|  |
| --- |
| 北京思源政务通科技集团有限公司 |
| **福州示范大学信息化建设** |
| 一卡通平台方案 |

|  |
| --- |
| 北京思源政务通科技集团有限公司  2019-10-17 |

福州师范大学一卡通平台方案

# 概述

本规范用于说明福州师范大学一卡通二维码（以下简称“二维码”）的应用场景、身份二维码数据结构、关键信息接口、安全要求、受理终端要求、手机APP要求等。

# 规范性引用文件

QRCode国家标准GB/T 18284-2000。

ECC椭圆曲线公钥密码算法（曲线ID NID\_secp256r1）。

# 术语和定义

| **术语/缩略语** | **解释** |
| --- | --- |
| 二维码 | 二维码是在平面上使用若干个与二进制相对应图形来表示记录数据信息的几何形体。 |
| 支付通道 | 接入支付平台，提供支付结算能力的机构，例如支付宝、微信、银联。 |
| 受理终端 | 用于识别和验证二维码的终端设备。 |
| 虚拟卡证书服务 | 用于提供虚拟卡和系统证书服务。 |
| 平台签名 | 由二维码平台私钥对虚拟卡交易平台生产的公钥进行签名以及返回的其他信息 |
| 机构签名 | 由虚拟卡交易平台的私钥对虚拟卡信息的签名 |
| 个人证书 | 利用机构证书私钥对个人的公钥以及其他信息进行签名 |
| 密基 | 安全管理私钥的软体 |
| 密照 | 安全存储私钥的载体，是特殊格式的一个文件 |

# 二维码场景说明

福州市大学本期二维码应用场景涉及到身份认证类场景有门禁和图书借阅，涉及到支付类的场景有食堂就餐、超市购物。

## 身份认证场景



图 1身份认证门禁场景流程

1. 师生登录“e福师”APP，通过学校组织账号认证，“e福师”APP身份二维码组件，通过用户证书和二维码规范生成身份二维码业务信息，提交给密基，进行用户私钥签名，生成身份二维码串信息；
2. 二维码字符串信息按照二维码编码规范二维码图片，并展示；
3. 二维码识读，机具识读到二维码信息，交由二维码组件进行二维码验证，二维码验证包括：证书时效性验证、证书签名验证、二维码时效性验证、业务域签名验证，验证完成，解析业务信息，提交给门禁控制组件身份信息，进行门禁的开关控制。
4. 门禁控制信息按照规则同步门禁管理系统，进行记录统计处理；
5. 按照福师大大数据平台数据同步规则，门禁系统数据给大数据。

## 支付场景流程



图 2建设银行在线二维码支付场景流程图

流程说明：

1. 建户流程
   1. 用户在APP端完成实名认证与学生/教职工信息登记并开通虚拟卡一卡通账户
   2. 点击身份码应用授权进入身份码服务
2. 用户授权获取实名认证平台的实名信息
3. 拉取组织平台学生/教职工信息
4. 创建虚拟卡一卡通账户
   1. 用户点击付款码应用进入付款码页面
5. 用户授权获取实名认证平台的实名信息
6. 进入建行绑卡流程并返回建行绑卡结果信息
7. 创建虚拟卡一卡通账户&建行账户信息关联关系
8. 支付流程：
9. 用户展示付款码并选择支付方式
10. 商户在商户扫码终端创建商品订单
11. 机具扫描二维码信息并将二维码信息上传至商家后台
12. 商家后台向建行发起支付扣款流程并接收扣款结果
13. 商户后台接收到支付扣款结果之后通知到虚拟卡一卡通平台由虚拟卡一卡通平台通知APP交易结果
14. 商家后台将交易信息上送至大数据平台由大数据平台做数据处理

# 整体接方案

## “e福师“一卡通平台整体设计



图 3“e福师”一卡通平台整体设计图

虚拟卡一卡通平台使用者为学生群体，教职工以及商户。虚拟一卡通的表现形式为身份二维码，一卡通实体卡为校园卡。一卡通的两种表现形式都由机具识别。身份码与校园卡的应用场景包括食堂，门禁，超市以及图书馆等。

主要业务应用包括：虚拟卡一卡通管理，系统门禁管理系统，食堂/超市计费系统，图书馆管理系统，补办卡系统。

统一身份认证平台，组织平台，实体卡综合管理平台为平台整体维护三套账户体系，分别是：实名信息，组织信息，校园卡信息。虚拟卡证书服务负载身份码的证书认证与颁发。虚拟卡风控管理系统则配置与维护二维码的安全策略参数。实体卡密钥管理系统，机具运维平台，综合服务平台维护实体卡与机具、实体卡的相关信息。建户支付平台则完成实际的核心支付交易。

