**安全服务平台接口定义**

**智控美信信息技术有限公司**

**2016年06月**

版本控制

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **版本** | **时间** | **编制/修订** | **审核** | **批准** | **修改说明** |
| 0.9 | 2016/6/6 | 张立利 |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

目 录

[1 前言 1](#_Toc453490765)

[1.1 目的 1](#_Toc453490766)

[1.2 范围 1](#_Toc453490767)

[1.3 内容提要 1](#_Toc453490768)

[2 安全服务平台API接口 1](#_Toc453490769)

[2.1 服务端API初始化连接接口 1](#_Toc453490772)

[2.2 服务器端登录口令 2](#_Toc453490773)

[2.2.1 认证初始化接口 3](#_Toc453490774)

[2.2.2 登录口令验证 3](#_Toc453490775)

[2.2.3 登录口令转换 4](#_Toc453490776)

[2.3 动态码接口 5](#_Toc453490777)

[2.3.1 时间型动态码生成 5](#_Toc453490778)

[2.3.2 时间型动态码校验 6](#_Toc453490779)

[2.4 信息数据保护接口 7](#_Toc453490780)

[2.4.1 数据加密接口 7](#_Toc453490781)

[2.4.2 数据解密接口 8](#_Toc453490782)

[2.5 PIN码保护接口 9](#_Toc453490783)

[2.5.1 产生PIN OFFSET 9](#_Toc453490784)

[2.5.2 验证PIN 10](#_Toc453490785)

[2.6 客户端接口 12](#_Toc453490786)

[2.6.1 认证接口 12](#_Toc453490787)

[2.6.2 Pin保护接口 12](#_Toc453490788)

1. 前言
   1. 目的

本文档针对统一认证接口进行说明，描述安全服务平台和应用系统交互的上送和返回字段，为开发设计人员提供依据。

* 1. 范围

预期读者：调用安全服务平台的关业务人员、技术人员、测试人员等项目相关人员。

* 1. 内容提要

本文为易民生系统调用的接口功能需求文档，内容包括项目在开发过程中所涉及到登录口令转换、登录口令验证、PIN码保护接口、动态码接口、以及加解密接口等。

1. 安全服务平台API接口

## 服务端API初始化连接接口

**构造方法：**

InfoholdHandle (String ConnectString, String gunionIDOfEsscAPI,int timeOut)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **接口名称** | | InfoholdHandle | | | | |
| **序号** | | **参数名称** | **中文名称** | **类型** | **备注** | **是否必输** |
| **输入参数：** | | | | | | |
| 1 | ConnectString | | 连接安全服务平台的url | String | ip及端口号，**易民生系统调用时该值为： "110.76.186.49:2181,110.76.186.49:2182,110.76.186.49:2183"** | Y |
| 2 | appId | | 应用ID | Int | 安全服务平台为每个应用分配的唯一应用ID，**易民生系统调用时该值为：YM** | Y |
| 3 | timeOut | | 连接超时时间 | Int | **易民生系统调用时该值为：8000** | Y |
| **返回值：** | | | | | | |
| 无 | | | | | | |

**调用实例：**

|  |
| --- |
| **String ConnectString = "110.76.186.49:81";**  **String appId= "YM";**  InfoholdHandle ***handle* = new** InfoholdHandle **(ConnectString, appId, 8000);**  **try {**  InfoholdVerPassword ***pwdApi*** = new InfoholdVerPassword(***handle***);//登录口令API  **String randomNum = *pwdApi*. InfoholdAuthInit();**  **} catch (Exception e) {**  **e.printStackTrace();**  **}** |

## 服务器端登录口令

**构造方法：**

InfoholdHandle InfoholdPassWordAPI (handle)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **接口名称** | | InfoholdPassWordAPI | | | | | |
| **序号** | | **参数名称** | **中文名称** | **类型** | | **备注** | **是否必输** |
| **输入参数：** | | | | | | | |
| 1 | handle | | 连接安全服务平台的handel | | InfoholdHandle |  | Y |
| **返回值：** | | | | | | | |
| 无 | | | | | | | |

### 认证初始化接口

**函数接口：**

String InfoholdAuthInit（int lenth）throws Exception

**接口说明：**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **接口名称** | InfoholdAuthInit | | | | | | | | | |
| **序号** | **参数名称** | | | **中文名称** | | **类型** | **备注** | | | **是否必输** |
| **输入参数：** | | | | | | | | | | |
| 1 | | lenth | 随机数长度 | | Int | | | **易民生系统调用时中该值为16** |  | |
| **返回值：** | | | | | | | | | | |
| 1 |  | | | 随机数 | | String |  | | |  |

