

标准收银台API-V3.1

文档修订记录

修订日期	修订内容	版本	修改人
2014/06/16	文档初建	V1.0	孙兴中
2014/09/09	完善文档	V1.1	连静
2015/05/19	新增RSA签名算法	V1.2	豆田莎
2016/01/19	1、删除申请Token步骤 2、修改请求字段version 值1.0.0->3.0.0 3、增加序列号reqSn	V2.0	韩雪平
2016/05/19	修改超时时间格式； 完善示例；	V2.1	豆田莎
2016/12/05	1、业务请求增加业务数据加密处理 2、同步返回增加数据加密 3、异步返回增加数据加密 4、修改商户前台同步通知返回格式为returnUrl?key=value 5、修改异步回调数据返回格式为noticeUrl?key=value 6、把数据统一返回为json格式 修改为： 数据同步返回为json格式	V3.0	胡雪峰
2017/09/27	通知参数增加交易类型	V3.1	李磊

1.概要

此文档专为先锋支付(以下统称先锋)支付平台的合作商户提供。目的是帮助商户的技术人员开发相关的接入程序。请相关技术人员详细阅读本手册。

2.产品说明

在收银台支付模式下，用户可以选择注册为先锋支付会员，也可以以匿名的方式进行支付，具体支付场景为：

- 1、在商户网站下单后跳转到先锋支付收银台。
- 2、用户可在收银台登陆后在完成跳转网银和其他支付操作；也可以不登陆，直接以匿名身份完成支付操作。

3.应用场景

3.1 收银台界面选择银行

 **先锋支付**
UCF PAY

 | 收银台

商家: 测试商户 | 产品信息: 测试商品

订单号: 20151111110427018 | 下单时间: 2015-11-11 11:05:30 | 交易金额: 0.10 元

储蓄卡

企业网银

网银支付

 中国工商银行
INDUSTRIAL BANK OF CHINA

 中国农业银行
AGRICULTURAL BANK OF CHINA

 中国建设银行
CHINA CONSTRUCTION BANK

 中国银行
BANK OF CHINA

其他银行 ▼

网银类型	单笔限额 (元)	每日限额 (元)	需要满足的条件
下一步			

3.2 收银台支付



中国农业银行
AGRICULTURAL BANK OF CHINA

在线支付平台

轻松在线 拥有无限

2015-11-11 11:12:04 星期三

优惠活动：尊敬的客户,我行支付界面进行了全新改版,详情请关注!

网银助手

订单信息

日期：2015/11/11 时间：11:07:52 支付类型：网上支付 币种：人民币

金额：**0.10** 商户：连连银通电... 商品：虚拟商品

订单号：20151111300270246

☐ K码支付

使用银行卡号、账户别名或动态验证码认证的支付方式

银行卡号：

请输入您的银行卡号\账户别名\电子支付卡号

验证码：


 [看不清，点击更换验证码](#)

☐ K宝/K令支付

下一步

重置

3.3完成支付后返回商户页面



先锋支付
UCF PAY

收银台

 恭喜您，支付成功！

2秒后为您返回商家界面 页面若未跳转，请点此[手动跳转](#)

先锋支付版所有 2005-2013 ICP证：辽ICP备13000797号

4.名词解释

名词	定义
商户订单号	本文所述的“商户订单号”为商户系统生成的唯一订单号。
商户号	商户在先锋支付平台注册的商户编码。

5.协议说明

- 1) 支付请求、订单查询，是HTTPS协议请求，商户以GET或POST方式发送到先锋支付平台。
- 2) 参数名称和参数说明中规定的固定值必须与列表中完全一致（大小写敏感）。
- 3) 商户接口签名方式为是RSA的签名，签名秘钥将通过安全渠道发送给商户。
- 4) 数据中不能包含“|”、“&”、“=”、“!”，这些字符为保留字符，中文变量使用UTF-8编码。

