# 中间业务代扣商户签约指导文档

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **修订历史** | | | | | |
| **编号** | **日期** | **修订描述** | **版本** | **作者** | **审核** |
| 1 | *2019.6.21* | *支持商户上送客户信息* | *1.1* | *梁学利* |  |
| 2 | *2020.3.10* | *新增判断是否安装手机银行APP方法* | *1.2* |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |

## 相关地址

1. 测试环境(ST)：<http://mobiletest.cmburl.cn/IGateway/Jump.aspx?funcid=0163002>
2. 测试查看短信验证码地址：http://218.18.231.140:8080/code/stcode.html
3. 生产环境：https://html.m.cmbchina.com/IGateway/Jump.aspx?funcid=0163002

## 模板签约

1. 上送字段

|  |  |  |
| --- | --- | --- |
| 字段名称 | 含义 | 是否必传 |
| MerchantNum | 商户号 | 必填 |
| SubMerchantNum | 二级商户号 | 可不传 |
| TemplateNum | 模版编号 | 必填 |
| Signature | 签名 | 必填 |

1. 签名生成规则
2. 拼接字符串：MerchantNum+SubMerchantNum+TemplateNum
3. 生成32位MD5字符串，字母大写：

string sMd5Request = MerchantNum+SubMerchantNum+TemplateNum;

byte[] baMd5Request = EncoderHelper.utf-8.GetBytes(sMd5Request);

string sMd5Respone = BaseFunc.MD5HashString(baMd5Request);

1. 对MD5进行DES加密：根据约定的秘钥，对MD5字符串进行DES加密，采用ECB模式，Padding为PKCS7，返回base64字符串

Convert.ToBase64String(DESWrapper.DESEncryptECB(EncoderHelper.UTF8.GetBytes(sMd5Respone ), EncoderHelper.UTF8.GetBytes(DESKey)));

如果是GET方式，则最后对密文进行编码，HttpUtility.UrlEncode，POST方式则不用

1. GET方式样例

1）签约数据：

商户号：000300

二级商户号：100001

模版编号：TEMP\_000300-01

DES加密秘钥：12345678

1. 计算过程：

拼接字符串：000300100001TEMP\_000300-01

32位MD5：BF3C02D77E4317842FE3B49278A18345

DES加密后的MD5：6yzOizKjFq3PyqlTK4uA8fKDmsidJeD+cUzTDYzFf8n+uVm31GQvyw==

对密文进行编码： 6yzOizKjFq3PyqlTK4uA8fKDmsidJeD%2bcUzTDYzFf8n%2buVm31GQvyw%3d%3d

最终结果： <http://mobiletest.cmburl.cn/IGateway/Jump.aspx?funcid=0163002&MerchantNum=000300&TemplateNum=TEMP_000300-01&SubMerchantNum=100001&Signature=6yzOizKjFq3PyqlTK4uA8fKDmsidJeD%2bcUzTDYzFf8n%2buVm31GQvyw%3d%3d>

1. POST方式样例

1）签约数据：

商户号：000300

二级商户号：100001

模版编号：TEMP\_000300-01

DES加密秘钥：12345678

1. 计算过程：

拼接字符串：000300100001TEMP\_000300-01

32位MD5：BF3C02D77E4317842FE3B49278A18345

DES加密后的MD5：6yzOizKjFq3PyqlTK4uA8fKDmsidJeD+cUzTDYzFf8n+uVm31GQvyw==

最终结果：

<form action="<http://mobiletest.cmburl.cn/IGateway/Jump.aspx?funcid=0163002>" method="post" >

<input type="hidden" name="MerchantNum" value="000300" />

<input type="hidden" name="SubMerchantNum" value="100001" />

<input type="hidden" name="TemplateNum" value="TEMP\_000300-01" />

<input type="hidden" name="Signature" value="6yzOizKjFq3PyqlTK4uA8fKDmsidJeD+cUzTDYzFf8n+uVm31GQvyw==" />

