■ 초기 설정

WebtoB Web Server 에서 인증서를 사용하기 위해 CSR 을 생성하는 방법입니다.

1. **초기 설정**

- CSR 을 생성하기 전에 다음의 몇 가지 사항을 필히 확인합니다.
부팅 후 Path 나 환경변수를 일일이 설정하지 않게 초기 설정파일을 사용하여 로그인 시 자동으로 실
행되도록 하고 있습니다. 그러나 간혹 초기 설정파일이 실행되지 않아서 에러가 생기는 경우가 있는
데 이럴 경우에 초기 설정파일을 다시 한번 실행 시켜야 합니다.

Linux 의 경우
bash 쉘 : .bash_profile
c 쉘 : .cshrc 등을 주로 사용합니다.
User 가 임의로 .bash_profile 을 실행시켜주면 되는데
리눅스의 경우
.bash_profile 혹은 . /root/.bash_profile 로 실행시켜 주면 됩니다.
(주의 : 실행을 의미하는 . 다음에 한 칸을 필히 띄워야 함.)

2. **비밀키 및 CSR 생성**

① 보통 path/ssl 에서 CSR 을 생성합니다.

$ CA -newreq
(newreq 라는 Commend 는 CSR 을 생성하는 option 입니다.) 이를 실행시키면
Generating a 1024 bit RSA Private key 라는 메시지라 나옵니다.

② 암호 입력
ex) **Enter PEM pass phase :**
verifying password - Enter PEM pass phase :
Private key 가 생성.

▶ 암호문을 잊어버리면 키를 사용할 수 없으므로 주의합니다.
▶ Private key 는 백업 복사본을 만들어 안전한 장소에 보관하여 비밀키가 손실
또는 분실되었을 경우 백업을 가지고 사용합니다.

■ CSR 생성

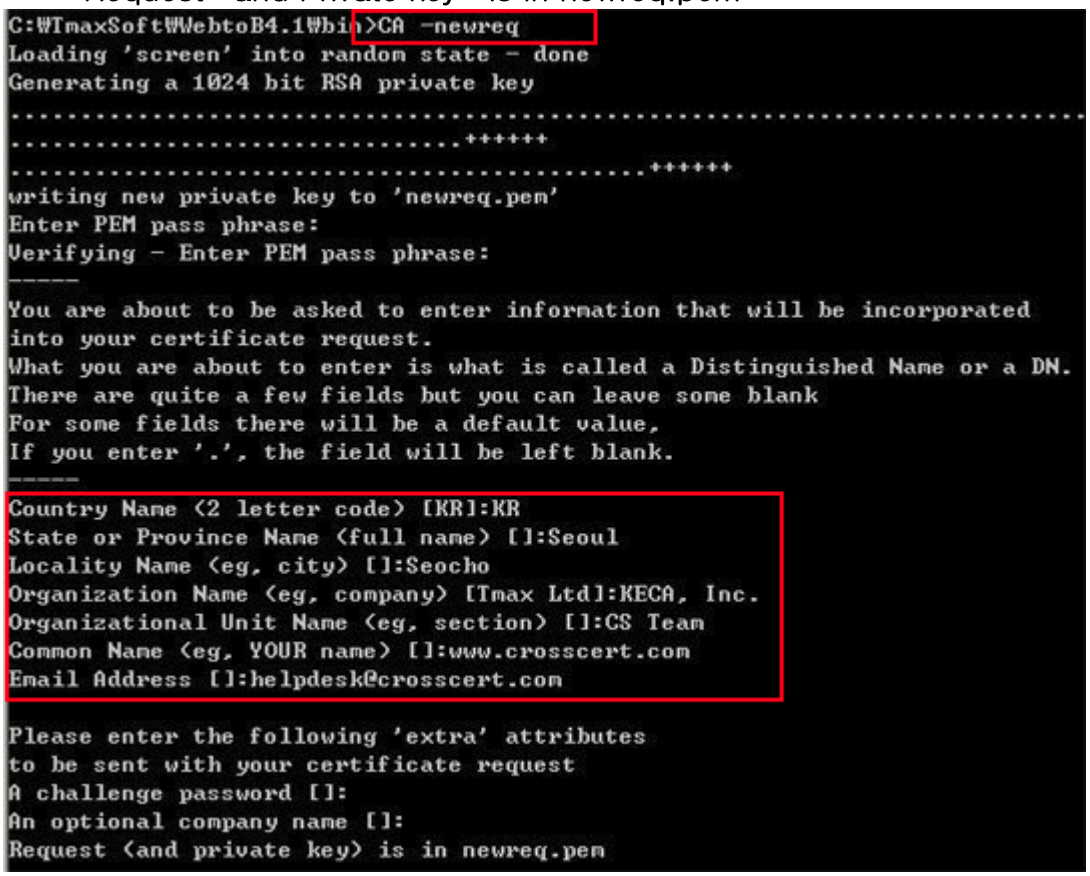
3. CSR 정보입력

- CSR 정보입력

다음 정보를 입력하라는 메시지가 나타납니다.

