# 批量代扣商户签约指导文档

## 相关地址

1. 测试环境(ST)：<http://mobiletest.cmburl.cn/IGateway/Jump.aspx?funcid=0026008>
2. 测试环境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=0026008>

## 测试环境账号:

借记卡：6225886555062486 774411

姓名：卜堂注

身份证号：339006197912113257

手机号：15603583602

## 模版签约

1. 上送字段：MerchantNum（商户编号）、TemplateNum（模版编号）、ChargeBasis（扣款依据）、JumpUrl（签约完成页面点击“完成”按钮的跳转链接，非必填）、PropelUrl（推送地址）、Signature（签名，验证数据的完整性）
2. 签名生成规则
3. 拼接字符串：string sMd5Request = MerchantNum + TemplateNum + ChargeBasis + JumpUrl + PropelUrl，此时JumpUrl ， PropelUrl用的是原始值而非编码后的值
4. 生成32位MD5字符串：

byte[] baMd5Request = Encoding.UTF8.GetBytes(sMd5Request);

string sMD5String = BaseFunc.MD5HashString(baMd5Request);

C、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，再将结果转换成16进制字符串：

byte[] bsign = DESWrapper.DESEncrypt(Encoding.UTF8.GetBytes(sMD5String), Encoding.UTF8.GetBytes(desKey));

string Signature = BaseFunc.HexString(bsign);

1. 完整链接形式

将MerchantNum 、TemplateNum 、ChargeBasis、JumpUrl、PropelUrl、Signature加到url的参数中，其中GET方式JumpUrl和PropelUrl需要先分别进行两次encodeURIComponent，POST方式只需要进行一次encodeURIComponent。

若商户信息中不指定用途，则可以不传ChargeBasis； 若指定用途，也可以不传ChargeBasis，此时会要求用户签约时手动输入该值。

1. GET方式样例
2. 签约数据：

商户编号：AK0769000516

模版编号：MB001

扣款依据：

完成页跳转链接：<http://99.6.150.121:832/HtmlBank/UserScene/DirectPay/Test/GetUrlForWithholding.aspx>

推送地址：cmbmobilebank://cmbls/functionjump?action=gofuncid&funcid=0026006

DES秘钥：12345678

1. 计算过程：

拼接字符串：AK0769000516MB001http://99.6.150.121:832/HtmlBank/UserScene/DirectPay/Test/GetUrlForWithholding.aspxcmbmobilebank://cmbls/functionjump?action=gofuncid&funcid=0026006

32位MD5值：E074FD4A3B7259ECC66A6093DAC24421

DES密文：D52B28D63A7A98592693A3FACE5F6A26D60B2EC979EF96D94A209F91B1332422FEB959B7D4642FCB

最终结果：http://mobiletest.cmburl.cn/IGateway/Jump.aspx?funcid=0026008&MerchantNum=AK0769000516&TemplateNum=MB001&ChargeBasis=&JumpUrl=http%253A%252F%252F99.6.150.121%253A832%252FHtmlBank%252FUserScene%252FDirectPay%252FTest%252FGetUrlForWithholding.aspx&PropelUrl=cmbmobilebank%253A%252F%252Fcmbls%252Ffunctionjump%253Faction%253Dgofuncid%2526funcid%253D0026006&Signature=D52B28D63A7A98592693A3FACE5F6A26D60B2EC979EF96D94A209F91B1332422FEB959B7D4642FCB

1. POST方式样例
2. 签约数据：

商户编号：AK0769000516

模版编号：MB001

扣款依据：

完成页跳转链接：<http://99.6.150.121:832/HtmlBank/UserScene/DirectPay/Test/GetUrlForWithholding.aspx>

推送地址：cmbmobilebank://cmbls/functionjump?action=gofuncid&funcid=0026006

DES秘钥：12345678

1. 计算过程：

拼接字符串：AK0769000516MB001http://99.6.150.121:832/HtmlBank/UserScene/DirectPay/Test/GetUrlForWithholding.aspxcmbmobilebank://cmbls/functionjump?action=gofuncid&funcid=0026006

