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

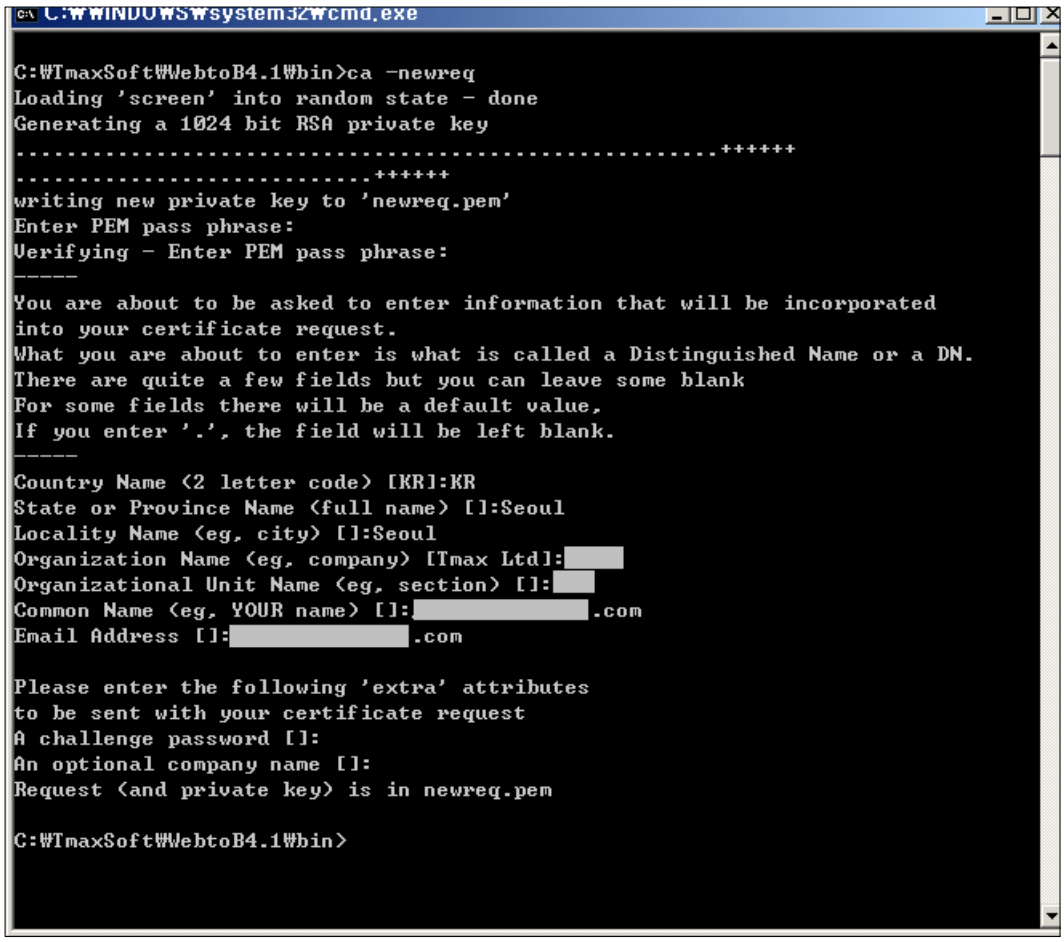
⑥ 이제 SSL 인증서의 설치가 완료되었습니다. VI장으로 이동하셔서 실제 웹페이지를 어떻게 수정해야 하는지 알아보겠습니다.

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.



※ 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+7NhOVKjoC6tFaANiX1WkOpea49fp7cVKWIYEWYJ3Exf8zsB
4DEypbzv5ToHHuvOU5mbTdrSlqpBJWAldL1AEiDYam60qSCdgCZcJYvC4y/SJgfc
ZittzyL+kNMKIRzeS4EDLEBLvcvP8kFmuT3f/LIVWYdDAzO7NYi6c1VPaNacJ6nI
ztrAGvzwodzLCmvNynAvyDKDFu1k2zPWM1TkwKVRLcnWMq1qImvelXJ/QuAy+XM1
KoKYWPmALryNH/4mEgpOCbZ/33d+sACKUhXpm/NFWPIZqDS/NoljYQsfQiVM3vcK
/nx7qdCuGc7zugD0aYneotzeuxuqZs2eCdGAK8A4ldWjWHDL5da8fAvZzy5qzE9p

