|  |  |
| --- | --- |
| ICS | 35.080 |
| CCS | L77 |

|  |
| --- |
| 3413 |

宿州市地方标准

DB 3413/T XXXX—2022

居民服务一卡通服务平台 接入技术规范

Resident service card service platform data coding specification

2022 - XX - XX发布

2022 - XX - XX实施

宿州市市场监督管理局  发布

1. 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》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由宿州市人力资源和社会保障局提出。

本文件由宿州市人力资源和社会保障局归口。

本文件起草单位：宿州市人力资源和社会保障局、宿州市数据资源管理局、宿州市交通运输局、宿州市公共交通有限公司、宿州市文化和旅游局。

本文件主要起草人：刘锋、程松、崔龙、张梦龙、朱俊臣、高庆涛、高元元、蒋春峰、付瑶、徐珂。

居民服务一卡通服务平台 接入接入规范

* 1. 范围

本文件规定了接入居民服务一卡通服务平台（以下简称一卡通平台）的基本要求、接入流程、接入方法和接入安全控制。

本文件适用于接入一卡通平台，开展与一卡通平台应用相关的软件设计和开发。

* 1. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 28452 信息安全技术 应用软件系统通用安全技术要求

GB/T 32918（所有部分） 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 35273-2020 信息安全技术 个人信息安全规范

LD/T 92 社会保险管理信息系统指标集与代码

ZWFW C0131-2018 国家政务服务平台统一身份认证隐私保护要求

* 1. 术语和定义

下列术语和定义适用于本文件。

居民服务一卡通服务平台 resident service all in one card service platform

遵循国家人力资源和社会保障部社会保障卡行业标准及相关文件要求，由本行政区域政府主管部门建设的，承担一卡通平台的管理、应用、接入、共享、协同功能的信息系统，负责一卡通平台相关接入方的应用系统接入，负责与省级、区域级、国家级平台的联动和协同。

管理方 management party

负责一卡通平台的主管部门。

接入方 access party

开通或支持一卡通平台应用的接入机构，包括政府机关、企事业单位、社会组织等。

应用系统 application system

接入方自有的信息化业务应用系统。

业务场景 business scenario

接入方向社会公众提供的服务项目。

* 1. 基本要求
     1. 基本技术要求

应用系统接入一卡通平台，应具备以下基本技术要求：

1. 具有固定的接入IP地址；
2. 以一卡通平台分配的用户ID、用户密码接入身份验证；
3. 软件设计应符合GB/T 28452的相关规定；
4. 系统安全防护能力应符合GB/T 22239中的安全等级保护三级的相关规定。
   * 1. 接入网络类型

应用系统可通过以下网络接入一卡通平台：

1. 国家电子政务外网；
2. 人力资源和社会保障业务专网；
3. 互联网。
   1. 接入流程
      1. 应用接入流程

一卡通平台的应用接入，由接入方和管理方协同开展，包括申请、测试和上线三个步骤。接入流程见图1。

接入方

管理方

开始

接入申请

接入审核

分配账号

接入方线上信息填报审核

接入信息审核

测试环境授权

上线审批

生产环境授权

应用测试

上线申请

上线启用

结束

申 请

测 试

上 线

1. 应用接入流程
   * 1. 接入申请

接入方申请接入应填报接入信息，管理方审核通过完成接入申请。

1. 接入方按管理方发布的申请表格式和要求，提交对接申请材料，包括接入IP、联系人、联系方式、机构信息、对接内容等基础信息；
2. 管理方审核接入方申请材料，审核通过后在一卡通平台分配账户信息和测试密钥。审核不通过通知接入方重新提交；
3. 接入方收到账号后，按一卡通平台在线填报要求，线上填报网点、设备、应用系统等运行信息及参数；
4. 管理方对接入方填报信息进行审核，并配置测试环境。
   * 1. 接入测试

接入测试形成应用接入的相关配置，完成应用系统改造及接入方、管理方联调联测。

1. 管理方通过对接入方的接入审核，根据接入方填报内容配置相关参数，对接入方授权开放测试环境；
2. 应用系统按照对接规范进行开发，配置账户信息和测试密钥。管理方和接入方双方开展联调测试。
   * 1. 上线启用

