Comodo Korea
국제표준인증 제휴기관

Tomcat (4.x, 5.x 공통) 웹 서버 인증서 설치

먼저 Tomcat 웹 서버에 CSR(Certificate Signing Request)을 생성하면서, keytool 도구로 keystore 를 만들었습니다.
그리고 생성된 keystore 에는 서버 개인키(비밀키)를 생성 되었습니다. Tomcat 웹 서버 인증서 설치 과정은 서버 개인키(비밀키)를 가지고 있는 keystore 에 발급된 인증서를 keytool 도구로 설치하는 과정입니다.
그리고 Tomcat 웹 서버의 설정 파일(server.xml) 에 SSL 인증서가 설치된 keystore 를 설정해 주게 됩니다.

※ Tomcat 웹 서버 인증서 설치 순서

1. 발급된 인증서 확인
2. 웹 서버로 발급된 인증서 올리기
3. keystore 에 루트인증서 설치하기
4. keystore 에 체인인증서 설치하기
5. keystore 에 웹 서버 인증서 설치하기
6. Tomcat 웹 서버 설정파일에 keystore 설정하기
7. Tomcat SSL restart
8. 8. 인증서 백업해두기

---

1. 발급된 인증서 확인

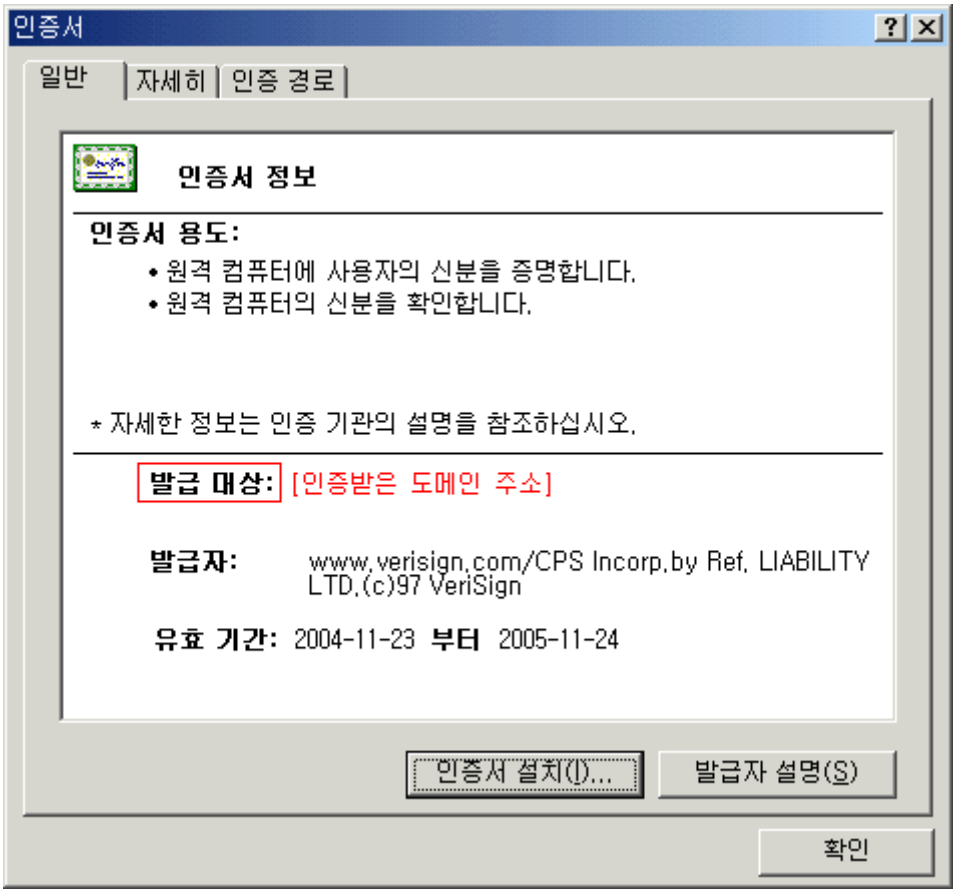
먼저 발급된 인증서를 확인합니다. 웹 서버 인증서와 루트인증서, 체인인증서, 세개의 파일이 발급됩니다.