大数据平台负责“e福师”APP与校园卡所产生的所有的交易数据的汇总、分析、统计与展示。

## “e福师“一卡通平台业务设计

## 关键流程说明

### 虚拟卡一卡通开卡流程



图 4虚拟卡一卡通开卡流程

本流程主要点有三个：第一实名用户；第二身份码开通；第三支付码开通。

### 扫码终端下载二维码交易平台根证书流程

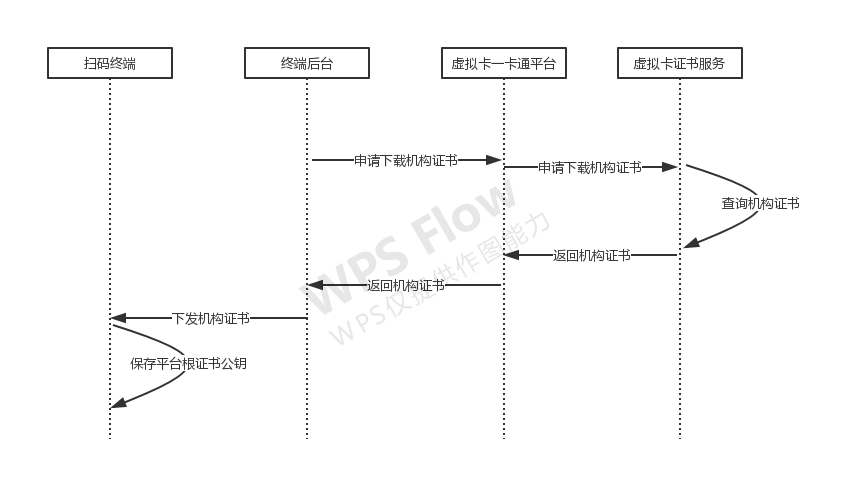
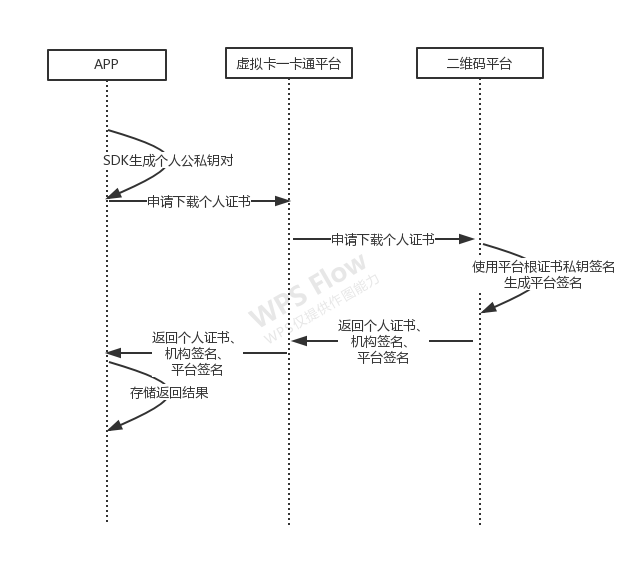


