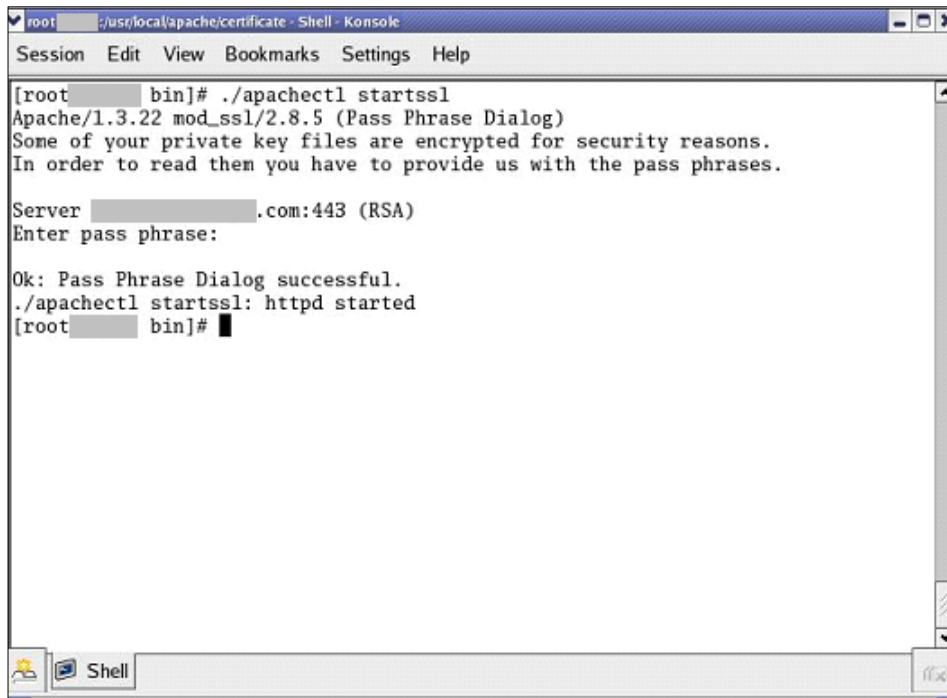


⑤ 웹 서버 재구동

- httpd.conf 파일에 오류가 없는지 확인
`/usr/local/apache/bin/apachectl -t`
 Syntax OK 라고 나오면 오류가 없습니다.
- 기존 아파치 서비스 중단
`/usr/local/apache/bin/apachectl stop`
- http, https 웹 서버를 구동
`/usr/local/apache/bin/apachectl start` 실행 후 인증서 개인키
 패스워드 입력하면 http(80), 과 https(443) 두 서비스가 실행



```

root@localhost:~# ./apachectl startssl
Apache/1.3.22 mod_ssl/2.8.5 (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 localhost.com:443 (RSA)
Enter pass phrase:

Ok: Pass Phrase Dialog successful.
./apachectl startssl: httpd started
root@localhost:~#
  
```

- ⑥ 이제 SSL 인증서의 설치가 완료되었습니다. VI장으로 이동하셔서 실제 웹페이지를 어떻게 수정해야 하는지 알아보겠습니다.

2.3 Web2B 서버에서 보안서버 구축하기

가. 개인키 생성 및 CSR 생성 방법

① CSR 정보 입력

Web2B 웹 서버의 홈 폴더 아래에 bin 폴더에 'CA' 명령어를 실행하여 CSR을 생성합니다.

```

ca C:\WINDOWS\system32\cmd.exe
C:\TmaxSoft\WebtoB4.1\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:
Verifying - Enter PEM pass phrase:
-----
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) []:Seoul
Locality Name (eg, city) []:Seoul
Organization Name (eg, company) [Tmax Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:.com
Email Address []:.com

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

C:\TmaxSoft\WebtoB4.1\bin>

