Comodo Korea
국제표준인증 제휴기관

WebtoB Web Server CSR(Certificate Signing Request) 생성

WebtoB Web Server 는 CA 명령어로 CertificateKeyFile (서버 암호키)을 생성합니다.
그리고 생성된 CertificateKeyFile 파일에서 CSR (Certificate Signing Request) 내용을 코모도코리아로 보내주시면 됩니다. 코모도코리아에서는 루트기관에서 발행하는 정식인증서 발급 절차를 밟게 됩니다.
그 후에 정식 인증서가 발급되고 웹 서버에 설치되면 웹 서버 SSL 설정은 마쳐지게 됩니다.

※ CSR(Certificate Signing Request) 생성 순서

1. CA 명령으로 CertificateKeyFile(서버 암호키) 생성
2. CertificateKeyFile(서버 암호키) 백업
3. CSR 파일 생성
4. 코모도코리아에 CSR 접수
5. 네트워크 확인 사항 - SSL 적용에 따른 방화벽, L4 switch 설정 확인
6. 코모도코리아 CSR 파일 답신 확인

1. CA 명령으로 CertificateKeyFile(서버 암호키) 생성

CA 프로그램은 $WEBTOBDIR\bin\ 에 있습니다. (- $WEBTOBDIR 변수는 WebtoB Web Server 가 설치된 디렉토리를 가리킵니다.)
다음 작업으로 CertificateKeyFile(서버 암호키) 생성합니다. 생성이 완료되면 'newreq.pem' 파일로 CertificateKey 파일이 생성됩니다.
서버 암호키(개인키)를 생성할 때에 Generating a 2048 bit RSA private key 으로 생성되는 것을 확인해 주시기 바라며, 다음은 서버 암호키를 생성할 때에 입력하는 예시입니다.

<입력 예>

Country Name (국가코드) : KR
State or Province Name (시/도) : Seoul
Locality Name (구/군) : Songpa
Organization Name (회사명) : Comodo Korea
Organizational Unit Name (부서명) : Digital Certificate Team
Common Name (인증 받을 도메인 주소) : www.comodokorea.co.kr
Email Address : (옵션 사항이므로 입력하지 않아도

됩니다.)
An optional company name : (옵션 사항이므로 입력하지 않아도 됩니다.)

```
[root@web1 root]# $WEBTOBDIR¥bin¥CA -newreq
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
......++++++
...++++++
writing new private key to 'newreq.pem'
Enter PEM pass phrase:
(CertificateKey 파일 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) []:songpa
Locality Name (eg, city) []:seoul
Organization Name (eg, company) [Tmax Ltd]:team
Organizational Unit Name (eg, section) []:digital cert
Common Name (eg, YOUR name)
```

z

```
[]:www.comodokorea.co.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

[root@web1 root]#
```

작업이 완료되면, 작업 디렉터리에 CertificateKey(서버 암호키) 파일인 newreq.pem 파일이 새로 생성됩니다.
문제가 발생된다면, 코모도코리아 메일로 에러상황을 리포트해 주시기 바랍니다.

2. CertificateKeyFile(서버 암호키) 백업

```
[root@web1 root]# sftp xxx.xx.xx.xx
> put newreq.pem
```

안전한 곳에 CertificateKey(서버 암호키) 파일을 백업 복사를 해 놓습니다.
※ CertificateKey(서버 암호키) 파일과 비밀번호는 결코 잃어버리시면 안 됩니다. (나중에 인증서가 설치되면 웹 서버 기동시에 비밀번호를 묻게 됩니다.)
안전한 장소에 백업해 두시기 바랍니다.

3. CSR 파일 생성

CA 명령으로 CertificateKey(서버 암호키) 파일인 newreq.pem 파일을 생성하였습니다.

newreq.pem 파일의 내용을 열어보면,
"RSA PRIVATE KEY" 항목(-----BEGIN RSA PRIVATE KEY----- 에서 ----END RSA PRIVATE KEY-----까지)과 "CERTIFICATE REQUEST" 항목(-----BEGIN CERTIFICATE REQUEST----- 에서 -----END CERTIFICATE REQUEST-----까지)으로 구성된 것을 볼 수 있습니다.

"RSA PRIVATE KEY" 항목은 CertificateKey(서버 암호키)에 해당하는 부분이고,

"CERTIFICATE REQUEST" 항목이 CSR(Certificate Signing Request)에 해당하는 부분입니다.
그래서 두 항목을 나누어서 CertificateKey(서버 암호키) 파일과 CSR(Certificate Signing Request) 항목을 만들어 줍니다.

<예시> 다음은 생성된 newreq.pem 파일의 간략한 내용입니다.

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

wgNaK2wJ9qa42GzfJEAZbFgP4Uzo3h7A7RKgbYFdGySaYyShYLy82tNOT5r4+bCl
... ...
M3Mofn6tz8za3yF+Dz6+aft/viwZYdWWqcWVl7TOoVxIkCLOz2uVSQ==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE REQUEST-----
MIIBsDCCARkCAQAwcDELMAkGA1UEBhMCS1IxDzANBgNVBAgTBnNvbmdwYTEOMAwG
... ...
XGJIkA==
-----END CERTIFICATE REQUEST-----
```

CertificateKey(서버 암호키)에 해당하는 부분인 "RSA PRIVATE KEY" 항목으로 privatekey2007.pem 파일을 만듭니다.
그리고 CSR 에 해당하는 부분인 "CERTIFICATE REQUEST" 항목으로 csr2007.txt 파일을 만듭니다.

다음은 만들어진 privatekey2007.pem, csr2007.txt 파일의 간략한 내용입니다.
<예시> privatekey2007.pem 파일 간략 내용

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

wgNaK2wJ9qa42GzfJEAZbFgP4Uzo3h7A7RKgbYFdGySaYyShYLy82tNOT5r4+bCl
... ...
M3Mofn6tz8za3yF+Dz6+aft/viwZYdWWqcWVl7TOoVxIkCLOz2uVSQ==
-----END RSA PRIVATE KEY-----
```

<예시> csr2007.txt 파일 간략 내용

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBsDCCARkCAQAwcDELMAkGA1UEBhMCS1IxDzANBgNVBAgTBnNvbmdwYTEOMAwG
... ...
XGJIkA==
-----END CERTIFICATE REQUEST-----
```

4. 코모도코리아에 CSR 접수

만드신 CSR(Certificate Signing Request) 파일 csr2007.txt 을 코모도코리아 메일로 첨부해서 발송해 주시기 바랍니다.

5. 네트워크 확인 사항 - SSL 적용에 따른 방화벽, L4 switch 설정 확인

고객님 웹 서버에 SSL 을 적용하게 되면, http:// (기본 80 포트)통신과 https:// (기본 443 포트) 통신를 사용하게 됩니다.
그러므로, 웹 서버에 설정된 방화벽이나 L4 switch 의 설정을 기존 80 포트 설정과 같이 443 포트도 추가 설정해 주셔야 합니다.
정식 인증서를 발행하기까지 웹 서버의 네트워크 환경설정에 443 포트를 열어주시는 계획을 세워주기 바랍니다.

6. 코모도코리아 CSR 파일 답신 확인

코모도코리아에 접수된 CSR 파일이 올바른지 회신을 드립니다. 회신을 확인하시기 바랍니다.
그리고 코모도코리아에서는 보내주신 CSR(Certificate Signing Request) 파일을 토대로 정식 인증서를 발급하게 됩니다.
정식 인증서 발급과 함께 인증서 설치 문서를 안내해 드립니다.