图 5扫码终端下载二维码交易平台根证书流程

### 个人证书下载流程

图 6个人证书下载流程

### 受理终端识别二维码流程

受理终端识别并验证二维码进行消费，个人或机构证书出码均采用统一的处理流程，具体流程如图所示：

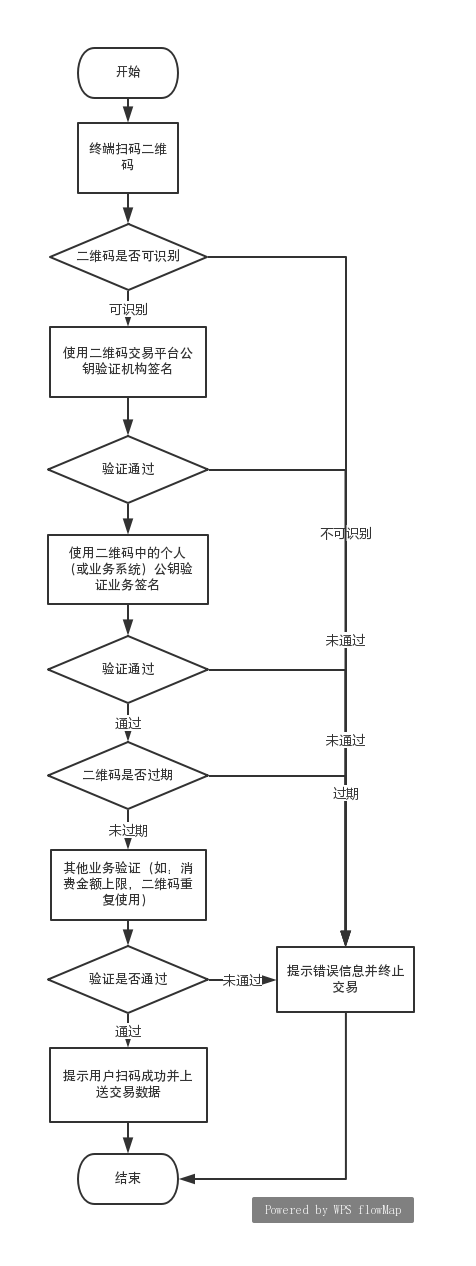


图 7 受理终端识别二维码流程示意图

流程说明：

1.受理终端扫描二维码，识别成功则进入后续处理，识别失败则终止交易。

2.受理终端使用根证书公钥验证二维码中的机构签名数据，验签通过则进入后续处理，验签失败则终止交易。

3.受理终端使用平台签发的个人（或业务系统）公钥验证二维码中的业务签名数据，验证通过则进入后续处理，验证失败则终止交易。

4.受理终端使用二维码中的码失效时间对比终端时间，如果超出失效时间则终止交易，未超出则进入后续处理。

5.受理终端对二维码中的其他业务信息域进行校验，（如：使用二维码中的金额上限信息验证本次消费金额、检查用户是否是黑名单，二维码是否已经被当前机具扫过等）。如果校验通过则进入后续处理，否则终止交易。

6.验证并记录交易数据，提示用户扫码成功。

## 关键接口定义

### APP调用接口

#### 虚拟卡证书签发

提供给“e福师”APP开通身份码接口，用户主动触发，需要经过统一身份认证和组织平台验证。

|  |  |
| --- | --- |
| 接口调用地址 | https：//ip:port/ vcard/userapi/v1/cert/sign |
| 接口提供者 | 虚拟卡一卡通业务系统 |
| 接口消费者 | “e福师”APP |
| 功能描述 | 虚拟卡一卡通业务系统提供给“e福师”app调用，用户认证虚拟卡，颁发虚拟卡证书 |

* **请求参数描述**

| 序号 | 参数名称 | 参数 | 参数类型 | 必填 | 说明 | 示例值 |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 时间戳 | timestamp | string | Y | 发送请求的时间，格式"yyyyMMddHH：mm：ss" | 20170809152711 |
| 2 | 用户登录令牌 | personToken | string | Y | “e福师“统一身份认证登录接口 |  |
| 3 | 公钥 | publicKey | string | Y | 出码应用系统根据密基算法生成的公钥6采用base64编码 |  |
| 4 | 用户签名 | sign | string | Y | 密基签名算法（SM3） |  |

* **响应值描述**

| 序号 | 参数名称 | 参数 | 参数类型 | 说明 | 示例值 |
| --- | --- | --- | --- | --- | --- |
| 1 | 返回码 | respCode | string | 01代表成功 | 01 |
| 2 | 返回消息 | respMsg | string | respCode = 01，数据放入data，  respCode = 其他， 错误消息放入 respMsg |  |
| 3 | 返回数据 | data | string | 返回内容数据域参考证书域 |  |
| data数据结构定义 | | | | | |
|  | 虚拟卡类型公钥 | vCardPublicKey | String | 虚拟卡类型公钥 |  |
|  | 平台公钥 | authPublicKey | String | 平台公钥 |  |
|  | 虚拟卡签发时间 | signTime | String | 虚拟卡签发时间戳 |  |
|  | 虚拟卡卡号 | vCardNoe | String | 虚拟卡卡号 |  |
|  | 虚拟卡类型编号 | vCardTypeNo | String | 虚拟卡类型编号 |  |
|  | 虚拟卡公钥 | vCardPublic | String | 虚拟卡公钥 |  |
|  | 虚拟卡证书失效时间 | effecitiveTime | String | 虚拟卡证书失效时间 |  |
|  | 虚拟卡类型签名 | vCardSign | String | 虚拟卡类型签名 |  |
|  | 平台签名 | signature | String | 平台签名 |  |

#### 虚拟卡证书下载

提供给“e福师”APP开通下载虚拟卡证书接口，客户端登录由APP初始化首页时调用。

|  |  |
| --- | --- |
| 接口调用地址 | https：//ip:port/ vcard/userapi/v1/cert/download |
| 接口提供者 | 虚拟卡一卡通业务系统 |
| 接口消费者 | “e福师”APP |
| 功能描述 | 虚拟卡一卡通业务系统提供给“e福师”app调用，客户端下载虚拟卡证书 |

