ICS 35.200
L65

中华人民共和国国家标准

GB/T XXXXX—XXXX
代替 GB/T20851.4-2007

电子收费 专用短程通信 第4部分：设备应用

Electronic toll collection－Dedicated short range communication－Part4：Equipment application

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

本稿完成日期 2017年3月

××××-××-××发布 ××××-××-××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 II
1 范围 1
2 规范性引用文件 1
3 术语、定义和缩略语 1
4 应用总则 1
5 关键设备总体技术要求 4
6 OBE 数据结构 6
7 ETC 应用接口 8
8 ETC 应用安全 13
9 ETC 交易流程 17
附录 A （规范性附录）OBE 的 ASN.1 型数据结构 31
附录 B （资料性附录）多个 T-APDU 拼接在同一个 LSDU 中的示例 37
附录 C （资料性附录）复合消费交易应用的 RSE～OBE 间 DSRC 数据帧定义 39

前　言

GB/T XXXXX-XXXX《电子收费 专用短程通信》分为五个部分:

——第1部分：物理层；

——第2部分：数据链路层；

——第3部分：应用层；

——第4部分：设备应用；

——第5部分：物理层主要参数测试方法。

本部分为GB/T XXXXX-XXXX的第4部分。

本部分代替GB/T 20851.4-2007《电子收费 专用短程通信 第4部分:设备应用》，与GB/T 20851.4-2007，除编辑性修改外主要技术变化如下：

