



中华人民共和国国家标准

GB/T ×××××—××××

电子收费 基于 DSRC 的 ETC 交易

Electronic toll collection—ETC Transaction for DSRC

(征求意见稿)

×××××-××-××发布

×××××-××-××实施

中华人民共和国国家质量监督检验检疫总局 发布
中国国家标准化管理委员会

目 次

前 言 II

1 范围 1

2 规范性引用文件..... 1

3 术语和定义 1

4 符号和缩略语..... 1

5 物理层 2

6 数据链路层 2

7 交易流程总体框架..... 2

8 DSRC 数据帧格式 2

9 ETC 交易中 ICC-PSAM 交易模式的选择 12

10 BST 中国标 IC 卡消费交易模式的标识 12

11 OBE 对 IC 卡处理模式的标识..... 14

12 VST 中应携带的国标 IC 卡相关信息 14

13 DSRC 交易之外的 OBE 应用处理流程..... 15

附 录 A（规范性附录） 关于 TransferChannel 和 SetMMI 拼接使用的说明 18

附 录 B（规范性附录） 数据结构..... 19

附 录 C（资料性附录） 记账卡应用的 RSE~OBE 间 DSRC 数据帧说明..... 21

 C.1 封闭式入口..... 21

 C.2 封闭式出口..... 22

附 录 D（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 25

 D.1 封闭式入口..... 25

 D.2 封闭式出口..... 27

附 录 E（资料性附录） 多个 T-APDU 拼接在同一个 LSDU 中的示例 28

前 言

本标准由全国智能运输系统标准化技术委员会（SAC/TC268）提出并归口。

本标准起草单位：

本标准主要起草人：

电子收费 基于 DSRC 的 ETC 交易

1 范围

本标准规定了高速公路电子收费应用中路侧设备（RSE）与车载设备（OBE）的DSRC物理、链路参数，及交易中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。

本标准仅涉及到高速公路ETC应用中所涉及的BST、VST、GetSecure、Transfer_Channel、SetMMI、Event-Report(Release)，其他原语的格式不在本标准所规定的范围内。

本部分适用于公路电子收费系统，自动车辆识别、路径识别、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

下列文件中的条款通过本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

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
JR/T 0025-2005 中国金融集成电路 IC 卡规范
GB/T 16262-2006 信息技术 抽象语法记法一（ASN.1）（ISO/IEC 8824:2002，IDT）
GB/T 16263.2-2006 信息技术 ASN.1 编码规则 第 2 部分：紧缩编码规则（PER）规范（ISO/IEC 8825-2:2002，IDT）
收费公路联网收费技术要求，交通部 2007 年第 35 号公告

3 术语和定义

4 符号和缩略语

4.1 符号

下列符号适用于本标准。
dBm 表征功率与1mW的比值，0dBm=1mW
RSUt 路侧单元发射天线
RSUr 路侧单元接收天线

4.2 缩略语

下列缩略语适用于本标准。
ASK 幅移键控（Amplitude Shift Keying）
BER 位误码率（Bit Error Rate）
DSRC 专用短程通信（Dedicated Short Range Communication）
e. i. r. p 等效全向辐射功率（Equivalent Isotropically Radiated Power）
ETC 电子收费（Electronic Toll Collection）
FSK 频移键控（Frequency Shift Keying）

OBU 车载单元 (On Board Unit)

RSU 路侧单元 (Roadside Unit)

XPD 交叉极化鉴别率 (Cross Polarization Discrimination)

5 物理层

5.1 前导码

为了增加通讯的可靠性和稳定性，在上、下行链路的前导码前加16位“1”。

6 数据链路层

由于各地应用中VST长度不一致，当带有IC卡预读信息时，VST长度会接近128字节。数据链路层参数Tu调整为3ms，N1调整为0-2。

7 交易流程总体框架

7.1 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OBU数据、ICC-PSAM消费交易、用户提示、链路释放等五个阶段。OBU和RSU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。