6.签名、加密规则

业务请求数据通过加密和签名两种方式保证数据安全性。

签名算法描述

根据所有的输入参数（不包括sign字段），按照参数名称进行自然排序(根据参数名称中的首字母进行A-Za-z的自然排序，如果首字母一样，则按照第二个字母进行排序，以此类推)，所得的排序集合按照标准的URI Query String格式以&符号链接在一起(注意：参数为空串的也需要加入链接)，首先进行MD5加密，返回一个小写的MD5串，然后将MD5串使用商户公钥执行RSA公钥加密，并将返回数据进行BASE64编码，所得BASE64编码串即为签名值。

伪代码描述：

```
String bizData = {"accountNo":"银行卡号","accountName":"户名","mobileNo":"手机号"};
//业务参数组装JSON格式
String data = AESCoder.encrypt(bizData,key); //使用AES进行加密，key是商户公钥
String requestData =
"data=fRQW79b/5n8FH1uyGPSu1Zm8lXK+mffKFOgvCYDT04BVkwM41g3qNZAO1yylA/seYGhmY=&mer
chantId=10000009999&reqSn=326263551863223&secId=RSA&service=REQ_WITHDRAW&version=4.0.
0";//按照参数名称排序,参数排序所有大写字母优先于小写字母。
String md5Val = MD5Utils.digest(requestData," utf-8" ).toLowerCase(); //首先进行MD5
byte[] signByte = RSAUtils.encryptByPublicKey(md5Val,key," utf-8" );
//然后执行RSA公钥加密，key是商户公钥。
String sign = Base64.encodeBase64String(signByte); //BASE64加密获得签名值
```

注：以上伪代码描述只是对实现原理的说明，使用java语言进行开发的商户可以直接调用demo中jar包下的com.ucf.sdk.UcfForOnline.createSign方法来获取sign。

RSA算法描述

名词缩写	
RSA	加密算法
X.509 标准	公钥编码标准

7.接入流程

7.1接入说明

先锋支付对商户提供统一的支付网关，地址如下：

<https://mapi.ucfpay.com/gateway.do>

7.2业务请求

以下参数列表中所有“非空”项：Y表示不允许为空，N表示可为空。

7.2.1 请求参数

变量名称	变量命名	长度定义	非空	说明
接口名称	service	MAX(30)	Y	固定值：TO_UCF_CASHIER
签名算法	secId	MAX(20)	Y	固定值：RSA
接口版本	version	MAX(10)	Y	固定值：4.0.0
序列号	reqSn	MAX(32)	Y	本次请求的唯一标识。请使用先锋提供的方法。
商户号	merchantId	MAX(32)	Y	唯一确定的一个商户号，商户在先锋开户时，由先锋告知商户。
加密业务数据	data	无限制	Y	本次请求中所有业务字段加密后的值。
订单签名数据	sign	无限制	Y	商户使用RSA签名算法将明文串进行签名后的数据。签名规则见6

data加密字段

变量名称	变量命名	长度定义	非空	说明
------	------	------	----	----

商户订单号	merchantNo	MAX(32)	Y	商户系统生成的订单号，唯一标识一笔支付订单，不同的商户订单号在先锋支付平台将对应不同的支付订单。
来源	source	MAX(1)	Y	固定值：1（表示PC端）
产品类型	productType	MAX(10)	N	接入收银台的产品类型： W：网银
付款方	payerId	MAX(32)	N	付款方ID，仅限与先锋支付实现用户关联的商户，选填
金额	amount	MAX(16)	Y	以分为单位
币种	transCur	MAX(10)	Y	固定值：156（表示人民币）
卡种	accountType	MAX(1)	N	固定值：1或者2 （1:借记卡 2:信用卡）
商品名称	productName	MAX(100)	Y	填写商户的商品名称
商品信息	productInfo	MAX(500)	N	填写所售商品详细信息，中文编码使用UTF-8
前台通知地址	returnUrl	MAX(320)	Y	需填写合法的URL，支持http或https协议；交易结束，将客户引导到商户的此URL，即通过客户浏览器post交易结果信息到商户的此URL
后台通知地址	noticeUrl	MAX(320)	N	需填写合法的URL，支持http或https协议；交易结束，支付系统将支付结果信息通知到此URL