32位MD5值：E074FD4A3B7259ECC66A6093DAC24421

DES密文：D52B28D63A7A98592693A3FACE5F6A26D60B2EC979EF96D94A209F91B1332422FEB959B7D4642FCB

最终结果：

<form action="<http://mobiletest.cmburl.cn/IGateway/Jump.aspx?funcid=0026008>" method="post" >

<input type="hidden" name="MerchantNum" value="AK0769000516" />

<input type="hidden" name="TemplateNum" value="MB001" />

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

<input type="hidden" name="JumpUrl" value="http%3A%2F%2F99.6.150.121%3A832%2FHtmlBank%2FUserScene%2FDirectPay%2FTest%2FGetUrlForWithholding.aspx" />

<input type="hidden" name="PropelUrl" value="cmbmobilebank%3A%2F%2Fcmbls%2Ffunctionjump%3Faction%3Dgofuncid%26funcid%3D0026006" />

<input type="hidden" name="Signature" value="D52B28D63A7A98592693A3FACE5F6A26D60B2EC979EF96D94A209F91B1332422FEB959B7D4642FCB" />

</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 | 必传 |
| ChargeBasis | 扣款依据 | 同模板签约 |
| Use | 用途代码 | 若商户信息中指定用途，必传 |
| CycleMode | 周期 | 如限定周期，必传，只能为Y(年)、M(月)、D(日) |
| Frequency | 频次 | 如限定周期，必传，不超过4位 |
| SingleLimit | 单笔限额 | 必传 |
| CycleLimit | 周期限额 | 必传 |
| ShroffAccount | 收款账号 | 非必传 |
| PartialDeductions | 是否允许部分扣款 | Y/N非必传，不传则默认为否 |
| ValidityPeriod | 有效期 | 必传，不超过3位，不能为0 |
| JumpUrl | 签约完成页面点击“完成”按钮的跳转链接 | 非必传，不填则不显示“完成”按钮 |
| PropelUrl | 推送链接 | 必传 |
| Signature | 签名信息 | 必传 |

1. 签名生成规则

拼接字符串：string sMd5Request = MerchantNum + ChargeBasis + Use + CycleMode + Frequency + SingleLimit + CycleLimit + ShroffAccount + PartialDeductions + ValidityPeriod + JumpUrl + PropelUrl

后面的生成方式同模板签约。

3、完整链接形式

跳转链接同模板签约，将1中列出的所有需要的参数加到url的参数中，同样地，GET方式JumpUrl和PropelUrl需要先分别进行两次encodeURIComponent，POST方式进行一次即可。

1. GET方式样例
2. 签约数据：

商户编号：AK0769000516

扣款依据：

用途代码：001

周期：D

频次：3

单笔限额：1000

周期限额：10000

收款账号：

是否允许部分扣款：N

有效期：24

完成页跳转链接：<http://99.6.150.121:832/HtmlBank/UserScene/DirectPay/Test/GetUrlForWithholding.aspx>

推送地址：cmbmobilebank://cmbls/functionjump?action=gofuncid&funcid=0026006

DES秘钥：12345678

1. 计算过程：

拼接字符串：AK0769000516001D3100010000N24http://99.6.150.121:832/HtmlBank/UserScene/DirectPay/Test/GetUrlForWithholding.aspxcmbmobilebank://cmbls/functionjump?action=gofuncid&funcid=0026006

32位MD5值：EF6FB8702C51F486B3E6C6408F865FF5

DES密文：9D20ED40A461ABC8E4ED62BEAC65F3560F20ED18B7B2899ADFD9DD27BDF2AF23FEB959B7D4642FCB

最终结果：

http://mobiletest.cmburl.cn/IGateway/Jump.aspx?funcid=0026008&MerchantNum=AK0769000516&TemplateNum=&ChargeBasis=&Use=001&CycleMode=D&Frequency=3&SingleLimit=1000&CycleLimit=10000&ValidityPeriod=24&ShroffAccount=&PartialDeductions=N&JumpUrl=http%253A%252F%252F99.6.150.121%253A832%252FHtmlBank%252FUserScene%252FDirectPay%252FTest%252FGetUrlForWithholding.aspx&PropelUrl=cmbmobilebank%253A%252F%252Fcmbls%252Ffunctionjump%253Faction%253Dgofuncid%2526funcid%253D0026006&Signature=9D20ED40A461ABC8E4ED62BEAC65F3560F20ED18B7B2899ADFD9DD27BDF2AF23FEB959B7D4642FCB

