

WebtoB Web Server 인증서 설치

Version 1.0

March 4, 2008

▶ 인증서 설치**2. 인증서 저장**

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

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 변경합니다. (아래의 스냅샷 참조)

Ex)

< CSR 의 내용을 포함한 newreq.pem >

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

Getay3V71VgK9ZNUd282AqaIhBnrrcTpAUoXyYb46Qr1+jfxYk0bS+juLWf/Kwgf
DzBd1R6qu6ksYOE+/rqz9bWbgasTpyqmqJyrhD0v5tJSy9TQYNSxi1REEdirM/8s
+x91AtDWRTLOAkavF7TKeb5D4wMC3eEpD05+4bNMgMpHPxns7P/zM0ytTliJC4r6
25QWaz+jyu8FugFVaRSNiFHlsLCXxZxjVf0NuegtftZpcaITmmX4qRq18qtydn+2
74FU4QfiWQEkV4IY0Vn14VahF/hCOZBtc0eaulX9feZTaLEjMD1+fM3G5ihVAXUL
6CxJ6J8gdW8S0iChDDEIvfe/QSmf1cRAP1Ted051Wh804akCElc0C7IGPk+Anp7D
d9iIPbAxiIBMqAb52/ZXkKJ4M+jkz5SZEARb1EEwzspKTSgYejYDkvVB+FLde0d7
711PaOCQ1f9onhqm90ARLdqQSQ1TDXLqQPgU1ZPhPSBE6JGZwqtMzvN1rUXum270
HO7jYnvxt091zn4dViHQwR8pAHedKhixquXsjsj8M03Tx0dg0WgypfKXVItHJhQP9
lvjTJZotEmspUTyqQAAIHm17PWZ7i5dH9mKfM3P60u35/gon5cwr+1YjsijXG7j2
Cat2ePfbU3kukwmxccaIz2oDQIhUVoKoSlwvYI8cfnFo7zhehCs0nMIXcSj6vpyt
goXXsHGVC9GKclWYB9L9WPIraUSk8B5WCJryFdYq1EPrGT8N6KSPD85R5U1x9okv
KP+Qguuxd08tJmqrkaclybv9PJiqcZ3hYSyjTm4N7myDd5eT+pu9Q==
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE REQUEST-----
MIIBODCCATkCAQAwY8xCzAJBgNVBAYTAktSMQ4wDAYDVQQIEwVTZW91bDEUMBIG
A1UEBxMLU29nb25nLWVrbmcxCzAJBgNVBAoTAK1DMQ4wDAYDVQQLEwVTRURFWDEY
MBYGA1UEAxMPd3d3LnN1ZGV4LmNvLmtyMSMwIQYJKoZIhvcNAQkBFhRoc2hvb25A
c2hpbmN1Z2F1LmNvbTCBnzANBjG9wOBAQEFAA0BjQAwgYkCgYEAv17VoyES
AR4vui0i7Rt9LUcsj7BX9lpC6RbmvkIRDcTBdSUa1LPmj7ABVTxfzbRR37YmNaIE
0i/2lj9DbaC0509KnHFptWrcjaV62H4Z+sq9Lo0GW7ifxcC1lpAKBh7P9r5jLhp
GXGAONMF0GNK0bgTtcYgTs0BPDJX1b08CwcCAwEAaAAMA0GCsqGSib3DQEBBAUA
A4GBAFuB0bSdrkGsqC6IxnD6+mAa6gq3CFAP7Yk5yUpfGYFnQwBLnK1qUqfbst0R
w826ojj6sVH2mxsm2C5sBb2J8h+NZQ2qo/aGYKF56g8ZQDnSmmVvTJph05xTgEOM
PIYNPQXSRGq9MewjJbiYHpTzsQ5k6d8m/e58H1h9CWwBVyat
-----END CERTIFICATE REQUEST-----
```

▶ 인증서 설치

< 인증서의 내용을 포함한 newreq.pem >

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

Getay3V71VgK9ZNUd282AqaIhBnrccTpAUoXyYb46Qrl+jfxYk0bS+juLWf/Kwgf
DzBdlR6qu6ksY0E+/rqz9bWbgasTpyqngJyrhD0v5tJSy9TQYNSxilREEdirM/8s
+x91AtDWRTLOAkavF7TKeb5D4wMC3eEpD05+4bNMgMpHPxns7P/zM0ytTliJC4r6
25QWaz+jyu8FugFVaRSNiFHLsLCXxZxjVf0NuegtftZpcaITmmX4gRq18qtydn+2
74FU4QfiWQEKV4IY0Vn14VahF/hCOZBtc0eaulX9feZTaLEjMD1+fM3G5ihVAXUL
6CxJ6J8gdW8S0iChDDEIvfe/QSmFlcRAP1Ted051Wh804akCElc0C7IGPk+Anp7D
d9iIPbAxiIBMqAb52/ZXkKJ4M+jkz5SZEArb1EEwszpKTSgYeYDkvVB+FLdeOd7
711PaOCQ1f9onhq90ARLdqQSQ1TDXLqQPgU1ZPhPSBE6JGZwqtMzvNlrUXum270
H07jYnvxt091zn4dViHQwR8pAHedKHixquXsjp8M03Tx0dg0WgypfKXVIthJhQP9
lvjTJZotEmspUTyqQAAIHml7PWZ7i5dH9mKfM3P60u35/gon5cwr+1YjsijXG7j2
Cat2ePfbU3kukwmxccaIz2oDQIhUvoKoSlwYI8cfnFo7zhehCs0nMIXcSJ6vpyt
goXXsHGVC9GKc1WYB9L9WPIraUSk8B5WCJryFdyqLEPrGT8N6KSPD85R5U1x9okv
KP+Qguuxd08tJmqzrkacllybv9PJiqcZ3hYSyJtm4N7myDd5eT+pu9Q==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIEOjCCBDugAwIBAgIQExfKUVhgCukghGichEsF9jANBgkqhkiG9w0BAQQFADCB
ujEFMBOGA1UEChMwVnVyaVNPZ224gVHJlc3QgTmV0d29yazEXMBUGA1UECXM0VnVya
aVNPZ224sIEluYy4wMzAxZG91bWVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbn
dmVyaWVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbn
SW5jb3JwLmJ5IFJlZi4gTElBQk1MSVRZIEURC4oYyYk5NybWZlZjU2LnVhbnVhbnVhbn
NzAxMjYwMDAwMDAaBQ0wOTAxMjYwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMD
BgNVBAAgTmV0d29yazEXMBUGA1UECjEwMzAxZG91bWVhbnVhbnVhbnVhbnVhbnVhbn
IENPTU1VTk1DQVRJT05TMSMwIQYDVOQLFBFdXN0b211ciBTYXRpc2ZlY3Rpb24g
dG9hbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbn
L3JwYSAoYyYkMzAxZG91bWVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbn
LjEnMCUGA1UECjEwMzAxZG91bWVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbnVhbn
VQDFA9tZWliZXIubmF0ZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgYQAMIGJAoGB
AJ7vXEDY4B83mvy061Tw/t73/R5CzSgYIdf5ND27FjqX0m3bdri3mVjZce8Ka3BM
UGacjIBRVo4f+eXhZENCW0LVPgyaRRFBs/WqmtJgmiIK8/pnaINNml0NwmKSKdim
KHJHChy0S4G2CdFd9KrvZRxmtAbgRjxcZ0LS8WJu+fhbAgMBAAGjggF5MIIBDTAJ
BgNVHRMEAjAAMIGsBgNVHSAEgaQwgaEwgZ4GC2CGSAGG+EUBBwEBMIGOMCgGCCsG
AQUFBwIBFhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vQ1BTMGIGCCsGAQUFBwIC
MFYwFRY0VnVyaVNPZ224sIEluYy4wMzAxZG91bWVhbnVhbnVhbnVhbnVhbnVhbnVhbn
LiBieSByZWZlcmVuY2UgG1hYi4gbHRkLiAoYyYk5NybWZlZjU2LnVhbnVhbnVhbnVhbn
hvCAQEEBAMCBkAwKAYDVR01BCEwHwYJYIZIAyB4QgQBBggrBgEFBQcDAQYIKwYB
BQUHAWIwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBzABhhhodHRw0i8vb2Nzc52
ZXJpc2lnbi5jb20wRgYDVR0fBDB8wPTA7oDmgN4Y1aHR0cDovL2Nybc52ZXJpc2ln
bi5jb20vQ2xhc3MzSW50ZXJlYXRpb25hbFNlcnZ1ci5jc291bWVhbnVhbnVhbnVhbn
BQADgYEAnTUwomIKlm/JQR+M207jMGytiFyGUNo0ET8TdIA02Fkumbzu7X+CKei9
Cfac3LRi7yzCmX2cIqqynyKs1NofDi+ZyURz91yudz2am0TPmWci8Evf6XdxLL6
9DmJmM0a640+Xl9wRNheaIPfnvua3oQMYqv/tA3hEx7cQSlwyDI=
-----END CERTIFICATE-----
```

