动终端 APP 向 B-OBU 转发响应；

11） B-OBU 通过 SE 的 APDU 命令对签名 S2 进行验证，如果验证不通过，则产生错误，同时结束退出，否则继续；

12） B-OBU 将 K1_Enc、K1_Mac、K2_Enc、K2_Mac 导入 SE，B-OBU 和 SE 应按以下流程进行处理：

a） 终端导入工作密钥密文 K1_Enc+工作密钥校验值 K1_Mac 到 SE；

b） SE 使用终端私钥解密工作密钥，得到工作密钥明文，使用工作密钥明文对 16 字节 0x00 做 SM4 加密，取加密结果前 8 字节作为工作密钥校验值，并与终端输入的校验值比对，若一致，则将工作密钥保存到 SE 安全区域，否则结束退出；

c） 终端导入 MAC 密钥密文 K2_Enc +MAC 密钥校验值 K2_Mac 到 SE；

d） SE 使用终端私钥解密 MAC 密钥，得到 MAC 密钥明文，使用 MAC 密钥明文对 16 字节 0x00 做 SM4 加密，取加密结果前 8 字节作为 MAC 密钥校验值，并与终端输入的校验值比对，若一致，则将 MAC 密钥保存到 SE 安全区域，否则结束退出。

13） 认证流程完成，后续每次通讯消息均采用密文+MAC 的方式进行。

4 B-OBU 在互联网通信的典型应用是圈存应用，其流程见附录 A.1 规定。

5 B-OBU 工作密钥包含工作密钥 K1 与 MAC 密钥 K2，K1、K2 有效性截止到下一次 B-OBU 工作密钥导入或 SE 下电。

6 交易命令报文使用工作密钥 K1 加密，以确保报文数据的保密性，加密方法应符合 A.1.2 的规定。

7 使用 MAC 密钥 K2 计算交易命令密文的 MAC，以确保报文数据的完整性与不可篡改性。计算 MAC 的方法应符合下列规定：

1） 将处理中心随机数 r2（16 字节）作为计算 MAC 的初始值；

2） 将 ENC_SM4(K1,msg)分成 16 字节为单位的数据块， 表示为 BLOCK1、BLOCK2、 BLOCK3、BLOCK4 等。最后的数据块有可能是 1~16 个字节；

3） 如果最后的数据块的长度是 16 字节的话，则在该数据块之后再加一个完整的 16 字节数据块 0x80000000000000000000000000000000’，转到第五步；

4） 如果最后的数据块的长度不足 16 字节，则在其后加入 0x80，如果达到 16 字节长度，则转到第五步；否则接着在其后加入 0x00 直到长度达到 16 字节；

