|  |  |
| --- | --- |
| 产品名称Product name | 密级Confidentiality level |
|  |  |
| 产品版本Product version | Total XX pages共XX页 |
| 1.0 |

功能清单接口说明书

|  |  |  |  |
| --- | --- | --- | --- |
| Prepared by  拟制 |  | Date  日期 |  |
| Reviewed by  评审人 |  | Date  日期 |  |
| Approved by  批准 |  | Date  日期 |  |
| Authorized by  签发 |  | Date  日期 |  |

杭州瑞成信息技术有限公司

All rights reserved

版权所有侵权必究

Revision record 修订记录

| Date  日期 | Revision Version  修订版本 | CR ID/ Defect ID CR号 | Section Number 修改章节 | Change  Description  修改描述 | Author  作者 |
| --- | --- | --- | --- | --- | --- |
| 2022.2.22 | 1.0 |  |  | 新建 |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

目录

[1. 名词描述 7](#_Toc96439565)

[2. 管理界面原型及服务调用 7](#_Toc96439566)

[2.1. 系统管理 7](#_Toc96439567)

[2.2. 应用管理 7](#_Toc96439568)

[2.2.1. 菜单路径 7](#_Toc96439569)

[2.2.2. 界面及服务标注 7](#_Toc96439570)

[2.2.3. 服务接口 7](#_Toc96439571)

[2.3. 加密机管理 7](#_Toc96439572)

[2.3.1. 菜单路径 7](#_Toc96439573)

[2.3.2. 界面及服务标注 8](#_Toc96439574)

[2.3.3. 服务接口 8](#_Toc96439575)

[2.4. 密钥管理 8](#_Toc96439576)

[2.4.1. 菜单路径 8](#_Toc96439577)

[2.4.2. 界面及服务标注 8](#_Toc96439578)

[2.4.3. 服务接口 8](#_Toc96439579)

[2.5. 日志管理 9](#_Toc96439580)

[2.5.1. 菜单路径 9](#_Toc96439581)

[2.5.2. 界面及服务标注 9](#_Toc96439582)

[2.5.3. 服务接口 9](#_Toc96439583)

[3. 服务开发规范 10](#_Toc96439584)

[3.1. 获取密钥 10](#_Toc96439585)

[3.1.1. 接口描述 10](#_Toc96439586)

[3.1.2. 服务接口 10](#_Toc96439587)

[3.1.2.1接口定义 10](#_Toc96439588)

[3.1.2.2请求参数 10](#_Toc96439589)

[3.1.2.3响应参数： 10](#_Toc96439590)

[3.2. 数据加密接口 11](#_Toc96439591)

[3.2.1. 接口描述 11](#_Toc96439592)

[3.2.2. 接口业务流程图 11](#_Toc96439593)

[3.2.3. 服务接口 12](#_Toc96439594)

[3.2.3.1接口定义 12](#_Toc96439595)

[3.2.3.2请求参数 12](#_Toc96439596)

[3.2.3.3响应参数 12](#_Toc96439597)

[3.3. 数据解密 12](#_Toc96439598)

[3.3.1. 接口描述 12](#_Toc96439599)

[3.3.2. 接口流程图 12](#_Toc96439600)

[3.3.3. 服务接口 13](#_Toc96439601)

[3.3.3.1接口定义 13](#_Toc96439602)

[3.3.3.2请求参数 13](#_Toc96439603)

[3.3.3.3响应参数 13](#_Toc96439604)

[3.4. 批量数据加密 14](#_Toc96439605)

[3.4.1. 接口描述 14](#_Toc96439606)

[3.4.2. 服务接口 14](#_Toc96439607)

[3.4.2.1接口定义 14](#_Toc96439608)

[3.4.2.2请求参数 14](#_Toc96439609)

[3.4.2.3响应参数： 14](#_Toc96439610)

[3.5. 批量数据解密接口 15](#_Toc96439611)

[3.5.1. 接口描述 15](#_Toc96439612)

[3.5.2. 服务接口 15](#_Toc96439613)

[3.5.2.1接口定义 15](#_Toc96439614)

[3.5.2.2请求参数 15](#_Toc96439615)

[3.5.2.3响应参数 16](#_Toc96439616)