· Country Name <2 letter code> [AU] : KR
· States or province Name <full name> : Seoul
· Locality Name <eg. city> [] : Seocho
· Organization Name <eg. company> : KECA, Inc.
· Organization Unit Name <eg. section> : CS Team
· Common Name <eg. www.crosscert.com> :
www.crosscert.com
· Email Address [] : helpdesk@crosscert.com

"추가 속성"을 입력하라는 메시지가 나타나면 skip 하셔도 무관합니다.
ex) A challenge password [] :
An optional company name [] :
Request <and Private key> is in newreq.pem



■ 인증서 확인

4. CSR 제출

위의 단계가 성공적으로 이뤄지면 CSR 파일이 생성됩니다.
(메모장이나 워드패드를 사용하여 newreq.pem 파일을 불러옵니다.

- newreq.pem 의 내용중 CSR 값은 아래와 같은 형식으로 나타납니다.

위 CSR 의 내용(-----BEGIN CERTIFICATE REQUEST 및 END CERTIFICATE REQUEST-----행포함)을 복사하여
한국전자인증(www.crosscert.com) 인증서 신청 4 단계 CSR 보내기 폼에 붙여 넣습니다.

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

■ 인증서 저장

- **직접 신청**시 다음과 같은 과정을 통해 인증서 설치를 합니다.
(신청대행시 다음의 1,2 번 과정을 한국전자인증에서 대행해 드립니다.)

1. **직접 신청**시 다음과 같은 과정을 통해 인증서를 설치합니다.

해당 디지털 ID 가 승인되면 E-mail 로 해당 기술 또는 서비스 담당자에게 송신됩니다. 서버 ID 는 예
를 들면 다음과 같이 나타납니다.

```
-----BEGIN CERTIFICATE-----
JIEBSDSCEXoCHQEwLQMJSoZILvoNVQECSQAwcSETMRkOAMUTBhMuVrMmIoAnBdNVBAoTF1J
TQSBEYXRhIFNtY3VyaXR5LCBJbmMuMRwwGgYDVQQLExNQZXJzb25hIENlcnRpZmljYXRlMSQwIg
YDVQQDExtPcGVuIE1hcmtldCBUZXN0IFNlcnZlciAxMTAwHhcNOTUwNzE5MjAyNzMwWhcNOTYw
NTE0MjAyOTEwWjBzMQswCQYDVQQGEwJVUzEgMB4GA1UEChMXUlNBIERhdGEgU2VjdXJpdHks
IEluYy4xHDAaBgNVBAsTE1BlcnNvbmEgQ2VydGlmaWNhdGUxJDAiBgNVBAMTG09wZW4gTWFya
2V0IFRlc3QgU2VydmVyIDExMDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDU/7lrgR6vkVNX40B
Aq1poGdSmGkD1iN3sEPfSTGxNJXY58XH3JoZ4nrF7mIfvpghNi1taYimvhbBPNqYe4yLPAgMBAAEw
DQYJKoZIhvcNAQECBQADQQBqyCpws9EaAjKKAefuNP+z+8NY8khckgyHN2LLpfhv+iP8m+bF66
HNDUlFz8ZrVOu3WQapgLPV90kIskNKXX3a
------END CERTIFICATE-----
```

■ 인증서 설치

2. **인증서 저장**

-----BEGIN CERTIFICATE ~ 에서 ~ END CERTIFICATE----- 까지 모든 문자를 복사하여 **newreq.pem** 파일 안에 CSR 위에 Overwriting 하여 넣습니다.

위의 과정을 실행하면서 동시에 CSR 은 삭제하고, 비밀키와 인증서가 **newreq.pem** 파일에 존재하게 됩니다. EX> newreq.pem 파일 안에서 -----BEGIN RSA PRIVATE KEY----- 에서 -----END RSA PRIVATE KEY----- 부분은 그대로 두고, 그 **아래에 생성되었던 CSR 을 이메일을 통해 받은 인증서의 내용과 변경**합니다. (아래의 스냅샷 참조)

