ICS 33.060.20
M 36

# T/ITS

# 中国智能交通产业联盟标准

T/ITS 0017-2014

# 电子收费 专用短程通信 支持扩展应用的关键设备：初始化设备

**Electronic toll collection Dedicated short range communication－ Key equipment supporting extended application:Issue equipment**

2014-11-24 发布 2015-01-01 实施

中国智能交通产业联盟 发布

# 目　　次

# 前　言

本标准按 GB/T 1.1—2009 给出的规则起草。

本标准由中国智能交通产业联盟提出并归口。

本标准起草单位：深圳市金溢科技有限公司、深圳成谷科技有限公司、交通运输部公路科学研究院、北京握奇智能科技有限公司、天津中兴智联科技有限公司、山东省交通科学研究所、北京万集科技股份有限公司、福建省海西物联网研究院。

本标准主要起草人：段作义、刘咏平、王笑京、宋向辉、段起志、孙志强、马国松、练源、代红娜、李健、于海、何辉。

本标准于 2014 年 11 月首次发布，本次为首次发布。

# 电子收费 专用短程通信

# 支持扩展应用的关键设备：初始化设备

## 1 范围

本部分规定了采用专用短程通信（DSRC）技术的电子不停车收费（ETC）系统中初始化设备的基本要求和组成、技术要求、功能和接口规范、环境及标志、包装、运输和贮存等。

本部分适用于高速公路、停车场电子不停车收费系统应用中的初始化设备，城市道路机动车限流收费等应用可参照使用。

## 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 20851.1-2007 电子收费 专用短程通信 第1部分：物理层

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

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

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

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

交通运输部2011年第13号公告《收费公路联网电子不停车收费技术要求》

## 3 术语、定义和缩略语

### 3.1 术语和定义

3.1.1

**OBU初始化**

用生产密钥替换OBU中ESAM内的初始密钥，并初始化文件信息。

3.1.2

**OBU个人化**

延长OBU“有效期”以及个人化车辆信息。

3.1.3

**OBU激活**

重置拆卸状态及延长OBU“有效期”。

3.1.4

**OBU检测**

读取车辆信息、系统信息以及卡片信息。

3.1.5

**可信发行网点**

已获得运营商授权认证的网点，允许联机和脱机发行操作。

3.1.6

**不可信发行网点**

未获得运营商授权认证的网点，只能联机发行操作。

3.1.7

**机卡联合认证**

机卡联合认证指同时使用管理员卡和初始化设备进行身份认证。

## 3.2 缩略语

下列缩略语适用于本部分。

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

ETC：电子收费(Electronic Toll Collection)

RSU：路侧单元(Road-Side Unit)

OBU：电子标签(On-Board Unit)

BST：信标服务部(Beacon Service Table)

VST：车辆服务表(Vehicle Service Table)

PSAM：消费访问安全模块(Payment Security Access Module)

ESAM：嵌入式安全控制模块(Embedded Secure Access Module)

AEI：汽车电子标识（Automotive electronic identification）

AVI：自动车辆识别（Automatic Vehicle Identification）

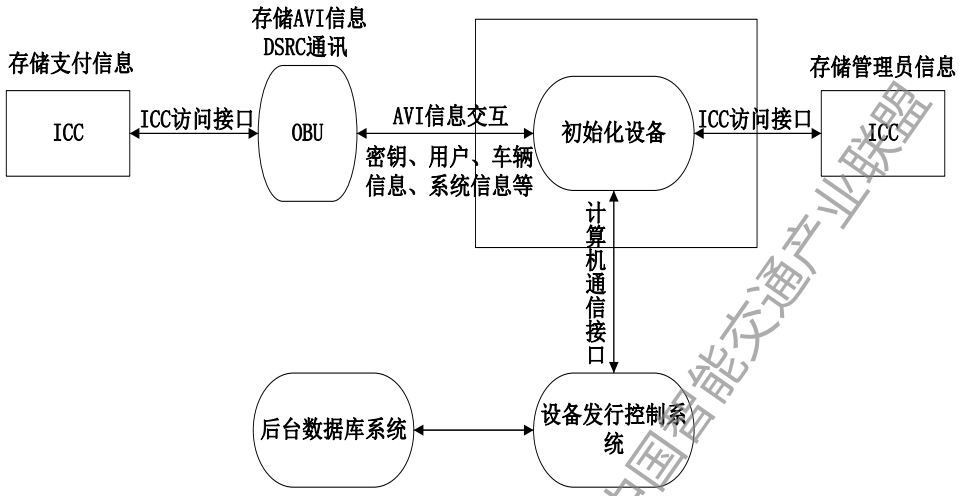
MLFF：多车道自由流（Multi Lane Free Flow）

EAT：电子年票（Electronic Annual Ticket）

# 4 基本要求和组成

## 4.1 ETC 发行系统构成

ETC 发行系统由前端系统和后台数据库系统组成，前端系统包括设备发行控制系统、初始化设备、OBU 以及 ICC。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 发行系统构成

## 4.2　设备分类

初始化设备按应用场合和应用方式的不同,可分为台式初始化设备、手持式初始化设备和其它初始化设备。

### 4.2.1　台式初始化设备

台式初始化设备是指与发行控制系统有线连接，且 DSRC 通讯距离较短的发行设备。

### 4.2.2　手持式初始化设备

手持式初始化设备指与发行控制系统无线连接，且 DSRC 通讯距离较远的发行设备。

### 4.2.3　其他初始化设备

其他初始化设备指除台式初始化设备和手持式初始化设备外的初始化设备,本部分暂不做定义。

## 4.3　工作模式

初始化设备具有脱机和联机两种工作模式：

a) 采用联机工作模式时，由发行控制系统控制发行流程，此时初始化设备作为透明通道，转发发行控制系统与 OBU 之间的数据通信，数据传入、流程控制等工作均由发行控制系统完成；

b) 采用脱机工作模式时，由初始化设备控制发行流程，数据传入、流程控制等工作均由初始化设备完成；

台式初始化设备只具有联机工作模式；手持式初始化设备具有脱机和联机两种工作模式。

## 4.4 发行模式

根据营业网点和工作模式的不同，OBU 发行模式可分为三种：

a) 可信联机模式: 在可信发行网点，初始化设备采用联机工作模式完成所有的 OBU 发行操作；
b) 可信脱机模式: 在可信发行网点，手持式初始化设备采用脱机工作模式完成 OBU 激活、检测工作；
c) 不可信联机模式：在不可信发行网点，手持式初始化设备采用联机工作模式完成所有的 OBU 发行操作。

## 4.5 设备功能

### 4.5.1 IC 卡读写

#### 4.5.1.1 接触式读写

具备接触式卡片读写功能，PSAM 卡座数量应不少于 2 个，并符合 ISO-7816 协议，PBOC 规范。

#### 4.5.1.2 非接触式读写

具备非接触式卡读写功能,符合 ISO14443 协议。

### 4.5.2 信息提示功能

具备指示灯、蜂鸣器提示功能，提示设备工作状态、运行状态。

### 4.5.3 摄像功能

适用于手持式初始化设备，200 万像素及以上摄像头；具有夜间拍照功能；

### 4.5.4 定位功能

适用于手持式初始化设备，具备定位功能，定位精度为 500m 之内，应至少支持 GPS、北斗和移动基站之一。

### 4.5.5 显示功能

适用于手持式初始化设备，具备显示功能，3.5 寸及以上彩色显示，分辨率至少 640×480。显示屏幕具有防水功能。

### 4.5.6 触摸功能

适用于手持式初始化设备，具有湿手触摸功能。

### 4.5.7 亮度调节

适用于手持式初始化设备，有亮度调节和记忆功能。

### 4.5.8 人机交互

适用于手持式初始化设备，具有触摸屏输入功能及键盘快捷键功能。

#### 4.5.9 时钟功能

适用于手持式初始化设备，具备时间手动设置以及联网自动校准功能,且更换电池或者电池无电时，时钟不会失效重置。

#### 4.5.10 语音功能

适用于手持式初始化设备，具有单声道语音提示信息播放功能。

#### 4.5.11 电源管理

适用于手持式初始化设备，有电量检测功能，提供电量指示以及低电报警功能。

#### 4.5.12 存储功能

适用于手持式初始化设备，具有图片、操作日志的存储功能。

#### 4.5.13 3G 功能

适用于手持式初始化设备，具有 3G 连接、断开、上网功能。

#### 4.5.14 Wifi 功能

适用于手持式初始化设备，具有 Wifi 连接、断开、上网功能。

### 4.6 性能要求

#### 4.6.1 总体要求

初始化设备应符合 GB/T 20851.1-2007、GB/T 20851.2-2007、GB/T 20851.3-2007、GB/T20851.4-2007 系列标准规定的 A 类上下行链路（ASK 调制方式，FM0 编码）各项要求。

#### 4.6.2 电池续航能力

适用于手持式初始化设备：

- 待机时间≥ 120 小时，工作时间≥ 8 小时；
- 电池充满电后：
  - 持续与 300 个以上电子标签激活、检测；
  - 联机工作模式下，连续与 100 个以上电子标签激活、检测；
- 电池使用寿命≥ 2 年；

#### 4.6.3 启动时间

适用于手持式初始化设备，冷启动≤30s，热启动≤1s。

#### 4.6.4 通讯区域

适用于手持式初始化设备，工作距离为 0.8-3 米；保证功率设置为最大时，距离目标标签 3 米范围内，手持机正对目标标签，与目标标签水平距离 2 米以外的标签不会被操作到，避免对非操作方向上的 OBU 进行误操作。

#### 4.6.5 可靠性

平均无故障时间≥ 50 000h

### 4.7 供电

#### 4.7.1 台式初始化设备

USB 接口，5V/1A DC。

#### 4.7.2 手持式初始化设备

采用电池供电。充电接口电气规格统一为 5V/3A，电池容量≥2000mAh。电池独立充电时，从电池无电到充满时间 ≤ 4 小时。

### 4.8 OBU 信号强度检测

适用于手持式初始化设备，具有 OBU 信号强度检测功能，确定 OBU 场强的 RSSI 值，确定玻璃衰减。

## 5 技术要求

### 5.1 物理层

初始化设备的物理层参数应符合 GB/T 20851.1-2007 中的 A 类各项要求外，还应符合以下技术要求。

表 1 手持式初始化设备下行链路技术要求

| 序号 | 参数 | 技术要求 |
|---|---|---|
| 1 | e.i.r.p | ≤20dBm |
| | | ≥10dBm |
| 2 | OBU场强检测精度 | ±3db |

表 2 台式初始化设备下行链路技术要求

| 序号 | 参数 | 技术要求 |
|---|---|---|
| 1 | e.i.r.p | ≤10dBm |
| | | ≥0dBm |

### 5.2 数据链路层

符合 RSU 技术要求。

## 6 台式初始化设备

### 6.1 台式初始化设备的接口

台式初始化设备的接口如图所示。

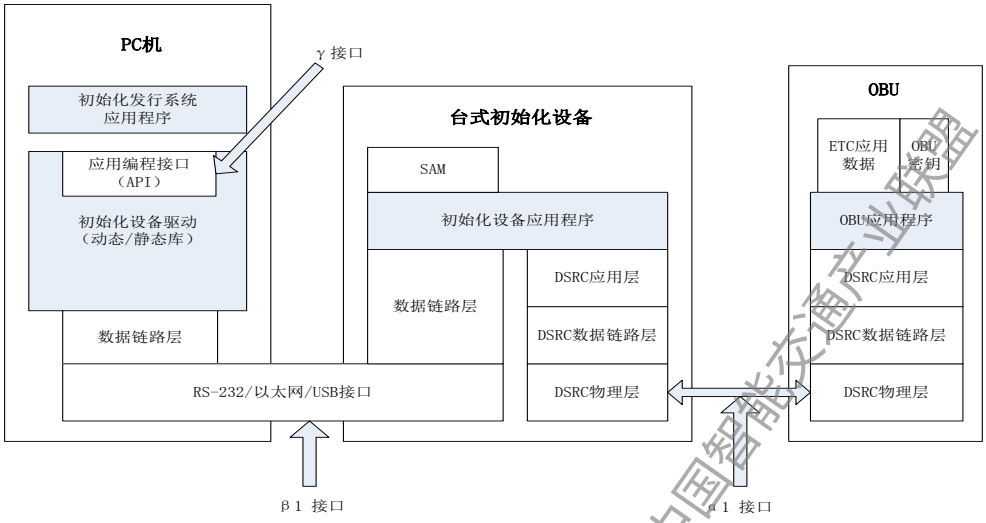



图 2　台式初始化设备的接口

其中：

- α1 接口：OBU 与台式初始化设备之间的 DSRC 接口；
- β1 接口：台式初始化设备与发行控制系统之间的接口；
- γ 接口：台式初始化设备驱动程序的应用编程接口。

## 6.2　初始化发行操作的类别

### 6.2.1 OBU 初始化

用 ETC 运营商密钥替换 OBU 供货时预置的传输密钥，本阶段需要替换的密钥如表 所示。

表 3　OBU 初始化阶段需要替换的密钥

| 密钥 | 说明 |
|---|---|
| 根目录 | |
| sysMasterKey | 系统主控密钥 |
| sysMaintainKey | 系统维护密钥 |
| 高速公路ETC应用目录——DF01 | |
| etcMasterKey | 高速公路ETC应用主控密钥 |
| etcMaintainKey | 高速公路ETC应用维护密钥 |
| etcAccessKey | 高速公路ETC应用认证密钥 |
| etcEncryptKey | 高速公路ETC应用加密密钥 |
| 多车道自由流(MLFF)ETC应用目录——DF28 | |
| mlffMasterKey | MLFF应用主控密钥 |
| mlffMaintainKey | MLFF应用维护密钥 |
| mlffAccessKey | MLFF应用访问密钥 |
| mlffAuthenticateKey | MLFF应用鉴别密钥 |
| mlffEncryptKey | MLFF应用加密密钥 |
| mlffmTACtKey | MLFF应用TAC密钥 |

### 6.2.2 OBU 个人化

更新“系统信息文件”、“高速公路 ETC 应用车辆信息文件”和“多车道自由流 ETC 应用车辆信息文件”。

### 6.2.3 OBU 激活

重置系统信息文件中的“拆卸状态”以及延长 OBU“有效期”。

### 6.2.4 系统信息读取

读取 OBU 中的系统信息。

### 6.2.5 车辆信息读取

读取 OBU 中的车辆信息。

### 6.2.6 汽车电子标识信息设置

更新 OBU 中 AEI 应用目录下驾驶证信息、行驶证信息和车牌信息。

### 6.2.7 汽车电子标识信息读取

读取 OBU 中 AEI 应用目录下驾驶证信息、行驶证信息和车牌信息。

### 6.2.8 电子年票信息设置

更新 OBU 中 EAT 应用目录下年票信息。

### 6.2.9 电子年票信息读取

读取 OBU 中 EAT 应用目录下年票信息。

## 6.3 α1 接口规范

### 6.3.1 初始化发行操作的 DSRC 交易流程

本部分规定了 OBU 初始化发行操作模式下，OBU 与初始化设备间 DSRC 数据帧流程。

为减少 OBU 与初始化设备之间的 DSRC 交互次数，确保初始化发行的互操作性和可靠性，OBU 与初始化设备均应按照下面的定义执行 TransferChannel 中的多个 APDU 拼接。

#### 6.3.1.1 OBU 初始化交易流程

描述了初始化设备在进行 OBU 初始化操作时的交易流程，见图 3 主要流程如下：

a) 初始化设备与 OBU 之间通过 BST/VST 完成初始化，且 VST 中带有系统文件信息、ESAM 随机数、ESAM 复位信息；

b) 初始化设备通过TransferChannel服务更新OBU中ESAM根目录下的“系统主控密钥”，并向ESAM取4字节的随机数；

c) 初始化设备通过TransferChannel服务更新OBU中ESAM根目录下的“系统维护密钥”；

d) 初始化设备通过TransferChannel服务选择OBU中ESAM的高速公路ETC应用目录(DF01)，并向ESAM取4字节的随机数；

e) 初始化设备通过TransferChannel服务更新OBU中高速公路ETC应用目录（DF01）下的“应用主控密钥”，并向ESAM取4字节的随机数；

f) 初始化设备通过TransferChannel服务更新OBU中高速公路ETC应用目录（DF01）下的“应用维护密钥”，并向ESAM取4字节的随机数；

g) 初始化设备通过TransferChannel服务更新OBU中高速公路ETC应用目录（DF01）下的“应用认证密钥”，并向ESAM取4字节的随机数；

h) 初始化设备通过TransferChannel服务更新OBU中高速公路ETC应用目录（DF01）下的“应用加密密钥”；

i) 初始化设备通过TransferChannel服务选择OBU中ESAM的多车道自由流ETC应用目录(DF28)，并向ESAM取4字节的随机数；

j) 初始化设备通过TransferChannel服务更新OBU中多车道自由流ETC应用目录(DF28)下的“应用主控密钥”，并向ESAM取4字节的随机数；

k) 初始化设备通过TransferChannel服务更新OBU中多车道自由流ETC应用目录(DF28)下的“应用维护密钥”，并向ESAM取4字节的随机数；

l) 初始化设备通过TransferChannel服务更新OBU中多车道自由流ETC应用目录(DF28)下的“应用访问密钥”，并向ESAM取4字节的随机数；

m) 初始化设备通过TransferChannel服务更新OBU中多车道自由流ETC应用目录(DF28)下的“应用鉴别密钥”；

n) 初始化设备通过TransferChannel服务更新OBU中多车道自由流ETC应用目录(DF28)下的“应用加密密钥”；

o) 初始化设备通过SetMMI服务进行OBU人机指示；

p) 初始化设备通过EVENT-RAEIORT服务释放OBU链路。

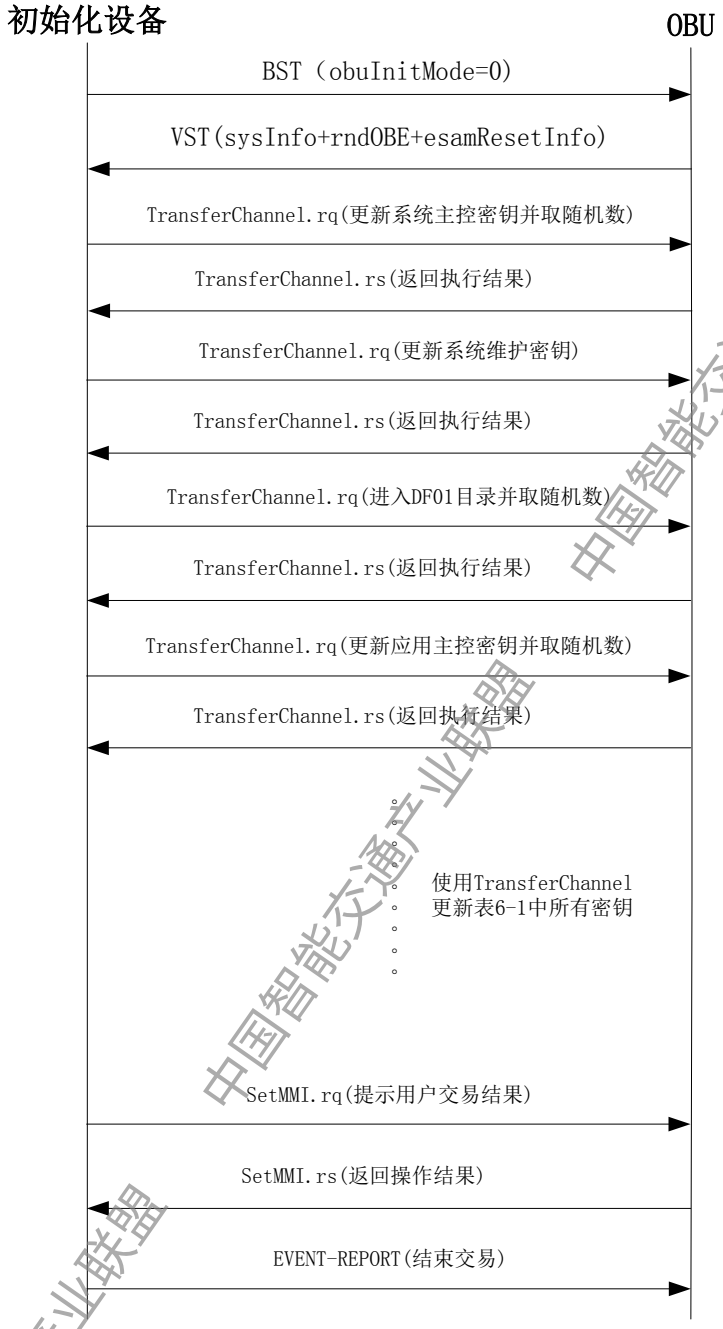



图 3　OBU 初始化交易流程

6.3.1.2 OBU 个人化

描述了初始化设备在进行 OBU 个人化操作时的交易流程，见图 4。 主要流程如下：

a) 初始化设备与 OBU 之间通过 BST/VST 完成初始化，且 VST 中带有系统文件信息、ESAM 随机数、ESAM 复位信息；

b) 初始化设备通过 TransferChannel 服务更新 OBU 中系统信息文件中的“合同签署日期”、“合同过期日期”以及“拆卸状态”三项数据；

c) 初始化设备通过 TransferChannel 服务选择 OBU 中 ESAM 的高速公路 ETC 应用目录

(DF01)，并向 ESAM 取 4 字节的随机数；

d) 初始化设备通过 TransferChannel 服务更新 OBU 中 DF01 目录下高速公路 ETC 应用车辆信息文件中的除保留字段外的所有数据项；

e) 初始化设备通过 TransferChannel 服务选择 OBU 中 ESAM 的根目录；

f) 初始化设备通过 TransferChannel 服务选择 OBU 中 ESAM 的多车道自由流 ETC 应用目录(DF28)，并向 ESAM 取 4 字节的随机数；