[3.6. 不可逆加密 16](#_Toc96439617)

[3.6.1. 接口描述 16](#_Toc96439618)

[3.6.2. 服务接口 16](#_Toc96439619)

[3.6.2.1接口定义 16](#_Toc96439620)

[3.6.2.2请求参数 17](#_Toc96439621)

[3.6.2.3响应参数 17](#_Toc96439622)

[3.7. 文件加密接口 17](#_Toc96439623)

[3.7.1. 接口描述 17](#_Toc96439624)

[3.7.2. 服务接口 17](#_Toc96439625)

[3.7.2.1接口定义 17](#_Toc96439626)

[3.7.2.2请求参数 18](#_Toc96439627)

[3.7.2.3响应参数： 18](#_Toc96439628)

[3.8. 文件解密接口 18](#_Toc96439629)

[3.8.1. 接口描述 18](#_Toc96439630)

[3.8.2. 服务接口 18](#_Toc96439631)

[3.8.2.1接口定义 18](#_Toc96439632)

[3.8.2.2请求参数 18](#_Toc96439633)

[3.8.2.3响应参数 19](#_Toc96439634)

[3.9. 数据签名接口 19](#_Toc96439635)

[3.9.1. 接口描述 19](#_Toc96439636)

[3.9.2. 服务接口 19](#_Toc96439637)

[3.9.2.1接口定义 19](#_Toc96439638)

[3.9.2.2请求参数 19](#_Toc96439639)

[3.9.2.3响应参数 20](#_Toc96439640)

[3.10. 数据验签接口 20](#_Toc96439641)

[3.10.1. 接口描述 20](#_Toc96439642)

[3.10.2. 服务接口 20](#_Toc96439643)

[3.10.2.1接口定义 20](#_Toc96439644)

[3.10.2.2请求参数 20](#_Toc96439645)

[3.10.2.3响应参数： 21](#_Toc96439646)

[3.11. 文件签名接口 21](#_Toc96439647)

[3.11.1. 接口描述 21](#_Toc96439648)

[3.11.2. 服务接口 21](#_Toc96439649)

[3.11.2.1接口定义 21](#_Toc96439650)

[3.11.2.2请求参数 21](#_Toc96439651)

[3.11.2.3响应参数 21](#_Toc96439652)

[3.12. 文件验签接口 22](#_Toc96439653)

[3.12.1. 接口描述 22](#_Toc96439654)

[3.12.2. 服务接口 22](#_Toc96439655)

[3.12.2.1接口定义 22](#_Toc96439656)

[3.12.2.2请求参数 22](#_Toc96439657)

[3.12.2.3响应参数 22](#_Toc96439658)

# 名词描述

1. 三方应用：接入到加解密服务平台的应用。

# 管理界面原型及服务调用

## 系统管理

使用平台原有的用户管理、角色管控、菜单资源管控

## 应用管理

对三方应用的添加、编辑、启用/禁用、删除、设置加密机、设置主密钥。

### 菜单路径

应用管理🡪 三方应用

### 界面及服务标注

### 服务接口

使用的是统一用户的增删改查。

* 设置加密机接口：

/risen/cipher/app/updateEncryptor.do

* 设置主密钥接口：

/risen/cipher/app/updateAppIpkIndex.do

## 加密机管理

### 菜单路径

加密机管理

### 界面及服务标注

### 服务接口

使用低代码平台进行配置出的表单设计，视图设计。

涉及到的接口是低代码内部自适应的增删改查接口。

## 密钥管理

### 菜单路径

密钥管理

### 界面及服务标注

### 服务接口

* 密钥配置：使用低代码视图设计,

调用api接口：/risen/core/uams/mag/showCoreUamsApp.do

视图配置时配置的请求参数

{

"CMD":"LIST",

"TYPE":"jsn\_grid"

}

* 密钥策略管理：密钥策略新建、编辑。使用低代码配置，

新建接口和编辑接口：使用的是低代码表单视图配置后低代码自适应接口。

查询列表接口：/risen/cipher/app/strategy/showCipherAppStrategy

* 密钥查看：

/risen/cipher/app/strategy/appStrategy/keyView.do get请求

## 日志管理

### 菜单路径

日志管理

### 界面及服务标注

### 服务接口

使用低代码视图设计,调用api接口：

* 登录日志：

/risen/core/mag/log/findByCustomQueryCoreLog.action

视图配置时默认请求参数：

{"strMap.CQ":"{\"OF\":[],\"CF\":[{\"GROUP\":[{\"colName\":\"crlogType\",\"OP\":\"LIKE\",\"value\":\"L\"}]}]}"}

