한국전자인증

Tomcat 4.x 인증서 설치 매뉴얼

Version 1.0

March 4, 2008

VeriSign

한국전자인증	Title **Tomcat 4.x 인증서 설치 매뉴얼**		
	문서번호: Tom-10000	버전: 1.0	작성일: 2008-03-04

제.개정 이력

1.0	2008-03-05	제정	김상우
개정	제.개정 일자	제.개정 페이지 및 내용	제.개정자

▶ 개인키 및 CSR생성

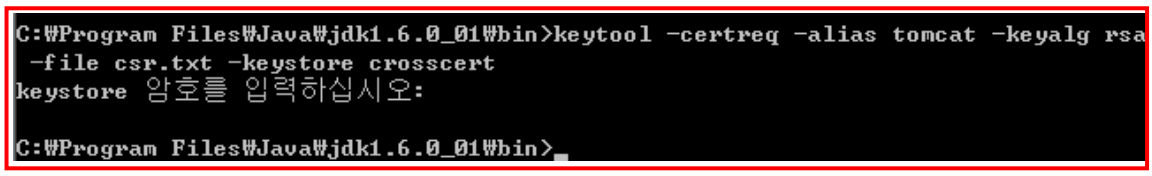
1. Tomcat은 Keytool을 통하여 개인키 및 CSR이 생성된다.
개인키 및 인증서 신청 시 필요한 CSR을 생성하기 위하여 Keytool 명령어를 아래와 같이 실행한다.
keytool –genkey keyalg rsa –alias 앨리어스명 –keystore 키스토어명

```
C:₩Program Files₩Java₩jdk1.6.0_01₩bin>keytool -genkey -keyalg rsa -alias tomcat
-keystore crosscert
keystore 암호를 입력하십시오:
```

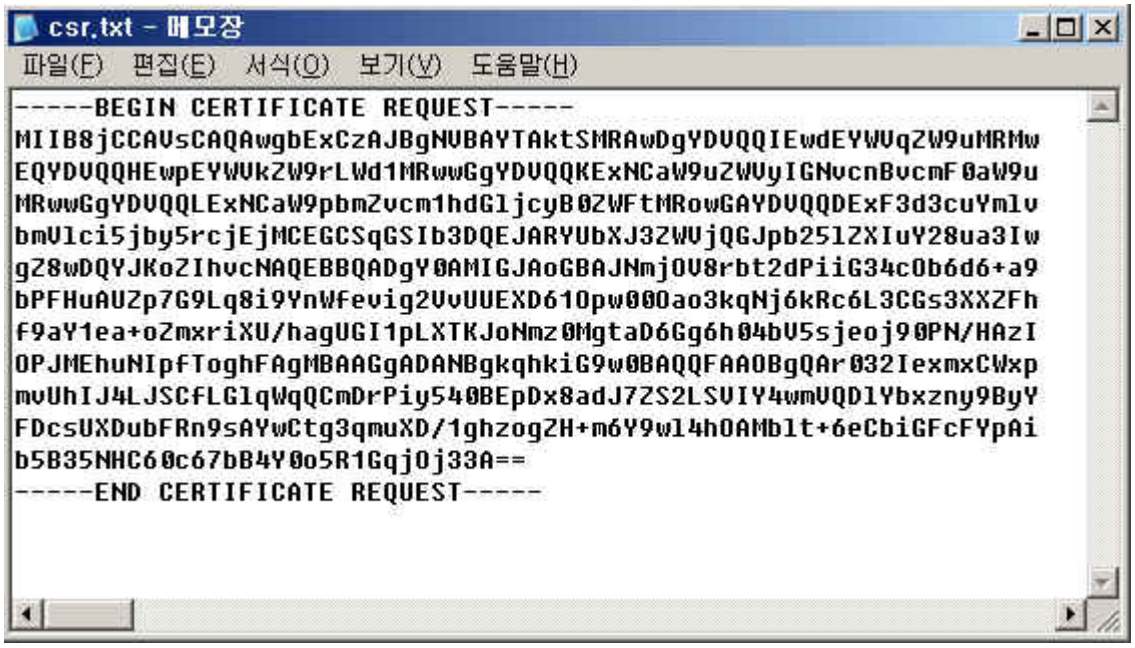
2. 1번 항목의 명령어를 입력하면 키스토어 패스워드 입력 후 DN값 입력 항목이 나오게 된다.

```
C:₩Program Files₩Java₩jdk1.6.0_01₩bin>keytool -genkey -keyalg rsa -alias tomcat
-keystore crosscert
keystore 암호를 입력하십시오:
새 암호를 다시 입력하십시오:
이름과 성을 입력하십시오.
  [Unknown]:  csteam.crosscert.com ──→ 해당 URL 입력 (ex. www.crosscert.com)
조직 단위 이름을 입력하십시오.
  [Unknown]:  csteam ──→ 부서명 입력 (ex. VCS Team)
조직 이름을 입력하십시오.
  [Unknown]:  Crosscert Inc. ──→ 회사명 입력 (ex. Crosscert)
구/군/시 이름을 입력하십시오?
  [Unknown]:  Seochogu ──→ 구/군/시 입력 (ex. Seocho-gu)
시/도 이름을 입력하십시오.
  [Unknown]:  Seoul ──→ 시/도 입력 (ex. Seoul)
이 조직의 두 자리 국가 코드를 입력하십시오.
  [Unknown]:  KR ──→ 국가코드 입력 (ex. KR)
CN=csteam.crosscert.com, OU=csteam, O=Crosscert Inc., L=Seochogu, ST=Seoul, C=KR
이(가) 맞습니까?
  [아니오]:  y

<tomcat>에 대한 키 암호를 입력하십시오.
        (keystore 암호와 같은 경우 Enter를 누르십시오):

C:₩Program Files₩Java₩jdk1.6.0_01₩bin>
```

