

■ 키 생성 및 CSR 생성

▶ 키 생성을 위해 OpenSSL 설치 디렉토리에서 아래 명령대로 생성

1. 랜덤 넘버 생성

```
$ openssl md5 * > rand.dat
```

2. 키 쌍 생성

```
openssl genrsa -rand rand.cat -des3 1024 > key.pem
```

```
[root@localhost ssl]# pwd
/usr/local/apache/ssl
[root@localhost ssl]# openssl md5 * > rand.dat
[root@localhost ssl]# ls
rand.dat
[root@localhost ssl]# openssl genrsa -rand rand.cat -des3 1024 > key.pem
0 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
Enter pass phrase:
Verifying - Enter pass phrase:
[root@localhost ssl]# ls
key.pem rand.dat
```

3. 생성된 키 쌍을 이용하여 CSR 생성

```
openssl req -new -key key.pem > csr.pem
```

(Enter PEM pass phrase : key 비밀번호설정)

- Country(국가 코드) :
 - State/province (시/도의 전체 이름) :
 - Locality(시, 구, 군 등의 이름) :
 - Organization(회사 이름) :
 - Organization Unit(부서명-예를 들면 전산팀,마케팅팀,운영팀 등) :
 - Common Name(host name+domain name 서비스할 전체 URL) :
- "추가 속성"을 입력하라는 메시지가 나타나면 그냥 무시하십시오.

(아래 실행 화면.)

■ CSR 확인

```

[root@localhost ssl]# openssl req -new -key key.pem > csr.pem
Enter pass phrase for key.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

-----
Country Name (2 letter code) [GB]:KR
State or Province Name (full name) [Berkshire]:Seoul
Locality Name (eg, city) [Newbury]:Secho-gu
Organization Name (eg, company) [My Company Ltd]:Crosscert
Organizational Unit Name (eg, section) []:IT Team
Common Name (eg, your name or your server's hostname) []:www.test.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