</form>

## 自定义签约

1. 上传字段

|  |  |  |
| --- | --- | --- |
| 字段名称 | 含义 | 是否必传 |
| MerchantNum | 商户号 | 必填 |
| SubMerchantNum | 二级商户号 | 选填 |
| SignSerialNum | 签约流水号，  25位签约流水号，要求全局唯一，若签约超时，允许商户按照签约流水进行协议查询 | 选填 |
| ChargeBasis | 扣款依据 | 选填 |
| Use | 3位用途代码 | 如果指定用途，则必填 |
| CycleMode | 周期模式  D:日,M:月,Y:年,U:无周期限制 | 如限定周期，则必填 |
| Frequency | 频次[1,9999] | 如上 |
| SingleLimit | 单笔限额 | 必填 |
| CycleLimit | 周期限额 | 必填 |
| ValidityPeriod | 有效期，月为单位,[0,999] | 必填 |
| ShroffAccount | 收款账号 | 选填 |
| PartialDeductions | 是否允许部分扣款(Y/N) | 选填，不填则默认为否 |
| Name | 签约人姓名 | 上送全量客户信息、上送部分客户信息商户必填，其他类型商户不填 |
| IdNo | 签约人证件号 | 上送全量客户信息类商户必填，其他商户不填 |
| IdNoType | 签约人证件类型 | 上送全量客户信息类商户必填，具体值见附件1，其他商户不填 |
| CardNo | 签约人卡号 | 上送全量客户信息、上送部分客户信息商户必填，其他类型商户不填 |
| Mobile | 签约人预留手机号 | 上送全量客户信息、上送部分客户信息商户必填，其他类型商户不填 |
| JumpUrl | 签约完成页面点击“完成”按钮的跳转链接 | 选填，不填则不显示“完成”按钮 |
| Signature | 签名 | 必填 |

1. 签约人信息加密

签约人姓名，签约人证件号，签约人证件类型，签约人卡号，签约人预留手机号，需要进行加密处理。

1. 加密方法：根据约定的秘钥，对明文字符串进行DES加密，采用ECB模式，Padding为PKCS7，返回base64字符串

Convert.ToBase64String(DESWrapper.DESEncryptECB(EncoderHelper.UTF8.GetBytes(明文字符串), EncoderHelper.UTF8.GetBytes(DESKey)));

B、如果是GET方式，则最后对密文进行编码，HttpUtility.UrlEncode，POST方式则不用

1. 签名生成规则

签约人姓名，签约人证件号，签约人证件类型，签约人卡号，签约人预留手机号，需要进行加密处理，计算签名时，用密文进行拼接计算。

1. 拼接字符串：MerchantNum+SubMerchantNum+SignSerialNum+ChargeBasis+Use+CycleMode+Frequency+SingleLimit+CycleLimit+ValidityPeriod+ShroffAccount+PartialDeductions+Name+IdNo+ IdNoType+ CardNo+ Mobile；
2. 生成32位MD5字符串，字母大写：

string sMd5Request = 拼接字符串；

byte[] baMd5Request = EncoderHelper.utf-8.GetBytes(sMd5Request);

string sMd5Respone = BaseFunc.MD5HashString(baMd5Request);

1. 对MD5进行DES加密：根据约定的秘钥，对MD5字符串进行DES加密，采用ECB模式，Padding为PKCS7，返回base64字符串

Convert.ToBase64String(DESWrapper.DESEncryptECB(EncoderHelper.UTF8.GetBytes(sMd5Respone ), EncoderHelper.UTF8.GetBytes(DESKey)));

如果是GET方式，则最后对密文进行编码，HttpUtility.UrlEncode，POST方式则不用

1. GET方式样例，以下数据仅为了演示参数生成的方法，商户在联调时，需要填写自己的商户号及相应的签约信息

1）签约数据：

商户号：000300

二级商户号：100001

DES加密秘钥：12345678

签约流水号：0003002018092509445300001

扣款依据：00123

用户代码：001

周期模式：D

频次：2

单笔限额：1000

周期限额：10000

有效期：60

收款账号：

是否允许部分扣款：N

签约人姓名：卜堂注

签约人证件号：339006197912113257

签约人证件类型：P01

签约人卡号：6225886555062486

签约人预留手机号：15603583602

签约完成后的跳转链接： <http://mobiletest.cmburl.cn/IGateway/Jump.aspx?funcid=0163002>

1. 计算过程：
2. 五要素加密
3. 姓名：加密后：FdgDqwCESMx8ZkZMItD9EQ==编码后FdgDqwCESMx8ZkZMItD9EQ%3d%3d
4. 证件类型：加密后：Y+SLdrhZRrw=编码后Y%2bSLdrhZRrw%3d
5. 证件号码：加密后：xLciBCdtc1C2pWRFs57ve9cl2N8Vjdji编码后xLciBCdtc1C2pWRFs57ve9cl2N8Vjdji
6. 卡号：加密后：vOaSvQkSf9q7LBevc3/o0f65WbfUZC/L编码后vOaSvQkSf9q7LBevc3%2fo0f65WbfUZC%2fL
7. 预留手机号：加密后：zy9sOstqgvckDNcxHpTVXQ==编码后zy9sOstqgvckDNcxHpTVXQ%3d%3d
8. 计算签名

