# php 网上支付讲座

# 1.目前两种支付方式

## 1.直接和银行对接

### 1.缺点是工作量大，而且需要资格审核

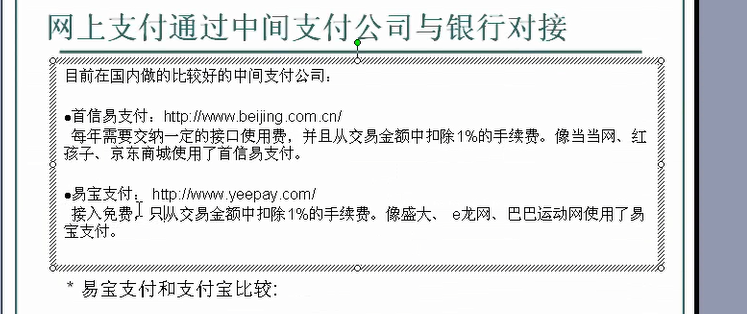
### 2.优点安全

## 2.和中间公司对接

### 1.缺点就是安全隐患

### 2.优点就是开发维护方便

# 2.开始选择一家公司



## 1.易宝<http://www.yeepay.com/>

# 2.开始开发使用易宝账号和密码

## 1.目前我们使用yeebay公司提供了用于测试的账号和密钥

### 1.1账号 ：$p1\_MerId = "10001126856";

### 1.2密钥： $merchantKey = "69cl522AV6q613Ii4W6u8K6XuW8vM1N6bFgyv769220IuYe9u37N4y7rI4Pl";

## 2.这个是打给易宝公司的钱，

# 4.设置开始界面

<tr>

<!-- 这里的银行的名字是不可以随便写的 -->

<td><input type=*"radio"* name=*"pd\_FrpId"* value=*"CMBCHINA-NET"*/>招商银行</td>

<td><input type=*"radio"* name=*"pd\_FrpId"* value=*"ICBC-NET"*/>工商银行</td>

<td><input type=*"radio"* name=*"pd\_FrpId"* value=*"ABC-NET"*/>农业银行</td>

<td><input type=*"radio"* name=*"pd\_FrpId"* value=*"CCB-NET"*/>建设银行</td>

</tr>



# 5.测试接收，支付请求参数说明

<?php//这里我们获取用户提交的信息

$pd\_FrpId=$\_REQUEST['pd\_FrpId']; //银行

$p2\_Order=$\_REQUEST['p2\_Order']; //订单号

$p3\_Amt=$\_REQUEST['p3\_Amt']; //金额

$p0\_Cmd="Buy"; //业务类型，固定 buy

$p1\_MerId="10001126856"; // 商户编号

$p4\_Cur="CNY"; // 交易币种 是 Max(10) 固定值 ”CNY

$p5\_Pid=""; //商品名称

$p6\_Pcat="";//种类

$p7\_Pdesc="";//商品介绍

//这是易宝支付成功后，给url返回信息 成功才会回复

$p8\_Url="http://localhost:80/myNetPayment/res.php";

// 商户接收支付成功数据的地址 否 Max(200) 支付成功后易宝支付会向该地址发送两次成功通知，

//该地址可以带参数，如:“ www.yeepay.com/callback.action?test=test”.

//注意：如不填p8\_Url的参数值支付成功后您将得不到支付成功的通知。

$p9\_SAF="0";//送货地址 否 Max(1) 为“1”: 需要用户将送货地址留在易宝支付系统;为“0”: 不需要，默认为 ”0”.

$pa\_MP=""; //商户扩展信息 否 Max(200) 返回时原样返回，此参数如用到中文，请注意转码.

$pr\_NeedResponse="1";

//应答机制 否 Max(1) 固定值为“1”: 需要应答机制;