7.2 通信链路建立及应用信息获取阶段

- RSE: BST
- OBE: VST

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。

7.3 获取 OBU 数据阶段

- RSE: GetSecure.Rq
- OBE: GetSecure.Rs

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

7.4 ICC-PSAM 消费交易阶段

- RSE: Transfer_Channel.Rq
- OBE: Transfer_Channel.Rs

使用多条Transfer_Channel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。

7.5 用户提示阶段

- RSE: SETMMI.Rq
- OBE: SETMMI.Rs

提示用户交易结果。

7.6 链路释放阶段

- RSE: Event_Report(Release)，RSE释放OBE。
- RSE释放与OBE的通信连接。

8 DSRC 数据帧格式

8.1 BST

8.1.1 简要说明

LLC层使用UI命令。

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

8.1.2 数据定义

```

BST ::= SEQUENCE {
    fill                BIT STRING (SIZE(3)),
    rsu                 BeaconID,
    time                Time,
    profile              Profile,
    mandapplications    ApplicationList,
    nonmandapplications ApplicationList OPTIONAL,
    profileList          SEQUENCE (0..127,...) OF Profile
}

```

注：高速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
    individualLID        INTEGER (0..16777215) -- 3字节
}

```

```

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

```

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，是否存在取决具体应用。其具体格式参见第6章。

profileList 一无扩展；0个Profile。

注：其编码为“0000 0000”

8.2 VST

8.2.1 简要说明

LLC层使用UI命令。

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

8.2.2 数据定义

```

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
  }

```

其中：

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，故取值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的示例可在GB/T 20851.4-2007（《电子收费
  --专用短程通信 设备应用》）中找到，参考SysInfoFile的相关内容。

```

本规范在国标GB/T 20851.3-2007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,
  gbICCIInfo       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。

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，其具体定义请参见其他相关规范。在国标 IC 卡应用中，本部分内容不存在。

gbICCIInfo 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, -- IC 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 的格式定义如下 (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

8.3 GetSecure.rq

8.3.1 简要说明

LLC层使用ACn命令。

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

GetSecure.rq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。

8.3.2 数据定义

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

注：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，故取值1。

ActionType::=INTEGER(0..127,...)

— 无扩展，getSecure为0，故取值0。

accessCredentials OCTET STRING (SIZE(0..127,...))

— 无扩展，Length为8，故取值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可以从前述VST中获得。

本示范工程规范中，accessCredentials不存在。

actionParameter Container

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

GB/T 20851.4-2007标准中规定：

```
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，故取值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。

根据国标GB/T 20851.4-2007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RSU / 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。

本规范规定, ETC应用中GetSecure.Rq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。本规范中信息鉴别密钥 (etcEncryptKey) 的密钥标识与加密密钥 (etcEncryptKey) 的密钥标识相同。

8.4 GetSecure.rs

8.4.1 简要说明

LLC层使用ACn响应。

APP层使用Action.reponse, T-APDUs= Action-Reponse。

GetSecure.rs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。

8.4.2 数据定义

```

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, 故取值1。

responseParameter Container

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

GB/T 20851.4-2007标准中规定:

```

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，故取值1。

file File,

File ::= OCTET STRING(SIZE(0..127, ...))

用于存放GetSecure.rq中请求文件的长度及内容。

authenticator OCTET STRING (SIZE(8))

用于存放RSU对OBU进行认证的信息鉴别码。本规范规定，在采用ESAM的MAC加密认证模式下，authenticator填入8字节的“0x00”。

8.5 Transfer_Channel.Rq

8.5.1 简要说明

LLC层使用ACn命令。

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

本规范规定，以外部组件的形式访问OBE中的用户IC卡不需要DSRC层面的安全认证，故不需要accessCredentials。

在ETC应用中，Transfer_Channel.Rq原语可通过RSE—OBE，提供一个操作OBE中用户IC卡的透明命令通道，亦即，可通过该通道透明地向用户IC卡发出指令。

8.5.2 数据定义