拼接字符串：000300100001000300201809250944530000100123001D210001000060NFdgDqwCESMx8ZkZMItD9EQ==xLciBCdtc1C2pWRFs57ve9cl2N8VjdjiY+SLdrhZRrw=vOaSvQkSf9q7LBevc3/o0f65WbfUZC/Lzy9sOstqgvckDNcxHpTVXQ==

32位MD5：1EFC980E7345B8BACCEF1AE8A1738365

DES加密后的MD5：9duGkGc3zLgG5Y6upTKfnVrvRyIuli5Fgn8d4fo/Ll7+uVm31GQvyw==

对密文进行编码： 9duGkGc3zLgG5Y6upTKfnVrvRyIuli5Fgn8d4fo%2fLl7%2buVm31GQvyw%3d%3d

最终结果： http://mobiletest.cmburl.cn/IGateway/Jump.aspx? funcid=0163002&MerchantNum=000300&SubMerchantNum=100001&SignSerialNum=0003002018092509445300001&TemplateNum=&ChargeBasis=00123&Use=001&CycleMode=D&Frequency=2&SingleLimit=1000&CycleLimit=10000&ValidityPeriod=60&ShroffAccount=&PartialDeductions=N&Name=FdgDqwCESMx8ZkZMItD9EQ%3d%3d&IdNo=xLciBCdtc1C2pWRFs57ve9cl2N8Vjdji&IdNoType=Y%2bSLdrhZRrw%3d&CardNo=vOaSvQkSf9q7LBevc3%2fo0f65WbfUZC%2fL&Mobile=zy9sOstqgvckDNcxHpTVXQ%3d%3d&JumpUrl=http://mobiletest.cmburl.cn/IGateway/Jump.aspx?funcid=0163002&Signature=9duGkGc3zLgG5Y6upTKfnVrvRyIuli5Fgn8d4fo%2fLl7%2buVm31GQvyw%3d%3d

1. POST方式样例，以下数据仅为了演示参数生成的方法，商户在联调时，需要填写自己的商户号及相应的签约信息

1）签约数据：

商户号：000300

二级商户号：100001

DES加密秘钥：12345678

签约流水号：0003002018092509445300001

扣款依据：00123

用户代码：001

周期模式：D

频次：2

单笔限额：1000

周期限额：10000

有效期：60

收款账号：

是否允许部分扣款：N

签约人姓名：卜堂注

签约人证件号：339006197912113257

签约人证件类型：P01

签约人卡号：6225886555062486

签约人预留手机号：15603583602

签约完成后的跳转链接： <http://mobiletest.cmburl.cn/IGateway/Jump.aspx?funcid=0163002>

1. 计算过程：
2. 五要素加密
3. 姓名：加密后：FdgDqwCESMx8ZkZMItD9EQ==
4. 证件类型：加密后：Y+SLdrhZRrw=
5. 证件号码：加密后：xLciBCdtc1C2pWRFs57ve9cl2N8Vjdji
6. 卡号：加密后：vOaSvQkSf9q7LBevc3/o0f65WbfUZC/L
7. 预留手机号：加密后：zy9sOstqgvckDNcxHpTVXQ==
8. 计算签名

拼接字符串：000300100001000300201809250944530000100123001D210001000060NFdgDqwCESMx8ZkZMItD9EQ==xLciBCdtc1C2pWRFs57ve9cl2N8VjdjiY+SLdrhZRrw=vOaSvQkSf9q7LBevc3/o0f65WbfUZC/Lzy9sOstqgvckDNcxHpTVXQ==