g) 初始化设备通过 TransferChannel 服务更新 OBU 中 DF28 目录下多车道自由流 ETC 应用车辆信息文件中的除保留字段外的所有数据项；

h) 初始化设备通过 SetMMI 服务进行 OBU 人机指示；

i) 初始化设备通过 EVENT-RAEIORT 服务释放 OBU 链路。

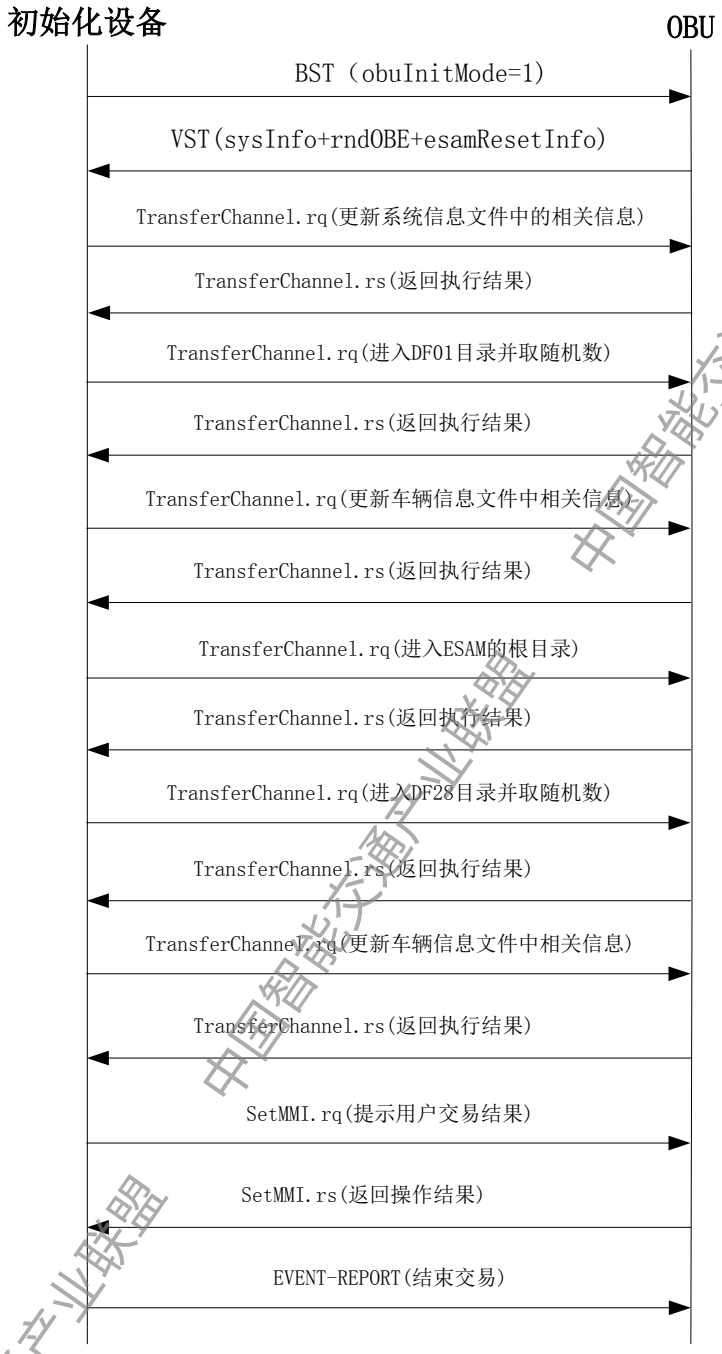



图 4　OBU 个人化交易流程

6.3.1.3 OBU 激活

描述了初始化设备在进行 OBU 激活操作时的交易流程，见图。主要流程如下：

a) 初始化设备与 OBU 之间通过 BST/VST 完成初始化，且 VST 中带有系统文件信息、ESAM 随机数、ESAM 复位信息；

b) 初始化设备通过 TransferChannel 服务更新 OBU 中系统信息文件中的“拆卸状态”和“有效期”数据；

c) 初始化设备通过 SetMMI 服务进行 OBU 人机指示；

d) 初始化设备通过 EVENT-RAEIORT 服务释放 OBU 链路。

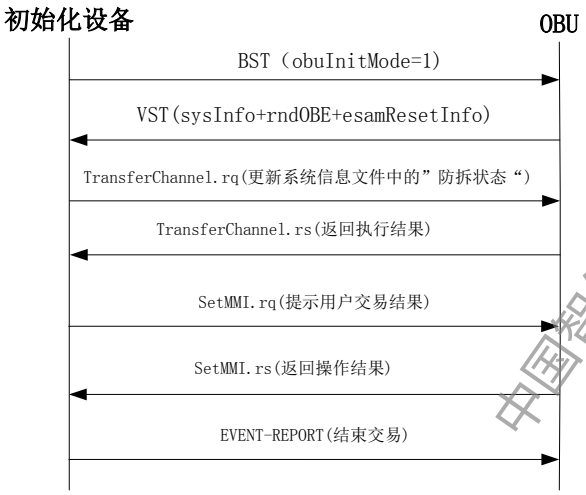



图 5　OBU 激活交易流程

### 6.3.1.4 系统信息读取

描述了初始化设备在进行系统信息读取操作时的交易流程，见图。主要流程如下：

a) 初始化设备与 OBU 之间通过 BST/VST 完成初始化；

b) 初始化设备通过 TransferChannel 服务读取 OBU 中 ESAM 根目录下系统信息文件中的前 7 项数据；

c) 初始化设备通过 SetMMI 服务进行 OBU 人机指示；

d) 初始化设备通过 EVENT-RAEIORT 服务释放 OBU 链路。

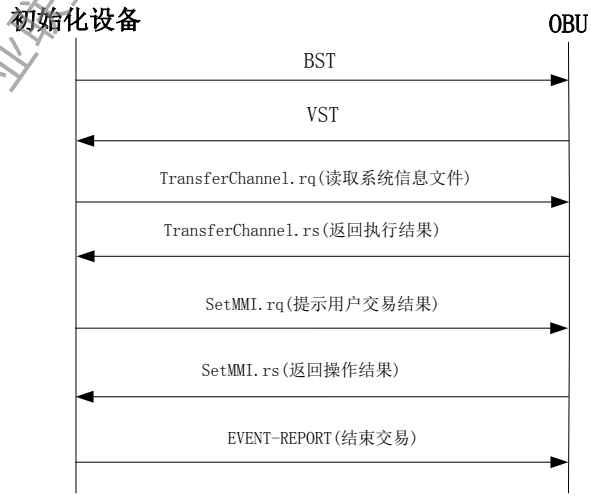



图 6　系统信息读取交易流程

#### 6.3.1.5 车辆信息读取

描述了初始化设备在进行车辆信息读取操作时的交易流程，见图。主要流程如下：

a) 初始化设备与 OBU 之间通过 BST/VST 完成初始化；

b) 初始化设备通过 GetSecure 服务读取 OBU 车辆信息文件(DID=1, FID=1)；

c) 初始化设备通过 SetMMI 服务进行 OBU 人机指示；

d) 初始化设备通过 EVENT-RAEIORT 服务释放 OBU 链路。

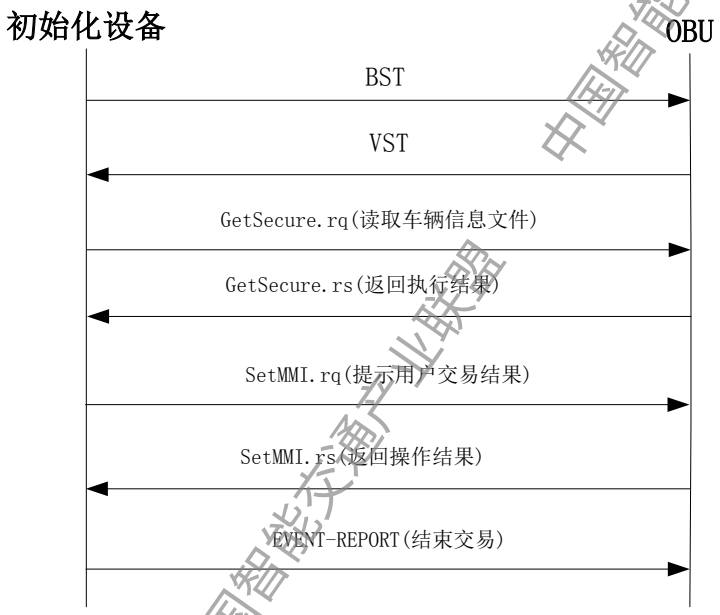



图 7　车辆信息读取交易流程

#### 6.3.1.6 汽车电子标识信息设置

描述了初始化设备在进行汽车电子标识信息设置操作时的交易流程，见图。主要流程如下：

a) 初始化设备与 OBU 之间通过 BST/VST 完成初始化，且 VST 中带有系统文件信息、ESAM 随机数；

b) 初始化设备通过 TransferChannel 服务选择 OBU 中双界面 CPU 卡 AEI 应用的目录（DF01），并向 ESAM 取 4 字节的随机数；

c) 初始化设备通过 TransferChannel 服务更新 OBU 中双界面 CPU 卡 DF01 目录下 AEI 应用驾驶证信息文件中的除保留字段外的所有数据项；

d) 初始化设备通过 TransferChannel 服务选择 OBU 中 ESAM 的 AEI 应用的目录(DF01)，并向 ESAM 取 4 字节的随机数；

e) 初始化设备通过 TransferChannel 服务更新 OBU 中 DF01 目录下 AEI 应用行驶证信息文件中的除保留字段外的所有数据项，并向 ESAM 取 4 字节的随机数；

f) 初始化设备通过 TransferChannel 服务更新 OBU 中 DF01 目录下 AEI 应用车牌信息文

件中的除保留字段外的所有数据项；

g) 初始化设备通过 SetMMI 服务进行 OBU 人机指示；

h) 初始化设备通过 EVENT-RAEIORT 服务释放 OBU 链路。

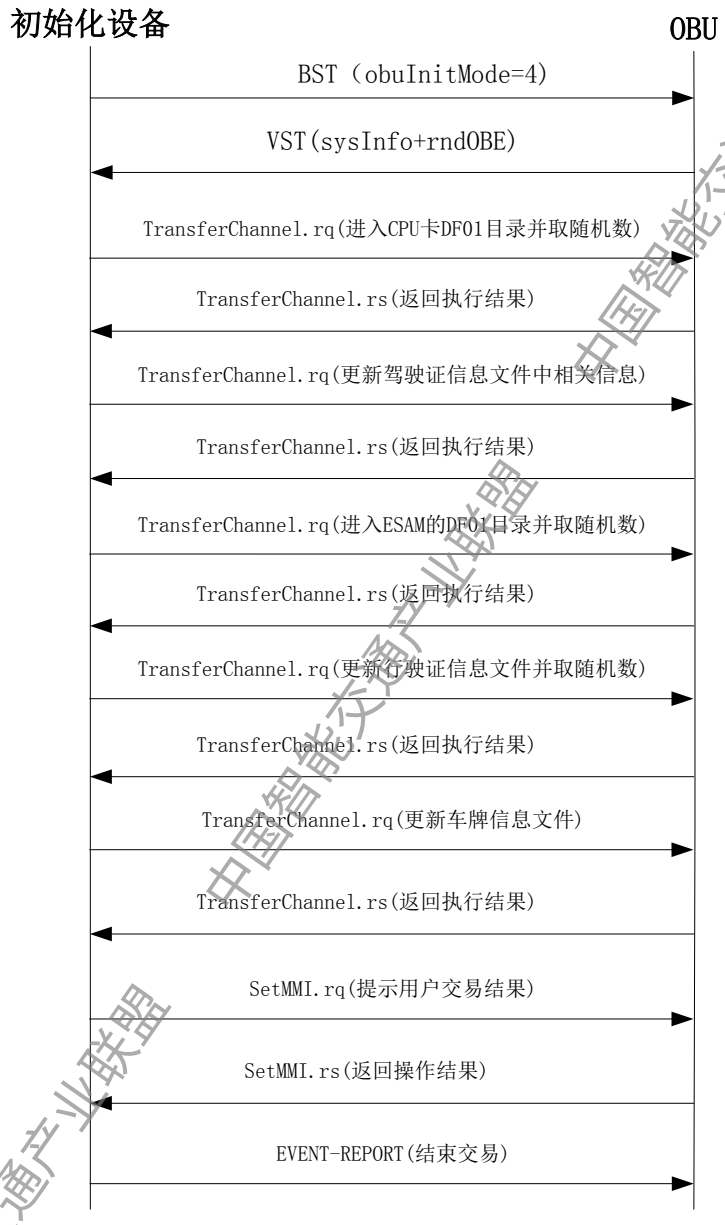



图 8　汽车电子标识信息设置交易流程

### 6.3.1.7 汽车电子标识信息读取

描述了初始化设备在进行汽车电子标识信息读取操作时的交易流程，见图。主要流程如下：

a) 初始化设备与 OBU 之间通过 BST/VST 完成初始化；

b) 初始化设备通过 GetSecure 服务读取 OBU 中的行驶证信息文件；

c) 初始化设备通过 GetSecure 服务读取 OBU 中的车牌信息文件；

d) 初始化设备通过 TransferChannel 服务选择 OBU 中双界面 CPU 卡 AEI 应用的目录（DF01）

e) 初始化设备通过 TransferChannel 服务读取 OBU 中双界面 CPU 卡 DF01 目录下 AEI 应用驾驶证信息文件；

f) 初始化设备通过 SetMMI 服务进行 OBU 人机指示；

g) 初始化设备通过 EVENT-RAEIORT 服务释放 OBU 链路。

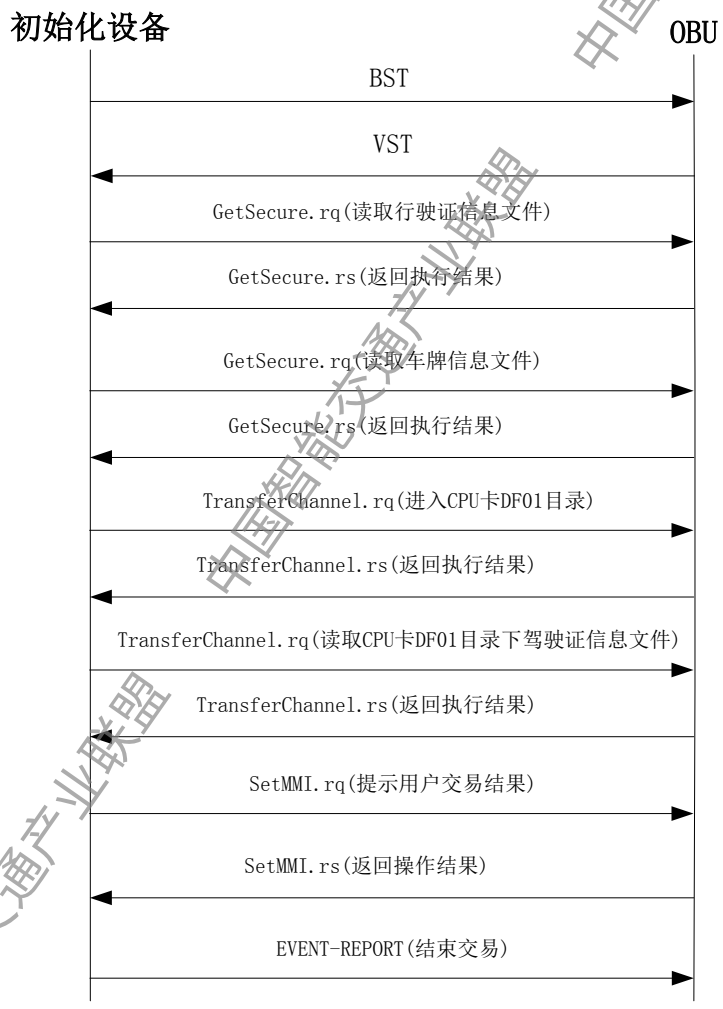



**图 9　汽车电子标识信息读取交易流程**

6.3.1.8 电子年票信息设置

描述了初始化设备在进行电子年票信息设置操作时的交易流程，见图。主要流程如下：

a) 初始化设备与 OBU 之间通过 BST/VST 完成初始化，且 VST 中带有系统文件信息、

ESAM 随机数；

b) 初始化设备通过 TransferChannel 服务选择 OBU 中 ESAM 的 AEI 应用的目录（DF01），并向 ESAM 取 4 字节的随机数；

c) 初始化设备通过 TransferChannel 服务更新 OBU 中 DF01 目录下 AEI 应用年票信息文件中的除保留字段外的所有数据项；

d) 初始化设备通过 SetMMI 服务进行 OBU 人机指示；

e) 初始化设备通过 EVENT-RAEIORT 服务释放 OBU 链路。

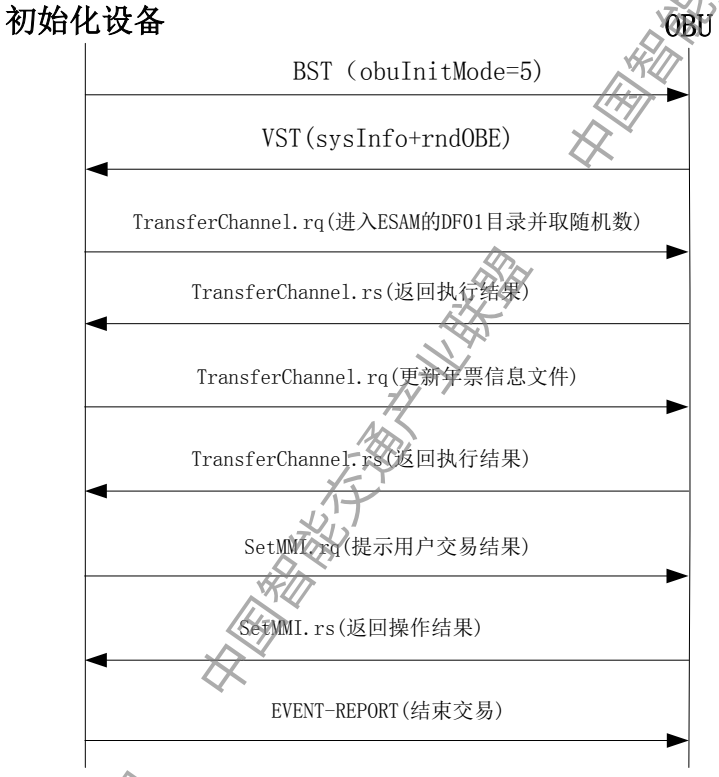



**图 10　电子年票信息设置交易流程**

6.3.1.9　电子年票信息读取

描述了初始化设备在进行电子年票信息读取操作时的交易流程，见图。主要流程如下：

a) 初始化设备与 OBU 之间通过 BST/VST 完成初始化；

b) 初始化设备通过 GetSecure 服务读取 OBU 中的年票信息文件；

c) 初始化设备通过 SetMMI 服务进行 OBU 人机指示；

d) 初始化设备通过 EVENT-RAEIORT 服务释放 OBU 链路。

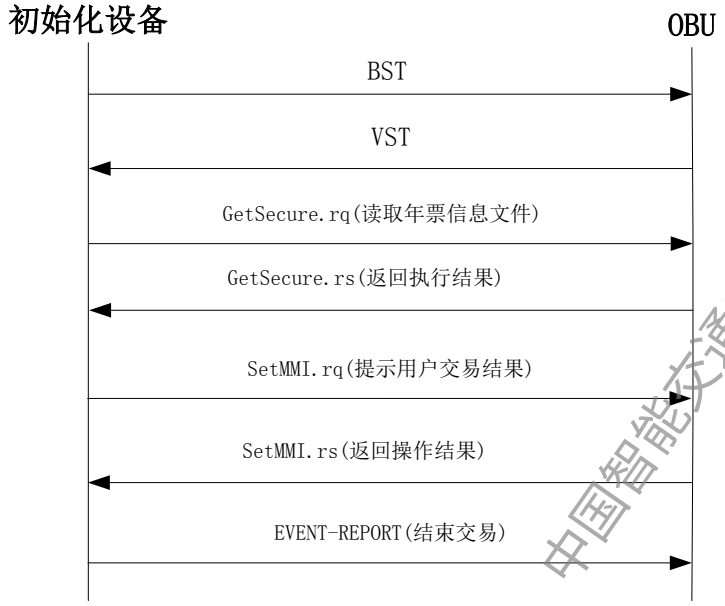



图 11　电子年票信息读取交易流程

## 6.4　β1 接口规范

### 6.4.1 物理接口形式

台式初始化设备与发行控制系统之间的通信接口至少支持下列几种方式之一：

- 标准串行接口

采用 RS-232、RS-485 等，要求通讯波特率至少达到 115200。

- 以太网接口

采用 100M 及以上以太网(RJ45 接口)，及 TCP/IP 协议进行连接。在 TCP/IP 方式下不限制台式初始化设备作为客户端或服务器端。

- USB 接口

兼容 USB1.1 及 USB2.0

### 6.4.2 通用数据帧格式

6.4.2.1　数据帧的结构

在各种接口应用模式及物理接口形式下，台式初始化设备和发行控制系统间通讯的数据帧格式均应满足如图所示。

| STX | RSCTL | DATA | BCC | ETX |
|---|---|---|---|---|

图 12　数据帧格式

数据帧中各数据域的说明如

表所示：

表 4　数据帧中各数据域的说明

| 字段 | 描述 |
|---|---|
| STX | 帧开始标志，2字节，取值为FFFFH |
| RSCTL | 数据帧序列号，1个字节<br>初始化设备发送的数据帧序列号为X8H，其中X为0，1，2，3，4，5，6，7，9<br>发行控制系统发送的数据帧序列号为8XH，其中X为0，1，2，3，4，5，6，7，9<br>帧序列号每次加1，用于标识每一次的通信 |
| DATA | 发送的数据 |
| BCC | 异或校验值，从RSCTL到DATA所有字节的异或值，1字节 |
| ETX | 帧结束标志，取值为FFH，1字节 |

#### 6.4.2.2 特殊字节转义处理

数据帧开始标志和帧结束标志为 FFH，其他字段不能出现 FFH，如果数据确实为 FFH，需对其进行转义处理。

发送数据时，如果在其他字段中出现 FFH 字节时，将 FFH 分解为 FEH 和 01H 这两个字节来发送；如果在其他字段中出现 FEH 字节时，需将 FEH 分解为 FEH 和 00H 这两个字节来发送。

接受数据时，如果出现“FE 01”这样连续两个字节时将之合为一个字节 FFH；如果出现“FE 00”这样连续两个字节时将之合为一个字节 FEH。

#### 6.4.2.3 通讯方式说明

初始化设备与发行控制系统之间是一种应答式的通讯方式:发行控制系统发送信息帧给初始化设备，初始化设备必须应答指令给发行控制系统，否则发行控制系统将反复发送直到初始化设备应答为止。

### 6.4.3 面向应用的集成指令数据接口帧格式定义

本部分以集成指令数据接口方式定义了面向应用的发行控制系统与初始化设备之间交互的原始应用数据帧的格式。

#### 6.4.3.1 数据帧列表

表 5　数据帧列表

| 指令名称 | 指令代码 | 功能说明 | 发送方 | 接收方 |
|---|---|---|---|---|
| 设备初始化指令 | C0H | 对初始化设备关键参数进行初始化设置 | 发行控制系统 | 初始化设备 |
| 设备状态信息帧 | B0H | 初始化设备的设备状态信息，含 PSAM 卡号 | 初始化设备 | 发行控制系统 |
| 开始交易指令 | C1H | 以初始设定的周期发送 BST，启动单个 OBU | 发行控制系统 | 初始化设备 |
| VST 响应信息帧 | B1H | 返回 OBU 的 VST 信息 | 初始化设备 | 发行控制系统 |
| 密钥替换指令 | C2H | 执行 OBU 初始化，完成密钥替换操作 | 发行控制系统 | 初始化设备 |
| 文件更新指令 | C3H | 执行 OBU 个人化，完成指定的文件信息更新 | 发行控制系统 | 初始化设备 |
| 更新命令执行响应 | B2H | 返回密钥替换及文件更新指令的执行结果 | 初始化设备 | 发行控制系统 |
| 文件读取指令 | C4H | 根据指定的参数信息读取相应的文件内容 | 发行控制系统 | 初始化设备 |
| OBU 文件信息帧 | B3H | 返回文件读取操作的执行结果及指定的文 | 初始化设备 | 发行控制系统 |
| 结束交易指令 | C5H | OBU 初始化完毕，进行用户提示，释放 OBU | 发行控制系统 | 初始化设备 |
| 交易结束响应帧 | B4H | 返回交易结束指令的执行结果 | 初始化设备 | 发行控制系统 |
| MAC 计算指令 | C6H | 计算初始化发行操作的 MAC 码 | 发行控制系统 | 初始化设备 |
| MAC 数据帧 | B5H | 返回 MAC 计算指令执行结果及 MAC 码 | 初始化设备 | 发行控制系统 |

### 6.4.3.2 设备初始化指令

表 6　设备初始化指令帧格式

| 位置 | 字节数 | 数据元 | 数据内容 |
|---|---|---|---|
| 0 | 1 | RSCTL | 数据帧序列号 |
| 1 | 1 | CMDType | 指令代码，此处取值为C0H，H代表十六进制 |
| 2 | 4 | UnixTime | UNIX时间 |
| 6 | 1 | BSTInterval | BST间隔时间（单位：毫秒，推荐取值为0x20） |
| 7 | 1 | TxPower | 功率级数 |
| 8 | 1 | PHYChannelID | 信道号 |
| 9 | 5 | Reserved | 保留字节，填充“00” |
| 14 | 1 | BCC | 异或校验值 |
| | | | |
| 帧信息描述 | | C0指令帧为初始化指令，对初始化设备进行工作参数设定；<br>初始化设备收到初始化指令后需应答B0帧信息给发行控制系统； | |

### 6.4.3.3 开始交易指令

表 7　开始交易指令帧格式

| 位置 | 字节数 | 数据元 | 数据内容 |
|---|---|---|---|
| 0 | 1 | RSCTL | 数据帧序列号 |
| 1 | 1 | CMDType | 指令代码，此处取值为C1H，H代表十六进制 |
| 2 | 1 | ObuInitMode | 指示OBU初始化发行操作的模式，其取值参见附录A.1 obuInitMode的编码 |
| 3 | 5 | Reserved | 保留字节，填充“00” |
| 8 | 1 | BCC | 异或校验值 |
| | | | |
| 帧信息描述 | C1指令帧为单个OBU初始化发行操作开始指令。收到此指令后，初始化设备应周期性发送BST轮询待初始化的OBU。BST中应指示命令帧中指定的OBU初始化发行操作的模式如在B1响应信息帧中未能包含有效的VST信息，则发行控制系统认为本次初始化交易失败 | | |

### 6.4.3.4 密钥替换指令

表 8　密钥替换指令帧格式

| 位置 | 字节数 | 数据元 | 数据内容 |
|---|---|---|---|
| 0 | 1 | RSCTL | 数据帧序列号 |
| 1 | 1 | CMDType | 指令代码，此处取值为C2H，H代表十六进制 |
| 2 | 1 | KCType | 指示密钥母卡类型 |
| 3 | 1 | TCType | 0-无传输卡保护；1-有传输卡保护；其他-保留 |
| 4 | 5 | Reserved | 保留字节，填充“00” |
| 9 | 1 | BCC | 异或校验值 |
| | | | |
| 帧信息描述 | C2指令帧指示初始化设备执行密钥替换操作，对初始化设备内置的密钥母卡及传输卡的操作指令类型由命令帧中的相关参数确定。 | | |

### 6.4.3.5 文件更新指令

表 9　文件更新指令帧格式

| 位置 | 字节数 | 数据元 | 数据内容 |
|---|---|---|---|
| 0 | 1 | RSCTL | 数据帧序列号 |
| 1 | 1 | CMDType | 指令代码，此处取值为C3H，H代表十六进制 |
| 2 | 1 | NumOfFiles | 需要更新的文件数量 |
| 3 | 1 | DIDnFID | 指示需要更新的文件的目录号和文件号 |
| 4 | 1 | Offset | 文件地址偏移量（需要写入数据的起始地址） |
| 5 | 1 | Length | 需要写入的数据长度 |
| 6 | N1 | FileContent | 需要写入的数据内容 |
| 6+N1 | 1 | DIDnFID | 指示需要更新的文件的目录号和文件号 |
| 7+N1 | 1 | Offset | 文件地址偏移量（需要写入数据的起始地址） |

表 9 文件更新指令帧格式（续）

| 位置 | 字节数 | 数据元 | 数据内容 |
|---|---|---|---|
| 8+N1 | 1 | Length | 需要写入的数据长度 |
| 9+N1 | N2 | FileContent | 需要写入的数据内容 |
| 9+N1+N2 | … | | |
| | 1 | BCC | 异或校验值 |
| | | | |
| 帧信息描述 | C3指令帧用于指示初始化设备更新指定目录下指定文件的指定信息<br>DIDnFID可用XYH表示，H代表十六进制。X表示目录号，Y表示文件号 | | |

