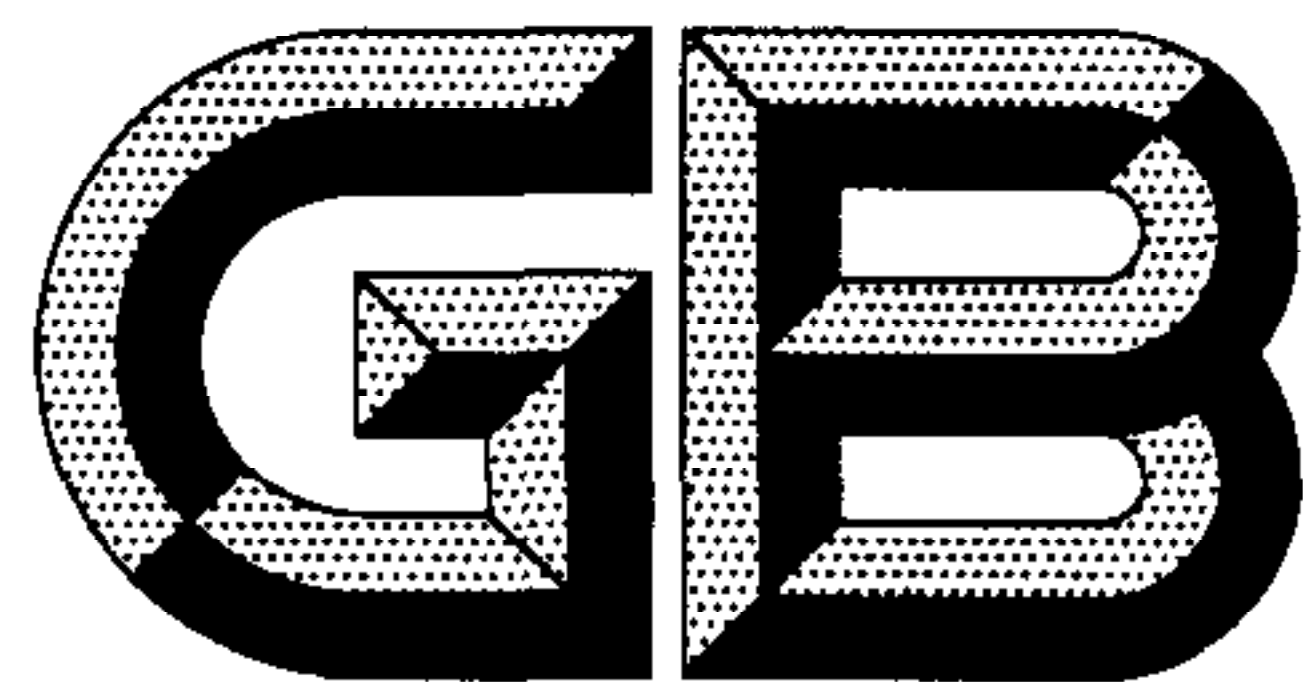




中华人民共和国国家标准

GB/T 28421—2012

电子收费 基于专用短程通信的电子 收费交易

Electronic toll collection—ETC transaction for DSRC

2012-06-29 发布

2012-10-01 实施



中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布

目 次

前言 Ⅲ

1 范围 1

2 规范性引用文件 1

3 术语、定义和缩略语 1

4 物理层 2

5 数据链路层 2

6 交易流程总体框架 2

7 DSRC 数据帧格式 3

8 ETC 交易中 ICC-PSAM 交易模式的选择 13

9 BST 中 CPU 用户卡消费交易模式的标识 13

10 OBE 对 CPU 用户卡处理模式的标识 15

11 VST 中应携带的 CPU 用户卡相关信息 15

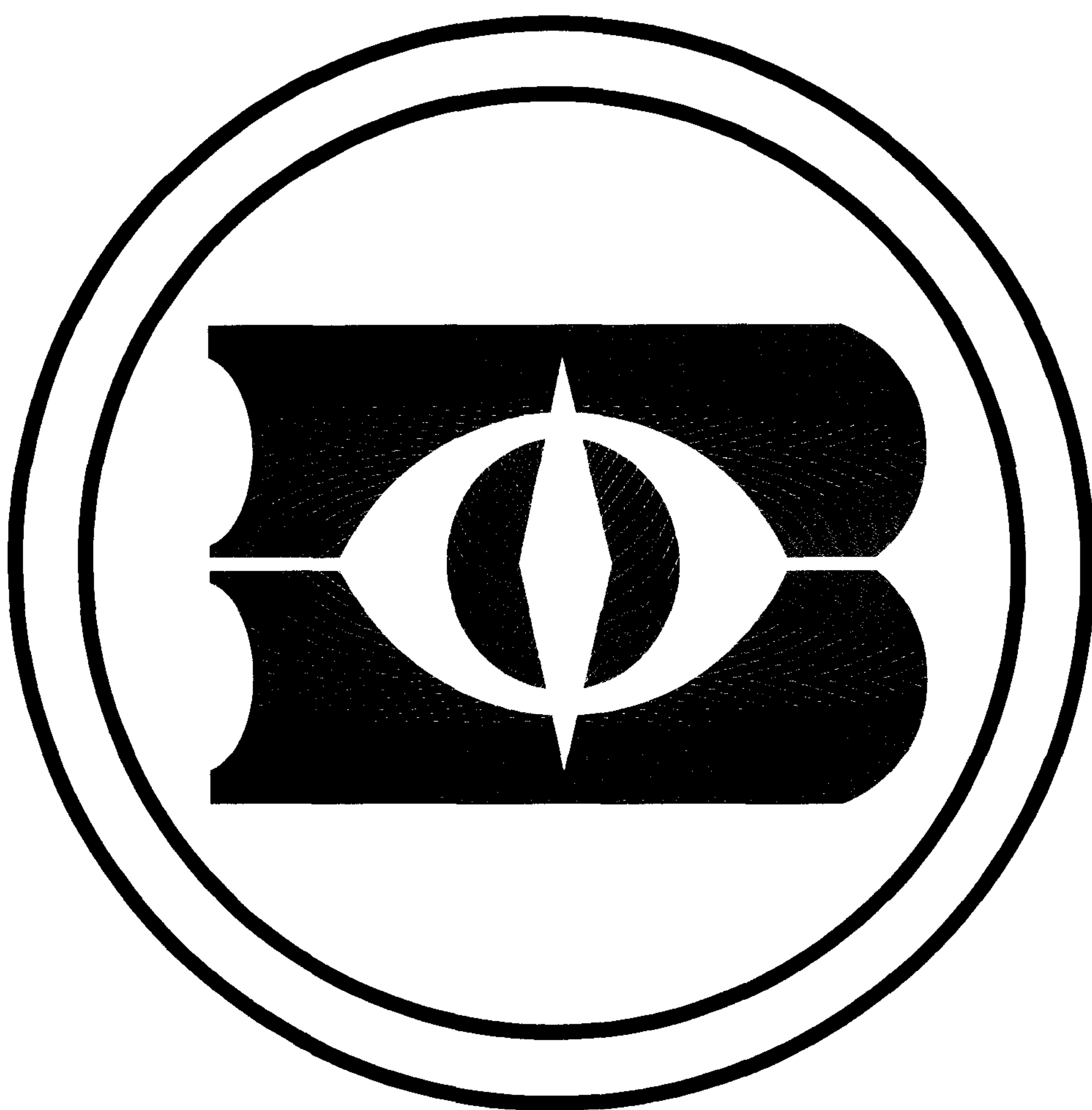
12 DSRC 交易之外的 OBE 应用处理流程 16

附录 A (资料性附录) 多个 T-APDU 拼接在同一个 LSDU 中的示例 19

附录 B (资料性附录) 储值卡/记账卡复合消费交易应用的 RSE~OBE 间 DSRC 数据帧定义 21

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。
本标准由全国智能运输系统标准化技术委员会(SAC/TC 268)提出并归口。
本标准起草单位:交通运输部公路科学研究院、上海东海电脑股份有限公司。
本标准主要起草人:杨蕴、陈丙勋、刘鸿伟、肖迪、王荣。



电子收费 基于专用短程通信的电子 收费交易

1 范围

本标准规定了公路电子收费应用中路侧设备(RSE)与车载设备(OBE)的专用短程通信(DSRC)物理、链路参数、交易流程总体框架、各静态数据帧的详细内容和格式编码,以及正常的交互时序。

本标准适用于公路电子收费系统,车辆出入管理、城市道路收费等领域可参照使用。

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。

- GB/T 20135 智能运输系统 电子收费 系统框架模型
- GB/T 20839 智能运输系统 通用术语
- GB/T 20851.1 电子收费 专用短程通信 第1部分:物理层
- GB/T 20851.2 电子收费 专用短程通信 第2部分:数据链路层
- GB/T 20851.3 电子收费 专用短程通信 第3部分:应用层
- GB/T 20851.4 电子收费 专用短程通信 第4部分:设备应用
- JR/T 0025—2005 中国金融集成电路 IC 卡规范

3 术语、定义和缩略语

3.1 术语和定义

GB/T 20135 和 GB/T 20839 中界定的术语和定义适用于本文件。

3.2 缩略语

下列缩略语适用于本文件。

- ASN.1:抽象语法记法一(Abstract Syntax Notation One)
- BST:信标服务表(Beacon Service Table)
- CPU:中央处理单元(Central Process Unit)
- DSRC:专用短程通信(Dedicated Short Range Communication)
- ETC:电子收费(Electronic Toll Collection)
- FCI:文件控制信息(File Control Information)
- ICC-PSAM:集成电路卡-消费安全访问模块(Integrate Circuit Card—Payment Security Access Module)
- LPDU:逻辑链路控制协议数据单元(LLC Protocol Data Unit)
- OBE:车载设备(On-board Equipment)
- OBU:车载单元(On-board Unit)

PBOC: 中国人民银行(People Bank of China)

RSE: 路侧设备(Roadside Equipment)

RSU: 路侧单元(Roadside Unit)

TAC: 交易认证码(Transaction Authorization Cryptogram)