```

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

```

注：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 20851.4-2007标准中规定：

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

其中：

channelid ChannelID,
ChannelID取icc =1。

apdu AduList
AduList ::= SEQUENCE OF OCTET STRING (0..127)
SEQUENCE OF中的每一个OCTET STRING包含一条完整IC卡指令，IC卡的指令格式如下：

命令头				命令体		
CLA	INS	P1	P2	Lc	DATA	Le

图1 IC卡的命令格式

8.6 Transfer_Channel.Rs

8.6.1 简要说明

LLC层使用ACn响应。
APP层使用Action.reponse, T-APDUs= Action-Reponse。
在ETC应用中，Transfer_Channel.Rs原语可通过RSE—OBE，提供一个返回OBE中用户IC卡针对此前命令执行的响应的透明通道。

8.6.2 数据定义

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，故取值1。

responseParameter Container
为Container类型，Container.Type=25 (ChannelRs)

GB/T 20851.4-2007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IC卡响应信息，IC卡的响应信息格式如下：

响应数据	响应状态字	
Le 字节的 DATA	SW1	SW2

图2 IC 卡的响应信息格式

Le长度有可能为0。
响应信息的顺序应当与Transfer_Channel.Rq原语中IC卡命令的顺序严格对应。

8.7 SetMMI.Rq

8.7.1 简要说明

LLC层使用ACn命令。
APP层使用Action.request，T-APDUs= Action-Request。
GB/T 20851.4-2007标准中规定，SetMMI中不需要accessCredentials。

8.7.2 数据定义

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

注：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，根据国标GB/T 20851.3-2007规定，取值为ETC应用 = 1。

ActionType ::= INTEGER (0..127,...)
-- 无扩展，ActionType=setMMI为4，故取值4。

actionParameter Container

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

GB/T 20851.4-2007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“交易失败”；

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”；

其它情况：不响。

8.8 SetMMIRs

8.8.1 简要说明

LLC层使用ACn响应。

APP层使用Action.reponse, T-APDUs= Action-Reponse。

8.8.2 数据定义

Action-Response ::= SEQUENCE {

fill	BIT STRING (SIZE(2)),
did	Dsrc-DID,
responseParameter	Container OPTIONAL,
iid	Dsrc-DID OPTIONAL,
ret	ReturnStatus

}

注：responseParameter不存在、iid不存在。

其中：

Dsrc-DID ::= INTEGER (0..127,...)

-- 无扩展，根据国标GB/T 20851.4-2007规定，取值为ETC应用 = 1。

8.9 Event_Report(Release)

8.9.1 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。

8.9.2 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
}

注：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，故应取值为系统（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。

9 ETC 交易中 ICC-PSAM 交易模式的选择

在高速公路联网不停车收费工程中，ICC-PSAM间交易采用复合消费交易模式。

10 BST 中国标 IC 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。

国 标 GB/T 20851.3-2007 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})

本规范在国标GB/T 20851.3-2007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用于指示路侧设备所支持的IC卡消费交易模式。
reservedInfo用于其他应用参数信息协商的扩展。
IccTransMode的结构定义如表2所示：

表2 IccTransMode 结构定义

Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
RSU支持的IC卡交易模式				RSU优先采用的IC卡交易模式		是否支持预处理

路侧系统所支持的国标IC卡消费交易模式使用iccTransMode的高4比特（Bit4~Bit6）进行指示，其编码定义如表3所示：

表3 路侧系统所支持的国标 IC 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
其它保留				

路侧系统优先采用的国标IC卡消费交易模式使用iccTransMode中Bit1~Bit2进行指示，其编码定义如下表所示：

表4 路侧系统优先采用的国标 IC 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

*注：高速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国标IC卡的OBE预处理的快速交易模式。其编码定义如下表所示：

表5 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

为适应国标IC卡文件格式及相关信息的地区性应用差异本规范在国标GB/T 20851. 3-2007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**用于指示路侧设备预读的IC卡中各文件的偏移量和长度。结构定义如表6所示：

表6 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用于指示路侧设备要求OBU在VST中返回系统信息文件的长度。结构定义如表7所示：

表7 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							

11 OBE 对 IC 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IC卡进行预处理。

contractVersion的编码规则如下：

表8 contractVersion 的编码规则

扩展标志 Bit7	Bit6～Bit4	Bit3～Bit0
0 – 无扩展	0 – OBE 对 IC 卡不做预处理 1 – OBE 对 IC 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

12 VST 中应携带的国标 IC 卡相关信息

车载设备可通过VST携带国标IC卡的相关预读信息，路侧设备可根据这些预读信息对卡片进行有效性判别，获取IC卡内的入口信息，以及钱包余额等。

车载设备应根据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中是否携带国标IC卡的相关预读信息。

本规范在国标GB/T 20851.3-2007的基础上对Container进行扩充定义如下：