### 6.4.3.6 文件读取指令

表 10　文件读取指令帧格式

| 位置 | 字节数 | 数据元 | 数据内容 |
|---|---|---|---|
| 0 | 1 | RSCTL | 数据帧序列号 |
| 1 | 1 | CMDType | 指令代码，此处取值为C4H，H代表十六进制 |
| 2 | 1 | NumOfFiles | 需要读取的文件数量 |
| 3 | 1 | DIDnFID | 指示需要读取的文件的目录号和文件号 |
| 4 | 1 | Offset | 文件地址偏移量（需要读取数据的起始地址） |
| 5 | 1 | Length | 需要读取的数据长度 |
| 6 | | DIDnFID | 需要读取的文件数量 |
| 7 | | Offset | 指示需要读取的文件的目录号和文件号 |
| 8 | | Length | 文件地址偏移量（需要读取数据的起始地址） |
| | … | | |
| | 1 | BCC | 异或校验值 |
| | | | |
| 帧信息描述 | C4指令帧用于指示初始化设备读取指定目录下指定文件的指定信息<br>DIDnFID可用XYH表示，H代表十六进制。X表示目录号，Y表示文件号 | | |

### 6.4.3.7 结束交易指令

表 11　结束交易指令帧格式

| 位置 | 字节数 | 数据元 | 数据内容 |
|---|---|---|---|
| 0 | 1 | RSCTL | 数据帧序列号 |
| 1 | 1 | CMDType | 指令代码，此处取值为C0H，H代表十六进制 |
| 2 | 1 | SetMMIMode | 执行OBU的用户提示方式，参照GB/T20851.4-2007进行编码 |
| 3 | 5 | Reserved | 保留字节，填充“00” |
| 8 | 1 | BCC | 异或校验值 |
| | | | |
| 帧信息描述 | C5指令帧用于结束当前的OBU初始化操作。收到此指令后，初始化设备应根据此前OBU初始化指令的执行结果，用SetMMI命令进行OBU人机界面提示，然后利用EVENT-RAEIORT释放与OBU之间的链接 | | |

### 6.4.3.8 MAC 计算指令

表 12　MAC 计算指令帧格式

| 位置 | 字节数 | 数据元 | 数据内容 |
|---|---|---|---|
| 0 | 1 | RSCTL | 数据帧序列号 |
| 1 | 1 | CMDType | 指令代码，此处取值为C0H，H代表十六进制 |
| 2 | 1 | Length | 用于MAC计算的数据长度 |
| 3 | N | Content | 用于MAC计算的数据内容 |
| 3+N | 1 | BCC | 异或校验值 |
| | | | |
| 帧信息描述 | | C6指令帧指示初始化设备使用内置的PSAM中指定的密钥对输入的发行信息计算MAC，并输出。此MAC将用于后台系统验证数据库中发行信息的正确性 | |

### 6.4.3.9 设备状态信息帧

表 13　设备状态信息帧格式

| 位置 | 字节数 | 数据元 | 数据内容 |
|---|---|---|---|
| 0 | 1 | RSCTL | 数据帧序列号 |
| 1 | 1 | FrameType | 指令代码，此处取值为B0H，H代表十六进制 |
| 2 | 1 | RSUStatus | 初始化设备主状态，0x0表示正常，否则表示异常 |
| 3 | 2 | RSUManuID | 初始化设备厂商代码，16进制表示 |
| 5 | 2 | RSUID | 初始化设备编号，16进制表示 |
| 7 | 2 | RSUVersion | 初始化设备软件版本号，16进制表示 |
| 9 | 5 | Reserved | 保留字节，填充“00” |
| 14 | 1 | BCC | 异或校验值 |
| | | | |
| 帧信息描述 | | 初始化设备在上电后或收到初始化指令后发送该帧信息给发行控制系统 | |

### 6.4.3.10VST 响应信息帧

表 14　VST 响应信息帧格式

| 位置 | 字节数 | 数据元 | 数据内容 |
|---|---|---|---|
| 0 | 1 | RSCTL | 数据帧序列号 |
| 1 | 1 | FrameType | 指令代码，此处取值为B1H，H代表十六进制 |
| 2 | 1 | ErrorCode | 执行状态代码 |
| 3 | 8 | ContractProvider | 服务提供商名称 |
| 11 | 1 | ContractType | 协约类型 |
| 12 | 1 | ContractVersion | 合同版本 |
| 13 | 8 | ContractSerialNumber | 合同序列号 |
| 21 | 4 | ContractSignedDate | 合同签署日期 |
| 25 | 4 | ContractExpiredDate | 合同过期日期 |
| 29 | 5 | Reserved | 保留字节，填充“00” |
| 34 | 1 | BCC | 异或校验值 |
| | | | |
| 帧信息描述 | | B1帧为C1命令帧的应答信息帧，用于返回OBU的VST信息<br>初始化设备应当在指定的超时时间内B1帧对C1命令帧进行应答 | |

### 6.4.3.11 更新命令指令响应帧

表 15　更新命令指令响应帧格式

| 位置 | 字节数 | 数据元 | 数据内容 |
|---|---|---|---|
| 0 | 1 | RSCTL | 数据帧序列号 |
| 1 | 1 | FrameType | 指令代码，此处取值为B2H，H代表十六进制 |
| 2 | 4 | ErrorCode | 执行状态代码，0x00表示成功，其他表示失败 |
| 9 | 5 | Reserved | 保留字节，填充“00” |
| 14 | 1 | BCC | 异或校验值 |
| | | | |
| 帧信息描述 | B2帧作为对C2和C3两个更新操作命令帧的应答，用于返回密钥替换及文件信息更新操作的执行结果 | | |

### 6.4.3.12 OBU 文件信息帧

表 16　OBU 文件信息帧格式

| 位置 | 字节数 | 数据元 | 数据内容 |
|---|---|---|---|
| 0 | 1 | RSCTL | 数据帧序列号 |
| 1 | 1 | FrameType | 指令代码，此处取值为B3H，H代表十六进制 |
| 2 | 1 | ErrorCode | 执行状态代码，0x00表示成功，其他表示失败 |
| 3 | 1 | NumOfFiles | 返回的文件的数量 |
| 4 | 1 | Length | 返回的数据的长度 |
| 5 | N1 | FileContent | 返回的数据的内容 |
| 5+N1 | 1 | Length | 返回的数据的长度 |
| 6+N1 | N2 | FileContent | 返回的数据的内容 |
| 6+N1+N2 | ... | | |
| | 1 | BCC | 异或校验值 |
| | | | |
| 帧信息描述 | B3帧作为C4帧的响应信息帧，当一次返回多个文件信息时，B3帧应当严格按照C4帧中读取的文件顺序返回相应的信息 | | |

### 6.4.3.13 交易结束响应帧

表 17　交易结束响应帧格式

| 位置 | 字节数 | 数据元 | 数据内容 |
|---|---|---|---|
| 0 | 1 | RSCTL | 数据帧序列号 |
| 1 | 1 | FrameType | 指令代码，此处取值为B4H，H代表十六进制 |
| 2 | 1 | ErrorCode | 执行状态代码，0x00表示成功，其他表示失败 |
| 3 | 5 | Reserved | 保留字节，填充“00” |
| 8 | 1 | BCC | 异或校验值 |
| | | | |
| 帧信息描述 | B4帧作为对C5命令帧的应答，用于返回OBU人机界面提示指令的执行结果<br>考虑到C5命令执行的正确与否不影响OBU初始化操作结果，因此B4帧可不作为OBU初始化操作执行结果的判定依据 | | |

6.4.3.14 MAC 数据帧

表 18　MAC 数据帧格式

| 位置 | 字节数 | 数据元 | 数据内容 |
|---|---|---|---|
| 0 | 1 | RSCTL | 数据帧序列号 |
| 1 | 1 | FrameType | 指令代码，此处取值为B5H，H代表十六进制 |
| 2 | 4 | ErrorCode | 执行状态代码，0x00表示成功，其他表示失败 |
| 6 | 1 | Length | 指示MAC的长度，通常为0x04或0x08 |
| 7 | 1 | MAC | PSAM计算得到的MAC值 |
| 14 | 1 | BCC | 异或校验值 |
| | | | |
| 帧信息描述 | | B5帧作为C6帧的响应信息帧，用于返回PSAM计算得到的MAC值 | |

## 6.5　γ 接口规范

### 6.5.1 γ 接口概述

为了便于系统集成商进行应用的开发，ETC 设备厂商可对 β 1 接口进行封装，以动态/静态库的形式提供台式初始化设备的应用编程接口(API)，即 γ 接口。γ 接口应支持 Windows、Linux 等主流操作系统。

### 6.5.2 面向应用的集成指令应用编程接口定义

本部分集成指令数据接口的方式定义了面向应用的台式初始化设备的应用编程接口，并以C/C++语言函数的方式进行描述。

#### 6.5.2.1 发行设备初始化

- 接口函数原型

int OBUProg_DevInit_Socket(char * pcIPAddress, int iPortNum, int * piManufactureorID, char * pcDllVer, char * pcDevVer);

int OBUProg_DevInit_Comm(char * pcComm, char * pcProtocol, int * piManufactureorID, char * pcDllVer, char * pcDevVer);

- 函数功能

完成 OBU 发行设备的初始化，建立 Socket 链接 / 打开并设备串口等，返回厂商 ID、设备及动态链接库版本号等信息。

根据初始化设备与发行控制系统的接口不同，可选用上述不同的初始化函数。对于采用 TCP/IP 协议接口的设备，使用 int OBUProg_DevInit_Socket()函数；对于采用串口接口的设备，使用 int OBUProg_DevInit_Comm()函数。

- 返回值

0 －设备初始化成功；其他－设备初始化失败。

- 输入参数

int OBUProg_DevInit_Socket()

  - char * pcIPAddress: 指向初始化设备 IP 地址字符串的指针；
  - int iPortNum: 初始化设备 Socket 通信的端口号；

int OBUProg_DevInit_Comm()

  - char * pcComm: 指向初始化设备串口号字符串；
  - char * pcProtocol: 指向所采用的串口通信协议控制字字符串的指针，如“115200，N,8,1”；

- 输出参数

int * piManufactureorID: 指向初始化设备生产商 ID 号的指针
char * pcDllVer：指向当前动态库链接库版本号字串的指针
char * pcDevVer：指向当前设备版本号字符串的指针

#### 6.5.2.2 OBU 初始化

- 接口函数原型

int OBUProg_OBUInit();

- 函数功能

完成 OBU 的初始化，即 OBU 内系统主控密钥和 ETC 应用主控密钥的替换，以及其他各项密钥的装载。

- 返回值

0 －OBU 初始化成功；其他－OBU 初始化失败。

- 输入参数

无

- 输出参数

无

#### 6.5.2.3 写入系统信息文件

- 接口函数原型

int OBUProg_Write_SysInfo(SysInfoType struSystemInfo);

其中 SysInfoType 为自定义结构体类型，包含系统信息文件的各数据项。其 C 语言定义如下：

```
typedef struct {
    char contractProvider[8];
    char contractType;
    char contractVersion;
    char contractSerialNumber[8];
    char contractSignedDate[4];
    char contractExpiredDate[4];
    char Reserved[64];
}SysInfoType;
```

- 函数功能

OBU 初始化阶段，在 ETC 应用维护密钥的保护下写入 OBU 系统信息，即并写入系统信息文件中的相关信息。

- 返回值

0－信息写入成功；其他－信息写入失败。

- 输入参数

SysInfoType struSystemInfo：包含系统信息文件中各项数据内容的结构体。

- 输出参数

无

#### 6.5.2.4 读取系统信息文件

- 接口函数原型

int OBUProg_Read_SysInfo(SysInfoType * pstruSystemInfo);

- 函数功能

读取 OBU 系统信息文件中的相关内容。

- 返回值

0 －读取信息成功；其他－读取信息失败。

- 输入参数

无

- 输出参数

SysInfoType * pstruSystemInfo：指向包含系统信息文件中各项数据内容的结构体的指针。

#### 6.5.2.5 写入车辆信息文件

- 接口函数原型

高速公路 ETC 车辆信息写入：

int OBUProg_Write_ETCVehicleInfo(ETCVehicleInfoType * pstruETCVehicleInfoType);

其中 ETCVehicleInfoType 为自定义结构体类型，包含 ETC 车辆信息文件中的各数据项。其 C 语言定义如下：

```
typedef struct {
    char vehicleLicencAEIlateNumber[12];
    char vehicleLicencAEIlateColor[2];
    char vehicleClass;
    char vehicleUserType;
    vehicleDimensionsType vehicleDimensions;
    char vehicleWheels;
    char vehicleAxles;
    char vehicleWheelBases[2];
    char vehicleWeightLimits[3];
    char vehicleSpecificInformation[16];
    char vehicleEngineNumber[16];
    char vehicleReserved[10];
```

```
}ETCVehicleInfoType;
typedef struct {
    char vehicleLength[2];
    char vehicleWidth;
    char vehicleHeight;
}vehicleDimensionsType;
```

多车道自由流 ETC 车辆信息写入：

```
int OBUProg_Write_MLFF_ETCVehicleInfo(mETCVehicleInfoType *
pstrumETCVehicleInfoType);
```

其中 mETCVehicleInfoType 为自定义结构体类型，包含 ETC 车辆信息文件中的各数据项。其 C 语言定义如下：

```
 typedef struct {
    char vehicleLicencAEIlateNumber[12];
    char vehicleLicencAEIlateColor[2];
    char vehicleClass;
    char vehicleUserType;
}mETCVehicleInfoType;
```

- 函数功能

OBU 个人化阶段，在 ETC 应用维护密钥的保护下写入用户(车辆)信息，即 ETC 应用车辆信息文件。

- 返回值

0—信息写入成功；其他－信息写入失败。

- 输入参数

ETCVehicleInfoType * pstruETCVehicleInfoType：包含高速公路 ETC 车辆信息文件中各项数据内容的结构体。

mETCVehicleInfoType * pstrumETCVehicleInfoType：包含多车道自由流 ETC 车辆信息文

件中各项数据内容的结构体。

- 输出参数

无

#### 6.5.2.6 读取车辆信息文件

- 接口函数原型

int OBUProg_Read_ETCVehicleInfo(ETCVehicleInfoType * pstruETCVehicleInfoType);

int OBUProg_Read_MLFF_ETCVehicleInfo(mETCVehicleInfoType *

pstrumETCVehicleInfoType);

- 函数功能

读取 OBU 内 ETC 车辆信息文件中的相关内容。

- 返回值

0－信息读取成功；其他－信息读取失败。

- 输入参数

无

- 输出参数

ETCVehicleInfoType * pstruETCVehicleInfoType：包含高速公路 ETC 车辆信息文件中各项数据内容的结构体。

mETCVehicleInfoType * pstrumETCVehicleInfoType：包含多车道自由流 ETC 车辆信息文件中各项数据内容的结构体。

#### 6.5.2.7 OBU 防拆标志重置

- 接口函数原型

int OBUProg_Reset_TamperFlag();

- 函数功能

重置 OBU 的防拆卸标志位。

- 返回值

0－重置成功；其他－重置失败。

- 输入参数

无

- 输出参数

无

#### 6.5.2.8 写入汽车电子标识文件

- 接口函数原型

int OBUProg_Write_ETCVehiclAEIlateInfo(ETCVehiclAEIlateInfoType *
pstruETCVehiclAEIlateInfoType);

其中ETCVehiclAEIlateInfoType为自定义结构体类型，包含驾驶证信息文件中的各数据项、行驶证信息文件中的各数据项及车牌信息文件中的各数据项。其C语言定义如下：

```
typedef struct {
    driverLicenseType driverLicense;
    drivingLicenceType drivingLicense;
    vehiclAEIlateType vehiclAEIlateType;
}ETCVehiclAEIlateInfoType;
typedef struct {
    char IDCard[9];
    char Name[10];
    char SexClass;
    char Nationality[2];
    char Birthday[4];
    char IssueDay[4];
    char ValidFrom[4];
    char ValidFor;
    char FileNumber[6];
    char Address[60];
```

```
        char Administer[19];
} driverLicenseType ;
typedef struct {
        char CarPlate[10];
        char VehicleTypeID[2];
        char UseCharacter;
        char VehicleBrand[4];
        char VIN[17];
        char EIN[10];
        char RegisterDate[4];
        char IssueDate[4];
        char FileNumber[8];
        char Seats;
        char GVM[2];
        char CurbWeight[2];
        char CarringWeight[2];
        char VehicleSize[6];
        char CarOwner[40];
        char CarAddress[60];
        char TowWeight[2];
        char InsitutionSeal[30];
        char Reserved[45];
} drivingLicenceType ;
typedef struct {
        char PlateType;
        char CarPlate[10];
        char CarPlateColor;
```

```
    char CarColor;
    char CarSpeed;
    char CarEnvFlag;
    char CarCheckNextTime[7];
    char Manufacturer[2];
    char Reserved[36];
} vehiclAEIlateType;
```

- 函数功能

在 ETC 应用维护密钥的保护下写入汽车电子标识信息，即驾驶证信息文件、行驶证信息文件及车牌信息文件。

- 返回值

0 －信息写入成功；其他－写入失败。

- 输入参数

ETCVehiclAEIlateInfoType * pstruETCVehiclAEIlateInfoType：包含 AEI 应用中驾驶证信息文件、行驶证信息文件及车牌信息文件中各项数据内容的结构体。

- 输出参数

无

#### 6.5.2.9 读取汽车电子标识文件

- 接口函数原型

```
int OBUProg_Read_ETCVehiclAEIlateInfo(ETCVehiclAEIlateInfoType *
pstruETCVehiclAEIlateInfoType);
```

- 函数功能

读取 OBU 内汽车电子标识的相关文件中的相关内容。

- 返回值

0 －信息读取成功；其他－信息读取失败。

- 输入参数

无

- 输出参数

ETCVehiclAEIlateInfoType * pstruETCVehiclAEIlateInfoType：包含 AEI 应用中驾驶证信息文件、行驶证信息文件及车牌信息文件中各项数据内容的结构体。

### 6.5.2.10 写入电子年票文件

- 接口函数原型

int OBUProg_Write_ETCVehicleAnnualTicketInfo(ETCVehicleAnnualTicketType * pstruETCVehicleAnnualTicketType);

其中 ETCVehicleAnnualTicketType 为自定义结构体类型，包含年票信息文件中的各数据项。其 C 语言定义如下：

```
typedef struct {
    char CarPlate[10];
    char SignedDate[4];
    char ExpiredDate[4];
    char Reserved[22];
}ETCVehicleAnnualTicketType;
```

- 函数功能

在 ETC 应用维护密钥的保护下写入电子年票信息，即年票信息文件。

- 返回值

0－信息写入成功；其他－写入失败。

- 输入参数

ETCVehicleAnnualTicketType * pstruETCVehicleAnnualTicketType：包含 EAT 应用年票信息文件中各项数据内容的结构体。

- 输出参数

无

#### 6.5.2.11 读取电子年票文件

- 接口函数原型

int OBUProg_Read_ETCVehicleAnnualTicketInfo(ETCVehicleAnnualTicketType * pstruETCVehicleAnnualTicketType);

- 函数功能

读取 OBU 内电子年票文件中的相关内容。

- 返回值

0－信息读取成功；其他－信息读取失败。

- 输入参数

无

- 输出参数

ETCVehicleAnnualTicketType * pstruETCVehicleAnnualTicketType：包含年票信息文件中各项数据内容的结构体。

#### 6.5.2.12 发行信息的 MAC 计算

- 接口函数原型

int OBUProg_Get_IssueInfo_MAC(char * pcIssueInfo, int iInfoLen, char * pcIssueInfoMAC);

- 函数功能

使用 SAM 中指定的密钥，对本函数输入的发行信息计算 MAC，并输出。此 MAC 将用于后台系统验证数据库中的发行信息的正确性。

- 返回值

0－MAC 计算成功；其他－MAC 计算失败。

- 输入参数

char * pcIssueInfo：指向用于 MAC 计算的发行信息数据的指针

int iInfoLen：用于 MAC 计算的发行信息数据的长度。

- 输出参数

char * pcIssueInfoMAC：指向计算得到的 MAC 数据的指针，MAC 的长度为 4 字节。

#### 6.5.2.13 释放设备

- 接口函数原型

int OBUProg_DevRelease();

- 函数功能

关闭设备，释放所占用的各项系统资源。

- 返回值

0－释放成功；其他－释放失败。

- 输入参数

无

- 输出参数

无

# 7　手持式初始化设备

## 7.1　手持式初始化设备的接口

手持式初始化设备的接口如图所示。

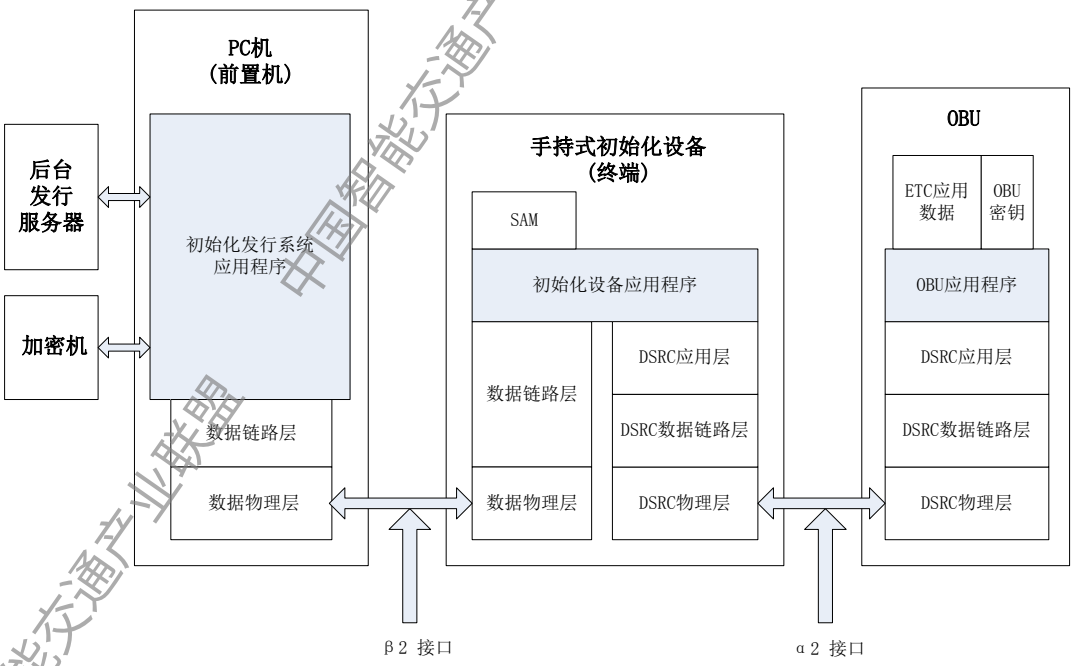



图 13　手持式初始化设备接口

其中：

- α2 接口：　OBU 与手持式初始化设备之间的 DSRC 接口，α2 接口规范要求与台式初始化设备中的α1 接口规范一致；

- β2 接口：手持式初始化设备与 PC 前置机之间的接口，β2 接口采用无线接口。

## 7.2 初始化发行操作的类别

### 7.2.1 机卡联合认证

实现终端与前置机之间的相互认证，机卡联合认证通过后，手持式初始化设备才能进行联机交易。在注销认证信息之前，系统只需要进行一次机卡联合认证。

机卡联合认证通过后，生成会话密钥，用于保证会话过程中所发送数据帧的真实性及完整性。

### 7.2.2 OBU 初始化

用 ETC 运营商密钥替换 OBU 供货时预置的传输密钥。此功能是联机操作，必须在机卡联合认证通过后才能执行。

### 7.2.3 OBU 个人化

更新“系统信息文件”、“高速公路 ETC 应用车辆信息文件”和“多车道自由流 ETC 应用车辆信息文件”。此功能是联机操作，必须在机卡联合认证通过后才能执行。

### 7.2.4 写系统信息

比对 OBU 车辆信息、更新 OBU 系统信息，复位 OBU 防拆位。此功能是联机操作，必须在机卡联合认证通过后才能执行。

### 7.2.5 后台信息查询

查询后台信息，结果返回至终端。

### 7.2.6 交易信息上传

上送脱机交易和联机交易后保存在终端内的交易信息。

### 7.2.7 激活

车辆拍照、复位 OBU 防拆位和延长有效期。激活可分为联机激活和脱机激活两种操作。对于联机操作，必须在机卡联合认证通过后才能执行。对于脱机操作，手持式初始化设备具有二次发行 PSAM 卡。

### 7.2.8 检测

验证系统信息、车辆信息、卡片信息的正确性。检测可分为脱机检测和联机检测两种操作。对于联机操作，必须在机卡联合认证通过后才能执行。对于脱机操作，手持式初始化设备具有二次发行 PSAM 卡。

### 7.2.9 汽车电子标识设置

更新 OBU 中“驾驶证信息文件”、“行驶证信息文件”和“车牌信息文件”。此功能是

联机操作，必须在机卡联合认证通过后才能执行。

#### 7.2.10 汽车电子标识稽查

验证驾驶证信息、行驶证信息、车牌信息的正确性。汽车电子标识稽查可分为脱机汽车电子标识稽查和联机汽车电子标识稽查两种操作。对于联机操作，必须在机卡联合认证通过后才能执行。对于脱机操作，手持式初始化设备具有二次发行 PSAM 卡。