1. POST方式样例
2. 签约数据：

商户编号：AK0769000516

扣款依据：

用途代码：001

周期：D

频次：3

单笔限额：1000

周期限额：10000

收款账号：

是否允许部分扣款：N

有效期：24

完成页跳转链接：<http://99.6.150.121:832/HtmlBank/UserScene/DirectPay/Test/GetUrlForWithholding.aspx>

推送地址：cmbmobilebank://cmbls/functionjump?action=gofuncid&funcid=0026006

DES秘钥：12345678

1. 计算过程：

拼接字符串：AK0769000516001D3100010000N24http://99.6.150.121:832/HtmlBank/UserScene/DirectPay/Test/GetUrlForWithholding.aspxcmbmobilebank://cmbls/functionjump?action=gofuncid&funcid=0026006

32位MD5值：EF6FB8702C51F486B3E6C6408F865FF5

DES密文：9D20ED40A461ABC8E4ED62BEAC65F3560F20ED18B7B2899ADFD9DD27BDF2AF23FEB959B7D4642FCB

最终结果：

<form action="<http://mobiletest.cmburl.cn/IGateway/Jump.aspx?funcid=0026008>" method="post" >

<input type="hidden" name="MerchantNum" value="AK0769000516" />

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

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

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

<input type="hidden" name="Frequency" value="3" />

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

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

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

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

<input type="hidden" name="ValidityPeriod" value="24" />

<input type="hidden" name="JumpUrl" value="http%3A%2F%2F99.6.150.121%3A832%2FHtmlBank%2FUserScene%2FDirectPay%2FTest%2FGetUrlForWithholding.aspx" />

<input type="hidden" name="PropelUrl" value="cmbmobilebank%3A%2F%2Fcmbls%2Ffunctionjump%3Faction%3Dgofuncid%26funcid%3D0026006" />

<input type="hidden" name="Signature" value="9D20ED40A461ABC8E4ED62BEAC65F3560F20ED18B7B2899ADFD9DD27BDF2AF23FEB959B7D4642FCB" />

</form>

## 签约通知说明

1. 通知方式

签约成功后，业务系统将协议内容主动通知给商户。

1. 流程描述

商户发起签约，提供接收通知的地址；

客户完成签约后，我行按通知地址向商户发送协议内容；

1. 通知内容

通知内容包括：协议编号、付款账户、扣款用途、扣款依据、单笔限额、周期内累计限额、有效期、等。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **字段名** | **字段说明** | **类型** | **长度** | **出现要求** | **备注** |
| xcnvnbr | 协议编号 | string | 24 | M |  |
| xclteac | 付款账号 | string | 35 | M |  |
| xtrsuse | 扣款用途 | string | 3 | O |  |
| xtrsbas | 扣款依据 | string | 30 | O |  |
| xdrttyp | 是否允许部分扣款 | string | 1 | M |  |
| xctatyp | 限制期限类型 | string | 1 | M | Y：年  M：月  D：日 |
| xctatrm | 限制期限 | dec | 8 | O | 期限长度 |
| xctacnt | 限制次数 | dec | 8 | O | 期限内限制扣款次数 |
| xsglamt | 单笔限额 | dec | 15 | O |  |
| xperamt | 周期限额 | dec | 15 | M | 期限内限制扣款金额 |
| xEftdat | 生效日期 | Date | 8 |  |  |
| xexpdat | 失效日期 | date | 8 |  |  |
|  |  |  |  |  |  |