```
Container ::= CHOICE {  
    ...,  
    gbICCIInfo [40] GBICCIInfo, --存放国标IC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或0019  
    iccBalance OCTET STRING (SIZE(0..127,...)) --0002  
}
```

iccIssueInfo中存放国标IC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中存放国标IC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中存放国标IC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IccReadPara指定。

其中，“卡片版本号”的高3比特（Bit5～Bit7）用于指示该国标IC卡所支持的消费交易模式，其编码定义如表9所示：

表9 OBE 所支持的国标 IC 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

其它保留			
------	--	--	--

注：国标 IC 卡应必须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 比特用于指示该国标 IC 卡的“应用版本号”，可作为卡片密钥的版本索引使用。

ETC 应用的当前“应用版本号”取值为“0x0”。

13 DSRC 交易之外的 OBE 应用处理流程

VST 中的预读信息（gbICCIInfo）应当在车辆（车载设备）进入天线通信区域之前预先从卡片中读出，并在车辆（车载设备）进入天线通信区域收到 BST 后直接在 VST 中传送给路侧设备，而无需再执行读卡操作读取相关信息。

在各种情况下，车载设备均应保持预读信息（gbICCIInfo）与卡片内相应信息的一致性。即，当卡片插入车载设备时，车载设备应自动执行信息预读及数据拼装操作，操作完成后车载设备进入休眠状态。当卡片插在车载设备内而其中信息发生改变时，亦即当车载设备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 IC 卡从车载设备中拔出时，车载设备应自动删除前述各项预读信息（gbICCIInfo）。

车载设备进入天线通信区域被唤醒之后，车载设备将用户 IC 卡上电后应当自动选择1001目录，进入待交易状态。

13.1 国标 IC 卡插入车载设备后的预处理

13.1.1 记账卡

记账卡在插入车载设备后应当执行如表9所示的预处理操作：

表10 记账卡插入车载设备后执行的预处理操作

用户 IC 卡		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 IC 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，以及其内国标 IC 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 IC 卡电源	

13.1.2 储值卡

储值卡在插入车载设备后应当执行如表9所示的预处理操作：

表11 储值卡插入车载设备后执行的预处理操作

用户 IC 卡		OBE	备注
卡片复位	←	复位用户卡	

用户 IC 卡		OBE	备注
进入 1001 目录	←	选择 1001 目录	从返回的 FCI 里面可以获得 PBOC 2.0 标准的 0015 文件内容。
返回 0015 文件	→	获得 IC 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，以及其内国标 IC 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 IC 卡电源	

13.2 交易后 OBE 的卡片信息更新处理流程

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。

13.2.1 记账卡

记账卡在DSRC交易完成后应当执行如表10所示的后处理操作：

表12 记账卡在 DSRC 交易完成后执行的后处理操作

用户 IC 卡		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，以及其内国标 IC 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 IC 卡电源	

13.2.2 储值卡

储值卡在DSRC交易完成后应当执行如表11所示的后处理操作：

表13 储值卡在 DSRC 交易完成后执行的后处理操作

用户 IC 卡		OBE	备注
	←	读 0012 / 0019 文件	

用户 IC 卡		OBE	备注
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，以及其内国标 IC 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 IC 卡电源	

附 录 A
(规范性附录)

关于 TransferChannel 和 SetMMI 拼接使用的说明

为了节约时间，本规范将最后一个TransferChannel和SetMMI拼接在一个DSRC帧中。如果采用通常的T-APDU拼接处理方式，则逻辑上可能存在信息提示错误，即：当最后一个TransferChannel命令执行失败的情况下，车载设备的MMI仍有可能提示正常交易。

为了避免这种情况的发生，TransferChannel.rq和SetMMI.rq应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”。

附 录 B
(规范性附录)
数据结构

