协议支付（首验标准版）API5-V1.0

目录

文档修订记录

修订日期	修订内容	版本	修改人
2018/11/13	开发版本创建	V1.0	邹玉梅

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

先锋支付提供协议支付免短验API接口，实现协议支付的通道能力。API接口模式由商户收集用户支付要素，通过支付申请提交给先锋支付。

3.应用场景

主要适用于持卡人在商户网站消费使用协议支付场景。

3.1免短验支付

消费用户在商户平台选中商品确认付款时，跳转到商户收银台选择银行并使用协议支付免短验支付方式，由商户平台收集用户信息，包括银行卡号，户名，身份证号码，银行预留手机号等，收集完支付要素后调用先锋支付的“免短验支付”接口，完成支付。

3.2订单查询

由于网络服务调用可能存在没有接到响应的情况，可通过查询接口进行订单状态查询，查询结果可作为订单最终状态进行处理。

4.名词解释

名词	定义
商户号	商户在先锋支付平台注册的商户编码，由先锋支付下发给商户，在先锋支付平台用于区分不同商户。
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。

5.协议说明

1）采用HTTP标准的GET或POST协议，发送请求到先锋支付平台。

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）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、加密说明

1）请求和应答报文通过签名和验签机制保证数据的传输安全和身份认证，签名方式为RSA2。

2）业务数据通过AES加密保证数据安全性，加密方式为AES/ECB/PKCS5Padding。

3）商户可以使用由先锋提供的SDK包进行加解密及签名验签处理。

7.接入说明

7.1接入地址

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接入准备

1）下载先锋签名验证工具包（sdk-tool.zip）

访问先锋商户后台首页https://b.ucfpay.com，右下方点击下载”先锋签名验证工具包 “（sdk-tool.zip）

2）使用先锋签名验证工具包生成商户密钥

解压
1）中下载的工具包（sdk-tool.zip），运行解压后文件夹内的“先锋支付RSA签名验签工具"，点击生成密钥（将生成Base64格式商户私钥和公钥，请妥善保存）

3）上传商户公钥

登录先锋商户后台https://b.ucfpay.com，选择“系统设置”菜单，点击”上传商户公钥 “，将 2）中生成的商户公钥（Base64格式字符串）上传

4）下载先锋公钥证书（ucfpay.der）

登录先锋商户后台https://b.ucfpay.com，选择“系统设置”菜单，点击”下载先锋证书 “，运行2）中“先锋支付RSA签名验签工具” ，点击”解析证书 “，将先锋公钥证书（ucfpay.der）解析成公钥字符串（Base64格式）

7.3调用示例（JAVA语言示例）

7.3.1请求报文处理流程：

1）将请求参数中data字段组装Map对象，例如：

```
Map<String, String> params = new HashMap<String, String>();
params.put("merchantNo", "1qaz2wsx");
params.put("bankId ", "ICBC");
……
```

2）使用先锋SDK生成请求数据

String reqData =UcfForOnline.generateRequest(service, version, merchantId, params, xf_pub_key, mer_pri_key);

说明：

（1）reqData 为进行过签名和加密后生成的请求数据；

（2）入参service为接口名称；

（3）入参version为接口版本，固定值为5.0.0；

（4）入参merchantId为商户号；

（5）入参params为上述 1）中组装的Map对象；

（6）入参xf_pub_key为先锋公钥；

（7）入参mer_pri_key为商户私钥；

3）向先锋网关发送请求数据reqData

向先锋API网关发送http请求，提交请求数据reqData。

7.3.2接收报文处理流程：

1）使用先锋SDK进行验签，例如：

String verifyResult = UcfForOnline.verify(params, xf_pub_key);

说明：

（1）verifyResult等于true为验签通过；

（2）入参params为先锋的响应报文(JSON字符串)；

（3）入参xf_pub_key为先锋公钥。

2）判断网关返回码code

（1）code=99000，接口调用成功，进行后续的 3）处理；

（2）code=99001，接口调用异常，无法确认订单状态，需要调用订单查询接口确认订单状态后再进行后续处理或者重新发送请求；

（3）其他返回码，接口调用失败，可置订单为失败。

3）网关返回码code=99000时，使用先锋SDK进行解密，例如：

String bizData = UcfForOnline.decryptData(params, mer_pri_key);