5） 按图 11 所示的算法对这些数据块使用指定密钥进行加密来产生 MAC；

6） 最终取计算结果高 4 字节作为 MAC。

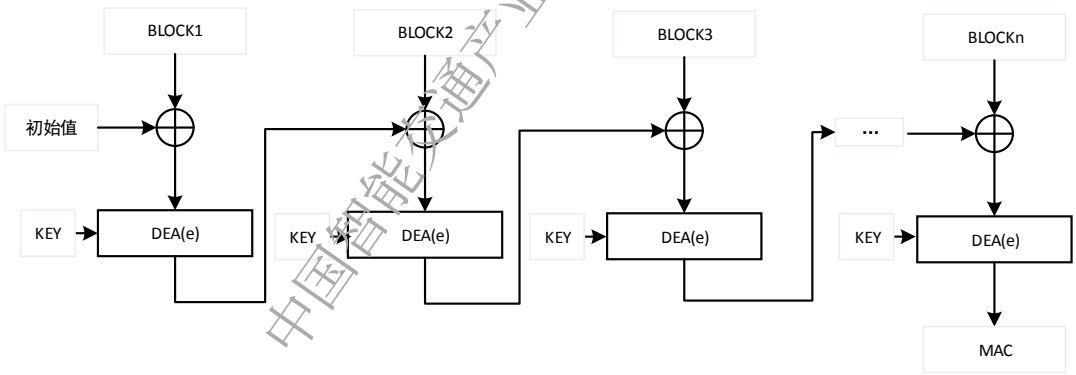

图11 通讯消息报文中的 MAC 算法

附 录 A

（规范性附录）

B-OBU

A.1 主要业务流程

A.1.1 圈存流程

圈存流程参照图 A-1 所示。

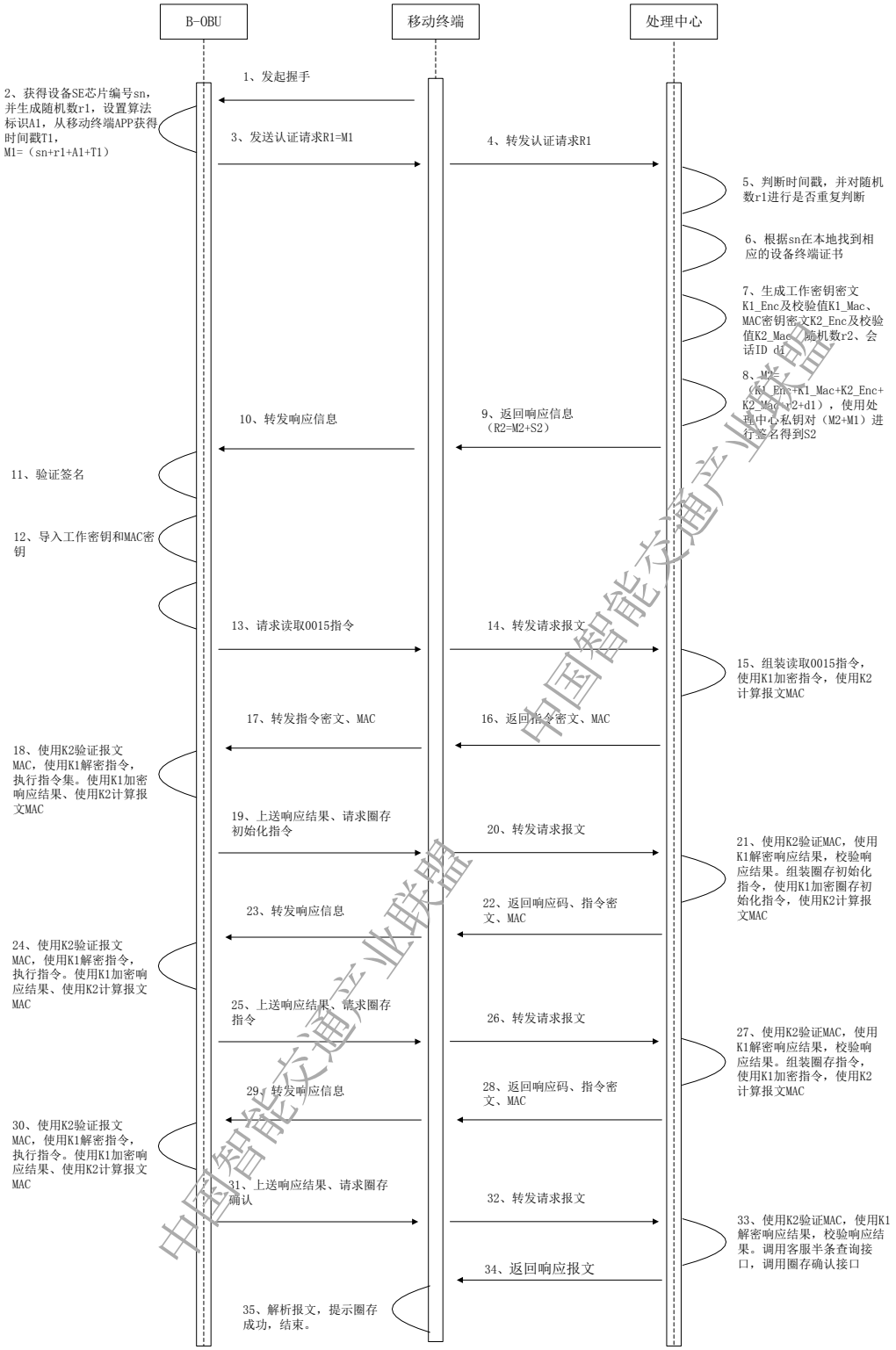

图 A 1 圈存流程

A.1.2 车路通信流程

车路通信场景是通过 RSU 与移动终端 APP 通过 B-OBU 建立逻辑通信链路。RSU 与 B-OBU 通过 5.8GHz DSRC 建立通信链路，B-OBU 与移动终端通过 BLE 建立通信链路，B-OBU 作为数据转发通道

设备。

在车路通信应用中，RSU 可推送消息到移动终端显示提醒，也可读取移动终端内的应用相关数据。在读取移动终端的数据时，移动终端返回数据的时延存在不可预期性，为保证高速通行状态下的一次交易成功率，将 RSU 读取移动终端数据的流程分为两种通道类型：实时通道和非实时通道。

车路通信实时通道的流程如图 A-2 所示。B-OBU 收到 RSU 发来的读取移动终端数据的实时通道类型消息后，应将消息转发给移动终端，并等待移动终端响应，之后将响应内容返回给 RSU。B-OBU 应支持超时功能，在一段时间内没有收到移动终端响应时，应向 RSU 返回超时消息。超时时间和消息在 DSRC 相关标准中定义。

车路通信非实时通道的流程如图 A-3 所示，非实时通道时，B-OBU 收到 RSU 转发给移动终端 APP 的指令时，应主动打开蓝牙模块并与移动终端 APP 建立链接。B-OBU 收到 RSU 发来的读取移动终端数据的非实时通道类型消息后，B-OBU 应将 RSU 到 B-OBU 的交互过程和 B-OBU 到移动终端的交互过程通过 B-OBU 的缓存隔离，保证响应及时性。缓存数据的时效、内容、类型，由应用层自行解析。

