

Q/CUP

中国银联股份有限公司规范性文档

中国银联移动支付业务 商户接入技术改造指南

中国银联股份有限公司 发布

版本修订信息

版本号	完成日期	拟稿和修改人	发布日期	变更说明
1.0.0	2012-11-21	陈超、郑晓燕		初稿
1.0.1	2013-05-15	陈超		新增 SDK 使用 ASP 版本

目录

1	文档说明.....	4
1.1	功能描述.....	4
1.2	阅读对象.....	4
1.3	业务术语.....	4
1.4	技术服务.....	5
2	功能演示.....	5
3	功能演示数据交互.....	6
3.1	消费交易流程.....	7
3.2	交易信息查询流程.....	9
4	商户开发步骤向导.....	9
4.1	支付控件调用开发步骤.....	10
4.2	后台交易开发步骤.....	10
4.3	查询接口开发步骤.....	10
5	商户联调步骤向导.....	11
6	前台通知与后台通知说明.....	11
7	查询接口说明.....	13
7.1	前台交易（消费等交易）.....	13
7.2	后台交易（退货、消费撤销等交易）.....	13
8	签名机制.....	13
8.1	生成待签名的字符串.....	13
8.1.1	需要参与签名的参数.....	13
8.1.2	生成待签名字符串.....	13
8.2	签名.....	14
8.3	如何验证是否移动支付业务请求.....	14
9	商户密钥获取与使用.....	15
10	SDK 使用.....	16
10.1	JSP/JAVA（java.zip）.....	16
10.2	PHP（php.zip）.....	17
10.3	ASP.NET（asp.net.zip）.....	18
10.4	ASP（asp.zip）.....	19
11	常见问题问答.....	20

1 文档说明

参与方描述:

商户	指加入银联网络，与银联签订银联移动支付业务合作协议开展银联移动支付业务的商户。
----	---

1.1 功能描述

中国银联移动支付系统，为商户和持卡人提供安全、方便、快捷的支付渠道，通过银联移动支付渠道，付款者可以直接通过银行卡进行移动手机支付。

1.2 阅读对象

《UPMP商户接入技术改造指南》文档是面向具有一定的网站开发能力，了解PHP、JAVA 等开发语言中的一种的网站开发、维护和管理人员。

1.3 业务术语

表1-1 业务术语

术语	解释
请求	通过 HTTP 协议把需要传输的数据发送给接收方的过程。
应答	通过 HTTP 协议把需要传输的数据返回给接收方的过程。
后台通知	服务器后台通知。中国银联移动支付根据得到的数据处理完成后，移动支付系统主动发起通知给商户的网站，同时携带处理完成的结果信息反馈给商户网站。
前台类交易	主要指用户需要参与交互的支付类交易，包括消费、预授权类交易。
后台类交易	主要指用户不需要参与交互，由商户后续发起的交易，包括消费撤销、退货、预授权撤销、预授权完成、预授权完成撤销等交易。