——在范围的规定中，在适用于公路电子收费系统基础上，增加了适用于城市道路电子收费系统（见1，2007年版1）；

——在规范性引用文件中，增加了电池要求和运输安全的规范性应用文件（见2）；

——删除了OBE数据组织中文件的类型（见表1）；

——删除了OBE密钥中密钥代码（见表2）；——修改了OBE文件属性中“无权限”为“禁止”（见表3）；

——修改了TDES安全计算算法为SM4算法（见5，2007年版5）；

——修改了OBE应支持的信息存储空间大小（见5.1.3，2007年版5.1.3）；

——修改了OBE应支持的标准配置部件和可选配置部件的规定（见5.1.4，2007年版5.1.4）；

——增加了OBE内置电池的安全性要求（见5.1.18）；

——增加了OBE唤醒灵敏度和等效全向辐射功率可调功能的规定（见5.1.12）；

——修改了RSE应内置PSAM安全认证模块为安全访问模块或者达到同样安全等级的芯片、板卡或辅助设备等规定（见5.2.3，2007年版5.2.3）；

——修改了RSE上位机通信接口要求（见5.2.4，2007年版5.2.4）；

——增加了RSE应具有网络监测接口要求（见5.2.3）；

——增加了RSE的等效全向辐射功率调节功能规定（见5.2.11）；

——删除了OBE数据结构与属性中文件类型、读写属性、系统密钥文件的密钥代码（见6.3.1和6.3.2）；

——修改了OBE的应用预留文件规定（见6.3.4，2007年版6.3.4、6.3.5和6.3.6）；

——修改了“GetSecure服务原语”中信息鉴别的MAC计算方法（见7.2，2007年版7.2）；

——修改了“SetSecure服务原语”中信息鉴别的MAC计算方法（见7.3，2007年版7.3）；

——增加了SetMMI中人机交互指示内容标识（见7.6.1）；

——增加了ETC交易流程的规定（见9）；

——增加了多个T-APDU拼接在同一个LSDU中的数据帧的规定（见附录B）；

——增加了ETC交易流程中复合消费交易应用的DSRC数据帧的定义（见附录B）。

本部分由全国智能运输系统标准化技术委员会（SAC/TC268）提出并归口。

本部分起草单位：交通运输部公路科学研究院、北京聚利科技股份有限公司、深圳市金溢科技股份有限公司、北京速通科技有限公司、北京万集科技股份有限公司等。

本部分主要起草人：

电子收费 专用短程通信 第4部分：设备应用

1 范围

本部分规定了用于电子收费（ETC）的专用短程通信设备的应用总则、技术要求、数据结构、应用接口和应用安全、交易流程。

本部分适用于公路和城市道路电子收费系统，自动车辆识别、车辆出入管理等领域可参照使用。

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 2423 电工电子产品环境测试

GB 4208 外壳防护登记（IP代码）

GB/T 20135-2006 智能运输系统 电子收费 系统框架模型

GB/T 20839-2007 智能运输系统 通用术语

GB/T XXXXX.1-XXXX 电子收费 专用短程通信 第1部分：物理层

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

GB/T XXXXX.3-XXXX 电子收费 专用短程通信 第3部分：应用层

JR/T 0025-2005 中国金融集成电路（IC）卡规范

ISO/IEC 7816 识别卡－带触点的集成电路卡

ISO/IEC 14443 识别卡－非接触卡规范

UL1642 美国锂电池安全标准

UN38.3 2009（5th Edition） 运输安全标准

3 术语、定义和缩略语

3.1 术语和定义

GB/T 20135-2006和GB/T 20839-2007中界定的术语适用于本文件。

3.2 缩略语

下列缩略语适用于本部分。

AVI 自动车辆识别（Automatic Vehicle Identification）

DID 目录标识（Directory Identifier）

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

ETC 电子收费（Electronic Toll Collection）

FID 文件标识（File Identifier）

ICC 集成电路卡（Integrate Circuit Card）

MAC 信息鉴别码（Message Authentication Code）

MTC 人工半自动收费（Manual Toll Collection）

OBE 车载设备（On Board Equipment）

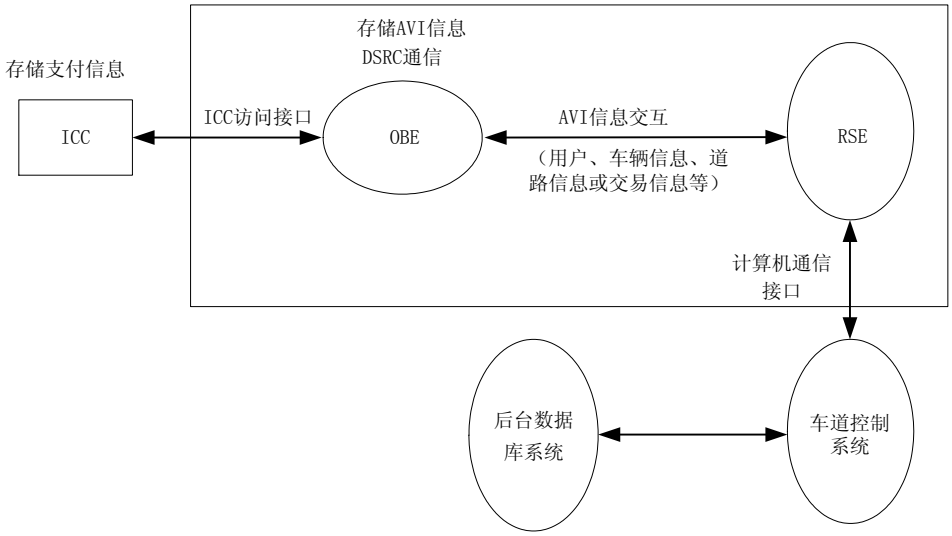
RSE 路侧设备（Roadside Equipment）

4 应用总则

4.1 ETC 系统构成

ETC系统由前端系统和后台数据库系统组成，前端系统包括车道控制系统、RSE、OBE以及ICC。

OBE应为双片式类型，即应支持ICC的读写。在ETC应用中，涉及电子支付的功能由ICC实现，OBE提供ICC至RSE信息转发功能。系统构成见图1。



注：方框中的内容为本部分所涉及的内容。

图1 ETC系统构成

典型ETC交易示例见图2。

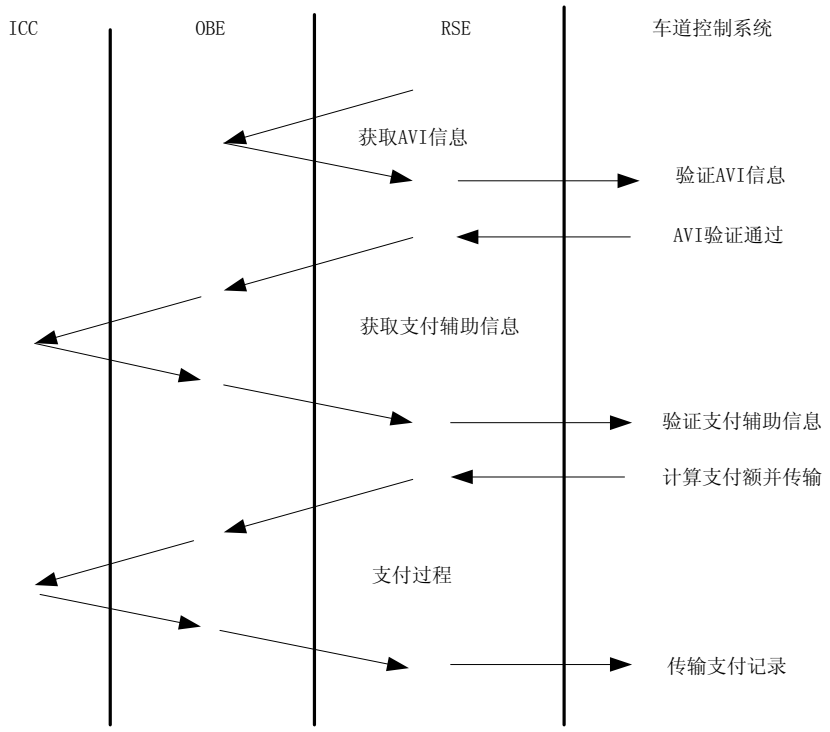


图2 ETC交易示例

4.2 OBE 数据一般规定

OBE内的数据采用目录与文件进行组织。

OBE内目录分为两类：系统目录及应用目录，系统目录为OBE的根目录，只有一个；应用目录是根目录下的子目录，可有多个，一个应用对应一个目录。每个目录下有多个文件，子目录下不应有其他子目录。

文件分为密钥文件和应用文件两类：密钥文件存储用以控制应用数据的安全访问的密钥；应用文件用于存储应用数据。

目录和文件分别以DID和FID来标识。目录编号DID范围为0x00－0x0F，其中DID为0x00者为根目录。文件编号FID范围为0x00－0x7F，其中FID为0x00者为密钥文件。根目录下的文件为系统文件，应用文件存储于应用目录中。对于ETC应用，目录号应为0x01。

OBE内的数据组织结构见表1。

表 1 OBE 数据组织结构表

目录/文件			ASN.1 数据结构[a]
0x00 根目录	0x00　系统密钥文件		SysKeyFile
	0x01　系统信息文件		SysInfoFile
	…		…
	0x01　ETC 应用目录	0x00　ETC 应用密钥文件	EtcAppKeyFile
		0x01　ETC 应用车辆信息文件	EtcAppVehicleFile
		…	…
	… 其它应用目录	…	…

4.3　OBE 密钥

密钥分为四类：主控密钥、维护密钥、认证密钥和加密密钥。主控密钥分系统主控密钥和应用主控密钥，系统主控密钥在系统密钥文件中，应用主控密钥在对应的应用密钥文件中。密钥的功能见表2。

表2 密钥功能

密钥类型	密钥功能	应用过程
主控密钥	（1）　认证通过后可创建文件； （2）　对自身进行安全写入； （3）　对同目录下其它密钥的安全写入； （4）　根目录下的主控密钥用于子目录主控密钥的写入	发行
维护密钥	本目录文件的安全方式写入	发行
认证密钥	本目录文件访问读写权限控制	交易
加密密钥	传输过程中数据的加密与解密处理	交易

4.4　文件属性

文件访问由密钥控制。

目录和文件的删除与创建在主控密钥的控制下进行。

普通文件（非密钥文件）有四种属性，见表3。

表3 文件属性

属性	描述
自由	自由读或写，不需要任何认证或加密处理，传输为明文数据
认证	认证后可以读或写，传输为明文数据
加密	读或写的数据内容进行加密处理，传输为密文数据
禁止	禁止读或者禁止写的权限

4.5　扩展应用接口

ETC设备应提供基于ACTION服务原语（见GB/T XXXXX.3-XXXX(电子收费 专用短程通信 第3部分：应用层)）所扩展的应用接口，见表4。

表4 扩展ETC应用接口

操作类型 (ActionType)	操作名称	描述
0	GetSecure	安全文件读取，提供MAC和安全加密接口
1	SetSecure	安全文件写入，提供MAC和安全加密接口
2	GetRand	取随机数，用于安全用途
3	TransferChannel	通道传输，用于向OBE部件传输APDU
4	SetMMI	设置人机界面，规范OBE需统一指示的内容

5 关键设备总体技术要求

5.1 OBE 总体技术要求

5.1.1 无线链路通信

OBE 和 RSE 之间的 DSRC 应符合 GB/T XXXXX.1-XXXX(电子收费 专用短程通信 第 1 部分：物理层)、GB/T XXXXX.2-XXXX(电子收费 专用短程通信 第 2 部分:数据链路层)、GB/T XXXXX.3-XXXX(电子收费 专用短程通信 第 3 部分：应用层)的相关规定。

5.1.2 安全

OBE 应提供安全访问模块，以存放访问控制密钥和 ETC 应用信息等。

OBE 应支持 SM4 算法的数据存取和访问控制。

OBE 中所有初始化数据的写入应采用 SM4 算法的加密方式传输。

OBE 应具备 ICC 读写接口，该接口应符合 ISO/IEC 7816 或 ISO/IEC 14443 TYPE-A 标准的相关规定。

OBE 支持的 ICC 交易流程应符合 JR/T 0025-2010。

5.1.3 信息存储

OBE 内的用户信息存储宜采用数据块的方式，寻址应采用目录和文件的方式。

OBE 内的安全访问模块应具有不小于 16k 字节存储空间。

5.1.4 部件

5.1.4.1 标准配置部件

OBE 应配置的部件：ICC 读写接口。

5.1.4.2 可选配置部件

OBE 可选的配置部件：扬声器、字符显示器、红绿指示灯、USB 接口、RS232 串口、蓝牙模块等。

5.1.5 防拆卸与恢复

OBE 应具备防止用户拆卸功能，一旦被拆卸，应当立即在 OBE 内的相应信息存储区中设置相应标志字节/标志位。

因拆卸而引起的 ETC 应用失效应能够通过软件设置的方式得到恢复。

5.1.6 应用的更新

OBE 应支持应用更新，更新可采用 DSRC 方式或有线方式。

5.1.7 交易记录

OBE 应支持不少于 50 条最新交易记录的存储，交易记录可采用 DSRC 方式或有线方式读出。

5.1.8 电池

OBE 电池应具备安全性，应通过 UL 1642 和 UN 38.3 认证。

5.1.9 可靠性

OBE 平均无故障时间应大于 50,000h。

5.1.10 平均免维护时间

OBE平均免维护时间不小于2年（按每天10次交易计算）。

5.1.11 环境条件

环境条件应符合：

a) 工作温度： 一般要求-25℃～+70℃（寒区-40℃～+70℃）；

b) 存储温度：-40℃～+70℃；

c) 相对工作湿度：5%～100%；

d) 静电：8kV；

e) 振动：应符合 GB/T 2423.13；

f) 冲击：应符合 GB/T 2423.6 试验 Eb 和导则。

5.1.12 其他要求

OBE 唤醒灵敏度可分为以下几档可调：-43dBm～-47dBm；-48dBm～-52dBm；-53dBm 以上。

OBE 的等效全向辐射功率可分为以下几档可调：-3dBm～+3dBm；+3dBm～+10dBm。

5.2 RSE 总体技术要求

5.2.1 工作方式

RSE 采用联机工作方式。

RSE 应提供应用层服务原语接口。

5.2.2 无线链路通信

RSE 和 OBE 之间的 DSRC 应符合 GB/T XXXXX.1-XXXX(电子收费 专用短程通信 第 1 部分：物理层)、GB/T XXXXX.2-XXXX(电子收费 专用短程通信 第 2 部分:数据链路层)、GB/T XXXXX.3-XXXX(电子收费 专用短程通信 第 2 部分：应用层)的相关规定。

5.2.3 安全

RSE 应设置安全访问模块或者达到同样安全等级的芯片、板卡或辅助设备等，以存放访问控制密钥，所有的加密和认证过程均通过安全硬件产品进行。

5.2.4 接口

RSE 应支持以太网方式的上位机通信接口，其他 RS232、RS485 或 USB 等接口形式可选。

RSE 应具有网络监测接口，支持 RSE 关键参数、配置管理、版本管理、诊断测试、日志管理、告警等信息的监测功能。

RSE 宜具有 TTL 电平的光电隔离接口。

5.2.5 程序和应用的更新

RSE应具有通过上位机接口进行在线程序和应用更新的能力。

5.2.6 安装

固定安装方式的RSE设备支持户外安装，防护等级应满足GB 4208的要求，并可采用路侧或者顶挂方式；宜采用顶挂安装方式，且吊装在车道正中，挂装高度不低于5.5m。

