Apache HTTP Server SSL 설정 방법

- Ver 1.4 -

2015. 2

금융결제원

개정 이력

버전	개정일	개정 내용
Ver 1.0	2008년 5월	Apache Web Server SSL 설명서 최초작성
Ver 1.1	2009년 1월	인증서 갱신 방법, 다중 SSL 서버 설정 방법 추가
Ver 1.2	2011년 12월	암호체계 고도화 관련 키 길이 변경(2,048bit)
Ver 1.3	2014년 9월	비밀번호 규칙 권고 내용 추가
Ver 1.4	2015년 2월	PKCS #12 파일 변환 관련 설명 추가

※ 본 문서는 정보통신부.한국정보보호진흥원의「보안서버 구축 가이드」를 참고하여 작성되었습니다.

< 목 차 >

1. Apache 서버에 OpenSSL과 mod_ssl의 설치 방법

○ Apache 서버에서 SSL 통신을 가능하게 하려면 OpenSSL과 mod_ssl이 필요합니다. 우선, 현재 서비스 중인 Apache 서버에 mod_ssl이 설치되어 있는지를 httpd -l 옵션을 사용하여 mod_ssl.c 또는 mod_ssl.so가 있는지 확인하시기 바랍니다. 만일 설치되어 있다면 Apache 서버의 버전에 맞는 개인키 생성 및 CSR 생성 방법 과정으로 이동하시기 바랍니다.

[그림] mod_ssl 설치 확인 예

○ OpenSSL은 Apache 버전과 mod_ssl의 버전을 확인한 후에 알맞은 OpenSSL을 설치해야 합니다. 예를 들어 Apache 1.3.3 버전에는 mod_ssl 2.1.6(또는 2.1.7)을 설치해야 하고, mod_ssl 2.1.6은 OpenSSL 0.8.1b와 0.9.1c 버전 사이에서만 동작합니다. 버전을 확인하지 않고 OpenSSL과 mod_ssl을 설치하면 Apache 컴파일 과정에서 오류가 발생합니다. Apache 지원 버전 및 정보는 mod_ssl 소스의 README.Version 파일이나 www.openssl.org 사이트에서 확인 가능합니다.

① OepnSSL의 설치(www.openssl.org)

- 압축 풀기

```
$ gzip -cd openssl-0.9.6.tar.gz | tar xvf -
```

- config 실행

```
$ ./config$ make$ make installconfig
```

☞ prefix를 주지 않으면 "/usr/local/ssl" 디렉토리에 설치됩니다.

☞ 다른 디렉토리에 설치할려면 아래와 같이 실행합니다.

```
$ ./config --prefix=/usr/local --openssldir=/usr/local/openssl
```

② mod_ssl의 설치(www.modssl.org)

- 압축 풀기

```
$ gzip -cd apache_1.3.19.tar.gz | tar xvf
$ gzip -cd mod_ssl-2.8.1-1.3.19.tar.gz | tar xvf
```

- mod_ssl 설정

```
$ cd mod_ssl-2.8.1-1.3.19
$ ./configure ₩
--with-apache=../apache_1.3.19 ₩
--with-ssl=../openssl-0.9.6 ₩
--prefix=/usr/local/apache
```

③ Apache 서버 설정(www.apache.org)

```
$ cd ../apache_1.3.x
$ SSL_BASE=../openssl-0.9.6 ₩
./configure ₩
--prefix=/usr/local/apache ₩
--enable-module=ssl
$ make
$ make certificate
$ make install
```

2. Apache 서버에서 개인키 및 CSR 생성 방법

① 랜덤 넘버 생성

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

② 개인키/공개키 키쌍 생성

※ 전자금융사기 피해 예방을 위한 인증서 개인키 비밀번호 설정 규칙 강화 권고
비밀번호는 "숫자, 영문, 특수문자(space 포함)" 포함하여 최소 10자리 이상으로 설정
(사용매체별 혼선 방지를 위해 ', ", \, ₩(|) 4종 제외)

```
$ openssl genrsa -rand rand.dat -des3 -out key.pem 2048
Generating RSA private key, 2048 bit long modulus
.............++++++
...++++++
e is 65537 (0x10001)
Enter pass phrase for key.pem: ******
Verifying - Enter pass phrase for key.pem: ******
```

※ 2012년 1월 1일부터 암호체계 고도화 관련하여 키 길이가 2,048bit로 변경됩니다. 반드시 " 2048" 옵션을 사용해야 발급이 가능합니다.