1.4 技术服务

在开发或使用银联移动支付接口时，产生疑问或出现问题：

银联客服热线：95516

2 功能演示

本章节功能演示以IOS控件UI界面为主。

步骤1：商户后台推送订单信息至移动支付系统，移动支付系统返回交易流水号至商户后台。

步骤2：商户后台转发交易流水号至手机客户端，调起支付控件，界面跳转到移动支付安全支付控件支付要素输入页面。

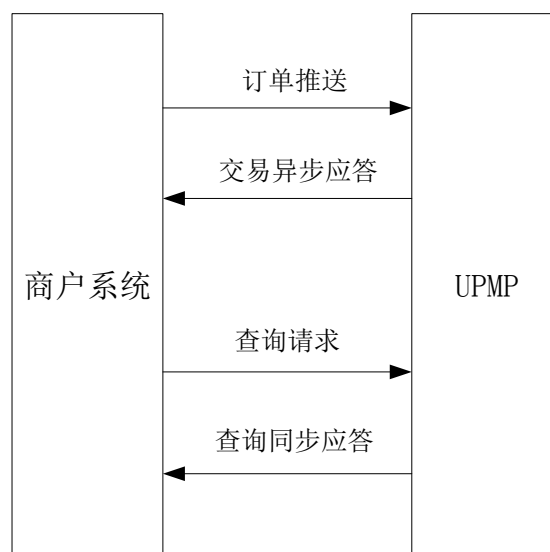


The screenshot displays a mobile application interface for UnionPay. At the top, the status bar shows '中国联通' (China Unicom) and the time '下午3:43'. Below the status bar is a blue header with three tabs: '返回' (Return), '储蓄卡快捷支付' (Debit Card Quick Payment), and '常用银行卡' (Common Bank Card). The main content area is a light blue box containing two input fields. The first field is labeled '卡号' (Card Number) and contains the text '626226 0902 1904 6814'. Below this field is the prompt '请输入银行卡卡号' (Please enter the bank card number). The second field is labeled '银行卡密码' (Bank Card Password) and contains the text '*****4'. Below this field is the prompt '请输入银行卡密码' (Please enter the bank card password). At the bottom of the light blue box is a large blue button labeled '确定支付' (Confirm Payment).

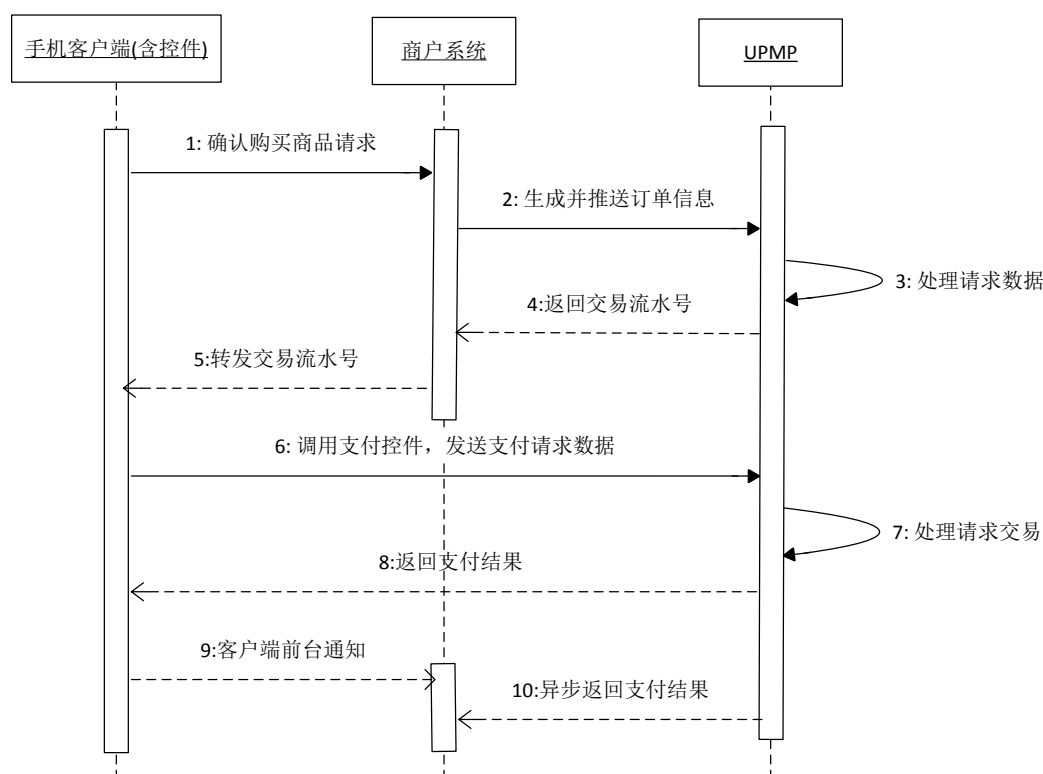
步骤3：支付结束提示完成信息，并可以返回控件界面



3 功能演示数据交互



3.1 消费交易流程



(1) 浏览并选购商品

用户通过手机客户端与商户系统交互浏览选购商品, 客户端向商户系统发送购买商品请求数据。

(2) 生成并推送订单信息请求数据

商户系统根据选购商品请求数据生成订单数据集, 把构造完成的订单信息数据集合按照移动支付系统的订单信息推送接口, 通过商户后台提交 (POST) 的方式传递给移动支付系统。