说明：

（1）bizData等于解密后的业务数据，例如：

{"mobileNo":"手机号",……,"sign":"HUBDYBICBSUIHUHDHBD"}；

（2）入参params为先锋的响应报文(JSON字符串)；

（3）入参mer_pri_key为商户私钥。

7.4后台异步通知重发机制

商户收到先锋支付平台的异步通知报文并验签成功后，需要给先锋支付平台返回“SUCCESS“（大写），先锋支付平台收到”SUCCESS“便会认为商户收到通知，否则将会重复通知商户。

重复通知采用退避策略，退避策略的具体方法为2^(i-1) 分钟发送重复通知，其中i是重新发送的次数i∈[1, 14]。在重新发送通知的过程中，只要有一次成功，则中断重发策略。如果通知 14
次后也没有被商户接收成功则不再发通知，商户可通过订单结果查询接口进行查询。

商户需要做好重复通知的控制，避免重复通知导致重复入账。

8.接口说明

8.1首验支付

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。

8.1.1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	由先锋支付定义，商户传入固定值：REQ_CONTRACT_PAY
接口版本	version	MAX(10)	Y	由先锋支付定义，商户传入固定值：5.0.0
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使用随机密钥进行AES加密后的值。
AES加密秘钥	tm	无限制	Y	本次请求的随机密钥
订单签名数据	sign	无限制	Y	商户使用RSA（商户私钥）签名算法将明文串进行签名后的数据。

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。 支付要素变更需更换商户订单号重新提交支付申请。
签约号	contractNo	MAX(64)	Y	银行卡签约成功后返回的签约号
金额	amount	MAX(16)	Y	以分为单位
币种	transCur	MAX(10)	Y	由先锋支付定义，商户传入固定值：156（表示人民币）
用户类型	userType	MAX(2)	N	由先锋支付定义，商户传入固定值：1（对私）。
开户省	branchProvince	MAX(32)	N	银行账户对应的开户省
开户市	branchCity	MAX(32)	N	银行账户对应的开户市
开户支行名称	branchName	MAX(32)	N	银行账户对应的开户支行名称
商品名称	productName	MAX(100)	Y	填写商户所售的商品名称
商品信息	productInfo	MAX(500)	N	填写所售商品详细信息
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

8.1.2返回参数（同步）

变量名称	变量命名	长度定义	非空	说明
网关返回码	code	MAX(5)	Y	详见：9 应答码说明
网关返回码描述	message	MAX(128)	N	详见：9 应答码说明
商户号	merchantId	MAX(32)	Y	原样返回请求传入的参数。
加密业务数据	data	无限制	N	本次应答中所有业务字段加密后的值。
AES加密秘钥	tm	无限制	N	本次应答的随机密钥
订单签名数据	sign	无限制	Y	使用RSA（先锋私钥）签名算法将明文串进行签名后的数据。

data业务字段：

变量名称	变量命名	长度定义	非空	说明

应答码	resCode	MAX(5)	Y	详见：9 应答码说明 调用先锋支付接口收到先锋支付返回应答码resCode，表示应答状态或失败错误码，不代表订单状态，不能以该字段作为支付订单状态依据
应答信息	resMessage	MAX(128)	N	详见：9 应答码说明
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
交易订单号	tradeNo	MAX(32)	N	先锋支付平台交易订单号
订单状态	status	MAX(2)	N	先锋支付交易订单状态： I（支付处理中） S（支付成功） F（支付失败） 调用先锋支付接口报网络异常、没有收到先锋支付返回报文，或者先锋支付返回status为空，不能当作失败，只能当作处理中，需要调用查询接口确认
交易完成时间	tradeTime	MAX(14)	N	格式：YYYYMMDDhhmmss 订单状态为终态S或F时存在
保留域	memo	MAX(2000)	N	商户保留域 原样回传

金额	amount	MAX(16)	N	以分为单位
币种	transCur	MAX(10)	N	由先锋支付定义， 固定值：156（表示人民币）

8.1.3后台通知（异步）

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14次，时间间隔依次延长。

变量名称	变量命名	长度定义	非空	说明
网关返回码	code	MAX(5)	Y	详见：9 应答码说明
网关返回码描述	message	MAX(128)	N	详见：9 应答码说明
商户号	merchantId	MAX(32)	Y	原样返回请求传入的参数。
加密业务数据	data	无限制	N	本次应答中所有业务字段加密后的值。
AES加密秘钥	tm	无限制	N	本次应答的随机密钥
订单签名数据	sign	无限制	Y	使用RSA（先锋私钥）签名算法将明文串进行签名后的数据。

data业务字段：

变量名称	变量命名	长度定义	非空	说明
应答码	resCode	MAX(5)	Y	详见：9 应答码说明 调用先锋支付接口收到先锋支付返回应答码resCode，表示应答状态或失败错误码，不代表订单状态，不能以该字段作为支付订单状态依据
应答信息	resMessage	MAX(128)	N	详见：9 应答码说明