```

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

```

```

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

```

```

Container ::= CHOICE {
    ...,
    sysInfo      [39] SysInfo,           --存放OBU中SysInfoFile中的部分内容
    gbICCIInfo   [40] GBICCIInfo,       --存放国标IC卡的相关预读信息
    PretreatPara [41] PretreatmentParameter, --指示预处理操作参数的reservedInfo
    ...
}

```

```

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

```

```

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

```

```

    iccBalance      OCTET STRING (SIZE(0..127,...))  --0002
}

```

```

PretreatmentParameter ::= SEQUENCE{
    fill            BIT STRING(SIZE(4))
    SysInfoFileMode BIT STRING (SIZE(8)) , --系统信息文件预读长度
    Length0002      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
}

```

附 录 C
(资料性附录)

记账卡应用的 RSE~OBE 间 DSRC 数据帧说明

本附录给出了采用传统消费交易模式的记账卡应用的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。

C.1 封闭式入口

C.1.1 BST

方向：RSE→OBE
功能：轮询通信区域内的 OBU，并与其协商通信参数及应用参数。
格式：参见本规范第 4.1 节。

C.1.2 VST

方向：OBE→RSE
功能：对 BST 进行应答，建立通信链路，与 RSU 协商通信参数及应用参数，并返回部分应用信息。
格式：参见本规范第 4.2 节及第 8 章“VST 中应携带的国标 IC 卡相关信息”。

C.1.3 GetSecure.rq ∪ TransferChannel.rq I

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；执行用户 IC 卡内部认证，获取写 0012 文件外部认证所需的随机数。
格式：
GetSecure.rq 的格式参见本规范第 4.3 节。
TransferChannel.rq I 的格式参见本规范第 4.5 节，其中 ApduList 的格式如表 C.1 所示：

表C.1 ApduList 的格式

数据项	数据内容
N of APDUs	2
Length of APDU-1	13
APDU-1 Info	0088000108+8 字节随机数
Length of APDU-2	5
APDU-2 Info	0084000008

C.1.4 GetSecure.rs ∪ TransferChannel.rs I

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；返回用户 IC 卡内部人认证所需的密文数据，外部认证所需的随机数。
格式：
GetSecure.rs 的格式请参见本规范第 4.4 节。
TransferChannel.rs I 的格式参见本规范第 4.6 节，其中 ApduList 的格式如表 C.2 示：

表C.2 ApduList 的格式

数据项	数据内容
N of APDUs	2
Length of APDU-1	10(8+2)
APDU-1 Info	8 字节加密结果+ SW1SW2
Length of APDU-2	10(8+2)
APDU-2 Info	8 字节随机数+ SW1SW2

C.1.5 TransferChannel.rq II ∪ SetMMI.rq

方向：RSE→OBE
功能：外部认证，写联网收费信息文件（0012 文件），通过蜂鸣器等人机界面，提示用户交易结果。
格式：

TransferChannel.rq II 的格式参见本规范第 4.5 节，其中 ApduList 的格式如表 C.3 示：

表C.3 ApduList 的格式

数据项	数据内容
N of APDUs	2
Length of APDU-1	13(5+8)
APDU-1 Info	0082000108+随机数加密结果
Length of APDU-2	41(5+36)
APDU-2 Info	00D6920024+0012 文件内容

SetMMI.rq 的格式参见本规范第 4.7 节。

C.1.6 TransferChannel.rs II ∪ SetMMI.rs

方向：OBE→RSE
功能：返回外部认证结果，写联网收费信息文件（0012 文件）的结果，及人机界面提示操作的结果。
格式：

TransferChannel.rs II 的格式参见本规范第 4.6 节，其中 ApduList 的格式如表 C.4 示：

表C.4 ApduList 的格式

数据项	数据内容
N of APDUs	2
Length of APDU-1	2
APDU-1 Info	SW1SW2
Length of APDU-2	2
APDU-2 Info	SW1SW2

SetMMI.rs 的格式参见本规范第 4.8 节。

C.1.7 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：参见本规范第 4.9 节

C.2 封闭式出口

C.2.1 BST
同 B.1.1。

C.2.2 VST
同 B.1.2。

C.2.3 GetSecure.rq ∪ TransferChannel.rq I
同 B.1.3。

C.2.4 GetSecure.rs ∪ TransferChannel.rs I
同 B.1.4。

C.2.5 TransferChannel.rq II ∪ SetMMI.rq
方向：RSE→OBE
功能：外部认证，写联网收费信息文件（0012 文件），计算 TAC 码，通过蜂鸣器等人机界面，提示用户交易结果。