※ 여기서 입력한 password는 CSR 생성, 인증서 설치, 보안서버 가동에서 사용되므로 반드시 기억하셔야 합니다.

③ 개인키 확인

```
$ openssl rsa -noout -text -in key.pem
Enter pass phrase for key.pem: ******
Private-Key: (2048 bit)
modulus:
    00:da:bf:f3:39:d7:c6:1f:bd:6f:a7:b8:aa:67:f2:
...
coefficient:
    6b:26:51:9e:fb:77:cf:7e:d4:2a:a6:d2:7f:21:fa:
    42:e4:7c:54:2e:5e:e9:fb:03:a6:25:d0:6a:fc:e9:
    e1:1b:45:82:61:c0:35:a9:50:25:0a:75:2a:f8:cc:
    87:10:30:9d:bd:36:8e:4b:f6:55:0d:08:30:e8:55:
    e4:00:3b:ec
```

④ CSR 생성

※ 해당하는 모든 입력은 영문자와 숫자만 허용합니다. 예시를 참조하세요.

```
Country Name (국가코드) : KR
State or Province Name (시/도) : Seoul
Locality Name (구/군) : GangNam
Organization Name (회사명) : KFTC
```

```
Organizational Unit Name (부서명) : Digital Certificate Center
Common Name (인증 받을 도메인 주소) : www.yessign.or.kr
```

```
$ openssl req -new -key key.pem -out csr.pem
Enter pass phrase for key.pem: ******
Private-Key: (2048 bit)
modulus:
    00:da:bf:f3:39:d7:c6:1f:bd:6f:a7:b8:aa:67:f2:
...
coefficient:
    6b:26:51:9e:fb:77:cf:7e:d4:2a:a6:d2:7f:21:fa:
    42:e4:7c:54:2e:5e:e9:fb:03:a6:25:d0:6a:fc:e9:
    e1:1b:45:82:61:c0:35:a9:50:25:0a:75:2a:f8:cc:
    87:10:30:9d:bd:36:8e:4b:f6:55:0d:08:30:e8:55:
    e4:00:3b:ec
```

