Comodo Korea
국제표준인증 제휴기관

Tomcat (4.x, 5.x 공통) CSR(Certificate Signing Request) 생성

Tomcat 4.x, 5.x 웹 서버를 사용하시는 경우에는 SSL 환경설정이 필요합니다.
SSL 환경설정은 JSSE(Java Secure Socket Extension) 1.0.2 (또는 이후 버전) 패키지가 웹 서버에 설치되어야 합니다.
그리고 Tomcat 4.x, 5.x 웹 서버는 JKS 형식의 키스토어로 인증서가 설정됩니다.
JKS 형식은 Java 표준 "Java KeyStore" 형식이고, keytool 도구에 의해서 설정할 수 있습니다. keytool 도구는 JDK 에 포함되어 있습니다. 그런데 JDK 1.4 패키지부터는 JSSE 패키지가 포함되어있으므로, 코모도코리아에서는 현재 최종 JDK 버젼인 J2SE(Java 2 Platform, Standard Edition) 설치를 권장해 드립니다.
Tomcat 4.x, 5.x 웹 서버의 SSL 환경설정을 마친 다음에는 keytool 도구로 keystore 를 만들면서, 서버 개인키(비밀키)를 생성합니다.
다음으로 생성된 서버 개인키(비밀키)를 토대로 CSR(Certificate Signing Request) 파일을 생성합니다.
생성된 CSR 파일을 코모도코리아로 보내주시면, 루트기관에서 발행하는 정식인증서 발급 절차를 밟게 됩니다.
그 후에 정식 인증서가 발급되고 웹 서버에 설치되면 웹 서버 SSL 설정은 마쳐지게 됩니다.

※ CSR(Certificate Signing Request) 생성 순서

1. SSL 환경 확인과 J2SE 설치 확인
2. keystore 생성
3. CSR 파일 생성
4. 개인키(비밀키) 설정된 keystore 백업
5. 코모도코리아에 CSR 접수
6. 네트워크 확인 사항 - SSL 적용에 따른 방화벽, L4 switch 설정 확인
7. 코모도코리아 CSR 파일 답신 확인

---

1. SSL 환경 확인과 J2SE 설치 확인

(인증서 갱신 고객님은 "**2. keystore 생성**"부터 진행해 주시면 됩니다.)
만약 Tomcat 4.x, 5.x 웹 서버와 다른 웹 서버(Apache, IIS 등)를 운영하고, 주 웹 서버(Apache, IIS 등)의 뒤에서 Tomcat 4.x 서버를 Servlet/JSP 컨테이너 서버로 사용할 경우에는 주 웹 서버에 SSL 인증서를 설정하고 SSL 환경을 만들게 됩니다.
이렇게 주 웹 서버와 Tomcat Servlet/JSP 컨테이너 서버로 운영하실 때에는 SSL 환경 설정을 주 웹 서버에 잡게 되므로 확인바랍니다.

Comodo Korea
국제표준인증 제휴기관

Tomcat 4.x 웹 서버에 J2SE 를 설치를 확인합니다.

```
[root@web1 root]# java -version
java version "1.4.2_05"
Java(TM) 2 Runtime Environment,
Standard Edition (build 1.4.2_05-b04)
Java HotSpot(TM) Client VM (build
1.4.2_05-b04, mixed mode)

[root@web1 root]# keytool
keytool 사용법:

-certreq     [-v] [-alias <별명>] [-
sigalg <서명 알고리즘>]
...
[root@web1 root]# ls -a
$JAVA_HOME/bin
...
keytool*
java*
[root@web1 root]#
```

위의 결과는 1.4.2_05 버젼의 java J2SE 패키지가 설치되었으며, keytool 도구와 경로 설정이 잘된 것을 확인할 수 있습니다.

J2SE 패키지 설치되지 않으셨다면, J2SE 패키지 설치 가이드를 참고해 주시기 바랍니다. (J2SE 패키지 설치 가이드 보기)

2. keystore 생성

JKS 형식의 keystore 를 생성합니다. 2048 비트 RSA 개인키(비밀키)가 keystore 에 만들어집니다.
keystore 를 생성하면서 키정보를 설정하게 되므로 아래 예시를 통해서 잘 설정해 주시기 바랍니다.
keystore 의 암호설정은 keystore 를 관리하는 암호가 되므로 잃어버리지 않도록 잘 기억하시기를 바랍니다.
그리고, "이름과 성을 입력(your first and last name)" 항목은 "인증 받을 도메인 주소"를 설정해 주시는 부분이므로 오해가 없으시기를 바랍니다.