### 登录口令验证

**函数接口：**

boolean InfoholdVerifyLoginPwd(String userID,String encPwd, String randomNum, String pwdHash)throws Exception

**接口说明：**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **接口名称** | | | InfoholdVerPassword | | | | |
| **序号** | | | **参数名称** | **中文名称** | **类型** | **备注** | **是否必输** |
| **输入参数：** | | | | | | | |
| 1 | userID | | | 用户唯一标识 | String | 用户在管理系统中的唯一标识（该标识不可修改） | Y |
| 2 | encPwd | | | 密码密文 | String | **客户端登录认证接口**输出的密码密文 | Y |
| 3 | randomNum | | | 随机数 | String | **认证初始化接口**获取的随机数 | Y |
| 4 | pwdHash | | | 口令HASH值 | String | **登录口令转换**接口获取的口令Hash | Y |
| **返回值：** | | | | | | | |
| 1 | |  | |  | Boolean | true正确，false错误 | Y |

### 登录口令转换

**函数接口：**

String InfoholdTransLoginPwd(String userID,String encPwd, String randomNum)throws Exception

**接口说明：**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **接口名称** | | | infoholdTransPassword | | | | | |
| **序号** | | | **参数名称** | **中文名称** | **类型** | **备注** | **是否必输** | |
| **输入参数：** | | | | | | | | |
| 1 | userID | | | 用户唯一标识 | String | 用户在管理系统中的唯一标识（该标识不可修改） | | Y |
| 2 | encPwd | | | 密码密文 | String | **客户端登录认证接口**输出的密码密文 | | Y |
| 3 | randomNum | | | 随机数 | String | **认证初始化接口**获取的随机数 | | Y |
| **返回值：** | | | | | | | | |
| 3 | |  | | 口令HASH值 | String | BCD编码的字符串 |  | |

## 服务端PIN保护接口

**构造方法：**

InfoholdDisposePinAPI (InfoholdHandle handle)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **接口名称** | | InfoholdCipherAPI | | | | | |
| **序号** | | **参数名称** | **中文名称** | **类型** | | **备注** | **是否必输** |
| **输入参数：** | | | | | | | |
| 1 | handle | | 连接安全服务平台的handel | | InfoholdHandle |  | Y |
| **返回值：** | | | | | | | |
| 无 | | | | | | | |

### 产生PIN OFFSET

**函数接口**

String InfoholdGenPinOffset(String encPin,String zpkName,String pvkName,String account1,String account2,String random)throws Exception

**接口说明：**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **接口名称** | | | InfoholdEncPinByPVK | | | | |
| **序号** | | | **参数名称** | **中文名称** | **类型** | **备注** | **是否必输** |
| **输入参数：** | | | | | | | |
| 1 | encPin | | | 密文PIN | String | Pin密文。  **调用客户端 PIN保护接口，输出的密文PIN；** | Y |
| 2 | zpkName | | | Zpk名称 | String | 转换密钥名称.  **易民生系统调用该接口时，该值为YM.00.zpk** | Y |
| 3 | pvkName | | | 存储密钥名称 | String | PIN存储加密密钥名称.  **易民生系统调用该接口时，该值为YM.00.pvk** | Y |
| 4 | account1 | | | 账号1 | String | 16到19位的数字；**易民生系统调用该接口时，值为16个0** | Y |
| 5 | account2 | | | 账号2 | String | 16到19位的数字；**易民生系统测试阶段，值为16个0，后期为虚拟账号。** | Y |
| 6 | random | | | 随机数 | String | 随机数。  **生成pin密文时使用的随机数。** | Y |
| **返回值：** | | | | | | | |
| 1 | |  | | Pin密文 | String |  | Y |

### 验证PIN

**函数接口：**

boolean InfoholdVerifyPin(String encPin,String zpkName,String pvkName,String account1,String account2,String random,String pinOffset)throws Exception