```

4. CSR 값 확인. (vi csr.pem)

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBrTCCARYCAQAwbTELMAkGA1UEBhMCN1IxDjAMBgNVBAgTBVNIb3VsMREwDwYD
VQQHEwhTZWNoby1ndTESMBAGA1UEChMJQ3Jvc3NjZXMOMRAwDgYDVQQLEwdJVCBU
ZWFtMRUwEwYDVQQDEwx3d3cudGVzdC5jb20wZ8wDQYJKoZIhvcNAQEBBQADgYOA
MIGJAoGBANdW5cJHAngalQP2Dn4M4IRvqxYYv7hZAZdzh167Daoyq219T87IXOC9
D8c3kwmPNLiEMIQPfdkSbPuGLpTiyMPJGJmGFOS7w1ZQKKLIR1e8mQvTwz1RNuPa
sq/U62GzXd1DXsmBkG6s/7SrqPjNswzm9ScfMr/YYgkde7Yns+IXAgMBAAGgADAN
BgkqhkiG9w0BAQUFAAQBgQB5oJungINVQCWwARaK5qEWVr2JhEsASQHTYQXHdXw4
Fm1JGafABMFVcyvz2CrpYttYIA51Lr7dsxrUeR/tVZSLNSC6qek/H/WfsuL0vdqC
mZtvRx5a2CQn1qAitth10c17109bis4oBH/L9I+mk+TTXapMgFdiFuCK00tdFS+H
pg==
-----END CERTIFICATE REQUEST-----

```

- CSR(Certificate Signing Request) 즉, 인증서 서명 요청입니다. 이는 자신이 설치할 웹서버에서 DN 값, 각종정보를 암호화한 파일로써 '한국전자인증' 신청란에서 붙여넣으면 됩니다.

■ 인증서 설치

1. 직접 CSR 및 KEY 생성시.

- 해당 디지털 ID 승인후 E-mail 로 기술 담당자에게 송신됩니다. 서버 ID 는 다음과 같이 나타납니다.

ServerName www.xxx.co.kr (인증서 URL)
 ServerAdmin admin@xxx.co.kr
 SSLEngine on
 SSLCipherSuite
 ALL:!ADH:!EXP56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL

- VirtualHost 설정부분에 아래처럼 SSL 관련 경로를 설정해 주시면 됩니다.

SSLCertificateFile /usr/local/apache/conf/ssl/cert.pem (인증서 파일 설정)

SSLCertificateKeyFile /usr/local/apache/conf/ssl/key.pem (키 파일 설정)

- * 시큐어 서버 인증서의 경우 다음의 설정을 추가 하셔야 합니다.

SSLCACertificateFile /usr/local/apache/conf/ssl/secureCA.pem (시큐어 체인인증서 파일)

- * 글로벌 서버 인증서(128bit SSL)의 경우엔 다음의 설정을 추가 하셔야 합니다.

SSLCACertificateFile /usr/local/apache/conf/ssl/intermediate.pem (글로벌 체인인증서 파일)

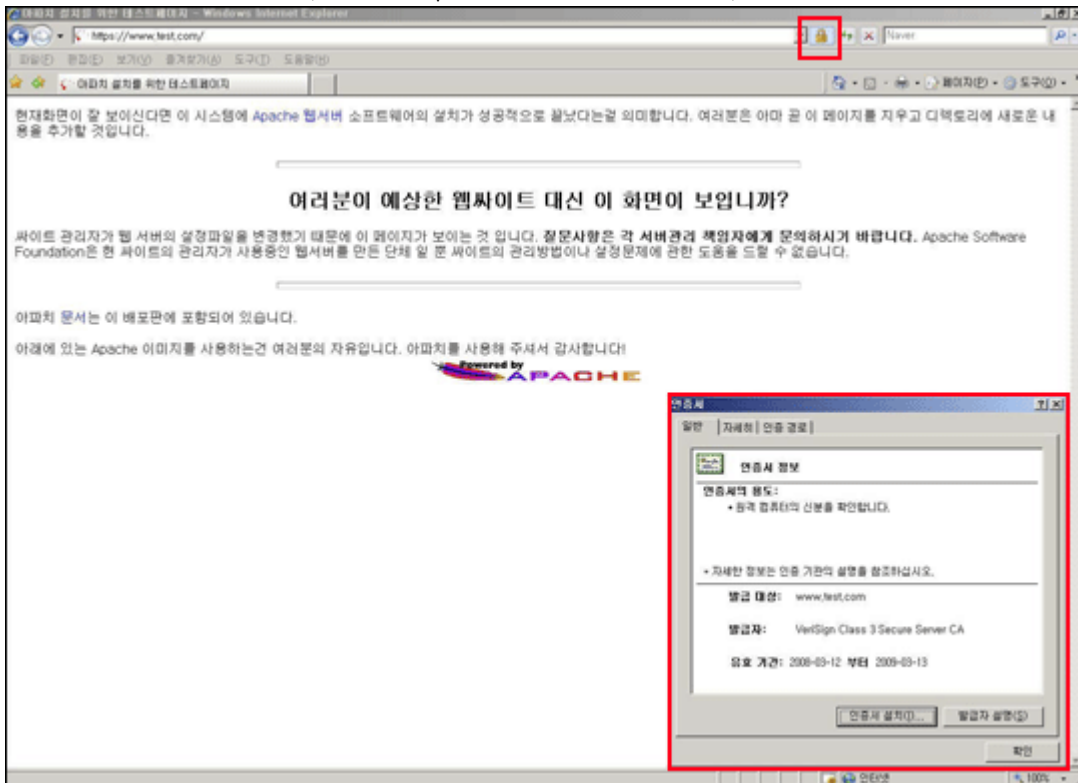
■ 인증서 확인

5. 아파치 재구동

\$ apachectl stop

\$ apachectl start (키비밀번호 입력)

6. 웹페이지에서 확인 (해당 https://URL 으로 확인)



■ 개인키 패스워드 변경,삭제 및 복구 방법(openssl)

- openssl 을 이용하여 개인키의 비밀번호를 변경할 수 있습니다.

1. 키 파일 패스워드 변경하기(openssl 이 설치되어 있는 디렉토리에서 설정)

```
$ openssl rsa -des3 -in key.pem -out newkey.pem
```

Pass-Phrase 를 물어보면...

처음에는 기존 패스워드 입력, 두 번째는 새로운 패스워드 입력.

2. 키 파일 패스워드 삭제하기(openssl 이 설치되어 있는 디렉토리에서 설정)

```
$ openssl rsa -in key.pem -out newkey.pem
```

3. 키 파일 삭제한 패스워드 복구하기(openssl 이 설치되어 있는 디렉토리에서 설정)

```
$ openssl rsa -in key.pem des3 -out newkey.pem
```

■ Conf 파일수정

■ 설치환경

Apache 1.x, 2.x, 2.2.x 에서 설정

www.test.com, www.test2.com 두개의 인증서 설치하기

- Httpd.conf 환경설정

(2.x 에선 ssl.conf

2.2.x 에선 httpd-ssl.conf)

- Virtualhost 로 하나의 ip 에 두개의 인증서 설정(두개의 포트 필요)

`/usr/local/apache/conf/httpd.conf` 에서 설정(2.x 에선 ssl.conf, 2.2.x 에선 httpd-ssl.conf)

1. 두 개의 Key 값과 Cert 인증서 저장(다른 폴더에 저장)