(3) 移动支付系统对请求数据进行处理

移动支付系统得到这些集合后, 会先进行安全校验等验证, 一系列验证通过后便会处理这次发送过来的数据请求。

(4) 返回交易流水号

移动支付系统返回商户系统交易流水号应答。

(5) 转发交易流水号

商户系统转发交易流水号至手机客户端。

(6) 调用支付控件, 发起支付请求数据

手机客户端收到交易流水号等要素，调起支付控件，用户输入支付信息后，客户端按照移动支付系统的支付接口规则组装并发送支付请求数据至移动支付系统。

(7) 移动支付系统对请求数据进行处理

移动支付系统得到这些集合后，会先进行安全校验等验证，一系列验证通过后便会处理这次发送过来的数据请求。

(8) 返回支付结果

移动支付系统返回结果至手机客户端。

(9) 返回支付结果

手机客户端发送前台支付结果通知（参数frontEndUrl）。

(10) 移动支付系统后台异步返回处理的结果数据

对于成功处理完成的交易，移动支付系统服务器主动发起通知，调用商户在请求时设定好的后台通知地址路径（参数backEndUrl），把支付结果数据反馈给商户。

(11) 商户对获取的返回结果数据进行处理

商户在前台通知处理页面（参数frontEndUrl指定页面）或服务器后台通知页面（参数backEndUrl指定页面）获取移动支付返回的结果数据后，可以结合自身网站的业务逻辑进行数据处理（如：订单更新等操作）。以后台通知为准。若未收到后台通知，需要发起交易信息查询请求。

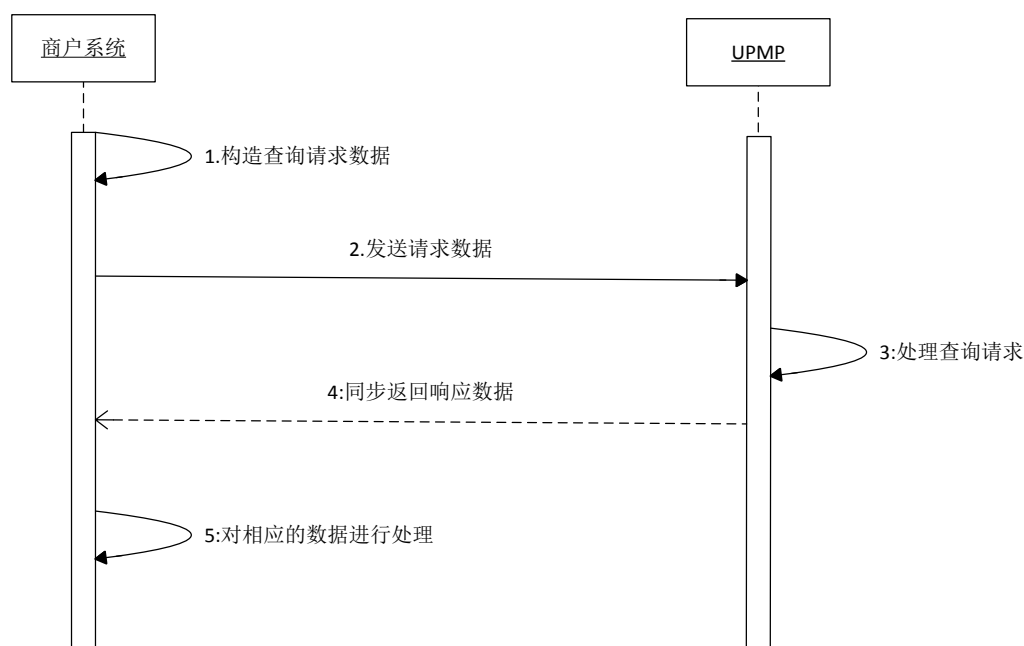
注意：商户后台接收到移动支付系统支付成功通知交易后，需返回UPMP后台确认已收到应答。