**接口说明：**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **接口名称** | InfoholdVerifyPIN | | | | | | | |
| **序号** | **参数名称** | **中文名称** | | **类型** | **备注** | | | **是否必输** |
| **输入参数：** | | | | | | | | |
| 1 | encPin | 密文PIN | | String | Pin密文。  **调用客户端 PIN保护接口，输出的密文PIN；** | | | Y |
| 2 | zpkName | Zpk名称 | | String | 转换密钥名称.  **易民生系统调用该接口时，该值为YM.00.zpk** | | | Y |
| 3 | pvkName | 存储密钥名称 | | String | PIN存储加密密钥名称.  **易民生系统调用该接口时，该值为YM.00.pvk** | | | Y |
| 4 | account1 | 账号1 | | String | 16到19位的数字；**易民生系统调用该接口时，值为16个0。** | | | Y |
| 5 | account2 | 账号2 | | String | 16到19位的数字；**易民生系统测试阶段，值为16个0，后期为虚拟账号。** | | | Y |
| 6 | random | 随机数 | | String | 随机数。  **生成pin密文时使用的随机数。** | | |  |
| 7 | pinOffset | pinOffset | | String | 调用产生pin Offset接口生成 | | | Y |
| **返回值：** | | | | | | | | |
| **1** |  | | boolean | | | true正确，false错误 | Y | |

Y

## 客户端JS加密控件

### 登录认证

该接口使用JS实现，业务系统在其jsp页面中调用。方法名为：

RSAUtils.encryptedPassword(random,pwd,modulus, exponent)

调用时必须引入security.js、jquery-1.8.0.min.js

参数说明：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **接口名称** | | | RSAUtils.encryptedPassword | | | | |
| **序号** | | | **参数名称** | **中文名称** | **类型** | **备注** | **是否必输** |
| **输入参数：** | | | | | | | |
| 1 | random | | | 随机数 | String | 16个字符的随机数 | Y |
| 2 | pwd | | | 密码明文 | String | 登录密码，明文 | Y |
| 3 | modulus | | | 公钥模 | String | 公钥配置文件中 **modulus1**的值 | Y |
| 4 | exponent | | | 公钥指数 | String | 公钥配置文件中 **exponent1**的值 | Y |
| **返回值：** | | | | | | | |
| 1 | |  | |  |  | 登录密码密文 | Y |

### Pin保护

该接口使用JS实现，业务系统在其jsp页面中调用。方法名为：

RSAUtils.encryptedPin(random,pin,modulus1,exponent1,modulus2,exponent2)

调用时必须引入security.js、jquery-1.8.0.min.js

参数说明：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **接口名称** | | | RSAUtils.encryptedPassword | | | | |
| **序号** | | | **参数名称** | **中文名称** | **类型** | **备注** | **是否必输** |
| **输入参数：** | | | | | | | |
| 1 | random | | | 随机数 | String | 16个字符的随机数 | Y |
| 2 | pin | | | 密码明文 | String | PIN明文 | Y |
| 3 | Modulus1 | | | 公钥模 | String | 公钥配置文件中 **modulus2**的值 | Y |
| 4 | Exponent1 | | | 公钥指数 | String | 公钥配置文件中 **exponent2**的值 | Y |
|  | Modulus2 | | | 公钥模 | String | 公钥配置文件中 **modulus1**的值 | Y |
|  | Exponent2 | | | 公钥指数 | String | 公钥配置文件中 **exponent1**的值 | Y |
| **返回值：** | | | | | | | |
| 1 | |  | |  |  | Pin密文 | Y |

## 信息数据保护接口

**构造方法：**

InfoholdCipherAPI(InfoholdHandle handle)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **接口名称** | | InfoholdCipherAPI | | | | | |
| **序号** | | **参数名称** | **中文名称** | **类型** | | **备注** | **是否必输** |
| **输入参数：** | | | | | | | |
| 1 | handle | | 连接安全服务平台的handel | | InfoholdHandle |  | Y |
| **返回值：** | | | | | | | |
| 无 | | | | | | | |

### 数据加密接口

**函数接口：**

String[] infoholdEncUserData (String userID,String plainData,int dataType,String masterKeyName) throws Exception