格式：
TransferChannel.rq II 的格式参见本规范第 4.5 节，其中 ApduList 的格式如表 C.5 示：

表C.5 ApduList 的格式

数据项	数据内容
N of APDUs	3
Length of APDU-1	13(5+8)
APDU-1 Info	0082000108+随机数加密结果
Length of APDU-2	41(5+36)
APDU-2 Info	00D6920024+0012 文件内容
Length of APDU-3	23(5+18)
APDU-3 Info	0088020112+TAC 计算数据域

SetMMI.rq 的格式参见本规范第 4.7 节。

C.2.6 TransferChannel.rs II ∪ SetMMI.rs
方向：OBE→RSE
功能：返回外部认证结果，写联网收费信息文件（0012 文件）的结果，TAC 码，及人机界面提示操作的结果。
格式：
TransferChannel.rs II 的格式参见本规范第 4.6 节，其中 ApduList 的格式如表 C.6 示：

表C.6 ApduList 的格式

数据项	数据内容
N of APDUs	3
Length of APDU-1	2
APDU-1 Info	SW1SW2
Length of APDU-2	2
APDU-2 Info	SW1SW2
Length of APDU-3	6(4+2)

APDU-3 Info	TAC+SW1SW2
-------------	------------

SetMML.rs 的格式参见本规范第 4.8 节。

C. 2. 7 EVENT-REPORT (Release)

同 B.1.7。

附录 D
(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

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。

D.1 封闭式入口

D.1.1 BST

同 B.1.1。

D.1.2 VST

同 B.1.2。

D.1.3 GetSecure.rq

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.rq 的格式参见本规范第 4.3 节。

D.1.4 GetSecure.rs

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.rs 的格式请参见本规范第 4.4 节。

D.1.5 TransferChannel.rq 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.rq I 的格式参见本规范第 4.5 节，其中 ApduList 的格式如表 D.1 所示：

表D.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	44
APDU-2 Info	80DCAAC827+AA2500+0x24 个字节（复合消费专用文件）

注：封闭式入口，交易金额为 0。

D.1.6 TransferChannel.rs 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.rs II 的格式参见本规范第 4.6 节，其中 ApduList 的格式如表 D.2 所示：

表D.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

D.1.7 TransferChannel.rq II ∪ SetMMI.rq

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.rq II 的格式参见本规范第 4.5 节，其中 ApduList 的格式如表 D.3 所示：

表D.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.rq 的格式参见本规范第 4.7 节。

D.1.8 TransferChannel.rs II ∪ SetMMI.rs

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.rs II 的格式参见本规范第 4.6 节，其中 ApduList 的格式如表 D.4 所示：

表D.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.rs 的格式参见本规范第 4.8 节。

D.1.9 EVENT-REPORT (Release)

同 B.1.7。

D.2 封闭式出口

D.2.1 BST

同 B.1.1。

D.2.2 VST

同 B.1.2。

D.2.3 GetSecure.rq

同 C.1.3。

D.2.4 GetSecure.rs

同 C.1.4。

D.2.5 TransferChannel.rq I

同 C.1.5。

注：封闭式出口，交易金额为车道软件实际费率计算结果。

D.2.6 TransferChannel.rs I

同 C.1.6。

D.2.7 TransferChannel.rq II ∪ SetMMI.rq

同 C.1.7。

D.2.8 TransferChannel.rs II ∪ SetMMI.rs

同 C.1.8。

D.2.9 EVENT-REPORT (Release)

同 C.1.9。

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

E.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。

E.2 GetSecure.rq ∪ TransferChannel.rq

表E.1 GetSecure.rq ∪ TransferChannel.rq 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

字节	位 (7...0)	值	描 述
#N+M+2	xxxx xxxx	XX	
#N+M+3	0111 1110	7E	帧结束标志

E.3 GetSecure.rs ∪ TransferChannel.rs

表E.2 GetSecure.rs ∪ TransferChannel.rs 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