3. CSR을 파일형태로 생성하기 위해 아래의 명령어를 실행한다.
keytool -certreq -alias 앨리어스명 -keyalg rsa -file csr.txt -keystore 키스토어명



4. CSR생성 시 설정했던 저장위치로 이동하여 CSR파일(예 : csr.txt)을 메모장이나 워드패드로 열어보면 -----BIGIN NEW CERTIFICATE REQUEST----- 부터 -----END NEW CERTIFICATE REQUEST----- 를 확인할 수 있다. 인증서 신청 시 이 내용을 이용하여 인증서 신청을 진행한다.

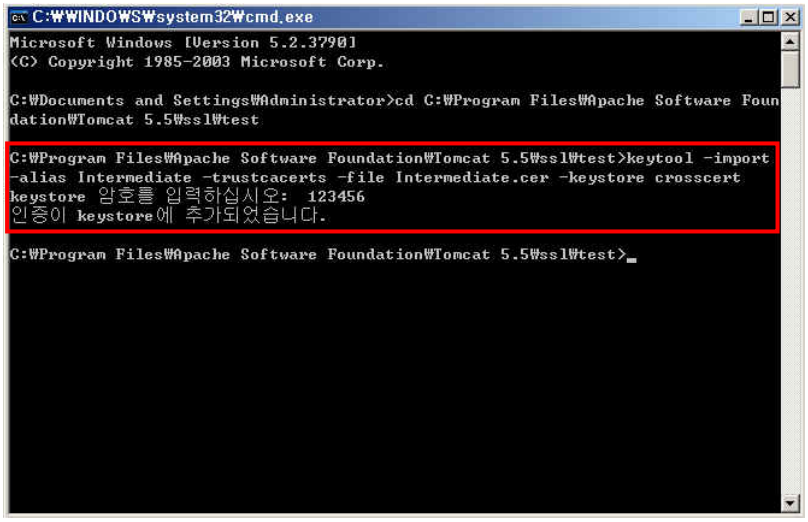


한국전자인증	Title **Tomcat 4.x 인증서 설치 매뉴얼**		
	문서번호: Tom-10000	버전: 1.0	작성일: 2008-03-04