注意：

- 1：以上步骤第2步与第10步之间的操作是异步的。
- 2：商户应该以后台通知为准。
- 3：商户不一定每笔交易均收到前台应答。

3.2 交易信息查询流程



(1) 构造查询请求数据

商户根据移动支付系统提供的查询接口规则，通过程序生成得到签名结果及报文信息传输给移动支付的数据集合。

(2) 发送请求数据

把构造完成的数据集合，通过POST的方式传递给移动支付。

(3) 移动支付系统对查询请求数据进行处理

移动支付系统得到这些集合后，会先进行安全校验等验证，一系列验证通过后便会处理这次发送过来的数据请求。

(4) 返回处理的结果数据

(5) 商户对获取的返回结果数据进行处理。

4 商户开发步骤向导

需要开发的接口包含：

- 1、开发支付控件调用接口。

2、开发查询接口。要求所有商户都开发此接口，当商户收不到UPMP前台和后台应答时，需要发起查询接口来查询交易状态。若不开发查询接口，会有产生大量单边账的风险。

3、开发订单推送、撤销、退货等后台类交易接口。

具体开发代码可参考我们提供的SDK包，查询接口可参考QueryExample类，后台交易类接口可参考PurchaseExample、RefundExample、VoidExample等类。

4.1 支付控件调用开发步骤

参考文档《中国银联手机支付控件使用指南》，该文档位于UPPayPluginEx-SND-X.X.X\upmp_doc目录下。其中UPPayPluginEx-SND-X.X.X请联系中国银联杨帅（yangshuail@unionpay.com）获取。

4.2 后台交易开发步骤

1、组装要发送给UPMP的数据对象（包括订单号、商户号、交易类型、交易金额、交易币种、交易时间等域），每个域的填写请参考《UPMP商户接入接口规范》文档。

2、把组装好的数据排序好并用&连接后签名，生成signature字段，具体签名机制请参照第8章节。

3、把所有数据，包括signature和signMethod用key=value并用&符号链接的方式，发送到UPMP交易接口的地址。

4.3 查询接口开发步骤

1、商户调用查询接口需要上送商户代码merId、交易类型transType、订单号orderNumber和订单时间orderTime等信息。

2、把组装好的数据排序好并用&连接后签名，生成signature字段，具体签名机制请参照第8章节。

3、把所有数据，包括signature和signMethod用key=value并用&符号链接的方式，发送到UPMP查询接口的地址。

说明：查询频率请参照第7章节说明。

5 商户联调步骤向导

1、测试环境

开发完成后，需要和UPMP平台进行联调，商户分别会先连UPMP的测试环境，并有对应的银联的技术开发人员配合联调。

银联UPMP商户接入开发测试环境地址需要联系业务人员。

订单推送、撤销、退货等交易类请求发送到后台交易地址，商户也可以主动发起查询请求来查询交易状态，发送到查询请求地址。

商户可利用银联提供的测试卡进行联调测试：

1) 借记卡卡号：62123411111111111111，密码：111111，手机号：13888888888，短信验证码测试环境不校验，可随便输6位数字。

2) 信用卡卡号：62123411111111111111，年份：12，月份：12，CVN2：123，短信验证码同上

3) 预付卡卡号：62123411111111111111，年份：12，月份：12，CVN2：123，短信验证码同上

2、准生产环境（PM环境）

测试环境联调通过后，商户需要连UPMP的准生产环境PM环境测试，PM环境的测试参数配置需要联系业务人员。

3、生产环境

当测试环境和PM环境测试都通过后，最后连接UPMP生产环境上线。参数配置同样联系业务人员。

6 前台通知与后台通知说明

商户需要提供两个地址frontEndUrl和backEndUrl（均通过订单推送报文域上送）。frontEndUrl（前台通知URL）是通过支付控件，用户点击“返回商户”按钮发送给商户的前台通知； backEndUrl（后台通知URL）是UPMP异步把交易状态为成功的交易通知给商户。不管收到前台通知还是后台通知，商户都需要验签。

在交易结束后，UPMP系统通过后台通知将交易结果发给商户。后台通知以标准的HTTP协议的POST方法向商户的后台通知URL发送，并设置一个超时计时器，通常设置为10s。商户收到通知，解析后应立即返回应答报文。仅当POST返回码为200时，才认为商户已经成功收到并且能正确解析后台通知，其他返回码则被认为通知失败。如果计时器超时，没有收到应答报文，也被认为通知失败。第一次通知失败后，会通过退避策略进行通知重发，最多发送五次。由于网络等原因，商户会收到重复的后台通知，商户应可以正确处理重复通知请求。