<입력 예>

Comodo Korea
국제표준인증 제휴기관

이름과 성을 입력(your first and last name) : www.comodokorea.co.kr
"이름과 성을 입력"항목은 "인증 받을 도메인 주소"를 설정해 주시는 부분입니다.
조직 단위 이름을 입력(organizational unit) : Digital Certificate Team
조직 이름을 입력(organization) : Comodo Korea
구/군/시 이름을 입력(City or Locality) : Songpa
시/도 이름을 입력(State or Province) : Seoul
두 자리 국가 코드(country code) : KR

- $SSL_KEY_STORE 변수는 ssl 개인키를 보관하는 디렉토리를 가리킵니다.

```
[root@web1 root]# keytool -genkey W
> -alias tomcat2007 W
> -keyalg RSA W
> -keysize 2048 W
> -keystore
$SSL_KEY_STORE/tomcat2007key
keystore 암호를 입력하십시요:  [암호
입력]
이름과 성을 입력하십시요.
  [Unknown]:  www.anycert.co.kr
조직 단위 이름을 입력하십시오.
  [Unknown]:  Digital Certificate
Team
조직 이름을 입력하십시오.
  [Unknown]:  Dotname Korea
구/군/시 이름을 입력하십시오?
  [Unknown]:  Songpa
시/도 이름을 입력하십시오.
  [Unknown]:  Seoul
이 조직의 두 자리 국가 코드를
입력하십시오.
  [Unknown]:  KR
CN=www.anycert.co.kr, OU=Digital
Certificate Team,
O=Dotname Korea, L=Songpa, ST=Seoul,
C=KR 이(가) 맞습니까?
```

```
  [아니오]:  y

에 대한 키 암호를 입력하십시요
        (keystore 암호와 같은 경우
RETURN 을 누르십시오): [RETURN 입력]
[root@web1 root]#
```

3. CSR 파일 생성

생성된 keystore 에서 CSR(Certificate Signing Request) 파일을 만듭니다.

- $SSL_KEY_STORE 변수는 ssl 개인키를 보관하는 디렉토리를 가리킵니다.

```
[root@web1 root]# keytool -certreq W
> -alias tomcat2007 W
> -file $SSL_KEY_STORE/tomcat2007.csr W
> -keystore $SSL_KEY_STORE/tomcat2007key
keystore 암호를 입력하십시오:  [암호 입력]
[root@web1 root]#
```

4. 개인키(비밀키) 설정된keystore 백업

- $SSL_KEY_STORE 변수는 ssl 개인키를 보관하는 디렉토리를 가리킵니다.

```
[root@web1 root]# cd $SSL_KEY_STORE
[root@web1 ssl]# sftp xxx.xx.xx.xx
> put tomcat2007key
```

안전한 곳에 개인키(비밀키) 설정된 keystore 를 백업 복사를 해 놓습니다.

※ 개인키(비밀키) 설정된 keystore 파일과 패스워드는 결코 잃어버리시면 안 됩니다. 안전한 장소에 백업해두시기 바랍니다.

5. 코모도코리아에 CSR 접수

생성된 CSR 파일을 출력해보면 다음과 같은 base64 형식의 문서를 볼 수 있습니다.

- 위의 작업과 계속 연관된 작업을 진행합니다.

```
[root@web1 ssl]# cat tomcat2007.csr
-----BEGIN NEW CERTIFICATE REQUEST-----
MIISDOIUlkmlsRRlkSllskjauASKJlalOSISLKjwBgNV
BAgTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBU
b3duMRQwEgYDVQQKEwtPcHBvcnR1bmlOaTEYMBYGA1UE
```

Comodo Korea
국제표준인증 계휴기관

```
CxMPT25saW5lIFNlcnZpY2VzMRowGAYDVQQDExF3d3cu
Zm9yd2FyZC5jby56YTBaMA0GCSqGSIb3DQEBAQUAAAkl
mLKSuljSOIjsfBWu5WLHD/G4BJ+PobiC9d7S6pDvAjuy
C+dPAnL0d91tXdm2j190D1kgDoSp5ZyGSgwJh2V7diuu
PlHDAgEDoAAwDQYJKoZIhvcNAQEEBQADQQBf8LSLKknl
sklSSLlworrr334ZmXD1AvUjuDPCWzFupReiq7UR8ZOw
JUUsllkfq/IuuIlz6oCq6htdH7/tvKhh
-----END NEW CERTIFICATE REQUEST-----
[root@web1 ssl]#
```

이 CSR 문서를 반드시 첫줄(-----BEGIN CERTIFICATE REQUEST-----)과 끝줄(-----END CERTIFICATE REQUEST-----)이 포함되도록 복사하여 메모장에 붙여넣기 합니다.
이 CSR 을 코모도코리아 메일로 첨부해 주시기 바랍니다.

6. 네트워크 확인 사항 - SSL 적용에 따른 방화벽, L4 switch 설정 확인

고객님 웹 서버에 SSL 을 적용하게 되면, http:// (기본 80 포트)통신과 https:// (기본 443 포트) 통신를 사용하게 됩니다.
그러므로, 웹 서버에 설정된 방화벽이나 L4 switch 의 설정을 기존 80 포트 설정과 같이 443 포트도 추가 설정해 주셔야 합니다.
정식 인증서를 발행하기까지 웹 서버의 네트워크 환경설정에 443 포트를 열어주시는 계획을 세워주기 바랍니다.

7. 코모도코리아 CSR 파일 답신 확인

코모도코리아에 접수된 CSR 파일이 올바른지 회신을 드립니다. 회신을 확인하시기 바랍니다.
그리고 코모도코리아에서는 보내주신 CSR(Certificate Signing Request) 파일을 토대로 정식 인증서를 발급하게 됩니다.
정식 인증서 발급과 함께 인증서 설치 문서를 안내해 드립니다.