车路通信流程中对 5.8GHz DSRC 协议的扩展，在 GB/T 20851 相关标准中定义。

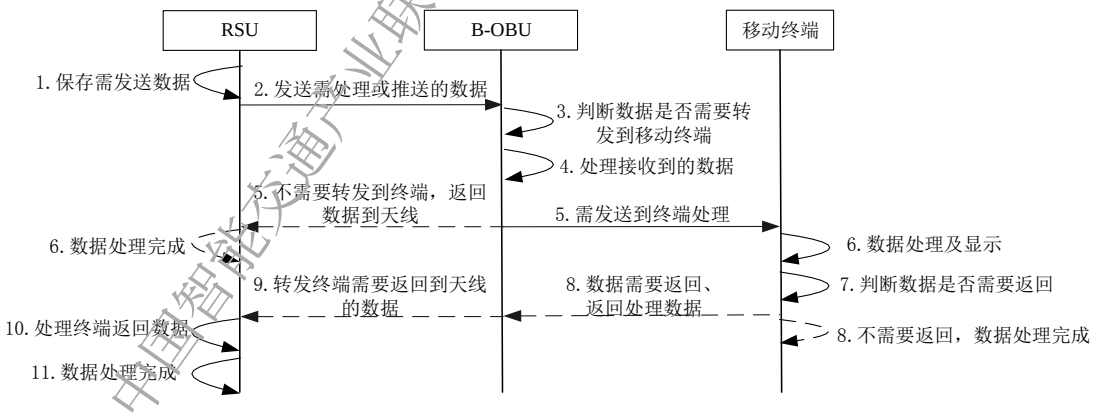

图 A2 实时通道车路通信流程

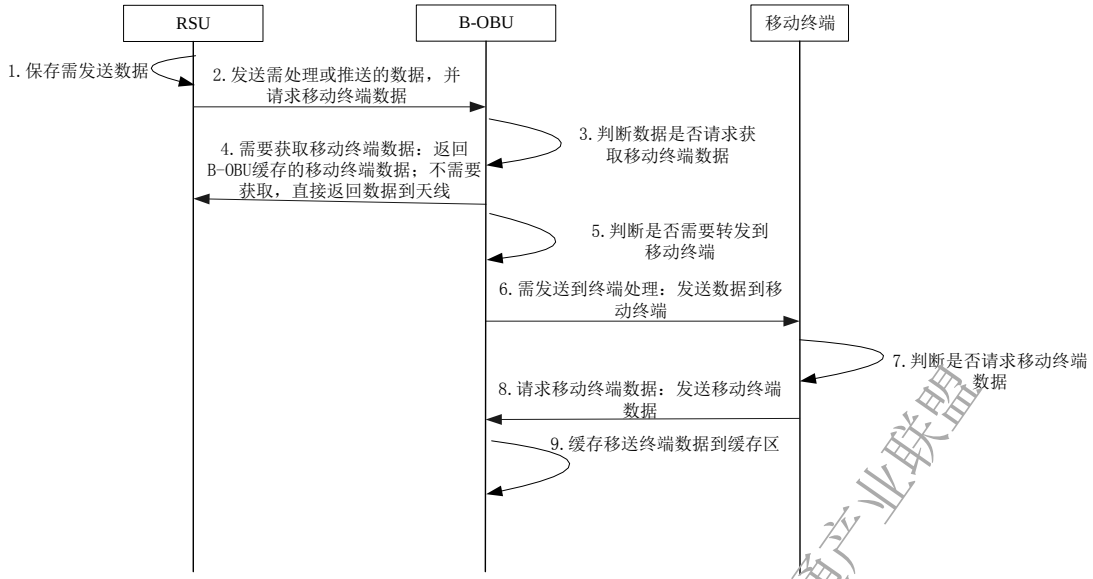

图 A3 非实时通道车路通信流程

A.1.3 移动终端APP与B-OBU信息交互流程

移动终端APP与B-OBU信息交互见图A-4所示。

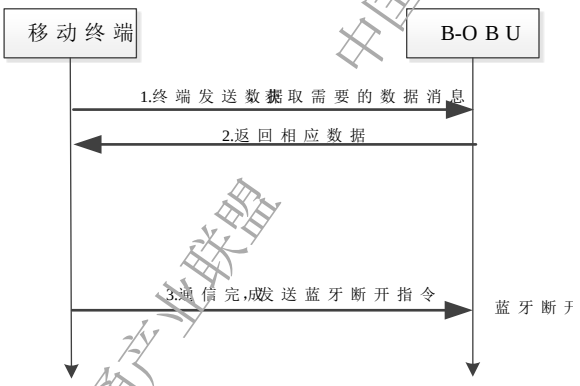

图 A4 移动终端与 B-OBU 会话基本流程

A.2 TLV格式

TLV 格式应符合下列规定：

1 TAG

固定一个字节。嵌套表示，0x80 表示 cmd，其对应的 value 为用户卡指令 TPDU 的合集。0x81 表示 resp，其对应的 value 为用户卡响应的合集，tag 对应每条 TPDU 指令的 tag。

TPDU 指令的 tag 的低 4 位从 0x01 增长，表示用户卡 TPDU 指令和回复的序号，表示执行和回复顺序，高 4 位具有特殊含义，具体见表 A-1：

表 A 1　TAG 数据格式规定

bit	说明
7	1：不返回执行结果；0：返回
6	1：执行失败时继续执行下一条指令；0：执行失败时不继续
5	保留
4	保留
3	指令和执行结果的序号
2	
1	
0	

2　LEN

变长表示。当需表示的长度小于 0x80 时，占一个字节，直接表示长度。当需表示的长度大于 0x80 时，变长表示，用 0x80+n 来表示后续 n 个字节代表长度。

示例：

1）　表示 0x77，LEN=0x77

2）　表示 0x88，LEN=0x81 0x88

3）　表示 0x0156，LEN=0x82 0x01 0x56

3　VAULE

值域，长度由 LEN 指定。

4　数据示例

1）　Cmd 示例

0x80 + LENc + 0x01 len1 tpdu1 + 0x02 len2 tpdu2 + 0x03 len3 tpdu3....

其中 LENc 指后续所有字节的长度；tpdu1、tpdu2 就是需要透传给用户卡的指令，设备将根据 TAG0x01,0x02 的序列号，按顺序发送给用户卡。

2）　RESP 示例

0x81 + LENr + 0x01 len1 resp1 + 0x02 len2 resp2 + 0x03 len3 tpdu3...

说明：

RESP 的 tpduID1、tpduID2、tpduID3 分别和 Cmd 的 tpduID1、tpduID2、tpduID3 相等，表示 Tpdu 指令和卡返回的 tag；

LENc　和 LENr 指后续所有字节的长度；

lenc1、lenc2 是 tpdu1、tpdu2 的长度；Lenr1、Lenr2 是 resp1、resp2 的长度，resp1、resp2 是 tpdu1、tpdu2 发给用户卡的返回数据；

一个命令包的长度不超过 384 字节。

错误码应符合表 A-2 的规定：

表 A 2　错误码规定

代码	说明
81	通信超时
83	通信错误
91	不支持的参数
93	数据分包错误
A0	卡类型错误
A1	其他错误
CF	执行失败
E1	比较错误(验签未通过)
E2	不支持的命令/无效命令
E3	无法读取卡片
EC	验证错误
F0	收到的位数错误
F5	收到的字节错误
F6	BCC 错误
F7	CRC 错误
F8	FIFO 溢出错误
FA	奇偶校验错误
FB	位冲突错误
FC	无应答错误
FD	访问超时
FF	数据长度错误
01	电量不足
02	升级中断
03	设备故障

A.3 参数设置规范

1 本标准延时设定基于蓝牙连接间隔为 20ms 的情况。

2 保活定时器 T1 用于发送端确认数据链路处于正常通讯状态，要求发送端每 60 个包检查是否收到 F1。

3 保活定时器 T2 用于接收端确认数据链路处于正常通讯状态，默认参考值宜设置为 1200ms，T2 定时器的最低值宜不低于 600ms。

注：针对 IOS 平台 30ms 的连接间隔，T2 默认参考值 1800ms,最低不低于 900ms。

4 触发计数器 T3 用于接收端在成功收到指定数量的数据包时返回临时响应帧以保持数据链路正常通讯。触发计数器 T3 要求至少在累计收到 30 个数据包时触发一次。建议每 10 个数据包回复一次临时响应帧。