웹 서버인증서 : [인증받은 도메인 이름으로 된].p7b
루트인증서 : TrustSign_Root.cer
체인인증서 : TrustSign_Chain.cer

위의 발급된 인증서는 코모도코리아에서 고객님께 전자 메일로 발급해 드립니다.
그러므로 전자 메일에 발급된 인증서 항목을 알려드리며, 발급된 인증서는 첨부파일로 첨부되어있습니다.

윈도우 PC 에서 발급 받으신 웹 서버 인증서([인증받은 도메인 이름으로 된].p7b 파일)를 열어서(double click) 내용을 확인합니다.(메모장이나 울트라 에디터에서 열지 않습니다.)
웹 서버 인증서를 열게 되면 다음과 같은 내용을 확인하실 수 있습니다.

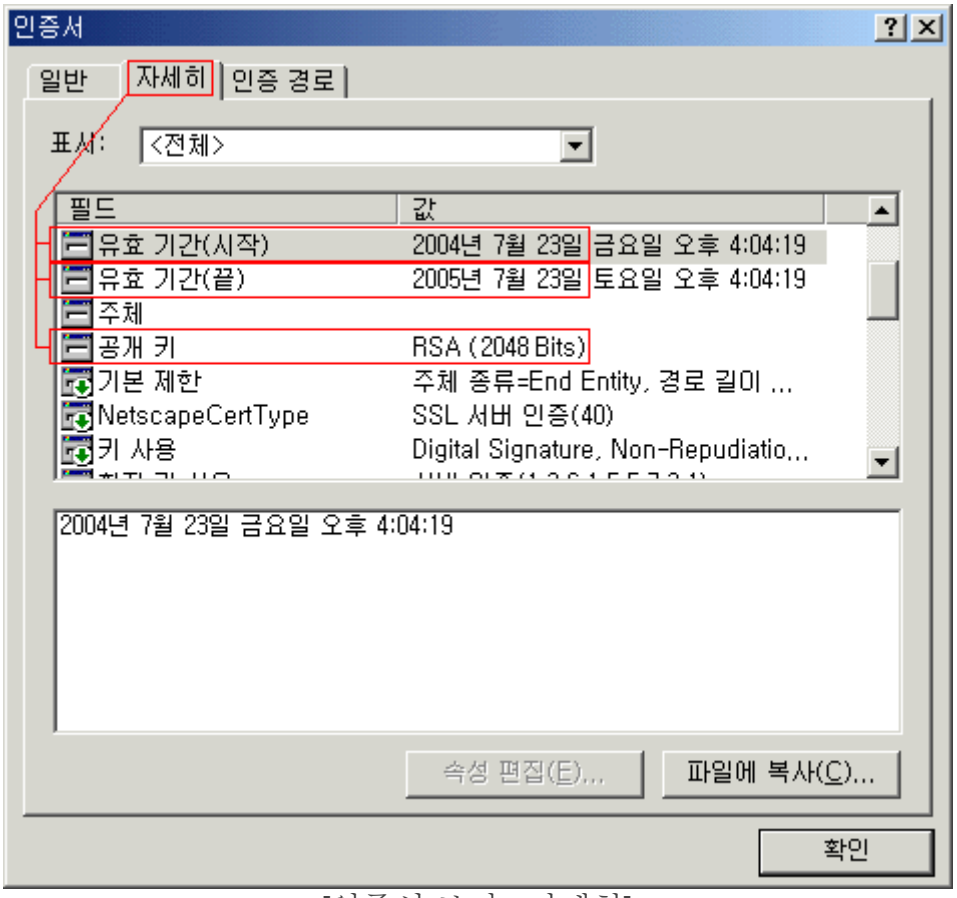
Comodo Korea
국제표준인증 제휴기관



[인증서 보기 - 일반]

웹 서버 인증서 정보의 [일반] 탭 부분에서 인증서 정보에서 인증서 용도가 "원격 컴퓨터에 사용자의 신분을 증명합니다." 와 "원격 컴퓨터의 신분을 확인합니다."를 확인 할 수 있습니다. 그리고 발급 대상에서 고객님이 인증받을 도메인 주소로 신청하신 도메인 주소가 맞는지 확인합니다.

