WebtoB Web Server SSL 설정 방법

- Ver 1.0 -

2008. 6

개정 이력

버전	개정일	개정 내용
Ver 1.0	2008년 6월	WebtoB Web Server SSL 설명서 최초작성

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

< 목 차 >

1. 개인키 및 CSR 생성 방법

① CA 명령어로 CertificateKeyFile(서버 암호키) 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
```

```
[root:/WebtoB] ./bin/CA -newreq
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
......++++++
...++++++
writing new private key to 'newreq.pem'
Enter PEM pass phrase: (개인키 비밀번호 설정)
Verifying - Enter PEM pass phrase: (비밀번호 재확인)
-----
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) [KR]:KR
State or Province Name (full name) []:Gangnam
Locality Name (eg, city) []:Seoul
Organization Name (eg, company) [Tmax Ltd]:KFTC
Organizational Unit Name (eg, section) []:Digital Certificate Center
Common Name (eg, YOUR name) []:www.yessign.or.kr
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Request (and private key) is in newreq.pem
```

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

② 개인키와 CSR 분리해서 저장

- 위의 과정에서 생성된 "newreq.pem"에는 개인키와 CSR 구문 2개가 포함되어

있습니다. 이 구문을 나누어서 개인키 부분은 "key.pem", CSR 부분은 "csr.txt" 파일로 구분하여 따로 저장합니다.

- "newreq.pem" 파일의 내용 예시입니다.

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,447AF17A17052543

MIICWwIBAAKBgQCRn2vwN9QfWyP+r27i29SFg3ErzX15T5GqRXc7/OLEKoJcfHDq
npIFpioaNyUbSbPtCwOfOOvU38Us8kGQWfrRF62WG69ZXcjewCWxOMQGkmfhhL9E
... ...
Z+zjmc/FF5JPp7IZXQJAILjbM2Rej66NAgK3TgpTfMs/5WshKan+P7MB9z7zEafp
9qPLOnW/QnsIX8iOnEIFsQf2Kiv/NhiqBUeXhArnCQ==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE REQUEST-----
MIIBqDCCARECAQAwaDEZMBcGA1UEAxMQd3d3LnRIc3QyNC5jby5rcjELMAkGA1UE
BhMCS1IxDjAMBgNVBAgTBXNIb3VsMRAwDgYDVQQHEwdrYW5nbmFtMQOwCwYDVQQK
... ...
u4q5RijXaYL3HAjtmrOuBsLW1QAu+5TYIP9TDyowK/Zf4cqQNjTFxhrrLda2jAT7
KvGrI4azQr8fJFy+yTy8yH8J3+B19SQjEaBrvR9T8YIcMe9nOUtnFw29IYQ=
-----END CERTIFICATE REQUEST-----
```

- "key.pem" 파일로 저장한 예시입니다.

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,447AF17A17052543

MIICWwIBAAKBgQCRn2vwN9QfWyP+r27i29SFg3ErzX15T5GqRXc7/OLEKoJcfHDq
npIFpioaNyUbSbPtCwOfOOvU38Us8kGQWfrRF62WG69ZXcjewCWxOMQGkmfhhL9E
... ...
Z+zjmc/FF5JPp7IZXQJAILjbM2Rej66NAgK3TgpTfMs/5WshKan+P7MB9z7zEafp
9qPLOnW/QnsIX8iOnEIFsQf2Kiv/NhiqBUeXhArnCQ==
-----END RSA PRIVATE KEY-----
```

- "csr.txt" 파일로 저장한 예시입니다.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqDCCARECAQAwaDEZMBcGA1UEAxMQd3d3LnRIc3QyNC5jby5rcjELMAkGA1UE
BhMCS1IxDjAMBgNVBAgTBXNIb3VsMRAwDgYDVQQHEwdrYW5nbmFtMQOwCwYDVQQK
... ...
u4q5RijXaYL3HAjtmrOuBsLW1QAu+5TYIP9TDyowK/Zf4cqQNjTFxhrrLda2jAT7
KvGrI4azQr8fJFy+yTy8yH8J3+B19SQjEaBrvR9T8YIcMe9nOUtnFw29IYQ=
-----END CERTIFICATE REQUEST-----
```