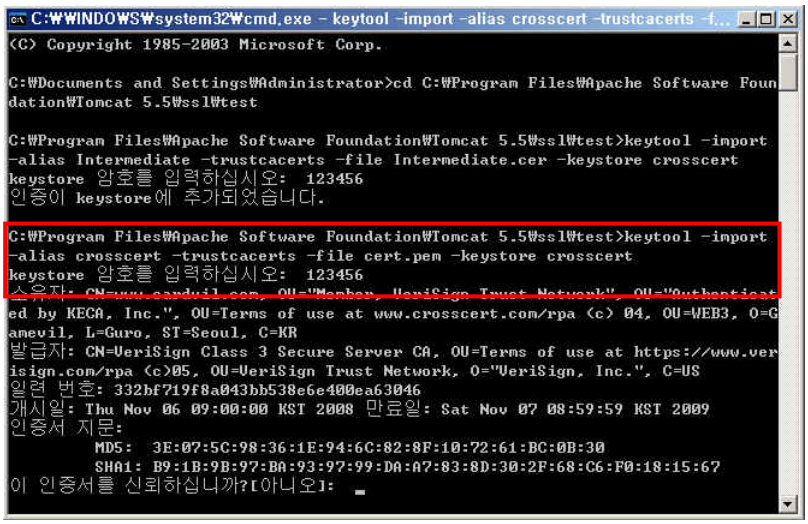
▶ 인증서 설치

1. 인증서는 이메일을 통하여 전송되게 된다. 전달받은 인증서가 담긴 이메일의 내용 중 -----BEGIN CERTIFICATE----- 부터 -----END CERTIFICATE----- 까지를 복사하여 메모장이나 워드패드에 붙여 넣은 후 임의의 파일명(예 : cert.pem)으로 저장한다.

2. 발급 받은 인증서를 탑재하기 전에 먼저 체인인증서를 키스토어에 탑재하여야 한다.
 keytool -import -alias Intermediate -trustcacerts -file **체인인증서 파일명** -keystore **키스토어명**

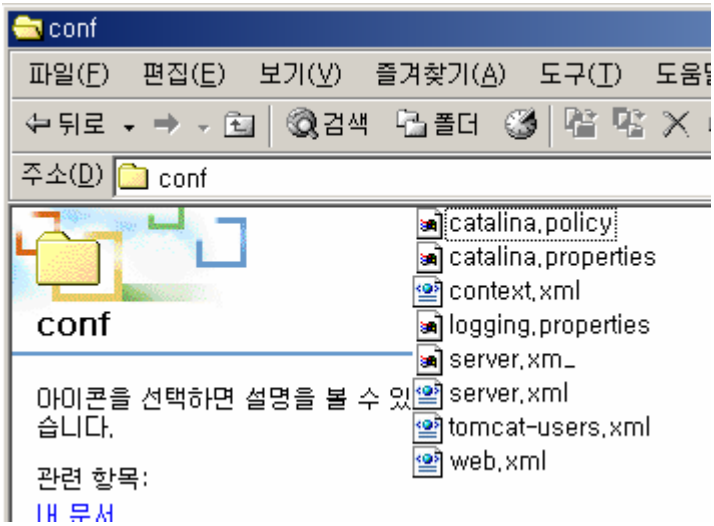


3. 발급 받은 인증서를 키스토어에 탑재한다.
 keytool -import -alias **앨리어스명** -trustcacerts -file **인증서 파일명** -keystore **키스토어명**