```
/usr/local/apache/conf/ssl/test
```

```
/usr/local/apache/conf/ssl/test2 에 저장.
```

httpd.conf 파일에서 관련부분 수정(2.x 에선 ssl.conf, 2.2.x 에선 httpd-ssl.conf)

- key.pem 파일과 cert.pem 파일 설정 후 체인인증서 추가

시큐어인증서의 경우

```
SSLCACertificateFile/usr/local/apache/conf/ssl/secureCA.pem
```

글로벌인증서의 경우

```
SSLCACertificateFile/usr/local/apache/conf/ssl/intermediate.pem
```

Ex.) www.test.com, www.test2.com

[ip : 192.168.0.2](http://192.168.0.2)

3. conf 파일 수정.(아래화면)

■ Conf 파일수정

```
<ifDefine SSL>
```

```
Listen 443
```

```
Listen 444 - 443 과 444 두개의 포트 Listen
```

```
</ifDefine>
```

```
NameVirtualHost 192.168.10.12:443
```


NameVirtualHost 192.168.10.12:444 – NameVirtualHost 로 포트를 잡아준다.

```
-----  
<VirtualHost _default_:443>  
DocumentRoot "/xxx/html" (홈디렉토리)  
ServerName www.test.com:443 (인증서 URL)  
ServerAdmin admin@xxx.co.kr
```

```
SSLCertificateFile /usr/local/apache/conf/ssl/test/cert.pem (인증서 파일  
설정)  
SSLCertificateKeyFile /usr/local/apache/conf/ssl/test/key.pem (키 파일  
설정)  
SSLCACertificateFile /usr/local/apache/conf/ssl/intermediate.pem  
(글로벌 인증서의 경우)  
SSLCACertificateFile /usr/local/apache/conf/ssl/secureCA.pem  
(시큐어 인증서의 경우)  
</VirtualHost>
```

```
<VirtualHost _default_:444>  
DocumentRoot "/xxx2/html" (홈디렉토리)  
ServerName www.test2.com:444(인증서 URL)  
ServerAdmin admin@xxx.co.kr
```

```
SSLCertificateFile /usr/local/apache/conf/ssl/test2/cert.pem (인증서 파일  
설정)  
SSLCertificateKeyFile /usr/local/apache/conf/ssl/test2/key.pem (키 파일  
설정)  
SSLCACertificateFile /usr/local/apache/conf/ssl/intermediate.pem  
(글로벌 인증서의 경우)  
SSLCACertificateFile /usr/local/apache/conf/ssl/secureCA.pem  
(시큐어 인증서의 경우)  
</VirtualHost>
```

■ Conf 수정 화면

```
MaxRequestsPerChild 0  
Port 80  
<IfDefine SSL>  
Listen 443  
Listen 444  
</IfDefine>  
User nobody  
Group nobody  
ServerName www.test.com
```

```

NameVirtualHost 192.168.0.2:443
NameVirtualHost 192.168.0.2:444

<VirtualHost 192.168.0.2:443>
DocumentRoot "/usr/local/apache/htdocs"
ServerName www.test.com:443
ServerAdmin root@test.com

SSLEngine on

SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL

SSLCertificateFile /usr/local/apache/conf/ssl/test/cert.pem
SSLCertificateKeyFile /usr/local/apache/conf/ssl/test/key.pem
SSLCACertificateFile /usr/local/apache/conf/ssl/intermediate.pem
#SSLCACertificateFile /usr/local/apache/conf/ssl/secureCA.pem

</VirtualHost>

<VirtualHost 192.168.0.2:444>
DocumentRoot "/usr/local/apache/htdocs2"
ServerName www.test2.com:444
ServerAdmin root@test.com

SSLEngine on

SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL

SSLCertificateFile /usr/local/apache/conf/ssl/test2/cert.pem
SSLCertificateKeyFile /usr/local/apache/conf/ssl/test2/key.pem
SSLCACertificateFile /usr/local/apache/conf/ssl/intermediate.pem
#SSLCACertificateFile /usr/local/apache/conf/ssl/secureCA.pem

</VirtualHost>

```

▶ 가상호스트 두개의 포트별 인증서 설정 완료.

4. 아파치 재구동

```
$ apachectl stop
```

```
$ apachectl startssl (2.2.x에선 apachectl start)
```

5. 웹페이지에서 확인 (해당 <https://URL> 과 <https://URL:444> 확인)