다음으로는 [자세히] 탭 부분에서



[인증서 보기 - 자세히]

발급한 웹 서버 인증서의 유효기간을 확인합니다. (유효 기간(시작)과 유효 기간(끝) 정보를 확인합니다.)
그리고 공개 키 부분에서 RSA (2048 Bits) 를 확인합니다. 코모도코리아에서 발행되는 인증서는 2048 Bits 키를 권고합니다. 꼭 확인해 주시기 바랍니다.

그리고 먼저 CSR(Certificate Signing Request) 파일을 생성하시면서, 서버키(개인키) keystore 로 생성했었습니다. 서버키(개인키) keystore 를 확인해 주시기 바랍니다. (CSR 생성때에 서버키(개인키) keystore 를 체크했으므로, 어디에 서버키(개인키) keystore 가 저장되어있는지 확인만 해 주시면 됩니다.)

2. 웹 서버로 발급된 인증서 올리기

발급받으신 인증서를 Tomcat 웹 서버에 복사합니다.(보통 Ftp 로 웹 서버로 올려 주시면 됩니다.)

3. keystore 에 루트인증서 설치하기

JKS 형식의 keystore 에 루트인증서부터 설치합니다. 순서가 중요합니다.

- $SSL_KEY_STORE 변수는 ssl 개인키를 보관하는 디렉토리를 가리킵니다.
- tomcat2007key 파일은 CSR 을 요청드렸을 때에 만들어진 서버키 keystore 입니다.
- root 알리아스 이름은 루트인증서 설치를 위한 임의의 알리아스 입니다.

루트인증서 설치시에 에러가 발생한다면, 에러 상태를 파악하시고 코모도코리아로 문의를 주시기 바랍니다.
간단한 에러 설명과 함께 현재 에러 리포트를 코모도코리아 메일로 통보해 주시기 바랍니다.

4. keystore 에 체인인증서 설치하기

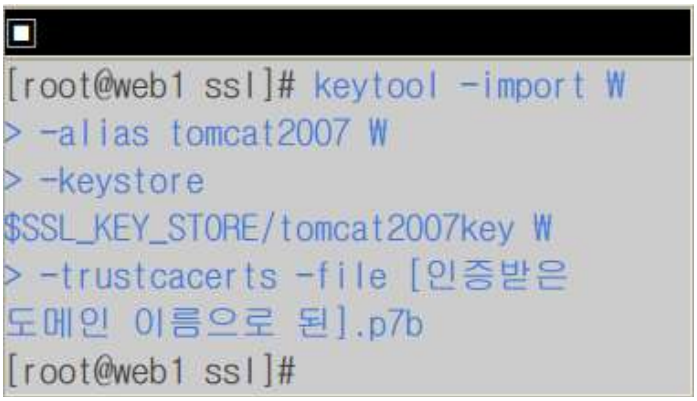
JKS 형식의 keystore 에 체인인증서를 설치합니다.
- $SSL_KEY_STORE 변수는 ssl 개인키를 보관하는 디렉토리를 가리킵니다.
- tomcat2007key 파일은 CSR 을 요청드렸을 때에 만들어진 서버키 keystore 입니다.
- chain 알리아스 이름은 체인인증서 설치를 위한 임의의 알리아스 입니다.

체인인증서 설치시에 에러가 발생한다면, 에러 상태를 파악하시고 코모도코리아로 문의를 주시기 바랍니다.
간단한 에러 설명과 함께 현재 에러 리포트를 코모도코리아 메일로 통보해 주시기 바랍니다.

5. keystore 에 웹 서버 인증서 설치하기

JKS 형식의 keystore 에 웹 서버 인증서를 설치합니다.

- 위와 연속된 작업을 처리합니다.



웹 서버 인증서 설치시에 에러가 발생한다면, 에러 상태를 파악하시고 코모도코리아로 문의를 주시기 바랍니다.
간단한 에러 설명과 함께 현재 에러 리포트를 코모도코리아 메일로 통보해 주시기 바랍니다.