其他字段：xTskNbr：任务流水号，xLnkUr：发送地址，xCprNbr：商户编码，xSgnCnl：签约渠道，xSgnSeq：商户签约流水号，xStsCod：协议状态，xSpl100：冗余代码，当做技术字段，商户无需校验和处理。

通知内容以HTTP POST方式往商户URL推送，字符编码采用UTF-8，每个字段为一个表单参数发送，系统对通知内容进行签名，签名值采用signature字段进行传递，签名规则为：

对所有请求参数（signature除外）进行排序（Arrays.sort），排序完成后按将所有键值对以“&”符号拼接的到待签名字符串：

key1=value1& key 2=value2&…

对待签名字符串进行签名，得到signature字段值。

签名算法采用**SHA1WithRSA**。

验签公钥下载地址：

测试环境：<http://121.15.180.72/CmbBank_B2B/UI/GateWay/GetPublicKey.aspx>

生产环境：<https://b2b.cmbchina.com/CmbBank_B2B/UI/GateWay/GetPublicKey.aspx>

**说明：**

测试环境商户接收通知的URL地址不支持域名，只支持往商户的80、443、8081端口发送通知；

生产环境商户接收通知的URL地址支持域名，只支持往商户的80、443、8080、8443端口发送通知；

接收通知示例代码：

|  |
| --- |
| /\*\*  \* 获取请求参数中所有的信息 这种方式会将url地址中的参数读到map中，会导多出来这些信息从而致验签失败，这个时候可以自行修改过滤掉url中的参数  \*  \* **@param** request  \* **@return**  \*/  **public** **static** Map<String, String> getAllRequestParam(  **final** HttpServletRequest request) {  Map<String, String> res = **new** HashMap<String, String>();  Enumeration<?> temp = request.getParameterNames();  **if** (**null** != temp) {  **while** (temp.hasMoreElements()) {  String en = (String) temp.nextElement();  String value = request.getParameter(en);  res.put(en, value);  }  }  }  **return** res;  }  /\*\*  \* 组织待验签数据  \* **@param** noticeData  \* **@return**  \*/  **public** String getVerifyData(Map<String, String> noticeData) {  String[] keys = noticeData.keySet().toArray(**new** String[] {});  Arrays.*sort*(keys);  StringBuilder buffer = **new** StringBuilder();  **for** (String key : keys) {  String value = noticeData.get(key);  buffer.append("&").append(key).append("=").append(value);  }  **return** buffer.substring(1);  }  /\*\*  \* 通知数据验签  \* strToSign: getVerifyData获取的数据  \* strSign:signature的值  \* publicKey:验签公钥  \*/  **public** **static** **boolean** isValidSignature(String strToSign, String strSign,  String publicKey) {  **try** {  KeyFactory keyFactory = KeyFactory.getInstance("RSA");  **byte**[] encodedKey = Base64.decode(publicKey);  PublicKey pubKey = keyFactory  .generatePublic(**new** X509EncodedKeySpec(encodedKey));  java.security.Signature signature = java.security.Signature  .*getInstance*("SHA1WithRSA");  signature.initVerify(pubKey);  signature.update(strToSign.getBytes("UTF-8"));  **boolean** bverify = signature.verify(Base64.decode(strSign));  **return** bverify;  } **catch** (Exception e) {  e.printStackTrace();  }  **return** **false**;  } |

## 协议查询

1. 接口说明

1.1报文概要

1.1.1报文规范

1.1.1.1、系统采用HTTP接入，报文格式采用JSON，固定使用UTF-8编码方式。

1.1.1.2、报文由数据域和签名域组成，数据域名称为request或response（分别对应请求报文和响应报文），签名域名称为signature。signature域值为对数据域内容（不包含换行符及字段之间的空格，以{开始，}结束）进行哈希计算后对哈希数据进行签名获得的值（哈希算法采用SHA256）。

1.1.1.3、数据域包含head部分和body部分，head包含报文概要信息，body包含业务数据明细。head为固定域，不同业务的head定义方式一致，body字段定义参见各业务接口的详细定义。