商户在接收到UPMP的前台通知或后台通知后，首先必须验证该消息的签名，然后根据订单号等信息，更新相应系统中的订单支付状态。前台通知因存在用户支付完毕后直接关闭手机App的情况，而不能保证每次都送达。后台通知由银联UPMP通知服务器主动发起，若发送失败，UPMP会继续发送，一共发送5次，若还是发送失败，也不继续发送。商户在未收到后台应答，建议请求30分钟后主动发起交易查询交易来查询交易状态。

另外，退货等后台类交易是异步过程，UPMP收到后台类交易请求后会回复一个请求已接受的应答。在交易处理后，UPMP会主动发送后台通知给商户，建议商户无论是否收到后台通知，在请求5分钟后主动发起交易查询交易来查询交易状态。

注：UPMP只针对成功交易会发送后台通知，失败交易不发送后台通知。因此，如未收到后台通知，建议商户主动发起交易查询交易，查询交易状态。

另外后台通知接收需要注意以下几点：

1) 后台通知采用POST的方式来发送，POST的地址是商户上送的backEndUrl域，backEndUrl域需要保证该地址的正确性。

2) 后台通知中，只要是非通信类错误（如通信超时，无法解析域名，没有路由等），都认为商户已经收到，不会进行重发。如果商户因为非通信类问题没有及时收到应答（比如应用切换等情况），或者收到应答时处理失败（处理逻辑的验证应该在测试环境下已经验证通过），商户应该对没有及时收到应答的交易通过查询接口来查询该交易的状态。

3) 确定通知成功由以下几个要素

A) 通知URL填写正确（商户必须要保证URL的正确性）

B) 通信正确（通信失败时必须重发）

C) 商户能够正确验签（测试环境要测试通过）

因此，只要生产上能够证明通信是正确的，即可认为通知成功。如果商户端因为某种特殊原因，没有正确处理后台通知，可以通过交易查询接口来纠正交易的状态。

7 查询接口说明

7.1 前台交易（消费等交易）

- 1、如果已收到后台通知，则不需要发起查询。
- 2、在订单发起后半小时内未收到后台通知，则需要发起查询。

7.2 后台交易（退货、消费撤销等交易）

- 1、如果已收到后台通知，则不需要发起查询。
- 2、在请求发起后2分钟未收到后台通知，则需要发起查询。
- 3、单笔查询情况，查询时间间隔一般以指数形式递增，例如： 2s、4s、8s、16s、32s，最多查5次。

8 签名机制

8.1 生成待签名的字符串

8.1.1 需要参与签名的参数

在请求参数列表中，除去signMethod、signature 两个参数外，其他需要使用到的参数皆是要签名的参数。

在应答参数列表中，除去signMethod、signature 两个参数外，凡是应答回来的参数皆是要签名的参数。

8.1.2 生成待签名字符串

对请求参数数组里的每一个值从 a 到 z 的顺序排序，若遇到相同首字母，则看第二个字母，以此类推。排序完成之后，分别等于对应的值，用“=”连接相应的值，最后把所有数组值以“&”字符连接起来。



注意：

- 1: 签名时将字符转化成字节流时指定的字符集与charset保持一致；
- 2: 根据 HTTP 协议要求，传递参数的值中如果存在特殊字符（如：&、@等），那么该值需要做 URL Encoding，这样请求接收方才能接收到正确的参数值。这种情况下，待签名数据应该是原生值而不是 encoding 之后的值。例如：调用某接口需要对请求参数 backEndUrl 进行数字签名，那么待签名数据应该是backEndUrl=http://www.yourdomain.com/，而不是backEndUrl=http%3A%2F%2Fwww.yourdomain.com%2F。

8.2 签名

在 MD5 签名时，需要商户私钥参与签名。商户私钥是由各个商户自己设定的由字母数字组成的8-16位字符串（字母大小写敏感）。目前暂时由业务人员统一分配，后续商户可登录到商户服务网站（https://**.com），进行设置。

