**乌鲁木齐市轨道交通工程**

**清分中心系统设备采购及系统集成项目**

**乌鲁木齐轨道交通HCE云端支付平台**

**技术方案**

**20170329v00.01**

| 版本号 | 日期 | 编写者 | 审核者 | 描述 |
| --- | --- | --- | --- | --- |
| 20170329v00.01 | 2017/3/29 | 杜小伟 |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. 前言 6

2. 参考 6

3. HCE技术简介 6

4. HCE云端支付系统 7

4.1. 系统概述 7

4.2. 系统的功能 8

4.2.1. 手机APP管理 8

4.2.2. 更新管理 8

4.2.3. 用户账户管理 9

4.2.4. 用户凭证管理 9

4.2.5. 交易安全管理 9

4.2.6. 交易结算处理 10

4.3. 手机APP端的功能 10

4.3.1. 用户注册 10

4.3.2. 用户登录 10

4.3.3. 密码修改 10

4.3.4. 资金来源绑定 10

4.3.5. 手机票生成 11

4.3.6. 手机票充值 11

4.3.7. 手机票消费 11

4.3.8. 密钥及关键数据存储 11

4.4. 云端支付业务划分 11

4.4.1. 手机用户注册、申请 11

4.4.2. 申请激活码 12

4.4.3. 云卡激活 12

4.4.4. 限制密钥更新 12

4.4.5. 风险参数设置 12

4.4.6. 云卡锁定 13

4.4.7. 云卡解锁 13

4.4.8. 云卡注销 13

4.4.9. 手机云卡在公共交通领域的消费交易 13

4.4.10. 重装应用和删除应用数据 13

4.4.11. 移动应用用户变更 13

4.4.12. 同一移动应用UserID 更换设备或新增设备 14

4.5. 系统可靠性及安全管理 14

4.5.1. 系统可靠性策略 14

4.5.2. 系统安全管理方案 14

4.6. 交易安全机制及防护 15

4.6.1. 交易数据的完整性。 15

4.6.2. 交易信息在传输过程中的保密性。 15

4.6.3. 交易的不可否认性。 16

4.6.4. 系统的风险监控和反制。 16

4.6.5. 客户端敏感数据安全 17

4.6.6. 云端支付系统CA子系统 17

4.7. 云卡业务应用流程 21

4.7.1. 应用场景 21

4.7.2. 注册 22

4.7.3. 云卡申请 22

4.7.4. 云卡激活 23

4.7.5. 云卡脱机消费 23

4.7.6. 对账 24

4.7.7. 移动应用 24

4.7.8. 支付组件 25

4.7.9. 支付插件 25

4.7.10. 账号申请 26

4.7.11. 凭证管理 26

4.7.12. 交易处理 27

4.7.13. 安全通信机制 27

4.7.14. 移动应用安全机制 28

4.7.15. 安全交易密钥存储及使用 28

5. 云卡在城市交通领域的应用分析 29

5.1. 城市交通云卡系统设计 29

5.1.1. 架构设计 29

5.1.2. 云卡设计 29

5.1.3. 方案安全性 31

5.2. 云卡的交易机具 31

# 前言

为了实现乌鲁木齐轨道交通自动售检票系统HCE手机云卡过闸， 本文主要介绍HCE云端支付技术的系统框架及手机模拟云卡的技术关键点，使AFC各系统开发者了解云卡系统的接入需求，及技术实现方案。