//收到易宝支付服务器点对点支付成功通知，必须回写以”success”（无关大小写）开头的字符串，

//即使您收到成功通知时发现该订单已经处理过，也要正确回写”success”，

//否则易宝支付将认为您的系统没有收到通知，启动重发机制，直到收到”success”为止。

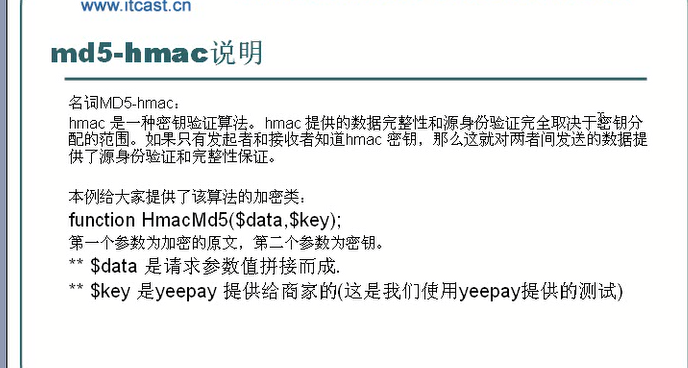
$hmac=HmacMd5($data,$merchantKey); 后面详解，这里不全

//hmac是签名串，是用于易宝和商家互相确认的关键字

//这里我们需要使用算法来生成( md5-hmac算法)

//我们把请求参数一个一个拼接(拼接的时候，顺序很重要!!!!)

# 6. 如何生成一个hmac签名串.Md5-hmac算法



## 2.测试

**function** HmacMd5($data,$key){

// RFC 2104 HMAC implementation for php.

// Creates an md5 HMAC.

// Eliminates the need to install mhash to compute a HMAC

// Hacked by Lance Rushing(NOTE: Hacked means written)

//需要配置环境支持iconv，否则中文参数不能正常处理

$key = iconv("GB2312","UTF-8",$key);

$data = iconv("GB2312","UTF-8",$data);

$b = 64; // byte length for md5

**if** (strlen($key) > $b) {

$key = pack("H\*",md5($key));

}

$key = str\_pad($key, $b, chr(0x00));

$ipad = str\_pad('', $b, chr(0x36));

$opad = str\_pad('', $b, chr(0x5c));

$k\_ipad = $key ^ $ipad ;

$k\_opad = $key ^ $opad;

**return** md5($k\_opad . pack("H\*",md5($k\_ipad . $data)));

}

//秘钥我们之前准备好的

$merchantKey = "69cl522AV6q613Ii4W6u8K6XuW8vM1N6bFgyv769220IuYe9u37N4y7rI4Pl";

**echo** HmacMd5("hellow", $merchantKey);

?>

# 7.开始使用Md5-hmac

# require\_once 'common.php'; 里面是函数Md5-hmac

//我们把请求参数一个一个拼接(拼接的时候，顺序很重要!!!!)

$data="";

$data=$data.$p0\_Cmd;

$data=$data.$p1\_MerId;

$data=$data.$p2\_Order;

$data=$data.$p3\_Amt;

$data=$data.$p4\_Cur;

$data=$data.$p5\_Pid;

$data=$data.$p6\_Pcat;

$data=$data.$p7\_Pdesc;

$data=$data.$p8\_Url;

$data=$data.$p9\_SAF;

$data=$data.$pa\_MP;

$data=$data.$pd\_FrpId;

$data=$data.$pr\_NeedResponse;

// $merchantKey 为秘钥 我们之前准备好的

$merchantKey = "69cl522AV6q613Ii4W6u8K6XuW8vM1N6bFgyv769220IuYe9u37N4y7rI4Pl";

//产生hmac需要两个参数，并调用相关API.

//参数1: STR，列表中的参数值按照签名顺序拼接所产生的字符串，注意null要转换为 ””，并确保无乱码.

//hmac是签名串，是用于易宝和商家互相确认的关键字

//这里我们需要使用算法来生成( md5-hmac算法)

//我们把请求参数一个一个拼接(拼接的时候，顺序很重要!!!!)

$hmac=HmacMd5($data,$merchantKey);

# 8.给出提示金额

你的订单号是<?php **echo** $p2\_Order; ?> 支付的金额是<?php **echo** $p3\_Amt;?>

<!--把要提交的数据用隐藏域表示-->

<form action=*"https://www.yeepay.com/app-merchant-proxy/node"* method=*"post"*>

<input type=*"hidden"* name=*"p0\_Cmd"* value="<?php **echo** $p0\_Cmd;?>"/>

<input type=*"hidden"* name=*"p1\_MerId"* value="<?php **echo** $p1\_MerId; ?>"/>

<input type=*"hidden"* name=*"p2\_Order"* value="<?php **echo** $p2\_Order; ?>"/>