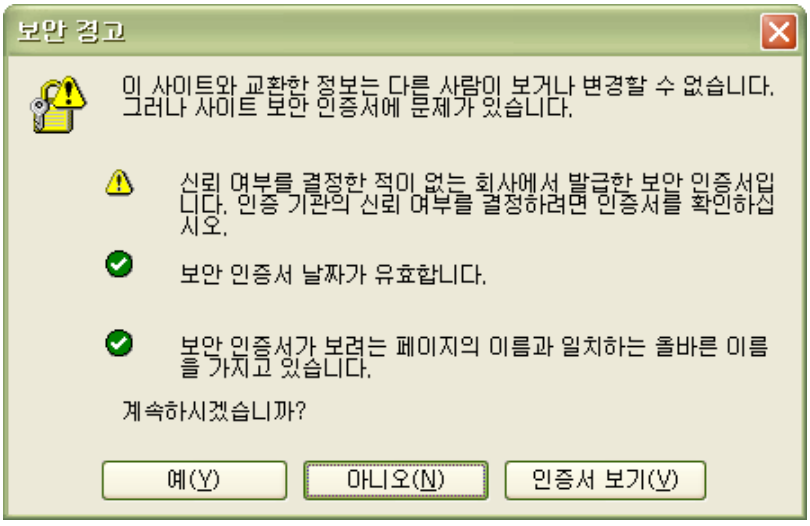
③ yessign에 CSR 제출

- yessign SSL 홈페이지(https://www.yessign.or.kr/ssl/)에 접속하셔서 인증서 발급요청을 하시고 CSR 입력부분에 "csr.txt" 파일의 내용을 붙여넣습니다.

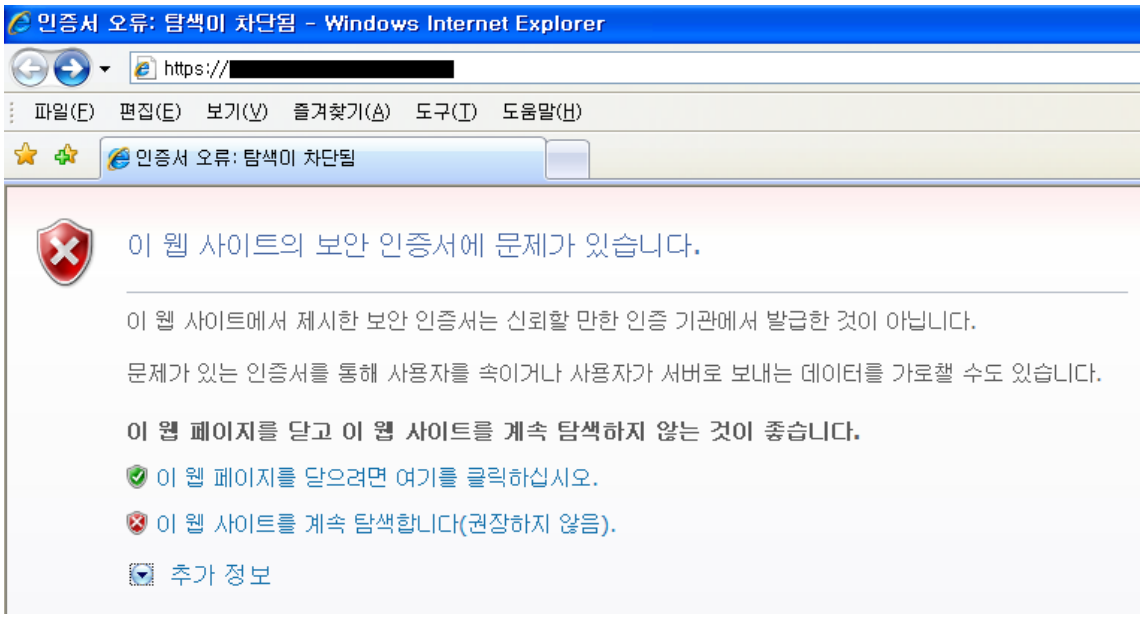
2. 보안서버 인증서 설치

※ SSL 웹서비스를 제공하기 위해서는 보안서버 인증서 설치시에 해당되는 체인 인증서를 설치하여야 합니다. 아래 설치 안내에 따라서 “보안서버 인증서”, “체인 인증서”를 모두 웹서버에 설치해야 모든 종류의 웹브라우저에서 서비스를 문제 없이 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. WebtoB 환경 설정하기

※ WebtoB는 환경 설정파일을 편집한 후에 컴파일 과정을 통해서 바이너리 환경 설정파일로 생성해서 웹서버를 재가동해야 적용되오니 아래 과정대로 진행해 주셔야 됩니다.

① WebtoB 설치디렉토리 밑에 “config" 디렉토리에서 기존에 존재하던 환경 설정 파일인 "http.m" 파일을 "http_ssl.m" 파일로 복사합니다.

② "http_ssl.m" 파일을 아래와 같이 수정합니다.

※ 443 포트로 SSL을 사용하는 "VHOST“를 생성합니다.