**接口说明：**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **接口名称** | | | infoholdEncUserData | | | | | | |
| **序号** | | | **参数名称** | | **中文名称** | | **类型** | **备注** | **是否必输** |
| **输入参数：** | | | | | | | | | |
| 1 | userID | | | | 用户的唯一标识 | | String | 用户在管理系统中的唯一标识（该标识不可修改 | Y |
| 2 | plainData | | | | 待加密数据 | | String |  | Y |
| 3 | datatype | | | | 数据类型 | | Int | 身份证号=1  手机号=2  银行账号=3  金额=4 | Y |
| 4 | masterKeyName | | | | 数据加密主密钥 | | String | 主密钥的名称。  **易民生系统调用该接口时，该值为YM.00.zek**； | Y |
| **返回值：** | | | | | | | | | |
| 1 | | 密文数据 | | String | | 身份证号：加密生日  手机号：加密中间第4-7位的数字  银行账号：前6与后4位不加密，其他数据加密  金额：全加密，金额长度小于20  返回的密文数据为：   将加密的数据与未加密的数据拼接返回； 如：  用户的身份证号为130529198605131864，加密后返回的密文为130529AW7ERFED1457YTRE1864  手机号为15801468604，加密后返回的密文为 158A2W3SEDR8604  银行账号为622260 091005065 1234，加密后返回的密文为 622260SEDRFTGYH&YHUJ4UJN1234  金额为456.45，加密后返回的密为 AWS345EDRFT7 | | | Y |
| 2 | |  | | String | | 当密钥类型为身份证号、手机号、银行账号时，返回数据的HASH值 | | |  |

### 数据解密接口

**函数接口：**

String infoholdDecUserData (String userID,String encData,int dataType,String masterKeyName) throws Exception

**接口说明：**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **接口名称** | | | infoholdDecData | | | | |
| **序号** | | | **参数名称** | **中文名称** | **类型** | **备注** | **是否必输** |
| **输入参数：** | | | | | | | |
| 1 | userID | | | 用户的唯一标识 | String | 用户在管理系统中的唯一标识（该标识不可修改 | Y |
| 3 | encData | | | 数据密文 | String | 数据加密接口产生的密文 | Y |
| 2 | dataType | | | 数据类型 | Int | 身份证号=1  手机号=2  账号=3  金额=4 | Y |
| 4 | masterKeyName | | | 数据加密主密钥 | String | 主密钥的名称。  **易民生系统调用该接口时，该值为YM.00.zek** | Y |
| **返回值：** | | | | | | | |
| 1 | |  | | | Stirng | 数据明文 | Y |

## 动态码接口

**构造方法：**

InfoholdOTPAPI (InfoholdHandle handle)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **接口名称** | | InfoholdOTPAPI | | | | | |
| **序号** | | **参数名称** | **中文名称** | **类型** | | **备注** | **是否必输** |
| **输入参数：** | | | | | | | |
| 1 | handle | | 连接安全服务平台的handel | | InfoholdHandle |  | Y |
| **返回值：** | | | | | | | |
| 无 | | | | | | | |

### 时间型动态码生成

**函数接口：**

String infoholdGenSMSCodeBytime(String phoneNumber, int codeLength,int interval,int windows) throws Exception

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **接口名称** | | | infoholdGenSMSCodeBytime | | | | |
| **序号** | | | **参数名称** | **中文名称** | **类型** | **备注** | **是否必输** |
| **输入参数：** | | | | | | | |
| 1 | phoneNumber | | | 手机号 | String | 手机号明文 | Y |
| 2 | codeLength | | | 动态码长度 | int | 生成动态码的长度，**易民生系统调用该接口时，该值为6；** | Y |
| 3 | interval | | | 窗口个数 | int | **易民生系统调用该接口时，该值为6；** | Y |
| 4 | Windows | | | 窗口期 | int | **易民生系统调用该接口时，该值为10；** | Y |
| **返回值：** | | | | | | | |
| 1 | |  | | 动态码 | String |  | Y |

**接口说明：**

### 时间型动态码校验

**函数接口：**

boolean infoholdVerSMSCodeBytime(String phoneNumber,String code, int codeLength,int interval,int windows) throws Exception

**接口说明：**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **接口名称** | | | infoholdVerSMSCodeBytime | | | | |
| **序号** | | | **参数名称** | **中文名称** | **类型** | **备注** | **是否必输** |
| **输入参数：** | | | | | | | |
| 1 | phoneNumber | | | 手机号 | String | 手机号明文 | Y |
| 2 | code | | | 动态码 | String | 调用**时间型动态码生成接口**输出的动态码 | Y |
| 3 | codeLength | | | 动态码长度 | Int | 动态码的长度，**易民生系统调用该接口时，该值为6；** | Y |
| 4 | interval | | | 窗口个数 | Int | **易民生系统调用该接口时，该值为6；** | Y |
| 5 | Windows | | | 窗口期 | Int | **易民生系统调用该接口时，该值为10；** | Y |
| **返回值：** | | | | | | | |
| 1 | |  | | | boolean | True正确，false错误 | Y |