#### 7.2.11 电子年票设置

更新 OBU 中“年票信息文件”。此功能是联机操作，必须在机卡联合认证通过后才能执行。

#### 7.2.12 电子年票稽查

验证年票信息的正确性。电子年票稽查可分为脱机电子年票稽查和电子年票稽查两种操作。对于联机操作，必须在机卡联合认证通过后才能执行。对于脱机操作，手持式初始化设备具有二次发行 PSAM 卡。

#### 7.2.13 照片上传

上送激活操作后保存在终端内的照片到服务器。此功能是联机操作，必须在机卡联合认证通过后才能执行。

#### 7.2.14 PSAM 卡认证

验证初始化设备中 PSAM 卡的有效性。此功能是联机操作，必须在机卡联合认证通过后才能执行。

#### 7.2.15 认证信息注销

注销机卡联合认证时产生的认证信息。

### 7.3 β2 接口规范

#### 7.3.1 物理接口形式

手持式初始化设备与发行控制系统之间的通信接口至少支持下列几种方式之一：

- Wi-Fi 接口

兼容 IEEEE 802.11b/g/n 标准。采用 Wifi 无线网络，及 TCP/IP 协议进行连接，在 TCP/IP 方式下手持式初始化设备作为客户端，PC 前置机为服务器端。

- 3G 接口

WCDMA，或 CDMA2000，或 TD-SCDMA。采用 3G 无线网络，及 TCP/IP 协议进行连接，在 TCP/IP 方式下手持式初始化设备作为客户端，PC 前置机为服务器端。

- 4G 接口

采用 4G 无线网络，及 TCP/IP 协议进行连接，在 TCP/IP 方式下手持式初始化设备作为客户端，PC 前置机为服务器端。

### 7.3.2 一般数据规定

#### 7.3.2.1 金额的表示

所有金额必须表示为以分为单位的 32 位无符号整型。这一定义与 PBOC2.0 规范中电子钱包金额表示相同。

#### 7.3.2.2 整数数值

在数据帧报文的传输中，凡涉及到整数，一律为无符号整数，以网络字节顺序传输，即都是高字节在前、低字节在后的方式。

#### 7.3.2.3 时间戳

时间戳的结构体格式，是便于终端编程的结构，前两个字节为 16 位二进制位整数表示的年份，字节顺序为 ARM/X86 体系结构顺序（即低字节在前、高字节在后），第三个字节为 8 位二进制位整数表示的月份（0x01~0x0C，即 1～12），第四个字节为表示的月份日期（0x01~0x1f，即 1～31），第五个字节为星期几（0～6），其中星期天为 0；第六个字节为 24 小时制的小时数，第七个字节为分钟，最后一个字节为秒。

#### 7.3.2.4 压缩十进制

每一个十进制数字用 4 位二进制数字表示，使用 8421 编码。一个字节表示两位十进制数。

#### 7.3.2.5 车辆信息密文数据长度

由于标准中的加密算法要求在车辆信息明文数据前增加 1 字节数据长度以及 8 字节校验信息，并且在车辆信息的明文后填充“8000”填充信息，将加密前的数据长度补齐为 8 的倍数，所以 ESAM 返回的加密后的车辆信息长度都是 8 的倍数。

在读取车辆信息时，只偏移读取前 59 个字节的文件信息即可。

#### 7.3.2.6 写车辆信息方式

写车辆信息时，是对车辆信息文件的前 59 个字节做偏移覆盖。使用明文加 MAC 的方式进行覆盖。

#### 7.3.2.7 机卡联合认证中密钥的分散次数

机卡联合认证中计算MAC时使用的密钥是二级分散后的国标CPU卡的记账TAC子密钥。

#### 7.3.2.8 数据帧中卡号的填写

“OBU 写车辆信息请求帧”和“后台信息查询请求帧”中的“国标 CPU 卡序列号”字段应填写插入 OBU 内的国标 CPU 卡卡号，以压缩十进制表示，如果读取不到卡号则以 8 字节“0xFF”进行填充。

#### 7.3.2.9 时间戳示例

例如:“2013 年 5 月 8 日 周三 11:27:18”转换成 8 字节时间戳表示为:DD070508030B1B12

#### 7.3.2.10 机卡联合认证终端计算 MAC 示例

机卡联合认证流程中，终端统一由卡片计算 MAC，使用内部认证指令，COS 指令参考如下：

0088020110 + 16 字节摘要信息 + 04

卡片返回的 4 字节数据即为 MAC。

#### 7.3.2.11 计算会话密钥时使用的数据源示例

例如使用 SHA1 算法得到 20 字节的摘要(Digest)码如下：

B21B96859A2D5511B109B2498CDD0353 11C8B129

计算第一组 MAC 使用的源数据：B21B96859A2D5511B109B2498CDD0353

计算第二组 MAC 使用的源数据：11 1B96859A2D5511B109B2498CDD0353

计算第三组 MAC 使用的源数据：B2 C8 96859A2D5511B109B2498CDD0353

计算第四组 MAC 使用的源数据：B21B B1 859A2D5511B109B2498CDD0353

计算第五组 MAC 使用的源数据：B21B96 29 9A2D5511B109B2498CDD0353

#### 7.3.2.12 SHA1 计算结果示例

例如源数据为 24 字节：

0001221DDD070508030A262CC54AC343DC070803050A2609

经 SHA1 算法散列后得 20 字节摘要码：

B21B96859A2D5511B109B2498CDD035311C8B129

#### 7.3.2.13HMAC_SHA1 计算结果示例

以 20 字节的“A5”作为密钥，以 64 字节的“A5”作为源数据，经过 HMAC_SHA1 加密计算后得到 20 字节数据为：

581ED91B67275B22D1CF0DE3E498F9A74D82B3EB

### 7.3.3 数据帧结构定义

每个数据帧的第一个字节都是帧类型，第二个字节都是帧长度。帧的末尾有若干填充字节，使得帧都是 16 字节对齐。帧长度包含了帧类型字节和帧末尾的填充字节。

初始化设备与发行控制系统之间是一种应答式的通讯方式：所有的协议流程都是“终端发出请求、前置机给出响应”这样的模式。

#### 7.3.3.1 数据帧列表

表 19 数据帧列表

| 数据帧名称 | 数据帧编号 | 发送方 | 接受方 |
|---|---|---|---|
| 挑战帧 | 0x00 | 初始化设备/发行控制系统 | 发行控制系统/初始化设备 |
| 认证信息帧 | 0x01 | 初始化设备 | 发行控制系统 |
| 响应认证信息帧 | 0x02 | 发行控制系统 | 初始化设备 |
| 写车辆信息请求帧 | 0x13 | 初始化设备 | 发行控制系统 |
| 写车辆信息应答帧 | 0x14 | 发行控制系统 | 初始化设备 |
| 读车辆信息请求帧 | 0x15 | 初始化设备 | 发行控制系统 |
| 读车辆信息应答帧 | 0x16 | 发行控制系统 | 初始化设备 |
| 写系统信息请求帧 | 0x17 | 初始化设备 | 发行控制系统 |
| 写系统信息应答帧 | 0x18 | 发行控制系统 | 初始化设备 |
| 系统信息比对请求帧 | 0x19 | 初始化设备 | 发行控制系统 |
| 系统信息比对应答帧 | 0x1A | 发行控制系统 | 初始化设备 |
| 后台信息查询请求帧 | 0x1B | 初始化设备 | 发行控制系统 |
| 后台信息查询应答帧 | 0x1C | 发行控制系统 | 初始化设备 |
| 交易信息上传帧 | 0x1D | 初始化设备 | 发行控制系统 |
| 交易信息上传应答帧 | 0x1E | 发行控制系统 | 初始化设备 |
| 注销认证信息请求帧 | 0x1F | 初始化设备 | 发行控制系统 |

表 19 数据帧列表（续）

| 数据帧名称 | 数据帧编号 | 发送方 | 接受方 |
|---|---|---|---|
| 注销认证信息应答帧 | 0x20 | 发行控制系统 | 初始化设备 |
| 替换密钥请求帧 | 0x21 | 初始化设备 | 发行控制系统 |
| 替换密钥应答帧 | 0x22 | 发行控制系统 | 初始化设备 |
| 系统信息初始化请求帧 | 0x23 | 初始化设备 | 发行控制系统 |
| 系统信息初始化应答帧 | 0x24 | 发行控制系统 | 初始化设备 |
| 写车牌信息请求帧 | 0x25 | 初始化设备 | 发行控制系统 |
| 写车牌信息应答帧 | 0x26 | 发行控制系统 | 初始化设备 |
| 车牌信息比对请求帧 | 0x27 | 初始化设备 | 发行控制系统 |
| 车牌信息比对应答帧 | 0x28 | 发行控制系统 | 初始化设备 |
| 写年票信息请求帧 | 0x29 | 初始化设备 | 发行控制系统 |
| 写年票信息应答帧 | 0x2A | 发行控制系统 | 初始化设备 |
| 年票信息比对请求帧 | 0x2B | 初始化设备 | 发行控制系统 |
| 年票信息比对应答帧 | 0x2C | 发行控制系统 | 初始化设备 |
| PSAM卡认证请求帧 | 0x2D | 初始化设备 | 发行控制系统 |
| PSAM卡认证应答帧 | 0x2E | 发行控制系统 | 初始化设备 |

### 7.3.3.2 挑战帧

表 20 挑战帧列表

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x00，表示该帧的类型为“挑战帧”。 |
| 帧长度 | 1 | 0x20，表示整个帧的长度。 |
| 填充字节 | 1 | 以“0xA5”字节进行填充。 |
| 填充字节 | 1 | 以“0xA5”字节进行填充。 |
| 随机数 | 4 | 发起挑战的一方生成；其中对于终端，必须是从IC卡通过Get Challenge指令获得。 |
| 时间戳 | 8 | 发起挑战的时刻，由发起挑战的一方生成，格式为“年月日周时分秒”，24小时制。 |
| 扩充信息 | 16 | 备用，暂时以“0xA5”字节进行填充。 |
| | | |
| 帧信息描述 | 初始化设备和发行控制系统相互发送的挑战信息，内含随机数，是机卡联合认证流程中相互生成MAC进行合法性校验的基础。同时保证了每次认证过程的独立性和唯一性。 | |

### 7.3.3.3 认证信息帧

表 21　认证信息帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x01，表示该帧的类型为“认证信息帧”。 |
| 帧长度 | 1 | 0x50，表示整个帧的长度。 |
| 管理员卡发行网络编号 | 2 | 压缩十进制表示的4位发行商网络编号，用于对比检查管理员卡是否属于系统内 |
| 管理员卡序列号 | 8 | 指管理员卡的8字节内部编号，压缩十进制编码。 |
| 终端物理串号 | 40 | 厂商提供的硬件统一编号(后补'\x0')，不足40字节后补“0x00”。ASCII编码。 |
| 身份认证码 | 16 | 生成算法见7.4.2节 |
| 扩展信息 | 12 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 由初始化设备发送到发行控制系统，内含初始化设备计算的身份认证码，在机卡联合认证流程中实现发行控制系统对终端和管理员卡的认证。<br>认证信息帧中的身份认证码，是按{发行控制系统随机数:4bytes, 管理员卡序列号:8bytes, 终端物理串号:40bytes, 终端时间戳:8bytes, 终端随机数:4bytes}顺序排列字段，组成身份认证码的明文，使用身份认证码生成算法生成 | |

### 7.3.3.4 响应认证信息帧

表 22　响应认证信息帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x02，表示该帧的类型为“响应认证信息帧” |
| 帧长度 | 1 | 0x30，表示整个帧的长度 |
| 终端机编号 | 6 | 管理编号，由发行控制系统提供，是终端的物理串号在系统中映射的唯一编号，二进制字节流 |
| 管理员编号 | 4 | 管理编号，由发行控制系统提供，是管理员卡号在系统中映射的唯一编号，编码方式，编码类型为整数数值型，网络字节序。 |
| 会话密钥整体超时时长 | 2 | 指会话密钥生成后的有效时长,超过该时长会话密钥自动失效。以分钟为单位，整数数值型 |
| 会话密钥空闲超时时长 | 2 | 指会话密钥生成后，手持机没有执行交易,空闲的时间长度超过该时长会话密钥自动失效。以分钟为单位，整数数值型 |
| 时间戳 | 8 | 指发行控制系统时间，格式为“年月日周时分秒”，24小时制 |
| 身份认证码 | 16 | 生成算法见7.4.2节 |
| 扩展信息 | 8 | 备用，暂时以“0xA5”字节进行填充 |
| | | |

表 22 响应认证信息帧（续）

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧信息描述 | 由发行控制系统发送到终端，内含发行控制系统计算的身份认证码，在机卡联合认证流程中实现终端对发行控制系统的认证<br>响应认证信息帧中的身份认证码，是按{终端机编号:6bytes, 管理员编号:4bytes, 发行控制系统时间戳:8bytes, 终端随机数:4bytes}顺序排列字段，组成身份认证码的明文，使用身份认证码生成算法生成 | |

### 7.3.3.5 OBU 写车辆信息请求帧

表 23 OBU 写车辆信息请求帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x13，表示该帧的类型为“OBU写车辆信息请求帧” |
| 帧长度 | 1 | 0x50，表示整个帧的长度 |
| 终端机编号 | 6 | 管理编号，由发行控制系统提供，是终端的物理串号在系统中映射的唯一编号，二进制字节流 |
| 管理员编号 | 4 | 管理编号，由发行控制系统提供，是管理员卡号在系统中映射的唯一编号，编码方式，编码类型为整数数值型，网络字节序 |
| 终端交易序号 | 4 | 终端交易日志中当前的流水号，由终端生成及维护，当日不可重复，对于同一笔交易，各帧的交易序号必须一致，编码类型为整数数值型，网络字节序。 |
| 填充字节 | 3 | 以“0xA5”字节进行填充 |
| OBU合同版本 | 1 | 指OBU中系统信息文件的“合同版本”，整数数值型 |
| OBU合同序列号 | 8 | 指OBU中系统信息文件的“合同序列号”，压缩十进制编码 |
| 国标CPU卡序列号 | 8 | 指插入OBU内部的国标CPU卡的8字节卡号，如未插入卡片则以“0xFF”填充，压缩十进制编码 |
| 随机数 | 8 | 在OBU使用Get Challenge指令获得随机数<br>“OBU合同版本”为“0x00”、“0x10”或“0x16”时，该随机数用于写OBU车辆信息文件时计算MAC，前4字节有效，后补4字节0<br>“OBU合同版本”为0x11时，该随机数用于之后的双向认证发行控制系统计算认证信息 |
| 时间戳 | 8 | 指终端时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 12 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于终端向发行控制系统发起写OBU车辆信息文件的请求 | |

#### 7.3.3.6 OBU 写车辆信息应答帧

表 24 OBU 写车辆信息应答帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x14，表示该帧的类型为“OBU写车辆信息应答帧” |
| 帧长度 | 1 | 0x70，表示整个帧的长度 |
| 应答返回码 | 1 | 0x00表示“指令可用于写OBU文件” |
| 填充字节 | 1 | 以“0xA5”字节进行填充 |
| 终端交易序号 | 4 | 与终端上送的“OBU写车辆信息请求帧”中的“终端交易序号”相同 |
| 写车辆信息指令 | 68 | 使用ESAM的“UpdateBinary”指令以偏移覆盖的方式，使用明文加MAC更新OBU车辆信息文件的前59个字节，由发行控制系统提供。具体指令参考《收费公路联网电子不停车收费技术要求》中OBU-SAM的相关规定。只有“应答返回码”返回“0x00”时该字段才有效，否则该字段以“0xA5”进行填充<br>“OBU写车辆信息请求帧”中“OBU合同版本”字段为“0x11”时，该字段用于发行控制系统返回双向认证时计算的认证信息，前8字节有效，之后补0 |
| 交易随机数 | 8 | 是发行控制系统对交易的唯一性生成的标识，终端在之后上送的数据帧中都应该携带该随机数，表明为同一笔交易。同一笔交易该随机数相同，不同的交易该随机数不同<br>该随机数也在终端读取车辆信息时参与使用，用于生成车辆信息的密文。<br>“OBU写车辆信息请求帧”中“OBU合同版本”字段为“0x11”时，该字段用于双向认证时发行控制系统返回随机数，供OBU计算认证信息 |
| 时间戳 | 8 | 指发行控制系统时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 4 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于OBU个人化流程中发行控制系统向终端回复写车辆信息文件的指令 | |

#### 7.3.3.7 OBU 读车辆信息请求帧

表 25　OBU 读车辆信息请求帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x15，表示该帧的类型为“OBU读车辆信息请求帧” |
| 帧长度 | 1 | 0x40，表示整个帧的长度 |
| 终端机编号 | 6 | 管理编号，由发行控制系统提供，是终端的物理串号在系统中映射的唯一编号，二进制字节流 |
| 管理员编号 | 4 | 管理编号，由发行控制系统提供，是管理员卡号在系统中映射的唯一编号，编码方式，编码类型为整数数值型，网络字节序 |
| 终端交易序号 | 4 | 终端交易日志中当前的流水号，由终端生成及维护，当日不可重复，对于同一笔交易，各帧的交易序号必须一致，编码类型为整数数值型，网络字节序 |
| 填充字节 | 3 | 以“0xA5”字节进行填充 |
| OBU合同版本 | 1 | 指OBU中系统信息文件的“合同版本”，整数数值型 |
| OBU合同序列号 | 8 | 指OBU中系统信息文件的“合同序列号”，压缩十进制编码 |
| 时间戳 | 8 | 指终端时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 12 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于向发行控制系统请求读OBU车辆信息文件所需要的随机数 | |

### 7.3.3.8 OBU 读车辆信息应答帧

表 26　OBU 读车辆信息应答帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x16，表示该帧的类型为“OBU读车辆信息应答帧” |
| 帧长度 | 1 | 0x30，表示整个帧的长度 |
| 应答返回码 | 1 | 0x00表示“成功，可读取车辆信息” |
| 填充字节 | 1 | 以“0xA5”字节进行填充 |
| 终端交易序号 | 4 | 与终端上送的“OBU读车辆信息应答帧”中的“终端交易序号”相同 |
| 交易随机数 | 8 | 是发行控制系统对交易的唯一性生成的标识,终端在之后上送的数据帧中都应该携带该随机数，表明为同一笔交易。同一笔交易该随机数相同，不同的交易该随机数不同。同时，该随机数也在终端读取车辆信息时参与使用，用于生成车辆信息的密文 |
| 时间戳 | 8 | 指发行控制系统时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 8 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于向终端返回读OBU车辆信息文件所需要的随机数 | |

7.3.3.9 OBU 写系统信息请求帧

**表 27 OBU 写系统信息请求帧**

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x17，表示该帧的类型为“OBU写系统信息请求帧” |
| 帧长度 | 1 | 0x90，表示整个帧的长度 |
| 终端机编号 | 6 | 管理编号，由发行控制系统提供，是终端的物理串号在系统中映射的唯一编号，二进制字节流 |
| 管理员编号 | 4 | 管理编号，由发行控制系统提供，是管理员卡号在系统中映射的唯一编号，编码方式，编码类型为整数数值型，网络字节序 |
| 终端交易序号 | 4 | 终端交易日志中当前的流水号，由终端生成及维护，当日不可重复，对于同一笔交易，各帧的交易序号必须一致，编码类型为整数数值型，网络字节序。 |
| 交易随机数 | 8 | 由发行控制系统生成，作为每笔交易的唯一标记，终端在之后上送的数据帧中都应该携带该随机数，表明为同一笔交易。同一笔交易该随机数相同，不同的交易该随机数不同 |
| 密钥分散因子 | 8 | 指产生OBU根目录下系统维护密钥和应用加密密钥使用的二级分散因子；<br>“OBU合同版本”为“0x11”和“0x12”时，该字段填写OBU复位信息，即2字节芯片厂商标识 + 2字节ITSC分配的ID号 + 4字节ESAM芯片序列号。<br>“OBU合同版本”为“0x00”或“0x10”时，且“密钥选择标识”字段为“0x0A”时，该字段填写OBU MAC地址（4个字节）+ OBU MAC地址按位取反（4个字节）。<br>其它版本填写OBU中系统信息文件的“合同序列号”，压缩十进制编码 |
| 车辆信息文件密文 | 72 | 读取OBU车辆信息后返回的密文。ESAM返回的密文数据长度为8的倍数，实际有效信息为车辆信息文件的前59字节的内容。72字节数据中包括1字节长度,8字节校验数据,59字节车辆信息以及5字节填充数据。<br>如果OBU返回明文信息，则直接上送59字节明文车辆信息，不足72字节后补0<br>如为双向认证获取的OBU车辆信息，则除了上送车辆明文信息外，还需上送8字节信息鉴别码，不足72字节后补0 |
| 随机数 | 4 | 在OBU的根目录下产生，用于写OBU系统信息文件时计算MAC。<br>当该字段为全0时，返回的“写系统信息应答帧”不返回有效的“写系统信息指令” |
| 时间戳 | 8 | 指终端时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 密钥选择标识 | 1 | 在“OBU合同版本”为“0x00”和“0x10”时，该字段有效，<br>指计算写OBU系统信息时使用的密钥<br>该字段为“0x0A”时，表示使用“应用维护密钥”计算写OBU系统信息安全报文<br>该字段为默认值“0xA5”时，表示使用默认的“系统维护密钥”计算写OBU系统信息安全报文 |
| 扩展信息 | 11 | 备用，暂时以“0xA5”字节进行填充 |
| | | |

表 27　OBU 写系统信息请求帧（续）

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧信息描述 | 用于终端向发行控制系统发起写OBU系统文件的请求，同时要求上送OBU的车辆信息，只有经过车辆信息的比对后发行控制系统才会返回写OBU系统信息所需要的指令<br>当终端只希望发行控制系统协助解密车辆信息，不需要写系统信息时（主要用于OBU检测业务），上送的“随机数”可以填充全0，此时发行控制系统返回的“写系统信息应答帧”中不返回有效的“写系统信息指令”，不能用于写系统信息 | |

### 7.3.3.10OBU 写系统信息应答帧

表 28　OBU 写系统信息应答帧

| 数据 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x18，表示该帧的类型为“OBU写系统信息应答帧” |
| 帧长度 | 1 | 0x80，表示整个帧的长度 |
| 应答返回码 | 1 | 0x00表示“指令可用于写OBU文件” |
| 填充字节 | 1 | 以“0xA5”字节进行填充 |
| 终端交易序号 | 4 | 与终端上送的“OBU写系统信息请求帧”中的“终端交易序号”相同 |
| 写系统信息指令 | 18 | 使用ESAM的“UpdateBinary”指令以偏移覆盖的方式，使用明文加MAC更新OBU系统信息文件中的“合同签署日期”、“合同过期日期”、“拆卸状态”，由发行控制系统提供。具体指令参考《收费公路联网电子不停车收费技术要求》中OBU-SAM的相关规定。只有“应答返回码”返回“0x00”时该字段才有效，否则该字段以“0xA5”进行填充<br>当“写系统信息请求帧”的随机数字段为全0时，该字段不返回写信息的COS指令，以“0xA5”进行填充 |
| 填充字节 | 2 | 以“0xA5”字节进行填充 |
| 车辆信息明文 | 59 | 是对终端上送的车辆信息密文解析后的车辆信息的明文内容，可用于终端展示。内容说明及编码方式参考《收费公路联网电子不停车收费技术要求》中表4-4的内容，与OBU内的车辆信息文件内容对应。只有“应答返回码”返回“0x00”和“0x03”时该字段才有效，否则该字段以“0xA5”进行填充 |
| 填充字节 | 1 | 以“0xA5”字节进行填充 |
| 时间戳 | 8 | 指发行控制系统时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 16 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于发行控制系统回应终端发起的写OBU系统文件的请求，回应内容包括车辆信息的明文以及写OBU系统信息的指令<br>终端上送的“OBU写系统信息请求帧”中的“随机数”为全0时，返回的 “写系统信息指令”无效，不能用于写系统信息 | |

### 7.3.3.11 OBU 系统信息比对请求帧

表 29　OBU 系统信息比对请求帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x19，表示该帧的类型为“OBU系统信息比对请求帧” |
| 帧长度 | 1 | 0x50，表示整个帧的长度 |
| 终端机编号 | 6 | 管理编号，由发行控制系统提供，是终端的物理串号在系统中映射的唯一编号，二进制字节流 |
| 管理员编号 | 4 | 管理编号，由发行控制系统提供，是管理员卡号在系统中映射的唯一编号，编码方式，编码类型为整数数值型，网络字节序 |
| 终端交易序号 | 4 | 终端交易日志中当前的流水号，由终端生成及维护，当日不可重复，对于同一笔交易，各帧的交易序号必须一致，编码类型为整数数值型，网络字节序 |
| 交易随机数 | 8 | 由发行控制系统生成，作为每笔交易的唯一标记，终端在之后上送的数据帧中都应该携带该随机数，表明为同一笔交易。同一笔交易该随机数相同，不同的交易该随机数不同 |
| OBU合同序列号 | 8 | 指OBU中系统信息文件的“合同序列号”，压缩十进制编码 |
| OBU合同签署日期 | 4 | 指OBU中系统信息文件的“合同签署日期”，格式为“yyyyMMdd”，压缩十进制编码 |
| OBU合同过期日期 | 4 | 指OBU中系统信息文件的“合同过期日期”，格式为“yyyyMMdd”，压缩十进制编码 |
| 拆卸状态 | 1 | 指OBU中系统信息文件的“拆卸状态” |
| 填充字节 | 3 | 以“0xA5”字节进行填充 |
| 时间戳 | 8 | 指终端时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 12 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于终端向发行控制系统申请确认指定的OBU是否已成功的更新了系统信息文件 | |