⑤ yessign에 CSR 제출

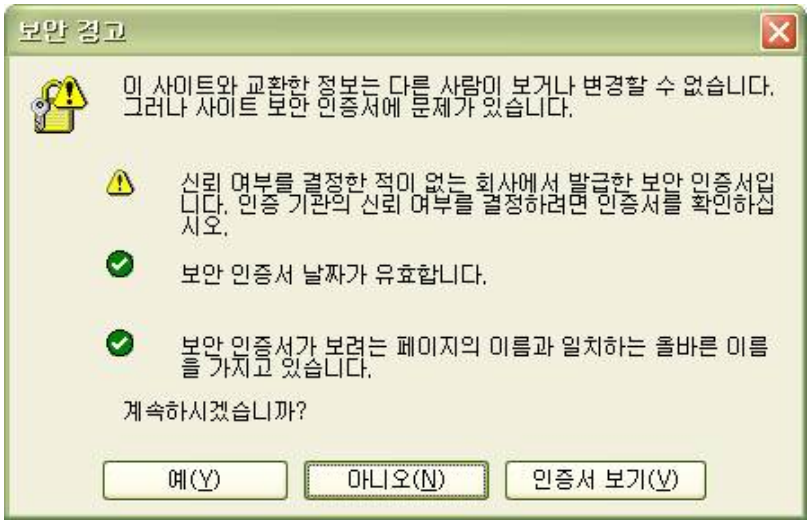
- 생성한 CSR 파일을 텍스트 편집기에서 열면 아래와 같은 형식의 내용으로 되어 있습니다.
- yessign SSL 홈페이지(https://www.yessign.or.kr/ssl/)에 접속하셔서 인증서 발급 요청을 하시고 CSR 입력부분에 해당 내용을 복사해서 붙여넣으셔서 사용하시면 됩니다.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBETCBvAIBADBXMQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0ZTEh
...
BrRh2nOTKgfMcT9h+1XxOwNRQ9/SIGV1y3+3abNiJmJBWnJ8Bg==
-----END CERTIFICATE REQUEST-----
```

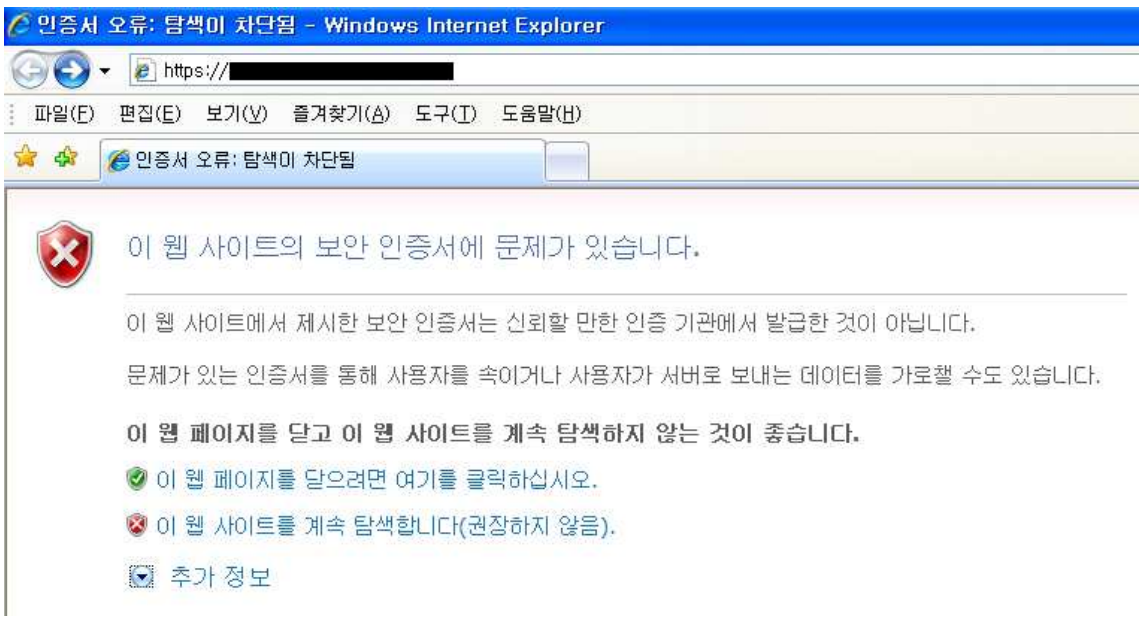
3. 보안서버 인증서 설치

※ SSL 웹서비스를 제공하기 위해서는 보안서버 인증서 설치시에 해당되는 체인인증서를 설치하여야 합니다. 아래 설치 안내에 따라서 "보안서버 인증서", "체인인증서"를 모두 웹서버에 설치해야 모든 종류의 웹브라우저에서 서비스를 문제없이 제공할 수 있습니다.

※ 보안서버 인증서 체인을 웹서버에 모두 설치하기 않으면, 웹브라우저에 따라서는 아래와 같이 보안경고창이 발생할 수 있습니다.



< Microsoft Internet Explorer 6.0 이하 버전의 경고창 >



< Microsoft Internet Explorer 7.0 버전의 경고 화면 >

가. 발급 인증서 확인하기

yessign SSL 홈페이지 관리자로부터 수신한 이메일의 첨부파일에는 다음과 같은 3종류의 인증서가 포함되어 있습니다.

- sslCERT.cer : 발급된 보안서버 인증서
- sslCA.cer : 보안서버 체인 인증서
- sslROOT.cer : 보안서버 루트 인증서

나. Apache 환경 설정하기

① 보안서버 인증서인 "sslCERT.cer" 파일과 "sslCA.cer" 파일을 FTP 등을 이용하여 웹서버에 업로드합니다.

② 환경설정 파일(httpd.conf 또는 ssl.conf)을 수정합니다.

※ 환경설정 파일에서 SSL 설정과 관련된 부분은 "[SSL Support]", "[SSL Global Context]", "[SSL Virtual Host Context]" 세부분입니다.

- [SSL Support] : SSL 지원에 대한 설정으로 기본 설정을 사용합니다.
- [SSL Global Context] : SSL 환경에 대한 설정으로 기본 설정을 사용합니다.
- [SSL Virtural Host Context] : SSL 인증서 설정 부분으로 아래 내용대로 설정합니다.