5 重传定时器 T4 用于发送端收到重传响应指令 F2 时的数据重发超时。超时时间建议设置为 200ms。最低宜不低于 100ms。发送端每收到一次 F2 需要对 T4 进行重置。

注：针对 IOS 平台 30ms 的连接间隔。T4 默认参考值 300ms，最低不低于 150ms。

6 重传定时器 T5 用于发送端发送最后一帧数据时等待结束包应答指令 F3 的数据重发超时。超时时间宜设置为 200ms，最低宜不低于 100ms。

注：针对 IOS 平台 30ms 的连接间隔。T4 默认参考值 300ms，最低不低于 150ms。

附 录 B

（规范性附录）

SE 模块

B.1 一般规定

B.1.1 SE的基本功能规定

SE 的基本功能应符合下列规定：

1 支持多应用，各应用之间相互独立；

2 支持多种文件类型，包括二进制文件、定长记录文件、变长记录文件、循环文件；

3 在通讯过程中支持多种安全保护机制（信息的机密性和完整性保护）；

4 支持多种安全访问方式和权限（认证功能和口令保护）；

5 支持 SM2、SM3、SM4 算法。

B.1.2 SE的基本参数规定

SE 的基本参数应符合下列规定：

1 非易失性存储器容量应不低于 32Kbytes；

2 卡片应支持 T=0 通信协议；

3 电源电压应支持 1.8V 和 3V 工作电压；

4 卡片工作温度宜为-25℃～+70℃，寒区宜为-40℃～+70℃。存储温度为宜-40℃～+85℃。相对工作湿度宜为 10%～95%；

5 外部工作时钟频率不低于 7.5MHz；

6 其他物理特性、电气特性应符合《识别卡 带触点的集成电路卡》（GB/T 16649）的规定；

7 安全等级应达到《安全芯片密码检测准则》（GM/T 0008）规定的 2 级及以上级别。

B.2 SE模块数据格式

B.2.1 文件结构图

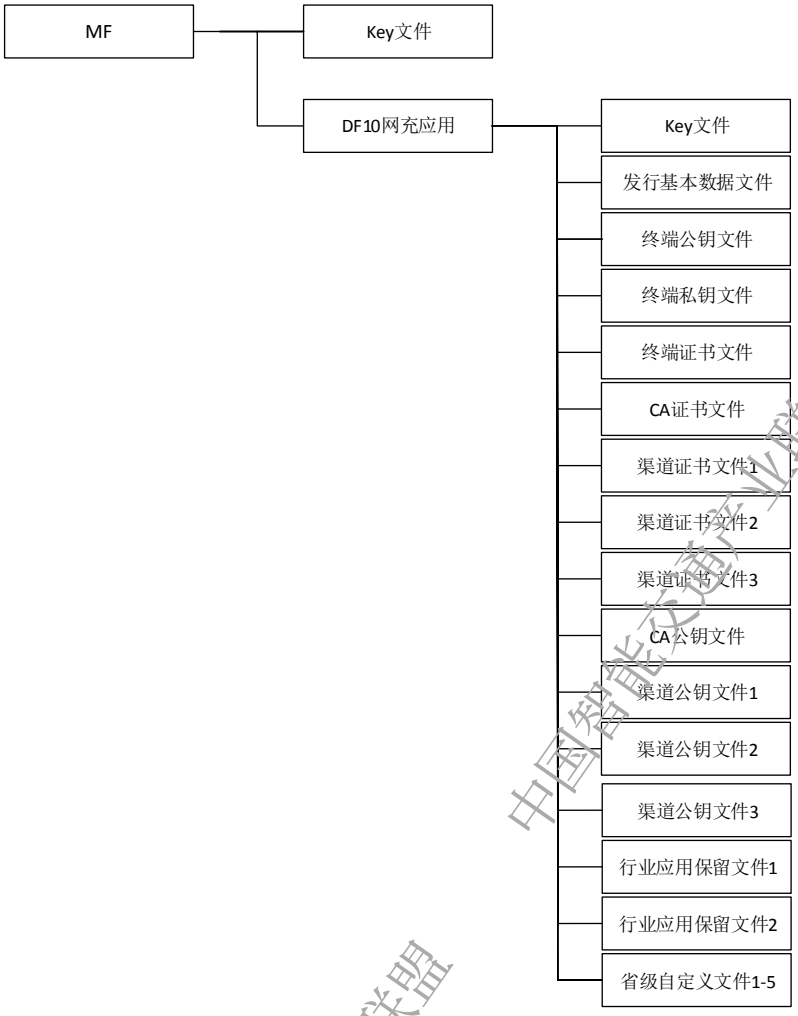

图 B 1 SE 文件结构图

B.2.2 详细文件结构

表 B 1 SE 详细文件结构

文件名称	文件类型	文件标识符	读权	写权
MF	主文件	3F00	建立权：$MK_{\_MF}$	
密钥文件	密钥文件	--	禁止	增加密钥权：$MK_{\_MF}$
网充应用目录	目录文件	DF10	建立权：$MK_{\_MF}$	擦除权：$MK_{\_MF}$
密钥文件	密钥文件	--	禁止	增加密钥权：$MK_{\_DF10}$
发行基本数据文件	二进制文件	EF01	自由	$DAMK_{\_DF10}$（密文+ MAC）
终端公钥文件	二进制文件	EF02	自由	UK1_DF10（外部认证）
终端私钥文件	私钥文件	EF03	禁止（COS 保证）	使用权限：自由； 更新权限： 外部认证密钥 $UK1_{\_DF10}$ 认证成功后可通过生成公私钥对指令写入，不能用写文件指令更新。
终端证书文件	二进制文件	EF04	自由	$DAMK_{\_DF10}$（密文+ MAC）