### 7.3.3.12 OBU 系统信息比对应答帧

表 30　OBU 系统信息比对应答帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x1A，表示该帧的类型为“OBU系统信息比对应答帧” |
| 帧长度 | 1 | 0x30，表示整个帧的长度 |
| 应答返回码 | 1 | 0x00表示“比对成功” |
| 填充字节 | 1 | 以“0xA5”字节进行填充 |
| 终端交易序号 | 4 | 与终端上送的“OBU写系统信息请求帧”中的“终端交易序号”相同 |
| 时间戳 | 8 | 指发行控制系统时间，格式为“年月日周时分秒”，24小时制 |

表 30　OBU 系统信息比对应答帧（续）

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 16 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于发行控制系统向终端回应指定OBU是否已经成功的书写了系统信息文件 | |

### 7.3.3.13后台信息查询请求帧

表 31　后台信息查询请求帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x1B，表示该帧的类型为“后台信息查询请求帧” |
| 帧长度 | 1 | 0x40，表示整个帧的长度 |
| 终端机编号 | 6 | 管理编号，由发行控制系统提供，是终端的物理串号在系统中映射的唯一编号，二进制字节流 |
| 管理员编号 | 4 | 管理编号，由发行控制系统提供，是管理员卡号在系统中映射的唯一编号，编码方式，编码类型为整数数值型，网络字节序 |
| 终端交易序号 | 4 | 终端交易日志中当前的流水号，由终端生成及维护，当日不可重复，对于同一笔交易，各帧的交易序号必须一致，编码类型为整数数值型，网络字节序 |
| 填充字节 | 3 | 以“0xA5”字节进行填充 |
| OBU合同版本 | 1 | 指OBU中系统信息文件的“合同版本”，整数数值型 |
| OBU合同序列号 | 8 | 指OBU中系统信息文件的“合同序列号”，压缩十进制编码 |
| 国标CPU卡序列号 | 8 | 指插入OBU内部的国标CPU卡的8字节卡号，如未插入卡片则以“0xFF”填充，压缩十进制编码 |
| 时间戳 | 8 | 指终端时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 4 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于终端向发行控制系统发起后台查询的请求，同时上送OBU合同序列号及合同版本号作为查询依据 | |

### 7.3.3.14后台信息查询应答帧

表 32　后台信息查询应答帧

| 数据 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x1C，表示该帧的类型为“后台信息查询应答帧” |
| 帧长度 | 1 | 0x70，表示整个帧的长度 |
| 应答返回码 | 1 | 0x00表示“后台信息查询成功”。卡片状态，OBU状态等信息也通过该字段返回 |
| 填充字节 | 1 | 以“0xA5”字节进行填充 |
| 终端交易序号 | 4 | 与终端上送的“后台信息查询请求帧”中的“终端交易序号”相同 |
| OBU启用日期 | 4 | 指数据库中记录的OBU合同签署日期，与OBU内存放日期的格式相同，压缩十进制表示。只有“应答返回码”返回“0x00”时该字段才有效，否则该字段以“0xA5”进行填充 |
| OBU到期日期 | 4 | 值数据库中记录的OBU合同过期日期，与OBU内存放日期的格式相同，压缩十进制表示。只有“应答返回码”返回“0x00”时该字段才有效，否则该字段以“0xA5”进行填充 |
| 车辆信息 | 59 | 内容说明及编码方式参考《收费公路联网电子不停车收费技术要求》中表4-4的内容，与OBU内的车辆信息文件内容对应。只有“应答返回码”返回“0x00”时该字段才有效，否则该字段以“0xA5”进行填充 |
| 填充字节 | 1 | 以“0xA5”字节进行填充 |
| 时间戳 | 8 | 指发行控制系统时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 12 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于发行控制系统回应终端发起的后台查询请求，回应内容包括卡片及OBU的状态、OBU有效期及绑定的车辆信息等 | |

### 7.3.3.15 交易信息上传帧

表 33　交易信息上传帧

| 数据 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x1D，表示该帧的类型为“交易信息上传帧” |
| 帧长度 | 1 | 0xE0，表示整个帧的长度 |
| 报文验证方式 | 1 | 如果是以“0xA5”填充，表示上传的是默认的联机交易记录,且用指纹码做报文验证<br>如果为0，表示上传的是脱机交易记录,且用指纹码做报文验证<br>如果为1，表示上传的是脱机交易记录,且用数字签名做报文验证 |
| OBU合同版本 | 1 | 指OBU中系统信息文件的“合同版本”，整数数值型 |
| 终端物理串号 | 40 | 厂商提供的硬件统一编号(后补'\x0')，不足40字节后补“0x00”。ASCII编码 |
| 管理员卡序列号 | 8 | 指操作业务时使用的管理员卡的8字节内部编号，压缩十进制编码 |
| 终端交易序号 | 4 | 指交易时终端给该笔交易分配的流水号，编码类型为整数数值型 |
| OBU合同序列号 | 8 | 指OBU中系统信息文件的“合同序列号”，压缩十进制编码 |

表 33 交易信息上传帧（续）

| 数据 | 长度(Byte) | 说明 |
|---|---|---|
| 国标CPU卡序列号 | 8 | 指插入OBU内部的国标CPU卡的8字节卡号<br>如未插入卡片则以“0xFF”填充，压缩十进制编码 |
| 写车辆信息随机数 | 4 | 在OBU的DF01目录下使用Get Challenge指令获得，用于写OBU车辆信息文件时计算MAC<br>如果交易流程中未更新车辆信息，该字段以全0进行填充 |
| 写车辆信息指令 | 68 | 使用ESAM的“UpdateBinary”指令以偏移覆盖的方式，使用明文加MAC更新OBU车辆信息文件的前59个字节<br>如果指令长度不足68字节，则后补“0x00”<br>如果交易流程中未更新车辆信息，该字段以“0xA5”进行填充 |
| 密钥分散因子 | 8 | 指产生OBU根目录下系统维护密钥使用的二级分散因子；<br>“OBU合同版本”为“0x11”和“0x12”时，该字段填写OBU复位信息，即2字节芯片厂商标识 + 2字节ITSC分配的ID号 + 4字节ESAM芯片序列号<br>“OBU合同版本”为“0x00”和“0x10”时，该字段填写OBU的MAC地址及地址取反后的8字节信息<br>其它版本该字段填写OBU合同序列号 |
| 写系统信息随机数 | 4 | 在OBU的根目录下产生，用于写OBU系统信息文件时计算MAC<br>如果交易流程中未更新系统信息，该字段以全0进行填充 |
| 写系统信息指令 | 20 | 使用ESAM的“UpdateBinary”指令以偏移覆盖的方式，使用明文加MAC更新OBU系统信息文件中的“合同签署日期”、“合同过期日期”、“拆卸状态”三个字段。<br>如果指令长度不足20字节，则后补“0x00”<br>如果交易流程中未更新系统信息，该字段以“0xA5”进行填充 |
| 交易时间 | 8 | 指终端机记录的交易发生的时间，格式为“年月日周时分秒” |
| 时间戳 | 8 | 指上传交易信息时的终端时间，格式为“年月日周时分秒”，24小时制。<br>在计算该报文的数字签名时,该字段内容与“交易时间”保持一致；<br>上传交易时该字段填写交易上传的时间点 |
| 指纹码/数字签名 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 16 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于上传终端内的单笔交易信息 | |

### 7.3.3.16交易信息上传应答帧

表 34　交易信息上传应答帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x1E，表示该帧的类型为“交易信息上传应答帧” |
| 帧长度 | 1 | 0x30，表示整个帧的长度 |
| 应答返回码 | 1 | 0x00表示“上传成功” |
| 填充字节 | 1 | 以“0xA5”字节进行填充 |
| 终端交易序号 | 4 | 与终端上送的“交易信息上传帧”中的“终端交易序号”相同 |
| 时间戳 | 8 | 指发行控制系统时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 使用该终端当前有效的会话密钥计算指纹码，生成算法见7.4.4节 |
| 扩展信息 | 16 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 发行控制系统应答终端，表示交易记录是否成功上传 | |

7.3.3.17注销认证信息请求帧

表 35　注销认证信息请求帧

| 数据 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x1F，表示该帧的类型为“注销认证信息请求帧” |
| 帧长度 | 1 | 0x40，表示整个帧的长度 |
| 终端机编号 | 6 | 管理编号，由发行控制系统提供，是终端的物理串号在系统中映射的唯一编号，二进制字节流 |
| 管理员编号 | 4 | 管理编号，由发行控制系统提供，是管理员卡号在系统中映射的唯一编号，编码方式，编码类型为整数数值型，网络字节序 |
| 终端交易序号 | 4 | 指终端记录的最后一条交易记录的终端机交易序号，编码类型为整数数值型，网络字节序<br>如果没有产生交易记录则填写0 |
| 交易时间 | 8 | 指终端记录的最后一笔交易记录的时间，格式为“年月日周时分秒”。如果没有产生交易记录则应该告知发行控制系统是哪一个交易日没有产生交易记录。则交易时间退化为交易日，“时分秒”部分可填写全0 |
| 时间戳 | 8 | 指上传交易信息时的终端时间，格式为“年月日周时分秒”，24小时制。 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 16 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于注销机卡联合认证信息产生的认证信息并确认所有交易信息都已经上传，成功后会话密钥将过期失效。请求帧中需携带最后一条交易记录的终端机交易序号及交易日期，用于确认是否所有的交易都已经成功上传 | |

### 7.3.3.18 注销认证信息应答帧

表 36　注销认证信息应答帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x20，表示该帧的类型为“注销认证信息应答帧” |
| 帧长度 | 1 | 0x30，表示整个帧的长度 |
| 应答返回码 | 1 | 0x00表示“注销成功” |
| 填充字节 | 1 | 以“0xA5”字节进行填充 |
| 终端交易序号 | 4 | 与“注销认证信息请求帧”中的“终端交易序号”字段相同 |
| 未上传的交易序号 | 4 | 指在交易日期内未上传交易信息的最小的终端交易序号，如果已经全部上传则填写0 |
| 时间戳 | 8 | 为明确告知终端“未上传的交易序号”隶属的交易日期，该字段与“注销认证信息请求帧”中的“时间戳”字段相同 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 8 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于返回信息表示机卡联合认证信息是否注销成功 | |

### 7.3.3.19 OBU 替换密钥请求帧

表 37　OBU 替换密钥请求帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x21，表示该帧的类型为“OBU替换密钥请求帧” |
| 帧长度 | 1 | 0x60，表示整个帧的长度 |
| 终端机编号 | 6 | 管理编号，由前置机提供，是终端的物理串号在系统中映射的唯一编号，编码类型为整数数值型 |
| 管理员编号 | 4 | 管理编号，由前置机提供，是管理员卡号在系统中映射的唯一编号，编码方式，编码类型为整数数值型 |
| 终端交易序号 | 4 | 终端交易日志中当前的流水号，由终端生成及维护，当日不可重复，对于同一笔交易，各帧的交易序号必须一致，编码类型为整数数值型 |
| 密钥分散因子 | 8 | 指ESAM卡商唯一指定的芯片序号或者OBU系统信息内的合同序列号 |
| 保护密钥分散因子 | 8 | 指ESAM卡商唯一指定的芯片序号或者OBU系统信息内的合同序列号 |
| 随机数 | 4 | 在OBU的根目录下产生，用于替换密钥时计算MAC |
| 帧标识 | 1 | 用于区分手持终端及桌面发行终端（两者取用会话密钥机制不一致），0x00表示手持终端，0xA5表示桌面发行终端 |
| 填充字节 | 3 | 以“0xA5”字节进行填充 |
| 替换密钥指令 | 5 | 替换密钥的5字节指令 |
| 密钥代码 | 1 | 指需要替换的密钥标识 |

表 37 OBU 替换密钥请求帧（续）

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| OBU协约类型 | 1 | 指OBU系统信息内的协约类型 |
| OBU合同版本 | 1 | 指OBU系统信息内的合同版本 |
| OBU发行方标识 | 8 | 指OBU系统信息内的8字节发行方标识 |
| 时间戳 | 8 | 指终端时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 16 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于替换密钥的请求帧，终端可申请替换OBU内的所有密钥，需要在该帧中指定需要替换的密钥，以及上传OBU的系统信息和ESAM的芯片序列号，发送一次请求帧只能替换一条密钥 | |

### 7.3.3.20OBU 替换密钥应答帧

表 38　OBU 替换密钥应答帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x22，表示该帧的类型为“OBU替换密钥应答帧” |
| 帧长度 | 1 | 0x50，表示整个帧的长度 |
| 应答返回码 | 1 | 0x00表示“成功，可替换密钥”，其它值见5.23节 |
| 密钥代码 | 1 | 指本次ESAM指令要替换的密钥的代码，与开始帧的“密钥代码”字段一致，终端可用于确认返回的ESAM指令是否过期，避免锁标签 |
| 终端交易序号 | 4 | 终端交易日志中当前的流水号，由终端生成及维护，当日不可重复，对于同一笔交易，各帧的交易序号必须一致，编码类型为整数数值型 |
| 随机数 | 4 | 该随机数是前置机计算ESAM指令中的MAC时使用的随机数，原值由终端上送，这里返回给终端，供终端判断该应答帧是否过期，避免错误的尝试锁标签 |
| 填充字节 | 4 | 以“0xA5”字节进行填充 |
| 密钥密文及MAC | 28 | 24字节密文，4字节MAC组成，直接送入ESAM中用于替换密钥 |
| 填充字节 | 4 | 以“0xA5”字节进行填充 |
| 时间戳 | 8 | 指终端时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 8 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于响应请求帧，携带OBU替换密钥所使用的ESAM指令 | |

### 7.3.3.21 OBU 文件信息初始化请求帧

表 39　OBU 文件信息初始化请求帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x23，表示该帧的类型为“OBU系统信息初始化请求帧” |
| 帧长度 | 1 | 0x40，表示整个帧的长度 |
| 终端机编号 | 6 | 管理编号，由前置机提供，是终端的物理串号在系统中映射的唯一编号，编码类型为整数数值型 |
| 管理员编号 | 4 | 管理编号，由前置机提供，是管理员卡号在系统中映射的唯一编号，编码方式，编码类型为整数数值型。 |
| 终端交易序号 | 4 | 终端交易日志中当前的流水号，由终端生成及维护，当日不可重复，对于同一笔交易，各帧的交易序号必须一致，编码类型为整数数值型 |
| 密钥分散因子 | 8 | 指ESAM卡商唯一指定的芯片序号或者OBU系统信息内的合同序列号 |
| 随机数 | 4 | 在OBU内产生，用于写OBU系统信息文件或车辆信息文件时计算MAC。 |
| 文件标识 | 1 | 0表示系统信息文件，1表示车辆信息文件，告知前置机需要初始化的文件。整数数值型 |
| 填充字节 | 3 | 以“0xA5”字节进行填充 |
| 时间戳 | 8 | 指终端时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 8 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 在OBU密钥装载业务中，除了需要替换OBU的密钥，还需要重新书写OBU的各个文件，尤其是系统信息文件和车辆信息文件 | |

### 7.3.3.22 OBU 文件信息初始化应答帧

表 40　OBU 文件信息初始化应答帧

| 数据 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x24，表示该帧的类型为“OBU文件信息初始化应答帧” |
| 帧长度 | 1 | 0x70，表示整个帧的长度 |
| 应答返回码 | 1 | 0x00表示“指令可用于写OBU文件”，其它值见5.23节 |
| 填充字节 | 1 | 以“0xA5”字节进行填充 |
| 终端交易序号 | 4 | 与终端上送的“OBU写系统信息请求帧”中的“终端交易序号”相同。 |
| 文件标识 | 1 | 0表示系统信息文件，1表示车辆信息文件，告知前置机需要初始化的文件。整数数值型 |
| 填充字节 | 3 | 以“0xA5”字节进行填充 |

表 40 OBU 文件信息初始化应答帧（续）

| 数据 | 长度(Byte) | 说明 |
|---|---|---|
| 写文件信息指令 | 68 | 使用ESAM的“UpdateBinary”指令覆盖OBU文件信息,由前置机提供。具体指令参考《收费公路联网电子不停车收费技术要求》中OBE-SAM的相关规定<br>只有“应答返回码”返回“0x00”时该字段才有效,否则该字段以“0xA5”进行填充<br>根据文件标识，该指令可返回写各种文件信息的指令，根据不同文件的长度，该字段内容部分有效或全部有效<br>如果指令长度不足68字节，则后补“0x00” |
| 时间戳 | 8 | 指前置机时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 8 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 是对“OBU文件信息初始化请求帧”的应答，其中包括写文件信息的ESAM指令。 | |

### 7.3.3.23写汽车电子标识信息请求帧

表 41　OBU 写汽车电子标识信息请求帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x25，表示该帧的类型为“OBU写车牌信息请求帧” |
| 帧长度 | 1 | 0x50，表示整个帧的长度 |
| 终端机编号 | 6 | 管理编号，由发行控制系统提供，是终端的物理串号在系统中映射的唯一编号，二进制字节流 |
| 管理员编号 | 4 | 管理编号，由发行控制系统提供，是管理员卡号在系统中映射的唯一编号，编码方式，编码类型为整数数值型，网络字节序 |
| 终端交易序号 | 4 | 终端交易日志中当前的流水号，由终端生成及维护，当日不可重复，对于同一笔交易，各帧的交易序号必须一致，编码类型为整数数值型，网络字节序 |
| 填充字节 | 3 | 以“0xA5”字节进行填充 |
| OBU合同版本 | 1 | 指OBU中系统信息文件的“合同版本”，整数数值型 |
| OBU合同序列号 | 8 | 指OBU中系统信息文件的“合同序列号”，压缩十进制编码 |
| 国标CPU卡序列号 | 8 | 指插入OBU内部的国标CPU卡的8字节卡号，如未插入卡片则以“0xFF”填充，压缩十进制编码 |
| 随机数 | 8 | 在OBU使用Get Challenge指令获得随机数<br>“OBU合同版本”为“0x00”、“0x10”或“0x16”时，该随机数用于写OBU车辆信息文件时计算MAC，前4字节有效，后补4字节0。<br>“OBU合同版本”为0x11时，该随机数用于之后的双向认证发行控制系统计算认证信息 |

表 41 OBU 文件信息初始化应答帧（续）

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 时间戳 | 8 | 指终端时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 12 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于终端向发行控制系统发起写OBU车牌信息文件的请求。根据业务需要使用标签合同序列号、国标CPU卡号唯一获取车牌的信息，用以填写OBU的车牌信息文件 | |

### 7.3.3.24OBU 写汽车电子标识信息应答帧

表 42 OBU 写汽车电子标识信息应答帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x26，表示该帧的类型为“OBU写车牌信息应答帧” |
| 帧长度 | 1 | 0x190 表示整个帧的长度 |
| 应答返回码 | 1 | 0x00表示“指令可用于写OBU文件” |
| 填充字节 | 1 | 以“0xA5”字节进行填充 |
| 终端交易序号 | 4 | 与终端上送的“OBU写车牌信息请求帧”中的“终端交易序号”相同。 |
| 写驾驶证信息指令 | 124 | 使用CPU的“UpdateBinary”指令以偏移覆盖的方式，使用明文加MAC更新驾驶证信息文件的前120个字节，由发行控制系统提供。只有“应答返回码”返回“0x00”时该字段才有效，否则该字段以“0xA5”进行填充 |
| 写行驶证信息 | 212 | 使用ESAM的“UpdateBinary”指令以偏移覆盖的方式，使用明文加MAC更新行驶证信息文件的前205个字节，由发行控制系统提供。只有“应答返回码”返回“0x00”时该字段才有效，否则该字段以“0xA5”进行填充 |
| 写车牌信息 | 28 | 使用ESAM的“UpdateBinary”指令以偏移覆盖的方式，使用明文加MAC更新车牌信息文件的前18个字节，由发行控制系统提供。只有“应答返回码”返回“0x00”时该字段才有效，否则该字段以“0xA5”进行填充 |
| 交易随机数 | 8 | 是发行控制系统对交易的唯一性生成的标识，终端在之后上送的数据帧中都应该携带该随机数，表明为同一笔交易。同一笔交易该随机数相同，不同的交易该随机数不同<br>该随机数也在终端读取车辆信息时参与使用，用于生成车辆信息的密文<br>“OBU写车辆信息请求帧”中“OBU合同版本”字段为“0x11”时，该字段用于双向认证时发行控制系统返回随机数，供OBU计算认证信息 |
| 时间戳 | 8 | 指发行控制系统时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 4 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于发行控制系统向终端回复写车牌信息文件的指令 | |

### 7.3.3.25OBU 汽车电子标识信息比对请求帧

表 43　OBU 汽车电子标识信息比对请求帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x27，表示该帧的类型为“OBU汽车电子标识信息比对请求帧” |
| 帧长度 | 1 | 0x190表示整个帧的长度 |
| 终端机编号 | 6 | 管理编号，由发行控制系统提供，是终端的物理串号在系统中映射的唯一编号，二进制字节流 |
| 管理员编号 | 4 | 管理编号，由发行控制系统提供，是管理员卡号在系统中映射的唯一编号，编码方式，编码类型为整数数值型，网络字节序 |
| 终端交易序号 | 4 | 终端交易日志中当前的流水号，由终端生成及维护，当日不可重复，对于同一笔交易，各帧的交易序号必须一致，编码类型为整数数值型，网络字节序 |
| 交易随机数 | 8 | 由发行控制系统生成，作为每笔交易的唯一标记，终端在之后上送的数据帧中都应该携带该随机数，表明为同一笔交易。同一笔交易该随机数相同，不同的交易该随机数不同 |
| 驾驶证信息 | 120 | 指OBU中AEI应用驾驶证信息文件所有数据项 |
| 行驶证信息 | 208 | 指OBU中AEI应用行驶证信息文件所有数据项 |
| 车牌信息 | 24 | 指OBU中AEI应用车牌信息文件所有数据项 |
| 时间戳 | 8 | 指终端时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| | | |
| 帧信息描述 | 用于终端向发行控制系统申请确认指定的汽车电子标识信息是否已成功的更新了 | |

### 7.3.3.26OBU 汽车电子标识比对应答帧

表 44　OBU 系统信息比对应答帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x28，表示该帧的类型为“OBU汽车电子标识信息比对应答帧” |
| 帧长度 | 1 | 0x30，表示整个帧的长度 |
| 应答返回码 | 1 | 0x00表示“比对成功” |
| 填充字节 | 1 | 以“0xA5”字节进行填充 |
| 终端交易序号 | 4 | 与终端上送的“OBU汽车电子标识信息比对请求帧”中的“终端交易序号”相同 |
| 时间戳 | 8 | 指发行控制系统时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 16 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于发行控制系统向终端回应指定OBU是否已经成功的书写了汽车电子标识信息文件 | |

### 7.3.3.27OBU 写电子年票信息请求帧

表 45　OBU 写电子年票信息请求帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x29，表示该帧的类型为“OBU写年票信息请求帧” |
| 帧长度 | 1 | 0x50，表示整个帧的长度 |
| 终端机编号 | 6 | 管理编号，由发行控制系统提供，是终端的物理串号在系统中映射的唯一编号，二进制字节流 |
| 管理员编号 | 4 | 管理编号，由发行控制系统提供，是管理员卡号在系统中映射的唯一编号，编码方式，编码类型为整数数值型，网络字节序 |
| 终端交易序号 | 4 | 终端交易日志中当前的流水号，由终端生成及维护，当日不可重复，对于同一笔交易，各帧的交易序号必须一致，编码类型为整数数值型，网络字节序 |
| 填充字节 | 3 | 以“0xA5”字节进行填充 |
| OBU合同版本 | 1 | 指OBU中系统信息文件的“合同版本”，整数数值型 |
| OBU合同序列号 | 8 | 指OBU中系统信息文件的“合同序列号”，压缩十进制编码 |
| 国标CPU卡序列号 | 8 | 指插入OBU内部的国标CPU卡的8字节卡号，如未插入卡片则以“0xFF”填充，压缩十进制编码 |
| 随机数 | 8 | 在OBU使用Get Challenge指令获得随机数<br>“OBU合同版本”为“0x00”、“0x10”或“0x16”时，该随机数用于写OBU车辆信息文件时计算MAC，前4字节有效，后补4字节0<br>“OBU合同版本”为0x11时，该随机数用于之后的双向认证发行控制系统计算认证信息 |
| 时间戳 | 8 | 指终端时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 12 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于终端向发行控制系统发起写OBU年票信息文件的请求 | |

### 7.3.3.28 OBU 写电子年票信息应答帧

表 46　OBU 写电子年票信息应答帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x2A，表示该帧的类型为“OBU写年票信息应答帧” |
| 帧长度 | 1 | 0x40 表示整个帧的长度 |
| 应答返回码 | 1 | 0x00表示“指令可用于写OBU文件” |
| 填充字节 | 1 | 以“0xA5”字节进行填充 |
| 终端交易序号 | 4 | 与终端上送的“OBU写车牌信息请求帧”中的“终端交易序号”相同 |