※ SSLNAME인 “yessignssl” 정의에서 인증서와 개인키 파일 경로를 설정합니다.

※ 빨간 구문 이외의 부분은 기존의 설정 내용을 그대로 사용합니다.

```
*DOMAIN
testWeb

*NODE
test    WEBTOBDIR="/usr/local/webtob",
        SHMKEY = 54000,
        DOCROOT="/usr/local/webtob/docs",
        HOSTNAME = "www.yessign.or.kr",
        PORT = "80",
        LOGGING = "log1",
        ERRORLOG = "log2",
        HTH = 1

*VHOST
yessignvhost    DOCROOT="/usr/local/webtob/docs",
        NODENAME= test,
        HOSTNAME = "www.yessign.or.kr",
        SSLNAME="yessignssl",
        PORT="443",
        SSLFLAG = Y

*SSL
yessignssl    CertificateFile = "/usr/local/webtob/ssl/sslCert.cer",
```

```
        CertificateKeyFile = "/usr/local/webtob/ssl/key.pem",
        CACertificateFile = "/usr/local/webtob/ssl/sslCA.cer"

*SVRGROUP
htmlg       NODENAME = test, SvrType = HTML
cgig        NODENAME = test, SVRTYPE = CGI
ssig        NODENAME = test, SVRTYPE = SSI

*SERVER
html        SVGNAME = htmlg, MinProc = 3, MaxProc = 10
cgi         SVGNAME = cgig, MinProc = 3, MaxProc = 10
ssi         SVGNAME = ssig, MinProc = 3, MaxProc =10

*URI
uri1        Uri = "/cgi-bin/", Svrtype = CGI

*ALIAS
alias1      URI = "/cgi-bin/",
        RealPath = "/usr/local/webtob/cgi-bin/"

*LOGGING
log1        Format = "DEFAULT",
        FileName = "/usr/local/webtob/log/access.log",
        Option = "sync"
log2        Format = "ERROR",
        FileName = "/usr/local/webtob/log/error.log",
        Option = "sync"

*EXT
htm         MimeType = "text/html", SvrType = HTML
```

③ 환경설정 파일인 "http_ssl.m" 파일을 컴파일 합니다.

```
[root:/WebtoB/config] ./bin/wscfl -i http_ssl.m -o sslconfig
        Current configuration:
                Number of client handler(HTH) = 1
                Supported maximum user per node = 975
                Supported maximum user per handler = 975
CFL is done successfully for node(test(test))
```

3. 보안 웹서버 가동

① 재설정한 환경파일이 적용되도록 WebtoB 서버를 재가동 합니다.

※ ssl 가동을 위한 환경설정은 “sslconfig"로 생성됩니다.

※ 비밀번호는 “1절”에서 “CertificateKeyFile(서버 암호키) 생성” 단계에서 입력한 비밀번호를 입력합니다.