表 B.1　SE 详细文件结构（续）

CA 证书文件	二进制文件	EF05	自由	DAMK_DF10（密文+ MAC）
渠道证书文件 1	二进制文件	EF06	自由	DAMK_DF10（密文+ MAC）
渠道证书文件 2	二进制文件	EF07	自由	DAMK_DF10（密文+ MAC）
渠道证书文件 3	二进制文件	EF08	自由	DAMK_DF10（密文+ MAC）
CA 公钥文件	二进制文件	EF09	自由	DAMK_DF10（密文+MAC）
渠道公钥文件 1	二进制文件	EF0A	自由	DAMK_DF10（密文+MAC）
渠道公钥文件 2	二进制文件	EF0B	自由	DAMK_DF10（密文+MAC）
渠道公钥文件 3	二进制文件	EF0C	自由	DAMK_DF10（密文+MAC）
行业应用保留文件 1	二进制文件	EF0D	自由	DAMK_DF10（密文+MAC）
行业应用保留文件 2	二进制文件	EF0E	自由	DAMK_DF10（密文+MAC）
省级自定义文件 1-5	省内自定义	EF1A-EF1E	省内自定义	省内自定义

B.2.3　对称密钥文件说明

1　MF 下密钥文件

表 B.2　MF 下对称密钥文件结构

密钥名称	密钥标识	密钥长度	算法标识	错误计数器	备注
系统主控密钥 MK_MF	00	10H	04	9	SM4 算法

说明：

1.　系统主控密钥在自身的线路保护控制下更新（密文+MAC）。

2.　DF10 下密钥文件的应用主控密钥在系统主控密钥的线路保护控制下装载。

2　DF10 网充应用目录下对称密钥文件

表 B.3　DF10 网充应用目录下对称密钥文件结构

密钥名称	密钥标识	密钥长度	算法标识	错误计数器	备注
应用主控密钥 MK_DF10	00	10H	04	9	SM4 算法
应用维护子密钥 DAMK_DF10	00	10H	04	9	SM4 算法
外部认证密钥 UK1_DF10	01	10H	04	9	SM4 算法

说明：

1.　应用主控密钥在系统主控密钥的线路保护控制下装载（密文+MAC）。

2.　应用主控密钥在自身的线路保护控制下更新（密文+MAC）。

B.2.4　发行基本数据文件（EF01）说明

表 B.4　发行基本数据文件（EF01）结构

字节	数据项	长度（字节）	备注
1～8	发卡方标识	8	与 OBE-SAM 编码规则一致
9	规范版本号	1	高 4 位：行业统一定义，当前定义为 0001； 低 4 位：由各省根据需要自定义
10～17	SE 芯片编号	8	见表 B-5 SE 芯片编号编码规则
18～21	启用时间	4	年月日 YYYYMMDD
22～45	保留	24	不使用，用 0xFF 填充

表 B.5　SE 芯片编号编码规则

字节	数据项	长度（字节）	说明
1	区域代码	1	省代码，压缩 BCD 码
2	应用类别	1	高 4 位：行业保留 低 4 位：省内自定义
3	终端类型	1	0x00 代表蓝牙 OBU 0x01-0x0F：行业保留 0x10-0xFF：省内自定义
4	芯片厂商代码	1	由发行方自行编码
5～8	顺序号	4	SE 芯片序列号

B.2.5　终端公钥文件（EF02）说明

表 B.6　终端公钥文件结构

字节	数据项	长度（byte）	备注
1～64	终端公钥	64	

B.2.6　终端私钥文件（EF03）说明

表 B.7　终端私钥文件结构

字节	数据项	长度（byte）	备注
1～32	终端私钥	32	

B.2.7　终端证书文件（EF04）结构说明

表 B.8　终端证书文件结构

字节	数据项	长度	备注
1～2	证书长度	2 字节	
3～1536	证书内容	1534 字节	

B.2.8　CA证书文件（EF05）结构说明

表 B.9　CA 证书文件结构

字节	数据项	长度	备注
1～2	证书长度	2 字节	
3～1536	证书内容	1534 字节	

B.2.9　渠道证书文件（EF06、EF07、EF08）结构说明

表 B-.10　渠道证书文件 1-3 结构

字节	数据项	长度	备注
1～2	证书长度	2 字节	
3～1536	证书内容	1534 字节	

B.2.10　CA公钥文件（EF09）及渠道公钥文件（EF0A、EF0B、EF0C）说明

表 B.11　CA 公钥文件及渠道公钥文件 1-3 结构

字节	数据项	长度	备注
1～64	终端公钥	64 字节	

B.2.11　行业应用保留文件1-2（EF0D、EF0E）结构说明

表 B.12　行业应用保留文件 1-2 结构

字节	数据项	长度	备注
1～1536	保留	1536 字节	

B.2.12　省级自定义文件（EF1A、EF1B、EF1C、EF1D、EF1E）结构说明

表 B.13　省级自定义文件 1-5 结构

文件存取控制	读：省内自定义	写：省内自定义	文件大小：省内自定义
字节	数据项	长度	备注
省内自定义	省内自定义	省内自定义	省内自定义

B.3　SE模块应用命令集

SE 模块除应支持 B.2.1-B.2.10、B.2.12、B.2.14 和 D.2.4 所定义的命令外，还应支持下列命令：

B.3.1　Generate Key Pair(SM2)（生成密钥对）

1　定义与范围

Generate Key Pair(SM2)命令用于生成基于 SM2 算法的公私钥对。

2　注意事项

需要满足报文数据中指定的公私钥文件的修改权限。

3　命令报文

表 B.14　Generate Key Pair 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	CE	-
P1	1	00	-
P2	1	00	-
Lc	-	04	--
DATA	-	xxxx	公钥文件 ID+私钥文件 ID
Le	1	00/40	需要取回的公钥长度

4　命令报文数据域

命令报文的数据由 2 个字节公钥文件 ID + 2 个字节的私钥文件 ID。

当公钥 ID 为 0x0000 时，公钥可以通过 Get Response 指令取回。

当公钥 ID 非 0x0000 时，直接写入公钥文件，不从指令返回。

5　响应报文数据域

响应报文数据包括随机数，长度为 Le 个字节。

6　响应报文状态码

表 B.15　响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6700	长度错误
61XX	需要通过 Get Response 指令取回的公钥数据
6581	Flash 操作失败
6981	文件类型不匹配
6982	权限不足
6A82	文件不存在
6A86	P1P2 错误

