ICS ×××

× ××

备案号：×××—×××

**DB61**

陕西省地方标准

DB61/×××-202X

城市轨道交通自动售检票系统

第7部分 密钥技术规范

（草稿）

202X-XX-XX发布 202X-XX-XX实施

陕西省市场监督管理局发布

目次

[1 范围 1](#_Toc4172)

[2 自动售检票系统密钥管理系统 1](#_Toc4500)

[2.1 系统架构 1](#_Toc11360)

[2.2 密钥类型 1](#_Toc17475)

[2.3 密钥管理 1](#_Toc14136)

[2.4 运行环境 2](#_Toc5167)

[2.5 性能要求 2](#_Toc27316)

[3 二维码乘车系统密钥管理系统 3](#_Toc12821)

[3.1 系统架构 3](#_Toc407)

[3.2 接口设计 3](#_Toc20182)

[3.3 密钥类型 4](#_Toc28088)

[3.4 密钥管理 4](#_Toc3939)

[3.5 密钥工作流程 5](#_Toc14552)

[4 人脸识别乘车系统密钥管理系统 6](#_Toc13515)

[4.1 系统架构 6](#_Toc11504)

[4.2 接口设计 7](#_Toc16820)

[4.3 密钥类型 8](#_Toc2109)

[4.4 密钥管理 8](#_Toc28889)

[4.5 密钥工作流程 8](#_Toc25165)

前 言

本文件按照GB/T 1.1—2020《标准化工作导则第1部分：标准化文件的结构和起草规则》给出的规则起草。

《城市轨道交通自动售检票系统》分为8个部分：

——城市轨道交通自动售检票系统 第1部分 总则

——城市轨道交通自动售检票系统 第2部分 业务规范

——城市轨道交通自动售检票系统 第3部分 技术规范

——城市轨道交通自动售检票系统 第4部分 通信数据接口规范

——城市轨道交通自动售检票系统 第5部分 编码规范

——城市轨道交通自动售检票系统 第6部分 读写器技术规范

——城市轨道交通自动售检票系统 第7部分 密钥技术规范

——城市轨道交通自动售检票系统 第8部分 人机界面规范

本部分由西安市轨道交通集团有限公司提出。

本部分由陕西省交通运输厅归口。

本部分起草单位：西安市轨道交通集团有限公司、方正国际软件系统有限公司、武汉小码联城科技有限公司、成都智元汇信息技术股份有限公司、上海华虹计通智能系统股份有限公司、中国软件与技术服务股份有限公司、广州地铁设计研究院股份有限公司。

本部分主要起草人：

本部分由西安市轨道交通集团有限公司负责解释。

本部分2010年首次发布，本次为首次修订。

联系信息如下：

单位：西安市轨道交通集团有限公司

电话：

地址：西安市凤城八路126号

邮编：710065

城市轨道交通自动售检票系统 第7部分 密钥技术规范

# 范围

本部分规定了城市轨道交通自动售检票系统、二维码乘车系统、人脸识别乘车系统密钥管理相关内容。

# 自动售检票系统密钥管理系统

## 系统架构

### 概述

自动售检票系统密钥管理系统应生成密钥卡片、管理密钥，并检查自动售检票系统的设备交易数据合法性。

### 主要功能

密钥管理系统应统一集中管理密钥为系统提供基础的密钥安全服务，包括密钥的生成、存储、下发、使用、备份、更新和销毁、认证ISAM卡、验证交易数据TAC码合法性。

## 密钥类型

### 概述

密钥管理系统的密钥卡类型应满足密钥的管理、传递、认证，离线、在线情况下的终端使用需要，应包含根密钥、主密钥、工作密钥和SAM卡密钥；其中根密钥是系统最初的原始密钥；分散加密根密钥后得到主密钥、工作密钥和SAM卡密钥；工作密钥不属于ISAM卡认证和TAC验证设备；SAM卡密钥不属于终端设备。