# 参考

《CJT 331-2010 城市公用事业互联互通卡通用技术要求》

《PBOC 第1部分(电子钱包卡片规范) 2005》

《PBOC 第2部分(电子钱包\_电子存折应用规范) 2010版》

# HCE技术简介

HCE （ host card emulation ） 是 Google 在 2013 年 年 底 发 布 的Android4.4(KitKat)版本中推出的新技术，中文名称是『主机卡模拟技术』。 基于该技术， VISA 和中国银联已先后发布了 HCE 云端支付技术规范，即用手机 APP软件模拟芯片卡的安全技术，实现银行卡发卡交易。HCE 的出现改变了传统的路由方式。卡模拟模式中的数据可以被路由到手机 APP 中所谓的 HCE 服务上，这就脱离了传统的 SE 芯片载体的限制，使得主机安装一个可以调用 HCE 服务的软件就能够作为 SE 存在，各类应用的卡密钥被存储在云端服务器（另外一种是本地终端模式，将密钥放在本地终端内，主要实现小额脱机支付），当交易进行时， Host CPU 将从云端调用相应密钥进行鉴权。目前在 HCE 的协议栈中已经实现了 ISO14443 和 ISO7816 的相应规范，能够支持常用的 NFC 卡模拟应用。

卡模拟关键技术在于密钥载体，在HCE技术之前有SWP-SD、SWP-SIM两种安全密钥的载体，但均是基于硬件的方式。在应用部署上需要对手机终端进行改造，使得用户体验变差。

为绕开密钥载体制约，满足应用发行方快速部署NFC应用/服务的需求，出现了基于主机卡模拟（HCE）的技术。由NFC控制器将智能卡指令数据通知到应用处理器（Application Processor），并由操作系统通知到制定的手机应用。相比于基于SE的卡模拟，通过主机卡模拟的方法，使得任何应用程序都可以模拟一个支付IC卡来与NFC读卡器直接通信。

基于HCE的移动支付模式相比于基于SE的移动支付模式具有如下优点：

* 不受SE发行方的控制
* HCE方案成本更低
* 解决卡片兼容性问题



# HCE云端支付系统

## 系统概述

云端支付系统的组成包括手机APP管理系统、账户管理系统、凭证管理系统、交易处理系统、安全管理系统、结算处理系统。系统组成如下图所示：

图1：系统组成框图

## 系统的功能

### 手机APP管理

#### 版本管理

手机APP连接网络后， APP 管理系统需要判断是否有新版本，用户风险控制参数文件是否过期，并提示用户更新。

#### 下载管理

APP 管理系统从安全管理系统获得安全密钥后，打包形成手机应用 APP。

打包好的 APP被 APP管理平台上载至 APP下载平台，供需要使用 HCE云支付应用的用户下载使用。

### 更新管理

APP管理系统管理APP版本，风险控制参数文件版本，做好版本的迭代处理。用户更新时，只需下载最新更新包。

### 用户账户管理

在用户使用 HCE云支付应用前，需通过手机已安装好的 HCE云支付 APP，向 HCE云支付业务系统申请云支付帐户。

HCE 云支付业务系统审核用户申请。申请审核通过后，向结算系统提交云端帐户建立请求。

HCE 云支付业务系统在结算系统建立云端帐户后，将云端帐户信息提交凭证系统，凭证系统建立手机帐户，并建立云端帐户和手机帐户的对应关系。凭证系统建立手机帐户的同时，向安全系统提交凭证信息，并从安全系统获得手机帐户的认证数据和钱包数据。

HCE云支付业务系统在凭证系统完成手机帐户构建后，向用户手机的 HCE云支付 APP回送手机帐户信息， APP在手机上建立手机帐户。

HCE云支付在用户账户构建完成后，在正常使用过程中将监控账户使用状态，发现用户交易异常，将建立账户黑名单管理，通过名单管理保证手机账户的资金安全。

### 用户凭证管理

凭证系统为每次手机帐户申请，独立形成一个系统唯一的凭证。该凭证具有其对应唯一的非对称认证密钥和对称计算密钥。

同一时间，系统内仅有唯一一个凭证所标识的手机帐户与唯一一个云端帐户对应。

### 交易安全管理

在手机帐户的认证上，系统采用非对称的安全算法。通过私钥对认证数据进行签名，将公钥提供给终端，使终端能认证手机帐户的同时，也防止手机帐户的伪造。

在交易的过程和交易数据的认证上，系统采用快速的对称的安全算法，保证数据的快速认证和准确性。

### 交易结算处理

#### 业务数据结算

HCE 云支付结算系统向安全系统提出交易数据安全认证请求。确认交易数据后，结算系统向凭证系统查询云端帐户和手机账户的对应关系，并将交易信息更新入云端帐户的交易列表中。完成信息确认和更新后，结算系统形成和地铁业务系统间的结算数据。

