

聚合支付接口文档V1.0.2

创建日期	版本号	内容	创建人
2017-05-09	V 1.0.0	聚合支付文档创建	孟璐
2017-08-08	V 1.0.1	聚合支付文档商户输入参数调整	杨杰
2017-09-01	V 1.0.2	聚合支付文档增加QQ公众号支付，扫码支付和商户报备	杨杰

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

先锋支付为满足广大商户O2O收银场景需要，方便消费者选择多种支付方式，而提供的聚合支付产品。

3应用场景

商户在线下放置收款二维码，由消费者扫描后输入金额形成订单，跳转至指定支付收银台（如微信支付）完成支付。

4名词解释

名词缩写	定义
订单号	本文所述的“单号”为商户系统生成的订单号。（唯一性）
商户代码	商户在先锋支付平台注册的商户编码（唯一性）。

5协议说明

- 1）接口请求参数商户以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）目前商户接口签名方式为是RSA的签名，RSA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.签名和加密规范

接口请求的业务数据需要经过AES加密处理，请求需要有签名。

6.1数据加密规范

商户所有请求支付的数据需经过加密处理，具体加密规则如下：

数据加密采用AES对称加密方式，将所有业务字段组装成JSON格式，加密后数据与接口参数一起参与签名。

伪代码描述：**注意AES加密算法：AES/ECB/PKCS5Padding**

```
String bizData = "{\"accountNo\":\"\",\"accountName\":\"\",\"mobileNo\":\"\"}"; //JSON
String data = AESCoder.encrypt(bizData,key); //AESJSONkeyRSA
```

6.2 签名规范

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升序排序，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：**注意RSA签名算法：SHA1withRSA**

```
String dateStr = data=ahduifh917yr781h3y816831&merchantId=123456780&secId=RSA&service=JH_PAY &reqSn=y
9ZUCiqAl8n5Uv4gOZX2mQEce4SjEKmx&version=4.0.0
String md5Val = MD5Utils.digest(dateStr,"utf-8").toLowerCase(); //dataStrMD5
byte[] signByte = RSAUtils.encryptByPublicKey(md5Val,key,"utf-8");//md5ValRSA
String sign = Base64.encodeBase64String(signByte); //BASE64
```

生成sign方法：java语言版,String sign = UcfForOnline.createSign(String signKey, String signName, Map<String, String> params, String type) signKey:密钥值 signName:sign params:参数 type:签名类型(RSA|MD5)

RSA算法标准

名词缩写	
RSA	加密算法
X.509 标准	公钥编码标准

6.3 序列号规范

reqSn序列号生成规则：保证唯一，以免和其他商户重复

reqSn java语言版：

String reqSn = UnRepeatCodeGenerator.createUnRepeatCode(merchantId, service, outOrderId);

其中outOrderId可为空，merchantId为先锋支付给商户开通的商户编号，service为接口说明中的服务名称，生成工具会提供给接入商户（见附件）

reqSn 非java语言版由商户自己生成，确保唯一即可。

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：

1、生产环境：<https://mapi.ucfpay.com/gateway.do>

生产环境商户号及密钥，见运营开通商户号说明邮件；

2、联调测试环境：<http://111.203.205.26:8085/gateway.do>

测试环境商户号：M200000250

测试密钥:

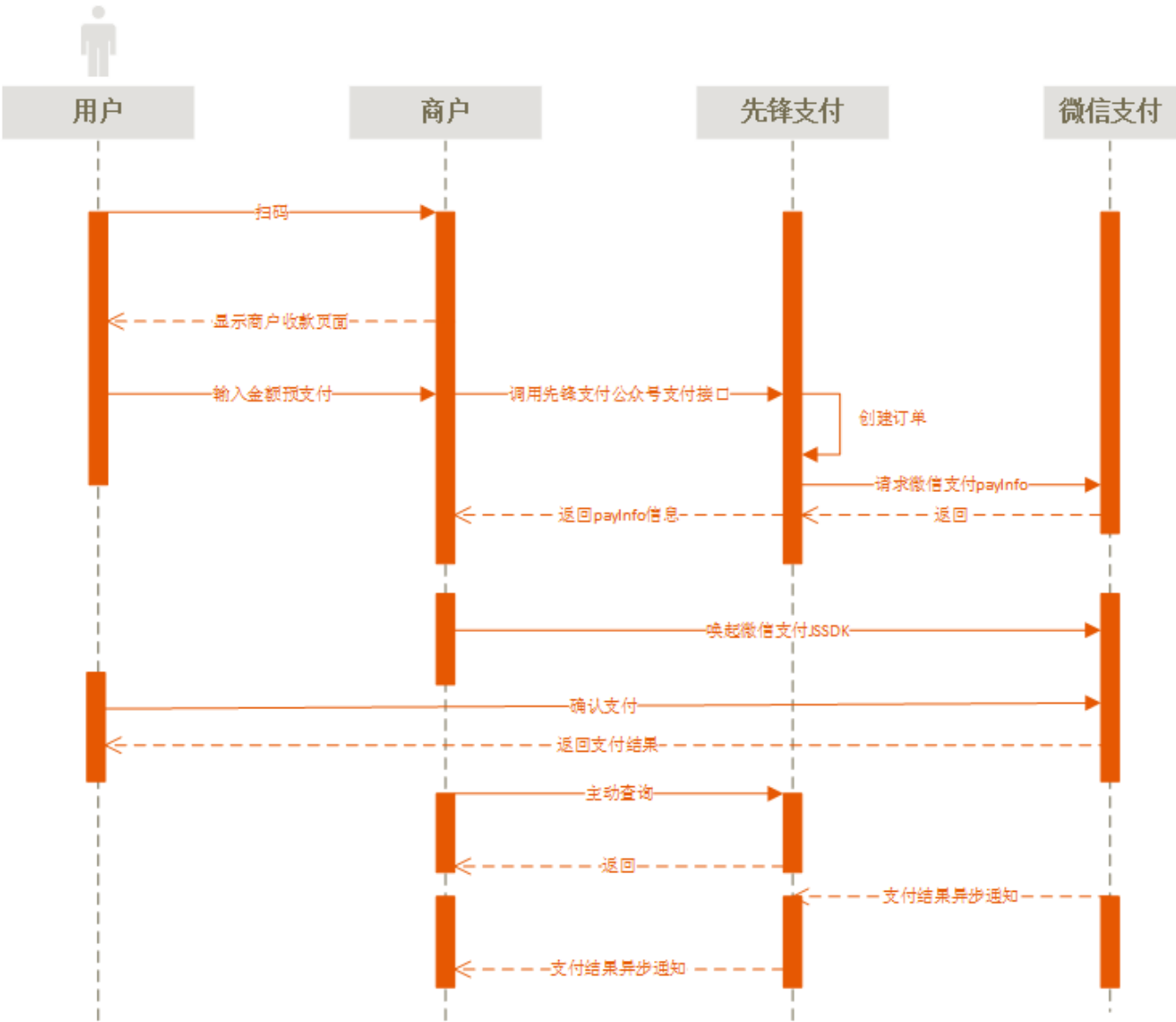
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDYBx+etRclHCchSGOtzk/hHBdAM+qaMKoYivh+jsqrBCshR62sH25mpL1EpQ
N8U1EfsZli02gv16nf6Kk/j2AiSsH+fbPBmOguWpX4ETCAvxBmoobCuqDgl8ilXSDNc65rxVags68azqWeYWZtT1gNXWU3llhRQArM6
VOh69GclQIDAQAB

7.2 接入规则

7.3请求说明

7.3.1 公众号支付 (公众号支付接口)

