商户通知验签算法

1. 背景

为防止数据被篡改和保障数据的完整性，建行向商户发送商户通知请求时，建行会对返回的参数数据进行数字签名，商户接收到建行发送的商户通知后，需要对接收到的参数数据进行数字签名的验签。

2. 数字签名机制简介

数字签名使用 RSA 数字摘要算法，算法类型为 RSA【MD5withRSA】，接收方使用对应的柜台公钥对签名数据进行验签。【商户公钥可在商户服务平台进行下载】。

3. 数字签名验签步骤

1）接收建行返回的参数，如：

http://128.192.155.62:8001/test/ccbNotify?RESULT=Y&ORDERID=151677281312212&AMOUNT=0.01&WAITTIME=null&TRACEID=101011503151677296442 8432&SIGN=80c3298a47b26cb9d8d708e1465c6b521edcce32b0deecab91257a3f41fc 6cf39fa43afa54dc8489a04615eee9dcca1f4b52ce677f70109f29745ff34033018353b78 e982cc860623b6c3df0d9c1a62ca010a019fff8544d4d8e154a010d7fc16cb590ccd87f3 4d8bea6added68cf1f9943fdb1d83616507a4588b68774b9fe1

2）获取签名数据，签名数据中的字段顺序请参考对应的接口文档，如：

RESULT=Y&ORDERID=151677281312212&AMOUNT=0.01&WAITTIME=null&TRACEID=101011503151677296442 8432

3）获取数字签名域，即 SIGN 字段值，如：

80c3298a47b26cb9d8d708e1465c6b521edcce32b0deecab91257a3f41fc6cf39fa4 3afa54dc8489a04615eee9dcca1f4b52ce677f70109f29745ff34033018353b78e982cc8 60623b6c3df0d9c1a62ca010a019fff8544d4d8e154a010d7fc16cb590ccd87f34d8bea6

added68cf1f9943fdb1d83616507a4588b68774b9fe1

4）将上面步骤中的值，传入验签方法进行验证。