请求时签名

当拿到请求时的待签名字符串后，需要把私钥进行MD5加密后拼接对待签名字符串后面（连接符&），形成新的字符串，利用 MD5 的签名函数对这个新的字符串进行签名运算，从而得到 32位签名结果字符串（该字符串赋值于参数signature）。

收到应答时验证签名

当获得到返回应答时的待签名字符串后，同理，需要把私钥进行MD5加密后拼接对待签名字符串后面（连接符&），形成新的字符串，利用 MD5 的签名函数对这个新的字符串进行签名运算，从而得到 32 位签名结果字符串。此时这个新的字符串需要与移动支付通知返回参数中的参数signature的值进行验证是否相等，来判断签名是否验证通过。

8.3 如何验证是否移动支付业务请求

获取移动支付返回数据之一的签名（signature）和签名方法（signMethod），除去 signMethod、signature 两个参数外同签名的方法，对返回的参数进行签名，与报文中的 signature是否一致。

如：收到报文：

```
backEndUrl=http://www.yourdomain.com/your_path/yourFrontEndUrl&chase  
t=UTF-8&frontEndUrl=http://www.yourdomain.com/your_path/yourFrontEndU  
rl&merId=001100041120001&orderAmount=1&orderCurrency=156&orderDescrip  
tion=desc&orderNumber=20121031141617&orderTime=20121031141617&orderTi  
meout=2012&transType=01&version=1.00
```

那么MD5加密串为:

```
backEndUrl=http://www.yourdomain.com/your_path/yourFrontEndUrl&chase  
t=UTF-8&frontEndUrl=http://www.yourdomain.com/your_path/yourFrontEndU  
rl&merId=001100041120001&orderAmount=1&orderCurrency=156&orderDescrip  
tion=desc&orderNumber=20121031141617&orderTime=20121031141617&orderTi  
meout=2012&transType=01&version=1.00&8ddcff3a80f4189c9d4d902c3c909
```

加密出来的签名: 89a203bd51095ed85f5732a4d32cf3dc。判断是否与收到报文的signature一致。



注意:

- 1: 待加密报文需取消收到报文中的signMethod与signature属性, 其他属性按照字典顺序排列
- 2: 增加的商户密钥的MD5加密串。

9 商户密钥获取与使用

商户密钥的作用, 是防止商户生成的订单内容在提交银联之前被恶意修改。商户发送报文时需要根据订单内容和商户密钥对订单内容进行加密。收到移动支付应答报文时需要对订单内容进行合法性验证。由于只有商户和移动支付知道“商户密钥”, 第三方无法产生对应的加密串。因而可以通过校验码检验订单内容是否为商户产生。商户需要保证密钥的保密性。

商户密钥获取方式: 暂时采取业务人员分配方式, 后续商户可以登录移动支付商户服务网站 (http://****), 在商户密钥信息进行设置或修改。

MD5加密算法: 即signature生产算法: MD5(报文内容&MD5(商户密钥))。详细例子请参考本文的“签名机制”章节。

10 SDK 使用

SDK只是为了方便商户测试而提供的样例代码，商户可以根据自己网站的需要，按照技术文档编写，并非一定要使用该代码。代码仅供参考

10.1 JSP/JAVA (java.zip)

目录说明：

UpmpSDK

```
|
|
|src-----类文件夹
|  |
|  |com.unionpay.upmp.sdk.conf
|  |
|  |  |
|  |  |↳UpmpConfig.java-----基础配置类文件
|  |
|  |com.unionpay.upmp.sdk.examples
|  |
|  |  |
|  |  |↳PurchaseExample.java----- 订单推送请求接口实例类文件
|  |  |
|  |  |↳QueryExample.java-----交易信息查询接口实例类文件
|  |  |
|  |  |↳RefundExample.java----- 退货接口实例类文件
|  |  |
|  |  |↳VoidExample.java----- 消费撤销接口实例类文件
|  |
|  |com.unionpay.upmp.sdk.service
|  |
|  |  |
|  |  |↳UpmpService.java----- 接口处理核心类
|  |
```



```

|   └com.unionpay.upmp.sdk.util
|       |
|       ├──HttpUtil.java----- HttpClient处理类文件
|       |
|       ├──httputil.properties----- HttpClient配置文件
|       |
|       ├──UpmpCore.java----- 公用函数类文件
|       |
|       └UpmpMd5Encrypt.java----- MD5签名类文件
|
|──web-----WEB目录
|   |
|   ├──notify_url.jsp ----- 异步通知页面
|   |
|   └WEB-INF
|       |
|       └lib（如果JAVA项目中包含这些架包，则不需要导入）
|           |
|           ├──commons-codec-1.5.jar
|           |
|           ├──commons-httpclient-3.1.jar
|           |
|           └commons-logging-1.1.1.jar
|
└readme.txt -----使用说明文本
    
```

