# 有效验证过程

1. **验证CRL和有效期**

**准备：**用到oracle数据库（开启数据库的操作在步骤1中），ocsp服务器，加密机（加密机ip：192.168.0.232），以及相应的ocsp的API接口

**过程：**

步骤1：开启加密机，开启oracle数据库；

步骤2：开启OCSP：1）su – ocsp（密码是：ocsp）

2）cd bin

3）OCSPConsole –s

出现Start OCSP server…..

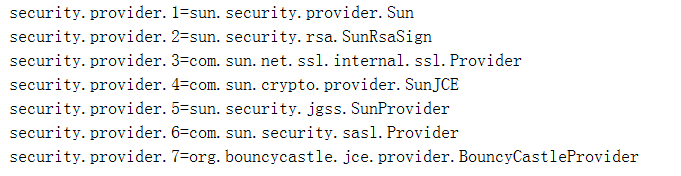
（忽略：这个是ocsp客户端的验证，客户端就在服务器所在的那个电脑上）打开OCSP查询客户端，选择查询证书状态，选择待查询证书文件，点击开始查询。查看返回的证书状态，出现“证书有效！”，就是证书有效的CRL。

步骤3：导入相应的API函数以及环境配置：环境jre1.5.

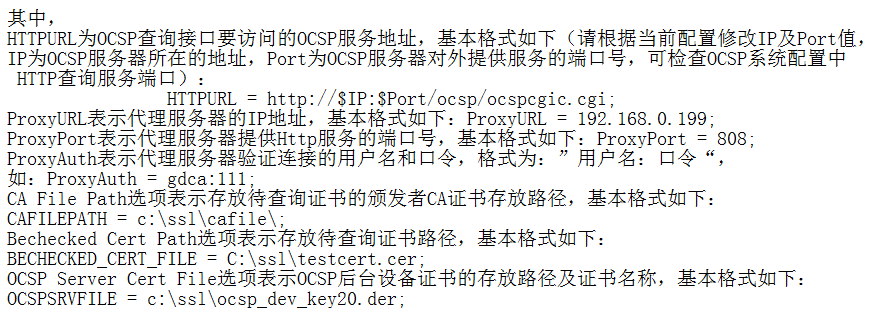
1）将Common.java,TestThread.java,Atest.java拷贝到工程目录下（在工程checkCert中的ocspcli包中已经存在）

2）导入jar包. bcprov-jdk15-xxx.jar包和ocsp\_cli\_jdk1.5\_v3.60003.jar包，（工程中部分已存在，如果确实，在测试证书工程中的jar包里获取）

3）到%JAVAHOME%\jre\lib\security修改java.security，添加security.provider.N = org.bouncycastle.jce.provider.BouncyCastleProvider,其中的N是根据你的文件中的序号来修改。例如：



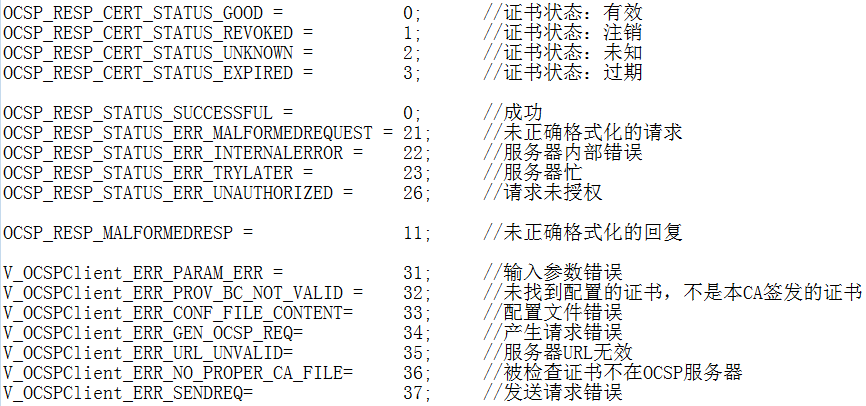
4）配置文件为Config文件下的ocspcli.ini，将Config文件放在C盘下，（如ocspcli.ini的目录是C:\Config,这个目录可以查看Atest.java或者examineCert中变量WIN\_CONF\_PATH，以及完整目录在函数getConfOption()中的conf\_path）:

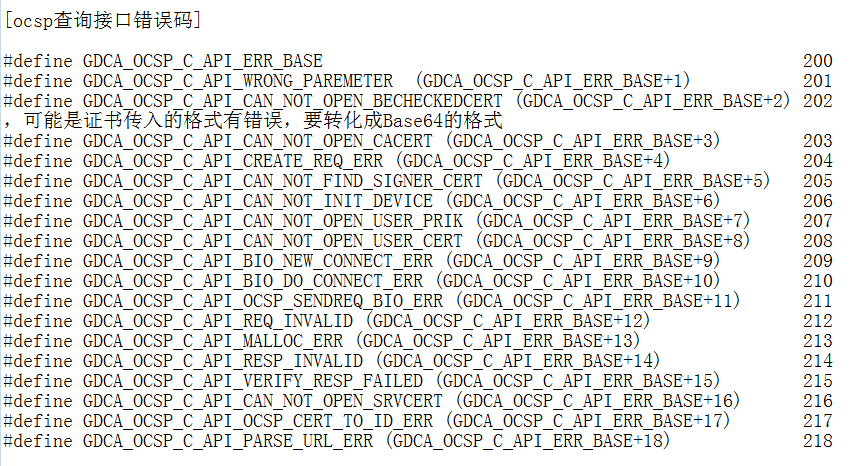


配置文件中代理服务器并没有用上，真正用上的参数是#OCSP Server HTTP URL和#CA File Path还有#Bechecked Cert Path和#OCSP Server Cert File。

5）把库OCSP\_JAVA\_API.dll、asip\_e.dll、libeay32.dll、SM3.dll加载到 java工程下

6）执行命令java ocspcli.Atest文件，返回码为0就是验证成功，（注意：挂失和注销都被认为是撤销）





注释：安装jdk（替代）：在测试证书工程的目录下有一个免安装的32位jdk\_1.5,将其拷贝到电脑上，配置相应的环境变量以及将工程运行环境jre替换成jdk\_1.5。（jdk\_1.5中已经配置好了dll文件，无需再导入，而且security中的文件也已经修改好了），还有相应的可以容纳1.5jdk的eclipse版本安装包

1. **验证根链**

**准备：**用到签名服务器（ip地址为：192.168.0.233），以及相应的API

**过程：**

步骤1：开启签名服务器。

步骤2：加载MyThread文件到工程中，导入dean\_svs\_v5.5.1.jar运行api\_test.Java

返回码为0即为验证成功。（在工程checkCert中的com.cslc.netsignagent包中已经存在）

其中api\_test.java中的inStream变量中的路径是要检查的证书的路径，记得修改。

**说明：验证根链用到的主要函数**

NetSignAgent类

描述：

验证传入证书有效性

函数原型：

public static int SVS\_VerifyCert (byte[] cert) throws NetSignException

输入参数：

byte[] cert 证书内容，支持BASE64编码和der编码格式

返回值：

Int 0 验证成功

其他 验证失败，返回值为错误码

异常：

NetSignException 异常

问题1：验证根链时，验证过程出错，错误信息为rv=57175

错误原因：可以是签名服务器的时间在证书生效的时间之前。

解决:进入<http://192.168.0.233:8080>，配置时间源，将当前服务器系统时间调到证书生效的时间之后就可以了。

密码：datech