5.2.7 通信区域

RSE设备通信区域宽度应可调整在3.3m范围内，见图3。

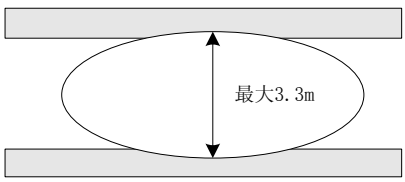


图 3 通信区域宽度示意图

5.2.8 供电

RSE设备应采用220V/50Hz交流电源供电。

5.2.9 可靠性

RSE 平均无故障时间应大于 70 000h。

5.2.10 环境条件

环境条件应符合：

a) 工作温度：一般要求-20℃～+55℃（寒区-35℃～+40℃）；
b) 存储温度：-40℃～+85℃；
c) 相对工作湿度：4%～100%；
d) 静电：8kV；
e) 振动：应符合 GB/T 2423.13；
f) 冲击：应符合 GB/T 2423.6 试验 Eb 和导则；
g) 盐雾：应符合 GB/T 2423.18；
h) 雷击：抗 4kV 10/200μs 雷击。

5.2.11 其他要求

RSE等效全向辐射功率应在GB/T XXXXX.1-XXXX规定的指标范围内并可调节。

6 OBE 数据结构

6.1 数据结构

OBE的数据分为系统数据和应用数据两类，数据结构见表5。

表5 OBE数据结构

目录号	文件号	文件名称	ASN.1 数据结构定义
0	0	系统密钥文件	SysKeyFile
	1	系统信息文件	SysInfoFile
1	0	ETC 应用密钥文件	EtcKeyFile
	1	ETC 应用车辆信息文件	EtcVehicleFile
	2	ETC 应用交易记录文件	EtcTransactionFile
	3	ETC 应用保留文件	EtcReservedFile
…	…	…	…
15	0	保留	…

6.2 系统数据

6.2.1 系统密钥文件

系统密钥文件的目录号为0，文件号为0，ASN.1定义为SysKeyFile, 系统密钥文件存储OBE系统信息安全访问控制密钥，文件内容见表6。

表6 系统密钥文件

序号	字段名称	ASN.1 类型	字段内容
1	sysMasterKey	Key	系统主控密钥
2	sysMaintainKey	Key	系统维护密钥

6.2.2 系统信息文件

系统信息文件的目录号为0，文件号为1，ASN.1定义为SysInfoFile,存储OBE发行及合同相关信息，文件内容见表7。

表7 系统信息文件

序号	字段名称	ASN.1 类型	字段内容
1	contractProvider	OCTET STRING (SIZE(8))	服务提供商名称
2	contractType	INTEGER(0..127, ...)	协约类型
3	contractVersion	INTEGER(0..127, ...)	合同版本
4	contractSerialNumber	ContractSerialNumber	合同序列号
5	contractSignedDate	Date	合同签署日期
6	contractExpiredDate	Date	合同过期日期
7	tamperedStatus	INTEGER(0..255)	拆卸状态
8	reserved	OCTET STRING (SIZE(72))	预留

6.3 ETC 应用数据

6.3.1 ETC 应用密钥文件

ETC应用密钥文件目录号为1，文件号为0，ASN.1定义为EtcKeyFile，存储OBE的ETC应用数据安全访问控制密钥，文件内容见表8。

表8 ETC应用密钥文件

序号	字段名称	ASN.1 类型	字段内容
1	etcMasterKey	Key	ETC 应用主控密钥
2	etcMaintainKey	Key	ETC 应用维护密钥
3	etcAccessKey	Key	ETC 应用认证密钥
4	etcEncryptKey	Key	ETC 应用加密密钥

6.3.2 ETC 应用车辆信息文件

ETC应用车辆信息文件目录号为1，文件号为1，ASN.1定义为EtcVehicleFile，文件内容见表9。

表9 ETC应用车辆信息文件

序号	字段名称	ASN.1 类型	字段内容
1	vehicleLicencePlateNumber	OCTET STRING (SIZE(12))	车牌号
2	vehicleLicencePlateColor	OCTET STRING (SIZE(2))	车牌颜色
3	vehicleClass	INTEGER(0..127, ...)	车型
4	vehicleUserType	INTEGER(0..127, ...)	车辆用户类别
5	vehicleDimensions	VehicleDimensions	车辆尺寸
6	vehicleWheels	INTEGER(0..127, ...)	车轮数
7	vehicleAxles	INTEGER(0..127, ...)	车轴数
8	vehicleWheelBases	INTEGER(0..65535)	轴距
9	vehicleWeightLimits	INTEGER(0..2^{24}-1)	车辆载重/座位数
10	vehicleSpecificInfomation	OCTET STRING(SIZE(16))	车辆特征描述
11	vehicleEngineNumber	OCTET STRING(SIZE(16))	车辆发动机号
12	vehicleReserved	OCTET STRING(SIZE(20))	保留字段

6.3.3 ETC 应用交易记录文件

ETC应用交易记录文件目录号为1，文件号为2，ASN.1定义为EtcTransactionFile，ETC交易记录空间写满时，记录用先入先出的方式循环进入记录区,文件内容见表10。

表10 ETC应用交易记录文件

序号	字段名称	ASN.1 类型	字段内容
1	recordCount	INTEGER(0..127, ...)	记录数
2	record1Length	INTEGER(0..127, ...)	第一条记录的长度
3	record1	OCTET STRING (SIZE(record1Length))	第一条记录内容
4	record2Length	INTEGER(0..127, ...)	第二条记录的长度
5	record2	OCTET STRING (SIZE(record2Length))	第二条记录内容
…	…	…	…
2n	recordnLength	INTEGER(0..127, ...)	第 n 条记录的长度
2n＋1	recordn	OCTET STRING (SIZE(recordnLength))	第 n 条记录内容