订单超时时间	expireTime	MAX(32)	N	订单超时时间，到达该时间点仍未支付成功的订单，先锋支付平台会将该订单置为失败，格式：yyyy-MM-dd HH:mm:ss，为空则使用先锋支付平台默认超时时间（交易申请时间起7天）
保留域	memo	MAX(2000)	N	商户保留域 原样回传

7.2.2 请求示例

```
<form id="payForm" action="Signature" method="post">
  <input type="text" id="service" name="service" value=" TO_UCF_CASHIER" />
  <input type="text" id="secId" name="secId" value="RSA" />
  <input type="text" id="version" name="version" value="4.0.0" />
  <input type="text" id="reqSn" name="reqSn" value="8TSNn5zs2r1ndMy6" />
  <input type="text" id="merchantId" name="merchantId" value="10000009999" />
  <input type="text" id="data" name="data"
value="IAQXEcQCLYE3x5GVQvpjDHlfL6zk9uTGnBtzrwbI1Ds+r3zFUaFp56jmZDMatuOdIMKyRcSHxCMCQ
3VRs8OqTPu75lzONYL90w=" />
  <input type="text" id="sign" name="sign" value="HUHUJIIIMONJIIIBYFTGICNDN" />
</form>
```

7.2.3 成功返回

跳转到网银界面。



中国农业银行
AGRICULTURAL BANK OF CHINA

在线支付平台

轻松在线 拥有无限

2015-10-28 18:40:35 星期三

优惠活动：尊敬的客户,我行支付界面进行了全新改版,详情请关注!

网银助手

订单信息

日期：2015/10/28 时间：18:38:27 支付类型：网上支付 币种：人民币

金额：**0.01** 商户：先锋支付有... 商品：ucfpay

订单号：1510280105516891

☐ K码支付

使用银行卡号、账户别名或动态验证码认证的支付方式

银行卡号：

请输入您的银行卡号\账户别名\电子支付卡号

验证码：



[看不清,点击更换验证码](#)

☐ K宝/K令支付

下一步

重置

7.2.4 失败返回

跳转到先锋支付失败页面。

? 不能识别的附件

7.3支付结果通知

先锋支付根据接口定义将订单支付结果发往商户系统(仅在支付成功和失败时进行通知)，通过post方式返回给商户提供的URL（支付请求中的returnUrl及noticeUrl）。

支付结果通知必须以后台（noticeUrl）通知为准。

7.3.1 通知参数

数据返回内容统一为一串密文，解密后是json格式。

变量名称	变量命名	长度定义	非空	说明
商户号	merchantId	MAX(32)	Y	支付请求传入的参数
商户订单号	merchantNo	MAX(32)	Y	支付请求传入的参数
金额	amount	MAX(16)	Y	以分为单位
币种	transCur	MAX(10)	Y	固定值：156（表示人民币）

交易成功时间	tradeTime	MAX(32)	Y	格式：YYYYMMDD Dhhmmss
交易订单号	tradeNo	MAX(32)	Y	先锋支付平台交易 订单号
保留域	memo	MAX(2000)	N	商户保留域原样回传
订单状态	status	MAX(1)	Y	S：成功 F：失败
交易类型	tradeType	MAX(10)	N	B2B、B2C
订单签名数据	sign	无限制	Y	商户使用RSA签名 算法将明文串进行 签名后的数据。签 名规则见6

注：

- 1、商户接收到通知数据后，需要先对返回的数据解密（参照jar包的解密方法）然后根据sign域对报文做验签，规则参照签名、加密规则6。
- 2、(1) 商户将 先锋支付结果通知 的参数（除了sign）排序后进行MD5加密然后得到小写的MD5的值；
(2) 商户将先锋发送的支付结果通知的RSA的sign解密成MD5的值（先BASE64解密，再RSA解密）；
(3) 判断这（1）和（2）的结果值是否相同，如果相同则验签成功；
- 3、第2条是对验签原理的说明，java开发商户可以调用demo中jar包的com.ucf.sdk.UcfForOnline.verify方法进行验签。
- 4、noticeUrl异步通知请不要以写死的数据来获取参数，请获取异步通知的全部报文，遍历取参。