Ex)
< CSR 의 내용을 포함한 newreq.pem >

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,D09340D1575A72FD

Getay3V7lVgK9ZNUd282AqaIhBnrrcTpAUoXyYb46Qrl+jfxYkObS+juLWf/Kwgf
DzBdlR6qu6ksYOE+/rqz9bWbgasTpyqnqJyrhDOv5tJSy9TQYNSxilREEdirM/8s
+x9lAtDWRTLOAkavF7TKeb5D4wMC3eEpDO5+4bNMgMpHPxns7P/zMOytTliJC4r6
25QWAz+jyu8FugFVaRSNiFHlsLCXxZxjVfONuegtftZpcaITmmX4qRql8qtydn+2
74FU4QfiWQEkV4IYOVnl4VahF/hCOZBtcOeaulX9feZTaLEjMDl+fM3G5ihVAXUL
6CxJ6J8gdW8SOiChDDEIvfe/QSmFlcRAPlTedO5lWh804akCElcOC7IGPk+Anp7D
d9iIPbAxiIBMqAb52/ZXkKJ4M+jkz5SZEARblEEwszpKTSgYejYDkvVB+FLde0d7
7llPaOCQlf9onhqm9OARLdqQSQlTDXLqQPgUlZPhPSBE6JGZwqtMzvNlrUXum270
HO7jYnvxtO9lzn4dViHQwR8pAHedKhixquXsjp8MO3TxOdgOWgypfKXVItHJhQP9
lvjTJZotEmspUTyqQAAIHml7PWZ7i5dH9mKfM3P6Ou35/gon5cwr+lYjsijXG7j2
Cat2ePfbU3kukwmxcqaIz2oDQIhUVoKoSlwvYI8cfnFo7zhehCsOnMIXcSJ6vpyt
goXXsHGVC9GKclWYB9L9WPIraUSk8B5WCJryFdYqlEPrGT8N6KSPD85R5Ulx9okv
KP+QguuxdO8tJmqzrkaclybv9PJiqcZ3hYSyjTm4N7myDd5eT+pu9Q==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE REQUEST-----
MIIBODCCATkCAQAwgY8xCzAJBgNVBAYTAktSMQ4wDAYDVQQIEwVTZW9lbDEUMBIG
AlUEBxMLU29nb25nLWRvbmcxCzAJBgNVBAoTAklDMQ4wDAYDVQQLEwVTRURFWDEY
MBYGAlUEAxMPd3d3LnNlZGV4LmNvLmtyMSMwIQYJKoZIhvcNAQkBFhRoc2hvb25A
c2hpbnNlZ2F1LmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAvl7VoyES
AR4viuOi7Rt9LUcsj7BX9lpC6RbmvkIRDcTBdSUalLPmj7ABVTxfzbRR37YNnAIE
Oi/2lj9DdbaCO5O9KnHFptWrCjaV62H4Z+sq9LoOGW7ifxcCllpAKBh7P9r5jLhp
GXGAONMFOGNKObgTtcYgTs0BPDJXlb08CwcCAwEAAaAAMA0GCSqGSIb3DQEBBAUA
A4GBAFuBObSdrkGsqC6IxnD6+mAa6gq3CfAP7Yk5yUpfGYFnQwBLnKlqUqfbst0R
w826ojj6sVH2mxsm2C5sBb2J8h+NZQ2qo/aGYKF56g8ZQDnSmnVvTJph05xTgEOM
PIYNPQXSRGq9MewjJbiYHpTzsQ5k6d8m/e58Hlh9CWWBVyat
-----END CERTIFICATE REQUEST-----
```

■ 인증서 설치

< 인증서의 내용을 포함한 newreq.pem >

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,D09340D1575A72FD

Getay3V7lVgK9ZNUd282AqaIhBnrrcTpAUoXyYb46Qrl+jfxYk0bS+juLWf/Kwgf
DzBdlR6qu6ksY0E+/rqz9bWbgasTpyqnqJyrhD0v5tJSy9TQYNSxilREEdirM/8s
+x9lAtDWRTL0AkavF7TKeb5D4wMC3eEpD05+4bNMgMpHPxns7P/zM0ytTliJC4r6
25QWAz+jyu8FugFVaRSNiFHlsLCXxZxjVf0NuegtftZpcaITmmX4qRql8qtydn+2
74FU4QfiWQEkV4IY0Vnl4VahF/hC0ZBtc0eaulX9feZTaLEjMDl+fM3G5ihVAXUL
6CxJ6J8gdW8S0iChDDEIvfe/QSmFlcRAPlTed05lWh804akCE1c0C7IGPk+Anp7D
d9iIPbAxiIBMqAb52/ZXkKJ4M+jkz5SZEARblEEwszpKTSgYejYDkvVB+FLde0d7
7llPaOCQlf9onhqm90ARLdqQSQlTDXLqQPgUlZPhPSBE6JGZwqtMzvNlrUXum270
H07jYnvxt09lzn4dViHQwR8pAHedKhixquXsjp8M03Tx0dg0WgypfKXVItHJhQP9
lvjTJZotEmspUTyqQAAIHml7PWZ7i5dH9mKfM3P60u35/gon5cwr+lYjsijXG7j2
Cat2ePfbU3kukwmxcqaIz2oDQIhUVoKoSlwvYI8cfnFo7zhehCs0nMIXcSJ6vpyt
goXXsHGVC9GKclWYB9L9WPIraUSk8B5WCJryFdYqlEPrGT8N6KSPD85R5Ulx9okv
KP+Qguuxd08tJmqzrkaclybv9PJiqcZ3hYSyjTm4N7myDd5eT+pu9Q==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIE0jCCBDugAwIBAgIQExfKUVhgcUkghGichEsF9jANBgkqhkiG9w0BAQQFADCB
ujEfMB0GA1UEChMWVmVyaVNpZ24gVHJlc3QgTmV0d29yazEXMBUGA1UECxM0VmVy
aVNpZ24sIEluYy4xMzAxBgNVBAsTKlZlcmlTaWduIEludGVybmF0aW9uYWwgU2Vy
dmVyIENBIC0gQ2xhc3MgMzFJMEcGA1UECxNAd3d3LnZlcmlzaWduLmNvbS9DUFMg
SW5jb3JwLmJ5IFJlZi4gTE1BQklMSVRZIExURC4oYyk5NyBWZXJpU2lnbjAeFw0w
NzAxMjYwMDAwMDBaFw0wOTAxMjUyMzU5NTlaMIIBFTELMAkGA1UEBhMCS1IxDjAM
BgNVBAgTBVNFTlVMMRUwEwYDVQQHFAxTZW9kYWVtdW4tZ3UxGjAYBgNVBAoUEVNL
IENPTUlVTklDQVRJT05TMSMwIQYDVQQLFBpDdXN0b21lciBTYXRpc2ZhY3Rpb24g
dGVhbTE1MDMGA1UECxMsVGVybXMgb2YgdXNlIGF0IHd3dy5jcm9zc2NlcnQuY29t
L3JwYSAoYykgMDQxJDAiBgNVBAsTG0F1dGhlbnRpY2F0ZWQgYnkgSOVDQSwgSW5j
LjEnMCUGA1UECxMeTWVtYmVyLCBWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMRgwFgYD
VQQDFA9tZW1iZXIubmF0ZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGB
AJ7vXEDY4B83mvy06lTw/t73/R5CzSgYIdf5ND27FjqXOm3bdri3mVjZce8Ka3BM
UGacjIBRVo4f+eXhZENcW0LVPgyaRRFBs/WqmtJgmiIK8/pnaINNml0NwmKSKdim
KHJHCby0S4G2CdFD9KrvZRxmtAbgRJxcZ0LS8WJu+fhbAgMBAAGjggF5MIIBdTAJ
BgNVHRMEAjAAMIGsBgNVHSAEgaQwgaEwgZ4GC2CGSAGG+EUBBwEBMIGOMCgGCCsG
AQUFBwIBFhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vQlBTMGIGCCsGAQUFBwIC
MFYwFRYOVmVyaVNpZ24sIEluYy4wAwIBARo9VmVyaVNpZ24ncyBDUFMgaW5jb3Jw
LiBieSByZWZlcmVuY2UgbGlhYi4gbHRkLiAoYyk5NyBWZXJpU2lnbjARBglghkgB
hvhCAQEEBAMCBkAwKAYDVR0lBCEwHwYJYIZIAYb4QgQBBggrBgEFBQcDAQYIKwYB
BQUHAwIwNAYIKwYBBQUHAQEEKDAmMCQGCCsGAQUFBzABhhhodHRw0i8vb2NzcC52
ZXJpc2lnbi5jb20wRgYDVR0fBD8wPTA7oDmgN4Y1aHR0cDovL2NybC52ZXJpc2ln
bi5jb20vQ2xhc3MzSW50ZXJuYXRpb25hbFN1cnZlci5jcmwwDQYJKoZIhvcNAQEE
BQADgYEAnTUwomIKlm/JQR+mZ07jMGytiFyGUNoOET8TdIAO2Fkumbzu7X+CKei9
Cfac3LRi7yz0zMx2cIqgynyKslNofDi+ZyURz9lyudz2am0TPmWci8Evf6XdvLL6
9DmJmM0a640+Xl9wRNheaIPfNvua3oQMYqv/tA3hEx7cQSlwyDI=
-----END CERTIFICATE-----
```

