

盛派网络

# 微信公众号+小程序快速开发

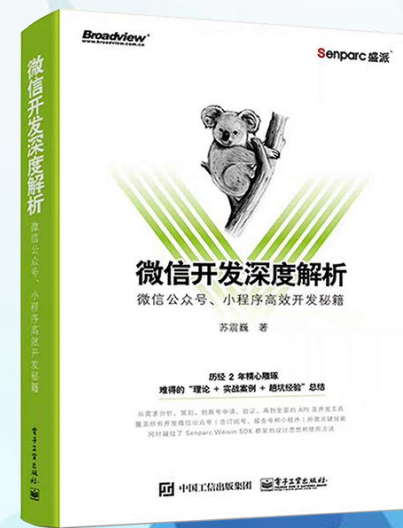
---

苏震巍

## 第21节：微信支付：微信支付接口规则

所需课时：2/5

延伸参考：《微信开发深度解析》第19章



## 学习目标：

- 1、学习微信支付的相关配置。
- 2、学习微信支付的基本业务流程以及规则。

提示：更多信息请仔细阅读《微信开发深度解析》第19章学习

## SDK 源代码:

<https://github.com/JeffreySu/WeiXinMPSDK>

**参考 Sample 源代码:**  
[Senparc.Weixin.MP.Sample](#)



**BookHelper:**  
<https://book.weixin.senparc.com>



## 课堂案例源代码下载:

<https://github.com/JeffreySu/WechatVideoCourse>

**微信入群加个人微信:** SenparcWechat (盛小嗨)  
**QQ学员群 (14群) :** 588231256

# 接口规则

几乎所有的微信支付流程都遵照同一套严格的规则，包括了协议规则、参数格式规定、安全规范等。

- 1) 协议规则
- 2) 参数规定
- 3) 安全规范
- 4) 获取Opeld



## 1) 协议规则

- 传输方式
- 提交方式
- 数据格式
- 字符编码
- 签名算法
- 签名要求
- 证书要求
- 判断逻辑

- 传输方式

为保证交易安全性，采用 HTTPS 传输。

Senparc.Weixi SDK 中所有的主动请求微信服务器的 URL 已经使用了 HTTPS 协议，但在微信支付的整个流程过程中，会涉及到回调地址（由微信服务器异步访问开发者服务器），此时的协议是由开发者服务器决定的，并且即使开发者服务器使用 HTTP 系统也不会返回错误信息，但是这样做是非常不安全的。DNS 劫持、运营商插入广告、数据被窃取、提交数据被修改等安全风险是一直存在的。

\*有关HTTPS和证书的知识再版的时候也可以考虑添加。参考  
[https://pay.weixin.qq.com/wiki/doc/api/jsapi.php?chapter=10\\_4](https://pay.weixin.qq.com/wiki/doc/api/jsapi.php?chapter=10_4)

- **提交方式**

采用 POST 方法提交。

Senparc.Weixin SDK 对于主动请求的 API 已经全部使用 POST 方法提交。



- **数据格式**

提交和返回数据都为 XML 格式，根节点名为 xml。

- 字符编码

统一采用 UTF-8 字符编码。

尤其在中文网站中，有的站点会全局设置 GB-2312 为默认的编码方式，**Senparc.Weixin SDK** 中默认的编码即为 **UTF-8**，在使用微信支付相关接口的时候请保留默认设置！

- 签名算法

MD5，后续会兼容 SHA1、SHA256、HMAC 等。

- 签名要求

请求和接收数据均需要校验签名，详细方法请参考本章 19.4.3 节《安全规范》。

**注意：**

很多开发者在回调的过程中往往会忽视对签名的验证，认为只要是已经有了HTTPS，微信发送过来的信息都是可信的，实际上主机名、IP、内容等信息都存在被篡改的可能，并且也不应该排除为了容错而多次收到同一条消息的可能，因此，在回调方法中必须对签名进行验证。



- 证书要求

调用申请退款、撤销订单接口需要商户证书（详情请见本章 19.4.3 节《安全规范》）。

简单地说，资金流入微信支付账户，不需要提供商户证书，但是有资金流出的时候（包括发红包、企业付款），必须要提供商户证书。



- 判断逻辑

先判断协议字段返回，再判断业务返回，最后判断交易状态。

这条规则也适用于其他场景。

## 2) 参数规定

- **body字段格式要求 (参考19.4.2.1)**
- **交易金额**
- **交易类型**
- **货币类型**
- **时间**
- **时间戳**
- **商户订单号**