1.1.1.4、商户接入时，可选择是否对body内容进行加密，若不使用加密，则通讯时HTTP请求头Content-Type值为application/json，若使用采用加密，则通讯时HTTP请求头Content-Type值为application/json\_enc。加密方式参见文档2.2节说明。

报文格式组织如下（以请求报文不加密为例）：

|  |
| --- |
| {  "request": {  "head": {  …  },  "body": {  …  }  },  "signature": "request值的哈希签名"  } |

若使用加密，则body内容为加密后的BASE64字符串，报文格式如下：

|  |
| --- |
| {  "request": {  "head": {  …  },  "body": "ASFASFASFASD"  },  "signature": "request值的哈希签名"  } |

1.1.2数据类型说明：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **类型** | **说明** | **分类** | **示例** |
|  | string | 字符串类型 | simpleType(简单类型) |  |
|  | date | 日期，格式为yyyyMMdd | simpleType(简单类型) |  |
|  | datetime | 日期和时间，格式为yyyyMMddHHmmss | simpleType(简单类型) |  |
|  | time | 时间，格式为HHmmss | simpleType(简单类型) |  |
|  | number(P，S) | 数字类型， P为精度位，S为小数位 | simpleType(简单类型) |  |
|  | list | 列表集合，名称对应列表名，集合中的参数单独描述 | complexType(复杂类型) |  |

出现要求：

M：必须出现；

C：条件出现，参数名必须出现，参数值可不出现；

ME：必须出现且于应答与请求保持一致

CE：如果出现，应答与请求保持一致

O：可选出现，参数名及值都可以不出现

1.2 报文定义



1.2.1 报文头

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **字段名** | **字段说明** | **类型** | **长度** | **出现要求** | **备注** |
| vernbr | 版本号 | string | 8 | ME | 固定为1.0 |
| mchnbr | 商户编号 | string | 8 | ME |  |
| mchtyp | 商户类型 | string | 15 | ME | 用于对接后台什么系统 |
| trscod | 交易编码 | string | 64 | ME | 用于标识什么业务 |
| msgidc | 报文通讯ID | string | 64 | ME | 返回报文原样返回（建议输入唯一值） |
| sigtim | 报文签名时间 | datetime | 14 | M | 格式：yyyyMMddHHmmss |
| retcod | 响应代码 | string | 1 | O | 本字段只返回报文有效，请求报文不需要传入。  S:与给业务系统通讯成功  F:与给业务系统通讯失败  E:与给业务系统通讯异常  **说明：本字段返回S只代表通讯上的成功，业务上是否成功请检查body内容中的相关字段** |
| retmsg | 响应描述信息 | string | 256 | O | 本字段只返回报文有效，请求报文不需要传入。 |

1.2.2 报文体

见下面文档：



1.2.3 报文示例

请求报文（未加密为例）：

|  |
| --- |
| {  "request": {  "head": {  "vernbr": "1.0",  "mchnbr": "AGP00001",  "mchtyp": "AGPNET",  "trscod": "A2DKVPLS",  "msgidc": "201808091330500001",  "sigtim": "20180831150000",  "sigalg": "SHA256WithRSA",  "sycflg": "0"  },  "body": "  <CMBSDKPGK>  <A2DKVPLSX1>  <CPRCOD>AK0769K00265</CPRCOD>  <CLTCNV></CLTCNV>  <EACNBR></EACNBR>  <CCYNBR></CCYNBR>  <CPRACT></CPRACT>  <STSCOD></STSCOD>  <SPL100></SPL100>  </A2DKVPLSX1>  </CMBSDKPGK>"  },  "signature": "VK6ld3CZ8oT9u/WhmMMjnmOVMa7fepEI/a8y0+KipeEs6dooWUC3nLjThZ1aDZUidtH4aIT8LPBMYtLEdNeW9AxYhu21hUyLIC0QabOzbkn  +ujXJmNP+9RtYUREFyjyeaaL4Zsbns5VIt+kJr2PclUUnrQC8LHOpnKZVZ2sWzcUSPRds23fNASF9O4hd/iFrSZXkIkDa0KuRM4xuT/BPEetgv3BcbBhI7BN  +gEQh43+ru+JlX5m+RgAZJwsbSgybUxEqsl5oWq7dpHx45nPnbjATstSzs2AiSw/yRsm7wZMu2IY+bnwIxe1TM25J89X6b6w2Sp/i7TOd/JHj75Qbew=="  } |