公众号接入流程：



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：JH_GZH_PAY
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	参见 6.3序列号规范
商户号	merchantId	MAX(32)	Y	由商户在先锋开户时，由先锋告知商户。
加密业务数据	data	无限制	Y	针对下方描述的加密字段加密得到的字符串。
签名	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

data6.1

变量名称	变量命名	长度定义	非空	说明
金额	amount	MAX(16)	Y	支付金额（单位：分）
订单号	outOrderId	MAX(32)	Y	商户系统生成 确保唯一性
商品名称	productName	MAX(256)	Y	商品名称
后台通知URL	noticeUrl	MAX(320)	Y	后台通知URL
前台通知URL	returnUrl	MAX(320)	Y	前台通知URL
失败通知URL	failUrl	MAX(320)	N	失败通知URL
取消支付URL	cancelUrl	MAX(320)	N	用户取消支付后跳转指定 页面（重定向）URL
是否支持信用卡	isLimitCreditPay	MAX(10)	Y	是否支持信用卡 0 无限制（信用卡，借记卡 ）1 不支持信用卡
支付类型	payType	MAX(10)	Y	微信支付：WXPAY 支付宝支付：ALIPAY QQ支付：QQPAY
业务类型	bizType	MAX(10)	Y	定值：200
子商户ID	subMerchantId	MAX(32)	Y	子商户ID
子商户名称	subMerchantName	MAX(128)	Y	子商户名称
方法版本	methodVersion	定值	Y	定值：1.0
商户类型	merchantType	MAX(5)	Y	定值：OUT
公众号ID	appId	MAX(50)	N	注意：微信公众号支付此 参数必传, 此参数为微信 公众号appId
用户标识	openId	MAX(128)	N	注意：微信公众号支付此 参数必传, 此参数为微信 用户在商户对应appid下 的唯一标识。
币种	transCur	MAX(10)	Y	人民币：156
商户授权令牌	appAuthToken	MAX(128)	N	注意：支付宝服务窗该参 数必传，通过该令牌来帮 助商户发起请求，完成业 务
卖家支付宝用户ID	sellerId	MAX(28)	N	注意：支付宝服务窗如果 该值为空，则默认为商户 签约账号对应的支付宝用 户ID
买家支付宝账号	buyerLogonId	MAX(128)	N	注意：支付宝服务窗买家 支付宝账号，和buyerId 不能同时为空
买家的支付宝唯一用户号	buyerId	MAX(32)	N	注意：支付宝服务窗买家的 支付宝唯一用户号（2 088开头的16位纯数字） ,和buyerLogonId不能同 时为空
订单标题	orderTitle	MAX(128)	N	注意：支付宝服务窗该参 数必传，订单标题
门店编号	storeId	MAX(32)	N	注意：支付宝服务窗该参 数必传，商户门店编号
终端号	terminalId	MAX(32)	N	注意：支付宝服务窗该参 数必传，商户机具终端编 号