```

※ Pass phrase : 개인키 비밀번호로 SSL 기동 때 확인

※ Common Name : 해당 웹 사이트의 도메인 명

② CSR 추출

```

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,885B4E9CEAF5B262

IMVvc0gj0XGFB7vS+7NhOVKjoC6iFaANiX1WkOpea49fp7cVKWIYEWYJ3Exf8zsB
4DEypbzv5ToHHuvOU5mbTdrSlqpBJWAlDL1AEiDYam60qSCdgCZcJYvC4y/SJgfc
ZittzyL+kNMKIRzeS4EDLEBLvcvP8kFmuT3f/LiVWYdDAzO7NVi6c1VPaNaCJ6nl
ztrAGvzwodzLCmvNynAvyDKDFu1k2zPwM1TkWkVRLcnWMq1qlmvelXJ/QuAy+XM1
KoKYWPmALryNH/4mEgpOCbZ/33d+sACKUhXpm/NFWPIZqDS/NoljYQstQiVM3vcK
/nx7qdCuGc7zugD0aYneotzeuxuqZs2eCdGAK8A4ldWjWHDL5da8AvZzy5qzE9p
RFuRwggjiUR7dcfYVvG8v9N/uF+yc+oGIEiXe1eoVmmuzeKULnkZwxHfzQIC1Ss1f
qyVo5GcTNA7ydNwhzhpl/8+ffmCz07MtoXjSMtnZj7hVe/WWhOREWdMDukwBcP
y3NDzsMHFLk5cVvRMeaTdcIkFY/scqGJ23y5MejgJ54FalWJe750MyLG3BYPPYZV
PNC/13ed4hJfoVfaoG0t/jkTB+YlbU9Vbbw8HymqV7i7+7U2Zr/F+7AHEXoGTTv
Dg90cb2LyOL7bt837FO809talydkcrhHa3KkMyP6/kuJDStj9KN54EoU+AoS9TsT
ge97ADlrKa/ASfv6gjT1md00FZEeqNgvLYIUDIXRctEtngPymDF6cA==
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE REQUEST-----
MIIByzCCATQCAQAwYoxCzAJBgNVBAYTAktSMQ4wDAYDVQQIEwVTZW91bDEOMAwG
A1UEBxMFU2VvdWwxDTALBgNVBAoTBEBtJQ0ExDDAKBgNVBAStA0IDQzEbMBkGA1UE
AxMSamNsZWJuc2lnbmdhdGUuY29IMSEwHwYJKoZIhvcNAQkBFhJqY2xlZUBzaWdu
Z2F0ZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANo9/NgLI/EpfOke
O3h8o+wZ0I3/Kah30HXvp+9STpqxpUJ3F8pg/vWKAIZZ1vTHPaTbBcNOPy0ZcmA
3CW2Uyd8Ad97QQYKvMw6jOPZXNGvAgMBAAGgADANBgkqhkiG9w0BAQQFAA0BgQAS
0AigImeRZKsPaDTHdRO3X14bvJSINkb8UCOSHJ5+A9L9lw1xZNOg6kfbLEgqc0IO
m2Agj0W1FbOyv5aGpkMFDhZketuQYK7XVT1155te/x3aZmw1NB0la2mhUI/a28M
JSHC5uBNGVCOoUOEtSEKUFti7a5Nt+2/4R/yo+z/SQ==
-----END CERTIFICATE REQUEST-----

```

생성된 `newreq.pem`에는 (암호화된) 개인 키와 CSR의 정보가 함께 포함되어 있습니다. CSR 정보는 다음과 같습니다.

```

-----BEGIN CERTIFICATE REQUEST-----
MIIByzCCATQCAQAwYoxCzAJBgNVBAYTAktSMQ4wDAYDVQQIEwVTZW91bDEOMAwG
A1UEBxMFU2VvdWwxDTALBgNVBAoTBEBtJQ0ExDDAKBgNVBAStA0IDQzEbMBkGA1UE
...
JSHC5uBNGVCOoUOEtSEKUFti7a5Nt+2/4R/yo+z/SQ==
-----END CERTIFICATE REQUEST-----

```

CSR 내용을 인증기관에게 메일로 송부하거나 인증서 신청화면에 붙여 넣으신 후 인증서 신청을 진행하시면 됩니다. 인증기관의 발급 절차에 따라서 인증서가 발급됩니다.