RFuRwgjiUR7dcfYVVg8v9N/uF+yc+oGlEiXe1eoVmmuzeKULnkZwxHfzQIC1Ss1f
qyVo5GCTNAd7ydNwhzhpl/8+ffmCz07MtoXjSMtnZj7hVe/WWhOREWdM0ukwtBcP
y3NDzsMHFLk5cVVrMeaTdclkFY/scqGJ23y5MejgJ54FalWJe750MyLG3BYPPYZV
PNC/l3ed4hJFoVfaoG0t/jkTB+YLbU9Vbbw8HymqV7l7t+7U2Zr/F+7AHEXoGTTv
Dg90cb2LyOL7bt837FQ8O9talydkcrhHa3KkMyP6/kuJDStj9KN54EoU+AoS9TsT
ge97ADlrKa/ASftv6gjT1mdO0FZEqNgvLYiUD1XRCtEtngPymDF6cA==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE REQUEST-----
MIIByzCCATQCAQAwgYoxCzAJBgNVBAYTAktSMQ4wDAYDVQQIEwVTZW91bDEOMAwG
A1UEBxMFU2VvdWwxDTALBgNVBAoTBEtJQ0ExDDAKBgNVBAsTA0lDQzEbMBkGA1UE
AxMSamNsZWUuc2lnbmdhdGUuY29tMSEwHwYJKoZIhvcNAQkBFhJqY2xlZUBzaWdu
Z2F0ZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANo9/NgLI/EpfOke
O3h8o+wZ0I3/Kah30HXVp+9STpqxptJI3F8pg/vWKAI2Z1vTHPaTbBcNOPy0ZcmA