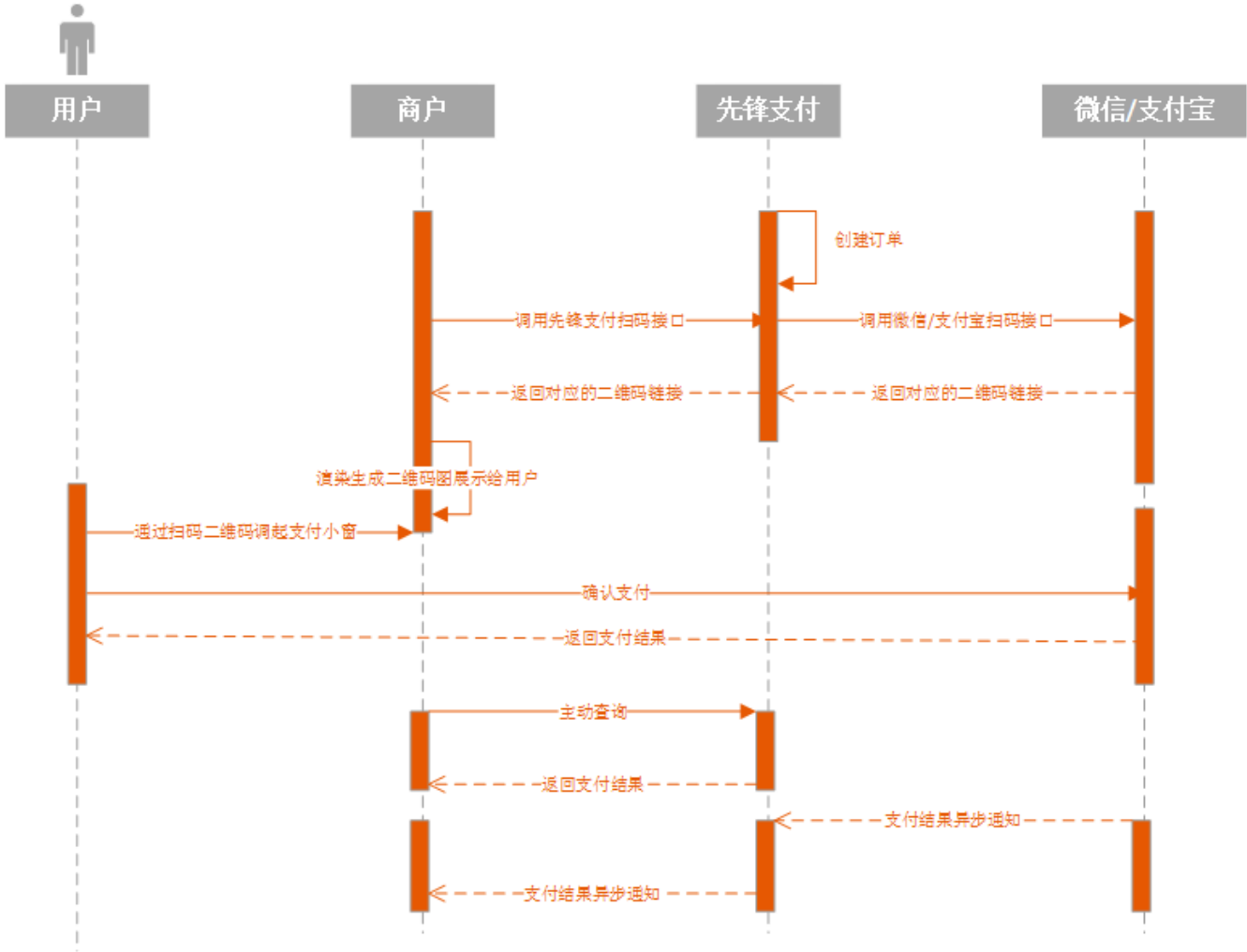
返回结果（采用6.1数据加密规范加密数据，需要解密）

变量名称	变量命名	长度定义	非空	说明
返回状态	status	MAX(8)	Y	00：操作成功 其他：失败
返回信息	respMsg	无限制	Y	返回信息
支付信息	payInfo	无限制	N	调起微信支付所需信息

7.3.2 扫码支付（正扫）

动态生成二维码，显示商品信息和金额，用户直接通过微信或者支付宝或者银联APP扫码即可进行支付

扫码支付正扫接入流程：



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：JH_PSCAN_PAY
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	参见 6.3序列号规范
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。
加密业务数据	data	无限制	Y	加密字段见下方说明

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（加密规则见6.1数据加密规范）

变量名称	变量命名	长度定义	非空	说明
金额	amount	MAX(16)	Y	支付金额（单位：分）
订单号	outOrderId	MAX(32)	Y	商户系统生成 确保唯一性
商品名称	productName	MAX(256)	Y	商品名称
后台通知URL	noticeUrl	MAX(320)	Y	后台通知URL
前台通知URL	returnUrl	MAX(320)	Y	前台通知URL
是否支持信用卡	isLimitCreditPay	MAX(10)	Y	是否支持信用卡 0 无限制（信用卡，借记卡） 1 不支持信用卡
支付类型	payType	MAX(10)	Y	微信支付：WXPAY 支付宝支付：ALIPAY Q Q支付：QQPAY
业务类型	bizType	MAX(10)	Y	定值：200
商户类型	merchantType	MAX(5)	Y	定值：OUT
子商户ID	subMerchantId	MAX(32)	Y	子商户号
子商户名称	subMerchantName	MAX(128)	Y	子商户名称
方法版本	methodVersion	定值	Y	定值:1.0
请求来源	source	MAX(10)	Y	1：PC 2：移动端
币种	transCur	MAX(10)	Y	人民币：156
门店编号	storeId	MAX(50)	N	门店编号
门店名称	storeName	MAX(100)	N	门店名称
终端设备号	terminalId	MAX(50)	N	终端设备号
交易场景	tradeScene	MAX(10)	N	ONLINE：线上 OFFLINE：线下 注意： 不传默认为线下