나. 인증서 설치 방법

① 메일로 받은 인증서를 저장합니다.

CSR 생성 과정에서 만들어진 `newreq.pem` 파일의 내용 중 위 부분의 개인 키와 인증기관에서 발급받은 `(domain_name).crt`의 내용을 합쳐서 `cert.pem`이란 새 이름으로 저장합니다.

```

1 -----BEGIN RSA PRIVATE KEY-----
2 Proc-Type: 4, ENCRYPTED
3 DEK-Info: DES-EDE3-CBC,885B4E9CEAF5B262
4
5 1MVVcOgJ0XGFB7vS+7NhOVKjoc6tFaAniX1WkOpea49fp7cVKWLYENYJ3Exf8zsB
6 4DEypbvz5ToHHuvOU5mbTdrSIqpBJWAIdL1AEiDYam6OqSCdgCzcJYvC4y/SJgfc
7 ZitczyL+kMMK1RzeS4EDLEBLvcvP8kFmuT3f/LIVWYdDAzO7NY16c1VPaNacJ6nI
8 ztFAGvzwodzLChvNynAvyDKDFu1k2zPWW1TkWkVRLcnWMq1qImve1XJ/QuAy+XM1
9 KoRYWmAlrYnH/4mEgpoCbZ/33d+sACKUHXpm/NFWPLZqDS/No1jYQsfQiVM3vcK
10 /nx7qdCuGc7zugDOaYneotzeuxuqZs2eCdGAK8A41dWjWHDL5da8fAvZzy5qzE9p
11 8JTq2vR1D/A1trcpzv1u8oqBnXXbXXJ4qAB4DEuh5o9B00hI3hLTEwIvu6UYiLbn
12 RFuRwGjiUR7dcfYVVG8v9N/uF+yc+oGIEiXe1eoVmmuzeKULnkZwxHfzQLC1Ss1f
13 qyVo5GCTNAd7ydNwhzhp1/8+ffmCz07MtOxJSMtnZj7hVe/WWhOREWdMOukwtBcP
14 y3NDzsMHFLk5cVvrMeaTdcIkFY/scqGJ23y5MejgJ54FaIwJe750MyLg3BYPPYZV
15 PNC/13ed4hJFoVfaoG0t/jkTB+YlB9Vbbw8HymqV717t+7U2Zr/F+7AHEXoGTTv
16 Dg90cb2LyOL7bt837FQ809talydkcrhHa3KkMyP6/kuJdStj9KN54Eou+aoS9TsT
17 ge97ADIrKa/ASftv6gjT1mdOOFZEQNgvLYiUD1XRctEtngPymDF6cA==
18 -----END RSA PRIVATE KEY-----
19 -----BEGIN CERTIFICATE-----
20 MIIEPjCCA46gAwIEAgIQRurwlgVMxeP6ZepunOLGZDANBgkqhkiG9w0BAQUFADBv
21 MQswCQYDVQQGEwJTRTEUMBIGA1UEChMLQWRkVHJ1c3QgQUlXJjAkBgNVBAsTHUFk
22 ZFRydXN0IEV4dGVybmFsIFRUUCBOZXR3b3JrMSIwIwIAVDVQDEx1B2GRUcnVzdCBF
23 eHRlcm5hbnB3b3B3b3B3b3B3b3B3b3B3b3B3b3B3b3B3b3B3b3B3b3B3b3B3b3B3