B.3.2　Data Encrypt(SM2)（公钥加密数据）

1　定义与范围

使用指令的卡片内公钥或者外部传入的公钥对数据进行非对称(SM2 算法)的加密。

使用内部公钥，需要满足公钥文件的使用权限。

2　命令报文

表 B.16　Data Encrypt 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	—
INS	1	C4	—
P1	1	00	P1P2 大数据传输控制字。见【说明 1】
P2	1	00	
Lc	1	xx	（2 或 66）+待加密数据长度
DATA	-	xxxx	
Le	1	xx	加密后的密文

【说明 1】：P1P2 传输控制字说明

表 B.17　P1P2 传输控制字说明

P1								P2								含义
B8	B7	B6	B5	B4	B3	B2	B1	B8	B7	B6	B5	B4	B3	B2	B1	
0	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	首块
X	x	1	1	1	1	1	1	1	1	1	1	1	1	1	1	有后续块
X	X	数据总长度（不全为 1 时，则为最后一块数据）														最后一块

3　命令报文数据域

✧　报文数据域由：公钥文件 ID（2 字节）+(公钥)+待加密数据组成。

■　当公钥文件 ID = 0x0000 时

数据域 =公钥文件 ID（2 字节）+ 公钥(64 字节) + 待加密数据 组成

■　当公钥文件 ID != 0x0000 时

数据域 =公钥文件 ID（2 字节）+ 待加密数据 组成

注：待加密数据长度要小于等于 158 字节。

4　响应报文数据域

✧　响应报文为公钥加密(SM2)后的密文,密文格式为：

C1（X，Y） + C3（Hash） + 密文长度（即要加密的数据长度，用 4 字节表示） + C2。

5　响应报文状态码

表 B.18　响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6700	长度错误
61XX	需要通过 Get Response 指令取回的密文

表 B.18　响应报文状态码（续）

6981	文件类型不匹配
6982	权限不足
6A82	文件不存在
6A84	数据接收缓冲区超限
6A86	P1P2 错误

B.3.3　Data Decipher(SM2)（数据解密SM2）

1　定义和范围

Data Decipher 命令用于非对称国密算法(SM2)的私钥对数据进行解密。

使用内部私钥时，需满足私钥文件的使用权限。

2　命令报文

表 B.19　Data Decipher 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	C8	-
P1	1	00	P1P2 大数据传输控制字。 见【说明 1】
P2	1	00	
Lc	1	xx	2+待解密数据长度总和
DATA	-	xxxx	
Le	1	xx	解密后的明文

【说明 1】：P1P2 传输控制字说明

表 B.20　P1P2 传输控制字说明

P1								P2								含义
B8	B7	B6	B5	B4	B3	B2	B1	B8	B7	B6	B5	B4	B3	B2	B1	
0	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	首块
X	x	1	1	1	1	1	1	1	1	1	1	1	1	1	1	有后续块
X	X	数据总长度（不全为 1 时，则为最后一块数据）														最后一块

3　命令报文数据域

✧　报文数据域由：私钥文件 ID（2 字节）+待解密数据组成。

待解密数据格式应为：

C1（X，Y）+C3（Hash）+ 密文长度（即要加密的数据长度，用 4 字节表示）+C2。

4　响应报文数据域

非对称密钥（SM2）解密后的明文。

5　响应报文状态码

表 B.21　响应报文状态码

状态字(HEX)	描述
9000	数据正确接受
6E00	CLA 不支持
6700	长度错误
61XX	需要通过 Get Response 指令取回解密后的明文
6981	文件类型不匹配
6982	权限不足
6A80	输入数据格式错误
6A82	文件不存在
6A84	数据接收缓冲区超限
6A86	P1P2 错误

B.3.4　Data Verify(SM2)（公钥验证签名）

1　定义与范围

使用指令的卡片内公钥或者外部传入的公钥对数据进行（SM2 算法）的验证签名。

使用内部公钥，需要满足公钥文件的使用权限。

2　命令报文

表 B.22　Data Encrypt 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	C6	-
P1	1	00	P1P2 大数据传输控制字。见【说明 1】
P2	1	00	
Lc	1	xx	-
DATA	-	xxxx	公钥文件(2Byte)+(公钥)+签名后的数据+原始数据
Le	-	-	-

【说明 1】：P1P2 传输控制字说明

表 B.23　P1P2 传输控制字说明

P1								P2								含义
B8	B7	B6	B5	B4	B3	B2	B1	B8	B7	B6	B5	B4	B3	B2	B1	
0	X	1	1	1	1	1	1	1	1	1	1	1	1	1	1	首块数据
1	x	1	1	1	1	1	1	1	1	1	1	1	1	1	1	中间块数据
1	X	数据总长度（不全为 1 时，则为最后一块数据）														最后一块数据

3　命令报文数据域

✧ 报文数据域由：公钥文件 ID（2 字节）+ (公钥 64 字节) + 签名后的值（64 字节）+ 原始数据。

■ 当公钥文件 ID = 0x0000 时

数据域 = 公钥文件 ID（2 字节）+ 公钥(64 字节) + 签名后的值（64 字节）+ 原始数据 组成

■ 当公钥文件 ID != 0x0000 时

数据域 = 公钥文件 ID（2 字节）+ 签名后的值(64 字节) + 原始数据 组成

4 响应报文数据域

无

5 响应报文状态码

表 B.24 响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6700	长度错误
6881	验签失败
6981	文件类型不匹配
6982	权限不足
6A82	文件不存在
6A84	数据接收缓冲区超限
6A86	P1P2 错误

B.3.5 Data Sign(SM2)（私钥签名）

1 定义与范围

使用指令的卡片内私钥或者外部传入的私钥对数据进行（SM2 算法）的签名。

使用内部私钥，需要满足私钥文件的使用权限。

2 命令报文

表 B.25 Data Encrypt 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	C2	-
P1	1	00	P1P2 大数据传输控制字。见【说明 1】
P2	1	00	
Lc	1	xx	-
DATA	-	xxxx	私钥文件(2Byte)+(私钥)+待签名数据
Le	X	Xx	签名后的值

【说明 1】：P1P2 传输控制字说明

表 B.26　P1P2 传输控制字说明

B8	B7	B6	B5	B4	B3	B2	B1	B8	B7	B6	B5	B4	B3	B2	B1	含义
0	X	1	1	1	1	1	1	1	1	1	1	1	1	1	1	首块数据
1	x	1	1	1	1	1	1	1	1	1	1	1	1	1	1	中间块数据
1	X	数据总长度（不全为 1 时，则为最后一块数据）														最后一块数据