### 母卡和母卡传输卡

母卡和母卡传输卡安装于票卡发行设备，用于发行用户卡。

密钥管理系统应与加密机联机，制作母卡和母卡传输卡。

### SAM卡

SAM卡应安装在车站终端设备上，是用于用户卡消费、充值使用的密钥卡。

密钥管理系统应与加密机联机，制作SAM卡，包括ISAM卡、PSAM卡。

## 密钥管理

### 密钥生成

密钥生成设备应包含加密机、工作站、外部读写器，经安全加密机制并通过密码及加密算法生成业务所需的密钥卡及密钥认证卡，并将密钥保存到加密机中，应采用分级管理、梯级生成、下发的方式将密钥加密后传递给下一级。

密钥管理系统应须遵循国家密钥管理相关规定。

### 密钥存储介质

密钥存储介质应包含如下要求：

1. 密钥管理系统应将密钥存储在CPU智能卡中；
2. 根密钥和主密钥应存储在具有密钥导出功能的CPU智能卡中；
3. 工作密钥、SAM卡密钥应存储在不具有导出功能CPU智能卡中。

### 密钥算法

密钥算法应采用国密算法。

### ISAM卡认证

密钥管理系统应远程认证ISAM卡使用权限，控制合法ISAM卡获取工作权限，实时记录ISAM卡登陆情况，确保充值终端安全可靠运行。

### TAC验证

终端应上送交易数据TAC码，由ACC系统验证交易合法性。

### SAM卡管理

ACC应监控管理SAM卡的使用情况，并建立SAM卡ID与设备间对应关系，SAM卡管理应包含如下要求：

a）对应关系应作为对交易数据合法性的判断依据；

b）初次安装SAM卡，ACC系统应自动维护SAM卡和设备的对应关系；

c）当SAM卡与设备对应关系发生变化时，ACC应自动更新对应关系，并记录SAM卡变更事件。

### 安全事故对策

#### 2.3.7.1用户卡丢失、泄密或被复制

密钥系统应防止丢失、泄露密码和复制的用户卡继续使用。

#### 2.3.7.2ISAM卡丢失

密钥系统应防止丢失的ISAM卡继续使用。

#### 2.3.7.3母卡、传输卡丢失或泄密

母卡或传输卡丢失、泄密时，密钥管理系统应作废所有用户卡、SAM卡，并重新发行新的密钥。

#### 2.3.7.4认证服务器丢失

认证服务器应被严格保护，如认证服务器母卡和母卡认证卡同时丢失，所有用户卡和SAM卡片应全部作废，系统应发行新的密钥，用来替换丢失或者泄密的密钥版本。

## 运行环境

本系统应运行于Windows 7或以上版本操作系统中。

## 性能要求

密钥卡的读写时间应在1200ms以内。

# 二维码乘车系统密钥管理系统

## 系统架构

### 概述

二维码密钥管理应为应用系统提供密码设备集中管理、多层级密钥认证管理、透明密码运算、安全审计等密码安全服务，包括密钥的生成、更新、校验、删除、备份，层级管理及各级密钥的认证。

### 主要功能

在二维码支付应用中，应能通过在发卡机构、收单机构、证书管理中心加入加密机服务器，以保护各机构之间的请求信息和交易数据的机密性、完整性、真实性。各机构之间在添加加密机服务器硬件设备后，原有工作流程应不受影响，在进行信息请求与交易过程中，加密机服务器应通过加密、签名、信息验证保护信息数据。