T-APDU: 传送-应用协议数据单元(Transfer Application Protocol Data Unit)

UI: 无编号信息(Unnumbered Information)

VST: 车辆服务表(Vehicle Service Table)

4 物理层

上、下行链路的前导码为 16 位二进制“1”后跟 16 位二进制“0”组成,其他规定见 GB/T 20851.1。

5 数据链路层

数据链路层参数 T_u 调整为 3 ms, N_1 调整为 0~2,其他规定见 GB/T 20851.2。

6 交易流程总体框架

6.1 通信阶段划分

整个交易过程可划分为通信链路建立及应用信息获取、获取 OBE 数据、ICC-PSAM 消费交易、用户提示、链路释放等五个阶段。OBE 和 RSE 之间的认证包含在前两个阶段中,ICC-PSAM 间安全认证过程包含在第三个阶段中。

6.1.1 通信链路建立及应用信息获取阶段

该阶段主要完成通信链路的建立,协商通信参数,协商应用参数,获取部分应用信息等。其过程如下:

- RSE:BST;
- OBE:VST。

6.1.2 获取 OBE 数据阶段

读取 OBE 信息,主要是车辆信息文件中的车型信息,可完成 OBE 和 RSE 间的认证。其过程如下:

- RSE:GetSecure.request;
- OBE:GetSecure.response。

6.1.3 ICC-PSAM 消费交易阶段

使用多条 TransferChannel 完成 ICC-PSAM 的消费交易流程。费率计算由车道计算机完成,车型来自于 OBE,计算过程同人工收费。其过程如下:

- RSE:TransferChannel.request;
- OBE:TransferChannel.response。

6.1.4 用户提示阶段

提示用户交易结果。其过程如下:

- RSE:SetMMI.request;

——OBE:SetMMI.response。

6.1.5 链路释放阶段

RSE 释放与 OBE 的通信连接。
RSE:Event-Report(Release)。

6.2 原语拼接

交易中多个原语可通过拼接的方式实现,示例参见附录 A。
最后一个 TransferChannel.request 和 SetMMI.request 可采用链接的方式拼接到同一个 LSDU 中,亦即采用“带有链接的拼接”,见 GB/T 20851.3。

7 DSRC 数据帧格式

7.1 概述

本标准只描述了 ETC 应用中涉及的 BST、VST、GetSecure、TransferChannel、SetMMI、Event-Report(Release),其他原语的格式不做规范。

7.2 BST

7.2.1 简要说明

LLC 层使用 UI 命令。
APP 层使用 Initialization.request,T-APDUs=Initialization-Request=BST。

7.2.2 数据定义

BST 的 ASN.1 数据结构说明如下。
BST ::= SEQUENCE{
 fill BIT STRING(SIZE(3)),
 rsu BeaconID,
 time Time,
 profile Profile,
 mandapplications ApplicationList,
 nonmandapplications ApplicationList OPTIONAL,
 profileList SEQUENCE(SIZE(0..127,...)) OF Profile
}

公路电子收费系统应用中无 nonmandapplications 数据元。
其中:

BeaconID ::= SEQUENCE{
 manufacturerID INTEGER(0..255), - -1 字节
 individuaLID INTEGER(0..16777215) - -3 字节
}

ApplicationList ::= SEQUENCE (SIZE (0..127,...)) OF
 SEQUENCE{

aid	DSRCApplicationEntityID,
did	Dsrc-DID OPTIONAL,
applicationParameter	ApplicationContextMark OPTIONAL
}	