3　命令报文数据域

✧　报文数据域由：私钥文件 ID（2 字节）+ (私钥 32 字节) + 待签名数据

■　当私钥文件 ID = 0x0000 时

数据域 = 私钥文件 ID（2 字节）+ 私钥(32 字节)　+待签名数据 组成

■　当公钥文件 ID != 0x0000 时

数据域 = 私钥文件 ID（2 字节）+ 待签名数据 组成

4　响应报文数据域

✧　签名后值

5　响应报文状态码

表 B.27　响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6700	长度错误
61xx	正确执行 XX 标识剩余数据长度。 （仅用于 T=0）
6981	文件类型不匹配
6982	权限不足
6A82	文件不存在
6A84	数据接收缓冲区超限
6A86	P1P2 错误

B.3.6　Import Key（导入非对称密钥）

1　定义与范围

本指令可以将 SM2 的公私密钥写入指定的密钥文件中。

2　注意事项

需要满足非对称密钥文件写权限时才能执行此命令。

3　命令报文

表 B.28　Import Key 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	00/04	-
INS	1	C3	-
P1	1	XX	【说明 1】
P2	1	XX	【说明 1】
Lc	1	XX	【说明 2】
DATA	XX	XX…XX	写入文件的数据
Le	-	-	不存在

【说明 1】:

若 P1 的高三位为 100，则低 5 位为短的文件标识符，P2 为欲读文件的偏移量。

表 B.29　报文编码说明（P1 高三位为 100）

P1								P2
b7	b6	b5	b4	b3	b2	b1	b0	
1	0	0	短文件标识符					文件的偏移量

若 P1 的最高位不为 1，则 P1 P2 为欲写文件的偏移量，所写的文件为当前文件。

表 B-30　报文编码说明（P1 最高位不为 1）

P1								P2
b7	b6	b5	b4	b3	b2	b1	b0	
0	文件的偏移量							

【说明 2】:

Lc 标识要写入的字节数:

——若为线路保护，Lc 为写入数据的长度+4 字节 MAC。

——若为加密线路保护，Lc 为加密后数据的长度+4 字节 MAC。

4　命令报文数据域

✧ 报文数据包括要写入的新数据。

✧ 若为线路保护文件数据域应包含 4 字节 MAC 码。

✧ 若为线路保护文件数据域应包含加密后的数据及 4 字节 MAC 码。

✧ 用维护密钥加密数据和计算 MAC，方法见“安全报文传送”。

5　响应报文数据域

无

6　响应报文状态码

表 B.31　响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6700	长度错误
6581	Flash 操作失败
6981	文件类型不匹配
6982	权限不足
6983	密钥锁定
6984	未取随机数
6A82	文件不存在
6A84	文件偏移量超出
6A86	P1P2 错误

B.3.7　Export Key（导出非对称密钥）

1　定义与范围

本指令可以将 SM2 的公钥以明文方式或者线路保护方式导出 SE。需要满足公钥文件的读取权限。

2　命令报文

表 B.32　Export Key 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	00/04	-
INS	1	C5	-
P1	1	XX	【说明 1】
P2	1	XX	【说明 1】
Lc	1	-	不存在（CLA=04 时除外）
DATA	XX	-	不存在（CLA=04 时，应包括 MAC）
Le	1	XX	要读取的数据长度

【说明 1:】

若 P1 的高三位为 100，则低 5 位为短的文件标识符，P2 为读的偏移量

表 B.33　报文编码说明（P1 高三位为 100）

P1								P2
b7	b6	b5	b4	b3	b2	b1	b0	
1	0	0	短文件标识符					文件的偏移量

若 P1 的最高位不为 1，则 P1 P2 为欲读文件的偏移量，所读的文件为当前文件。

表 B.34　报文编码说明（P1 最高位不为 1）

P1								P2
b7	b6	b5	b4	b3	b2	b1	b0	
0	文件的偏移量							

3　命令报文数据域

✧　一般情况下，命令报文数据域不存在。

✧　当使用安全报文时，命令报文数据域中应包含 MAC。

✧　用维护密钥加密数据和计算 MAC，方法见“安全报文传送”。

4　响应报文数据域

✧　响应报文数据域由读取的数据组成。

✧　若为线路保护则由读取的数据附上 4 字节 MAC 组成。

✧　若为线路加密保护则由被加密过的数据附上 4 字节 MAC 码组成。

5　响应报文状态码

表 B.35　响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6700	长度错误
61xx	正确执行 XX 标识响应数据长度。 可用 Get Response 命令取回响应数据（仅用于 T=0）
6581	Flash 操作失败
6981	文件类型不匹配
6982	权限不足
6983	密钥锁定
6984	未取随机数
6988	Mac 错误
6A81	不支持此功能
6A82	文件不存在
6A84	文件偏移量超出
6CXX	Le 长度错误
9403	密钥不存在

B.3.8　Import Session key(公钥SM2导入对称密钥)

1　定义与范围

Import Session key 使用非对称算法的公钥对对称密钥加密后导入卡片内部，成功导入后可以通过 Session Ope 指令，根据不同的算法标识调用不同的对称算法对输入的数据进行加密/解密以及计算 MAC 操作。

2　命令报文

表 B.36　Import Session key 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	D5	-
P1	1	00	P1P2 私钥 ID，为 0x0000 时，采用外部传入私钥。
P2	1	00	
Lc	1	xx	-
DATA	-	xxxx	算法标识+密钥类型+私钥+公钥加密的对称密钥+密钥校验值
Le	-	-	-