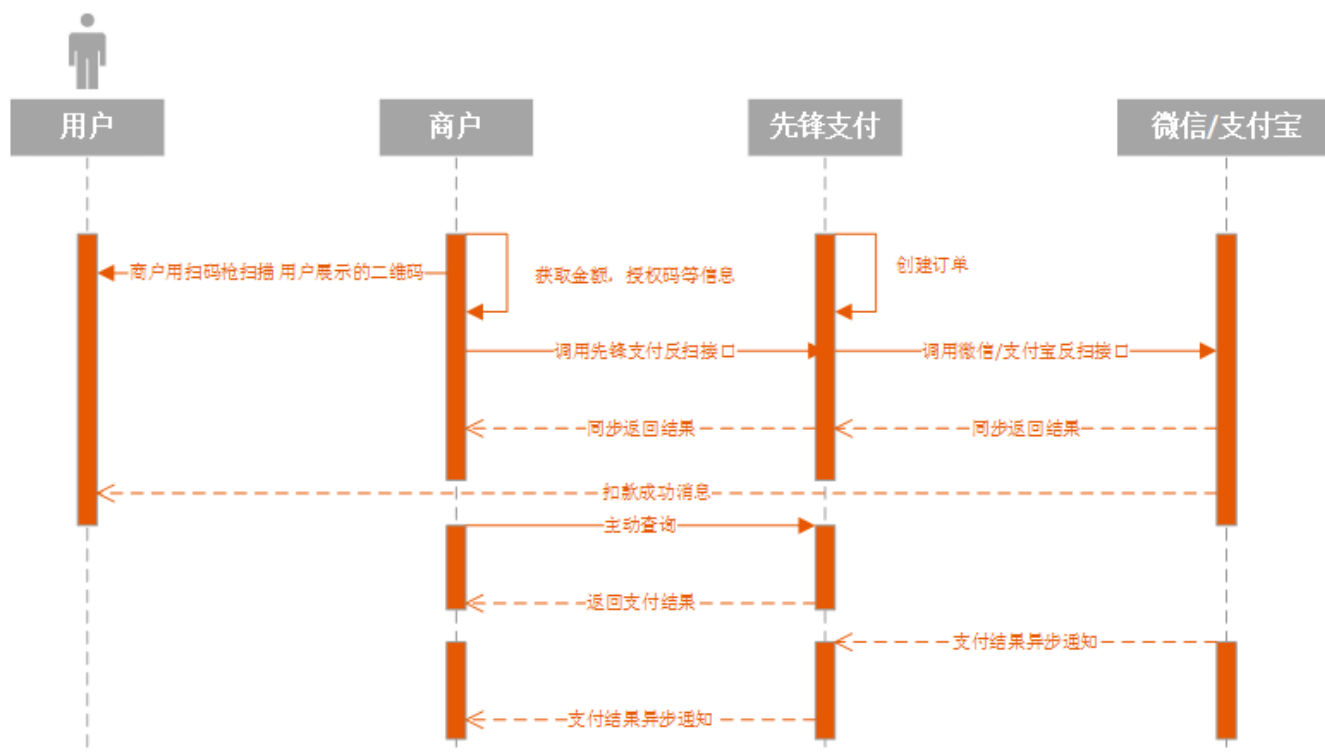
返回结果（采用6.1数据加密规范加密数据，需要解密）

变量名称	变量命名	长度定义	非空	说明
返回状态	status	MAX(8)	Y	00：操作成功 其他：失败
返回信息	respMsg	无限制	Y	返回信息
微信或者支付宝或者银联 返回生成二维码URL	payInfo	无限制	N	微信或者支付宝或者银联 返回生成二维码URL