密钥管理系统应兼容不同品牌、型号的硬件设备，可对硬件设备动态、实时管理，并提供安全、实时、连续的密钥管理和监控服务；应包含增加、启用、停用、删除硬件设备的功能。

密钥管理系统应提供便捷、安全的密钥管理、CA机构管理、业务日志审计、密钥统计、密钥归档、日志归档、配置信息管理、数据库模块、权限管理服务的二次开发接口。

## 接口设计

密钥管理系统密钥接口要求如表1所示：

表1密钥接口

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 接口名称：verifysignbyEY  功能：公钥验签 | | | | |
| 字段名称 | 类型 | 长度 | 可空 | 备注 |
| pubkey | String | 128 | 否 | 验签公钥 |
| data | String | N | 否 | 原始数据 |
| signData | String | N | 否 | 签名数据 |
| 返回参数： | | | | |
| 字段名称 | 类型 | 长度 | 可空 |  |
| errCode | String | 2 | 否 | 错误代码 |
| length | Int | N | 否 | 数据长度 |
| obj | Object | N | 否 | 返回数据 |
| 接口名称：signaturebyEW  功能：私钥签名 | | | | |
| 字段名称 | 类型 | 长度 | 可空 | 备注 |
| sm2Index | String | 2 | 否 | 密钥索引号 |
| key | String | N | 是 | 私钥 |
| data | String | N | 否 | 原始数据 |
| 返回参数： | | | | |
| 字段名称 | 类型 | 长度 | 可空 |  |
| errCode | String | 2 | 否 | 错误代码 |
| length | Int | N | 否 | 数据长度 |
| obj | Object | N | 否 | 返回数据 |

## 密钥类型

密钥类型应分为根密钥、机构密钥、用户密钥，可进行三级认证，应使用国密算法。

根密钥应为三级认证的第一级认证，包括公钥及私钥。公钥应按规范做成证书定时下发到闸机中，私钥应保存在加密机中。

机构密钥应为三级认证的第二级认证，为不同的发码机构独有，用于区分不同发码机构。公钥证书应放入二维码结构中进行认证，私钥应保存在加密机中。

用户密钥应为三级认证的第三级认证，密钥应保存在用户的终端设备中，并应定时更新用户的密钥保证数据的安全。

## 密钥管理

### 收单机构接收公钥证书

证书管理中心与收单机构双方应约定用于通信保护的非对称密钥对，并交换公钥，证书管理中心应将生成的根公钥证书发送至收单机构。

### 发卡机构申请公钥证书

证书管理中心与发卡机构双方应约定用于通信保护的非对称密钥对，并交换公钥；发卡机构申请公钥证书时应向证书管理中心上传公钥证书请求文件，证书管理中心验证通过后应将生成的根公钥证书发送至发卡机构。

### 文件结构

发卡机构向证书管理中心发送的公钥证书请求文件内容要求如表2所示：

表2公钥证书请求文件内容

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 字段格式 | 长度 | 可空 | 备注 |
| 记录头 | b | 1 | 否 | 0x23 |
| 服务标识 | b | 4 | 否 | 标识一个交通服务，将相应应用的私有应用标识扩展（PIX），右补16进‘0’构成。‘01010000’=交通电子现金应用 |
| 证书格式 | b | 4 | 否 | 16进制‘02’ |
| 发卡机构代码 | Cn8 | 4 | 否 | 发卡机构代码，由证书管理中心统一分配 |
| 证书失效日期 | N4 | 2 | 否 | 月和年（MMYY），在该月最后一天证书失效 |
| 记录号 | N6 | 3 | 否 | 发卡机构公钥证书记录号 |
| 发卡机构公钥签名算法标识 | b | 1 | 否 | 发卡机构公钥签名算法。  ‘04’（16进制）：SM2 |
| 发卡机构公钥加密算法标识 | b | 1 | 否 | 发卡机构公钥签名算法。  ‘04’（16进制）：SM2 |
| 公钥参数标识 | b | 1 | 否 | 用于标识椭圆曲线参数。默认为16进制‘00’ |
| 发卡机构公钥模长 | b | 1 | 否 | 33byte |
| 发卡机构公钥 | b | 33 | 否 | SM2算法标识椭圆曲线上的一个点，采用SM2中点压缩方式进行计算 |
| 数字签名 | b | 64 | 否 | 发卡机构使用其私钥对本序号1-11数据计算的SM2签名r||s |