响应报文：

|  |
| --- |
| {  "response": {  "head": {  "vernbr": "1.0",  "mchnbr": "AGP00001",  "mchtyp": "AGPNET",  "trscod": "A2DKVPLS",  "msgidc": "201808091330500001",  "sigtim": "20180831150000",  "sigalg": "SHA256WithRSA",  "sycflg": "0"  "retcod": "S"  },  "body": ""  },  "signature": "AtDgV375/H2mHeeGuxM24FLbfmI0+Lup0MbkKuH4BFHT1o6/Hoibm6BvPxuH4F9xDqVPebzXwKly3/7h9+N82iYjg9++BC9Sao2Pvj5pDereWxCH3camOFhsbypQCqbkv6Eaha5KGhbYZmMqoebE27nX968wDZCgrawtM15s31MXhRXJ2j+Tzg0GZm78auK03h4FvAgCIZLklckuXvxG/KMMJlMIcO8GBYkIzDOTikPo3kQbmQg4qpiJQOoFXimoSECDa7LJsnQ7lQR6mtV3K89My7NsJh3z5ueXoRLD5HP7hkL2/uQpio29Q5rFS2Qgtt2HnD/J3LD5mpFfH5HPiw=="  } |
|  |

## 

1. 安全控制说明
   1. 安全控制方式

2.1.1 HTTPS服务

生产环境提供HTTPS接入。

2.1.2数据加密与解密（可选）

接入双方各自拥有一对RSA非对称密钥（标准的2048位X.509证书格式，可使用CA颁发的证书，也可采用工具生成），分别将公钥证书提供给对方进行。报文发送方使用对方公钥对请求报文中body部分进行加密（加解密算法采用RSA，填充模式采用PKCS#1 v1.5），接收方收到报文后采用己方私钥对加密内容进行解密。

2.1.3数据签名与验签

报文发送方需对报文内容进行哈希运算，并使用己方私钥对哈希结果进行签名（签名算法采用SHA256WithRSA），接收方使用对方提供的公钥对签名进行验证

* 1. 加密规范

2.2.1、若采用加密接入，则组装完body报文后，采用接收方公钥对body报文进行加密运算，加解密算法采用RSA，填充模式采用PKCS#1 v1.5；

2.2.2、对加密运算得到的字节数组进行BASE64，得到body域的值；

* 1. 签名规范

2.3.1、数字签名保证数据的可靠性和防抵赖性。数字签名由业务发起方编制，由业务接收方核验。

2.3.2、签名过程如下：

1）对请求报文或响应报文中的request、response节点中的内容(以{开始，以}结束，不包含报文字段间的空格和换行)进行哈希计算，哈希算法采用SHA256，得到计算后的字节数组。

2）使用商户私钥对哈希结果进行签名，签名算法采用SHA256WithRSA，对签名运算后的字节数组进行BASE64后获得signature的值。

## 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. 不限定周期时，CycleMode和Frequency可以不传，但传的话需两个都要传；
3. 协议有效期以月为单位；
4. 扣款依据ChargeBasis只能包含数字和字母，长度不超过20位；
5. 数据编码采用UTF-8；
6. 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、推送地址、秘钥等所有参数；
7. 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；
8. 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；
9. 商户参数配置等请请找主机联系人（一般为刘毅）进行支持，签约时若有弹框“温馨提示”报错，且错误内容有错误码，例如FIS9999-EPC0057等，也找主机联系人支持，对于url的生成规则如仍有疑问可联系手机银行联系人（一般为姜威）进行支持。