7.3.3 扫码支付（反扫）

商户通过扫码枪扫描用户微信或者支付宝付款码进行扣款

扫码支付反扫接入流程：



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：JH_RSCAN_PAY
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	参见 6.3序列号规范
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。
加密业务数据	data	无限制	Y	加密字段见下方说明
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（加密规则见6.1数据加密规范）

变量名称	变量命名	长度定义	非空	说明
金额	amount	MAX(16)	Y	支付金额（单位：分）
订单号	outOrderId	MAX(32)	Y	商户系统生成确保唯一性
商品名称	productName	MAX(256)	Y	商品名称
后台通知URL	noticeUrl	MAX(320)	Y	后台通知URL
前台通知URL	returnUrl	MAX(320)	Y	前台通知URL
支付类型	payType	MAX(10)	Y	微信支付：WXPAY 支付宝支付：ALIPAY Q Q支付：QQPAY
业务类型	bizType	MAX(10)	Y	定值：200
授权码	authCode	MAX(128)	Y	扫码支付授权码

商户类型	merchantType	MAX(5)	Y	定值：OUT
子商户ID	subMerchantId	MAX(32)	Y	子商户号
子商户名称	subMerchantName	MAX(128)	Y	子商户名称
方法版本	methodVersion	定值	Y	定值:1.0
币种	transCur	MAX(10)	Y	人民币：156

返回结果（采用6.1数据加密规范加密数据，需要解密）

变量名称	变量命名	长度定义	非空	说明
返回状态	status	MAX(8)	Y	00：操作成功 其他：失败
返回信息	respMsg	无限制	Y	返回信息
订单状态	orderStatus	MAX(2)	N	00 成功 01 失败 02 处理中 03 待支付

7.3.4 单笔订单查询(通用)

根据订单号从商户系统单笔查询先锋订单的处理结果。

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：JH_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	参见 6.3序列号规范
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。
加密业务数据	data	无限制	Y	加密字段见下方说明
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（加密规则见6.1数据加密规范）

变量名称	变量命名	长度定义	非空	说明
商户订单号	outOrderId	MAX(32)	Y	需要查询的商户订单号
方法版本	methodVersion	定值	Y	定值:1.0

返回结果（采用6.1数据加密规范加密数据，需要解密）

变量名称	变量命名	长度定义	非空	说明
返回状态	status	MAX(8)	Y	00：操作成功 其他：失败
返回信息	respMsg	无限制	Y	返回信息
商户号	merchantId	MAX(32)	N	支付请求传入的参数

商户订单号	outOrderId	MAX(32)	N	支付请求传入的参数
金额	amount	MAX(16)	N	以分为单位
订单状态	orderStatus	MAX(1)	N	00：成功 01：失败 02：处理中 03：待支付
交易成功时间	tradeTime	MAX(32)	N	格式：yyyy-MM-dd HH:mm:ss
微信或者支付宝单号	outTradeNo	MAX(100)	N	微信或者支付宝单号
卡类型	bankReturnCardType	MAX(2)	N	0：零钱 1：储蓄卡 2：信用卡

7.3.5 商户报备

报备子商户信息到微信进行审核

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：JH_MERCHANT_REPORT
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	参见 6.3序列号规范
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。
加密业务数据	data	无限制	Y	加密字段见下方说明
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（加密规则见6.1数据加密规范）

变量名称	变量命名	长度定义	非空	说明
报备类型	reportType	MAX(10)	Y	微信报备：WXPAY 支付宝报备：ALIPAY Q Q报备：QQPAY
商户名称	merchantName	MAX(50)	Y	该名称是公司主体全称，绑定公众号时会对主体一致性校验
商户简称	merchantShortname	MAX(20)	Y	该名称是显示给消费者看的商户名称
客服电话	servicePhone	MAX(20)	Y	例如：010-89920000
联系人	contact	MAX(20)	N	注意：报备类型为支付宝时必传
联系电话	contactPhone	MAX(11)	N	例如：13800000000
联系邮箱	contactEmail	MAX(30)	N	例如：test@test.com