* **请求参数描述**

| 序号 | 参数名称 | 参数 | 参数类型 | 必填 | 说明 | 示例值 |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 时间戳 | timestamp | string | Y | 发送请求的时间，格式"yyyyMMddHH：mm：ss" | 20170809152711 |
| 2 | 用户登录令牌 | personToken | string | Y | “e福师“统一身份认证登录接口 |  |
| 3 | 虚拟卡卡号 | vCardNo | string | Y | 虚拟卡卡号 |  |
| 4 | 用户签名 | sign | string | Y | 密基签名算法（SM3） |  |

* **响应值描述**

| 序号 | 参数名称 | 参数 | 参数类型 | 说明 | 示例值 |
| --- | --- | --- | --- | --- | --- |
| 1 | 返回码 | respCode | string | 01代表成功 | 01 |
| 2 | 返回消息 | respMsg | string | respCode = 01，数据放入data，  respCode = 其他， 错误消息放入 respMsg |  |
| 3 | 返回数据 | data | string | 返回内容数据域参考证书域 |  |
| data数据结构定义 | | | | | |
|  | 虚拟卡类型公钥 | vCardPublicKey | String | 虚拟卡类型公钥 |  |
|  | 平台公钥 | authPublicKey | String | 平台公钥 |  |
|  | 虚拟卡签发时间 | signTime | String | 虚拟卡签发时间戳 |  |
|  | 虚拟卡卡号 | vCardNoe | String | 虚拟卡卡号 |  |
|  | 虚拟卡类型编号 | vCardTypeNo | String | 虚拟卡类型编号 |  |
|  | 虚拟卡公钥 | vCardPublic | String | 虚拟卡公钥 |  |
|  | 虚拟卡证书失效时间 | effecitiveTime | String | 虚拟卡证书失效时间 |  |
|  | 虚拟卡类型签名 | vCardSign | String | 虚拟卡类型签名 |  |
|  | 平台签名 | signature | String | 平台签名 |  |

#### 虚拟卡业务风控参数获取

提供给“e福师”APP开通获取虚拟卡风控指标接口，客户端登录由APP初始化首页时调用。

|  |  |
| --- | --- |
| 接口调用地址 | https：//ip:port/ vcard/userapi/v1/ riskIndex /get |
| 接口提供者 | 虚拟卡一卡通业务系统 |
| 接口消费者 | “e福师”APP |
| 功能描述 | 虚拟卡一卡通业务系统提供给“e福师”app调用，客户端获取风控指标 |

* **请求参数描述**

| 序号 | 参数名称 | 参数 | 参数类型 | 必填 | 说明 | 示例值 |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 时间戳 | timestamp | string | Y | 发送请求的时间，格式"yyyyMMddHH：mm：ss" | 20170809152711 |
| 2 | 用户登录令牌 | personToken | string | Y | “e福师“统一身份认证登录接口 |  |
| 3 | 虚拟卡卡号 | vCardNo | string | Y | 虚拟卡卡号 |  |
| 4 | 用户签名 | sign | string | Y | 密基签名算法（SM3） |  |

* **响应值描述**

| 序号 | 参数名称 | 参数 | 参数类型 | 说明 | 示例值 |
| --- | --- | --- | --- | --- | --- |
| 1 | 返回码 | respCode | string | 01代表成功 | 01 |
| 2 | 返回消息 | respMsg | string | respCode = 01，数据放入data，  respCode = 其他， 错误消息放入 respMsg |  |
| 3 | 返回数据 | data | string | 返回内容数据域参考证书域 |  |
| data数据结构定义 | | | | | |
|  | 离线时长 | offlinelength | Int | 离线时长 |  |
|  | 离线出码次数 | offlineUsageTimes | Int | 离线出码次数 |  |

#### 付款码获取

提供给“e福师”APP开通获取付款码接口，用户主动触发。

|  |  |
| --- | --- |
| 接口调用地址 | https：//ip:port/ vcard/userapi/v1/ payQrcode/get |
| 接口提供者 | 虚拟卡一卡通业务系统 |
| 接口消费者 | “e福师”APP |
| 功能描述 | 虚拟卡一卡通业务系统提供给“e福师”app调用，获取付款码接口 |

* **请求参数描述**

| 序号 | 参数名称 | 参数 | 参数类型 | 必填 | 说明 | 示例值 |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 时间戳 | timestamp | string | Y | 发送请求的时间，格式"yyyyMMddHH：mm：ss" | 20170809152711 |
| 2 | 用户登录令牌 | personToken | string | Y | “e福师“统一身份认证登录接口 |  |
| 3 | 临时公钥 | publicKey | String | Y | 客户临时公钥信息 |  |
| 4 | 付款码类型 | payQRcodeType | String | Y | 1-校园卡二维码  2-银行卡二维码 | 1 |
| 5 | 用户签名 | sign | string | Y | 密基签名算法（SM3） |  |