表 46 OBU 写电子年票信息应答帧（续）

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 写年票信息指令 | 24 | 使用ESAM的“UpdateBinary”指令以偏移覆盖的方式，使用明文加MAC更新年票信息文件的前18个字节，由发行控制系统提供。只有“应答返回码”返回“0x00”时该字段才有效，否则该字段以“0xA5”进行填充 |
| 交易随机数 | 8 | 是发行控制系统对交易的唯一性生成的标识，终端在之后上送的数据帧中都应该携带该随机数，表明为同一笔交易。同一笔交易该随机数相同，不同的交易该随机数不同<br>该随机数也在终端读取车辆信息时参与使用，用于生成车辆信息的密文“OBU写车辆信息请求帧”中“OBU合同版本”字段为“0x11”时，该字段用于双向认证时发行控制系统返回随机数，供OBU计算认证信息。 |
| 时间戳 | 8 | 指发行控制系统时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| | | |
| 帧信息描述 | 用于发行控制系统向终端回复写年票信息文件的指令 | |

### 7.3.3.29OBU 电子年票信息比对请求帧

表 47　OBU 电子年票信息比对请求帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x2B，表示该帧的类型为“OBU电子年票信息比对请求帧” |
| 帧长度 | 1 | 0x50表示整个帧的长度 |
| 终端机编号 | 6 | 管理编号，由发行控制系统提供，是终端的物理串号在系统中映射的唯一编号，二进制字节流 |
| 管理员编号 | 4 | 管理编号，由发行控制系统提供，是管理员卡号在系统中映射的唯一编号，编码方式，编码类型为整数数值型，网络字节序 |
| 终端交易序号 | 4 | 终端交易日志中当前的流水号，由终端生成及维护，当日不可重复，对于同一笔交易，各帧的交易序号必须一致，编码类型为整数数值型，网络字节序 |
| 交易随机数 | 8 | 由发行控制系统生成，作为每笔交易的唯一标记，终端在之后上送的数据帧中都应该携带该随机数，表明为同一笔交易。同一笔交易该随机数相同，不同的交易该随机数不同 |
| 年票信息 | 20 | 指OBU中EAT应用年票信息文件所有数据项 |
| 时间戳 | 8 | 指终端时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 12 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于终端向发行控制系统申请确认指定的汽车电子标识信息是否已成功的更新了 | |

### 7.3.3.30OBU 电子年票比对应答帧

表 48　电子年票信息比对应答帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x2C，表示该帧的类型为“OBU电子年票信息比对应答帧” |
| 帧长度 | 1 | 0x30，表示整个帧的长度 |
| 应答返回码 | 1 | 0x00表示“比对成功” |
| 填充字节 | 1 | 以“0xA5”字节进行填充 |
| 终端交易序号 | 4 | 与终端上送的“OBU电子年票信息比对请求帧”中的“终端交易序号”相同 |
| 时间戳 | 8 | 指发行控制系统时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 16 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于发行控制系统向终端回应指定OBU是否已经成功的书写了电子年票信息文件 | |

### 7.3.3.31PSAM 卡认证请求帧

表 49　PSAM 卡认证请求帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x2D，表示该帧的类型为“PSAM卡认证请求帧” |
| 帧长度 | 1 | 0x40表示整个帧的长度 |
| 终端机编号 | 6 | 管理编号，由发行控制系统提供，是终端的物理串号在系统中映射的唯一编号，二进制字节流 |
| 管理员编号 | 4 | 管理编号，由发行控制系统提供，是管理员卡号在系统中映射的唯一编号，编码方式，编码类型为整数数值型，网络字节序 |
| 终端交易序号 | 4 | 终端交易日志中当前的流水号，由终端生成及维护，当日不可重复，对于同一笔交易，各帧的交易序号必须一致，编码类型为整数数值型，网络字节序 |
| 交易随机数 | 8 | 由发行控制系统生成，作为每笔交易的唯一标记，终端在之后上送的数据帧中都应该携带该随机数，表明为同一笔交易。同一笔交易该随机数相同，不同的交易该随机数不同 |
| PSAM卡号 | 8 | 指初始化设备中PSAM卡的卡号 |
| 时间戳 | 8 | 指终端时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 8 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于终端向发行控制系统申请确认指定的PSAM卡是否有效 | |

### 7.3.3.32PSAM 卡认证应答帧

表 50　PSAM 卡认证应答帧

| 字段名称 | 长度(Byte) | 说明 |
|---|---|---|
| 帧类型编号 | 1 | 0x2E，表示该帧的类型为“PSAM卡认证应答帧” |
| 帧长度 | 1 | 0x30，表示整个帧的长度 |
| 应答返回码 | 1 | 0x00表示“卡片有效” |
| 填充字节 | 1 | 以“0xA5”字节进行填充 |
| 终端交易序号 | 4 | 与终端上送的“PSAM卡认证请求帧”中的“终端交易序号”相同 |
| 时间戳 | 8 | 指发行控制系统时间，格式为“年月日周时分秒”，24小时制 |
| 指纹码 | 16 | 生成算法见7.4.4节 |
| 扩展信息 | 16 | 备用，暂时以“0xA5”字节进行填充 |
| | | |
| 帧信息描述 | 用于发行控制系统向终端回应指定PSAM是否有效 | |

### 7.3.3.33 应答返回码列表

表 51　应答返回码列表

| 应答返回码 | 含义 |
|---|---|
| 0x00 | 成功，无错误 |
| 0x01 | 服务不可用，请联系系统管理员 |
| 0x02 | 会话超时，请重新执行机卡联合认证 |
| 0x03 | 返回车辆信息有效,但COS指令不可用于写文件 |
| 0x04 | 该CPU卡未发行 |
| 0x05 | 该CPU卡已禁用或挂失 |
| 0x06 | 该车牌号在系统中没有任何记录 |
| 0x07 | 该CPU卡内绑定车牌与系统不符，请重新进行CPU卡个性化定制 |
| 0x08 | 该标签未发行 |
| 0x09 | 该标签已禁用或挂失 |
| 0x0A | 未经过车辆信息的比对检查，请重新进行标签个性化定制 |
| 0x0B | 车辆信息比对失败，请重新进行标签个性化定制 |
| 0x0C | 系统信息比对失败，请重新进行标签个性化定制 |
| 0x0D | 查询失败，未找到相应匹配记录 |
| 0x0E | 该标签合同序列号与卡号绑定关系不符 |
| 0x0F | 交易信息上传失败 |
| 0x10 | 有交易信息未上传 |

### 7.3.4 交易流程

#### 7.3.4.1 机卡联合认证交易流程

描述了手持式初始化设备在进行机卡联合认证操作时的交易流程，见图 14.主要流程如下：

a) 在管理员卡的 1001 目录下使用 Get Challenge 指令获取随机数；
b) 终端向前置机发送“挑战帧”，包含管理员卡生成的随机数；
c) 前置机记录终端上送的“挑战帧”，并生成随机数；
d) 前置机向终端发送挑战帧，包含前置机生成的随机数；
e) 终端计算身份认证码；
f) 终端向前置机发送“认证信息帧”，包含身份认证码等信息；
g) 前置机使用身份认证码生成算法重新计算终端上送的身份认证码，并比对；
h) 前置机计算身份认证码；
i) 步骤七比对成功后，前置机生成会话密钥并保存。
j) 前置机向终端发送“响应认证信息帧”，包含终前置机生成的身份认证码；
k) 终端使用身份认证码生成算法重新计算前置机返回的身份认证码，并比对；
l) 比对成功后，终端生成会话密钥并保存。

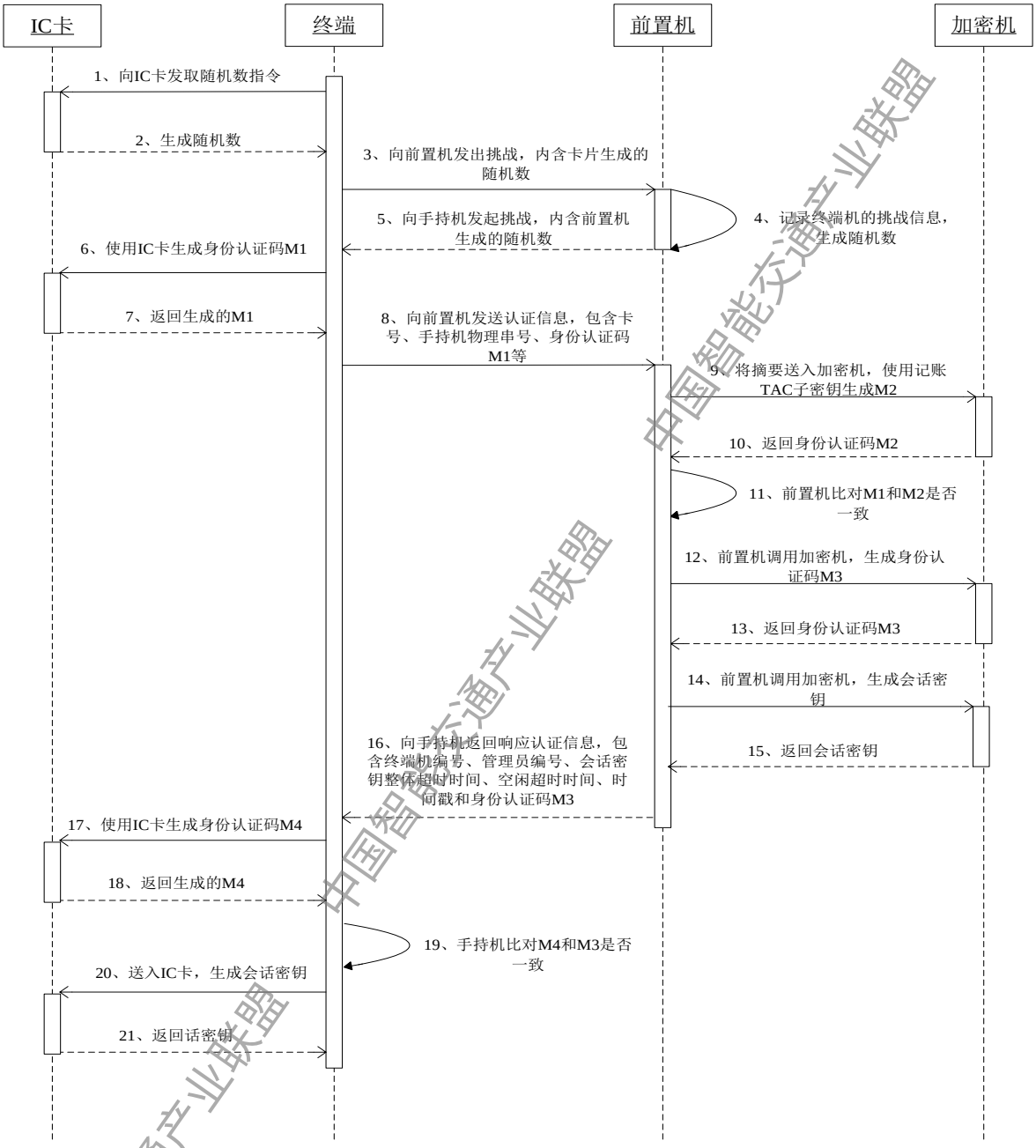



**图 14　机卡联合认证交易流程**

### 7.3.4.2 OBU 初始化交易流程

描述了手持式初始化设备在进行 OBU 初始化操作时的交易流程，见图 15。主要流程如下：

a) 终端获取 OBU 合同序列号、国标 CPU 卡号，同时在 OBU 的根目录下使用 ESAM 的 Get Challenge 指令获取随机数，用于下一步替换 OBU 系统主控密钥时计算 MAC；

b) 终端向前置机发送“OBU 替换密钥请求帧”，请求替换系统主控密钥；

c) 前置机根据收到的信息使用加密机计算 MAC，生成写系统主控密钥的 KeyData.

d) 前置机向终端发送“OBU 替换密钥响应帧”，包含替换密钥的指令；

e) 终端通过 TransferChannel 服务更新 OBU 中的系统主控密钥；

f) 重复以上操作，更新系统维护密钥、高速公路 ETC 应用主控密钥、高速公路 ETC 应用维护密钥、高速公路 ETC 应用认证密钥、高速公路 ETC 应用加密密钥、MLFF 应用主控密钥、MLFF 应用维护密钥、MLFF 应用访问密钥、MLFF 应用鉴别密钥、MLFF 应用加密密钥等；

g) 终端向前置机发送“OBU 文件信息初始化请求帧”，请求初始化系统信息文件；

h) 前置机根据收到的信息使用加密机计算 MAC，生成写系统信息文件的指令；

i) 前置机向终端发送“OBU 文件信息初始化响应帧”，包含写系统信息文件的指令；

j) 终端通过 TransferChannel 服务更新 OBU 中的系统信息文件；

k) 重复以上操作，更新车辆信息文件。

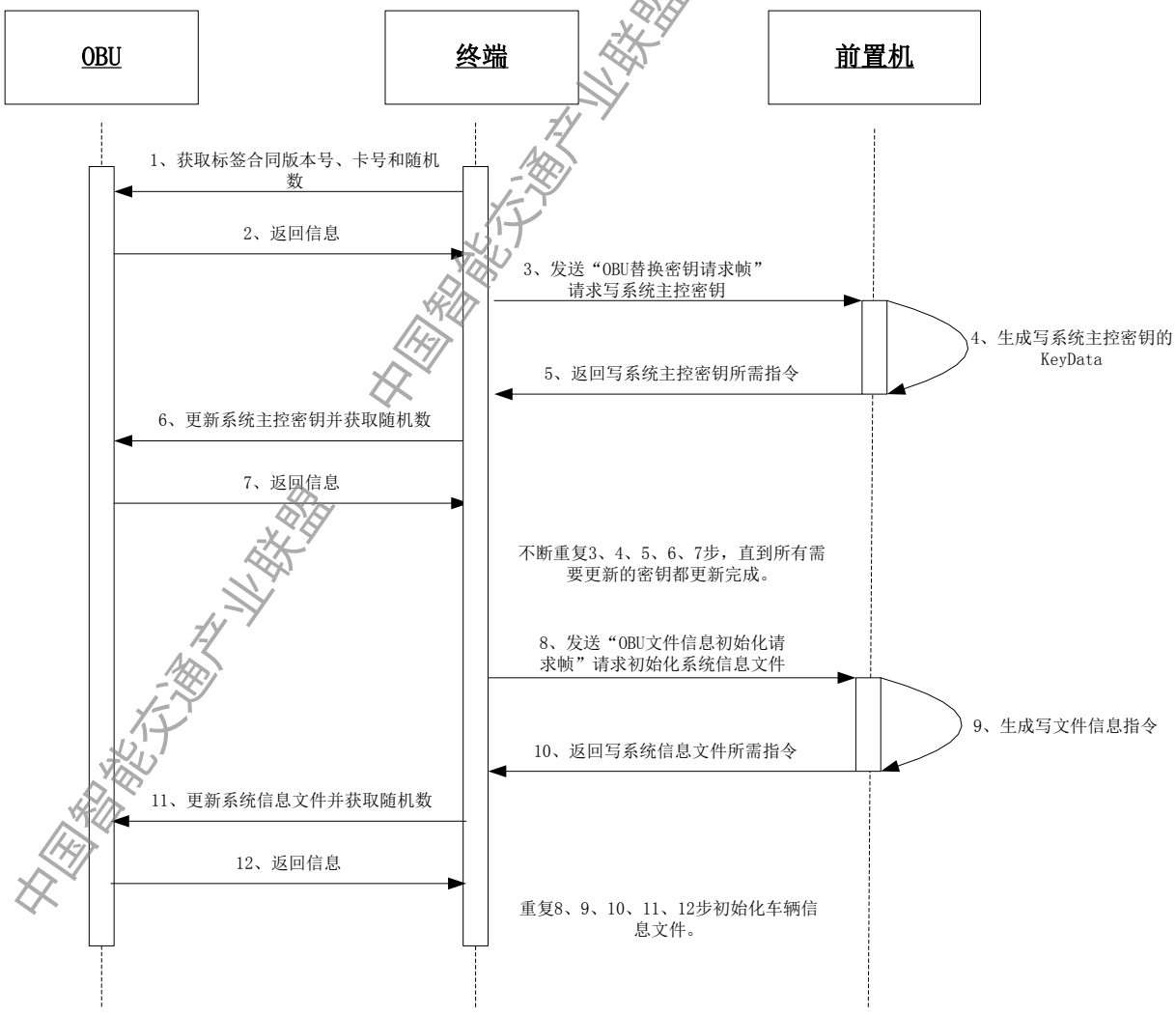



图 15　OBU 初始化交易流程

#### 7.3.4.3 OBU 个人化交易流程

描述了手持式初始化设备在进行 OBU 个人化操作时的交易流程，见图 16 主要流程如下：

a) 终端获取 OBU 合同序列号、国标 CPU 卡号，同时在 OBU 的 DF01 目录下使用 ESAM 的 Get Challenge 指令获取随机数，用于下一步写 OBU 车辆信息文件时计算 MAC；

b) 终端向前置机发送“OBU 写车辆信息请求帧”，包含 OBU 合同序列号，卡号、写车辆信息使用的随机数等信息；

c) 前置机根据业务规则判断上送的信息是否合法，并查找相应的车辆信息，使用终端上送的随机数计算写车辆信息使用的 MAC，并拼装写车辆信息文件需要使用的 ESAM 指令。同时，重新生成“交易随机数”，作为每笔交易的唯一标记，终端在之后上送的数据帧中都应该携带该随机数，表明为同一笔交易（在同一天内，反复生成的“交易随机数”不会重复）。同一笔交易该随机数相同，不同的交易该随机数不同。同时，该随机数也在终端读取车辆信息时参与使用，用于生成车辆信息的密文；

d) 前置机向终端发送“OBU 写车辆信息应答帧”，包含应答返回码、写车辆信息的 ESAM 指令以及“交易随机数”等信息；

e) 终端判断应答返回码，判断是否可以写 OBU 的车辆信息，只有返回码为 0x00 时，终端使用接收到的 ESAM 指令写 OBU 的车辆信息文件。其它返回码则进入异常处理流程；

f) 使用前置机返回的“交易随机数”读取 OBU 车辆信息文件，OBU 返回读取到的车辆信息文件密文；

g) 在 OBU 的根目录下使用 ESAM 的 Get Challenge 指令获取随机数，用于下一步写 OBU 系统信息文件时计算 MAC；

h) 终端向前置机发送“OBU 写系统信息请求帧”，包含读取到的车辆信息密文，写 OBU 系统信息需要用到的随机数，以及从前置机获取的“交易随机数”等信息；

i) 前置机先判断“交易随机数”，判断之前是否比对过车辆信息，比对过则继续，没有比对过则使用“交易随机数”解密上送的车辆信息密文后进行比对。只有比对通过，才使用上送的写系统信息随机数计算 MAC，并拼装相应的 ESAM 指令。比对失败则返回指定的应答返回码；

j) 前置机向终端发送“OBU 写系统信息应答帧”，包含应答返回码、写 OBU 系统信息需要使用的 ESAM 指令等信息；

k) 终端判断应答返回码，只有返回码表示处理成功时，终端使用接收到的 ESAM 指令写 OBU 的系统信息文件。其它返回码则进入异常处理流程；

l) 终端重新读取 OBU 的系统信息，以确保系统信息更新成功；

m) 终端向前置机发送“OBU 系统信息比对请求帧”，包含读取到的 OBU 系统信息，以

及从前置机获取的“交易随机数”等信息；

n) 前置机先判断“交易随机数”在系统中是否有记录，并比对上送的 OBU 系统信息和系统中记录是否一致。比对失败则返回指定的应答返回码；

o) 前置机向终端发送“OBU 系统信息比对应答帧”，包含应答返回码等信息。

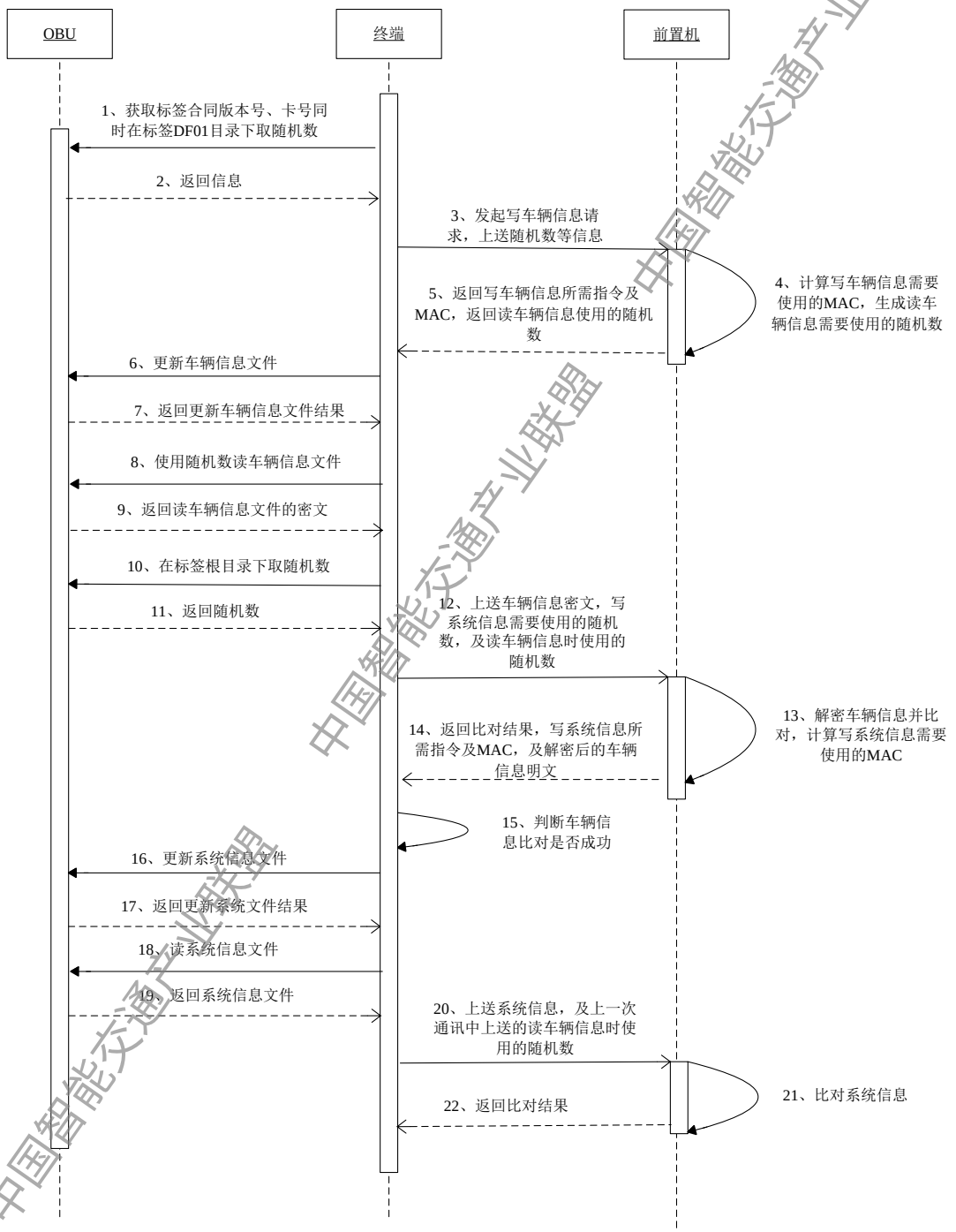





图 16　OBU 个人化交易流程

#### 7.3.4.4 OBU 写系统信息交易流程

描述了手持式初始化设备在进行 OBU 写系统信息操作时的交易流程，见图 17 主要流程如下：

a) 终端获取 OBU 合同序列号；
b) 终端向前置机发送“OBU 读车辆信息请求帧”；
c) 前置机判断该 OBU 是否发行，并生成“交易随机数”，作为每笔交易的唯一标记，终端在之后上送的数据帧中都应该携带该随机数，表明为同一笔交易。同一笔交易该随机数相同，不同的交易该随机数不同。同时，该随机数也在终端读取车辆信息时参与使用，用于生成车辆信息的密文；
d) 前置机向终端发送“OBU 读车辆信息应答帧”，包含应答返回码、“交易随机数”等信息；
e) 终端判断应答返回码，判断是否可以继续交易流程，只有返回码为表示处理成功时，终端才继续进行交易。其它返回码则进入异常处理流程；
f) 使用前置机返回的“交易随机数”读取 OBU 车辆信息文件，OBU 返回读取到的车辆信息文件密文；
g) 在 OBU 的根目录下使用 ESAM 的 Get Challenge 指令获取随机数，用于下一步写 OBU 系统信息文件时计算 MAC；
h) 终端向前置机发送“OBU 写系统信息请求帧”，包含读取到的车辆信息密文，写 OBU 系统信息需要用到的随机数，以及从前置机获取的“交易随机数”等信息；
i) 前置机先判断“交易随机数”在系统中是否有记录，并判断该 OBU 之前是否比对过车辆信息，如果没有则使用“交易随机数”解密终端上送的车辆信息密文，得到车辆信息明文后和系统记录的进行比对；如果该 OBU 的车辆信息已经比对过则忽略上送的车辆信息密文。只有比对通过，才使用上送的写系统信息随机数计算 MAC，并拼装相应的 ESAM 指令。比对失败则返回指定的应答返回码；
j) 前置机向终端发送“OBU 写系统信息应答帧”，包含应答返回码、写 OBU 系统信息需要使用的 ESAM 指令等信息；
k) 终端判断应答返回码，只有返回码表示处理成功时，终端使用接收到的 ESAM 指令写 OBU 的系统信息文件。其它返回码则进入异常处理流程，可终止交易或者重新发起该交易，必要时可发起个性化定制交易。如果超时，重新发起该交易；
l) 终端重新读取 OBU 的系统信息，以确保系统信息更新成功；
m) 终端向前置机发送“OBU 系统信息比对请求帧”，包含读取到的 OBU 系统信息，以及从前置机获取的“交易随机数”等信息；
n) 前置机先判断“交易随机数”在系统中是否有记录，并比对上送的 OBU 系统信息和