7.3.2 商户前台通知显示（同步）

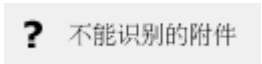
报文

【通知商户】内容：

返回加密数据：
ZG8durJCYFEHAreFNWpvpf2IU27NpHdhuDYwZrvvcVPqd+moTcUB1qKAUJWRutk9gAKzSKdY+IAQXEcQ
CLYE3x5GVQvpjDHIfl6zk9uTGnBtzrwbI1Ds+r3zFUaFp56jmZDMatuOdIMKyRcSHxCMCQ3VRs8OqTPu75lz
ONLY90w=
解密后格式，商户前台同步返回格式为key=value格式：
returnUrl?amount=10&memo=&merchantId=10000009999&merchantNo=20150109022501484&status
=S&tradeNo=201501151426021031610000004010&tradeTime=20150115142602&transCur=156

注：returnUrl是商户传过来的前台通知地址。

页面



7.3.3 商户后台通知（异步）

报文

【通知商户】内容：

返回加密数据：
ZG8durJCYFEHAreFNWpvpf2IU27NpHdhuDYwZrvvcVPqd+moTcUB1qKAUJWRutk9gAKzSKdY+IAQXEcQ
CLYE3x5GVQvpjDHlfl6zk9uTGnBtzrwbI1Ds+r3zFUaFp56jmZDMatuOdIMKyRcSHxCMCQ3VRs8OqTPu75lz
ONLY90w=
解密后格式，数据异步返回为key=value格式：
noticeUrl?amount=10&memo=&merchantId=10000009999&merchantNo=20150109022501484&status
=S&tradeNo=201501151426021031610000004010&tradeTime=20150115142602&transCur=156&sign=
HUDOSJSKDNVCHHUIHCDHOSJOIHSCJB

注：noticeUrl是商户传过来的后台通知地址。

7.4 商户后台通知应答

商户收到先锋的报文并验签成功，需要给先锋支付平台返回“SUCCESS ”（大写），先锋支付收到“ SUCCESS ”便会认为商户收到通知，否则将会重复通知商户，最多通知20次，时间间隔依次延长。

7.5 单笔订单查询

商户系统根据商户订单号单笔查询先锋订单的处理结果

7.5.1请求参数

变量名称	变量命名	长度定义	非空	说明
接口名称	service	MAX(30)	Y	固定值：REQ_ORDER_QUERY_BY_ID
签名算法	secId	MAX(20)	Y	固定值：RSA
接口版本	version	MAX(10)	Y	固定值：4.0.0
序列号	reqSn	MAX(32)	Y	本次请求的唯一标识。请使用先锋提供的方法（见demo示例）。

商户号	merchantId	MAX(32)	Y	唯一确定的一个商户号，由商户在先锋开户时，由先锋告知商户。
商户订单号	merchantNo	MAX(32)	Y	商户系统生成的订单号，唯一标识一笔支付订单，不同的商户订单号在先锋支付平台将对应不同的订单。
订单签名数据	sign	无限制	Y	商户使用RSA签名算法将明文串进行签名后的数据。签名规则见6

7.5.2 请求示例

```
<form id="payForm" action="Signature" method="post">
  <input type="text" id="service" name="service" value="REQ_ORDER_QUERY_BY_ID" />
  <input type="text" id="secId" name="secId" value="RSA" />
  <input type="text" id="version" name="version" value="4.0.0" />
  <input type="text" id="reqSn" name="reqSn" value="USO1iEEfv4QyKtQnzNhKfX1of" />
  <input type="text" id="merchantId" name="merchantId" value="10000009999" />
  <input type="text" id="merchantNo" name="merchantNo" value="20150111064334277" />
  <input type="text" id="sign" name="sign" value="HUHUNDIDJOIEDIONEFIGBRI" />
</form>
```