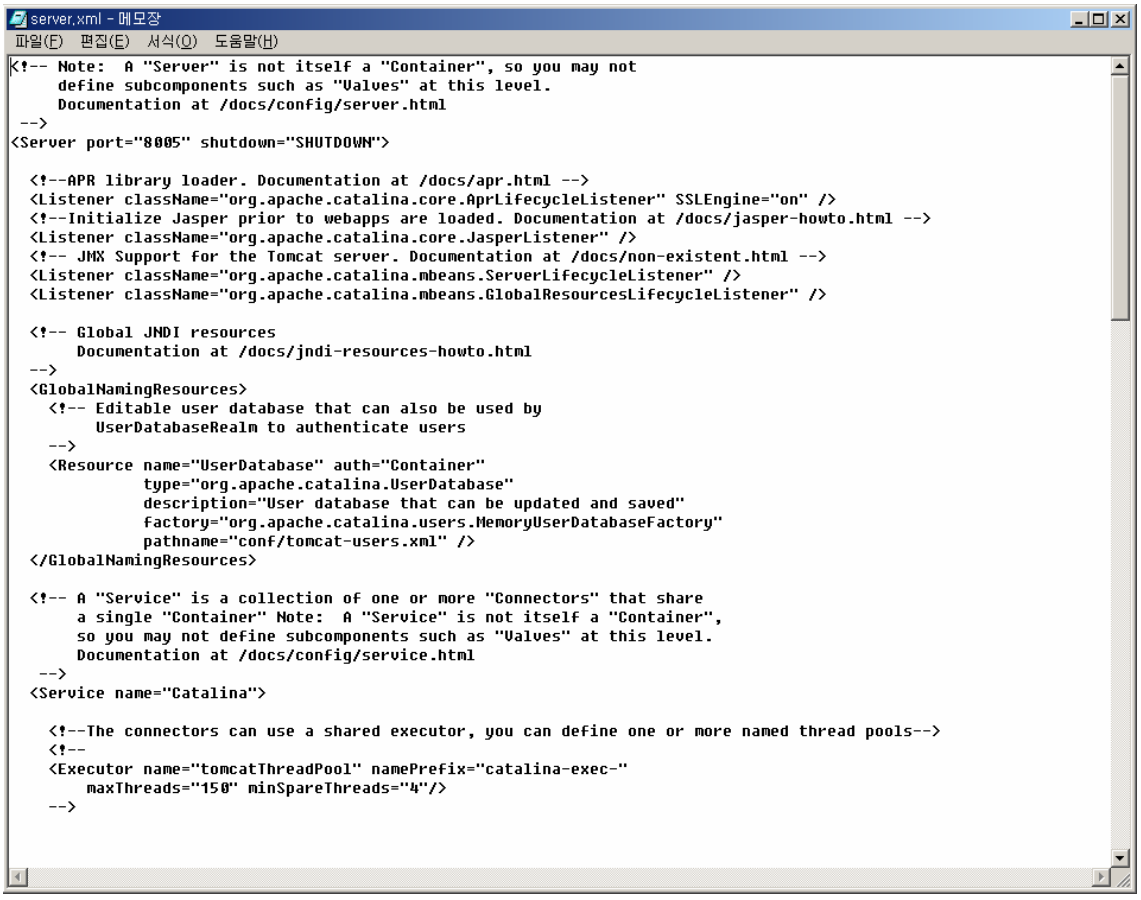


▶ SSL 적용

1. Tomcat 4.x의 환경설정 디렉토리로 이동한다.



2. server.xml파일을 메모장과 같은 프로그램을 통해 오픈한다.



3. Tomcat 4.x의 경우 server.xml파일에서 아래와 같이 설정해 주어야 한다. (SSL의 기본포트 : 443)

```
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
           port="SSL에 사용할 포트" enableLookups="true" scheme="https" secure="true"
           acceptCount="100"
           useURIValidationHack="flase" disableUploadTimeout="true"
           keystoreFile="키스토어 경로"
           keystorePass="키스토어 패스워드"
           clientAuth="false" sslProtocol="TLS" />
```

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->

<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
           port="8443" enableLookups="true" scheme="https" secure="true"
           acceptCount="100"
           useURIValidationHack="false" disableUploadTimeout="true"
           keystoreFile="C:\Program Files\Apache Software Foundation\Tomcat 4.1\Key\crosscert"
           keystorePass="123456"
           clientAuth="false" sslProtocol="TLS" />
```

4. https로 접속하여 인증서가 정상적으로 탑재되었는지 확인한다.