■ Conf 수정

3. 환경파일 작성

http.m 환경파일에 있는 *DOMAIN, *NODE, *VHOST, *SVRGROUP, *SERVER, *SSL 부분을

확인.

- DOCROOT : 도큐먼트의 경로가 정확히 설정되어 있는지 확인.
- PORT : *NODE 와 *VHOST 에 있는 Port 를 적절히 지정. (*VHOST 의 포트는 여러 개를 동시에 사용할 수 있습니다.)
- SSLFLAG(default - off) : SSLFLAG 가 y 상태이면 SSL 을 이용하겠다는 것.
- SSLNAME : SSL 을 이용하는 경우 이에 대한 설정을 나타냄. (SSLFLAG 가 on 상태일 경우에만 적용됩니다.)

4. **환경파일 컴파일**

VHOST 에서 SSLNAME 에서 선언한 *SSL 절을 수정한다.

```
*SSL
ssl         CertificateFile = "C:/TmaxSoft/WebtoB4.1/ssl/newreq.pem", (인증서 파일)
            CertificateKeyFile = "C:/TmaxSoft/WebtoB4.1/ssl/newreq.pem" (키 파일)
            CACertificateFile = "C:/TmaxSoft/WebtoB4.1/ssl/secureCA.pem", (시큐어 체인 파일)
#           CACertificateFile = "C:/TmaxSoft/WebtoB4.1/ssl/intermediate.pem", (글로벌 체인 파일)
            CACertificatePath = "C:/TmaxSoft/WebtoB4.1/ssl" (체인인증서 파일경로)
            RandomFile = "/root/webtob/ssl/urandom, 2048",
            RandomFilePerConnection = "/root/webtob/ssl/urandom, 512",
            VerifyClient = 0,
            VerifyDepth = 10
```

* 시큐어 인증서의 경우 secureCA.pem 설정.
* 글로벌 서버의 경우엔 intermediate.pem 설정.

5. **환경파일 컴파일**

- 컴파일 작업은 wscfl 명령에 의해 이뤄진다.

```
$ wscfl -i http.m
```

$ CFL is done successfully for node<NODE NAME> // 컴파일 성공

■ 웹서버 재구동

6. **WebtoB 재구동**

- 컴파일이 끝나면 필히 WebtoB 를 재구동해야 합니다.

$ wsdown // WebtoB 를 종료하기 위한 프로그램
Do you really want to down whole webtob ? <y : n> :
$wsboot //WebtoB 를 기동하기 위한 프로그램
wsboot for node< > is starting :

Enter PEM pass phrase : // 암호를 기재

▶ 인증서 설치 완료.

■ 인증서 저장

- **직접 신청**시 다음과 같은 과정을 통해 인증서 설치를 합니다.

(신청대행시 아래 서버 ID – cert.pem 파일을 따로 첨부해드립니다.)