* **响应值描述**

| 序号 | 参数名称 | 参数 | 参数类型 | 说明 | 示例值 |
| --- | --- | --- | --- | --- | --- |
| 1 | 返回码 | respCode | string | 01代表成功 | 01 |
| 2 | 返回消息 | respMsg | string | respCode = 01，数据放入data，  respCode = 其他， 错误消息放入 respMsg |  |
| 3 | 返回数据 | data | string | 返回内容数据域参考证书域 |  |
| data数据结构定义 | | | | | |
|  | 二维码值密文 | qrCode | String | 使用请求参数中的临时公钥加密的二维码串 |  |

### 一卡通调用接口

#### 终端下载根证书接口

虚拟卡交易系统提供给一卡通终端后台下载虚拟卡类型证书；

|  |  |
| --- | --- |
| 接口调用地址 | https：//ip:port/ vcardTradingSystem /api/v1/ vCardTypeCert/get |
| 接口提供者 | 虚拟卡交易系统 |
| 接口消费者 | 终端后台业务系统 |
| 功能描述 | 虚拟卡交易系统提供给一卡通终端后台下载虚拟卡类型证书 |

* **请求参数描述**

| 序号 | 参数名称 | 参数 | 参数类型 | 必填 | 说明 | 示例值 |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 时间戳 | timestamp | string | Y | 发送请求的时间，格式"yyyyMMddHH：mm：ss" | 20170809152711 |
| 2 | 开发者ID | developerId | string | Y | 开发者ID，由平台提供 |  |
| 3 | 虚拟卡类型编号 | vCardTypeNo | string | Y | 虚拟卡类型编号 |  |
| 4 | 签名 | sign | string | Y |  | RSA签名 |

* **响应值描述**

| 序号 | 参数名称 | 参数 | 参数类型 | 说明 | 示例值 |
| --- | --- | --- | --- | --- | --- |
| 1 | 返回码 | respCode | string | 01代表成功 | 01 |
| 2 | 返回消息 | respMsg | string | respCode = 01，数据放入data，  respCode = 其他， 错误消息放入 respMsg |  |
| 3 | 返回数据 | data | string | 返回内容数据域参考证书域 |  |
| 4 | 签名 | sign | string |  |  |
| Data数据结构定义 | | | | | |
|  | 平台公钥 | authPublicKey | String | 平台公钥 |  |
|  | 证书签发时间 | signTime | String | 证书签发时间戳 |  |
|  | 虚拟卡类型编号 | vCardTypeNo | String | 虚拟卡类型编号 |  |
|  | 虚拟卡类型公钥 | vCardTypePublic | String | 虚拟卡类型公钥 |  |
|  | 证书失效时间 | effecitiveTime | String | 证书失效时间 |  |
|  | 平台签名 | signature | String | 平台签名 |  |

#### 支付结果通知接口(思源提供)

|  |  |
| --- | --- |
| 接口调用地址 | https://ip:port/ vcard/api/v1/gateway |
| 接口编号 | vcard.terminal.payResultNotify |
| 接口提供者 | 虚拟卡平台 |
| 接口消费者 | 一卡通支付系统 |
| 功能描述 | 用户完成支付之后通知虚拟卡平台消费结果，虚拟卡平台想APP端发起消息通知 |

* **请求参数描述**

| 序号 | 参数名称 | 参数 | 参数类型 | 参数长度 | 必填 | 说明 | 示例值 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 接口版本 | version | string | 8 | Y | 接口版本 | 1.0.0 |
| 2 | 接口名 | method | string | 30 | Y | 接口名 | vcard.terminal.downOrgCert |
| 3 | 时间戳 | timestamp | string | 14 | Y | 发送请求的时间，格式"yyyyMMddHH：mm：ss" | 20170809152711 |
| 4 | 开发者ID | developerId | string | 32 | Y | 开发者ID，由平台提供 |  |
|  | 请求id | requestId | String | 36 |  |  |  |
| 5 | 业务数据 | data | string | - | Y | 以json格式编码的业务数据 |  |
| 6 | 签名 | sign | string | 512 | Y |  | RSA签名 |
| 数据域格式 | | | | | | | |
| 1 | 商户业务订单号 | bsPayOrderNo | String | 64 | Y | 订单号 | 12345678901  2345678 |
| 3 | 支付平台交易流水号 | payPlatTradeFlowNo | String | 64 | Y | 支付平台流水号 | 1000200030000 |
|  | 商户编号 | merchantName | String | 64 | Y | 商户编号 | 20133333011 |
|  | 商户名称 | merchantName | String | 64 | Y | 商户名称 | 云南过桥米线 |
|  | 用户标识 | userId | String | 64 | Y | 用户标识 | 学号/工号 |
| 6 | 交易金额 | tranAmt | Number | - | Y | 单位为分 | 2000 |
|  | 交易描述 | tradeDetail | String | 256 | Y | 交易明细/内容 | 如:米饭1元，宫保鸡丁12元  辣子鸡丁13元 |
| 8 | 交易日期 | tranDate | String | 8 | Y | (用户支付成功的时间)交易日期格式yyyyMMdd | 20170605 |
| 9 | 交易时间 | tranTime | String | 6 | Y | (用户支付成功的时间)交易时间HHmmss | 123002 |
| 10 | 交易状态 | tranStatus | String | 1 | Y | 交易状态：  1-待支付  2-支付成功  3-支付失败  4-交易关闭 | 1 |
|  | 支付方式 | payWay | String | 1 | Y | 1-校园卡  2-建行钱包  3-建行卡  4-银联卡 | 2 |