系统中记录是否一致。比对失败则返回指定的应答返回码；

o) 前置机向终端发送“OBU 系统信息比对应答帧”，包含应答返回码等信息。

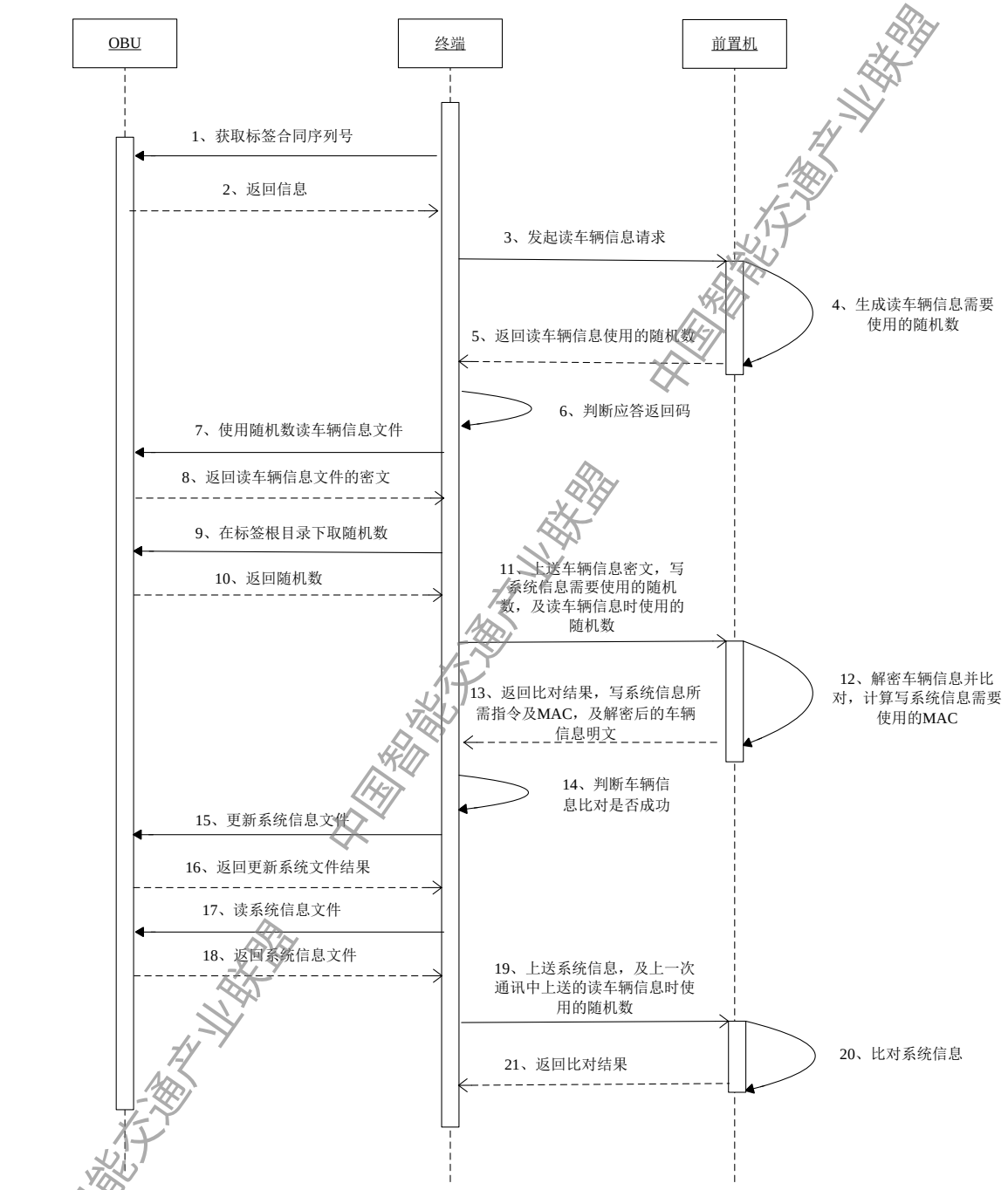





图 17　OBU 写系统信息交易流程

### 7.3.4.5 后台信息查询交易流程

描述了手持式初始化设备在进行后台信息查询操作时的交易流程，见图 18 主要流程如下：

a) 终端获取 OBU 合同序列号、合同版本号及国标 CPU 卡号；

b) 终端向前置机发起信息查询请求，请求帧中上传从 OBU 获取到的信息；

c) 前置机根据 OBU 合同序列号查询信息，并返回终端显示在界面上。

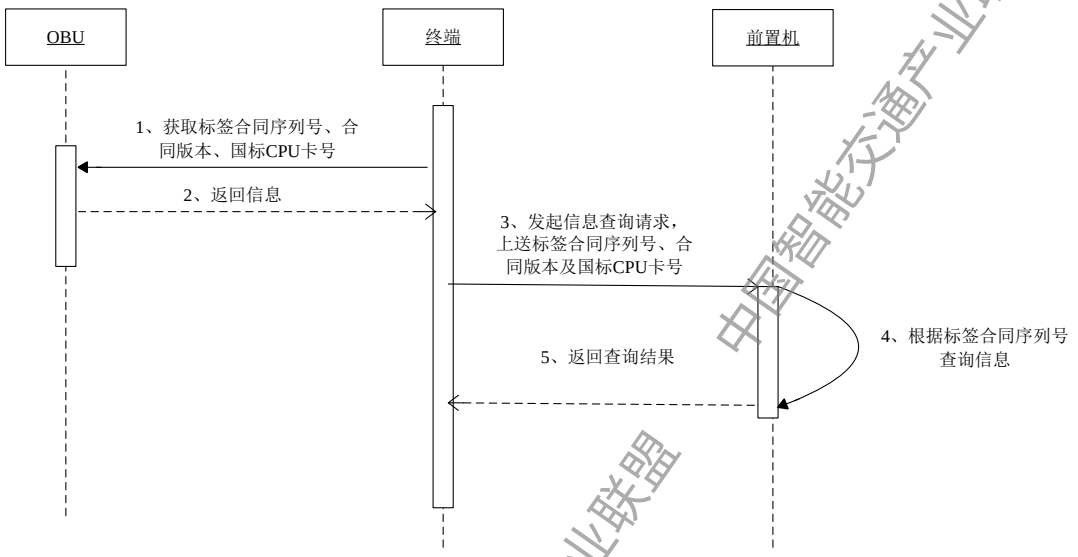



图 18　后台信息查询交易流程

### 7.3.4.6 交易信息上传

描述了手持式初始化设备在进行交易信息上传操作时的交易流程，见图 19 主要流程如下：

a) 终端读取存储的交易信息，并通过“交易信息上传帧”逐条上传信息；

b) 前置机记录交易信息，并更新信息；

c) 前置机返回“交易信息上传应答帧”，明确告知终端上送信息是否成功；

d) 终端判断返回码；

e) 不断重复步骤一到步骤四，直至所有交易信息均上传成功。

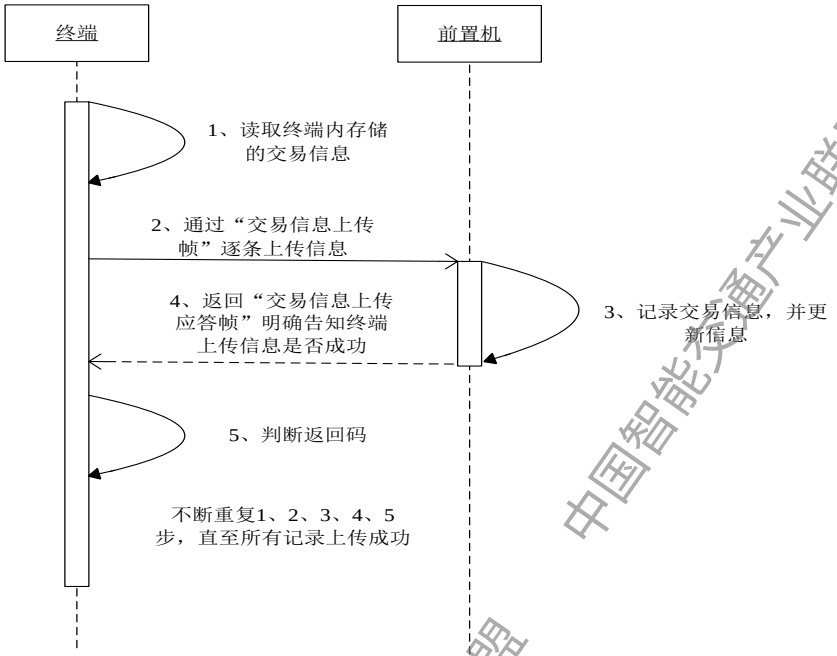



图 19　交易信息上传交易流程

#### 7.3.4.7 激活流程

- 联机激活流程

联机激活采用“OBU 写系统信息流程”完成 OBU 防拆复位和延长有效期业务。

- 脱机激活流程

脱机激活流程与台式初始化设备的“OBU 激活”操作流程一致。

#### 7.3.4.8 检测流程

- 联机检测流程

联机检测采用“OBU 写系统信息流程”完成 OBU 检测。

- 脱机检测流程

脱机检测流程与台式初始化设备的“系统信息读取”和“车辆信息读取”操作流程一致。

#### 7.3.4.9 汽车电子标识写入流程

描述了手持式初始化设备在进行汽车电子标识写入操作时的交易流程，见图。主要流程如下：

a) 终端获取 OBU 合同序列号、合同版本号、及国标 CPU 卡号及 AEI 应用目录下的随机

数；

b) 终端向前置机发起汽车电子标识写入请求，请求帧中上传从 OBU 获取到的信息；

c) 前置机计算写汽车电子标识需要的 MAC；

d) 前置机向终端返回“汽车电子标识写入响应帧”，包含写汽车电子标识文件的指令；

e) 终端通过 TransferChannel 服务更新 OBU 汽车电子标识文件。

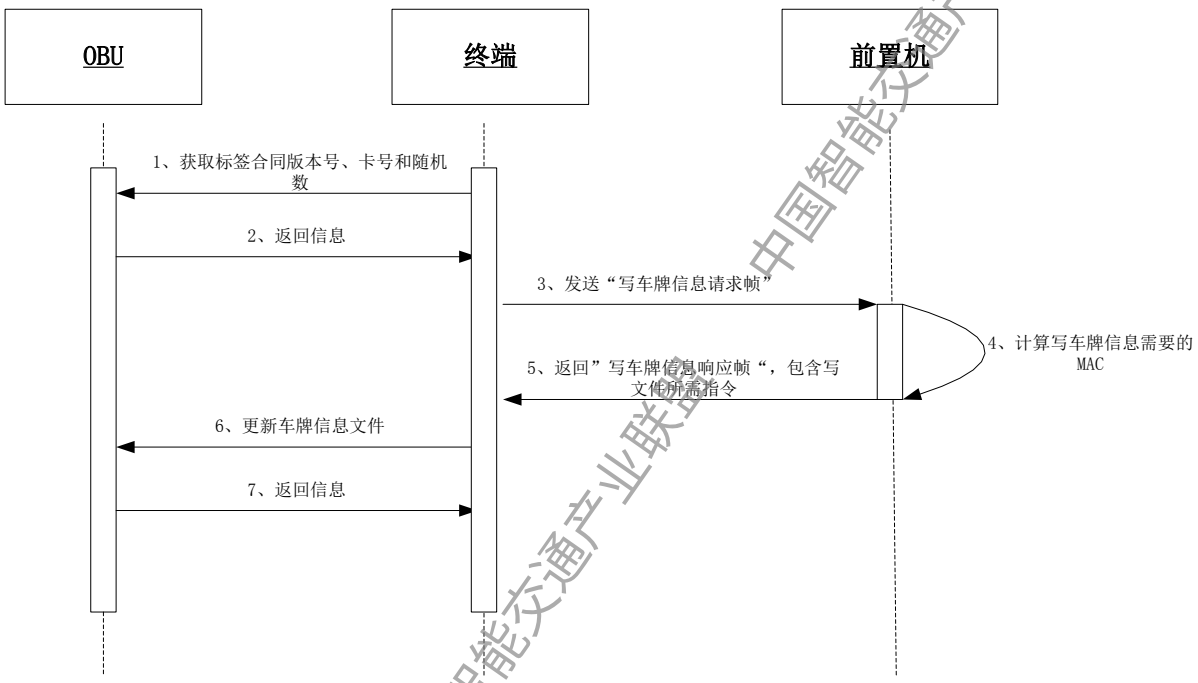



图 20 汽车电子标识写入交易流程

### 7.3.4.10 汽车电子标识稽查流程

描述了手持式初始化设备在进行汽车电子标识稽查操作时的交易流程，见图主要流程如下：

a) 终端获取 OBU 合同序列号、合同版本号、及国标 CPU 卡号；

b) 终端获取 OBU 中 AEI 目录下的汽车电子标识信息；

c) 终端向前置机发送“汽车电子标识比对请求帧”；

d) 前置机比对服务器中的汽车电子标识信息，确定汽车电子标识信息的正确性；

e) 前置机向终端发送“汽车电子标识比对应答帧”给终端，包含应答返回码等信息。

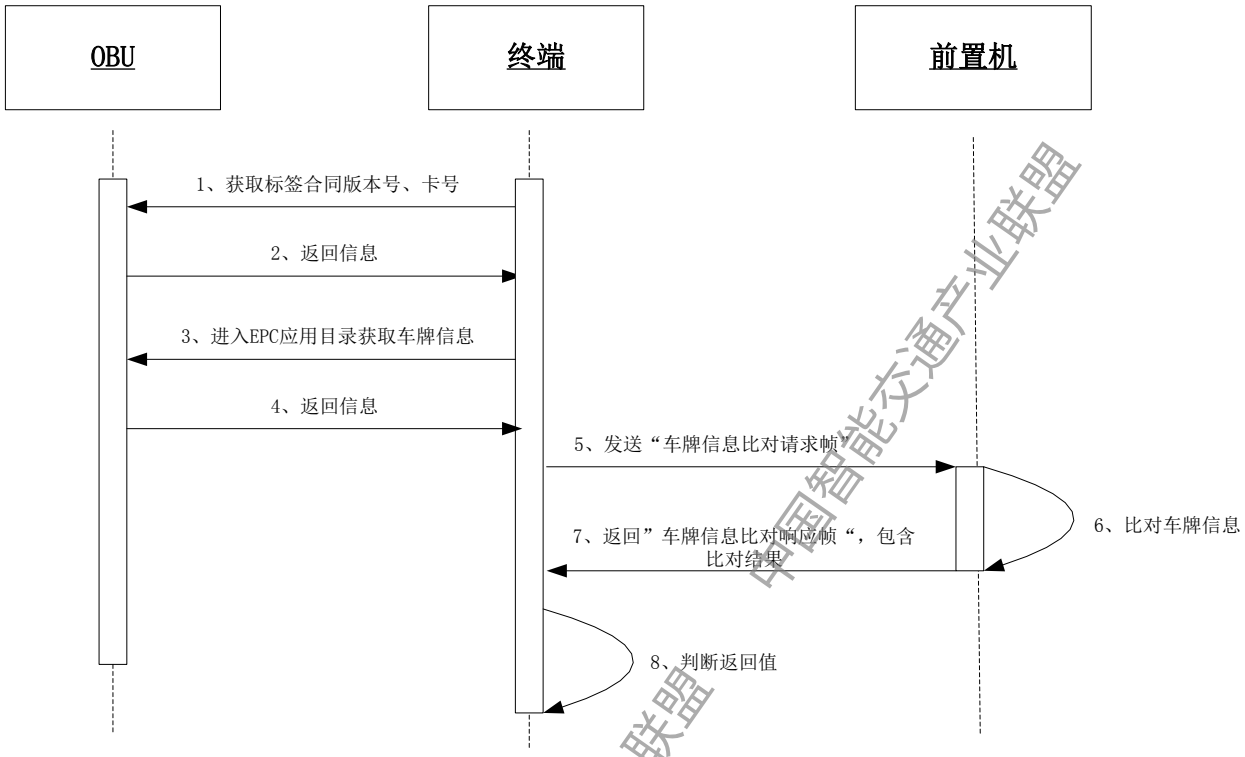



图 21　汽车电子标识稽查交易流程

### 7.3.4.11 电子年票写入流程

描述了手持式初始化设备在进行电子年票写入操作时的交易流程，见图.主要流程如下：

a) 终端获取 OBU 合同序列号、合同版本号、及国标 CPU 卡号及 EAT 应用目录下的随机数；

b) 终端向前置机发起电子年票写入请求，请求帧中上传从 OBU 获取到的信息；

c) 前置机计算写电子年票需要的 MAC；

d) 前置机向终端返回“电子年票写入响应帧”，包含写电子年票文件的指令；

e) 终端通过 TransferChannel 服务更新 OBU 电子年票文件。

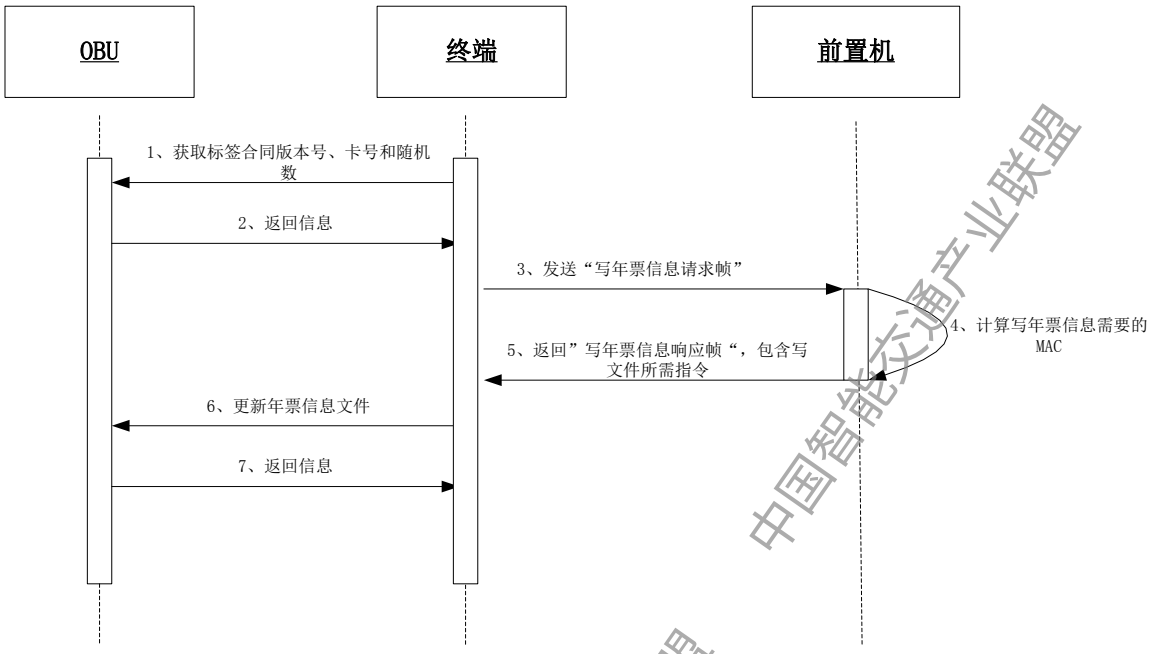



图 22　电子年票写入交易流程

### 7.3.4.12电子年票稽查流程

描述了手持式初始化设备在进行电子年票稽查操作时的交易流程，见图.主要流程如下：

a) 终端获取 OBU 合同序列号、合同版本号、及国标 CPU 卡号；

b) 终端获取 OBU 中 EAT 目录下的电子年票信息；

c) 终端向前置机发送“电子年票比对请求帧”；

d) 前置机比对服务器中的电子年票信息，确定电子年票信息的正确性；

e) 前置机向终端发送“电子年票比对应答帧”给终端，包含应答返回码等信息。

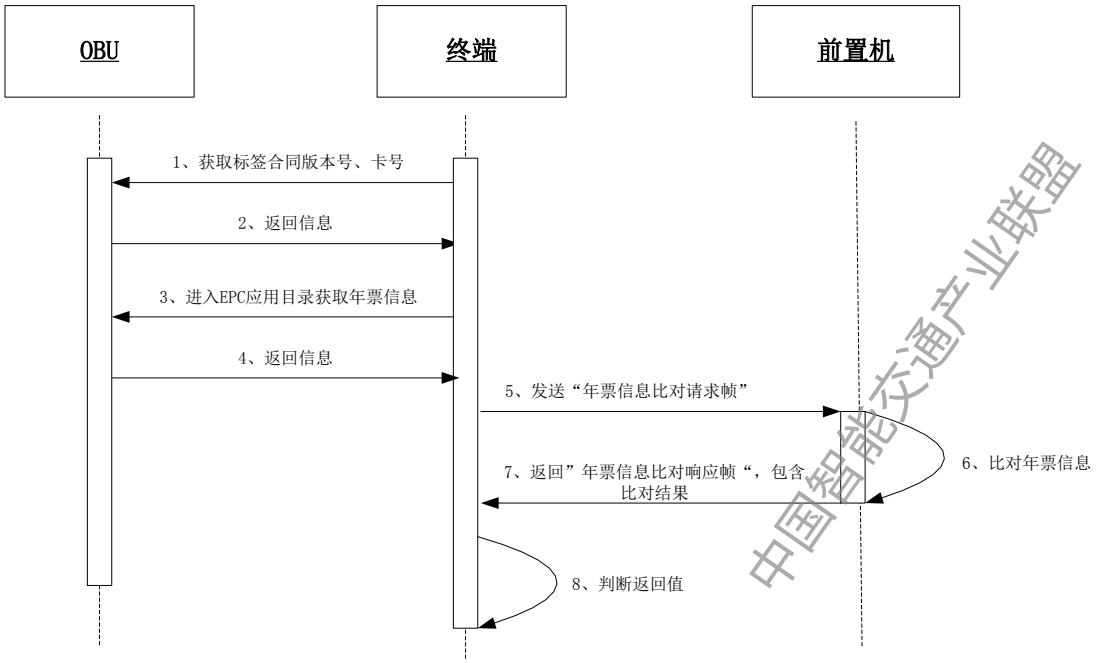



图 23　电子年票稽查交易流程

### 7.3.4.13 照片上传流程

考虑到图片适宜单独用二进制编码传输，图片上传分两步完成：先传关键的基本信息，再传图片，交易流程见图。

照片关键基本信息包含该笔业务的标签合同序列号、车牌号、车牌颜色等信息，具体见 JSON 编码 key 值表。

基本信息需要计算指纹码，计算方法见 7.4.6 节。

表 52　JSON 编码 key 值表

| 字段名 | Key | ValueType |
|---|---|---|
| 合同序列号 | ContractSerialNo | char(16) |
| 车牌号 | VehiclAEIlateNo | varchar(24) |
| 车牌颜色 | VehiclAEIlateColor | short |
| 终端机编号 | PosID | ulong |
| 管理员编号 | AdmID | int |
| 终端交易序号 | PosTSN | uint |
| 交易日期 | TransTime | DateTime |
| 定位信息 | LocationInfo | Locationtype |
| 指纹码 | FingerPrint | char(32) |

其中，定位信息字段的类型为复合型，格式如下表：

表 53　定位信息格式

| 定位信息 | key | valueType |
|---|---|---|
| 经度 | Longitude | varchar(10) |
| 纬度 | Latitude | varchar(10) |
| 扩展信息 | ExtendInfo | varchar(10) |