1. **직접 신청**시 다음과 같은 과정을 통해 인증서를 설치합니다.

해당 디지털 ID 가 승인되면 E-mail 로 해당 기술 또는 서비스 담당자에게 송신됩니다. 서버 ID 는 예 를 들면 다음과 같이 나타납니다.


```
-----BEGIN CERTIFICATE-----
JIEBSDSCEXoCHQEwLQMJSoZILvoNVQECSQAwcSETMRkOAMUTBhMuVrMmIoAnBdNVBAoTF1J
TQSBEYXRhIFNlY3VyaXR5LCBJbmMuMRwwGgYDVQQLExNQZXJzb25hIENlcnRpZmljYXRlMSQwIg
YDVQQDExtPcGVuIE1hcmtldCBUZXN0IFNlcnZlciAxMTAwHhcNOTUwNzE5MjAyNzMwWhcNOTYw
NTE0MjAyOTEwWjBzMQswCQYDVQQGEwJVUzEgMB4GA1UEChMXUlNBIERhdGEgU2VjdXJpdHks
IEluYy4xHDAaBgNVBAsTE1BlcnNvbmEgQ2VydGlmaWNhdGUxJDAiBgNVBAMTG09wZW4gTWFya
2V0IFRlc3QgU2VydmVyIDExMDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDU/7lrgR6vkVNX40B
Aq1poGdSmGkD1iN3sEPfSTGxNJXY58XH3JoZ4nrF7mIfvpghNi1taYimvhbBPNqYe4yLPAgMBAAEw
DQYJKoZIhvcNAQECBQADQQBqyCpws9EaAjKKAefuNP+ z+ 8NY8khckgyHN2LLpfhv+ iP8m+ bF66
HNDUlFz8ZrVOu3WQapgLPV90kIskNKXX3a
------END CERTIFICATE-----
```


■ 인증서 설치

2. **인증서 저장**

-----BEGIN CERTIFICATE ~ 에서 ~ END CERTIFICATE----- 까지 모든 문자(또는 첨부해 드린 **cert.pem** 파일)를 복사하여 기존 **newreq.pem** 파일 안에 아래와 같이 Overwriting 하여 넣습니다.