HCE 云支付和地铁通业务系统根据结算数据完成资金结算和划拨。

#### 资金通道结算

HCE 云支付结算系统还需与资金来源通道进行资金对账，三方的资金对账无误后完成资金通道的结算和划拨。

## 手机APP端的功能

### 用户注册

用户通过手机注册云卡APP 账户，提供手机硬件信息IMEI等串号信息到云平台注册。

### 用户登录

用户通过手机号和密码登录APP。忘记密码可以提供密码重置功能。

### 密码修改

APP在用户页面提供用户密钥修改和手势密钥功能。

### 资金来源绑定

用户在申请云卡之前需要绑定资金来源，目前可绑定的资金通道有银联、微信、支付宝。用户可以根据自己需求选择。

### 手机票生成

手机帐户构建完成后，向HCE云支付平台回送手机帐户信息，APP在手机上建立手机帐户。然后再根据交通部规范以及轨道交通卡结构完成手机票的卡目录的构建以及从安全管理系统获取消费密钥和TAC计算密钥。

### 手机票充值

用户需要使用手机帐户进行公交快速支付时，需先通过 HCE云支付 APP向账户管理系统申请手机帐户充值。账户管理系统允许后，APP需通过第三方支付（银联支付，支付宝，微信支付等）完成充值，并从账户管理系统获得手机帐户的认证数据和钱包数据完成对手机票的充值。

### 手机票消费

手机帐户充值完成后，手机可在有效期内完成单次公共交通快速支付。交易时需根据地铁储值票交易流程规范，对交易数据生成交易认证码。并将手机票交易数据发送云端支付平台结算系统。

### 密钥及关键数据存储

云端支付平台需要对脱机交易密钥和TAC计算密钥，以及卡关键数据进行存储，任何时候都不能给云端支付以外的应用获取到该密钥和关键数据。

密钥存储：申请账户及形成卡片时，平台通过地铁空发接口获取卡片相关密钥，并存储于平台内。

关键数据：通过算法把关键数据进行加密，以文件方式保存在手机端。

## 云端支付业务划分

### 手机用户注册、申请

乌鲁木齐地铁用户可以从地铁官网站或指定下载渠道下载、安装移动应用。用户完成乌鲁木齐地铁APP的下载与安装后，在此APP上完成用户注册之后，即可使用地铁云卡业务。用户在地铁APP上进行用户注册时，可以使用以下几种UserID：用户登录名、证件类型和证件编码,手机号码等。

注册乌鲁木齐地铁APP的用户可以通过此流程申请云卡：用户根据提示录入相关信息，乌鲁木齐地铁APP进行部分信息的客户端合法性校验。录入的信息包括了用户身份信息、用户手机号信息等。申请受理成功后会通过短信方式提示发送成功，并提示请申请激活码。

### 申请激活码

用户的移动应用在云卡申请的最后一步获得了云端支付平台发给其的激活码申请通知。移动应用在该流程中可以手动发起激活码申请。申请受理成功后会通过短信方式发送激活码。

### 云卡激活

当用户获得激活码后，用户可通过登录移动应用激活云卡。用户输入必要的验证要素与激活码，从云端支付平台下载并激活云账户。

### 限制密钥更新

此过程由云端支付平台的自动任务发起，有两种情况触发此自动任务：

1.移动应用将限制密钥使用情况送至云端支付平台。

2.云端支付平台根据限制密钥更新规则自动触发。

### 风险参数设置

云端支付平台修改云卡的风险参数之后，会通知移动应用进行风险参数更新。可以更新的风险参数有：限制密钥过期前自动更新、限制密钥下载数量、限制密钥更新阀值、是否允许通过移动应用注销云卡。

