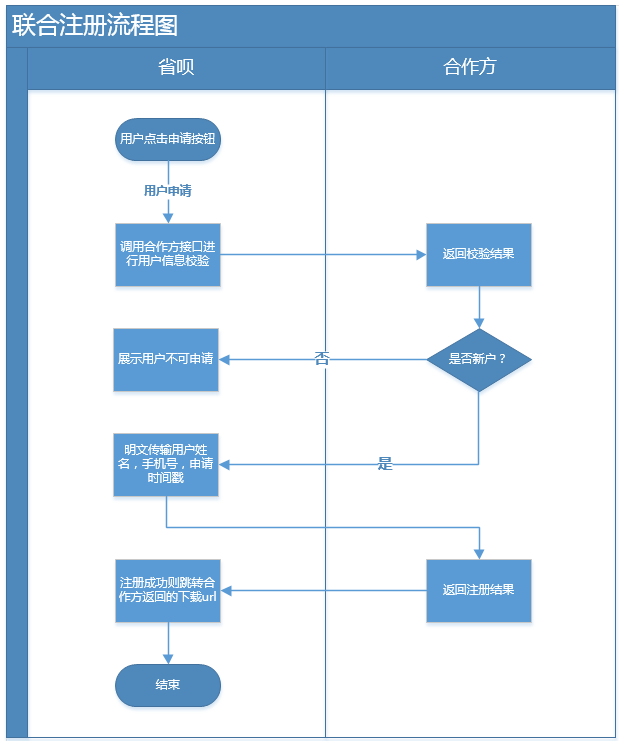
**省呗联合注册接口文档**

1. **业务流程说明**

用户点击贷款产品进行申请，省呗加密用户信息，向合作方进行信息校验并进行联合注册。同时，省呗客户端会打开合作方返回的链接，将合作方的页面呈现给用户



# 2.联合注册接口概述

通过省呗联合注册接口，合作机构能够和省呗实现联合注册。

|  |  |
| --- | --- |
| **接口** | **功能描述** |
| 注册发标 | 查询登录/注册用户在机构方的记录  如果没有在机构方注册，推送用户数据到机构方 |

# 3.接口约定

1. 没有特殊说明所有的编码方式都为UTF-8
2. 没有特殊说明所有HTTP接口都为POST方式

header Content-Type: application/x-www-form-urlencoded

charset 使用 UTF-8

1. 没有特殊说明所有响应数据的格式都为JSON
2. 没有特殊说明，默认超时设置为3秒

# 加密

出于安全考虑,在传输过程中，必须对相关信息进行加密。

加密算法采用AES，如果没有特别商定的情况，key由省呗提供。

具体加密流程：

1. 获取iv，iv值为key值的前16个字节。
2. 填充需要加密的字节数组到加密块大小的倍数
3. 使用 AES/CBC/NoPadding 的方式进行加密
4. 对加密后的数组调用 org.apache.commons.codec.binary.Base64 方法，转换成 base64字符串。

# 签名

为保证传输内容的合法性，需要对传输内容进行签名。

签名算法采用MD5。

具体签名过程：

1. 对用户信息进行 MD5 签名，然后在签名结果后面拼接上 secretKey (secretKey由省呗提供，和加密使用同一个Key)。
2. 对拼接后的字符串再次进行 MD5 签名，签名结果作为 sign 的值。

加密签名示例:

var encodedUserInfo = encrypt(key,JSON.stringify({

"mobile":"13701234567",

"username":"张三"

}));

var sign = signature(key,encodedUserInfo);

//最终URL参数字符串

var paramStr="data=#{encodedUserInfo}&sign=#{sign}";

代码说明：

1. "#{param}"根据情况替换成实际值。
2. "encrypt"为加密过程。
3. "signature"为签名过程。
4. **加密和签名demo**



# 接口详细定义

## 6.1校验接口

### 6.1.1调用方向

省呗->机构

### 6.1.2 接口详细说明

校验用户是否已在机构注册。校验接口传递MD5后的手机号，并附带签名，签名规则如上【5.】所述。

### 6.1.3 接口地址

机构提供

### 6.1.4 接口参数定义

|  |  |  |  |
| --- | --- | --- | --- |
| **参数** | **类型** | **说明** | **是否必须** |
| mobile | String | 手机号MD5 | 是 |

样例数据：

mobile = 13717566001

密钥 = 5C0706A63D4B4C6E

生成Post请求的内容:

sign=b2e8e55399f80dce916d0b215855f037&data=c04c324993ab38b2e8aa6c380e89044c&

### 6.1.5 接口响应定义

|  |  |  |  |
| --- | --- | --- | --- |
| **参数** | **类型** | **说明** | **是否必须** |
| code | String | 0：新用户；1：老用户；非0/1：失败 无论成功失败都返回 | 是 |
| msg | String | 返回结果文字说明 | 是 |

## 6.2. 注册接口

### 6.2.1调用方向

省呗->机构

### 6.2.2 接口详细说明

如果非机构老用户,立即调用注册接口。注册接口发送加密后的用户数据，并附带签名。加密规则及签名规则如上【4.】及【5.】所述。

### 6.2.3 接口地址

机构提供

### 6.2.4 接口参数定义

|  |  |  |  |
| --- | --- | --- | --- |
| **参数** | **类型** | **说明** | **是否必须** |
| mobile | String | 手机号 | 是 |
| username | String | 用户名 | 是 |

样例数据：

mobile = 13717566001

username = custName

密钥= 5C0706A63D4B4C6E

加密后的数据：F9tZzGtwCZwnn/vlr2k6AzmBaEgSUjjJxM6+aAzg4er3p73Ii/POAHz49oKQOs95b3rxAHKgcgzgduY4gLypgMblA7VLrfp0U3OA/yACMBA=

生成Post请求的内容:

sign=4a0e7e2e60f4adbf51a457d073a78c1b&data=F9tZzGtwCZwnn%2Fvlr2k6AzmBaEgSUjjJxM6%2BaAzg4er3p73Ii%2FPOAHz49oKQOs95b3rxAHKgcgzgduY4gLypgMblA7VLrfp0U3OA%2FyACMBA%3D&

备注：使用示例程序Codec.java时，因使用HashMap，最终进入加密的json串可能有变，故生成的加密后的数据可能与上面的不一致。但只需【加密后的数据：】能够正常解密，加解密就是正常的。

### 6.2.5 接口响应定义

|  |  |  |  |
| --- | --- | --- | --- |
| **参数** | **类型** | **说明** | **是否必须** |
| code | String | 0：用户数据接收成功；非0：失败 无论成功失败都返回 | 是 |
| msg | String | 返回结果文字说明 | 是 |
| url | String | 用户需要跳转的下载url | 是 |

返回值示例：

{

"code": "0",

"msg" : "no error"

"url" : "https://www.smyfinancial.com"

}

备注：通过省呗联合注册渠道注册的用户，用户再次点击时，不会再调用机构撞库注册接口，而向用户直接展示机构提供的下载url