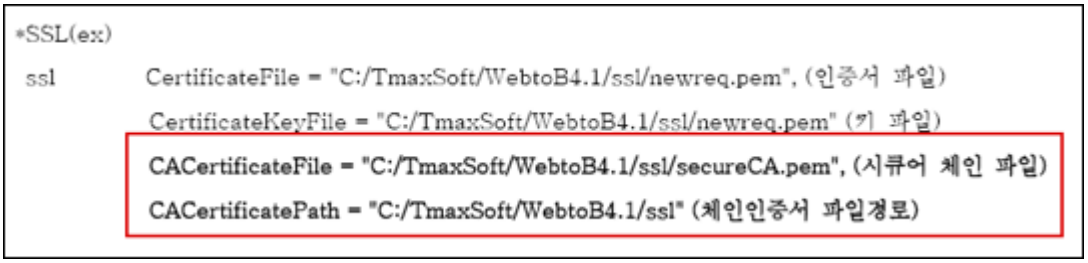
< 인증서의 내용을 포함한 newreq.pem >

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,D09340D1575A72FD

Getay3V7lVgK9ZNUd282AqaIhBnrrcTpAUoXyYb46Qrl+jfxYk0bS+juLWf/Kwgf
DzBdlR6qu6ksY0E+/rqz9bWbgasTpyqnqJyrhD0v5tJSy9TQYNSxilREEdirM/8s
+x9lAtDWRTL0AkavF7TKeb5D4wMC3eEpD05+4bNMgMpHPxns7P/zM0ytTliJC4r6
25QWAz+jyu8FugFVaRSNiFHlsLCXxZxjVf0NuegtftZpcaITmmX4qRql8qtydn+2
74FU4QfiWQEkV4IY0Vnl4VahF/hC0ZBtc0eaulX9feZTaLEjMDl+fM3G5ihVAXUL
6CxJ6J8gdW8S0iChDDEIvfe/QSmFlcRAPlTed05lWh804akCE1c0C7IGPk+Anp7D
d9iIPbAxiIBMqAb52/ZXkKJ4M+jkz5SZEARblEEwszpKTSgYejYDkvVB+FLde0d7
7llPa0CQ1f9onhqm90ARLdqQSQlTDXLqQPgUlZPhPSBE6JGZwqtMzvNlrUXum270
H07jYnvxt09lzn4dViHQwR8pAHedKhixquXsjp8M03Tx0dg0WgypfKXVItHJhQP9
lvjTJZotEmspUTyqQAAIHml7PWZ7i5dH9mKfM3P60u35/gon5cwr+lYjsijXG7j2
Cat2ePfbU3kukwmxcqaIz2oDQIhUVoKoSlwvYI8cfnFo7zhehCs0nMIXcSJ6vpyt
goXXsHGVC9GKclWYB9L9WPIraUSk8B5WCJryFdYqlEPrGT8N6KSPD85R5Ulx9okv
KP+QguuxdO8tJmqzrkaclybv9PJiqcZ3hYSyjTm4N7myDd5eT+pu9Q==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIE0jCCBDugAwIBAgIQExfKUVhgcUkghGichEsF9jANBgkqhkiG9w0BAQQFADCB
ujEfMB0GA1UEChMWVmVyaVNpZ24gVHJ1c3QgTmV0d29yazEXMBUGA1UECxM0VmVy
aVNpZ24sIEluYy4xMzAxBgNVBAsTKlZlcmlTaWduIEludGVybmF0aW9uYWwgU2Vy
dmVyIENBIC0gQ2xhc3MgMzFJMEcGA1UECxNAd3d3LnZlcmlzaWduLmNvbS9DUFMg
SW5jb3JwLmJ5IFJlZi4gTElBQklMSVRZIExURC4oYyk5NyBWZXJpU2lnbjAeFw0w
NzAxMjYwMDAwMDBaFw0wOTAxMjUyMzU5NTlaMIIBFTELMAkGA1UEBhMCSlIxDjAM
BgNVBAgTBVNFTlVMMRUwEwYDVQQHFAxTZW9kYWVtdW4tZ3UxGjAYBgNVBAoUEVNL
IENPTUlVTklDQVRJT05TMSMwIQYDVQQLFBpDdXN0b21lciBTYXRpc2ZhY3Rpb24g
dGVhbTE1MDMGA1UECxMsVGVybXMgb2YgdXNlIGF0IHd3dy5jcm9zc2NlcnQuY29t
L3JwYSAoYykgMDQxJDAiBgNVBAsTG0F1dGhlbnRpY2F0ZWQgYnkgSOVDQSwgSW5j
LjEnMCUGA1UECxMeTWVtYmVyLCBWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMRgwFgYD
VQQDFA9tZW1iZXIubmF0ZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGB
AJ7vXEDY4B83mvy061Tw/t73/R5CzSgYIdf5ND27FjqX0m3bdri3mVjZce8Ka3BM
UGacjIBRVo4f+eXhZENcW0LVPgyaRRFBs/WqmtJgmiIK8/pnaINNml0NwmKSKdim
KHJHCby0S4G2CdFD9KrvZRxmtAbgRJxcZ0LS8WJu+fhbAgMBAAGjggF5MIIBdTAJ
BgNVHRMEAjAAMIGsBgNVHSAEgaQwgaEwgZ4GC2CGSAGG+EUBBwEBMIGOMCgGCCsG
AQUFBwIBFhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vQlBTMGIGCCsGAQUFBwIC
MFYwFRYOVmVyaVNpZ24sIEluYy4wAwIBARo9VmVyaVNpZ24ncyBDUFMgaW5jb3Jw
LiBieSByZWZlcmVuY2UgbGlhYi4gbHRkLiAoYyk5NyBWZXJpU2lnbjARBglghkgB
hvhCAQEEBAMCBkAwKAYDVR0lBCEwHwYJYIZIAYb4QgQBBggrBgEFBQcDAQYIKwYB
BQUHAwIwNAYIKwYBBQUHAQEEKDAmMCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC52
ZXJpc2lnbi5jb20wRgYDVR0fBD8wPTA7oDmgN4YlaHR0cDovL2NybC52ZXJpc2ln
bi5jb20vQ2xhc3MzSW50ZXJuYXRpb25hbFNlcnZlci5jcmwwDQYJKoZIhvcNAQEE
BQADgYEAnTUwomIKlm/JQR+mZ07jMGytiFyGUNoOET8TdIA02Fkumbzu7X+CKei9
Cfac3LRi7yz0zMx2cIqgynyKslNofDi+ZyURz9lyudz2am0TPmWci8Evf6XdvLL6
9DmJmM0a640+Xl9wRNheaIPfNvua3oQMYqv/tA3hEx7cQSlwyDI=
-----END CERTIFICATE-----
```

■ Conf 수정

- 2007 년 4 월 이후에 적용된 시큐어 인증서는 첨부된 체인인증서를 함께 설치합니다.
  - http.m 환경파일 수정



3. **환경파일 컴파일**
   - 컴파일 작업은 **wscfl** 명령에 의해 이뤄진다.

     $ wscfl -i http.m

   $ CFL is done successfully for node<NODE NAME> // 컴파일 성공
4. **WebtoB 재구동**
   - 컴파일이 끝나면 필히 WebtoB 를 재구동해야 합니다.

   $ wsdown // WebtoB 를 종료하기 위한 프로그램
   Do you really want to down whole webtob ? <y : n> :
   $wsboot //WebtoB 를 기동하기 위한 프로그램
   wsboot for node< > is starting :
   Enter PEM pass phrase : // 암호를 기재

   ▶ 인증서 갱신설치 완료.

■ 환경파일 수정

- **두개의 가상호스트{test1.crosscert.com(이하 A), test2.crosscert.com(이하 B)}** 인증서를 발급 받은 후에 두개의 SSL 웹 서버 인증서를 설치하는 방법입니다.

1. **VHOST 에서 Vhost 추가 (http.m 환경파일)**