### 云卡锁定

支付平台发现风险或其他需要的锁定云卡的情况下，自主发起锁定云卡的操作。

### 云卡解锁

支付平台确认风险解除或其他需要时，自主发起云卡解锁的操作。

### 云卡注销

用户通过支付平台客服或从移动应用上进行云卡注销，注销时，提供证件类型、证件号、移动应用名称、手机号和设备信息等。

### 手机云卡在公共交通领域的消费交易

用户在公共交通机具（公交车载机、地铁闸机等）处刷手机，完成快速脱机交易，包括轨道交通计程计时复合应用进出闸交易。

### 重装应用和删除应用数据

用户重装应用或删除应用数据之后登录移动应用。进行手机移动应用、云端支付平台、主账户等关系的变更。

APP存储数据与程序非同一目录，在用户卸载程序时，可选择不删除应用数据，再次安装应用后，可重新加载用户数据并校验是否合法，合法情况下，可继续使用。平台可以做账户移植的功能，即用户需要更换手机时，先在已安装的手机上选择备份，必须联网情况下，备份的数据上传到后台，然后更换手机、登陆账户，并完成认证等校验合法性的操作。更换过程中，被备份机暂停使用。

### 移动应用用户变更

该流程仅发生在移动应用端，和云端支付平台无关。移动应用的处理流程为：

1.用户使用别的移动应用UserID 应登录移动应用使用云服务。

2.移动应用判断CPS Library 绑定的UserID 是否和当前UserID 一致。

3.如果不一致，移动应用禁止该UserID 使用云卡服务。

### 同一移动应用UserID 更换设备或新增设备

用户使用同一个UserID 更换一个设备或新增一个设备登录同一个应用。用户的更换设备或新增设备上必须没有使用其他的UserID 注册过云卡服务。如果用户的更换设备或新增设备上已经使用其他UserID 在该移动应用中注册过云服务，那么更换设备或新增设备的移动应用将禁止该用户使用云卡业务。

## 系统可靠性及安全管理

### 系统可靠性策略

根据轨道交通快速支付的特点，系统在不同阶段，不同流程上选择了不同的安全算法，保证认证准确、高效。

在手机帐户的认证上，系统采用非对称的安全算法。通过私钥对认证数据进行认证加密，将公钥提供给终端，使终端能认证手机帐户的同时，也防止手机帐户的伪造。

在交易的过程和交易数据的认证上，系统采用快速的对称的安全算法，保证数据的快速认证和准确性。

### 系统安全管理方案

手机帐户资金以及敏感数据的安全性在云支付平台采用独立的网络安全管理单元存储。高级别敏感数据如云卡消费子密钥不需要从云端下载到手机应用端，只存在云平台密闭环境以保证账户绝对安全。从手机硬件获得部分硬件资源作为账户第二级及以下敏感信息的存储区域。手机APP从远端授信系统获得加密方法将账户次要敏感信息进行加密写入硬件存储区域。硬件存储区域只允许合法应用程序访问，将避免手机系统被ROOT后而引起的数据安全问题。

## 交易安全机制及防护

### 交易数据的完整性。

云端交易结算系统还对充值交易数据内票卡联机交易序号以及脱机消费交易数据内票卡脱机交易序号进行管理，保证交易数据的完整性。



图4：脱机交易结算框图

### 交易信息在传输过程中的保密性。

交易信息在传输过程中采用对称加密方式，保证在传输过程中以密文传输传送，而加密方式是由云端平台与手机APP约定加解密算法。

交易传输过程保密性框图如下如：



图5：传输过程保密性框图

### 交易的不可否认性。

手机账户采用联机充值，云端平台链接通卡充值中心完成票卡的充值过程。充值交易记录将包含充值记录安全认证码TAC保证充值交易数据的不可否认性和合法性。

脱机交易数据分为手机端和机具端分别上送各自的交易数据采集中心。手机账户完成脱机交易结算框图如下图。手机账户完成一次公共交通小额支付，手机APP记录交易相关信息，并通过手机端TAC计算密钥产生交易数据安全认证码形成一条完成交易记录。在有网络时上送给云端交易管理系统。机具端按照通卡已有数据交互规范产生交易记录，按已有数据采集方式上送交易到通卡数据采集系统。安全认证码TAC保证消费交易数据的不可否认性和合法性。