6.3.4 ETC 应用保留文件

ETC应用应预留保留文件。

7 ETC 应用接口

7.1 ACTION 服务原语

ETC应用在应用层服务原语ACTION之上扩展出ETC应用接口，其中ACTION服务原语如下：

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

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

ActionType::=INTEGER(0..127,...)
    － 已经定义如下操作：
    －  0  GetSecure
    －  1  SetSecure
    －  2  GetRand
    －  3  TransferChannel
    －  4  SetMMI
```

ActionType中，5…80 保留给DSRC应用，81…127保留给私有应用。

7.2 GetSecure 服务原语

7.2.1 功能

GetSecure用于实现安全的数据读取，并提供可选的认证、加密和信息鉴别的机制。其中：

a） 认证：RSE端提供访问凭证，OBE端验证通过后才允许读取；

b） 加密：OBE端对数据加密后再传输到RSE端，RSE端需对之解密后才可获取原始数据；

c） 信息鉴别：对所传输的数据进行加密运算产生MAC，随数据后一起传输；RSE端接收到首先对之进行验证,无误后进行后续处理。

本接口中，a）和b）为可选项，c）为必备项；对于无需b）或c）的情形，需调用Get服务实现。

上述三者视安全要求可组合运用。

如果同时出现b）和c）的情形，先计算MAC后再加密。

7.2.2 接口

7.2.2.1 请求（GetSecure.request）

GetSecure.request参数要求见表11。

表11 GetSecure.request参数要求

参数	取值	参数说明
mode	TRUE	确认模式，需应答
did	Dsrc-DID	ETC应用等于1
actionType	0	等于0
accessCredentials	—	可选

actionParameter	GetSecureRq::=SEQUENCE{
	fill BIT STRING (SIZE(7)),
	fileid FID,
	offset INTEGER(0..32767,...),
	length INTEGER(0..127,...),
	rndRsuForAuthen Rand,
	keyIdForAuthen INTEGER(0..255),
	keyIdForEncrypt INTEGER(0..255) OPTIONAL
	}
		
		文件标识
		操作数据起始位置
		操作数据长度
		产生MAC用随机数
		产生MAC用密钥索引号
		加密密钥索引号

iid	—	不存在

7.2.2.2 应答（GetSecure.response）

GetSecure.response参数要求见表12。

表12 GetSecure.response参数要求

参数	取值	参数说明
did	Dsrc-DID	ETC应用对应1

responseParameter	GetSecureRs::=SEQUENCE {
	fileid FID,
	file File,
	authenticator OCTET STRING (SIZE(8))
	}
		可选
		文件标识
		读取的数据（可能加密）
		鉴别码

iid	—	不存在
ret	ReturnStatus	必备

7.3 SetSecure 服务原语

7.3.1 功能

SetSecure用于实现安全的数据写入，并提供可选的认证、加密和信息鉴别的机制。其中：

a) 认证：RSE端提供访问凭证，OBE端验证通过后才允许读取；

b) 加密：OBE端对数据加密后再传输到RSE端，RSE端需对之解密后才可获取原始数据；

c) 信息鉴别：对所传输的数据进行加密运算产生信息鉴别码，随数据后一起传输；RSE端接收到首先对之进行验证,无误后进行后续处理。

本接口中，a）和b）为可选项，c）为必选项；对于无需b）或c）的情形，需调用Set服务实现。

上述三者示安全要求可组合运用。

如果同时出现b）和c）的情形，先计算MAC后再加密。

7.3.2 接口

7.3.2.1 请求（SetSecure.request）

SetSecure.request参数要求见表13。

表13 SetSecure.request参数要求

参数	取值	参数说明
mode	TRUE	确认模式，需应答
did	Dsrc-DID	ETC应用等于1
actionType	1	等于1
accessCredentials	—	可选

actionParameter	SetSecureRq::=SEQUENCE{
	fill BIT STRING (SIZE(7)),
	fileid FID,
	offset INTEGER(0.. 32767,...),
	length INTEGER(0..127,...),
	file File,
	rndRsuForAuthen Rand,
	keyIdForAuthen INTEGER(0..255),
	keyIdForEncrypt INTEGER(0..255) OPTIONAL
	}
		
		文件标识
		操作数据起始位置
		操作数据长度
		数据内容（可能加密）
		产生MAC用随机数
		产生MAC用密钥索引号
		加密密钥索引号

iid	—	不存在

7.3.2.2 应答（SetSecure.response）

SetSecure.response参数要求见表14。

表14 SetSecure.response参数要求

参数	取值	参数说明
did	Dsrc-DID	ETC应用等于1
responseParameter	—	不存在
iid	—	不存在
ret	ReturnStatus	必备

7.4 GetRand 服务原语

7.4.1 功能

GetRand服务用于获取8字节随机数。

7.4.2 接口

7.4.2.1 请求（GetRand.request）

GetRand.request参数要求见表15。

表15 GetRand.request参数要求

参数	取值	参数说明
mode	TRUE	确认模式，需应答
did	Dsrc-DID	ETC应用等于1
actionType	2	等于2