```
*VHOST
Vhost1    DOCROOT="/usr/local/webapp/webtob/docs/test1/",
          PORT = "443",
          SSLFLAG=Y,
          SSLNAME="ssl1",
          ....................,
          HostName = "test1.crosscert.com"
Vhost2    DOCROOT="/usr/local/webapp/webtob/docs/test2/",
          PORT = "444",
          SSLFLAG=Y,
          SSLNAME="ssl2",
          ....................,
          HostName = "test2.crosscert.com"
*SSL
ssl1      CertificateFile = "/usr/local/webapp/webtob/ssl/test1/newreq.pem",
          CertificateKeyFile = "/usr/local/webapp/webtob/ssl/test1/newreq.pem",
          CACertificateFile = "/usr/local/webapp/webtob/ssl/secureCA.pem", (시큐어 체인)
        # CACertificateFile = "/usr/local/webapp/webtob/ssl/intermediate.pem", (글로벌 체인)
          CACertificatePath = "/usr/local/webapp/webtob/ssl", (체인인증서 경로)
          RandomFile = "/usr/local/webapp/webtob/bin/.rnd, 2048",
          RandomFilePerConnection = "/usr/local/webapp/webtob/bin/.rnd, 512",

ssl2      CertificateFile = "/usr/local/webapp/webtob/ssl/test2/newreq.pem",
          CertificateKeyFile = "/usr/local/webapp/webtob/ssl/test2/newreq.pem",
          CACertificateFile = "/usr/local/webapp/webtob/ssl/secureCA.pem", (시큐어 체인)
        # CACertificateFile = "/usr/local/webapp/webtob/ssl/intermediate.pem", (글로벌 체인)
          CACertificatePath = "/usr/local/webapp/webtob/ssl", (체인인증서 경로)
          RandomFile = "/usr/local/webapp/webtob/bin/.rnd, 2048",
          RandomFilePerConnection = "/usr/local/webapp/webtob/bin/.rnd, 512",
```

■ 인증서 설치

A. 가상호스트 설정(test1.crosscert.com)

WebToB 에서 SSL 설정을 하기 위해서는 SSL 을 설정하고 싶은 Virtual Host(A,B)를 선언한 VHOST 절에서 SSLFLAG 를 선언해야 합니다.
다음은 SSLFLAG 의 사용 예입니다.

```
SSLFLAG=Y,
```

위와 같이 SSLFLAG 를 Y 로 설정하여 SSL 을 이용하겠다고 선언한 후에는, 미리 발급 받은 SSL 웹 서버 인증서를 설정 해주어야 합니다.
다음은 SSL 웹 서버 인증서 설정 예 입니다.

```
*SSL
 ssl1   CertificateFile = "인증서파일경로/newreq.pem",
        CertificateKeyFile = " 인증서파일경로 /newreq.pem",
        CACertificateFile = "/usr/local/webapp/webtob/ssl/secureCA.pem", (시큐어 체인)
        CACertificateFile = "/usr/local/webapp/webtob/ssl/intermediate.pem", (글로벌 체인)
        CACertificatePath = "/usr/local/webapp/webtob/ssl", (체인인증서 경로)
   ☞ 시큐어 인증서일 경우 secureCA.pem
     글로벌 인증서일 경우 intermediate.pem 설정은 필히 해주셔야 합니다.
        RandomFile = "WebToB홈디렉토리경로/bin/.rnd, 2048"
        RandomFilePerConnection = "WebToB홈디렉토리경로/bin/.rnd, 512"
        VerifyClient = 0,
        VerifyDepth = 10
```

마지막으로 ssl1 을 선언한 후 VHOST 절에서 SSLNAME="ssl1" 항목을 선언하면,
ssl1 에 설정되어져 있는 SSL 웹 서버 인증서 SSL 암호화통신 서비스를 최종적으로 설정하는 것
입니다.

■ 웹서버 재구동

B. 가상호스트 설정(test2.crosscert.com)

동일한 서버에서 SSL 포트는 공유가 안되기 때문에, SSL 포트만 well-known 포트 및
사용중인 포트를 제외한 포트로 설정해줍니다. 다음은 설정 예입니다.
PORT = "444",
- A 와 같이 SSL 웹서버 인증서를 설치 합니다.

