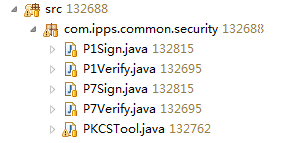
pcks为源代码，pkcs.jar为对应jar包, pkcsdemo为运行程序，可按照pkcsdemo使用说明运行。

# 一、pkcs程序结构说明



PKCSTool:提供签名、验签证书加载，签名、验签等方法

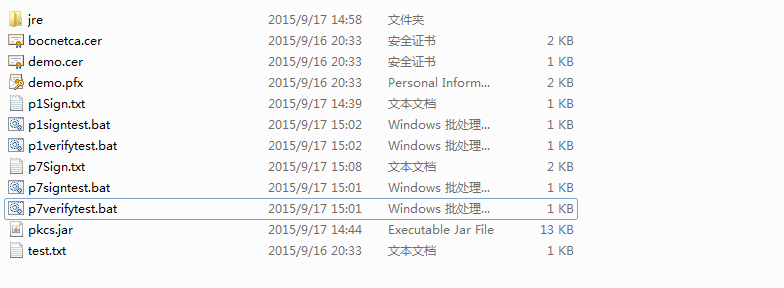
P1Sign：P1签名示例

P1Verify：P1验证签名示例

P7Sign：P7签名示例

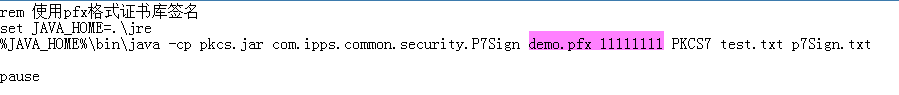
P7Verify：P7签名示例

# 二、pkcsdemo使用说明

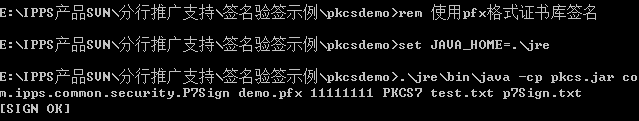


1、P7签名

将签名证书置于pkcsdemo目录下，修改p7signtest.bat配置



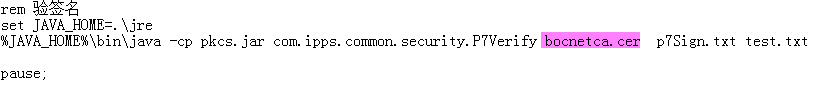
签名原文串原文保存在test.txt文本中，点击p7signtest.bat运行



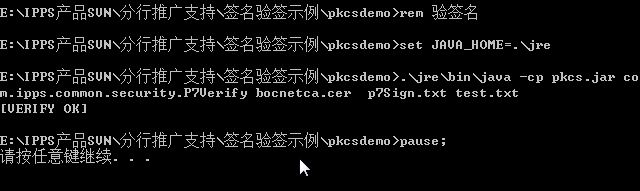
看到SIGN OK表示签名成功，可在p7Sign.txt查看签名结果

2、P7验证签名

将签名证书对应的根证书置于pkcsdemo目录，修改p7verifytest.bat配置



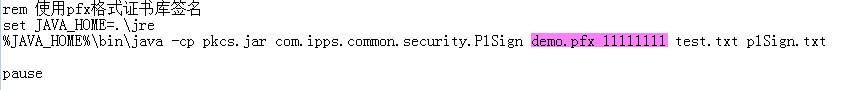
签名原文串原文保存在test.txt文本中，签名结果串保存在p7Sign.txt文本中。点击p7verifytest.bat运行。



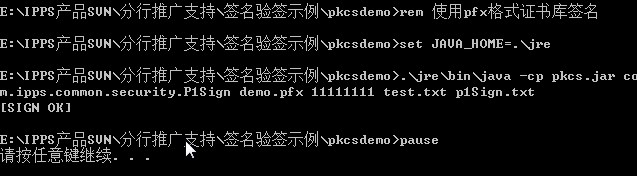
看到VERIFY OK即验证签名成功

3、P1签名

将签名证书置于pkcsdemo目录下，修改p1signtest.bat配置



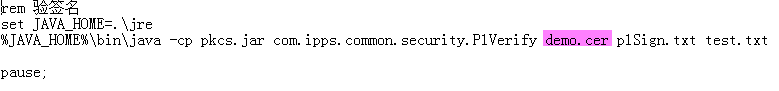
名原文串原文保存在test.txt文本中，点击p7signtest.bat运行



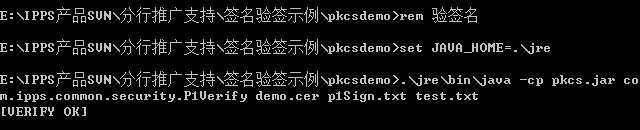
看到SIGN OK表示签名成功，可在p1Sign.txt查看签名结果

4、P1验证签名

将签名证书对应的公钥证书置于pkcsdemo目录，修改p1verifytest.bat配置



签名原文串原文保存在test.txt文本中，签名结果串保存在p1Sign.txt文本中。点击p1verifytest.bat运行。



看到VERIFY OK即验证签名成功