金额	amount	MAX(16)	Y	以分为单位
商户号	merchantId	MAX(32)	Y	支付请求传入的参数
商户支订单号	merchantNo	MAX(32)	Y	支付请求传入的参数
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(2)	Y	先锋支付交易订单状态： S（支付成功） F（支付失败）
交易完成时间	tradeTime	MAX(14)	Y	格式：YYYYMMDDhhmmss 订单状态为终态S或F时存在
币种	transCur	MAX(10)	Y	固定值：156（表示人民币）
保留域	memo	MAX(2000)	N	商户保留域 原样回传

8.2 订单查询

8.2.1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：REQ_PROTOCOL_QUERY_BY_ID
接口版本	version	MAX(10)	Y	固定值：5.0.0
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使用随机密钥进行AES加密后的值。
AES加密秘钥	tm	无限制	Y	本次请求的随机密钥，通过RSA（先锋公钥）加密算法加密后生成AES加密密钥。
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。

data业务字段：

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	需要查询的商户订单号。

8.2.2返回参数（同步）

变量名称	变量命名	长度定义	非空	说明
网关返回码	code	MAX(5)	Y	详见：9 应答码说明
网关返回码描述	message	MAX(128)	N	详见：9 应答码说明
商户号	merchantId	MAX(32)	Y	原样返回请求传入的参数。
加密业务数据	data	无限制	N	本次应答中所有业务字段加密后的值。
AES加密秘钥	tm	无限制	N	本次应答的随机密钥
订单签名数据	sign	无限制	Y	使用RSA（先锋私钥）签名算法将明文串进行签名后的数据。

data业务字段：

变量名称	变量命名	长度定义	非空	说明

应答码	resCode	MAX(5)	Y	详见：9 应答码说明 调用先锋支付接口收到先锋支付返回应答码resCode，表示应答状态或失败错误码，不代表订单状态，不能以该字段作为支付订单状态依据 当resCode=10009时，表示先锋支付未落单，可以原单号重新发起
应答信息	resMessage	MAX(128)	N	详见：9 应答码说明
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
交易订单号	tradeNo	MAX(32)	N	先锋支付平台 交易订单号
订单状态	status	MAX(2)	N	先锋支付交易订单状态： I（支付处理中） S（支付成功） F（支付失败） 调用先锋支付接口报网络异常、没有收到先锋支付返回报文，或者先锋支付返回status为空，不能当作失败，只能当作处理中，需要调用查询接口确认

交易完成时间	tradeTime	MAX(14)	N	格式：yyyyMMdd HHmmss 订单状态为终态S或F时存在
签约号	contractNo	MAX(64)	N	签约成功时候返回
保留域	memo	MAX(2000)	N	商户保留域 原样回传

9.1网关返回码

应答码	含义
99000	接口调用成功
99001	接口调用异常
其他返回码，接口调用失败，具体如下：	
99016	参数无效
99020	签名校验失败
99021	service不存在
99022	sign key 不存在
99023	verify sign failure
99024	服务调用异常
99025	转发URL异常
99026	参数异常
99027	service为空
99028	merchantId 为空
99029	商户密钥不存在
99030	防重复请求码校验失败
99031	服务版本号version错误
99032	请求IP非法
99033	数据解密失败
99034	数据加密失败

9.2业务返回码

应答码	含义

00000	成功
10000	参数不合法
10001	参数值传入错误
10003	渠道未开通
10007	用户或商户编号不存在
10009	交易记录不存在
10011	未开通无卡支付
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
10031	产品编码配置异常
20000	系统内部错误
20001	服务调用超时
20003	通讯异常
20001	服务调用超时
20003	通讯异常
20004	短信校验次数超限
20005	短信校验失败
20006	短信发送次数超限
20007	短信发送失败
99999	未定义错误类型

10.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。

商户传参时noticeUrl的格式	1、需要加上http://头 2、地址末尾请不要加斜线 / 3、地址请不要采用GET传参数，例如：http://shanghu.com?value1=1&value2=2