24 gZMxCzAJBgNVBAYTA1VTMQswCQYDVQQIEwJVVDExMDEwMDEwMDEwMDEwMDEwMDEw
25 IENpdHkxHjAcBgNVBAoTFVRlc3B3b3B3b3B3b3B3b3B3b3B3b3B3b3B3b3B3b3B3b3
26 aHR0cDovL3d3dy51c2VydHJ1c3QuY29tMRswCQYDVQQDEwJVVVE4gLSBEQVRRBQ29y
27 cCBTR0MwgwEiMAOGCSqGSIb3DQEBAQUAA4IBDwAwggEKAAoIBAQDf7lgQoituvCSO
28 vySGCefgCA8uK3oT1Bu99raAjmUFkwAevK/id44ZDRJH7Kyto/oucPjebvtWQhWe
29 L1zvI94huQV2JxkPT9bnLS+1B1j8qYRCutTSJy+8ik7FugaoEymyfQYWWjAcPJT
30 AMBEUIK1Vm82+UrgRIagTU7WR25JSstn16eEbbmOHvT8/83nNuCcBwyyMyIVOLTg
31 zBfAssD0/jI/KSqVe9jyp04PVHhDyCzCQPb/1zdXpo+vK68R4pqrnHKH7EquF9C
32 BQvsRjDRcgV6VZt9e/feLShurK1rgRMvKisaRWXve/rtIy/NEjUw9EoD1w6n3AY
33 MyB3xKkVAgMBAAgGjggEXMIIBEzAfBgNVHSMEGDAwggBStvZhg6NLQm9/reJ1TvA73g
34 JMtUGjAdBgNVHQ4EFgQUUzLRS89/+uDxoF2FTpLSnkUdtE8wDgYDVROPAQH/BAQD
35 AgEGMA8GA1UdEwEB/wQFMAMBaf8wIAVDVRO1BBkwFwYKKwYBBA6CnwoDAwYJYIZI
36 Ayb4QgQBMBEGA1UdIAQKMAgwBgYEVR0gADB7BgNVHR8EdDByMDIgaNqA0hjJodHRw
37 Oi8vY3JslmNvbW9kb2NhLmNvbS9BZGRUcnVzdEV4dGVybmFsQ0FSb290LmNybDA2
38 oDsgMoYwaHR0cDovL2Nybc5jb21vZG8ubmV0L0FkZFRydXNORXh0ZXJ1YXwDQVJv
39 b3QuY3JslmNvbS9BZGRUcnVzdEV4dGVybmFsQ0FSb290LmNybDA2
40 aUB/vxpxAAAnYv9QkSr/gk/8B2AvGD+x+R5ywXfd8FJ38wDOSHfVsg/RS4iJYdPx
41 Gz+noljAA/288Drk7cwSu8m5rnsEoARyv+neLdKnUWYAc9K9fqqeU5Z9abIYPo6t
42 V1B+99Ww/z11ZYKM11fDj/dg9sKNNIf8TOP1278cqvaGzebfET+NB/dtgxPAOIg5
43 YKF+MOHj1d6ku2NvL0mKaCzulnmsBGHhT04OnXJM9nk4yMdlaw+UD3S0vMjPVO25
44 dXGWDYoGC+vdOPAsfcYumEQOMcCte14smV13tqQCLZ3uFMAJctHynNf