32位MD5：1EFC980E7345B8BACCEF1AE8A1738365

DES加密后的MD5：9duGkGc3zLgG5Y6upTKfnVrvRyIuli5Fgn8d4fo/Ll7+uVm31GQvyw==

最终结果：

H5签约：

<form action="<http://mobiletest.cmburl.cn/IGateway/Jump.aspx?funcid=0163002>" method="post" >

<input type="hidden" name="MerchantNum" value="000300" />

<input type="hidden" name="SubMerchantNum" value="100001" />

<input type="hidden" name="SignSerialNum" value="0003002018092509445300001" />

<input type="hidden" name="ChargeBasis" value="00123" />

<input type="hidden" name="Use" value="001" />

<input type="hidden" name="CycleMode" value="D" />

<input type="hidden" name="Frequency" value="2" />

<input type="hidden" name="SingleLimit" value="1000" />

<input type="hidden" name="CycleLimit" value="10000" />

<input type="hidden" name="ValidityPeriod" value="60" />

<input type="hidden" name="ShroffAccount" value="" />

<input type="hidden" name="PartialDeductions" value="N" />

<input type="hidden" name="Name" value=" FdgDqwCESMx8ZkZMItD9EQ==" />

<input type="hidden" name="IdNo" value=" xLciBCdtc1C2pWRFs57ve9cl2N8Vjdji " />

<input type="hidden" name="IdNoType" value=" Y+SLdrhZRrw=" />

<input type="hidden" name="CardNo" value=" vOaSvQkSf9q7LBevc3/o0f65WbfUZC/L " />

<input type="hidden" name="Mobile" value=" zy9sOstqgvckDNcxHpTVXQ==" />

<input type="hidden" name="JumpUrl" value="<http://mobiletest.cmburl.cn/IGateway/Jump.aspx?funcid=0163002>" />

<input type="hidden" name="Signature" value="9duGkGc3zLgG5Y6upTKfnVrvRyIuli5Fgn8d4fo/Ll7+uVm31GQvyw==" />

</form>

注：使用APP直接跳转模式，将链接更换为：cmbmobilebank://cmbls/FunctionJump?id=1&action=gofuncid&funcid=0026003&clean=true&closeCurrentView=true&cmb\_app\_trans\_parms\_start=here

## 使用招行APP签约或者解约



## 测试环境账号:

借记卡：6225886555062486 774411

姓名：卜堂注

身份证号：339006197912113257

证件类型：P01

手机号：15603583602

## 注意事项与常见问题

1. 生成签名时，拼接字符串的顺序需按照指定的顺序进行；
2. 样例中给的各个参数均为测试环境的样例，生产上各个商户需要使用自己的参数设置，包括完成页跳转链接、秘钥等所有参数；
3. 商户的秘钥要求同时包含大写字母、小写字母、数字、特殊字符，且是无规律的8位字符串；
4. 签约时页面提示：“商户签约信息不正确 请联系商户”，表示验签不通过，请检查签名是否按照要求正确生成，注意不同环境使用的秘钥不同；

### 附录1：证件类型

|  |  |
| --- | --- |
| 证件类型编码 | 证件类型描述 |
| P01 | 居民身份证 |
| P03 | 临时居民身份证 |
| P04 | 军人证 |
| P08 | 武警身份证 |
| P16 | 居民户口簿 |
| P20 | 港澳居民来往内地通行证 |
| P21 | 台湾居民来往大陆通行 |
| P31 | 护照 |
| P34 | 外国人永久居留证 |

### 附录2：判断手机上是否安装招商银行APP

**1.Android平台样例**

private boolean isCMBAppInstalled()

{

PackageInfo packageInfo;

try

{

packageInfo = getPackageManager().getPackageInfo("cmb.pb", 0);

}

catch (PackageManager.NameNotFoundException e)

{

packageInfo = null;

}

if(packageInfo ==null)

{

//System.out.println("没有安装");

return false;

}

else

{

//System.out.println("已经安装");

return true;

}

}

**2.iOS平台样例**

需要先在商户的APP的plist文件中LSApplicationQueriesSchemes下添加cmbmobilebank的scheme。

NSURL \*url = [NSURL URLWithString:

@"cmbmobilebank://CMBLS/FunctionJump?action=gofuncid&funcid=200015&serverid= CMBEUserPay&cmb\_app\_trans\_parms\_start=here&…"];

if (![[UIApplication sharedApplication] canOpenURL:url]) {

//未安装手机银行

} else {

//已安装手机银行

}