上线启用完成应用系统在生产环境的启用部署，开通服务。

1. 测试通过后，接入方形成测试报告，向管理方提交上线申请；
2. 管理方审核上线申请，在一卡通平台生产环境分配正式密钥；
3. 接入方接收到正式密钥在生产环境完成配置上线对接。
   1. 接口要求
      1. 基本要求

一卡通平台提供标准的应用接口，按照国家安全标准进行加密传输，供应用系统调用。接入方应填写的接入基本信息，通过以下方式接入一卡通平台：HTTP接入、H5页面接入。应用接入基本信息见表1 。

1. 应用接入基本信息

| 信息 | 说明 |
| --- | --- |
| 单位名称 | 应用申报单位对应本单位社会统一信用代码的正式全称 |
| 社会统一信用代码 | 应用申报单位登记的有效社会信用代码 |
| 服务事项 | 应用接入与一卡通服务目录对应的服务事项 |
| 应用场景 | 向社会公众提供服务的简要说明 |
| 申请单位联系人与联系方式 | 联系人姓名、电话、邮箱等 |
| 业务系统IP | 应符合4.2要求范围的固定IP地址 |
| 应用网点信息 | 设备部署的网点信息 |
| 应用设备 | 通过什么设备进行调用服务 |

* + 1. HTTP接入方式技术要求

1. 采用HTTP/1.1协议，使用POST方法提交请求，请求包含身份令牌（access\_token）参数；
2. 请求及返回报文为JSON格式，字符编码为UTF-8，格式应符合LD/T 92的相关规定；
3. 应用系统应按照备案的IP地址接入。
   * 1. H5页面接入方式技术要求
4. 采用HTTP/1.1协议，使用GET方法提交请求；
5. 请求及返回报文字符编码为UTF-8，格式应符合LD/T 92的相关规定；
6. 应用系统拼接URL地址及携带参数，发起GET请求，调用一卡通平台H5页面。参数说明见7.2；
7. 应用系统应按照备案的IP地址接入。
   1. 接入方法
      1. HTTP方式接入

API方式实现数据层面交互。通过该方式进行对接，应用系统获取所需要的数据，根据自身业务逻辑，开发相应页面，实现数据展示及业务办理。

API接入应符合HTTP restful风格。签名相关的公共参数统一放在请求HTTP的header中。HTTP的签名设定见附录A。



输入参数见表2。

1. API请求参数

| 参数 | 是否必填 | 类型 | 说明 |
| --- | --- | --- | --- |
| ip | 是 | 字符串 | 应用服务IP |
| port | 是 | 字符串 | 应用服务端口 |
| sceneCode | 是 | 字符串 | 应用场景编码 |
| serviceCode | 是 | 字符串 | 接口服务编码 |
| version | 是 | 字符串 | 接口服务版本 |
| accessToken | 是 | 字符串 | 服务调用凭证令牌 |
| token | 否 | 字符串 | 调用者信息凭证（无连续访问不传） |
| flag | 否 | 字符 | 0：不保留访问信息，1：保留访问信息 |

* + 1. H5应用接入

接入方采用基于HTTP协议的URL通信方式，发起HTTP请求，将经过统一算法进行加密及签名的参数串提交到一卡通平台，一卡通平台对相关参数进行解析核验，核验通过后返回对应的H5应用资源。核验不通过时向接入方提示错误信息。

* + - 1. 数据交互说明

1. 通过互联网进行访问；
2. 接入方按照一卡通平台H5标准规范拼接URL地址及携带参数；
3. 由一卡通平台H5解析参数，对应用进行身份鉴权，应用访问鉴权。鉴权通过后返回所请求的H5资源，用于在接入方应用端展示。



约定：所有请求的charset必须为UTF-8。输入参数见表3。

1. H5请求参数

| 参数 | 是否必填 | 类型 | 说明 |
| --- | --- | --- | --- |
| ip | 是 | 字符串 | 应用服务IP |
| port | 是 | 字符串 | 应用服务端口 |
| sceneCode | 是 | 字符串 | 应用场景编码 |
| serviceCode | 是 | 字符串 | 接口服务编码 |
| version | 是 | 字符串 | 接口服务版本 |
| Access\_token | 是 | 字符串 | 服务调用凭证令牌 |
| token | 否 | 字符串 | 调用者信息凭证（无连续访问不传） |
| security | 是 | 字符串 | 加密串 |
| \_api\_signaturea | 是 | 字符串 | 访问签名a |
| a访问签名见附录B。 | | | |