### 系统的风险监控和反制。

#### 交易流水管理

* PSAM内建立特殊数据文件

PSAM内建立特殊的数据文件，用于记录PSAM的累计交易次数，也就是 PSAM的交易流水。

* PSAM的交易流水能在产生交易认证TAC的同时进行加一的修改

这一特殊数据文件，除了产生交易认证TAC的命令外，其他任何命令只能读取，不能改写。在使用产生交易认证TAC产生交易认证TAC的同时，PSAM交易流水加一，保证车票的交易认证TAC和PSAM的交易流水的唯一对应关系。

#### 脱机交易计数管理

票卡的交易计数能在完成交易产生TAC的同时进行加一的修改

这一特殊数据文件，除了消费命令外，其他任何命令只能读取，不能改写。在消费产生交易认证TAC的同时，票卡交易计数加一，保证车票交易计数与交易认证TAC、PSAM的交易流水的唯一对应关系。

#### 车票的信用管理

云端支付平台的账户管理系统对单一账户的充值消费数据进行统一，检查充值消费金额，在发现异常充值或者消费的情况发生时及时预警。根据多次业务规则判断，最终采取对手机账户的例如系统黑名单。

### 客户端敏感数据安全

客户端不存在高级敏感数据，例如消费子密钥等。

### 云端支付系统CA子系统

CA子系统是指通过建立基于数字证书认证的移动设备接入安全防护体系，为交通卡应用系统提供统一的身份认证、访问控制、数据的保密性、完整性、抗抵赖的技术防护手段。

为实现以上技术要求结合交通卡云服务系统实际现状，本方案采用企业版证书认证服务器，结合无线安全认证网关，搭建基于证书认证服务器的安全防护体系。本次系统的建设以满足业务应用安全需求为出发点，实现如下的安全服务功能：

* **统一身份标识**

PKI/CA证书认证服务器能够为移动办公设备以及人员签发可信的证书，从而保障人员身份信息以及设备身份信息可信问题。

* **统一的安全认证**

当用户访问业务系统时，首先需要进行基于数字证书的统一身份认证。只有通过身份认证后，用户才能根据自身权限，实现对业务系统的访问。

* **高强度访问控制**

跟据安全需求，采用数字证书、密钥等的安全认证方式，可提高访问控制安全强度。访问控制的目的是允许拥有权限的用户对应用的合法访问，拒绝没有访问权限的用户对应用的非法访问。跟据安全需求，采用数字证书、密钥等的安全认证方式，可提高访问控制安全强度。

* **数据保全服务**

CA身份认证系统对业务系统涉及的重要数据提供数字信封、数字签名功能，使得任何非法的数据修改过程能够被及时发现，保证数据从生成、流转、共享到存储整个生命周期内的完整性和一致性，实现业务数据的安全传输功能。