accessCredentials	—	可选
actionParameter	—	不存在
iid	—	不存在

7.4.2.2 应答（GetRand.response）

GetRand.response参数要求见表16。

表16 GetRand.response参数要求

参数	取值	参数说明
did	Dsrc-DID	ETC应用等于1

responseParameter	GetRandRs::=SEQUENCE {
	rand Rand
	}
		可选
		随机数

iid	—	不存在
ret	ReturnStatus	必备

7.5 TransferChannel 服务原语

7.5.1 功能

为RSE与OBE部件之间（如ICC、显示器、蜂鸣器等）通信提供通道传输功能，OBE充当RSE与外部件之间的转发器。已经定义的外部件通道标识号见表17。

表17 通道标识号定义表

通道标识号 (ChannelID)	名称	说明
0	OBE	OBE本身
1	ICC	ICC
2	SAM	SAM模块
3	DISPLAY	显示器
4	BEEPER	蜂鸣器
5	SPEAKER	扬声器
6	PRINTER	打印设备
7	SERIAL INTERFACE	串行口
8	USB	USB接口
9	PARALLEL INTERFACE	并行口

7.5.2 接口

7.5.2.1 请求（TransferChannel.request）

TransferChannel.request参数要求见表18。

表18 TransferChannel.request参数要求

参数	取值	参数说明
mode	TRUE	确认模式，需应答
did	Dsrc-DID	ETC应用等于1
actionType	3	等于3
accessCredentials	—	可选

actionParameter	ChannelRq::=SEQUENCE{
	channelid ChannelID,
	apdu ApduList
	}
		
		通道标识号
		通道指令数据

iid	—	不存在

7.5.2.2 应答（TransferChannel.response）

TransferChannel.response参数要求见表19。

表19 TransferChannel.response参数要求

参数	取值	参数说明
did	Dsrc-DID	ETC应用等于1
responseParameter	ChannelRs::=SEQUENCE { channelid ChannelID, apdu ApduList }	可选 通道标识号 通道应答数据
iid	—	不存在
ret	ReturnStatus	必备

7.6 SetMMI服务原语

7.6.1 功能

用于规范OBE应用人机界面指示的内容，已经要求指示的内容见表20。

表20 MMI标识定义

指示内容标识	名称	说明
0	ok	交易处理正常完成
1	error	交易处理异常
2	contactOperator	请联系运营商
3	noCard	无卡

7.6.2 接口

7.6.2.1 请求（SetMMI.request）

SetMMI.request参数要求见表21。

表21 SetMMI.request参数要求

参数	取值	参数说明
mode	TRUE	确认模式，需应答
did	Dsrc-DID	ETC应用等于1
actionType	4	等于4
accessCredentials	—	不存在
actionParameter	SetMMIRq::=INTEGER{ ok (0), error (1), contactOperator (2), noCard （3） } (0..127,...)	 0：正常 1：异常 2：与运营商联系 3：无卡
iid	—	不存在

7.6.2.2 应答（SetMMI.response）

SetMMI.response参数要求见表22。

表22 SetMMI.response参数定义

参数	取值	参数说明
did	Dsrc-DID	ETC应用等于1
responseParameter	—	不存在
ret	ReturnStatus	必备

8 ETC 应用安全

8.1 安全方式

主要安全保护手段有：

a) 访问许可：访问数据应提供许可凭证，OBE 验证通过后才允许访问；

b) 信息鉴别：随关键数据一起传送一组鉴别码，RSE 验证后才认为为合法数据；

c) 加密保护：在传输过程中对数据进行加密。

8.2 访问许可

OBE 访问许可认证通过后，RSE 具备访问权限，访问许可见图 4。过程如下：

a) RSE 通过 Get 服务取得 contractSerialNumber,通过 GetRand 服务或直接从 VST 中获取 RndOBE，RndOBE 宜从 VST 中获取；

b) RSE 利用 MasterAccessKey（主认证密钥，16 字节）和 contractSerialNumber 分散出临时认证密钥 tmpAccessKey（16 字节），分散算法如下：

tmpAccessKey＝SM4(MasterEtcAppAccessKey, contractSerialNumber)

c) RSE 利用临时密钥 tmpAccessKey 加密 RndOBE(8 字节)，产生 accessCredentials，算法如下：

accessCredentials＝SM4(tmpAccessKey, RndOBE)

d) RSE 后续指令携带 accessCredentials，发送到 OBE；

e) OBE 利用 AccessKey 和 RndOBE 计算出 tmpAccessCredentials，算法同 c)；

f) OBE 比较 accessCredentials 和 tmpAccessCredentials 是否相等，相等则赋予该 RSE 访问许可权限。

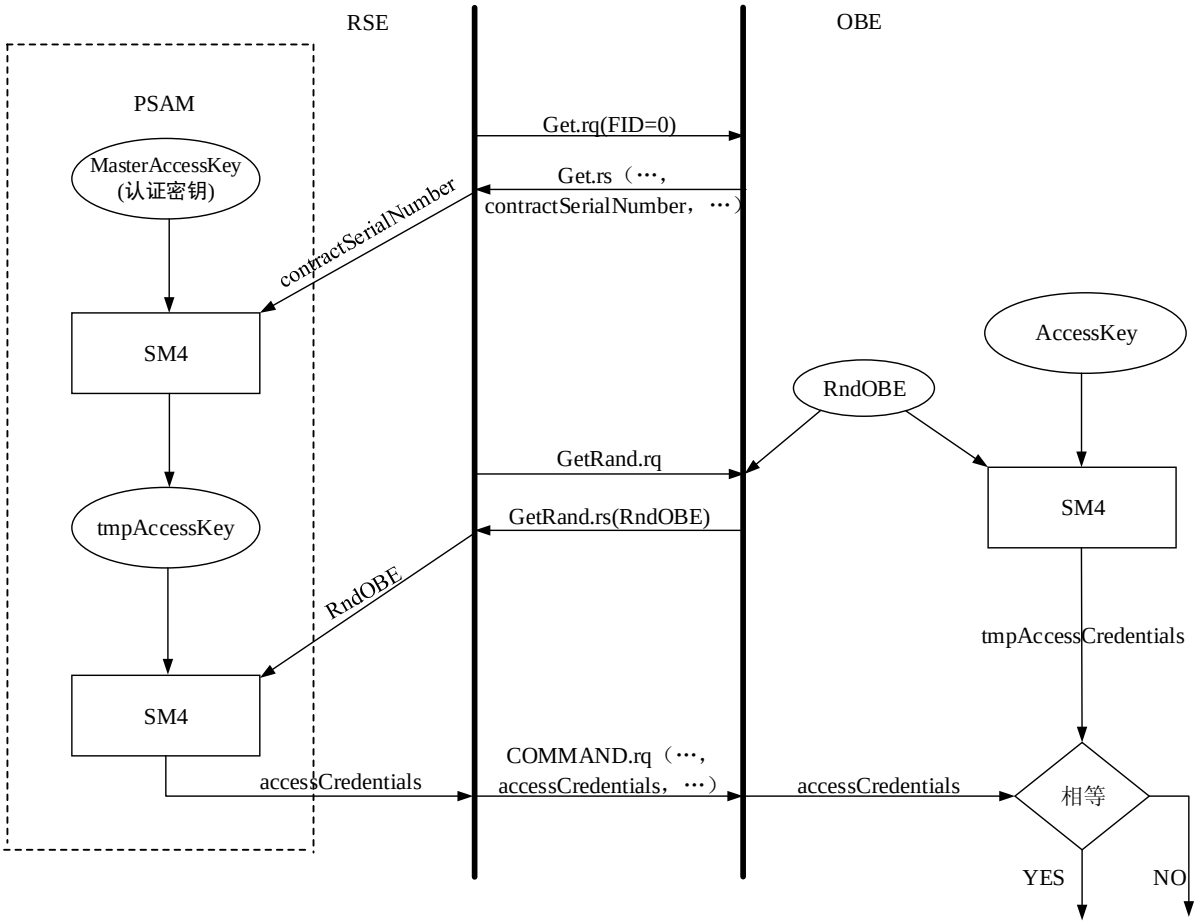


图 4 访问许可认证

8.3 信息鉴别

信息鉴别主要是针对 OBE 信息的鉴别，以鉴别码的方式实现，信息鉴别见图 5。过程如下：

a) RSE 通过 Get 服务取得 contractSerialNumber；

b) RSE 产生随机数 rndRSUForAuthen(8 字节)，并随 GetSecure 服务一起发送至 OBE；