证书管理中心私钥对发卡机构公钥进行签名的公钥签名文件内容如表3所示：

表3公钥签名文件内容

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 字段格式 | 长度 | 可空 | 备注 |
| 记录头 | b | 1 | 否 | 0x24 |
| 服务标识 | b | 4 | 否 | 标识一个交通服务，将相应应用的私有应用标识扩展（PIX），右补16进制‘0’构成。‘01010000’=交通电子现金应用 |
| 中心CA公钥索引 | b | 1 | 否 | 证书管理中心CA系统用来签发发卡机构公钥证书的公钥索引 |
| 证书格式 | b | 1 | 否 | 十六进制‘12’ |
| 发卡机构代码 | Cn8 | 4 | 否 | 发卡机构代码，由证书管理中心统一分配 |
| 证书失效日期 | N4 | 2 | 否 | 月和年（MMYY），在该月最后一天证书失效 |
| 证书序列号 | b | 3 | 否 | 由根CA分配给这张证书唯一二进制数 |
| 发卡机构公钥签名算法标识 | b | 1 | 否 | 发卡机构公钥签名算法。  ‘04’（16进制）：SM2 |
| 发卡机构公钥加密算法标识 | b | 1 | 否 | 发卡机构公钥签名算法。  ‘04’（16进制）：SM2 |
| 公钥参数标识 | b | 1 | 否 | 用于标识椭圆曲线参数。默认为16进制‘00’ |
| 发卡机构公钥长度 | b | 1 | 否 | 标识发卡机构公钥的字节长度 |
| 发卡机构公钥 | b | 33 | 否 | SM2算法标识椭圆曲线上的一个点 |
| 数字签名 | b | 64 | 否 | 发卡机构使用其私钥对本序号1-11数据计算的SM2签名r||s |

## 密钥工作流程

### 数据加密

密钥系统应对二维码数据加密，并保证所有密钥存储的安全性。数据加密应包含如下要求：

a）密钥系统应使用机构密钥和用户密钥对二维码数据进行加密。

b）二维码数据应包括发卡机构公钥证书、二维码业务数据、发卡机构授权签名数据以及支付账户用户私钥签名数据。

数据加密流程如图1所示：



图1数据加密流程

### 受理终端验签

终端应使用密钥系统提供的公钥证书验证二维码的合法性和有效性。

# 人脸识别乘车系统密钥管理系统

## 系统架构

### 概述

人脸识别乘车系统应对密钥进行统一集中管理，应为人脸终端子系统、人脸对比子系统、人脸后台管理系统子系统提供基础的密钥安全服务。应加密管理人脸识别终端软件、内网传输数据、公网传输数据、人脸图片信息。系统应包含人脸识别终端软件密钥、内网数据传输公私钥、公网数据传输公私钥、人脸图片和信息加密密钥。

### 主要功能

人脸密钥管理的密钥生成、存储、下发、备份、恢复、加密、解密、签名、验签、安全审计功能，应使用硬件密码设备统一管理，为其它子系统或外部系统平台提供密钥服务。

密钥管理系统应兼容不同品牌、型号的硬件设备，可对硬件设备动态、实时管理，并提供安全、实时、连续的密钥管理和监控服务；系统应包含增加、启用、停用、删除硬件设备功能；系统应对工作密钥提供安全管理服务，并开放接口服务。