ApplicationList 编码说明如下：

- ApplicationList 的 SEQUENCE{}元素无扩展；
- 1 个应用,取值 1；
- 无 did；
- 有/无 applicationParameter。
- aid=1。

applicationParameter 可用于指示当前使用的交易模型等应用参数信息,是否存在取决于具体应用。其具体格式见第 9 章。

profileList - -无扩展;0 个 Profile。
其编码为“0000 0000”。

7.3 VST

7.3.1 简要说明

LLC 层使用 UI 命令。
APP 层使用 Initialization. response, T-APDUs=Initialization-Response=VST。

7.3.2 数据定义

VST 的 ASN.1 数据结构说明如下。

VST ::= SEQUENCE{	
fill	BIT STRING (SIZE(4)),
profile	Profile,
applications	ApplicationList,
obuConfiguration	ObuConfiguration
}	

其中：

ApplicationList ::= SEQUENCE (SIZE (0..127,...)) OF	
SEQUENCE{	
aid	DSRCApplicationEntityID,
did	Dsrc-DID OPTIONAL,
applicationParameter	ApplicationContextMark OPTIONAL
}	

ApplicationList 编码说明如下：

- SEQUENCE{}元素无扩展；
- 有 did；
- 有 applicationParameter；
- aid=1。

Dsrc-DID ::= INTEGER(0..127,...)
--无扩展,ETC 应用目录号为 1,取值 1。

GB/T 20851.3 中,applicationParameter 的类型定义为 ApplicationContextMark,其 ASN.1 定义如下:

ApplicationContextMark ::= Container
 (WITH COMPONENTS {octetstring PRESENT})
--ApplicationContextMark 的示例见 GB/T 20851.4,参考 SysInfoFile 的相关内容。

本标准在 GB/T 20851.3 的基础上补充规定 VST 中的 applicationParameter 的 ASN.1 定义为:

VSTApplicationContextMark ::= SEQUENCE {
 sysInfo Container,
 rndOBE Container OPTIONAL,
 privateInfo Container OPTIONAL,
 gbICCInfo Container OPTIONAL,
 reservedInfo1 Container OPTIONAL,
 reservedInfo2 Container OPTIONAL,
 reservedInfo3 Container OPTIONAL,
 reservedInfo4 Container OPTIONAL,
 reservedInfo5 Container OPTIONAL
}

reservedInfo1~5 保留给未来其他应用系统使用。

本标准在 GB/T 20851.3 的基础上对 Container 进行扩充定义如下:

Container ::= CHOICE{
 ...,
 sysInfo [39] SysInfo, --存放 OBE 中 SysInfoFile 中的部分内容,减少上传无效数据
 ...
}

SysInfo 的 ASN.1 类型定义为:

SysInfo ::= SEQUENCE{
 contractProvider OCTET STRING (SIZE(8)),
 contractType INTEGER(0..127,...),
 contractVersion INTEGER(0..127,...),
 contractSerialNumber ContractSerialNumber,
 contractSignedDate Date,
 contractExpiredDate Date
}

rndOBE 使用 Container[29],其 ASN.1 类型为 Rand。

Rand ::= OCTET STRING (SIZE(8))

privateInfo 用于存放各地方专有应用的相关信息,具体定义见相应地方规范。

gbICCInfo 用于存放国标储值卡、记账卡中卡片发行信息、钱包余额及入口信息等。

VST 中,ObuStatus 的 ASN.1 定义如下:

```
ObuStatus ::= SEQUENCE{
    iccPresent      BOOLEAN, --存在(0),无(1)
    iccType         BIT STRING (SIZE(3)),
    iccStatus       BOOLEAN, --CPU 用户卡正常(0),出错(1)
    locked          BOOLEAN, --OBU 未锁(0),被锁(1)
    tampered        BOOLEAN, --OBU 未被拆动(0),被拆动(1)
    battery         BOOLEAN, --OBU 电池正常(0),电池电量低(1)
    reservedBits    BIT STRING (SIZE(8)) --ESAM 第 27 字节“拆卸状态”
}
```

其中,iccType 的最低有效位(Bit4)指示卡片是 CPU 卡还是逻辑加密卡,次低有效位(Bit5)指示卡片使用接触式界面还是非接触界面。据此规则,iccType 的格式定义见表 1。

表 1 iccType 编码含义

	Bit6(保留比特)	Bit5	Bit4
接触式 CPU 卡	0	0	0
非接触 CPU 卡	0	1	0
接触式逻辑加密卡	0	0	1
非接触逻辑加密卡	0	1	1

7.4 GetSecure.request

7.4.1 简要说明

LLC 层使用 ACn 命令。
APP 层使用 Action.request, T-APDUs=Action-Request。

GetSecure.request 原语可携带访问证书(AccessCredentials),用于获得读取 OBE 中数据的权限,实现 OBE 对 RSE 的单方向认证。

该原语请求从 OBE 中获得一个使用指定密钥计算得到的鉴别报文(Authenticator),在保护 DSRC 传输过程中的数据完整性的同时,也实现了 RSE 对 OBE 合法性的单方向认证。

7.4.2 数据定义

GetSecure.request 的 ASN.1 数据结构说明如下。

```
Action-Request ::= SEQUENCE{
    mode          BOOLEAN,
    did           Dsrc-DID,
    actionType     ActionType,
    accessCredentials OCTET STRING (SIZE(0..127,...)) OPTIONAL,
    actionParameter Container OPTIONAL,
    iid           Dsrc-DID OPTIONAL
}
```

accessCredentials 可选性使用,actionParameter 应存在、iid 不存在。

其中:

- mode:采用确认模式,取值为 1。
- Dsrc-DID::=INTEGER(0..127,...) 无扩展,ETC 应用目录号为 1,取值 1。
- ActionType::=INTEGER(0..127,...) 无扩展,getSecure 为 0,取值 0。
- accessCredentials OCTET STRING (SIZE(0..127,...))

无扩展,Length 为 8,取值 8。accessCredentials 的取值为 8 字节。

accessCredentials 为 RSE 计算得到的访问证书,可用于 accessCredentials 计算的随机数 RndOBE 可从前述 VST 中获得。

actionParameter Container
为 Container 类型,Container. Type=20(GetSecureRq)

GB/T 20851.4 中规定:

GetSecureRq::=SEQUENCE{
 fill BIT STRING (SIZE(7)),
 fileid FID,
 offset INTEGER(0..65535,...),
 length INTEGER(0..127,...),
 rndRsuForAuthen Rand,
 keyIdForAuthen INTEGER(0..255),
 keyIdForEncrypt INTEGER(0..255) OPTIONAL
}

fileid FID,

FID::=INTEGER(0..127,...),无扩展。ETC 应用目录号=1(前面已定义),车辆信息文件的文件号=1,取值 1。

offset INTEGER(0..65535,...),
无扩展,取值等于实际的偏移量。

length INTEGER(0..127,...),
无扩展,取值等于需要读取的数据的实际长度。

根据 GB/T 20851.4 规定,ETC 车辆信息文件的文件内容定义如下:

EtcVehicleFile::=SEQUENCE{
 vehicleLicencePlateNumber OCTET STRING (SIZE(12)),
 vehicleLicencePlateColor OCTET STRING (SIZE(2)),
 vehicleClass INTEGER(0..127,...),
 vehicleUserType INTEGER(0..127,...),
 vehicleDimensions VehicleDimensions,
 vehicleWheels INTEGER(0..127,...),
 vehicleAxles INTEGER(0..127,...),
 vehicleWheelBases INTEGER(0..65535),
 vehicleWeightLimits INTEGER(0..16777215),

vehicleSpecificInfomation	OCTET STRING (SIZE(16)),
vehicleEngineNumber	OCTET STRING(SIZE(16)),
vehicleReserved	OCTET STRING(SIZE(10))

}

rndRsuForAuthen Rand,
其定义为 OCTET STRING (SIZE(8)),占 8 字节。填入 RSE/车道计算机产生的随机数。

keyIdForAuthen INTEGER(0..255),
用于指示信息鉴别密钥(etcEncryptKey)的密钥标识。

keyIdForEncrypt INTEGER(0..255),
用于指示加密密钥(etcEncryptKey)的版本密钥标识。

ETC 应用中 GetSecure.request 请求的车辆信息文件需要加密,keyIdForEncrypt 应存在,并用于指示加密密钥(etcEncryptKey)的密钥标识。信息鉴别密钥(etcEncryptKey)的密钥标识与加密密钥(etcEncryptKey)的密钥标识相同。

7.5 GetSecure.response

7.5.1 简要说明

LLC 层使用 ACh 响应。
APP 层使用 Action.response,T-APDUs=Action-Response。

GetSecure.response 原语应携带 OBE 使用指定密钥计算得到的鉴别报文(Authenticator),在保护 DSRC 传输过程中的数据完整性的同时,也让 RSE 完成对 OBE 合法性的单方向认证。

7.5.2 数据定义

GetSecure.response 的 ASN.1 数据结构说明如下。

```
Action-Response ::= SEQUENCE {
    fill          BIT STRING (SIZE(2)),
    did           Dsrc-DID,
    responseParameter Container OPTIONAL,
    iid           Dsrc-DID OPTIONAL,
    ret           ReturnStatus
}
```

注: responseParameter 应存在、iid 不存在。

其中:

- Dsrc-DID::=INTEGER(0..127,...) 无扩展,ETC 应用目录号为 1,取值 1。
- responseParameter Container

为 Container 类型,Container.Type=21(GetSecureRs)

GB/T 20851.4 中规定:

```
GetSecureRs ::= SEQUENCE {
    fileid      FID,
```

```
file          File,
authenticator  OCTET STRING (SIZE(8))
}
```

其中：

- fileid FID,
FID::= INTEGER(0..127,...),无扩展,车辆信息文件的文件号=1,取值 1;
- file File,
File::= OCTET STRING(SIZE(0..127,...))

用于存放 GetSecure.request 中请求文件的长度及内容;

- authenticator OCTET STRING (SIZE(8))

用于存放 RSE 对 OBE 进行认证的信息鉴别码。本标准规定,在采用 ESAM 的 MAC 加密认证模式下,authenticator 填入 8 字节的“0x00”。

7.6 TransferChannel.request

7.6.1 简要说明

LLC 层使用 ACn 命令。

APP 层使用 Action.request,T-APDUs= Action-Request。

以外部组件的形式访问 OBE 中的 CPU 用户卡不需要 DSRC 层面的安全认证,故不需要 access-Credentials。

在 ETC 应用中,TransferChannel.request 原语可通过 RSE→OBE,提供一个操作 OBE 中 CPU 用户卡的透明命令通道,亦即可通过该通道透明地向 CPU 用户卡发出指令。

7.6.2 数据定义

TransferChannel.request 的 ASN.1 数据结构说明如下。

```
Action-Request::=SEQUENCE{
    mode          BOOLEAN,
    did           Dsrc-DID,
    actionType     ActionType,
    accessCredentials  OCTET STRING (SIZE(0..127,...)) OPTIONAL,
    actionParameter  Container OPTIONAL,
    iid           Dsrc-DID OPTIONAL
}
```

accessCredentials 应不存在、actionParameter 应存在、iid 不存在。

其中：

- mode:采用确认模式,取值为 1;
- Dsrc-DID::=INTEGER(0..127,...)无扩展,ETC 应用目录号为 1,故取值 1。
- ActionType::=INTEGER(0..127,...)无扩展,transferChannel 为 3,故取值 3。
- actionParameter Container

为 Container 类型,Container.Type=24(ChannelRq)

GB/T 20851.4 中规定：

ChannelRq ::= SEQUENCE {
 channelid ChannelID,
 apdu ApduList
}

其中：
channelid ChannelID,
ChannelID 取 icc=1。

apdu ApduList
ApduList ::= SEQUENCE OF OCTET STRING(0..127)

SEQUENCE OF 中的每一个 OCTET STRING 包含一条完整 CPU 用户卡指令, CPU 用户卡的指令格式见表 2。

表 2 CPU 用户卡的命令格式

命 令 头				命 令 体		
CLA	INS	P1	P2	Lc	DATA	Le

7.7 TransferChannel.response

7.7.1 简要说明

LLC 层使用 ACh 响应。
APP 层使用 Action.response, T-APDU= Action-Response。
在 ETC 应用中, TransferChannel.response 原语可通过 RSE→OBE, 提供一个返回 OBE 中 CPU 用户卡针对此前命令执行的响应的透明通道。

7.7.2 数据定义

TransferChannel.response 的 ASN.1 数据结构说明如下。

Action-Response ::= SEQUENCE {
 fill BIT STRING (SIZE(2)),
 did Dsrc-DID,
 responseParameter Container OPTIONAL,
 iid Dsrc-DID OPTIONAL,
 ret ReturnStatus
}

responseParameter 应存在、iid 不存在。

- 其中：
- Dsrc-DID ::= INTEGER(0..127,...) 无扩展, ETC 应用目录号为 1, 取值 1。
 - responseParameter Container

为 Container 类型, Container.Type=25(ChannelRs)
GB/T 20851.4 标准中规定：
ChannelRs ::= SEQUENCE {

channelid ChannelID,
apdu ApduList
}

其中:

channelid ChannelID,
ChannelID 取 icc=1。

apdu ApduList

ApduList ::= SEQUENCE OF OCTET STRING(0..127)