* 操作日志：

/risen/core/mag/log/findByCustomQueryCoreLog.action

视图配置时默认请求参数：

{"strMap.CQ": "{\"OF\":[],\"CF\":[{\"GROUP\":[{\"colName\":\"crlogType\",\"OP\":\"LIKE\",\"value\":\"A\"}, {\"OP\": \"OR\" },{ \"colName\": \"crlogType\", \"OP\": \"LIKE\", \"value\": \"D\"},{ \"OP\": \"OR\" },{ \"colName\": \"crlogType\", \"OP\": \"LIKE\", \"value\": \"U\" }]}]}"}

* 服务日志：

/risen/cipher/service/log/showCipherServiceLog.do

视图配置时默认请求参数：

{"CMD":"LIST","TYPE":"jsn\_grid","strMap.CQ":"{\"OF\":[],\"CF\":[]}","strMap.ECQ":"{\"OF\":[],\"CF\":[]}"}

# 服务开发规范

## 获取密钥

### 接口描述

为了满足加密粒度的要求，应用系统需要使用不同的密钥来对不同的数据进行加密，因此应用系统在需要新密钥对新数据进行加密时，需要调用该接口来获取新密钥。

### 服务接口

#### 3.1.2.1接口定义

接口名称：/api/getDataKey通信协议：http 请求方式：post

#### 3.1.2.2请求参数

{

    "appCode": "8C09761853134B6DA11B906162253ECC",//应用唯一标识

    "size": "2"//本次生成的密钥数量

}

#### 3.1.2.3响应参数：

{

    "message": "成功",//当失败时返回原因

    "data": [

        {

            "dataKey": "517f0aa50dd0536d5f3a32774181a046"//数据密钥

        },

        {

            "dataKey": "c92473c7760a85feba00e001ddbdcba7"//数据密钥

        }

    ],

    "code": 200//根据 code 类型判断本次操作是否成功

}

## 数据加密接口

### 接口描述

对于一些重要的用户信息、组织机构信息、日志信息等可以使用该接口对相关的数据进行加密。

### 接口业务流程图



### 服务接口

#### 3.2.3.1接口定义

接口名称： /api/encryptData通信协议：http 请求方式：post

#### 3.2.3.2请求参数

{

"appCode": "DFB41EB431524D84A34F64546FF341DE", //应用唯一标识

"dataKey": "47ac46530bac8de869896c8db7de7c69", //数据密钥

"data": "13212344321" //明文数据

}

#### 3.2.3.3响应参数

{

"message": "成功", //当失败时返回原因

"data": "b6c4b63f8d3b74813d30830ca7accb3fdbe57d625ddd1615a733d6d64544eaa3", //密文数据

"code": 200 //根据 code 类型判断本次操作是否成功

}

## 数据解密

### 接口描述

用于数据的解密操作，在应用系统的数据进行页面展示时，调用此接口将数据解密后展示明文。

### 接口流程图



### 服务接口

#### 3.3.3.1接口定义

接口名称： /api/decryptData 通信协议：http 请求方式：post

#### 3.3.3.2请求参数

{

"appCode": "01bc857f5c1245708b1247236d9869fe", //应用唯一标识

"dataKey": "5fb1192655db0f620dca5cfdb2da3ed2",//数据密钥

"data": "b6c4b63f8d3b74813d30830ca7accb3fdbe57d625ddd1615a733d6d64544eaa3" //密文数据