* 1. 接入安全控制
     1. 身份验证

接入方身份验证基于IP白名单和token访问令牌，验证通信身份的合法性。通信报文添加时间戳校验，验证应用访问的唯一性。

1. 应用系统使用一卡通平台分配的用户ID和密码，申请调用获取身份令牌；
2. 一卡通平台对应用系统的IP、用户ID和密码进行身份校验，通过后给应用系统分配token访问令牌。
   * 1. 传输加密

传输加密使用标准国密对称加密SM4算法，对服务接口报文进行全程传输加密。

安全鉴权采用请求签名机制，签名采用国密非对称SM2算法，SM2算法应符合GB/T 32918（所有部分）的相关规定，双方以安全方式存储接口鉴权密钥，同时公私钥传输过程中需加密，进一步保障安全性。

密钥由管理方统一生成和分配管理。

* + 1. 加密传输过程
       1. 应用系统

1. 应用系统对访问参数经MD5压缩加密生成签名摘要M1，并使用应用系统的非对称SM2私钥进行签名，生成A1；并将A1放置head中传输，key为SIGN\_KEY；
2. 应用系统随机生成对称SM4密钥随机串B，并将访问入参进行加密生成C，同时将B使用一卡通平台提供的SM2公钥进行加密,生成D1；并将D1放置head中传输，key为ENCRYPT\_KEY；
3. 向管理方发起访问，其中服务访问head包括加密通信数据D1、签名A1和报文体C。
   * + 1. 一卡通平台
4. 一卡通平台用SM2私钥对D1进行解密，获取应用系统随机生成对称SM4密钥随机串B；
5. 通过B对加密通信信息C进行解密，获取到访问入参明文；
6. 用获取到的入参明文进行MD5压缩加密，生成M2；
7. 一卡通平台用应用系统提供的非对称SM2公钥对A1进行解密，并与M2进行比对验签；
8. 验签通过，说明通信信息中途没有被篡改，信息传输完整，签名验证通过，可正常对访问响应处理。
   * 1. 个人隐私保护

应用系统从一卡通平台获取的个人信息数据，应按照个人信息保护法要求开展个人隐私保护。 应用系统需提供个人信息展示功能的，应按照ZWFW C0131-2018中6.4规定的要求进行数据脱敏，未脱敏信息不应直接展示。应用系统需向第三方应用系统提供个人信息共享功能的，应按照GB/T 35273-2020的要求进行数据保护处理，前置本人授权同意环节。

1. 姓名、社会保障号等二级以上隐私数据，按要求脱敏范围不少于50%。

姓名脱敏：\*\*红，展示最后1-2个汉字，其他隐藏。

社会保障号脱敏：\*\*\*\*\*\*\*\*\*\*\*\*\*\*4321，展示最后4位，其他隐藏。

2. （资料性）  
   HTTP访问签名参数说明
   1. API访问签名参数表

| 参数 | 是否必填 | 类型 | 说明 |
| --- | --- | --- | --- |
| ENCRYPT\_KEY | 是 | 字符串 | SM2加密SM4密钥所得 |
| SIGN\_KEYa | 是 | 字符串 | 访问报文参数MD5签名a |
| a访问报文参数MD5签名见表A2。 | | | |

* 1. 访问报文参数MD5签名SIGN\_KEY参数表

| 参数类型 | 名称 | 含义 | 类型 | 必填 | 备注 |
| --- | --- | --- | --- | --- | --- |
| 公共参数 | deviceSerial | 设备序列号 | string | 是 | 设备序列号 |
| timestamp | 时间戳 | number | 是 | 调用时间戳 |
| 业务参数 | data | 参数 | json | 是 | 业务参数，如姓名、身份证号、社保号等 |

1. （资料性）  
   H5访问签名参数说明
   1. 访问签名参数\_api\_signature参数表

| 参数类型 | 名称 | 含义 | 类型 | 必填 | 备注 |
| --- | --- | --- | --- | --- | --- |
| 公共参数 | deviceSerial | 设备序列号 | string | 是 | 设备序列号 |
| timestamp | 时间戳 | number | 是 | 调用时间戳 |
| 业务参数 | data | 参数 | json | 是 | 业务参数，如姓名、身份证号、社保号等 |