人脸识别乘车系统密钥管理系统架构如图2所示：

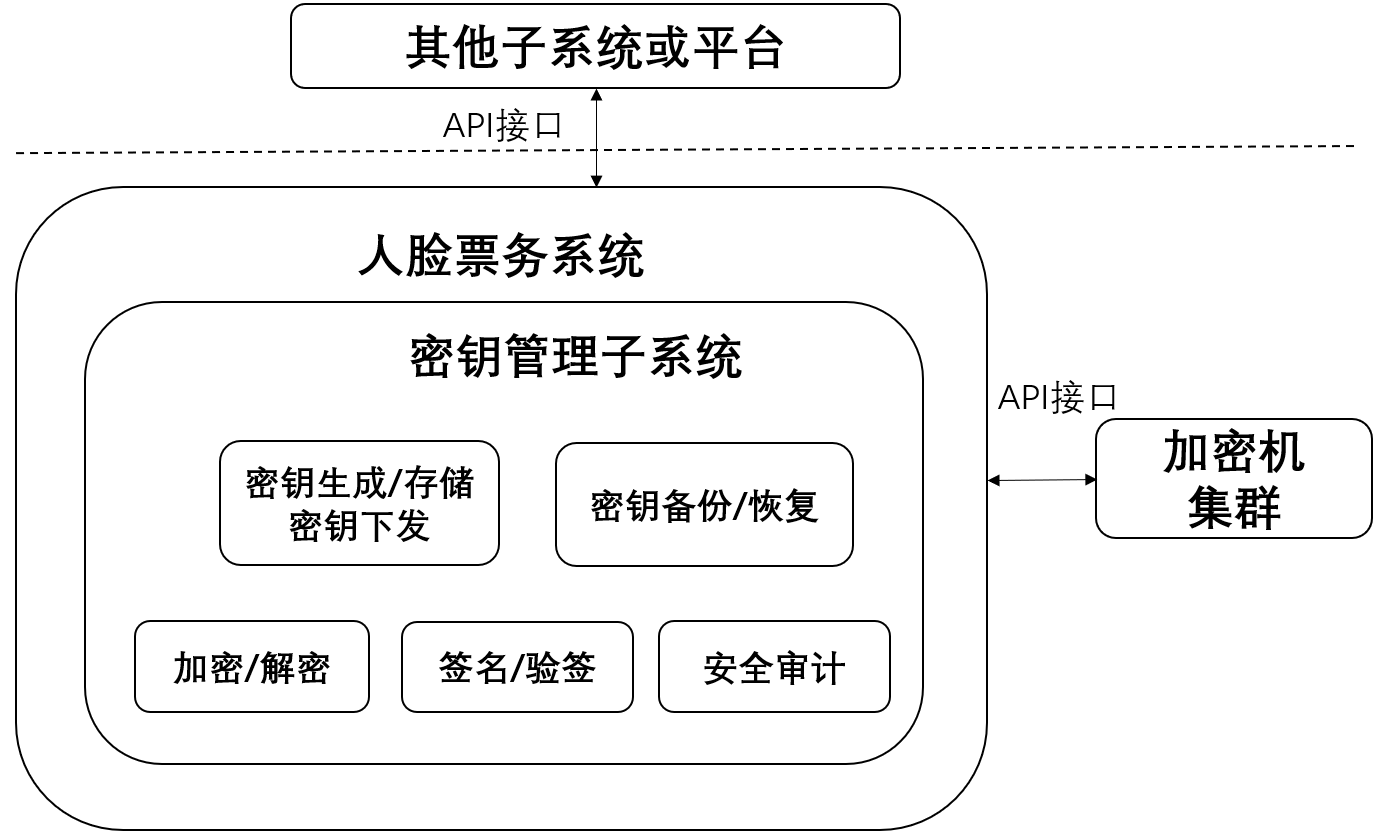


图2人脸识别乘车系统密钥管理系统架构

## 接口设计

密钥管理系统人脸图片加密请求报文如表4所示：

表4人脸图片加密请求报文

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 类型 | 必填 | 说明 |
| stationNo | String | Y | 站点编号 |
| image | String | Y | 人脸图片明文(base64) |

密钥管理系统人脸图片加密应答报文如表5所示：

表5人脸图片加密应答报文

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 类型 | 必填 | 说明 |
| code | String | Y | 响应编码 |
| msg | String | Y | 响应信息 |
| data | Object | Y | 响应数据 |
| data.image | String | N | 人脸图片密文(base64) |

密钥管理系统人脸图片解密请求报文如表6所示：

表6人脸图片解密请求报文

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 类型 | 必填 | 说明 |
| stationNo | String | Y | 站点编号 |
| image | String | Y | 人脸图片密文(base64) |

密钥管理系统人脸图片解密应答报文如表7所示：

表7人脸图片解密应答报文

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 类型 | 必填 | 说明 |
| code | String | Y | 响应编码 |
| msg | String | Y | 响应信息 |
| data | Object | Y | 响应数据 |
| data.image | String | N | 人脸图片明文(base64) |

## 密钥类型

人脸识别乘车系统密钥应分为人脸识别终端软件密钥、内网数据传输公私钥、公网数据传输公私钥、人脸图片加密密钥，并应使用国密算法。

## 密钥管理

### 报文的签名和验签

为防止业务各方之间交易过程中报文信息被恶意篡改，业务各方之间的交易报文应采用签名机制，以保证交易的安全性。交易请求方应实现对请求参数数据的签名，交易服务端应根据请求参数，对签名进行验证，拒绝签名不合法的请求。

### 内网数据传输加密

密钥系统应加密处理内网传输数据。

内网数据传输公私钥应用于对内网传输的数据进行数字签名。应采用非对称加密公私钥(如RSA)，私钥应用于对报文进行签名，公钥应用于对报文进行验签。私钥应保存到加密机，公钥应保存到本地。