}

#### 3.3.3.3响应参数

{

"message": "成功",//当失败时返回原因

"data": "123456789123456789",//明文数据

"code": 200//根据 code 类型判断本次操作是否成功

}

## 批量数据加密

### 接口描述

提供给三方应用，进行批量对数据进行加密操作。

### 服务接口

#### 3.4.2.1接口定义

接口名称： /api/batchEncrypt 通信协议：http 请求方式：post

#### 3.4.2.2请求参数

{

    "appCode": "01BC857F5C1245708B1247236D9869FE",//应用唯一标识

    "batchData": [

        {

            "dataKey": "9ac0979a0242c6a0c0ed1ade0e653421",//数据密钥

            "IDCard1": "123456789123456789"//明文数据

        },

        {

            "dataKey": "dfab61e346c9ba682d785cf60366b8d3",//数据密钥

            "IDCard2": "987654321987654321"//明文数据

        }

    ]

}

#### 3.4.2.3响应参数：

{

    "message": "成功",//当失败时返回原因

    "data": [

        {

            "IDCard1": "3a9574cf82aa215bc5d4e65ab1960e0e7bc59419f9951779d5e94231089d7b6f"//密文数据

        },

        {

            "IDCard2": "ec05e7341effe2aca141b44081b13e4914e63acf48f87e4fe2929872e03c292b"//密文数据

        }

    ],

    "code": 200//根据 code 类型判断本次操作是否成功

}

## 批量数据解密接口

### 接口描述

对大量密文数据进行批量解密，提高三方应用系统的解密效率。

### 服务接口

#### 3.5.2.1接口定义

接口名称： /api/batchDecrypt 通信协议：http 请求方式：post

#### 3.5.2.2请求参数

{

    "appCode": "01BC857F5C1245708B1247236D9869FE",//应用唯一标识

    "batchData": [

        {

            "dataKey": "9ac0979a0242c6a0c0ed1ade0e653421",//数据密钥

            "IDCard1": "3a9574cf82aa215bc5d4e65ab1960e0e7bc59419f9951779d5e94231089d7b6f" //密文数据

        },

        {

            "dataKey": "dfab61e346c9ba682d785cf60366b8d3",//数据密钥

            "IDCard2": "ec05e7341effe2aca141b44081b13e4914e63acf48f87e4fe2929872e03c292b"//密文数据

        }

    ]

}

#### 3.5.2.3响应参数

{

    "message": "成功",//当失败时返回原因

    "data": [

        {

            "IDCard1": "123456789123456789"//明文数据

        },

        {

            "IDCard2": "987654321987654321"//明文数据

        }

    ],

    "code": 200//根据 code 类型判断本次操作是否成功

}

## 不可逆加密

### 接口描述

不可逆加密是指数据哈希。数据哈希使用的是sm3算法，具备有不可逆性，因此使用该算法进行加密的数据是那些不需要再进行解密的数据。该方法不需要使用数据密钥。常用此接口加密的数据例如用户的登录密码。

### 服务接口

#### 3.6.2.1接口定义

接口名称：

通信协议：http 请求方式：post

#### 3.6.2.2请求参数

{

    "appCode": "01bc857f5c1245708b1247236d9869fe", //应用唯一标识

"data":"123456789123456789" //明文数据

}

#### 3.6.2.3响应参数

{ "message": "成功",//当失败时返回原因

"data":"f72a78ff84bd13e6a011f5427e53fa278989e0afe9d5f2dd811ffa 58d6c290b2", //密文数据

"code": 200//根据 code 类型判断本次操作是否成功

}

## 文件加密接口

### 接口描述

为了保证存储安全，服务器内部存放的文件应该都是密文，因此在文件的收发文过程产生的文件，都应该进行加密，使文件以密文的形式在服务器上存储。将文件BASE64编码后调用接口服务进行加密操作,文件超过4MB建议使用本地API方法。