SEQUENCE OF 中的每一个 OCTET STRING 包含一条完整 CPU 用户卡响应信息,CPU 用户卡的响应信息格式见表 3。

表 3 CPU 用户卡的响应信息格式

响 应 数 据		响 应 状 态 字	
Le 字节的 DATA		SW1	SW2

Le 长度有可能为 0。

响应信息的顺序应当与 TransferChannel.request 原语中 CPU 用户卡命令的顺序严格对应。

7.8 SetMMI.request

7.8.1 简要说明

LLC 层使用 ACn 命令。

APP 层使用 Action.request,T-APDUs= Action-Request。

GB/T 20851.4 标准中规定,SetMMI 中不需要 accessCredentials。

7.8.2 数据定义

SetMMI.request 的 ASN.1 数据结构说明如下。

Action-Request ::= SEQUENCE{
 mode BOOLEAN,
 did Dsrc-DID,
 actionType ActionType,
 accessCredentials OCTET STRING (SIZE(0..127,...)) OPTIONAL,
 actionParameter Container OPTIONAL,
 iid Dsrc-DID OPTIONAL
}

accessCredentials 应不存在、actionParameter 应存在、iid 不存在。

其中:

- mode:采用确认模式,取值为 1
- Dsrc-DID ::= INTEGER(0..127,...) 无扩展,根据 GB/T 20851.3 规定,取值为 ETC 应用=1。
- ActionType ::= INTEGER(0..127,...) 无扩展,ActionType=setMMI 为 4,取值 4。
- actionParameter Container

为 Container 类型,Container. Type=26(SetMMIRq)

GB/T 20851.4 标准中规定:

```
SetMMIRq ::= INTEGER{
    ok                (0),      --交易正常
    nok               (1),      --交易异常(通信、设备故障等技术方面异常)
    contactOperator   (2),      --联系运营商(过期、黑名单等管理方面异常)
    noCard            (3)       --无卡(卡片没有插好)
}
```

其取值取决于实际情况(如:交易结果、obuStatus 的设置等)

响音的模式:

- 交易正常:一声短促“嘀”;
- 交易异常:三声短促“嘀”;显示“操作失败”;
- 联系运营商:三声短促“嘀”;显示“联系运营商”;
- 无卡:设计一个声音;显示“请插卡”;
- 其他情况:不响。

7.9 SetMMI. response

7.9.1 简要说明

LLC 层使用 ACn 响应。
APP 层使用 Action. response, T-APDUs= Action-Response。

7.9.2 数据定义

SetMMI. response 的 ASN.1 数据结构说明如下。

```
Action-Response ::= SEQUENCE{
    fill                BIT STRING (SIZE(2)),
    did                 Dsrc-DID,
    responseParameter   Container OPTIONAL,
    iid                 Dsrc-DID OPTIONAL,
    ret                 ReturnStatus
}
```

responseParameter 不存在、iid 不存在。

其中:

Dsrc-DID ::= INTEGER(0..127,...)
--无扩展,根据 GB/T 20851.4 规定,取值为 ETC 应用=1。

7.10 Event-Report(Release)

7.10.1 简要说明

LLC 层使用 UI 命令,无需响应。
APP 层使用 Action. request, T-APDUs= event-report-request。
Event-Report(Release)用于释放 OBE,让 OBE 进入休眠状态。

7.10.2 数据定义

Event-Report-Request ::= SEQUENCE{
mode BOOLEAN,
did DirectoryID,
eventType EventType,
accessCredentials OCTET STRING (SIZE(0..127,...)) OPTIONAL,
eventParameter Container OPTIONAL,
iid Dsrc-DID OPTIONAL
}

accessCredentials 应不存在、actionParameter 应不存在、iid 应不存在。
其中：

- mode: 采用非确认模式, 取值为 0
- Dsrc-DID ::= INTEGER(0..127,...) 无扩展, 因为 Event-Report 与应用无关, 应取值为系统 (OBE)=0。
- eventType EventType,
EventType ::= INTEGER(
release (0)
) (0..127,...)
-- (1~80) 保留为 DSRC 应用
-- (81~127) 保留为自用
无扩展, eventType=0。

8 ETC 交易中 ICC-PSAM 交易模式的选择

在公路不停车收费系统中, ICC-PSAM 间交易采用复合消费交易模式。复合消费交易见 JR/T 0025—2005 规定, 复合消费交易应用 RSE 和 OBE 交互 DSRC 数据帧格式见附录 B。

9 BST 中 CPU 用户卡消费交易模式的标识

路侧系统可支持的交易模式可通过 BST 中 ApplicationList 内的 applicationParameter 进行指示。
GB/T 20851.3 中规定 BST 中 applicationParameter 的类型定义为 ApplicationContextMark, 其 ASN.1 定义如下：

ApplicationContextMark ::= Container
(WITH COMPONENTS {octetstring PRESENT})

本标准在 GB/T 20851.3 的基础上规定 BST 中的 applicationParameter 的 ASN.1 定义为：

BSTApplicationContextMark ::= SEQUENCE {
iccTransMode BIT STRING (SIZE(7)),
reservedInfo Container OPTIONAL
}

其中: iccTransMode 用于指示 RSE 所支持的 CPU 用户卡消费交易模式。
reservedInfo 用于其他应用参数信息协商的扩展。
IccTransMode 的结构定义见表 4。

表 4 IccTransMode 结构定义

Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
RSE 支持的 CPU 用户卡交易模式				RSE 优先采用的 CPU 用户卡交易模式		是否支持预处理

路侧系统所支持的 CPU 用户卡消费交易模式使用 iccTransMode 的高 4 比特 (Bit3~Bit6) 进行指示,其编码定义见表 5 所示。

表 5 路侧系统所支持的 CPU 用户卡消费交易模式编码

支持的消费交易模式	储 值 卡		记 账 卡	
	Bit6	Bit5	Bit4	Bit3
支持传统消费和复合交易模式	0	0	0	0
仅支持复合消费交易模式	0	1	0	1
其他保留	—	—	—	—

路侧系统优先采用的 CPU 用户卡消费交易模式使用 iccTransMode 中 Bit1~Bit2 进行指示,其编码定义见表 6。

表 6 路侧系统优先采用的 CPU 用户卡消费交易模式编码

优先采用的消费交易模式	储 值 卡	记 账 卡
	Bit2	Bit1
传统消费交易模式	0	0
复合消费交易模式	1	1

公路联网电子收费应用中 Bit2 、Bit1 的取值应为 1。

iccTransMode 的最低有效位 (Bit0) 用于指示路侧系统是否支持 CPU 用户卡的 OBE 预处理的快速交易模式。其编码定义见表 7。

表 7 OBE 预处理快速交易模式支持性编码

是否支持	Bit0
不支持	0
支持	1

为适应 CPU 用户卡文件格式及相关信息的地区性应用差异本标准在 GB/T 20851.3 的基础上对 Container 进行扩充定义,如用于指示预处理操作参数的 reservedInfo,其 ASN.1 定义如下:

```
Container ::= CHOICE{
    ...,
    pretreatPara [41] PretreatmentParameter, --指示预处理操作参数的 reservedInfo
    ...
}
```