- body字段格式要求（参考19.4.2.1）

- **交易金额**

交易金额默认为人民币交易，接口中参数支付金额单位为“分”，最小单位也是“分”，因此参数值必须为整数，不能带小数点。对账单中的交易金额单位为“元”。外币交易的支付金额同样精确到币种的最小单位，不能带小数点。

### • 交易类型

交易类型有两大类：

1. JSAPI：公众号支付  
NATIVE：原生扫码支付  
APP：App 支付
2. MICROPAY：刷卡支付，刷卡支付有单独的支付接口，不调用统一下单接口



- **货币类型**

目前默认的是 CNY：人民币。

- **时间**

标准北京时间，时区为东八区。如果商户的系统时间为非标准北京时间，参数值必须根据商户系统所在时区先换算成标准北京时间，例如商户所在地为 0 时区的伦敦，当地时间为 2014 年 11 月 11 日 0 时 0 分 0 秒，换算成北京时间为 2014 年 11 月 11 日 8 时 0 分 0 秒。

- **时间戳**

标准北京时间，时区为东八区，自 1970 年 1 月 1 日 0 点 0 分 0 秒以来的秒数。注意：部分系统取到的值为毫秒级，需要转换成秒（10 位数字）。

### • 商户订单号

商户支付的订单号由商户自定义生成，微信支付要求商户订单号保持唯一性（建议根据当前系统时间加随机序列来生成订单号）。重新发起一笔支付要使用原订单号，避免重复支付；已支付过或已调用关单、撤销（请见本章 19.6 节《微信支付API》）的订单号不能重新发起支付。



- 银行类型

微信目前为各类银行和机构对应设置了 252 个不同的银行编码，由于内容比较长，可以扫描下方二维码进行查看：



577#564



### 3) 安全规范

- 签名算法
- 生成随机数算法
- 商户证书安全
- 商户回调 API 安全

- 签名算法

微信支付的签名算法和 JS-SDK 等逻辑基本一致（参考第 18 章 18.2.2 节《获取签名》），这里不再赘述。

为了提高安全性和可维护性，我们还是将这部分算法封装到了独立的方法中。具体位置为：RequestHandler 类中的 CreateMd5Sign() 方法，相关参数说明如表所示。

参数名称	类型	必填	说明
key	string	是	参数名
value	string	否	参数值，为 null 时此 key-value 不参与签名

注意，此方法不能一次性带入所有的参数完成签名，而是带入最后一个需要签名的参数，然后统一生成签名。其余的参数都储存在 RequestHandler 类中的 Parameters 变量中。其中参数 key 是必填的（哪怕为空字符串，但不能为 null），value 为 null 时，这个 key-value 不会参与到签名过程中。

- **生成随机数算法**

微信支付 API 接口协议中包含字段 `nonce_str`，主要保证签名不可预测。

实现此算法的方法为 `TenPayV3Util.GetNoncestr()`，实现的原理为取随机数然后转乘随机字符串，再进行一次 MD5 加密。

### • 商户证书安全

证书文件必须要防止被他人下载，因此，不能放在可以被下载到文件的目录中，例如 wwwroot 目录下（包括子目录或虚拟目录），应放在当前应用程序池控制账户拥有访问权限的其他目录中（通常为 ApplicationPoolIdentity 或 NetworkService 等内置账户）。商户服务器要需要做好病毒和木马防护工作，以防被非法侵入者窃取证书文件。

**注意：**对于服务器使用的是使用虚拟主机“空间”的情况，当无法使用“空间”以外的储存路径时，建议将证书文件放在 App\_Data 目录下（此目录是受访问保护的，无法直接通过网页访问下载其中的文件），并重命名文件，以 # 开头，如：#apiclient\_cert.p12。



- **商户回调 API 安全**

如 19.4.1 节《协议规则》中建议的那样，回调的方法应当使用 HTTPS 协议，并且进行一系列充分的安全验证。



## 4) 获取OpenId

微信支付所使用的 OpenId 即所绑定的微信公众号的 OpenId，授权方式都是 OAuth2.0，对于网站类型的应用请参考本视频教程第15-17课，或书本第 16 章《微信网页授权（OAuth 2.0）》

## 课后作业：

- 1、默认货币类型缩写为？
- 2、微信支付时间为什么时区的时间？
- 3、微信支付使用什么参数识别不同的用户？该参数如何获取？