**终端或第三方调用聚合支付接口数据安全校验流程**

**涉及到的数据安全校验的接口：**

|  |  |  |
| --- | --- | --- |
| **序号** | **接口** | **备注** |
| 1 | /pay/ali\_face\_init | 支付宝刷脸初始化接口 |
| 2 | /pay/wx\_face\_init | 微信刷脸初始化接口 |
| 3 | /pay/pay | 统一支付接口，含：  微信扫码付；  支付宝扫码付；  支付宝刷脸付； |
| 4 | /pay/wx\_face\_pay | 微信刷脸支付接口 |
| 5 | /pay/precreate\_qr\_code | 交易预创建接口（获取二维码），含：  支付宝交易预创建接口；  微信交易预创建接口； |
| 6 | /pay/refund | 统一退款接口 |
| 7 | /pay/query | 统一交易查询接口 |
| 8 | /pay/refund\_query | 统一退款查询接口 |

**数据安全校验流程：**

1. 平台拥有SM2的公私钥对，公钥由终端、第三方（以下简称已方）通过公钥接口（/user/public\_key）获取，接口调用参见接口文档；
2. 乙方通过参数下载获取公钥，并将公钥写入到芯片中或保存；
3. 乙方签到时，通过产生16字节随机数，并用SM2公钥对16字节随机数进行加密，采用C1C3C2模式，将随机数密文、SN、model等上送至平台，即调用工作密钥接口（/user/key），接口调用参见接口文档；
4. 乙方通过调用工作密钥接口，获取工作密钥密文key；
5. 乙方收到工作密钥密文之后，用之前产生的随机数对密文进行SM4解密，解密后的数据为工作密钥明文mak，将明文存储在芯片中或保存（须保证数据不能被窃取）
6. mac值计算原理，加密采用SM4算法，mak为密钥，具体原理简述如下：
7. 将http报文按每16字节分块，不足补b'\x00'；
8. 对第一个块加密得密文M；
9. 用M异或第2个块，得到异或结果XOR；
10. 对XOR加密得到密文M2；
11. 用M2异或第3个块，得到异或结果XOR2；
12. ……依次类推
13. 将最后加密的结果取前16字节转换为16进制字符串作为mac值；

注：

1、退款接口（/pay/refund），前端可直接调用

2、平台，终端，及第三方统一将计算的mac值，放于http header中，字段名统一mac；