▶ Conf 수정

3. 환경파일 작성

http.m 환경파일에 있는 *DOMAIN, *NODE, *VHOST, *SVRGROUP, *SERVER, *SSL부분을 확인.

- DOCROOT : 도큐먼트의 경로가 정확히 설정되어 있는지 확인.
- PORT : *NODE 와 *VHOST에 있는 Port를 적절히 지정.
(*VHOST의 포트는 여러 개를 동시에 사용할 수 있습니다.)
- SSLFLAG(default - off) : SSLFLAG가 y상태이면 SSL을 이용하겠다는 것.
- SSLNAME : SSL을 이용하는 경우 이에 대한 설정을 나타냄.
(SSLFLAG가 on상태일 경우에만 적용됩니다.)

4. *SSL 경로설정

VHOST에서 SSLNAME에서 선언한 *SSL절을 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**5. WebtoB 재구동**

- 컴파일이 끝나면 필히 WebtoB를 재구동해야 합니다.

```
$ wsdown // WebtoB를 종료하기 위한 프로그램
```

```
Do you really want to down whole webtoB ? <y : n> :
```

```
$ wsboot //WebtoB를 기동하기 위한 프로그램
```

```
wsboot for node< > is starting :
```

```
Enter PEM pass phrase : // 암호를 기재
```

=> 인증서 설치 완료.