c) OBE 利用 EncryptKey（16 字节）对 rndRSUForAuthen、File 内容进行 MAC 计算，得出鉴别码 authenticator 并随 File 一起作为响应参数发往 RSE。其中 MAC 计算方法如下：

1) 将 File 内容进行 CRC 计算（多项式 $X^{16}+X^{12}+X^5+1$，起始 FFFFH），产生两字节 CRC0 和 CRC1；

2) 将 rndRSUForAuthen 最低两个字节分别更换为 CRC1，CRC0，形成 8 字节临时数据；

3) 利用 EncryptKey 对 8 字节数据进行加密计算产生 authenticator，算法如下：

authenticator＝SM4(EncryptKey, CRC0||CRC1||rndRSUForAuthen（高 6 字节））

d) OBE 在响应中发送 File 和 authenticator 至 RSE；

e) RSE 利用 contractSerialNumber 和 MasterEncryptKey 计算出临时密钥 tmpEncryptKey（16 字节），算法如下：

tmpEncryptKey＝SM4(MasterEtcAppAuthenKey, contractSerialNumber)

f) RSE 利用临时密钥 tmpKey、rndRSUForAuthen 及 File，遵循 c）中的算法计算 MAC 码 tmpAuthenticator；

g) RSE 比较 authenticator 和 tmpAuthenticator，如果结果相等则为合法数据，否则非法。

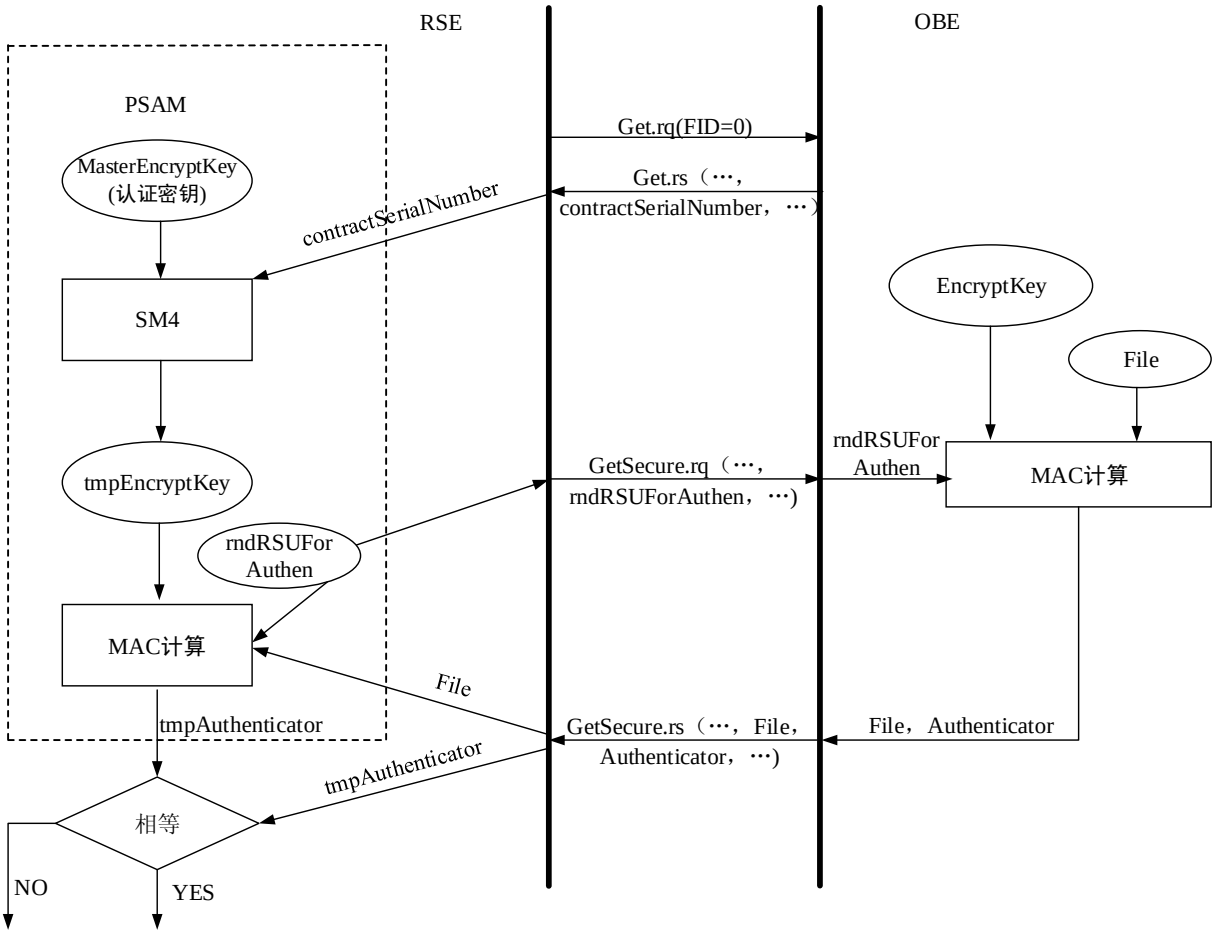


图 5 OBE 信息鉴别

8.4 获取信息加密

获取 OBE 信息加密算法基于 SM4 实现，见图 6。算法流程如下：

a) RSE 发送 GetSecure 服务至 OBE；

b) OBE 将文件数据按 8 字节分组，不足则补 0；

c) OBE 利用 EncryptKey 对上述结果(8 的整数倍长度)进行 TDES 解密，产生解密结果 decryptFile，算法如下：

$$decryptFile=SM4^{-1}\ (EncryptKey,\ Encrypfile)$$

d) OBE 将 decryptFile 随 GetSecure.rs 发送至 RSE；

e) RSE 利用 MasterEncryptKey 和 contractSerialNumber 产生临时加密密钥 tmpEncryptKey，算法如下：

$$tmpEncryptKey=SM4(MasterEncryptKey,\ contractSerialNumber)$$

f) RSE 利用 tmpEncryptKey 对 decryptFile 加密，结果去掉多余 0 字节后即为所读取数据内容。

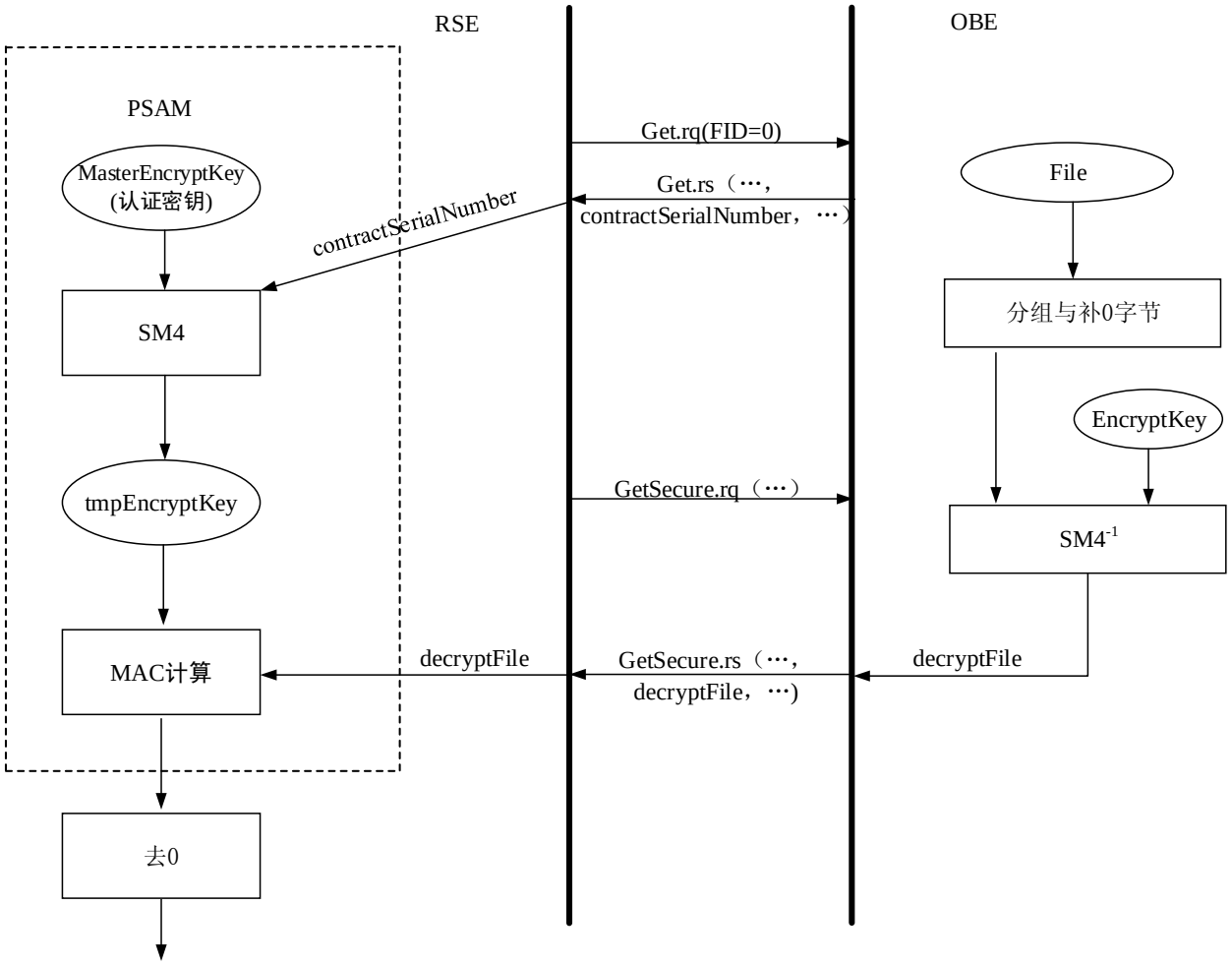


图 6 获取信息加密

8.5 写入信息加密

写入信息加密算法基于 SM4 实现，见图 7。算法流程如下：

a) RSE 将文件数据按 8 字节分组，不足则补 0；

b) RSE 利用 MasterEncryptKey 和 contractSerialNumber 产生临时加密密钥 tmpEncryptKey：

tmpEncryptKey=SM4(MasterEncryptKey, contractSerialNumber)

c) RSE 利用 tmpEncryptKey 对（a）结果加密，加密后的数据 decryptFile 随 SetSecure 服务发送至 OBE；

d) OBE 利用 EncryptKey 对 decryptFile（8 的整数倍长度）进行 SM4 解密，产生解密结果 decryptFile：

decryptFile=$SM4^{-1}$ (EncryptKey, Encrypfile)

e) OBE 将解密后的数据去掉多余 0 后写入 OBE 文件，并应答 SetSecure。

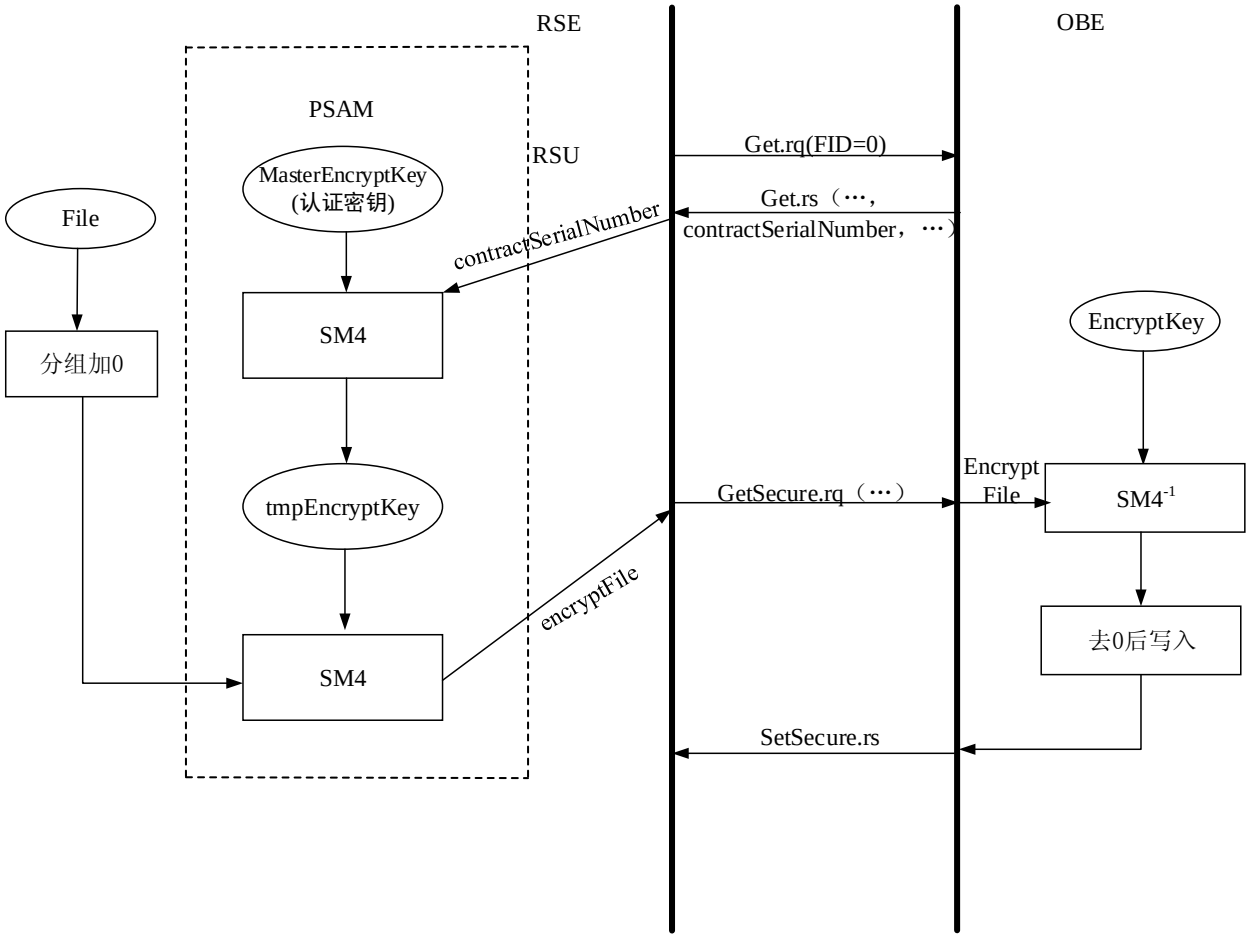


图 7 写入信息加密

9 ETC 交易流程

9.1 交易流程总体框架

9.1.1 通信阶段划分

ETC交易流程可划分为通信链路建立及应用信息获取、获取OBE数据、ICC-RSE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-RSE间安全认证过程包含在第三个阶段中。

在公路ETC应用中，ICC-RSE间交易采用复合消费交易模式。复合消费交易见JR/T 0025-2010规定，复合消费交易应用RSE和OBE交互DSRC数据帧格式见附录C。ICC为储值卡或记账卡。

9.1.1.1 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

9.1.1.2 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

9.1.1.3 ICC-RSE 消费交易阶段

使用多条TransferChannel完成ICC－RSE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

9.1.1.4 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

9.1.1.5 链路释放阶段

RSE释放与OBE的通信连接。

RSE：Event-Report(Release)。

9.1.2 原语拼接

交易中多个原语可通过拼接的方式实现，示例见附录B。

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 XXXXX.3。

9.2 DSRC 数据帧格式

9.2.1 概述

本节只描述了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。

9.2.2 BST

9.2.2.1 简要说明

LLC层使用UI命令。

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

9.2.2.2 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
    }
```