6. Tomcat 웹 서버 설정파일에 keystore 설정하기

Tomcat 웹 서버 버젼을 선택해 주시기 바랍니다.

◉ Tomcat 4.xx ○ Tomcat 5.0.x

$TOMCAT/conf/server.xml 웹 서버 설정 파일이 있습니다. ($TOMCAT 변수는 Tomcat 설치 디렉토리를 가르킵니다.)
다음은 server.xml 파일의 [Define a SSL Coyote HTTP/1.1 Connector] 부분에 인증서 설치 영역의 원본 내용입니다.

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<!--
<Connector
className="org.apache.coyote.tomcat4.CoyoteConnector"
     port="8443" minProcessors="5" maxProcessors="75"
     enableLookups="true"
     acceptCount="100" debug="0" scheme="https" secure="true"
     useURIValidationHack="false" disableUploadTimeout="true">
   <Factory
className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
         clientAuth="false" protocol="TLS" />
</Connector>
-->
```

[Define a SSL Coyote HTTP/1.1 Connector] 설정에서 기본적으로 Tomcat 설정은 8443 포트를 사용하도록 된 것을 443(https) 포트로 바꾸어 줍니다. 그리고 기본적으로 [Define a SSL Coyote HTTP/1.1 Connector] 설정이 <!--

, --> 주석(comment)으로 막힌 것을 풀어줍니다.

그리고 [Factory] 항목에서 Tomcat 웹 서버에 SSL 인증서가 설치된 keystoreFile 을 설정합니다.
다음 설정 예시를 참고하시고, 설정해 주시기 바랍니다.
- $SSL_KEY_STORE 변수는 ssl 개인키를 보관하는 디렉토리를 가리킵니다.
- tomcat2007key 파일은 CSR 을 요청드렸을 때에 만들어진 서버키 keystore 입니다.

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<!-- 주석으로 싸여진 것을 풀어줍니다. -->
<Connector
className="org.apache.coyote.tomcat4.CoyoteConnector"
     port="443" minProcessors="5" maxProcessors="75"
     enableLookups="true"
     acceptCount="100" debug="0" scheme="https" secure="true"
     useURIValidationHack="false" disableUploadTimeout="true">
   <Factory
className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
         keystoreFile="$SSL_KEY_STORE/tomcat2007key"
         keystorePass="[keystore 암호]"
         clientAuth="false" protocol="TLS" />
</Connector>
```

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port
8443 -->
<!--
    <Connector port="8443"
               maxThreads="150" minSpareThreads="25"
maxSpareThreads="75"
               enableLookups="false"
disableUploadTimeout="true"
               acceptCount="100" debug="0"
scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS"
/>
-->

<!-- Define a SSL Coyote HTTP/1.1 Connector on port
8443 -->
<!-- 주석으로 싸여진 것을 풀어줍니다. -->
    <Connector port="443"
               maxThreads="150" minSpareThreads="25"
```

```
maxSpareThreads="75"
               enableLookups="false"
disableUploadTimeout="true"
               acceptCount="100" debug="0"
scheme="https" secure="true"

keystoreFiles="$SSL_KEY_STORE/tomcat2007key"
               keystorePass="[keystore 암호]"
               clientAuth="false" sslProtocol="TLS"
/>
```

7. Tomcat SSL restart

- $TOMCAT 변수는 Tomcat 설치 디렉토리를 가르킵니다.

```
[root@web1 root]#
$TOMCAT/bin/shutdown.sh
[root@web1 root]#
$TOMCAT/bin/startup.sh
[root@web1 root]#
```

에러로 인해서 재 기동되지 않는다면, stdout.log 파일의 에러 상태를 파악해 주시고, 코모도코리아로 문의를 주시기 바랍니다.
간단한 에러 설명과 함께 현재 에러 로그를 리포트해서 코모도코리아 메일로 통보해 주시기 바랍니다.

8. 인증서 백업해 두기

개인키 파일을 백업해둡니다.

<개인키 파일을 꼭 백업해두셔야 하며, 백업을 하지 않아 발생하는 문제에 대해서는 재발급 비용이 추가될 수 있습니다.>