### 公网数据传输加密

密钥系统应加密处理公网传输数据。

公网数据传输公私钥应用于对公网传输的数据进行安全加密。应采用非对称加密公私钥，对报文应进行加密传输。私钥应保存到加密机，公钥应保存到本地。

## 密钥工作流程

密钥系统应加密人脸图片信息，并保证人脸图片信息的安全性，生成的密钥应存储在数据库中，加解密过程应使用对应的密钥。

人脸图片加密密钥应用于对人脸图片进行安全加密。采用对称加密算法加密人脸图片信息，密钥应存储在数据库中。

人脸识别乘车系统数据加解密、分发流程如图3所示：

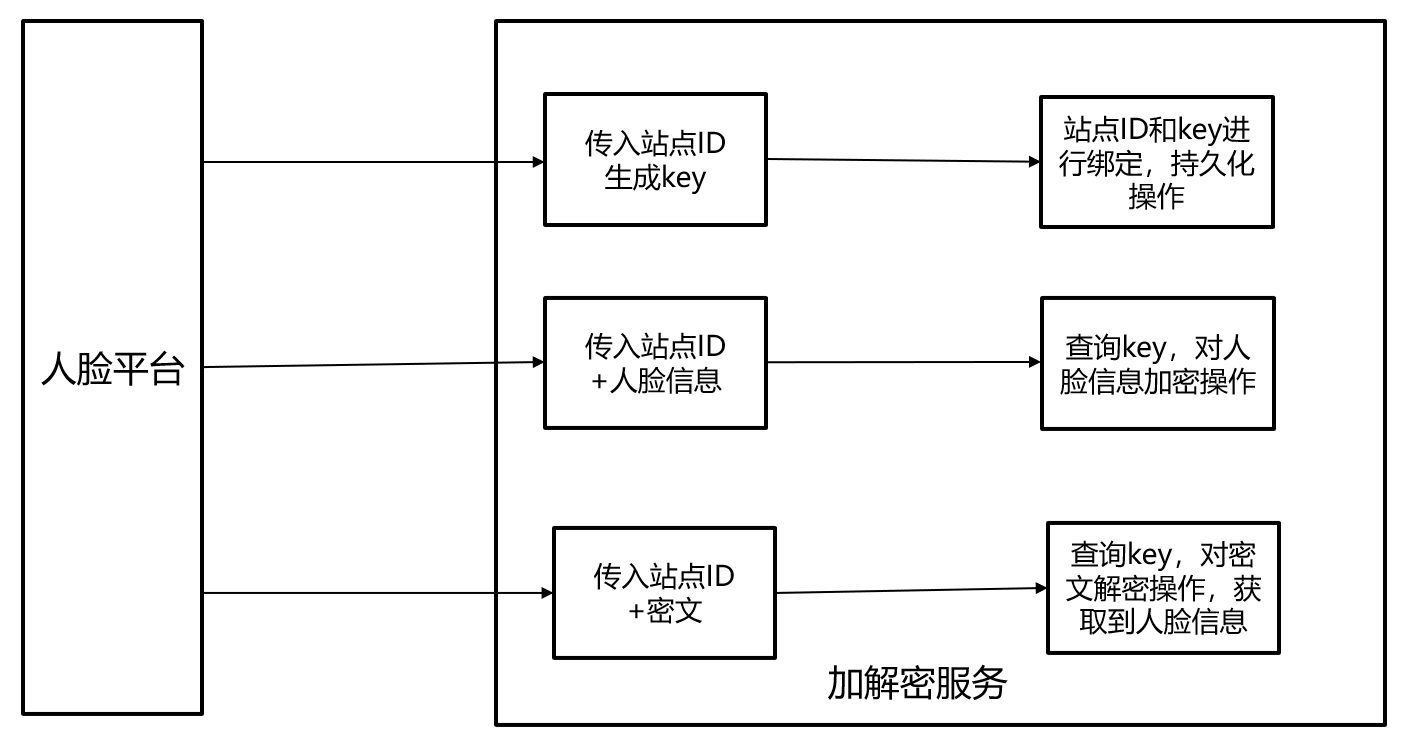


图3 数据加解密、分发流程