3　命令报文数据域

对称算法标识+密钥类型+私钥+公钥加密后的对称密钥密文（SM2 加密固有 96 字节密文+4 字节对称密钥密文长度+对称密钥密文）+密钥校验值

对称算法标识如下：

表 B.37　对称算法标识

对称算法标识	HEX 值
3DES	0x00
SM4	0x04

密钥类型如下：

表 B.38　密钥类型

密钥类型	HEX 值
工作密钥	0x00
Mac 密钥	0x01

密钥校验值为密钥明文用对称算法标识指定的对称算法对一个全零数据块加密所得结果的前 8 字节数据。

4　响应报文数据域

无

5　响应报文状态码

表 B.39　响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6981	文件类型不匹配
6982	私钥使用权限不足
6A80	密钥长度错误
6A81	密钥校验失败
6A82	文件不存在
6A83	密钥类型错误

B.3.9　Export Session key(公钥SM2导出对称密钥)

1　定义与范围

Export Session key 根据外部传入的对称算法算法标识，生成对称密钥并通过外部传入公钥或者卡片内部公钥导出公钥加密后的对称密钥密文。成功导出后可以通过 Session Oper 指令，通过不同的算法标识调用不同的对称算法对输入的数据进行加密/解密以及计算 MAC 操作。

2　命令报文

表 B.40　Export Session key 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	D8	-
P1	1	00	P1P2 公钥 ID，为 0x0000 时，采用外部传入公钥。
P2	1	00	
Lc	1	xx	-
DATA	-	xxxx	算法标识+（公钥）
Le	-	-	-

3　命令报文数据域

P1P2 = 0x0000：对称算法标识+密钥类型+公钥。

P1P2 != 0x0000：对称算法标识+密钥类型。

4　响应报文数据域

无

5　响应报文状态码

表 B.41　响应报文状态码

状态字(HEX)	描述
9000	指令执行成功
6E00	CLA 不支持
6700	长度错误
61XX	通过 Get Response 指令回去对称密钥密文
6981	文件类型不匹配
6982	权限不足
6A80	数据内容错误
6A82	文件不存在

B.3.10　Session Oper（对称密钥加密、解密、MAC计算）

1　定义与范围

Session Oper 使用 Import Session Key 或者 Export Session key 指令导入或者生成的会话密钥，来对数据进行加密、解密、计算 MAC。

2　命令报文

表 B.42　Session Oper 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	D7	-
P1	1	XX	算法控制字（见:【说明 1】）
P2	1	00	-
Lc	1	xx	-
DATA	-	xxxx	数据
Le	-	-	不存在

【说明 1】

P1 应用控制参数说明：

表 B.43　P1 应用控制参数说明

BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0	含义
						0	0	加密
						1	0	解密
						0	1	计算 MAC
				0	0	X	X	唯一一组数据块（计算 MAC 时第一个数据块为初始向量）
				0	1	X	X	第一组数据块（计算 MAC 时第一个数据块为初始向量）
				1	0	X	X	中间数据块
				1	1	X	X	最后一组数据块

3　命令报文数据域

✧ 加密解密

欲执行加解密操作的数据，必须为所执行加解密算法分组长度的整数倍。

✧ Mac 计算

欲执行 Mac 计算的数据。

4 响应报文数据域

✧ 加密结果、解密结果或 MAC。

5 响应报文状态码

表 B.44 响应报文状态码

状态字(HEX)	描述
9000	指令执行成功
6E00	CLA 不支持
6700	长度错误
61XX	通过 Get Response 获取相应数据
6901	会话密钥类型错误
6986	P1P2 错误
6A86	P1P2 错误

B.3.11 Hash Asymc（摘要&签名/验签）

1 定义与范围

对输入数据做摘要操作和签名验签操作。

2 命令报文

表 B.45 Hash Asymc 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	—
INS	1	CD	—
P1	1	XX	00：计算 Hash，返回 Hash 结果 01：计算 Hash&签名，返回 Hash&签名结果 02：计算 Hash&验签，返回 Hash&验签结果
P2	1	XX	Bit0：0：SHA1+RSA Bit0：1：SM3+SM2 Bit7-6：00：唯一一包 Bit7-6：01：第一包 Bit7-6：10：中间包 Bit7-6：11：最后一包 Bit5-1：保留
Lc	1	XX	—
DATA	XX	XX….XX	要处理的数据
Le	1	00	—

3　命令报文数据域

➢ 当 P2 Bit0 为 1 时（SM3+SM2）

第一包或唯一一包数据：

■ P1=0：待 Hash 数据。

■ P1=1：私钥文件 ID（2 字节）+公钥文件 ID（2 字节）+用户标识长度（1 字节）+ 用户标识（n 字节） + 待签名数据。

■ P1=2：公钥文件 ID（2 字节） + 用户标识长度（1 字节） +用户标识（n 字节）+ 签名后的值（64 字节） + 待验签数据。

中间包或最后一包数据：

■ P1=0：待 Hash 数据。

■ P1=1：待签名数据。

■ P1=2：待验签数据。

➢ 当 P2 Bit0 为 0 时（RSA+SHA1）

第一包或唯一一包数据：

■ P1=0：待 Hash 数据。

■ P1=1：私钥文件 ID（2 字节） + 待签名数据。

■ P1=2：公钥文件 ID（2 字节） + 签名后的值（0x80 字节） + 待验签数据。

中间包或最后一包数据：

■ P1=0：待 Hash 数据。

■ P1=1：待签名数据。

■ P1=2：待验签数据。

4　响应报文数据域

P1=00：计算 Hash，返回 Hash 结果；

P1=01：对输入待签名数据做哈希，再对哈希结果做签名，返回 Hash 值和签名值。

P1=02：对输入待验签数据做哈希，再对输入的签名值和计算的哈希值做验签，如果操作失败，返回状态码，成功则返回 Hash 结果。

5　响应报文状态码

表 B.46　响应报文状态码

状态字(HEX)	描述
9000	本次指令执行成功
6E00	CLA 不支持
6700	长度错误
61XX	正确执行 XX 标识剩余数据长度。 （仅用于 T=0）
6881	验签失败
6981	文件类型不匹配
6A82	文件不存在
6A84	数据接收缓冲区超限
6A86	P1P2 错误

中国智能交通产业联盟

标准

电子收费（ETC）设备蓝牙应用接口规范

T/ITS 0055-2017

北京市海淀区西土城路 8 号（100088）

中国智能交通产业联盟印刷

网址：http://www.c-its.org

2017 年 12 月第一版　2017 年 12 月第一次印刷