10.2 PHP（php.zip）

UpmpSDK
|

```

├─conf
│   │
│   └─upmp_config.php -----基础配置文件
│
├─examples
│   │
│   └─purchase.php ----- 订单推送请求接口实例文件
│       │
│       └─query.php -----交易信息查询接口实例文件
│           │
│           └─refund.php ----- 退货接口实例文件
│               │
│               └─void.php ----- 消费撤销接口实例文件
│
├─lib
│   │
│   └─upmp_core.php -----公用函数文件
│       │
│       └─upmp_service.php ----- 接口处理核心类
│
├─notify_url.php -----服务器异步通知页面文件
│
└─readme.txt -----使用说明文本
    
```

10.3 ASP.NET (asp.net.zip)

```

UpmpSDK
│
├─App_Code
│   │
│   └─UpmpConfig.cs -----基础配置文件
│       │
│       └─UpmpCore.cs -----公用函数文件
│           │
│           └─UpmpService.cs ----- 接口处理核心类
│
├─examples
│   │
│   └─purchase.aspx -----订单推送请求接口实例文件
│       │
│       └─purchase.aspx.cs ----- 订单推送请求接口实例文件
│           │
│           └─query.aspx ----- 交易信息查询接口实例文件
│               │
│               └─query.aspx.cs -----交易信息查询接口实例文件
│
    
```

```

|   |refund.aspx -----退货接口实例文件
|   |refund.aspx.cs ----- 退货接口实例文件
|   |
|   |void.aspx -----消费撤销接口实例文件
|   |void.aspx.cs ----- 消费撤销接口实例文件
|
|notify_url.php -----服务器异步通知页面文件
|notify_url.php -----服务器异步通知页面文件
|
|readme.txt -----使用说明文本

```

10.4 ASP (asp.zip)

UpmpSDK

```

|
|class
|   |
|   |upmp_core.asp -----公用函数文件
|   |
|   |upmp_md5.asp -----MD5 签名类文件
|   |
|   |upmp_service.asp ----- 接口处理核心类
|   |
|conf
|   |
|   |upmp_config.asp -----基础配置文件
|
|examples
|   |
|   |purchase.asp ----- 订单推送请求接口实例文件
|   |
|   |query.asp -----交易信息查询接口实例文件
|   |
|   |refund.asp ----- 退货接口实例文件
|   |
|   |void.asp ----- 消费撤销接口实例文件
|
|notify_url.asp -----服务器异步通知页面文件
|
|readme.txt -----使用说明文本

```

11 常见问题问答

Q: 如何获取商户密钥?

A: 测试环境请联系技术人员配置
生产环境请联系业务部门。
详见第9章节商户密钥获取与使用

Q: 如何签名?

A: 见第8章节签名机制

Q: 报文域中frontEndUrl、frontEndUrl和backEndUrl要填什么?

A: 见第6章节

Q: 商户接收到UPMP的前台应答和后台通知, 以哪个为准?

A: 以后台通知为准。

Q: 商户收到后台通知的要素?

A: 参考《UPMP商户接入接口规范》

Q: 如果发起了消费等前台类交易, 多久后调用查询接口?

A: 见第7章节查询接口说明

Q: 如果发起了退货等后续类交易, 多久后调用查询接口?

A: 见第7章节查询接口说明

Q: 消费撤销和退货有何不同?

A: 当天的交易可以执行消费撤销, 只能全额消费撤销。

隔天的交易可以退货, 退货可以进行多次退货, 每次金额小于原始金额, 订单退款总金额不能大于此订单原始金额。

Q: 对账文件中的对账数据只会有成功交易的数据, 是吧?

A: 是的。