```
<VirtualHost _default_:443>
# General setup for the virtual host
DocumentRoot htdocs            ## 웹문서 루트 경로
ServerName www.test.co.kr      ## 인증받은 도메인 주소
ErrorLog logs/error_log        ## 에러로그 설정
TransferLog logs/access_log    ## 접속 로그 설정

SSLEngine on                   ## SSLEngine을 on으로 해야 동작

# Server Certificate:
SSLCertificateFile conf/ssl/sslCert.cer   ## SSL 서버인증서 파일

# Server Private Key:
SSLCertificateKeyFile conf/ssl/key.pem    ## SSL 서버인증서에 대한 개인키 파일

# Server Certificate Chain:
SSLCertificateChainFile conf/ssl/sslCA.cer ## SSL 서버인증서 발급자 인증서 파일
```

※ Apache 2.2.x 이상의 버전에서는 conf/extra/httpd-ssl.conf 파일에 위의 Virtual Host 정보를 작성하고, httpd.conf 파일에서 conf/extra/httpd-ssl.conf 파일을 include 하도록 설정합니다("Include conf/extra/httpd-ssl.conf" 주석 해제).

4. 보안 웹서버 가동

① 재설정한 환경파일이 적용되도록 Apache 서버를 재가동 합니다.

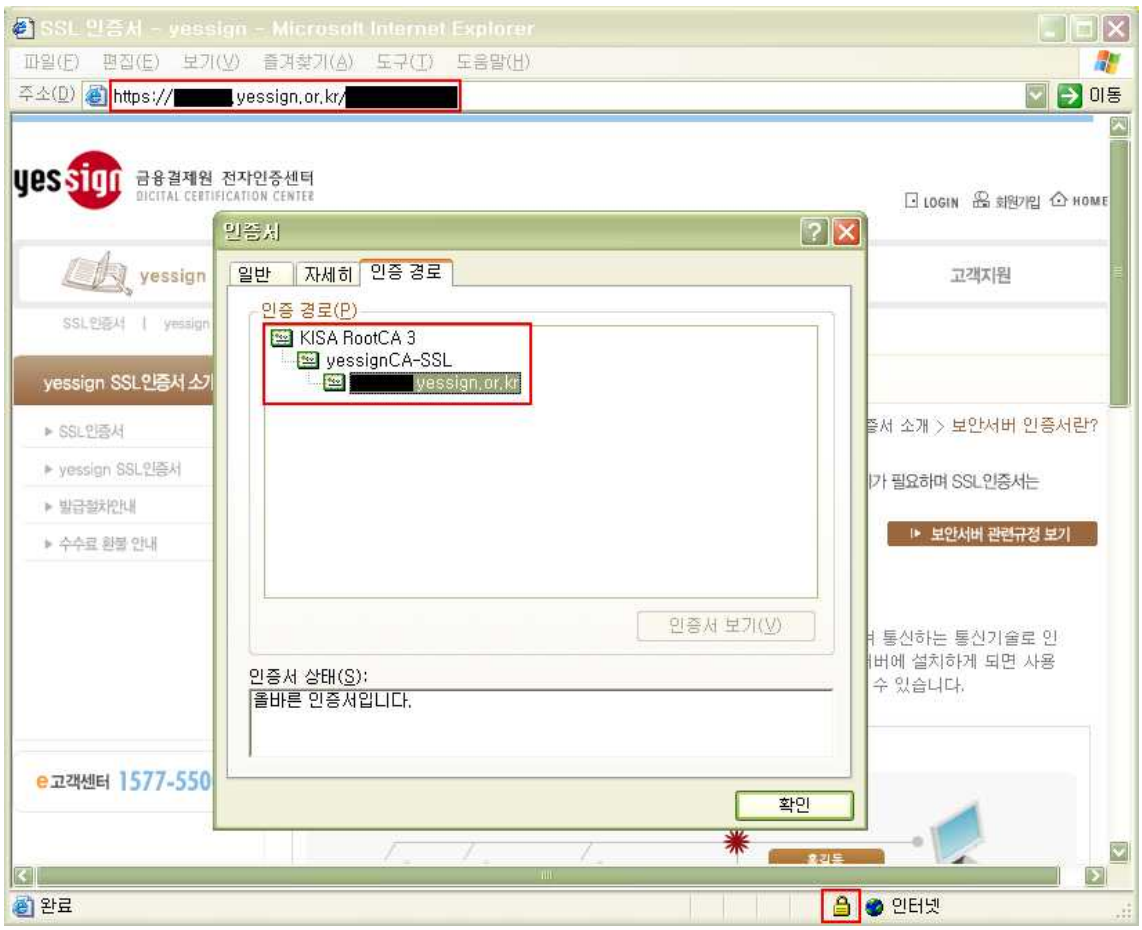
```
$ ./apachectl startssl
Apache/1.3.31 mod_ssl/2.8.19 (Pass Phrase Dialog)