其中,PretreatmentParameter 的 ASN.1 定义为:

```
PretreatmentParameter ::= SEQUENCE{
    fill                BIT STRING(SIZE(4)),
    sysInfoFileMode     BIT STRING (SIZE(8)),--系统信息文件预读长度
    offset0002          OCTET STRING (SIZE(2)) OPTIONAL,--预处理需要读取的电子钱包文
                        --件偏移量和长度
    offset0012          OCTET STRING (SIZE(2)) OPTIONAL,--收费信息文件偏移量和长度
    offset0015          OCTET STRING (SIZE(2)) OPTIONAL,--卡片发行文件偏移量和长度
    offset0019          OCTET STRING (SIZE(2)) OPTIONAL --复合消费文件偏移量和长度
}
```

其中,offset00 ** 用于指示 RSE 预读的 CPU 用户卡中各文件的偏移量和长度。结构定义见表 8 所示。

表 8 offset00 ** 结构定义

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
用户卡文件预读的偏移量								用户卡文件预读的长度							

sysInfoFileMode 用于指示 RSE 要求 OBE 在 VST 中返回系统信息文件的长度。结构定义见表 9。

表 9 sysInfoFileMode 结构定义

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
返回系统信息文件的字节数							

10 OBE 对 CPU 用户卡处理模式的标识

OBE 通过系统信息文件(目录号为 0,文件号为 1)中的合同版本(contractVersion)来标识 OBE 是否针对 CPU 用户卡进行预处理。

contractVersion 的编码规则见表 10。

表 10 contractVersion 的编码规则

扩展标志 Bit7	Bit6~Bit4	Bit3~Bit0
0:无扩展	0:OBE 对 CPU 用户卡不做预处理 1:OBE 对 CPU 用户卡做预处理 2~7:保留	1:OBE~RSE 之间采用 ESAM~PSAM 进行安全认证 2~15:保留

11 VST 中应携带的 CPU 用户卡相关信息

OBE 可通过 VST 携带 CPU 用户卡的相关预读信息,RSE 可根据这些预读信息对卡片进行有效性判别,获取 CPU 用户卡内的入口信息,以及钱包余额等。

OBE 应根据 BST 中 iccTransMode 的最低有效位(Bit0)所指示的路侧系统是否支持“OBE 预处理

的快速交易模式”确定是否在 VST 中是否携带 CPU 用户卡的相关预读信息。

本标准在 GB/T 20851.3 的基础上对 Container 进行扩充定义如下：

```
Container ::= CHOICE{
    ...,
    gbICCIInfo      [40] GBICCIInfo, --存放 CPU 用户卡的相关预读信息
    ...
}
```

GBICCIInfo 的 ASN.1 类型定义为：

```
GBICCIInfo ::= SEQUENCE{
    iccIssueInfo      OCTET STRING (SIZE(0..127,...)), --0015
    iccUniTollInfo     OCTET STRING (SIZE(0..127,...)), --0012/0019
    iccBalance         OCTET STRING (SIZE(0..127,...)) --0002
}
```

iccIssueInfo 中存放 CPU 用户卡“联网收费应用目录”(1001 目录)下卡片“发行基本数据文件”(0015 文件)中的相关信息,iccUniTollInfo 中存放 CPU 用户卡“联网收费应用目录”(1001 目录)下卡片“联网收费信息文件”(0012 文件)或“复合消费专用文件”(0019 文件)中的相关信息,iccBalance 中存放 CPU 用户卡“联网收费应用目录”(1001 目录)下卡片“电子钱包文件”(0002 文件)中的相关信息。具体读取的内容由 BST 中 pretreatPara 指定。

其中,“卡片版本号”的高 3 比特(Bit5~Bit7)用于指示该 CPU 用户卡所支持的消费交易模式,其编码定义见表 11。

表 11 OBE 所支持的 CPU 用户卡消费交易模式编码

支持的消费交易模式	Bit7(保留比特)	Bit6	Bit5
支持传统消费和复合交易模式	0	0	0
仅支持复合消费交易模式	0	0	1
其他保留	—	—	—

CPU 用户卡应支持复合消费交易模式,可选择性支持传统消费交易模式。

“卡片版本号”的低 4 比特用于指示该 CPU 用户卡的“应用版本号”。

12 DSRC 交易之外的 OBE 应用处理流程

12.1 流程概述

VST 中的预读信息(gbICCIInfo)应当在车辆(OBE)进入天线通信区域之前预先从 CPU 用户卡中读出,并在车辆(OBE)进入天线通信区域收到 BST 后直接在 VST 中传送给 RSE,而无需再执行读卡操作读取相关信息。

在各种情况下,OBE 均应保持预读信息(gbICCIInfo)与卡片内相应信息的一致性。即当卡片插入 OBE 时,OBE 应自动执行信息预读及数据拼装操作,操作完成后 OBE 进入休眠状态。当卡片插在 OBE 内而其中信息发生改变时,亦即当 OBE 在收费车道内完成交易(包括正常、异常等各种交易)后,进入休眠状态之前应当再次执行信息预读及数据拼装操作。

当 CPU 用户卡从 OBE 中拔出时,OBE 应自动删除前述各项预读信息(gbICCIInfo)。

OBE 进入天线通信区域被唤醒之后,OBE 将用户 CPU 用户卡卡上电后应当自动选择 1001 目录,进入待交易状态。

12.2 CPU 用户卡插入 OBE 后的预处理

12.2.1 记账卡

记账卡在插入 OBE 后应当执行如表 12 所示的预处理操作。

表 12 记账卡插入 OBE 后执行的预处理操作

CPU 用户卡	方向	OBE	备注
卡片复位	←	复位用户卡	
进入 1001 目录	←	选择 1001 目录	从返回的 FCI 里面可以获取 PBOC 2.0 标准的 0015 文件内容
返回 0015 文件	→	获得 CPU 用户卡卡号等信息	从 0015 文件中的卡片类型(第 9 字节)判定卡片为记账卡还是储值卡
	←	读 0012/0019 文件	
返回 0012/0019 文件	→	获得 0012/0019 文件	
		组装 VST 信息	OBE 应根据 BST 中指示的,以及其内 CPU 用户卡所优选和支持的交易模式,确定从 0012 文件还是 0019 文件中获取用于写入 VST 的相关信息
		关停用户 CPU 用户卡电源	

12.2.2 储值卡

储值卡在插入 OBE 后应当执行如表 13 所示的预处理操作。

表 13 储值卡插入 OBE 后执行的预处理操作

CPU 用户卡	方向	OBE	备注
卡片复位	←	复位用户卡	
进入 1001 目录	←	选择 1001 目录	从返回的 FCI 里面可以获取 PBOC 2.0 标准的 0015 文件内容
返回 0015 文件	→	获得 CPU 用户卡卡号等信息	从 0015 文件中的卡片类型(第 9 字节)判定卡片为记账卡还是储值卡
	←	读 0012/0019 文件	
返回 0012/0019 文件	→	获得 0012/0019 文件	
	←	读 0002 文件/钱包余额	
返回 0002 文件/钱包余额	→	获得钱包余额	
		组装 VST 信息	OBE 应根据 BST 中指示的,以及其内 CPU 用户卡所优选和支持的交易模式,确定从 0012 文件还是 0019 文件中获取用于写入 VST 的相关信息
		关停用户 CPU 用户卡电源	