采用SSL数据加密技术保护隧道传输安全，避免数据传输过程中被窃取、盗用或篡改。

#### CA建设内容

为实现以上技术要求结合交通卡云服务系统实际现状，本方案采用信安证书认证服务器，结合信安无线认证网关，搭建基于证书认证服务器的安全防护体系。

各系统模块的主要作用如下：

* 证书认证服务器

证书认证服务器作为安全防护体系的基础，主要实现对用户的身份标示，为用户的身份认证提供统一的用户管理平台。

证书认证服务器通过对每个用户颁发数字证书，数字证书成为用户的唯一身份标示。

证书认证服务器通过为用户颁发证书，同时建立的统一的用户身份信息库，由证书认证服务器的目录服务为各应用系统提供身份认证的相关信息，从而建立的统一的用户管理体系。

* 无线安全认证网关

无线安全认证网关结合证书认证服务器为移动办公设备提供统一的接入认证服务；

无线安全认证网关结合证书认证服务器为应用提供统一的身份认证服务；

无线安全认证网关使用密钥、数字信封技术对应用系统的通讯、数据进行加密，保障应用系统数据的保密性、完整性、抗抵赖。

* 安全客户端

提供基于证书的数据加解密接口通过与交通卡云系统app系统集成，实现用户通过移动设备访问应用系统数据时，采用数据加密技术保护隧道传输安全；

安全客户端app提供java整合包，更加人性化。

#### CA网络拓扑图



如上图所示，整个业务流程：安卓设备通过交通卡云系统下载证书到手机内（短信、邮件等形式校验），下载信道通过无线网关加密，防止被窃取。之后，格尔安全客户端获取证书信息，进行身份识别，校验通过后与无线安全认证网关之间建立安全加密信道。

#### CA架构设计

本解决方案在总体架构上分为以下两个层面：

1. 首先建设网络信任体系的基础设施—公钥基础设施PKI（证书认证服务器）；
2. 在PKI基础上，建立应用安全支撑平台（无线安全认证网关），安全支撑平台为上层应用提供全面的安全服务，包括：移动接入认证、强身份认证、保密性与完整性、防抵赖服务。

**公钥基础设施PKI（数字证书系统）**

**应用安全支撑平台（认证、加密、数字签名）**

**各应用系统（如：OA、ERP等）**

系统总体框架

* 公钥基础设施PKI

公钥基础设施PKI（Public Key Infrastructure）是利用公开密钥技术所构建的、国际公认的唯一能够全面解决网络安全问题的、普遍适用的一种基础设施。在PKI中，最基本的元素是数字证书，所有安全的操作通过证书来实现；PKI还包括签置这些证书的证书中心CA(Certificate Authority)，登记和批准证书签置的登记机构(RA)，以及存储和发布这些证书的电子目录（LDAP）等；这些PKI的基本元素有机地结合在一起就构成了PKI，以下我们也公钥基础设施PKI称为证书认证服务器。

通过CA颁发的数字证书，基于应用安全支撑平台，各种网络应用可以有效地实现强身份认证，并进一步实现机密信息的保密性、完整性与不可抵赖性。证书认证服务器通过数字证书以及管理这些数字证书的一整套设施，维持网络世界的秩序；通过提供一系列的安全服务，为网络电子商务、电子政务提供有力的安全保障。

* 应用安全支撑平台

公钥基础设施PKI（证书认证服务器）是网络安全信任体系的基础设施，但是，证书认证服务器并不直接为上层的各种应用提供各种安全服务；应用系统所需要的安全服务必须通过相应的安全产品来提供。

应用安全支撑平台是在证书认证服务器的基础上，由相应的安全产品所组成的、向上层应用提供基础安全服务的支撑性平台。

本CA子系统应用安全支撑平台由无线安全认证网关组成。

## 云卡业务应用流程

### 应用场景



### 注册



### 云卡申请



### 云卡激活



### 云卡脱机消费



### 对账



### 移动应用



### 支付组件



### 支付插件



### 账号申请



### 凭证管理



### 交易处理



### 安全通信机制



### 移动应用安全机制



### 安全交易密钥存储及使用

|  |  |  |
| --- | --- | --- |
| **密钥类型** | **存储位置** | **用途描述** |
| IMK | 服务器 | 发卡行主密钥 |
| CMK | 服务器 | 卡片主密钥 |
| LUK\_A1 | DEK2加密存储在手机终端 | 一密多次限制密钥 |
| LUK\_A2 | DEK2加密存储在手机终端 | 一密一次限制密钥 |
| TK | 激活过程中由凭证管理系 统生成并发送给客户端 | 客户端与云支付平台报文加密传输 |
| DEK | 由服务器随机生成，凭证申请时下发并用KEK加密存储在手机 | DEK1用于加密云卡信息数据 |
| KEK | 内存 | 用于加解密DEK，并用于交易时作为 CDCVM脱机移动应用PIN验证时Hash校验的密钥 |
| AEK | 内存 | 用于加密存储Access PIN的密钥 |
| Access PIN | 加密存储在手机终端 | CDCVM及KEK使用 |