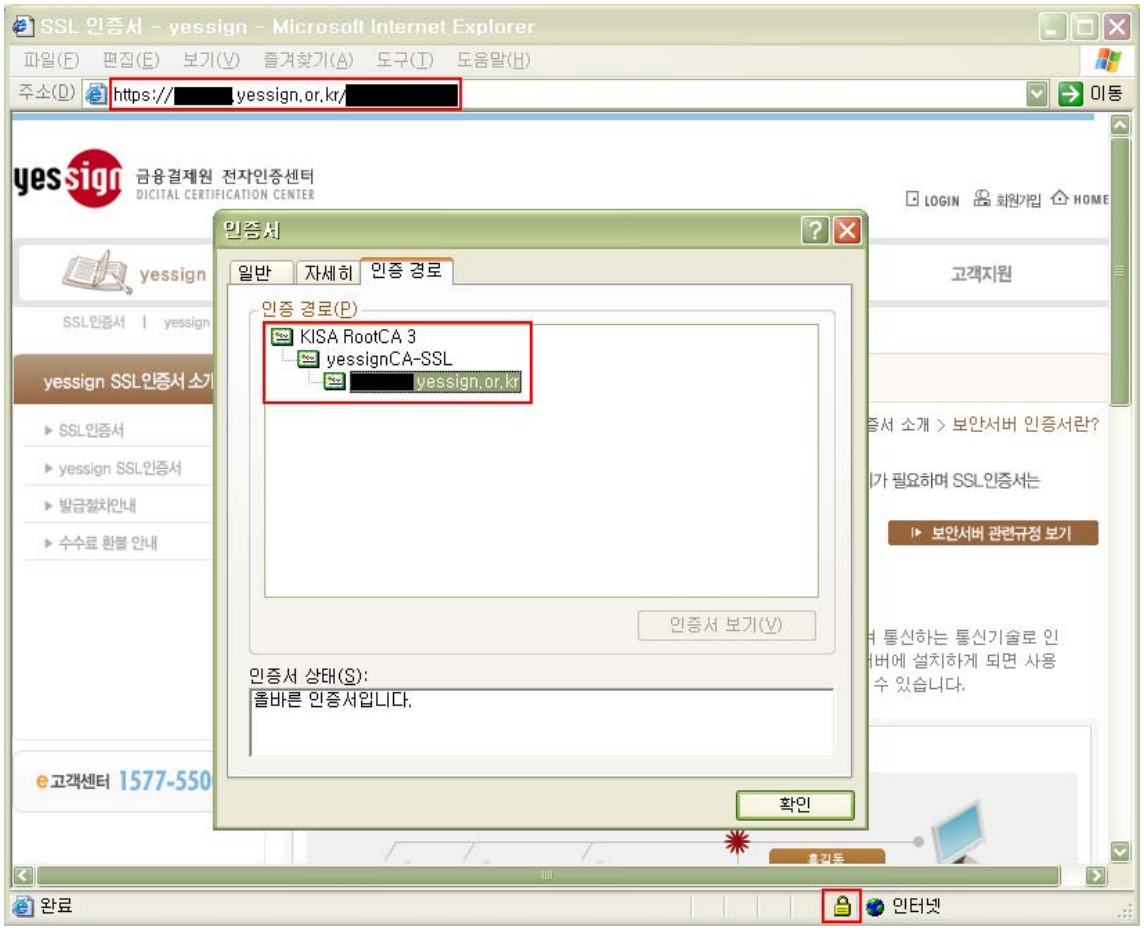
```
[root:/WebtoB] ./bin/wsboot -f sslconfig

WSBOOT for node(test) is starting:

Today: 2007/06/22
        WSBOOT: WSM is starting: 06/22/04 16:05:22
        WSBOOT: HTL is starting: 06/22/04 16:05:22
        WSBOOT: HTH is starting: 06/22/04 16:05:22
         Current WebtoB Configuration:
                Number of client handler(HTH) = 1
                Supported maximum user per node = 975
                Supported maximum user per handler = 975
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 www.yessign.or.kr:443 (RSA)
Enter pass phrase: ********
        WSBOOT: SVR(/usr/local/webtob/bin/htmls) is starting: 06/22/04 16:05:26
        WSBOOT: SVR(/usr/local/webtob/bin/htmls) is starting: 06/22/04 16:05:26
        WSBOOT: SVR(/usr/local/webtob/bin/htmls) is starting: 06/22/04 16:05:26
        WSBOOT: SVR(/usr/local/webtob/bin/cgis) is starting: 06/22/04 16:05:26
        WSBOOT: SVR(/usr/local/webtob/bin/cgis) is starting: 06/22/04 16:05:26
        WSBOOT: SVR(/usr/local/webtob/bin/cgis) is starting: 06/22/04 16:05:26
        WSBOOT: SVR(/usr/local/webtob/bin/ssis) is starting: 06/22/04 16:05:26
        WSBOOT: SVR(/usr/local/webtob/bin/ssis) is starting: 06/22/04 16:05:26
        WSBOOT: SVR(/usr/local/webtob/bin/ssis) is starting: 06/22/04 16:05:26
```

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.


SSL 인증서 - yessign - Microsoft Internet Explorer
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
주소(D) https://[redacted].yessign.or.kr/[redacted]
이동
yessign 금융결제원 전자인증센터 DICITAL CERTIFICATION CENTER
LOGIN 회원가입 HOME
고객지원
인증서
일반 자세히 인증 경로
인증 경로(P)
KISA RootCA 3
yessignCA-SSL
[redacted].yessign.or.kr
인증서 보기(V)
인증서 상태(S):
올바른 인증서입니다.
확인
yessign SSL인증서 소개
SSL인증서
yessign SSL인증서
발급절차안내
수수료 환불 안내
보안서버 관련규정 보기
e고객센터 1577-550
완료
인터넷

4. 다른 서버에 SSL 인증서와 키 복사하기

① “2. 보안서버 인증서 설치” 단계에서 사용한 서버 인증서(sslCert.cer), CA 인증서(sslCA.cer), 개인키(key.pem) 파일을 다른 웹서버에 복사합니다.

② “2. 보안서버 인증서 설치” 단계에서 설명한 대로 환경설정을 통하여 SSL 인증서 사용 환경을 설정합니다.

③ “3절”의 과정대로 웹서버를 재가동하고 SSL 적용을 웹브라우저로 확인합니다.