3CW2Uyd8Ad97QQYKVmW6jOPZXNGvAgMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQAS
0AlgjMeRZKsPaDTHdRO3Xf4bvUSfNkb8UCQSHJ5+A9L9Iw1xZNQg6kfbLEgqc0f0
m2Agj0W1FbOyv5aGpkMFDAhZketuQYK7XVTt155te/x3aZmw1NB0la2mhUl/a28M
JSHC5uBNGVCOoUOEtSEkUfTi7a5Nt+2/4R/dy+z/SQ==
-----END CERTIFICATE REQUEST-----
```

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIIByzCCATQCAQAwgYoxCzAJBgNVBAYTAktSMQ4wDAYDVQQIEwVTZW91bDEOMAwG
A1UEBxMFU2VvdWwxDTALBgNVBAoTBEtJQ0ExDDAKBgNVBAsTA0lDQzEbMBkGA1UE
...
JSHC5uBNGVCOoUOEtSEkUfTi7a5Nt+2/4R/요+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).crt의 내용을 합쳐서 cert.pem이란 새 이름으로 저장합니다.

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

lMVVcOgjOXGFB7vS+7NhOVKjoC6tFaANiX1WkOpea49fp7cVKWlYEWYJ3Exf8zsB
4DEypbzv5ToHHuvOU5mbTdrSIqpBJWAIdL1AEiDYam6OqSCdgCZcJYvC4y/SJgfc
ZittzyL+kNMKlRzeS4EDLEBLvcvP8kFmuT3f/LIVWYdDAzO7NYi6c1VPaNacJ6nI
ztrAGvzwodzLCmvNynAvyDKDFu1k2zPWM1TkwKVRLcnWMq1qImvelXJ/QuAy+XM1
KoKYWPmALryNH/4mEgpOCbZ/33d+sACKUhXpm/NFWPlZqDS/NoljYQsfQiVM3vcK
/nx7qdCuGc7zugDOaYneotzeuxuqZs2eCdGAK8A4ldWjWHDL5da8fAvZzy5qzE9p
8JTq2vR1D/A1trcpzv1u8oqBnXXbXXJ4qAB4DEuh5o9BOOhI3hLTEwIvu6UYiLBn
RFuRwgjiUR7dcfYVVg8v9N/uF+yc+oGIEiXe1eoVmmuzeKULnkZwxHfzQlC1Ss1f
qyVo5GCTNAd7ydNwhzhpl/8+ffmCzO7MtoXjSMtnZj7hVe/WWhOREWdMOukwtBcP
y3NDzsMHFLk5cVVrMeaTdcIkFY/scqGJ23y5MejgJ54FaIWJe75OMyLG3BYPPYZV
PNC/l3ed4hJFoVfaoGOt/jkTB+YLbU9Vbbw8HymqV7l7t+7U2Zr/F+7AHEXoGTTv
Dg9Ocb2LyOL7bt837FQ8O9talydkcrhHa3KkMyP6/kuJDStj9KN54EoU+AoS9TsT
ge97ADIrKa/ASftv6gjTimdOOFZEqNgvLYiUD1XRCtEtngPymDF6cA==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIEpjCCA46gAwIBAgIQRurwlgVMxeP6ZepunOLGZDANBgkqhkiG9w0BAQUFADBv
MQswCQYDVQQGEwJTRTEUMBIGA1UEChMLQWRkVHJ1c3QgQUIxJjAkBgNVBAsTHUFk
ZFRydXNOIEV4dGVybmFsIFRUUCBOZXR3b3JrMSIwIAYDVQQDExlBZGRUcnVzdCBF
eHRlcm5hbCBDQSBSb290MB4XDTA1MDYwNzA4MDkxMFoXDTIwMDUzMDEwNDgzOFow
gZMxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJVVDEXMBUGA1UEBxMOU2FsdCBMYWtl
IENpdHkxHjAcBgNVBAoTFVRoZSBVUOVSVFJVU1QgTmVOd29yazEhMB8GA1UECxMY
aHROcDovL3d3dy51c2VydHJ1c3QuY29tMRswGQYDVQQDExJVVE4gLSBEQVRBQ29y
cCBTROMwggEiMAOGCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDf7lgQoituVcSO
vy5GCefgCA8uK3oTlBu99raAjmUFkwAevK/iD44ZDRJH7Kyto/oucPjebvtWQhWe
LlzvI94huQV2JxkPT9bDnLS+lBlj8qYRCutTSJy+8ik7FugaoEymyfQYWWjAcPJT
AMBeUIKlVm82+UrgRIagTU7WR25JSstn16bEBbmOHvT8/83nNuCcBWyyMyIVOLTg
zBfAssDO/jI/KSqVe9jypO4PVHyhDYCzCQPB/1zdXpo+vK68R4pqrnHKH7EquF9C
BQvsRjDRcgvK6VZt9e/feL5hurKlrgRMvKisaRWXve/rtIy/NfjUw9EoDlw6n3AY
MyB3xKKvAgMBAAGjggEXMIIBEzAfBgNVHSMEGDAWgBStvZh6NLQm9/rEJlTvA73g
JMtUGjAdBgNVHQ4EFgQUUzLRs89/+uDxoF2FTpLSnkUdtE8wDgYDVROPAQH/BAQD
AgEGMA8GA1UdEwEB/wQFMAMBAf8wIAYDVROlBBkwFwYKKwYBBAGCNwoDAwYJYIZI
AYb4QgQBMBEGA1UdIAQKMAgwBgYEVROgADB7BgNVHR8EdDByMDigNqA0hjJodHRw
Oi8vY3JsLmNvbW9kb2NhLmNvbS9BZGRUcnVzdEV4dGVybmFsQOFSb29OLmNybDA2
oDSgMoYwaHROcDovL2NybC5jb21vZG8ubmVOLOFkZFRydXNORXhOZXJuYWxDQVJv
b3QuY3JsMAOGCSqGSIb3DQEBBQUAA4IBAQBjhpIQsRP6N76OKrYbikP1XK4OFN/3
aUB/vxpxAAnYv9QkSr/gk/8B2AvGD+x+R5ywXfd8FJ38wDOShFvSg/RS4iJYdPxD
Gz+no1jaA/288Drk7cwSu8m5rnsEoARyv+neLdKnUWYAc9K9fqqeU5Z9abIYPo6t
VlB+99Ww/zliZYKMllfDj/dg9sKNNIf8TOPl278cqvaGzebfET+NB/dtgxPAOIg5
YKF+MOHjiD6ku2NvLOmKaCzulmmsBGHhTO4OnXJM9nk4yMdIaW+UD3SOvMjPVO25
dXGWDYoGC+vdOPA8fcYumEZqOMcCtci4smV13tqQCLZ3uFMAJctHynNf
```

② Config 설정

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

```
*DOMAIN
webtob1

*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
```