电子收费应用中无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。具体格式见9.3。

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

9.2.3 VST

9.2.3.1 简要说明

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

9.2.3.2 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 XXXXX.3中，applicationParameter的类型定义为ApplicationContextMark，其ASN.1定义如下：

```
ApplicationContextMark::=Container
        (WITH COMPONENTS {octetstring  PRENSENT})
    -- ApplicationContextMark的示例见附录A 中SysInfoFile的相关内容。
```

本标准在GB/T XXXXX.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。

在GB/T XXXXX.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，具体定义自行规定。

gbICCInfo 用于存放 ICC 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,  -- ICC
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))  --OBE 的系统信息文件第 27 字节“拆卸状态”
}
```

其中，iccType 的最低有效位（Bit4）指示 ICC 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 23。

表 23 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

9.2.4 GetSecure.request

9.2.4.1 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。

9.2.4.2 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9.2.3所述的VST中获得。

actionParameter　Container
为Container类型，Container.Type=20（GetSecureRq）
根据7.2中规定：

```
GetSecureRq::=SEQUENCE{
  fill                BIT STRING (SIZE(7)),
  fileid              FID,
  offset              INTEGER(0..32767,...),
  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，车辆信息文件的文件号 =1，取值1。

offset　INTEGER(0..32767,...),
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6.3.2中规定，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(20))
}
```

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。

9.2.5 GetSecure.response

9.2.5.1 简要说明

LLC层使用ACn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。

9.2.5.2 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）

根据7.2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。本应用下authenticator填入8字节的“0x00”。

9.2.6 TransferChannel.request

9.2.6.1 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ICC不需要DSRC层面的安全认证，故不需要accessCredentials.

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

9.2.6.2 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）

根据7.5中规定：

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

其中：

channelid　　ChannelID,

ChannelID取icc =1。

apdu　　ApduList

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

SEQUENCE OF中的每一个OCTET STRING包含一条完整ICC指令，ICC的指令格式见表24。

表 24 ICC 的命令格式

命令头				命令体		
CLA	INS	P1	P2	Lc	DATA	Le

9.2.7 TransferChannel.response

9.2.7.1 简要说明

LLC层使用ACn响应。

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

在ETC应用中，TransferChannel.response原语可通过RSE－OBE，提供一个返回OBE中ICC针对此前命令执行的响应的透明通道。

9.2.7.2 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）

根据7.5中规定：

```
ChannelRs::=SEQUENCE {
    channelid          ChannelID,
    apdu               ApduList
    }
```

其中：

```
channelid          ChannelID,
```

ChannelID取icc =1。

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

SEQUENCE OF中的每一个OCTET STRING包含一条完整ICC响应信息，ICC的响应信息格式见表25。

表 25 ICC 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。

响应信息的的顺序应当与TransferChannel.request原语中ICC命令的顺序严格对应。

9.2.8 SetMMI.request

9.2.8.1 简要说明

LLC层使用ACn命令。

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

根据7.6中规定，SetMMI中不需要accessCredentials。

9.2.8.2 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 XXXXX.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）

根据7.6中规定：

```
SetMMIRq::=INTEGER{
    ok              (0),    --交易正常
    error           (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）
} (0..127,...)
```

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”；
- 其它情况：不响。

9.2.9 SetMMI.response

9.2.9.1 简要说明

LLC层使用ACn响应。

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

9.2.9.2 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4.2中规定，取值为ETC应用 = 1。
```

9.2.10 Event-Report(Release)

9.2.10.1 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。

9.2.10.2 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。

9.3 BST 中 ICC 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 XXXXX.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  PRENSENT})
```

本标准在GB/T XXXXX.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ICC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26。

表 26 iccTransMode 结构定义

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

路侧系统所支持的ICC消费交易模式使用iccTransMode的高4比特（Bit4～Bit6）进行指示，其编码定义见表27。

表 27 路侧系统所支持的 ICC 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ICC消费交易模式使用iccTransMode中Bit1～Bit2进行指示，其编码定义见表28。

表 28 路侧系统优先采用的 ICC 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ICC的OBE预处理的快速交易模式。其编码定义见表29。

表 29 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ICC文件格式及相关信息的地区性应用差异，在GB/T XXXXX.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
    preReadFile0002     OCTET STRING (SIZE(2)) OPTIONAL, --需预读取ICC中0002文件偏移
                                                         --量和长度
    preReadFile0012     OCTET STRING (SIZE(2)) OPTIONAL, --需预读取ICC中0012文件偏移量
                                                         --和长度
    preReadFile0015     OCTET STRING (SIZE(2)) OPTIONAL, --需预读取ICC中0015文件偏移量
                                                         --和长度
    preReadFile0019     OCTET STRING (SIZE(2)) OPTIONAL --需预读取ICC中0019文件偏移量
                                                         --和长度
    }
```

注：在公路ETC应用中，ICC-RSE间交易采用复合消费交易模式,0002文件为ICC中电子钱包文件偏移量和长度，0012文件为ICC中收费信息文件偏移量和长度，0015文件为卡片发行基本数据文件偏移量和长度，0019文件为符合消费文件偏移量和长度。

其中，preReadFile00**用于指示RSE预读的各文件的偏移量和长度。结构定义见表30。

表 30 preReadFile0*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31。

表 31 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							

9.4 OBE 对 ICC 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ICC进行预处理。

contractVersion的编码规则见表32。

表 32 contractVersion 的编码规则

扩展标志 Bit7	Bit6～Bit4	Bit3～Bit0
0－ 无扩展	0 ： OBE 对 ICC 不做预处理 1： OBE 对 ICC 做预处理 2 ～ 7：保留	1 ： OBE～RSE 之间采用进行安全认证 2 ～ 15 ： 保留

9.5 VST 中应携带的 ICC 相关信息

在公路ETC应用中，ICC-RSE交易采用的复合消费交易模式时，OBE可通过VST携带ICC的相关预读信息，获取公路ETC应用所需文件。

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ICC的相关预读信息。

本标准在GB/T XXXXX.3的基础上对Container进行扩充定义如下：

```
Container::=CHOICE{
    ...,
    gbICCInfo       [40] GBICCInfo, --存放ICC的相关预读信息
    ...
}
```

GBICCInfo的ASN.1类型定义为：

```
GBICCInfo ::=SEQUENCE {
  iccIssueInfo      OCTET STRING (SIZE(0..127,…)),
  iccUniTollInfo    OCTET STRING (SIZE(0..127,…)),
  iccBalance        OCTET STRING (SIZE(0..127,…))
}
```

iccIssueInfo中存放ICC “发行基本数据文件”的相关信息，iccUniTollInfo中存放ICC “联网收费信息文件”或“复合消费专用文件”中的相关信息，iccBalance中存放ICC “电子钱包文件”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 ICC 所支持的消费交易模式，其编码定义见表 33。

表 33 OBE 所支持的 ICC 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	-	-	-

ICC 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 ICC 的“应用版本号”。

9.6 DSRC 交易之外的 OBE 应用处理流程

VST 中的预读信息（gbICCInfo）应当在车辆（OBE）进入天线通信区域之前预先从 ICC 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（gbICCInfo）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 ICC 从 OBE 中拔出时，OBE 应自动删除前述各项预读信息（gbICCInfo）。