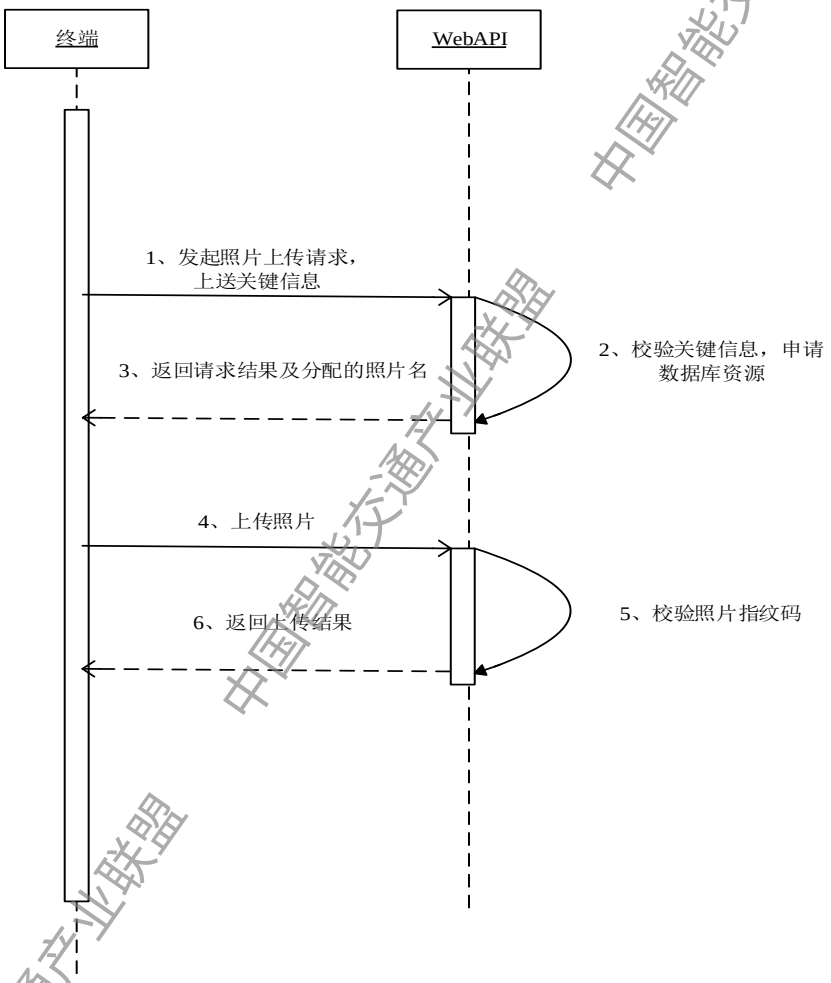



图 24　照片上传交易流程

### 7.3.4.14PSAM 卡认证流程

描述了手持式初始化设备在进行 PSAM 卡认证操作时的交易流程，见图 18，主要流程如下：

a) 终端读取 PSAM 卡的卡号；

b) 终端向前置机发送“PSAM 卡认证请求帧”；

c) 前置机比对 PSAM 的黑白名单，确定需认证的 PSAM 卡是否有效；

d) 前置机向终端发送“PSAM 卡认证应答帧”给终端，包含应答返回码等信息。

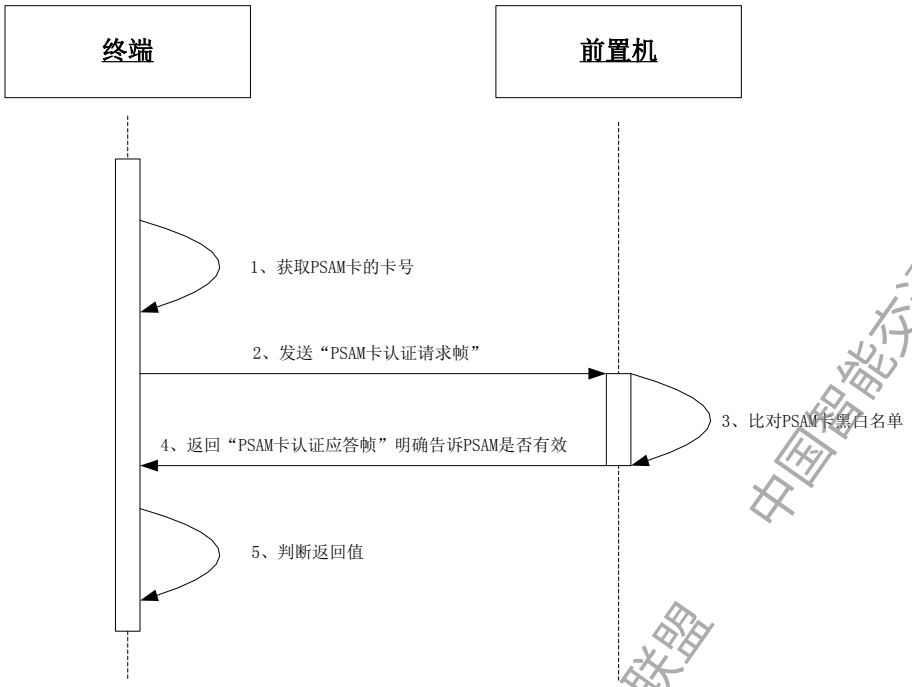



图 25　PSAM 卡认证交易流程

### 7.3.4.15 认证信息注销流程

描述了手持式初始化设备在进行认证信息注销操作时的交易流程，见图.主要流程如下：

a) 终端读取最后一笔交易的终端交易序号；

b) 向前置机发送“注销认证信息请求帧”，附带最后一笔交易的终端交易序号及日期；

c) 前置机检查当日交易信息是否全部上送，并置会话密钥失效；

d) 前置机返回“注销认证信息应答帧”，明确告知终端是否允许退出，是否有交易记录没有上传；

e) 终端判断返回码，注销认证信息。

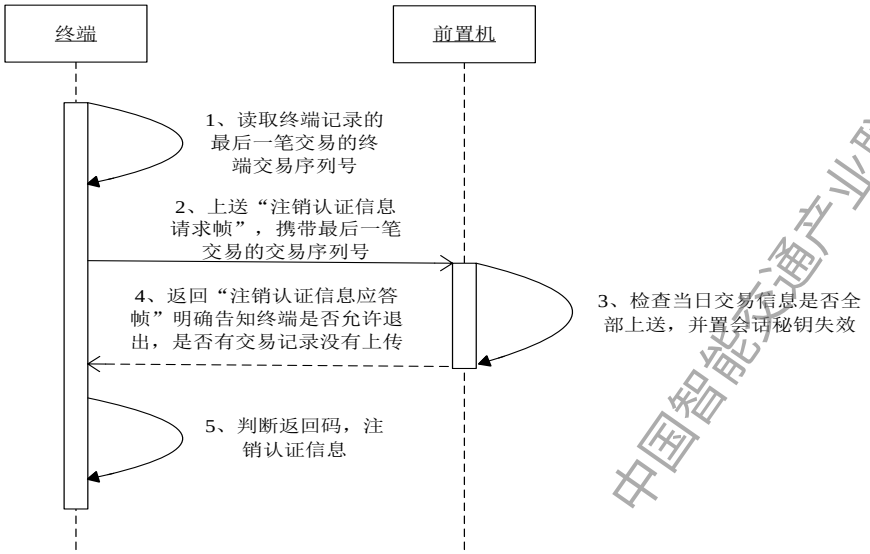



图 26　认证信息注销交易流程

### 7.3.5 异常处理

#### 7.3.5.1 崩溃恢复

- 软崩溃

终端必须将交易中间过程记录在非易失性存储器内。在交易记录未丢失的前提下，终端崩溃重启之后，首先进行机卡联合认证，之后应从最后一条未完成的交易开始重试。

- 硬崩溃

如果交易记录丢失无法恢复重试，必须要求进行报修等人工干预，最大可能地降低交易记录丢失风险。

### 7.3.6 超时处理

#### 7.3.6.1 超时总则

标签发行交易对整体超时时间不做要求，只对单步超时做时间限制。由于写 OBU 车辆信息和写 OBU 系统信息属于幂等性操作，原则上单步超时时允许重新发送数据帧。

#### 7.3.6.2 单步超时的分类

针对单步超时，根据通信双方的不同，分为两种：

- 标签和终端 DSRC 通信的超时；

- 终端和前置机请求-应答往返超时。

#### 7.3.6.3 超时的判别标准

单步超时后终端重复发送信息三次，依然超时无响应，视为整体超时；

从终端向 OBU 发出命令开始，到终端收到 OBU 处理命令的返回值，单步超时限定为100ms。超过 100ms，判定为单步超时。

从终端向前置机发出请求开始，到终端接收到前置机的应答，单步超时限定为 30s。超过30s，判定为单步超时。

#### 7.3.6.4 超时的处理策略

整体超时处理策略

- 在 OBU 成功写车辆信息之前发生整体超时则需要终止本次交易，并人工重新发起OBU 个性化定制交易。
- 在 OBU 成功写车辆信息之后发生整体超时，可自动发起 OBU 写系统信息交易流程补写 OBU 的系统信息，或者人工重新发起当此交易。

#### 7.3.6.5 单步超时处理策略

- OBU 和终端 DSRC 通信超时，最多重试三次发送 DSRC 指令，直到 OBU 回复响应信息。三次后依然无响应，视为整体超时，转入整体超时处理流程；
- 终端和前置机请求-应答往返超时，最多重试三次发送相同的数据帧，直到收到前置机的应答帧。三次后依然无响应，视为整体超时，转入整体超时处理流程；

#### 7.3.6.6 OBU 掉电

OBU 在交易过程中掉电，是由于系统交易时间过长而引起。会引起 DSRC 通信的单步超时或返回异常信息。OBU 掉电后执行各项 ESAM 指令会失败，尤其是写文件指令。在得到OBU 明确返回 ESAM 指令执行失败后，可视为系统交易整体超时，其处理策略可与整体超时处理策略保持一致。

### 7.4 应用安全

#### 7.4.1 安全方式

主要安全保护手段有：

a) 身份认证：发行控制系统与初始化设备通信需互相通过身份认证后才可进行；

b) 加密保护：在传输过程中对数据进行加密；

c) 数字签名：对脱机交易数据进行数字签名。

### 7.4.2 身份认证

身份认证指初始化设备和发行控制系统之间相互验证，以身份认证码的方式实现。身份认证见图 26。身份认证码产生过程如下：

a) 被验证的一方，根据具体帧的要求拼装数据，组成用于计算身份认证码的明文；

b) 将送入的明文字符串使用 SHA1 算法得到 20 字节的摘要(Digest)码；

c) 截取摘要（Digest）码的前 16 个字节；

d) 使用国标 CPU 卡的记账 TAC 子密钥，对这 16 字节数据做 MAC 计算，得到 4 字节 MAC。初始化设备由管理员卡计算，PC 端由加密机计算；

e) 将该 4 字节 MAC 重复 4 次，即最终的 16 字节身份认证码。

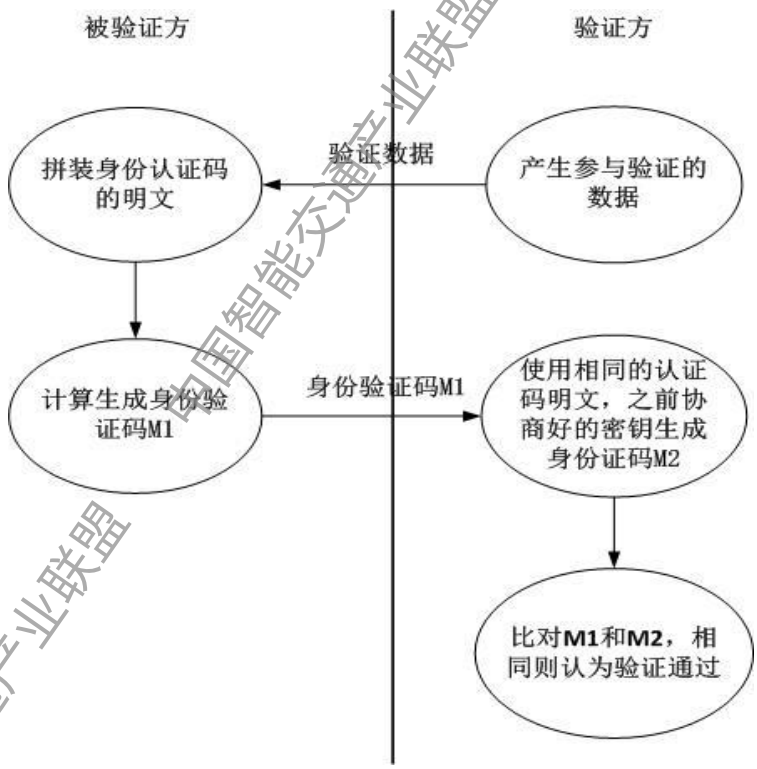



图 26　身份认证

### 7.4.3 会话加密

初始化设备和发行控制系统每一次通信都需要对数据进行加密，保证会话过程中所发送数据帧的真实性及完整性。会话加密以会话密钥和指纹码的方式实现。会话密钥的产生过程如下：

a)　将如下字段按顺序排列，生成长度为 24 字节的数据；

表 54

| 序号 | 名称 | 长度(Byte) |
|---|---|---|
| 1 | 发行控制系统随机数 | 4 |
| 2 | 发行控制系统时间戳 | 8 |
| 3 | 初始化设备随机数 | 4 |
| 4 | 初始化设备时间戳 | 8 |

b) 对拼接的 24 字节数据使用 SHA1 算法得到 20 字节的摘要(Digest)码；

c) 截取摘要（Digest）码的前 16 个字节；

d) 使用国标 CPU 卡的记账 TAC 子密钥，对这 16 字节数据做 MAC 计算，得到 4 字节 MAC；

e) 依次将摘要码的第 17 到第 20 字节取代第 1 到第 4 字节，依照步骤 d 相同的做法，生成第二组到第五组 4 字节 MAC；

f) 将上述 5 组 4 个字节数按顺序串接起来，得到 160 位的会话密钥。

### 7.4.4 指纹码

使用机卡联合认证之后得到的 160 位（bit）会话密钥对整个数据帧（包含指纹码和扩充信息在内）进行 HMAC_SHA1 运算，截取前 16 个字节即指纹码，回填数据帧的指纹码字段即可。

### 7.4.5 数字签名

初始化设备对脱机交易信息需要进行数字签名。数字签名过程如下：

a) 使用机卡联合认证后产生的会话密钥对“交易信息上传帧”进行 HMAC_SHA1 运算，生成 20 字节加密数据，步骤一计算方法与指纹码生成方法一致，只是不需要截取数据；

b) 在 20 字节加密数据后添加 4 字节数据“0x80000000”,组成 24 字节数据；

c) 使用管理员卡的记账 TAC 子密钥，对这 24 字节数据做 MAC 计算，得到 4 字节 MAC；

d) 将该 4 字节 MAC 重复 4 次，即最终的 16 字节数字签名。

### 7.4.6 照片信息加密

初始化设备对上传的照片信息需要进行安全计算，计算方法如下：

a) 使用 SHA1 算法对图片的二进制数据进行散列运算，得到 20 字节的摘要码，该摘要码进行 Base64 编码后，填写到基本信息中约定的字符串字段；

b) 对基本信息进行 JSON 编码，去除无意义的 White space，用 UTF-8 编码转为字节流；

c) 用会话密钥对字节流做 HMAC_SHA1 运算，获得的 20 个字节即为基本信息的指纹码；

d) 基本信息 JSON 编码作为 POST 操作的内容，上述 20 字节指纹码用 Base64 编码转换为字符串作为 POST 操作的 fingerprint 参数，传递给指定的后台服务地址。

## 8 环境与电磁兼容

### 8.1 环境

环境条件应符合：

a） 防护等级：IP67（可防尘；可防淋水）。参照《GB 4208-2008 外壳防护等级(IP 代码》

b） 跌落：不带包装，高度 1 米，1 角 3 棱 6 面都要包括，符合 GB2423.8。

## 8.2 电磁兼容

ESD 抗静电：试验等级为 4 级，15 kV 空气放电，8 kV 接触放电。参照《GB/T 17626.2-2006 电磁兼容试验和测量技术 静电放电抗扰度试验》。

# 9 标志、包装、运输及贮存

## 9.1 标志

### 9.1.1 产品标志

在产品表面应标明产品名称、型号、序号、生产批号及制造日期、制造单位等标志。

### 9.1.2 包装标志

产品包装箱上应有产品名称、型号、制造单位、地址、出厂日期以及包装储运标志。其中包装储运图示标志应符合 GB/T 191-2008 的规定。

## 9.2 包装

产品应采用包装箱进行包装。包装箱应符合防振、防潮、防雨的要求。包装箱内应附有产品合格证、说明书和装箱单。产品使用说明书应符合 GB/T 9969-2008 的规定。产品合格证应符合 GB/T 14436—1993 的规定。

## 9.3 运输及贮存

a） 包装好的产品均应能承受汽车、火车、轮船和飞机等的运输；

b） 长途运输时不应装在敞开的船舱和车厢内，应注意防雨水、防尘埃和机械损伤，中途转运不应存在露天仓库中，在运输过程中不应与易燃、易腐蚀的物品同车运输；

c） 产品贮存应在符合 GB/T 4798.1—2005 气候环境条件内贮存，且空气中不得有对产品起腐蚀作用的有害物质。

# 附录 A

（规范性附录）

# 初始化设备的 ANS.1 型数据定义

## A.1 BST 中 OBU 初始化发行操作类型的标识

初始化设备所执行的各种 OBU 初始化发行操作的模式，可通过 BST 中 ApplicationList 内的 applicationParameter 进行指示。

国标 GB/T 20851.3-2007 中规定 BST 中的 applicationParameter 的类型定义为 ApplicationContextMark，其 ASN.1 定义如下：

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

本规范在国标 GB/T 20851.3-2007 的基础上规定，补充定义 OBU 初始化发行操作时 BST 中的 applicationParameter，其 ASN.1 定义为：

```
OBU-INIT-BSTApplicationContextMark ::= SEQUENCE {
        obuInitMode INTEGER (SIZE(0..127)),
        reservedInfo    Container     OPTIONAL
}
```

其中：

obuInitMode 用于指示初始化设备所执行的各种 OBU 初始化发行操作的类型。

reservedInfo 用于其他应用参数信息协商的扩展。

obuInitMode 的编码如表 A.1 所示：

表 A.1 obuInitMode 的编码

| ObuInitMode取值 | 初始化发行操作类型 |
|---|---|
| 0 | OBU初始化（密钥替换） |
| 1 | OBU系统信息更新 |
| 2 | OBU车辆信息更新 |
| 3 | ESAM信息读取 |
| 4 | OBU汽车电子标识信息更新 |
| 5 | OBU电子年票信息更新 |
| 其他 | 保留 |

## A.2 VST 中应携带的 OBU 初始化发行操作相关信息

OBU 应根据 BST 中 ObuInitMode 所指示的各种 OBU 初始化发行操作类型，来确定在其 VST 的 VSTApplicationContextMark 中所应携带的 OBU 初始化应用相关信息。

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 {
```

…,

esamResetInfo [80] ESAMResetInfo, --存放高速公路 ETC 应用 IC 卡的相关预读信息

…,

}

ESAMResetInfo 的 ASN.1 类型定义为：

```
ESAMResetInfo ::= SEQUENCE {
    idOfMOC          OCTETSTRING(SIZE(1)), --
    regIDOfESAM      OCTETSTRING(SIZE(2)), --芯片厂商注册标识
    regIDOfOBU       OCTETSTRING(SIZE(2)), --由 ITSC 分配
    versionOfCOS     OCTETSTRING(SIZE(1)), --主版本号+次版本号
    reVerOfCOS       OCTETSTRING(SIZE(1)), --
    year             OCTETSTRING(SIZE(1)), --生产年份
    month            OCTETSTRING(SIZE(1)), --生产月份
    day              OCTETSTRING(SIZE(1)), --生产日
    verOfESAMStruc   OCTETSTRING(SIZE(1)), --ESAM 结构版本号
    snOfESAM         OCTETSTRING(SIZE(4)), --ESAM 序列号
}
```

注：ESAMResetInfo 为 ESAM 复位信息中的历史字节所包含的内容。

VST 内 VSTApplicationContextMark 中应携带的 OBU 初始化发行操作相关信息与 BST 内 obuInitMode 所指示初始化设备初始化发行操作类型的对应关系如表 A.2 所示：

表 A.2 不同模式下 VST 中应携带的ＯＢＵ初始化操作相关信息,

| obuInitMode | VSTApplicationContextMark中应携带的信息 |
|---|---|
| 0 | sysInfo+rndOBU+esamResetInfo<br>其中：<br>rndOBU为从ESAM中取得的4字节随机数+“00000000”;<br>esamResetInfo占用VSTApplicationContextMark中可选项reservedInfo1的位置;<br>其他可选项不存在 |
| 1 | sysInfo+rndOBU+esamResetInfo<br>其中：<br>rndOBU为从ESAM中取得的4字节随机数+“00000000”;<br>esamResetInfo占用VSTApplicationContextMark中可选项reservedInfo1的位置;<br>其他可选项不存在 |

表 A.2 不同模式下 VST 中应携带的ＯＢＵ初始化操作相关信息(续)

| obuInitMode | VSTApplicationContextMark中应携带的信息 |
|---|---|
| 2 | sysInfo+rndOBU<br>其中：<br>rndOBU为从ESAM中取得的4字节随机数+“00000000”；<br>其他可选项不存在 |
| 3 | sysInfo+rndOBU<br>其中：<br>rndOBU为符合国家标准用于GetSecure的accessCredentials计算的8字节随机数；<br>其他可选项不存在 |
| 4 | sysInfo+rndOBU<br>其中：<br>rndOBU为从ESAM中取得的4字节随机数+“00000000”；<br>其他可选项不存在 |
| 5 | sysInfo+rndOBU<br>其中：<br>rndOBU为从ESAM中取得的4字节随机数+“00000000”<br>其他可选项不存在 |
| 其他 | —— |

# 附录 B

（规范性附录）

AEI 应用中的文件结构

## B.1 驾驶证信息文件

表 B.1 驾驶证信息文件

| 文件标识符 | 0012 | | |
|---|---|---|---|
| 文件类型 | 二进制文件 | | |
| 文件主体空间 | 120个字节 | | |
| 操作权限 | 读写需要身份认证，线路保护写 | | |
| 字节 | 数据元 | 长度 | 说明 |
| 1-9 | 证号 | 9 | IDCard |
| 10-19 | 姓名 | 10 | Name |
| 20 | 性别+准驾车型 | 1 | SexClass |
| 21-22 | 国籍 | 2 | Nationality |
| 23-26 | 出生日期 | 4 | Birthday |
| 27-30 | 初次领证日期 | 4 | IssueDay |
| 31-34 | 有效起始日期 | 4 | ValidFrom |
| 35 | 有效期限 | 1 | ValidFor |
| 36-41 | 档案编号 | 6 | FileNumber |
| 42-101 | 住址 | 60 | Address |
| 102-120 | 发证机关章 | 19 | Administer |
| 注：驾驶证信息文件存放在双界面 CPU 卡中的 AEI 应用目录（DF01）下。 | | | |

## B.2 行驶证信息文件

表 B.2 行驶证信息文件

| 文件标识符 | EF01 | | |
|---|---|---|---|
| 文件类型 | 二进制文件 | | |
| 文件主体空间 | 205个字节 | | |
| 操作权限 | 读写需要身份认证，线路保护写 | | |
| 字节 | 数据元 | 长度 | 说明 |
| 1-10 | 车牌号 | 10 | CarPlate |
| 11-12 | 车辆类型 | 2 | VehicleTypeID |
| 13 | 使用性质 | 1 | UseCharacter |
| 14-17 | 车辆品牌 | 4 | VehicleBrand |
| 18-34 | 车辆识别代号 | 17 | VIN |

表 B.2 行驶证信息文件（续）

| 文件标识符 | EF01 | | |
|---|---|---|---|
| 35-44 | 发动机号码 | 10 | EIN |
| 45-48 | 注册日期 | 4 | RegisterDate |
| 49-52 | 发证日期 | 4 | IssueDate |
| 53-60 | 档案编号 | 8 | FileNumber |
| 61 | 核定载人数 | 1 | Seats |
| 62-63 | 总质量 | 2 | GVM |
| 64-65 | 整备质量 | 2 | CurbWeight |
| 66-67 | 核定载质量 | 2 | CarringWeight |
| 68-73 | 外廓尺寸 | 6 | VehicleSize |
| 74-113 | 所有人 | 40 | CarOwner |
| 114-173 | 地址 | 60 | CarAddress |
| 174-175 | 准牵引总质量 | 2 | TowWeight |
| 176-205 | 发证机关章 | 30 | InsitutionSeal |
| 206-250 | 保留 | 45 | RFU |
| 注：行驶证信息文件存放在 ESAM 中的 AEI 应用目录（DF01）下。 | | | |

## B.3 车牌信息文件

表 B.3 车牌信息文件

| 文件标识符 | EF02 | | |
|---|---|---|---|
| 文件类型 | 二进制文件 | | |
| 文件主体空间 | 60个字节 | | |
| 操作权限 | 自由读，线路保护写 | | |
| 字节 | 数据元 | 长度 | 说明 |
| 1 | 车牌种类 | 1 | PlateType |
| 2-11 | 车牌号码 | 10 | CarPlate |
| 12 | 车牌颜色 | 1 | CarPlateColor |
| 13 | 车身颜色 | 1 | CarColor |
| 14 | 速度 | 1 | CarSpeed |
| 15 | 黄标车标识 | 1 | CarEnvFlag |
| 16-22 | 下次年检时间 | 7 | CarCheckNextTime |
| 23-24 | 生产厂商 | 2 | Manufacturer |
| 25-28 | 备用字段1 | 4 | |
| 29-32 | 备用字段2 | 4 | |
| 33-36 | 备用字段3 | 4 | |
| 37-40 | 备用字段4 | 4 | |
| 41-44 | 备用字段5 | 4 | |
| 45-48 | 备用字段6 | 4 | |
| 49-60 | 备用字段7 | 12 | |
| 注：行驶证信息文件存放在 ESAM 中的 AEI 应用目录（DF01）下。 | | | |

# 附录 C

（规范性附录）

EAT 应用中的文件结构

## C.1 年票信息文件

表 C.1 年票信息文件

| 文件标识符 | EF04 | | |
|---|---|---|---|
| 文件类型 | 二进制文件 | | |
| 文件主体空间 | 40个字节 | | |
| 操作权限 | 自由读，线路保护写 | | |
| 字节 | 数据元 | 长度 | 说明 |
| 1-10 | 车牌号码 | 10 | CarPlate |
| 11-14 | 有效开始日期 | 4 | SignedDate |
| 15-18 | 有效结束日期 | 4 | ExpiredDate |
| 19-40 | 备用字段 | 22 | |
| 注：年票信息文件存放在 ESAM 中的 EAT 应用目录（DF01）下 | | | |

T/ITS 0017-2014

中国智能交通产业联盟

标准

**电子收费 专用短程通信**

**支持扩展应用的关键设备：初始化设备**

T/ITS 0017-2014

北京市海淀区西土城路 8 号（100088）

中国智能交通产业联盟印刷

网址：http://www.c-its.org

2014年11月第一版　2014年11月第一次印刷