<input type=*"hidden"* name=*"p3\_Amt"* value="<?php **echo** $p3\_Amt; ?>"/>

<input type=*"hidden"* name=*"p4\_Cur"* value="<?php **echo** $p4\_Cur;?>"/>

<input type=*"hidden"* name=*"p5\_Pid"* value="<?php **echo** $p5\_Pid?>"/>

<input type=*"hidden"* name=*"p6\_Pcat"* value="<?php **echo** $p6\_Pcat;?>"/>

<input type=*"hidden"* name=*"p7\_Pdesc"* value="<?php **echo** $p7\_Pdesc;?>"/>

<input type=*"hidden"* name=*"p8\_Url"* value="<?php **echo** $p8\_Url;?>"/>

<input type=*"hidden"* name=*"p9\_SAF"* value="<?php **echo** $p9\_SAF;?>"/>

<input type=*"hidden"* name=*"pa\_MP"* value="<?php **echo** $pa\_MP;?>"/>

<input type=*"hidden"* name=*"pd\_FrpId"* value="<?php **echo** $pd\_FrpId;?>"/>

<input type=*"hidden"* name=*"pr\_NeedResponse"* value="<?php **echo** $pr\_NeedResponse;?>"/>

<input type=*"hidden"* name=*"hmac"* value="<?php **echo** $hmac;?>"/>

<input type=*"submit"* value=*"确认网上支付"*/>

</form>

</html>

# 9.上面的完成之后会自动回调这个东西，然后到我们之前写的url

<?php

//echo "支付成功!";

**include\_once** 'common.php';

//获取从易宝支付网关返回的信息

//$p1\_MerId=

$p1\_MerId="10001126856";//就是自己的商号.

$r0\_Cmd=$\_REQUEST['r0\_Cmd'];

$r1\_Code=$\_REQUEST['r1\_Code'];

$r2\_TrxId=$\_REQUEST['r2\_TrxId'];

$r3\_Amt=$\_REQUEST['r3\_Amt'];

$r4\_Cur=$\_REQUEST['r4\_Cur'];

$r5\_Pid=$\_REQUEST['r5\_Pid'];

$r6\_Order=$\_REQUEST['r6\_Order'];

$r7\_Uid=$\_REQUEST['r7\_Uid'];

$r8\_MP=$\_REQUEST['r8\_MP'];

$r9\_BType=$\_REQUEST['r9\_BType'];

$hmac=$\_REQUEST['hmac'];

//拼接

$res\_src="";

$res\_src=$res\_src.$p1\_MerId;

$res\_src=$res\_src.$r0\_Cmd;

$res\_src=$res\_src.$r1\_Code;

$res\_src=$res\_src.$r2\_TrxId;

$res\_src=$res\_src.$r3\_Amt;

$res\_src=$res\_src.$r4\_Cur;

$res\_src=$res\_src.$r5\_Pid;

$res\_src=$res\_src.$r6\_Order;

$res\_src=$res\_src.$r7\_Uid;

$res\_src=$res\_src.$r8\_MP;

$res\_src=$res\_src.$r9\_BType;

$merchantKey = "69cl522AV6q613Ii4W6u8K6XuW8vM1N6bFgyv769220IuYe9u37N4y7rI4Pl";

//对返回的结果进行md5-hmac加密处理，和返回的hmac签名串比较

**if**(HmacMd5($res\_src,$merchantKey)==$hmac){

**if**($r1\_Code==1){

**if**($r9\_BType==1){

**echo** '交易成功!';

**echo** '订单号为'.$r6\_Order.'支付成功!'.'所付金额是'.$r3\_Amt."易宝支付订单号".$r2\_TrxId;

**echo** '<br/>浏览器重定向';

}**elseif**($r9\_BType==2){

**echo** 'success';

**echo** '<br/>交易成功!';

**echo** '<br/>服务器点对点通讯';

}

}

}**else**{

**echo** "签名被篡改";

}

?>

# 10.防止刷新

## 1.通过订单结果看看

强调:

防止用户反复刷新回调页面

方法很多，这里我就抛砖一个

/\*//假设我们点卡充值

//order 表

// id status

14567 未付款

//---- gameCard表

// id pwd balance余钱

// 12345 ???? 12

$sql="update gameCard set banlance

=balance+10 where id=12345";

//更新数据库

//1.根据订单的状态看看该订单是否付款

if(订单付款否==false){

$sql="update gameCard set banlance

=balance+10 where id=12345";

$sql="update order set status=已付款 where id=14567"

}else{

//不搭理

}\*/