### 服务接口

#### 3.7.2.1接口定义

接口名称： /api/encryptFile 通信协议：http 请求方式：post

#### 3.7.2.2请求参数

{

    "appCode": "01BC857F5C1245708B1247236D9869FE",//应用唯一标识

    "dataKey": "b04d4bd00a04832290f9d17f07379bfe",//数据密钥

    "fileContent": "BASE64 编码文件内容"//明文 BASE64 编码

}

#### 3.7.2.3响应参数：

{

    "message": "成功",//当失败时返回原因

    "data": " BASE64 编码文件内容",//密文 BASE64 编码

    "code": 200//根据 code 类型判断本次操作是否成功

}

## 文件解密接口

### 接口描述

三方应用在服务器上存储的是加密后的文件，当三方应用需要查看文件内容时，必须调用文件的解密接口将文件解密。

### 服务接口

#### 3.8.2.1接口定义

接口名称： 通信协议：http 请求方式：post

#### 3.8.2.2请求参数

{

    "appCode": "01BC857F5C1245708B1247236D9869FE",//应用唯一标识

    "dataKey": "b04d4bd00a04832290f9d17f07379bfe",//数据密钥

    "fileContent": "BASE64 文件编码内容"//密文 BASE64 编码

}

#### 3.8.2.3响应参数

{

    "message": "成功",//当失败时返回原因

    "data": " BASE64 文件编码",//明文 BASE64 编码

    "code": 200//根据 code 类型判断本次操作是否成功

}

## 数据签名接口

### 接口描述

三方应用系统调用此服务对数据进行签名操作。签名操作可用来验证数据是否被篡改。

### 服务接口

#### 3.9.2.1接口定义

接口名称： /api/signData 通信协议：http 请求方式：post

#### 3.9.2.2请求参数

{

    "appCode":"540EA9EFDAB94DA583E323BDE1703A92",//应用唯一标识

    "data":"2233399877"//签名数据

}

#### 3.9.2.3响应参数

{

    "message": "成功",//当失败时返回原因

    "data": "bfa0cdf00fda8a9a1ca0fbb2e1c2c816b1ade49a4fb0a20af7139eeb08c039c041d3d275e468217db3329552faf17f17860d60350e8b557d0c7d84321fcd7a4f",//签名值

    "code": 200//根据 code 类型判断本次操作是否成功

}

## 数据验签接口

### 接口描述

提供给三方应用系统，用来验证签名数据。验证数据在流转和存储过程中的真实性。

### 服务接口

#### 3.10.2.1接口定义

接口名称： /api/verifyData 通信协议：http 请求方式：post

#### 3.10.2.2请求参数

{

    "appCode":"540EA9EFDAB94DA583E323BDE1703A92",//应用唯一标识

    "data":"2233399877",//签名数据

    "signature":"bfa0cdf00fda8a9a1ca0fbb2e1c2c816b1ade49a4fb0a20af7139eeb08c039c041d3d275e468217db3329552faf17f17860d60350e8b557d0c7d84321fcd7a4f"//签名值

}

#### 3.10.2.3响应参数：

{

    "message": "成功",//当失败时返回原因

    "data": "true",//成功后返回标识

    "code": 200//根据 code 类型判断本次操作是否成功

}

## 文件签名接口

### 接口描述

应用系统调用此服务对文件签名用于对文件生成的base64编码数据签名操作。此签名数据用来验证文件是否被篡改。

### 服务接口

#### 3.11.2.1接口定义

接口名称： /api/signFile 通信协议：http请求方式：post

#### 3.11.2.2请求参数

{

    "appCode": "540EA9EFDAB94DA583E323BDE1703A92",//应用唯一标识

    "fileContent":"BASE64 文件编码内容",//BASE64 编码

}

#### 3.11.2.3响应参数

{

    "message": "成功",//当失败时返回原因

    "data": "7b183e3bd1a7d68bd3a26cf201a22298a6e4dd34cb9787550e1d3e856abc0441c78b04dc28318186fcdf6bc861560dc05d37f9561407b9e7d54675b825235de5",//签名值

    "code": 200//根据 code 类型判断本次操作是否成功

}

## 文件验签接口

### 接口描述

用于三方应用系统对文件进行验签操作，验证文件在流转和存储过程中的真实性。

### 服务接口

#### 3.12.2.1接口定义

接口名称： /api/verifyFile 通信协议：http 请求方式：post

#### 3.12.2.2请求参数

{

    "appCode": "540EA9EFDAB94DA583E323BDE1703A92",//应用唯一标识

    "fileContent":"BASE64 文件编码内容",//BASE64 编码

    "signature":"9621278774caaf0f72f9d2eae01620cc5d6884c14d03582b37b33792eca896a23f3a9c45ab052ab7258c884187097a0b5979c558eaefcad222711c0c37ec198e"//签名值

}

#### 3.12.2.3响应参数

{

    "message": "成功",//当失败时返回原因

    "data": "true",//成功后返回标识

    "code": 200//根据 code 类型判断本次操作是否成功

}