```
ssl2   CertificateFile = "인증서파일경로/newreq.pem",
       CertificateKeyFile = " 인증서파일경로 /newreq.pem",
       CACertificateFile = "/usr/local/webapp/webtob/ssl/secureCA.pem", (시큐어 체인)
       CACertificateFile = "/usr/local/webapp/webtob/ssl/intermediate.pem", (글로벌 체인)
       CACertificatePath = "/usr/local/webapp/webtob/ssl", (체인인증서 경로)
  ☞ 시큐어 인증서일 경우 secureCA.pem
    글로벌 인증서일 경우 intermediate.pem 설정은 필히 해주셔야 합니다.
       RandomFile = "WebToB홈디렉토리경로/bin/.rnd, 2048"
       RandomFilePerConnection = "WebToB홈디렉토리경로/bin/.rnd, 512"
       VerifyClient = 0,
       VerifyDepth = 10
```

2. http.m 컴파일
   $ wscfl .I http.m

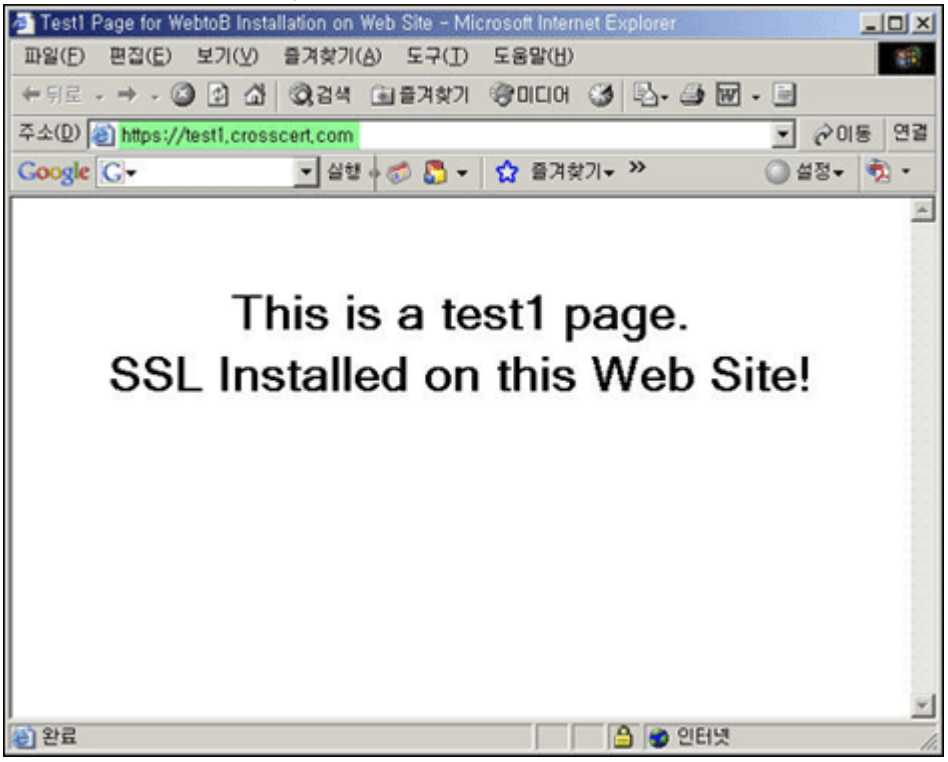
3. **웹투비 재구동.**
   - 컴파일이 끝나면 필히 WebtoB 를 재구동해야 합니다.
   $ wsdown // WebtoB 를 종료하기 위한 프로그램
   Do you really want to down whole webtob ? <y : n> :
   $ wsboot //WebtoB 를 기동하기 위한 프로그램
   wsboot for node< > is starting :
   Enter PEM pass phrase : // 암호를 기재
   ▶ 인증서 설치 완료.

■ 인증서 확인

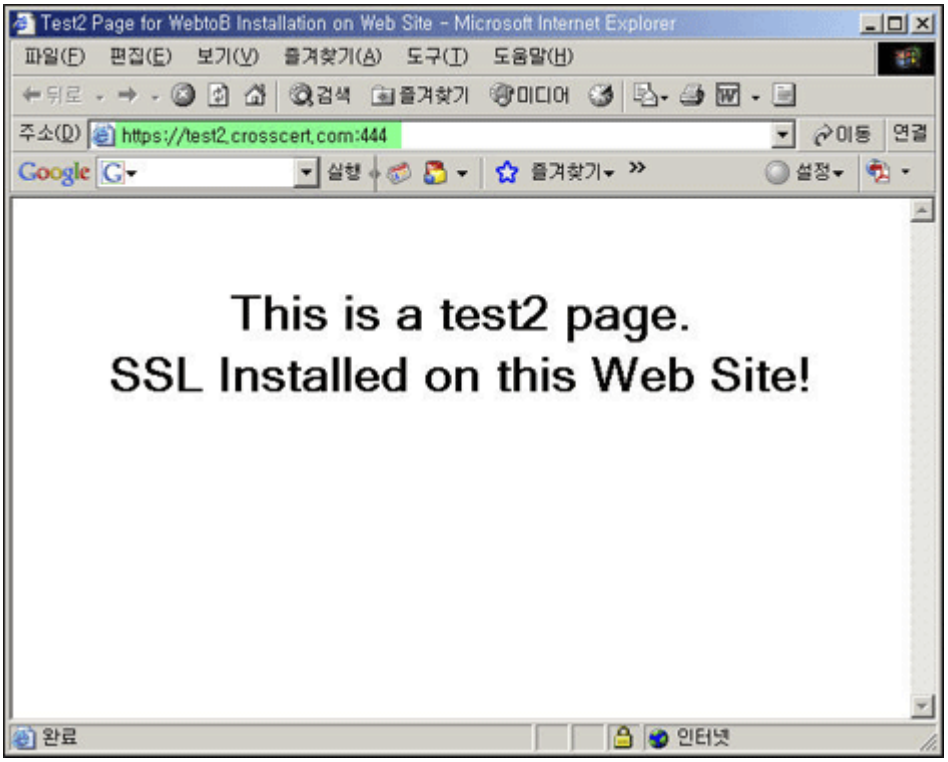
4. **테스트** - 설정한 SSL 포트가 Listen 상태인지 확인

```
# netstat -na | grep ] LISTEN
    *.443                *.*              0      0 24576      0 LISTEN
    *.444                *.*              0      0 24576      0 LISTEN
```

- 웹 브라우저에서 https://test1.crosscert.com 접속



- 웹 브라우저에서 https://test1.crosscert.com:444 접속


Test2 Page for WebtoB Installation on Web Site - Microsoft Internet Explorer
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
뒤로 검색 즐겨찾기 미디어
주소(D) https://test2.crosscert.com:444
이동 연결
Google 실행 즐겨찾기 설정
This is a test2 page.
SSL Installed on this Web Site!
완료
인터넷