经营类目	business	MAX(32)	Y	行业类目，请填写对应的ID， 见详细列表 例如：101
联系人类型	contactWechatidType	MAX(32)	N	注意：报备类型为支付宝时必传 取值范围：LEGAL_PERSON:法人；CONTROLLER：实际控制人；AGENT：代理人；OTHER：其他
联系人帐号	contactWechatid	MAX(32)	N	例如：OPENID_012312321
商户备注	merchantRemark	MAX(20)	Y	同一个受理机构，特约商户“商户备注”唯一。商户备注重复时，生成商户识别码失败，并返回提示信息“商户备注已存在，请修改后重新提交” 例如：商户的唯一备注
方法版本	methodVersion	定值	Y	定值:1.0
子商户ID	subMerchantId	MAX(32)	Y	子商户ID
商户类型	merchantType	MAX(5)	Y	定值：OUT
渠道号	channelId	MAX(32)	N	渠道号
身份证号	idCardNo	MAX(32)	N	注意：报备类型为支付宝时必传
商户来源	source	MAX(20)	N	注意：报备类型为支付宝时可传，渠道商的支付宝PID
交易场景	tradeScene	MAX(10)	N	ONLINE：线上 OFFLINE：线下 注意：不传默认为线下

返回结果（采用6.1数据加密规范加密数据，需要解密）·

变量名称	变量命名	长度定义	非空	说明
返回状态	status	MAX(8)	Y	00：操作成功 其他：失败
返回信息	respMsg	无限制	Y	返回信息

7.4支付结果通知机制

先锋支付支付平台对商户的支付请求数据处理完成后，会将处理的结果（**成功才通知，失败和异常不通知，商户通过订单结果查询来查询订单状态，商户要保障订单的幂等，避免重复通知入账**）数据通过服务器主动通知的方式通知给商户的通知地址，此地址就是支付请求时的 noticeUrl。通知机制为常见7.4

7.4.1 6.1

通知参数获取方式建议为遍历请求中的参数列表。用以增加接口的扩展性。（注）

伪代码描述：

```
//先锋支付异步通知商户返回数据格式为：data=密文串
String parameters=request.getParameter("data");
String dataJson = AESCoder.decrypt(parameters, rsaPublicKey);//rsaPublicKey为先锋支付给商户开通的商户号的公钥
JSONObject jsonObject = JSONObject.parseObject(dataJson);

Iterator paiter = jsonObject.keySet().iterator();//此处需要遍历 获取签名值signValue 和 签名字段signParameters

//验签
boolean verifyResult = UcfForOnline.verify(rsaPublicKey,"sign", signValue, signParameters, "RSA");
```

变量名称	变量命名	长度定义	非空	说明
商户号	merchantId	MAX(32)	Y	由商户在先锋开户时，由先锋告知商户。
订单号	outOrderId	MAX(32)	Y	商户系统生成确保唯一性
金额	amount	MAX(16)	Y	支付金额 单位:分
交易时间	tradeTime	MAX(50)	Y	格式为：“yyyy-MM-dd HH:mm:ss”
订单状态	orderStatus	MAX(2)	Y	00：成功
微信或者支付宝单号	outTradeNo	MAX(50)	Y	微信或者支付宝单号
卡类型	bankReturnCardType	MAX(2)	Y	0：零钱 1：储蓄卡 2：信用卡
签名	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

变量名称	变量命名	长度定义	非空	说明
响应状态	errno	MAX(32)	Y	“0” 受理成功，其他失败
响应信息	errorMsg	MAX(32)	Y	响应信息

7.5补单机制（通知重发机制）

在交易结束后先锋支付后台会将交易结果发送给商户,若一次没有发送成功，通过退避策略重新发送后台交易通知。退避策略的具体方法为 2^i (i-1) 分钟发送后台交易结果通知，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。其中i是重新发送的次数， $i \in [1, 14]$ 。

如果通知 14 次后也没有被商户接受成功则不再发通知，由商户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**）。

商户端在接收到交易通知时，应该立即确认已经收到，并且丢弃重复的交易结果通知。