12.3 交易后 OBE 的卡片信息更新处理流程

12.3.1 概述

OBE 在天线通信区域内完成上述 ETC 封闭式入、出口/开放式收费交易主流程后,在电子标签进入休眠状态之前,还应当继续完成如下“交易后 OBE 的卡片信息更新处理”。在前述交易失败的情况下,OBE 亦应通过超时休眠等机制,确保“交易后 OBE 的卡片信息更新处理”的执行。

12.3.2 记账卡

记账卡在 DSRC 交易完成后应当执行如表 14 所示的后处理操作。

表 14 记账卡在 DSRC 交易完成后执行的后处理操作

CPU 用户卡	方向	OBE	备注
	←	读 0012/0019 文件	
返回 0012/0019 文件	→	获得 0012/0019 文件	
		更新 VST 信息	OBE 应根据 BST 中指示的,以及其内 CPU 用户卡所优选和支持的交易模式,确定从 0012 文件还是 0019 文件中获取用于写入 VST 的相关信息
		关停用户 CPU 用户卡电源	

12.3.3 储值卡

储值卡在 DSRC 交易完成后应当执行如表 15 所示的后处理操作。

表 15 储值卡在 DSRC 交易完成后执行的后处理操作

CPU 用户卡	方向	OBE	备注
	←	读 0012/0019 文件	
返回 0012/0019 文件	→	获得 0012/0019 文件	
	←	读 0002 文件/钱包余额	
返回 0002 文件/钱包余额	→	获得钱包余额	
		更新 VST 信息	OBE 应根据 BST 中指示的,以及其内 CPU 用户卡所优选和支持的交易模式,确定从 0012 文件还是 0019 文件中获取用于写入 VST 的相关信息
		关停用户 CPU 用户卡电源	

附录 A
(资料性附录)
多个 T-APDU 拼接在同一个 LSDU 中的示例

A.1 说明

本附录以 GetSecure 和 TransferChannel 服务为例,对多个 T-APDU 拼接在同一个 LSDU 中的数据帧进行示例说明。

A.2 GetSecure.request ∪ TransferChannel.request

具体见表 A.1。

表 A.1 GetSecure.request ∪ TransferChannel.request 数据帧

字节	位(7...0)	值	描述
#01	0111 1110	7E	帧起始标志
#02	xxxx xxx0	XX	链路地址(MAC)
#03	xxxx xxx0	XX	
#04	xxxx xxx0	XX	
#05	xxxx xxx1	XX	
#06	0100 0000	40	MAC 控制域
#07	X111 0111	X7	LLC 控制域
#08	1001 0001	91	分段字头
#09	0000	0D	T-APDU: Action.request
	1		AccessCredential 存在
	1		ActionParameter 存在
	0		不存在 IID
	1		确认模式 (Confirmed mode=1)
#10	0000 0001	01	DID
#11	0000 0000	00	ActionType=0 (getSecure)
#N			
#N+1	1001 1001	91	分段字头
#N+2	0000	05	T-APDU: Action.request
	0		AccessCredential 不存在
	1		ActionParameter 存在
	0		不存在 IID
	1		确认模式 (Confirmed mode=1)
#N+3	0000 0001	01	DID
#N+4	0000 0011	03	ActionType=3 (transferChannel)
.....			
#N+M	xxxx xxxx	XX	
#N+M+1	xxxx xxxx	XX	帧校验序列
#N+M+2	xxxx xxxx	XX	
#N+M+3	0111 1110	7E	帧结束标志

A.3 GetSecure. response ∪ TransferChannel. response

具体见表 A. 2。

表 A. 2 GetSecure. response ∪ TransferChannel. response 数据帧

字节	位(7...0)	值	描 述
# 01	0111 1110	7E	帧起始标志
# 02	xxxx xxx0	XX	链路地址(MAC)
# 03	xxxx xxx0	XX	
# 04	xxxx xxx0	XX	
# 05	xxxx xxx1	XX	
# 06	1110 0000	E0	MAC 控制域
# 07	X111 0111	X7	LLC 控制域
# 08	0000 0000	00	LLC 状态响应域
# 09	1001 0001	91	分段字头
# 10	0001	18	T-APDU: Action. response
	1		存在 responseParameter
	0		不存在 IID
	00		填充比特, 设置为 0
# 11	0000 0000	00	DID
# 12	0001 0101	15	responseParameter. ContainerType=21 (GetSecureRs)
# N			
# N+1	1001 1001	91	分段字头
# N+2	0001	18	T-APDU: Action. response
	1		存在 responseParameter
	0		不存在 IID
	00		填充比特, 设置为 0
	0000 0000	00	DID
# N+3	0001 1001	19	responseParameter. ContainerType=25 (ChannelRs)
.....			
# N+M	xxxx xxxx	XX	
# N+M+1	xxxx xxxx	XX	帧校验序列
# N+M+2	xxxx xxxx	XX	
# N+M+3	0111 1110	7E	帧结束标志

附录 B

(资料性附录)

储值卡/记账卡复合消费交易应用的 RSE~OBE 间 DSRC 数据帧定义

B.1 概述

本附录定义复合消费交易流程的储值卡/记账卡 RSE~OBE 间 DSRC 数据帧。
开放式收费系统采用与封闭式出口相同的交易流程。

B.2 封闭式入口

B.2.1 BST

方向: RSE→OBE

功能: 轮询通信区域内的 OBE, 并与其协商通信参数及应用参数。

格式: 参见 7.1。

B.2.2 VST

方向: OBE→RSE

功能: 对 BST 进行应答, 建立通信链路, 与 RSE 协商通信参数及应用参数, 并返回部分应用信息。

格式: 参见 7.2 及第 11 章“VST 中应携带的 CPU 用户卡相关信息”。

B.2.3 GetSecure.request

方向: RSE→OBE

功能: 以安全的方式获取 OBE 内“ETC 应用车辆信息文件”中的相关车型参数信息。

格式: GetSecure.request 的格式参见 7.3。

B.2.4 GetSecure.response

方向: OBE→RSE

功能: 以安全的方式将 OBE 内“ETC 应用车辆信息文件”中的相关车型参数信息返回给 RSE, 并携带相关安全数据供 RSE 对 OBE 身份的合法性进行正; 返回复合消费交易初始化结果。

格式: GetSecure.response 的格式请参见 7.4。

B.2.5 TransferChannel.request I

方向: RSE→OBE

功能: 复合消费初始化; 复合消费写 0019 文件。

格式: TransferChannel.request I 的格式参见 7.5, 其中 ApduList 的格式如表 B.1 所示。

表 B.1 ApduList 的格式

数 据 项	数 据 内 容
N of APDUs	2
Length of APDU-1	16(5+11)
APDU-1 Info	805003020B+DATA(1 字节密钥标识+4 字节交易金额+6 字节终端机编号)
Length of APDU-2	48
APDU-2 Info	80DCAAC827+AA2500+0x28 个字节(复合消费专用文件)