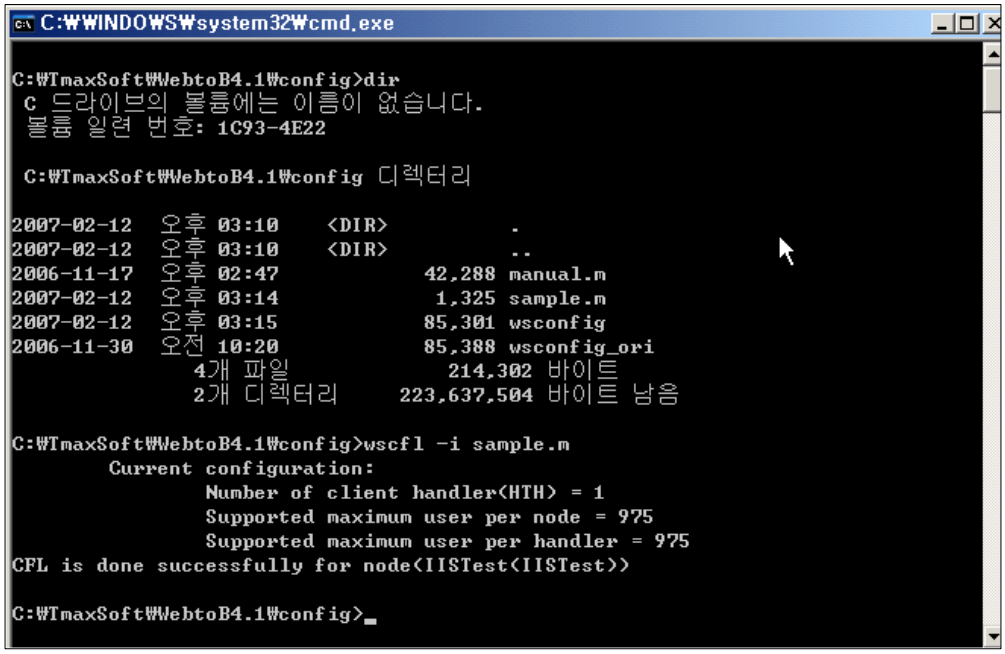
```
*SVRGROUP
htmlg           NODENAME = "IISTest", SVRTYPE = HTML
cgig            NODENAME = "IISTest", SVRTYPE = CGI
ssig            NODENAME = "IISTest", SVRTYPE = SSI

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

*URI
uri1            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/IITest_[redacted]/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

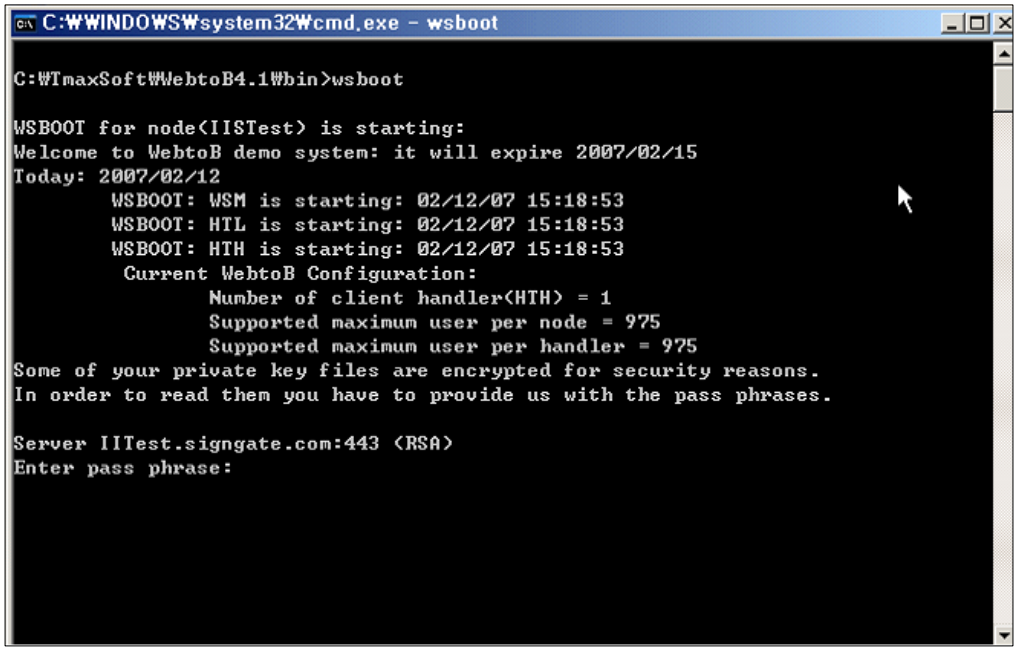
수정된 sample.m파일을 웹 서버에서 사용할 수 있도록 wscfl 명령어를 사용하여 컴파일 하는 과정이 필요합니다.

예) wscfl -i sample.m



④ 웹 서버 구동

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



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