Some of your private key files are encrypted for security reasons.
In order to read them you have to provide us with the pass phrases.

Server web:443 (RSA)
Enter pass phrase: [개인키 비밀번호 입력]

Ok: Pass Phrase Dialog successful.
$APACHE/bin/apachectl startssl: httpd started
```

※ Apache 2.2.x 이상의 버전에서는 위 명령어 대신 "./apachectl start"로 기동합니다(개인키 비밀번호 입력을 요구함을 확인).

② 웹브라우저로 웹서버를 "https://" 프로토콜로 접근하면 브라우저 하단에 노란 자물쇠 아이콘(Internet Explorer일 경우)이 표시되고 해당 아이콘을 더블 클릭하여 인증서의 경로가 완전하게 표시되는 것을 확인합니다.



5. 다른 서버에 SSL 인증서와 키 복사하기

① "3절"에서 설치한 인증서와 개인키 파일을 다른 아파치 서버에 복사합니다.

② "3절 나항"과 동일하게 SSL과 관련된 환경설정을 합니다.

③ "4절"의 과정대로 웹서버를 재가동하고 SSL 적용을 웹브라우저로 확인합니다.

6. 인증서 갱신하기

① "2절"의 내용을 참고하여 키 파일, CSR 파일을 생성합니다.

② 생성된 CSR을 yessign 홈페이지에 제출하고 SSL 인증서를 발급 받습니다.

③ 생성한 키 파일 및 발급받은 인증서 파일로 기존의 파일들을 대체하고 Apache 서버를 재기동합니다.

7. 다중 SSL 서버 설정

① Apache 웹서버는 Name-Based Virtual Host 기능을 지원합니다. 즉, 동일한 서버에서 동일한 IP, 동일한 Port로 둘 이상의 도메인을 서비스 할 수 있습니다.