* **响应值描述**

| 序号 | 参数名称 | 参数 | 参数类型 | 参数长度 | 说明 | 示例值 |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 返回码 | respCode | string | 2 | 01代表成功 | 01 |
| 2 | 返回消息 | respMsg | string | - | respCode = 01，数据放入data，  respCode = 其他， 错误消息放入 respMsg |  |
| 3 | 返回数据 | data | string | - |  |  |
| 4 | 签名 | sign | string | 512 |  |  |

#### 身份码在线核验

虚拟卡交易系统提供给一卡通终端后台校验身份码；

|  |  |
| --- | --- |
| 接口调用地址 | https：//ip:port/ vcardTradingSystem /api/v1/ qrCode/ check |
| 接口提供者 | 虚拟卡交易系统 |
| 接口消费者 | 终端后台业务系统 |
| 功能描述 | 虚拟卡交易系统提供给一卡通终端后台校验身份码 |

* **请求参数描述**

| 序号 | 参数名称 | 参数 | 参数类型 | 必填 | 说明 | 示例值 |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 时间戳 | timestamp | string | Y | 发送请求的时间，格式"yyyyMMddHH：mm：ss" | 20170809152711 |
| 2 | 开发者ID | developerId | string | Y | 开发者ID，由平台提供 |  |
| 3 | 二维码串 | qrCode | string | Y | 二维码串 |  |
| 4 | 签名 | sign | string | Y |  | RSA签名 |

* **响应值描述**

| 序号 | 参数名称 | 参数 | 参数类型 | 说明 | 示例值 |
| --- | --- | --- | --- | --- | --- |
| 1 | 返回码 | respCode | string | 01代表成功 | 01 |
| 2 | 返回消息 | respMsg | string | respCode = 01，数据放入data，  respCode = 其他， 错误消息放入 respMsg |  |
| 3 | 返回数据 | data | string | 返回内容数据域参考证书域 |  |
| 4 | 签名 | sign | string |  |  |
| Data数据结构定义 | | | | | |
|  | 用户类型 | Type | String | 平台公钥 |  |
|  | 学号 | studentNo | String | 学号 |  |
|  | 教职工号 | staffNo | String | 教职工号 |  |

#### 身份码交易信息提交

### 建行提供接口

#### 生成付款码

|  |  |
| --- | --- |
| 接口调用地址 |  |
| 接口编号 |  |
| 接口提供者 | 建设银行 |
| 接口消费者 | 虚拟卡后台业务系统 |
| 功能描述 | 查询生产用户付款码 |

* **请求参数描述**

| 序号 | 参数名称 | 参数 | 参数类型 | 参数长度 | 必填 | 说明 | 示例值 |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

* **响应值描述**

| 序号 | 参数名称 | 参数 | 参数类型 | 参数长度 | 说明 | 示例值 |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

### 一卡通提供接口

#### 一卡通实体卡信息查询

|  |  |
| --- | --- |
| 接口调用地址 |  |
| 接口编号 |  |
| 接口提供者 | 一卡通平台 |
| 接口消费者 | 虚拟卡后台业务系统 |
| 功能描述 | 查询用户实体卡信息接口 |

* **请求参数描述**

| 序号 | 参数名称 | 参数 | 参数类型 | 参数长度 | 必填 | 说明 | 示例值 |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

* **响应值描述**

| 序号 | 参数名称 | 参数 | 参数类型 | 参数长度 | 说明 | 示例值 |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |



# 身份码规范说明

## 身份码结构定义

| 信息域 | 序号 | 数据元 | 长度  （字节） | 备注 |
| --- | --- | --- | --- | --- |
| 版本域 | 1 | 二维码版本号 | 1 | 标识当前二维码版本.当前固定值为0x01 |
| 证书域 | 2 | 用户身份标识 | 8 | 用户12位实名标识，在用户实名认证时生成 |
| 3 | 公钥类型 | 1 | 标注公钥类型：  1、机构2、个人  机构：机构代表服务机构一对公私钥（此方式建议出码应用APP在线生成二维码） 个人：个人代表个人用户每人一对公私钥 |
| 4 | 用户公钥 | 66 | 密基生成，采用ecc算法。 |
| 5 | 应用服务机构码 | 2 | 应用服务机构的唯一标识，在证书管理系统中注册，对应一个机构证书。 |
| 6 | 用户公钥失效时间 | 4 | 公钥失效时间。该值为4字节无符号整形数字。计算从UTC-8时区的2017年1月1日0时0分0秒起流逝的秒数。例如：失效时间为超过当前时间1天，时间流逝秒数为1277621929，四位字节为0x4C 0x26 0xF6 0xA9。 |
| 7 | 机构签名 | 72 | 使用密基ECC算法，签名原文为证书域2-6项内容构成的字节数组。 |
| 业务域 | 8 | 二维码识别号 | 8 | 机构生成的二维码唯一标识。 |
| 9 | 二维码失效时间 | 4 | 二维码失效时间。该值为4字节无符号整形数字。计算从UTC-8时区的2017年1月1日0时0分0秒起流逝的秒数。例如：失效时间为超过当前时间1天，时间流逝秒数为1277621929，四位字节为0x4C 0x26 0xF6 0xA9，  受理终端需验证此数据项的有效性。 |
| 10 | 业务其他信息 | 32 | 二维码中附带的业务其他信息，详细定义参看8.2.1业务信息结构定义 |
| 11 | 业务签名 | 72 | 使用密基ECC算法，使用用户证书私钥对业务信息域2-9项内容的签名。 |

总长度：268字节。

## 业务信息结构定义

目前试行标准如下

32个字节从左至右依次编号为1到32，其中第1位记录用户类型，第2至6位记录学号/教职工编号，第7至11位记录学号/教职工编号，第12~32位预留。

| 信息域 | 序号 | 长度（字节） | 备注 |
| --- | --- | --- | --- |
| 用户类型 | 1 | 1 | 记录用户类型，如学生、教职工、外聘人员 |
| 学号/工号 | 2 | 5 | 学生/教职工在学校的唯一编号 |
| 借书证号 | 3 | 5 | 借书证号 |
| 预留 | 4 | 21 | 预留 |

# 安全体系

## 数据安全

二维码支付时，代表着用户意愿本身，因为二维码信息必须具备不可伪造，防篡改的特性。二维码的数据构成包含2个大域（1）平台授权信息（2）业务数据。

平台证书是采用平台公钥对二维码生成主体的信息进行签名的后的证书数据。平台证书域保证了二维码的生成主体经过了缴费平台的认证，其安全性由基于密基的非对称加密算法ECC算法本身保证。具备不可伪造和防篡改特点。

业务数据中具备一项数据内容：业务签名。该签名使用的密钥对公钥经过了平台的认证，其安全性由平台证书保证。通过业务签名即可保证业务数据确实由持有密钥对的APP生成，也就代表了用户意愿本身。

## 存储安全

二维码支付交易中涉及关键、敏感数据需要进行安全保护。

密基SDK可将用户个人私钥存储在密照中，再讲密照存储在手机SE，TEE等安全区域，防止信息泄露和被篡改

## 通信安全

### 传输安全

二维码支付交易涉及各系统之间进行信息传输，各系统之间应建立安全通信信道，应对交易数据采用数字签名和加密等安全方式进行传输，确保数据不对监听和篡改，例如：基于 SSL/TLS 的 HTTPS 进行传输等。