OBE 进入天线通信区域被唤醒之后，OBE 将用户 ICC 上电后应当进入 ETC 应用目录，进入待交易状态。

附 录 A
（规范性附录）
OBE 的 ASN.1 型数据结构

```
ETCModule  DEFINITIONS::= BEGIN
   -- EXPORTS everything;
        Container1-0::=[20] GetSecureRq
        Container1-1::=[21] GetSecureRs
        Container1-2::=[22] SetSecureRq
        Container1-3::=[23] SetSecureRs
        Container1-4::=[24] ChannelRq
        Container1-5::=[25] ChannelRs
        Container1-6::=[26] SetMMIRq
        Container1-7::=[27] SetMMIRs
        Container1-8::=[28] Key
        Container1-9::=[29] Rand
        Container1-10::=[30] Date

        Container1-11::=[31] SysKeyFile
        Container1-12::=[32] SysInfoFile
        Container1-13::=[33] EtcKeyFile
        Container1-14::=[34] EtcVehicleFile
        Container1-15::=[35] EtcTransactionFile
        Container1-16::=[36] MidStationFile
        Container1-17::=[37] ErpAPPFile
        Container1-18::=[38] EtcReservedFile

        Container1-19::=[39] SysInfo --存放OBE中SysInfoFile中的部分内容
        Container1-20::=[39] GBICCInfo  --存放相关预读信息
        Container1-21::=[39] PretreatmentParameter --指示预处理操作参数的reservedInfo

        ChannelID::=INTEGER{
            obe              (0),
            icc              (1),
            sam              (2),
            display          (3),
            beeper           (4),
            printer          (5),
            serialInterface  (6),
            parallelInterface (7)
        }(0..127,...)

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

        BSTApplicationContextMark ::= SEQUENCE {
```

```
    iccTransMode            BIT STRING (SIZE(7)),
    reservedInfo            Container       OPTIONAL
}

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

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

ContractSerialNumber::=SEQUENCE{
    contractProviderID          OCTET STRING (SIZE(2)),
    contractInividualID         OCTET STRING (SIZE(6))
    }
-- 由统一机构为contractProviderID编码

Date::=SEQUENCE{
    year    OCTET STRING(SIZE(2)),    -- BCD编码，YYYY
    month   OCTET STRING(SIZE(1)),    -- BCD编码，MM
    day     OCTET STRING(SIZE(1))     -- BCD编码，DD
    }

EtcKeyFile::=SEQUENCE{
    etcMasterKey            Key,    -- 16字节密钥
    etcMaintainKey          Key,
    etcAccessKey            Key,
    etcEncryptKey           Key
    }

MidStationFile::=OCTET STRING (SIZE(40))   --具体内容由标识站应用定义
EtcReservedFile::=OCTET STRING (SIZE(40))  --备ETC系统扩展用途
EtcTransactionFile::=SEQUENCE OF Record

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(20))
}
-- vehicleLicencePlateNumber：车牌号码，全牌照（汉字＋字母＋数字）信息，采用字符
  --型存贮，汉字采用GB2312码，如：“京”编码为“BEA9”。
-- vehicleLicencePlateColor：车牌颜色，二进制编码表示（0－蓝色，1－黄色，2－黑色，
   --3－白）。
-- vehicleClass：车辆类型，1字节，1-一型车；2-二型车；3-三型车；4-四型车；5-五型
  --车；6-六型车；7～10：自定义；11～20：用于计重收费货车车型分类。其中，11-一型
  --车；12-二型车；13-三型车；14-四型车；15-五型车；16-六型车；17～20：自定义计
  --重货车车型；21～--50：自定义；50～255：保留给未来使用。
-- vehicleUserType: 车辆用户类型，1字节，0-普通车；6-公务车；8-军警车；10-紧急车；
  --12-免费；14-车队；0～20内其他：自定义；21～255：保留给未来使用。
-- vehicleDimensions: 车辆尺寸，二进制分别表示长（2字节）、宽（1字节）、高（1字
  --节）。单位为分米。如0x012C、0x28、0x1E表示30米长、4米高、3米宽。
-- vehicleWheels: 车轮数，二进制表示的数目
-- vehicleAxles: 车轴数，二进制表示的数目。
-- vehicleWheelbases: 轴距，二进制表示，长度为2个字节，单位为分米。如0x28，表示
  --轴距为4米。
-- vehicleWeightLimits: 车辆载重（货车）或座位数（客车），二进制表示，单位为公斤
   --/座。
-- vehicleSpecificInfomation: 车辆特征描述，字符用ASCII编码表示，汉字用机内码表
   --示，如“奔驰307”。
-- vehicleEngineNumber：车辆发动机号。
-- vehicleReserved： 保留

ErpAppFile::=OCTET STRING (SIZE(40)) -- ERP应用自定义

GBICCInfo ::=SEQUENCE {
    iccIssueInfo        OCTET STRING (SIZE(0..127, ...)),
    iccUniTollInfo      OCTET STRING (SIZE(0..127, ...)),
    iccBalance          OCTET STRING (SIZE(0..127,...))
}

GetRandRs::=SEQUENCE {
    rand      Rand      -- 8字节随机数
    }

GetSecureRq::=SEQUENCE{
    fill                BIT STRING (SIZE(7)),
```

```
    fileid              FID,
    offset              INTEGER(0..32767,...),
    length              INTEGER(0..127,...),
    rndRsuForAuthen     Rand,
    keyIdForAuthen      INTEGER(0..255),
    keyIdForEncrypt     INTEGER(0..255) OPTIONAL
    }

GetSecureRs::=SEQUENCE {
    fileid              FID,
    file                File,
    authenticator       OCTET STRING (SIZE(8))
    }

Key::=OCTET STRING (SIZE(16))

PretreatmentParameter ::= SEQUENCE{
    fill                BIT STRING(SIZE(4)),
    sysInfoFileMode     BIT STRING (SIZE(8)), --系统信息文件预读长度
    preReadFile0002     OCTET STRING (SIZE(2)) OPTIONAL, --需预读取ICC中0002文件
                                                          --偏移量和长度
    preReadFile0012     OCTET STRING (SIZE(2)) OPTIONAL, --需预读取ICC中0012文件
                                                         --偏移量和长度
    preReadFile0015     OCTET STRING (SIZE(2)) OPTIONAL, --需预读取ICC中0015文件
                                                          --偏移量和长度
    preReadFile0019     OCTET STRING (SIZE(2)) OPTIONAL --需预读取ICC中0019文件
                                                         --偏移量和长度
    }
Rand::=OCTET STRING (SIZE(8))

SetMMIRq::=INTEGER{
    ok                  (0),    --交易正常
    error               (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）
    } (0..127,...)

SetSecureRq::=SEQUENCE{
    fill                BIT STRING (SIZE(7)),
    fileid              FID,
    offset              INTEGER(0..32767,...),
    length              INTEGER(0..127,...),
    file                File,
    rndRsuForAuthen     Rand,
```

```
    keyIdForAuthen      INTEGER(0..255),
    keyIdForEncrypt     INTEGER(0..255) OPTIONAL    --如果不选，表示数据没有加密
    }

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

SysInfoFile::= SEQUENCE{
    contractProvider            OCTET STRING (SIZE(8)),
    contractType                INTEGER(0..127,...),
    contractVersion             INTEGER(0..127,...),
    contractSerialNumber        ContractSerialNumber,
    contractSignedDate          Date,
    contractExpiredDate         Date,
    reserved                    OCTET STRING (SIZE(64))
}
--contractProvider：服务提供商，ASCII编码，服务提供商汉字简单描述，如“华北高速”
--contractType：服务类型，服务提供商所提供的服务种类，由各联网收费区域自定义（如
  --不同费率定义等）
-- contractVersion：服务版本，服务提供商提供的服务版本，由各联网收费区域自定义
-- contractSerialNumber：服务序列号，由服务商编号和个体序列号组成
-- contractSignedDate：合同签署生效日期，BCD编码 YYYYMMDD
-- contractExpiredDate：合同过期日期，BCD编码，YYYYMMDD

SysKeyFile::=SEQUENCE{
    sysMasterKey            Key,
    sysMaintainKey          Key
    }

VehicleDimensions::=SEQUENCE{
    vehicleLength               INTEGER(0..65535),
    vehicleWidth                INTEGER(0..255),
    vehicleHeigth               INTEGER(0..255)
    }

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
    }

END
```

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

B.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。

B.2 GetSecure.request ∪ TransferChannel.request

具体见表B.1。

表 B.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

B.3 GetSecure.response ∪ TransferChannel.response

具体见表B.2。

表 B.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 C
（资料性附录）
复合消费交易应用的 RSE～OBE 间 DSRC 数据帧定义

C.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。

C.2 封闭式入口

C.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：见9.2.2 。

C.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：见9.2.3 及9.5 “VST中应携带的ICC相关信息”。

C.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 的格式见 9.2.4 。

C.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 的格式请见 9.2.5 。

C.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 的格式见 9.2.6 ，其中 ApduList 的格式见表 C.1：

表C.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。

C.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 的格式见 9.2.7 ，其中 ApduList 的格式见表 C.2。

表C.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

C.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 的格式见 9.2.6 ，其中 ApduList 的格式见表 C.3。

表C.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 的格式见 9.2.8。

C.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 的格式见 9.2.7 ，其中 ApduList 的格式见表 C.4。

表C.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 的格式见 9.2.9 。

C.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：见 9.2.10

C.3 封闭式出口

C.3.1 BST

同 C.2.1。

C.3.2 VST

同 C.2.2。

C.3.3 GetSecure.request

同 C.2.3。

C.3.4 GetSecure.response

同 C.2.4。

C.3.5 TransferChannel.request I

同 C.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。

C.3.6 TransferChannel.response I

同 C.2.6。

C.3.7 TransferChannel.request II ∪ SetMMI.request

同 C.2.7。

C.3.8 TransferChannel.response II ∪ SetMMI.response

同 C.2.8。

C.3.9 EVENT-REPORT(Release)

同 C .2.9。