```
Listen 80

NameVirtualHost 11.22.33.44

<VirtualHost 11.22.33.44>
ServerName www.domain1.com
...
</VirtualHost>

<VirtualHost 11.22.33.44>
ServerName www.domain2.com
...
</VirtualHost>
```

[일반적인 Virtual Host 설정 예시]

② 위와 같은 환경에서 SSL 서버를 추가하고자 할 경우 기존의 VirtualHost 설정에 모두 ":80"을 추가하고, SSL VirtualHost는 "_default_:443"으로 설정합니다.

```
Listen 80
Listen 443

NameVirtualHost 11.22.33.44:80

<VirtualHost 11.22.33.44:80>
ServerName www.domain1.com
...
</VirtualHost>

<VirtualHost 11.22.33.44:80>
ServerName www.domain2.com
...
</VirtualHost>

...

<VirtualHost _default_:443>
ServerName www.domain1.com:443
...
</VirtualHost>
```

[하나의 SSL서버를 포함한 Virtual Host 설정 예시]

③ Virtual Host 기능을 이용하여 둘 이상의 도메인에 SSL을 적용하고자 할 때는 443이 아닌 별도의 포트 번호를 설정해주고 실제 웹페이지를 호출할 때도 해당 포트 번호를 포함한 URL로 호출해야 합니다.
(예: https://www.domain2.com:444/)

```
Listen 80
Listen 443
Listen 444

NameVirtualHost 11.22.33.44:80

<VirtualHost 11.22.33.44:80>
ServerName www.domain1.com
...
</VirtualHost>

<VirtualHost 11.22.33.44:80>
ServerName www.domain2.com
...
</VirtualHost>

...

<VirtualHost _default_:443>
ServerName www.domain1.com:443
...
</VirtualHost>

<VirtualHost _default_:444>
ServerName www.domain2.com:444
...
</VirtualHost>
```

[여러 개의 SSL서버를 포함한 Virtual Host 설정 예시]

※ 443이 아닌 포트는 일반적으로 방화벽에 의해 차단되어 있을 가능성이 높습니다. Apache 기동 후 서버 외부에서 telnet 등의 방법으로 해당 포트가 열려 있는지 확인해야 합니다.

8. PKCS #12 파일 변환 방법

※ PKCS #12 파일(*.pfx) : 인증서와 개인키를 함께 저장한 파일. 타 기종 웹서버간의 SSL 인증서 복사를 위해 필요한 파일 형태.

가. PKCS #12 파일 추출

- OpenSSL 설치 : 파일 변환을 실행할 서버에 OpenSSL을 설치합니다.
  (참고 : http://www.openssl.org)
- OpenSSL이 설치된 환경에서 다음 명령어를 실행합니다.
  > **openssl pkcs12 -export -out [출력파일명] -inkey [키파일명] -in [인증서파일명]**
- 출력파일명 : 추출할 파일명 (예: ssl_cert.pfx)
- 키파일명 : 사용중인 개인키 파일명 (예: key.pem)
- 인증서파일명 : 사용중인 인증서 파일명 (예: sslCERT.cer)
- 예시
  > **openssl pkcs12 -export -out test.pfx -inkey key.pem -in sslCERT.cer**

나. PKCS #12 파일 설치

- OpenSSL이 설치된 환경에서 다음 명령어를 실행합니다.
  > **openssl pkcs12 -in [입력파일명] -out [임시파일명] -nodes**
- 입력파일명 : 입력할 파일명 (예: ssl_cert.pfx)
- 임시파일명 : 인증서와 키를 임시로 저장할 파일명 (예: test.pem)
- 예시
  > **openssl pkcs12 -in test.pfx -out test.pem -nodes**
- 생성된 임시파일에서 인증서와 개인키를 따로 잘라내어 파일로 저장합니다.
  • 개인키 : "-----BEGIN PRIVATE KEY----- ~ -----END PRIVATE KEY-----"