封闭式入口,交易金额为 0。

B.2.6 TransferChannel, response I

方向:OBE→RSE
功能:返回复合消费初始化及复合消费写 0019 文件结果。
格式:TransferChannel, response II 的格式参见 7.6,其中 ApduList 的格式如表 B.2 所示。

表 B.2 ApduList 的格式

数 据 项	数 据 内 容
N of APDUs	2
Length of APDU-1	17(8+2)
APDU-1 Info	RetData(4 字节旧余额+2 字节电子钱包脱机交易序号+3 字节透支限额+1 字节密钥版本号+1 字节算法标识+4 字节伪随机数)+SW1SW2
Length of APDU-2	2
APDU-2 Info	SW1SW2

B.2.7 TransferChannel, request II ∪ SetMMI, request

方向:RSE→OBE
功能:卡片复合消费交易,通过蜂鸣器等人机界面,提示用户交易结果。
格式:TransferChannel, request II 的格式参见 7.5,其中 ApduList 的格式如表 B.3 所示:

表 B.3 ApduList 的格式

数 据 项	数 据 内 容
N of APDUs	1
Length of APDU-1	20(5+15)
APDU-1 Info	805401000F+4 字节终端交易序号+7 字节交易日期时间+4 字节 MAC1

SetMMI, request 的格式参见 7.7。

B. 2. 8 TransferChannel. response II ∪ SetMMI. response

方向:OBE→RSE
功能:返回卡片复合消费交易结果,及人机界面提示操作的结果。
格式:TransferChannel. response II 的格式参见 7. 6,其中 ApduList 的格式如表 B. 4 所示。

表 B. 4 ApduList 的格式

数 据 项	数 据 内 容
N of APDUs	1
Length of APDU-1	10
APDU-1 Info	4 字节 TAC+4 字节 MAC2+SW1SW2

SetMMI. response 的格式参见 7. 8。

B. 2. 9 EVENT-REPORT(Release)

方向:OBE→RSE
功能:结束交易,释放与电子标签的通信连接。
格式:参见 7. 9

B. 3 封闭式出口

B. 3. 1 BST

同 E. 2. 1。

B. 3. 2 VST

同 E. 2. 2。

B. 3. 3 GetSecure. request

同 E. 2. 3。

B. 3. 4 GetSecure. response

同 B. 2. 4。

B. 3. 5 TransferChannel. request I

同 E. 2. 5。
注:封闭式出口,交易金额为车道软件实际费率计算结果。

B. 3. 6 TransferChannel. response I

同 E. 2. 6。

B. 3. 7 TransferChannel. request II ∪ SetMMI. request

同 E. 2. 7。

B. 3. 8 TransferChannel. response II ∪ SetMMI. response

同 B. 2. 8。

B. 3. 9 EVENT-REPORT(Release)

同 B. 2. 9。

中 华 人 民 共 和 国
国 家 标 准
电子收费 基于专用短程通信的电子
收费交易

GB/T 28421—2012

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100013)
北京市西城区三里河北街16号(100045)

网址 www.spc.net.cn

总编室:(010)64275323 发行中心:(010)51780235

读者服务部:(010)68523946

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

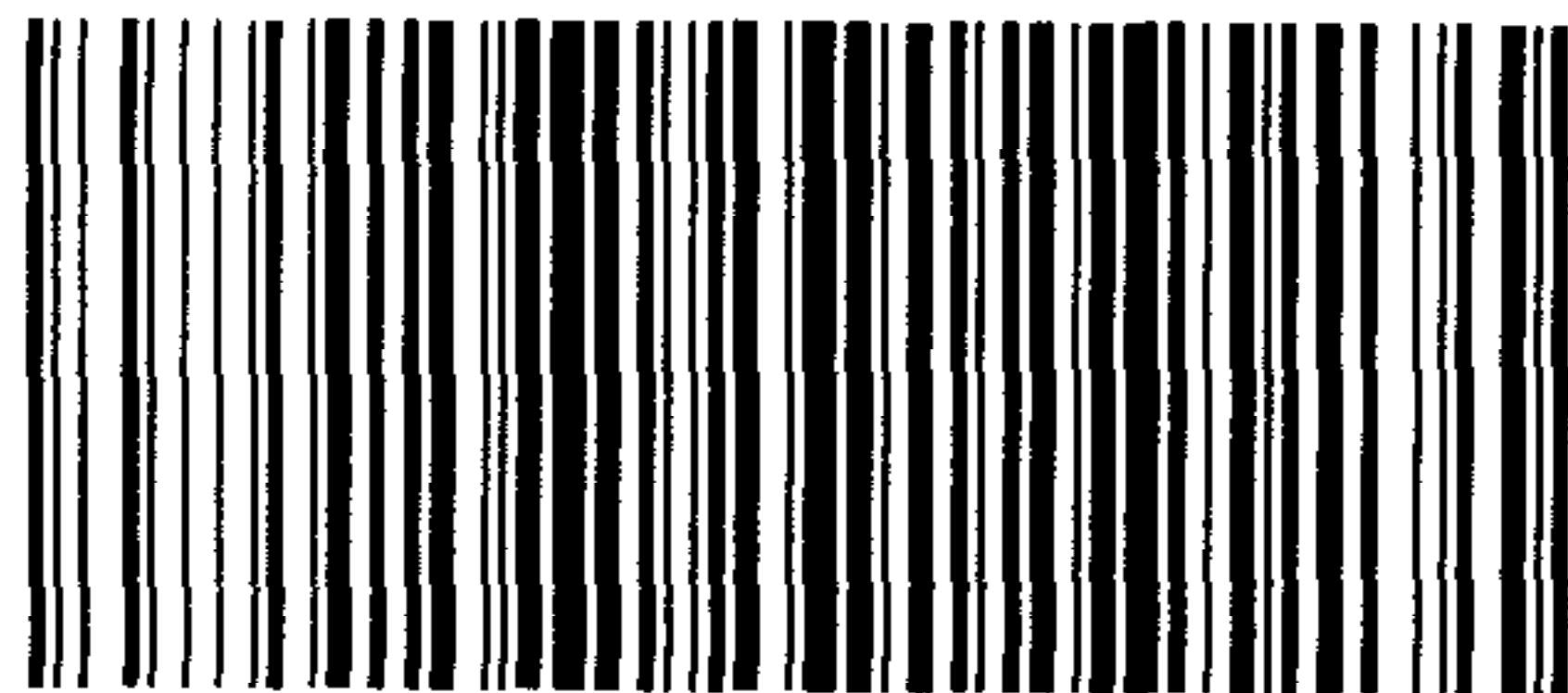
*

开本 880×1230 1/16 印张 2 字数 48 千字
2012年9月第一版 2012年9月第一次印刷

*

书号: 155066·1-45462 定价 30.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68510107



GB/T 28421-2012