7.5.3 返回参数

查询成功

变量名称	变量命名	长度定义	非空	说明
商户号	merchantId	MAX(32)	Y	支付请求传入的参数
商户订单号	merchantNo	MAX(32)	Y	支付请求传入的参数
金额	amount	MAX(16)	Y	以分为单位
币种	transCur	MAX(10)	Y	目前只支持人民币：156

保留域	memo	MAX(2000)	Y	商户保留域 原样回传
交易订单号	tradeNo	MAX(32)	Y	先锋支付平台交易订单号
订单状态	status	MAX(1)	Y	S：成功 F：失败 I：处理中
交易成功时间	tradeTime	MAX(32)	N	格式：YYYYMMDDhhmmss

查询失败

变量名称	变量命名	长度定义	非空	说明
应答码	errorCode	MAX(8)	Y	详见：8应答码说明
应答码信息	errorMsg	无限制	N	详见：8应答码说明

7.5.4 返回格式

数据返回内容统一为一串密文，解密后是json格式。

失败样例：

返回加密数据：
ZG8durJCYFEHAreFNWpvpf2IU27NpHdhuDYwZrvvcVPqd+moTcUB1qKAUJWRutk9gAKzSKdY+IAQXEcQCLYE3x5GVQvpjDHlfL6zk9uTGnBtzrwbI1Ds+r3zFUaFp56jmZDMatuOdIMKyRcSHxCMCQ3VRs8OqTPu75lzONYL90w=
解密后格式：
{"resCode":"10009","resMessage":"交易记录不存在"}

成功样例：

返回加密数据：
ZG8durJCYFEHAreFNWpvpf2IU27NpHdhuDYwZrvvcVPqd+moTcUB1qKAUJWRutk9gAKzSKdY+IAQXEcQCLYE3x5GVQvpjDHlfL6zk9uTGnBtzrwbI1Ds+r3zFUaFp56jmZDMatuOdIMKyRcSHxCMCQ3VRs8OqTPu75lzONYL90w=
解密后格式：
{"merchantId":"10000009999","merchantNo":"20150111064334277","amount":"10","transCur":"156","memo":"","tradeNo":"201501151845241031610000004029","status":"I","tradeTime":"20151127132311"}

8.应答码说明

应答码	应答码含义
00000	成功
00001	已受理
00002	订单处理中
10000	参数不合法
10001	参数值传入错误
10002	业务不支持
10003	渠道未开通
10004	银行返回失败
10005	订单重复提交
10006	订单已超时关闭
10007	用户或商户编号不存在
10008	业务处理中
10009	交易记录不存在
10010	账户余额不足
10011	未开通无卡支付
10012	退款次数超限
10013	累计退款金额超限
10014	卡BIN查询无记录
10015	鉴权失败
10024	姓名、身份证、卡号不一致
10025	超银行限额
10026	账户不存在
10027	银行通讯异常
10028	账户状态异常
10029	打款认证次数超限
10030	未进行支付操作
10031	产品编码配置异常

20000	系统内部错误
20001	服务调用超时
20002	支付平台内部服务调用错误
99999	未定义错误类型
99020	验签失败

9.常见问题

问题	说明
为什么收到不到通知信息	我方存在白名单策略，商户需要将我方出口IP添加到网关，且我方需要将商户接收通知的IP加入白名单。
网银支付页面商户名称为什么不一样	支付渠道所限制，不影响用户充值或支付。
网银支付为什么有的显示银行页面、有的显示银联页面	先锋支付会根据商户请求选择最合适的支付渠道。
两个通知页面的地址noticeUrl和returnUrl如何调用	1、noticeUrl：是在用户支付成功后，支付通知以http的形式通知商户成功，叫后台通知地址。 2、returnUrl：是在用户跳转网银支付成功后，返回商户网站的前台URL。
商户传参时noticeUrl和returnUrl的格式	1、需要加上 http://头 2、地址末尾请不要加斜线 / 3、假设商户传参地址形如： http://shanghu.com?value1=1&value2=2 商户本地进行RSA加密计算sign值的时候，需要把value1和value2 也加密。
accountType 卡种	借记卡的请传值=1，信用卡的请传值=2，借贷不区分请在请求先锋传参的时候，不传该参数。