支付网关回调签名方案

商户验签步骤如下

1:获取回调请求请求头header里面Authorization中的sign
2:解析回调通知请求报文获取到请求体body
3:获取收钱吧公钥（请联系收钱吧相应技术对接人提供）
4:采用RSA的SHA256WithRSA签名算法，对获取的回调信息进行验签。
5:返回验签结果

Java代码示例

```
/**  验签
 * @param data 签名原数据
 * @param sign 签名
 * @param publicKey 收钱吧公钥
 */
public static boolean validateSign(String data, String sign, String publicKey){
    try {
        Signature signature = Signature.getInstance("SHA256WithRSA");
        PublicKey localPublicKey = getPublicKeyFromX509("RSA", publicKey);
        signature.initVerify(localPublicKey);
        signature.update(data.getBytes());
        byte[] bytesSign = Base64.decode(sign);
        return signature.verify(bytesSign);
    }catch (Exception e){
        e.printStackTrace();
        return false;
    }
}

public static PublicKey getPublicKeyFromX509(String algorithm, String publicKey) throws Exception {
    KeyFactory keyFactory = KeyFactory.getInstance(algorithm);
    return keyFactory.generatePublic(new X509EncodedKeySpec(Base64.decode(publicKey)));
}
```

Python代码示例

```
"""
param sign: 签名
param body: 请求体
param pubKey: 公钥
"""
from Crypto.PublicKey import RSA
from Crypto.Signature import PKCS1_v1_5
from Crypto.Hash import SHA256
import base64
h = SHA256.new(body) # 对请求体进行SHA256加密
pubKey = RSA.importKey(PUBLIC_KEY) # 获取公钥
verifier = PKCS1_v1_5.new(pubKey) # 创建验证
verifier.verify(h, base64.b64decode(sign)) # 验证签名是否一致，sign需要base64解密
```

C#代码示例

PHP代码示例

```
public function validateSign(){
     $data = file_get_contents("php://input");
     $sign =getallheaders();
     $PUBLIC_KEY="公钥";  //（这里传入收钱吧提供的公钥）
     $result = FALSE;
     $result = (openssl_verify($data, base64_decode($sign['Authorization']), $PUBLIC_KEY, OPENSSL_ALGO_SHA256)===1);
    if($result){
        echo '验签成功';
    }else{
        echo '验签失败';
    }
}
```