公网环境下，二维码信息不应以明文形式传输。

### 传输数据的完整性

应具备对传输数据的鉴别机制，出码应用机构APP确保发出二维码数据的完整性，并且受理终端对接收的二维码数据进行完整性校验。

### 传输数据的保密性

各方应对传输的数据进行保密性保护，数据传输应使用https加密通道传输，不应引起信息泄露。

## 签名安全

证书签名采用基于互联集团提供的密基ECC非对称加密算法，保证签名的安全。

接口签名采用RSA非对称密钥，私钥签名，公钥验签，防止数据篡改

## 使用安全

### 合法性检查和风险控制

应用软件与后台系统应具备合法性检查，通过签名验签等密码技术与后台系统进行双向认证，确保后台系统和应用软件的合法性，并设置超时时间。

### 密钥安全要求

出码应用机构申请的签发公钥证书最长有效期不得超过1天，应保证密钥定期更新。

受理终端验签时，根据证书编号选择对应根证书进行验签。

### 支付安全

用户支付过程中涉及的安全要求如下：

a. 二维码具备分钟级时效性，并且时效性具备动态调整能力；

b. 每个用户只可单终端登录，新终端登录旧终端自动下线；

c. 限制二维码连续生码次数，次数可动态配置，超过限制需要验证用户身份合法性；

d. 更换设备登陆，需要验证用户身份的合法性；

e. 二维码应每分钟自动更新；

f. 支付过程中应保证相关设备及系统安全。

g. 相同二维码同一机具尽可刷一次。

### 用户安全

客户端应验证用户的身份，可采用如下方式进行验证：

a. 用户提供验证信息，例如：客户端密码或口令等；

b. 用户提供所持设备的验证，例如：手机动态验证码，令牌等。

各业务管理平台建设过程中，应该做到用户敏感信息（如用户密码，证件号，银行卡号等）加密存储，掩码展示。严格控制用户信息安全不外泄，用户信息下载等权限，使用RBAC模式设计管理系统权限。系统间传递用户信息时加密传输，落地后解密，存储时加密。

# 受理终端性能要求

## 通用要求

二维码与刷卡部分必须分开。二维码扫码隔离直线距离不少6厘米。

应保证在二维码数据图像旋转、不规则变形、图像亮度变化、局部污损等各种复杂情况下，可准确识读，并具有较强的自动纠错能力。

## 存储

终端应该存储至少1000条交易记录，存储容量应不低于300KB。安全存储机具自身程序、平台证书、交易数据等参数。且确保机具断电这些数据不丢失。

## 通信

具备无线通信模块如 2G/3G/4G，如果是地铁闸机应具备 WLAN 端口，支持接入局域网、 互联网，并支持二维码机构密钥更新下载。

终端应能够准实时将用户扫码行为同步到服务器端。

## 时钟

具备高精度时钟模块，并可进行精确授时，应保证正常使用时两次授时期间时间误差不 能大于 2 秒。

## 二维码读取器

### 一般要求

应支持识别二进制编码格式的二维码，支持识别旋转、倾斜、偏转的二维码，并可以通 过 USB-HID 方式对二维码进行读取。

### 读取与计算时间

应在 200ms 内完成二维码读取与验证。

### 编码方式

应支持QR Code等常用码制。

### 读取精确度

可支持识别旋转、倾斜、偏转的二维码。

## 终端监控与管理

应具备远程管理能力，远程监测终端心跳、终端远程进行软件升级、机构证书下载与更新、黑白名单下载与更新、能远程识别终端问题且具有应急处理能力。

# 手机客户端要求

## 存储

应保障用户公私钥、机构授权数据等信息安全，可采用敏感数据分段存储，且手机客户端程序应保证分段数据组合过程的编程逻辑的安全性。

## 手机号绑定

应要求用户使用手机号注册账号或绑定账号的安全手机，手机号绑定过程中需要验证短信码以确保绑定行为属于用户本人操作。

## 用户实名认证

接入应用系统应要求用户进行实名认证，获取用户的实名信息包括：姓名、身份证号、身份证有效期、身份证照片（正反面）等，且在身份证有效期截止前通知用户再次认证。

用户账号未进行实名认证的情况下，应停止向该账号提供支付交易或其他与个人信用相关的服务功能。

## 银行卡绑定

含有线上支付功能的接入应用系统应支持用户账号绑定用于金融支付的银行卡（含：储蓄卡、信用卡），银行卡绑定要求账号通过实名认证，绑定过程中应向金融机构系统核对银行卡信息并确认该卡属于用户本人名下，且通过短信码验证该银行卡在银行预留的手机号码。

# 支付交易性能要求

## 整体性能要求

应在用户扫描二维码消费后的9秒内完成支付扣款并收到支付成功消息的通知。

## 受理终端要求

受理终端应在二维码识读与验证成功（耗时不超过200ms）后即刻提示消费成功。

原则上应确保每笔二维码消费数据均在2秒内上送至受理终端后台。

## 受理终端后台要求

应确保收到的每笔二维码消费数据均在2秒内完成数据格式标准化处理并上送至虚拟卡交易平台。

## 虚拟卡交易平台要求

应确保收到的每笔二维码消费数据均在2秒内完成数据处理并上送至出码应用系统后台。

## 出码应用机构要求

应确保收到的每笔二维码消费流水均在3秒内完成扣款处理并向其下APP下发扣款成功通知。