```

② Config 설정

SSL은 443 포트를 사용하기 때문에 버추얼 호스트 노드를 하나를 추가해야 합니다. 아래는 SSL을 적용시킨 config 파일 예입니다.

```

+DOMAIN
webtoB4.1

+NODE
IISTest      WEBTOBDIR="C:/TmaxSoft/WebtoB4.1",
              SHMKEY = 54000,
              DOCROOT="C:/TmaxSoft/WebtoB4.1/docs",
              PORT = "80,443",
              HTH = 1,
              NODENAME = "${(NODENAME)",
              LOGGING = "log1",
              ERRORLOG = "log2"

+VHOST
ssl1
              NODENAME = "IISTest",
              HostName="IITest.signgate.com",
              DOCROOT="C:/TmaxSoft/WebtoB4.1/docs",
              PORT="443",
              SSLFLAG=Y,
              SSLName=ssl1

+SVRGROUP
htmlg      NODENAME = "IISTest", SVRTYPE = HTML
cgig      NODENAME = "IISTest", SVRTYPE = CGI
ssig      NODENAME = "IISTest", SVRTYPE = SSI

+SERVER
html      SVGNAME = htmlg, MinProc = 2, MaxProc = 10
cgi      SVGNAME = cgig, MinProc = 4, MaxProc = 10
ssi      SVGNAME = ssig, MinProc = 2, MaxProc = 10
    
```

```

+SVRGROUP
htmlg      NODENAME = "IISTest", SVRTYPE = HTML
cgig      NODENAME = "IISTest", SVRTYPE = CGI
ssig      NODENAME = "IISTest", SVRTYPE = SSI

+SERVER
html      SVGNAME = htmlg, MinProc = 2, MaxProc = 10
cgi      SVGNAME = cgig, MinProc = 4, MaxProc = 10
ssi      SVGNAME = ssig, MinProc = 2, MaxProc = 10

+URI
url1      Uri = "/cgi-bin/", Svrtype = CGI

+ALIAS
alias1    URI = "/cgi-bin/", RealPath = "C:/TmaxSoft/WebtoB4.1/cgi-bin/"

+LOGGING
log1      Format = "DEFAULT", FileName = "C:/TmaxSoft/WebtoB4.1/log/access.log",
              Option = "sync"
log2      Format = "ERROR", FileName = "C:/TmaxSoft/WebtoB4.1/log/error.log",
              Option = "sync"

+SSL
ssl1      CertificateFile="C:\TmaxSoft\WebtoB4.1\ssl\cert.pem",
              CertificateKeyFile="C:\TmaxSoft\WebtoB4.1\ssl\cert.pem"
              #CaCertificateFile="C:/Documents and Settings/Administrator/바탕 화면/IITestL.../rootca.

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

※ 붉은 색 네모 부분을 추가해 주셔야 하며, 주석 처리되어 있는 CaCertificateFile 부분(#)은 생략 가능합니다.

③ Config 컴파일

수정된 sample.m파일을 웹 서버에서 사용할 수 있도록 wscfl 명령어를 사용하여 컴파일 하는 과정이 필요합니다.

예) wscfl -i sample.m

```

C:\WINDOWS\system32\cmd.exe
C:\TmaxSoft\WebtoB4.1\config>dir
C 드라이브의 볼륨에는 이름이 없습니다.
볼륨 일련 번호: 1C93-4E22

C:\TmaxSoft\WebtoB4.1\config 디렉터리

2007-02-12 오후 03:10 <DIR>          .
2007-02-12 오후 03:10 <DIR>          ..
2006-11-17 오후 02:47                42,288 manual.m
2007-02-12 오후 03:14                1,325 sample.m
2007-02-12 오후 03:15               85,301 wsconfig
2006-11-30 오전 10:20               85,388 wsconfig_ori
                4개 파일                214,302 바이트
                2개 디렉터리       223,637,504 바이트 남음

C:\TmaxSoft\WebtoB4.1\config>wscfl -i sample.m
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<IISTest<IISTest>>

C:\TmaxSoft\WebtoB4.1\config>

```

④ 웹 서버 구동

Wsboot 명령어를 사용하여 서버를 구동하고, 인증서 생성과정에서 입력해주셨던 개인키 비밀번호를 입력하시면 됩니다.

```

C:\WINDOWS\system32\cmd.exe - wsboot
C:\TmaxSoft\WebtoB4.1\bin>wsboot

WSBOOT for node<IISTest> is starting:
Welcome to WebtoB demo system: it will expire 2007/02/15
Today: 2007/02/12
WSBOOT: WSM is starting: 02/12/07 15:18:53
WSBOOT: HTL is starting: 02/12/07 15:18:53
WSBOOT: HTH is starting: 02/12/07 15:18:53
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 IISTest.signgate.com:443 <RSA>
Enter pass phrase:

```

⑤ 이제 SSL 인증서의 설치가 완료되었습니다. VI장으로 이동하셔서 실제 웹페이지를 어떻게 수정해야 하는지 알아보겠습니다.