**中行支付签名与验签过程**

# 1商户请求报文的签名过程

## 1.1商户获取自己的私钥软证书

中行现在提供两种商户私钥软证书，都是pfx格式文件，有密码。

* **我行自建BOCCA软证书**
* **第三方CFCA软证书**

请商户从分行申请。

注意：测试环境和生产环境的证书是不同的

## 1.2商户将要加签的数据域组成PlainText串

商户根据中行提供的交易接口文档，将交易请求报文中的要加签的数据域的值拼成明文串，如订单支付的明文串：

PlainText=orderNo|orderTime|curCode|orderAmount|merchantNo

## 1.3商户使用私钥软证书生成SignData

商户参考中行提供的签名验签包的源代码，组织商户自己的签名函数，使用该函数和私钥软证书对明文串运算，得到商户签名后的数据SignData。

## 1.4商户提交请求报文到中行

商户将签名后的数据SignData作为请求报文的一个域，使用Https的POST方式提交到中行。

# 2商户验证中行应答报文过程

## 2.1商户获取中行二级根证书

中行的二级根证是：bocnet ca.cer

注意：测试环境和生产环境的证书是不同的



## 2.2商户从中行应答报文解析出PlainText和SignData

商户接收中行返回的报文，结合中行文档说明，从中解析出要加签的数据域：

如订单应答报文中一种场景是：

PlainText=merchantNo|orderNo|orderSeq|cardTyp|payTime|orderStatus|payAmount

还有中行签名的数据域SignData

## 2.3商户使用中行二级根证书验证中行签名

商户参考中行提供的签名验签包的源代码，组织商户自己的验签函数，使用该函数和二级根证书对明文串PlainText和SignData运算，验证其是否为合法数据。

## 2.4商户验签成功后更新商户交易状态

如果验证中行签名成功，根据交易报文中的交易状态更新商户自己的交易状态。

如果是CFCA证书，从浏览器导出CFCA证书时会有两个同名证书，此时一定要注意导出用于加签（如下图看**密钥用法**为**Digital Signature**）的证书而不是用于加密的证书。