# 云卡在城市交通领域的应用分析

## 城市交通云卡系统设计

### 架构设计



1. HCE云卡和应用系统整合架构图

* 票卡云服务端：负责生成一张具有唯一性、合法性、安全的票卡，保证和手机端APP数据交换安全、和读写器端数据交换合法。
* NFC手机APP：负责手机票卡的安全存储，票卡数据安全交换。
* 读写器端：保证对手机APP端发送的票卡数据合法性、正确性进行效验。

### 云卡设计

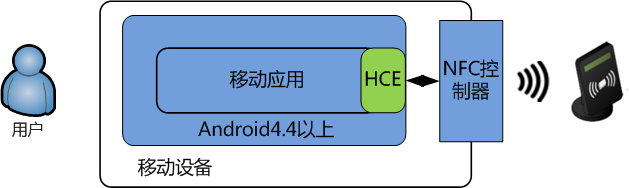
由于NFC-SWP方案安全载体集成在手机设备内的成本较高，安全载体发行方通常不会无条件或免费向应用提供方开放，因此，应用提供方向安全载体发行方支付一定的费用，以换取安全载体内的存储空间。通过HCE模式，将减少生态系统的参与方、缩短NFC价值链，因此成本将会大大降低。同时由于发卡主体无需再去管理和采购SE模块，TSM平台不再是必须选项，因此也降低了发卡方的运营管理成本；从受理上看，HCE技术兼容EMV终端的受理，存量的EMV终端无需做任何改造就可以直接复用，降级了HCE的部署成本。

HCE作为安卓系统特征，要求在移动应用中通过Manifest定义HostApduService声明来实现对安全应用的路由。在移动应用的安装过程中，移动应用将AID注册到移动设备的操作系统中，从而保证基于这些支付应用AID的交易可以路由到此移动应用中。

手机端HCE云卡和读写器端通讯协议遵循ISO7816-4协议，通讯流程和手机票卡数据结构如下：



1. HCE云卡结构



1. HCE云卡工作原理

### 方案安全性

云端支付平台采用多重安全保护手段用于安全防护。

首先是通信安全。云端支付产品方案在通信通道方面采用双重加密技术，链路层使用TLS/SSL，消息层使用会话密钥加密技术，使所有传输数据均经过双重加密的安全保护。

第二是客户端敏感数据存储。移动应用中的敏感数据（包括密钥及其他信息）等使用反编译技术进行加密保护，加密密钥与设备和应用相关，当移动应用被攻击和被非法读取时，云端支付控件能够及时发现并完成报警。在用户访问交易凭证时，需要用户输入Access pin，防止用户手机丢失时云端支付卡被盗刷。

第三是后台风险监控和反制。云端支付平台或发卡方可以对交易进行监控，对于异常的可能被攻击的交易可以直接拒绝，如异常情况超出发卡行或云端支付的接收范围，则可以对云端支付卡进行删除或暂停处理。

* 手机APP安全设计

获取NFC手机终端的基础信息、保证手机操作系统是非ROOT操作系统。票卡服务器会对手机终端进行基础的合法性验证，验证当前手机环境是可信的。

* 票卡信息安全设计

票卡信息在传输、存储均有加密解密过程、沙盒等安全技术等安全保障保证票卡的安全。

## 云卡的交易机具

鉴于云卡采用的HCE方案，安全性由手机端和后台服务端控制，终端机具目前无需增加硬件接口与后台服务端链接。

云卡与读写器物理层通信基于ISO14443A-4协议，读写器硬件基站芯片需要支持ISO14443A-4协议卡片类型。在已支持通卡的终端机具上，对云卡的支持只需按照通卡原有的通卡交易流程处理即可，无需增加新的业务流程。