

WebtoB Web Server에서 CSR 생성방법

WebtoB Web 서버에서 인증서(128bit 암호화 제공)를 사용하기 위해 CSR을 생성하는 방법이다.

1. 초기 설정

CSR을 생성하기 전에 다음의 몇 가지 사항을 필히 확인한다.

부팅 후 path나 환경변수를 일일이 설정하지 않기 위해 초기 설정파일을 사용하여 로그인 시에 자동으로 실행되도록 한다. 그러나 간혹 초기 설정파일이 실행되지 않아서 예러가 생기는 경우가 있는데 이럴 경우에 초기 설정파일을 다시 한번 실행시킨다.

리눅스의 경우

bash셸 : `.bash_profile`

c 셸 : `.cshrc`

등을 주로 사용한다.

User가 임의로 `.bash_profile`을 실행시켜주면 되는데 리눅스의 경우 `.bash_profile`

혹은 `./root/.bash_profile`로 실행시켜 주면 된다.

(주의 : 실행을 의미하는 `.` 다음에 한 칸을 필히 띄워야 한다.)

2. 비밀키 및 CSR생성

(1) 보통 `path/ssl` 에서 CSR을 생성한다.

```
$ CA -newreq
```

(`newreq`라는 Commend는 CSR을 생성하는 option이다. 예로 인증서를 만드는 옵션은 `newcert`이다.)

위를 실행시키면

```
Using configuration from path/to/ssl/wbssl.cnf
```

```
Generating a 1024 bit RSA Private key
```

라는 메시지가 뜬다.

(2) 암호 입력

ex) Enter PEM pass phase :

```
verifying password - Enter PEM pass phase :
```

⇒ Private key가 생성.

⇒ 암호문을 잊어버리면 키를 사용할 수 없으므로 주의.

⇒ Private key는 백업 복사본을 만들어 안전한 장소에 보관하여 비밀키가 손실 또는 분실되었을 경우 백업을 가지고 사용한다.

(3) CSR 정보입력

다음 정보를 입력하라는 메시지가 나타난다.

- Country Name <2 letter code> [AU] : KR

국가코드 - 국가에 해당하는 두 글자의 ISO 약어(예: 호주는 au, 영국은 gb, 멕시코는 mx)를 입력한다.

- States or province Name <full name> [some-state] : Seoul
State/province (시/도의 전체 이름) - 완전한 이름을 입력한다.
(예를 들면 NSW가 아닌 New South Wales).

- Locality Name <eg. city> [] : Seocho
Locality(시, 구, 군 등의 이름)

- Organization Name <eg. company> [Internet widgets Pty Ltd] : KECA, Inc.
Organization(소속 단체/회사 이름) - 도메인 이름(CrossCert 등록 과정의 단계 1)을 소유하고 해당 권한 입증(CrossCert 등록 과정의 단계 2)이 있는 단체이어야 한다.

- Organization Unit Name <eg. section> [] : CS Team
Organization Unit(단체 내의 소속 부서(예를 들면 마케팅, 판매, MIS 등))

- Common Name <eg. Your name or your server's hostname> []
: www.crosscert.com
Common Name - 해당 사이트(예: www.bookstore.com)의 승인된 전체 도메인 이름을 입력한다. 이 이름은 사용하려는 https URL과 일치해야 한다. 이 이름도 소속 단체가 소유하는 도메인 이름으로 끝나야 한다.

- Email Address [] : helpdesk@crosscert.com

"추가 속성"을 입력하라는 메시지가 나타나면 skip 하셔도 무관하다.

Ex) A challenge password [] :

An optional company name [] :

Request <and Private key> is in newreq.pem

3. CSR 제출

위의 단계가 성공적으로 이뤄지면 CSR파일이 생성된다.

newreq.pem의 내용은 다음과 같은 형식으로 나타난다.

```
-----BEGIN CERTIFICATE REQUEST-----  
MIIBETCBvAIBADBXMqswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0ZTEh  
MB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMRAwDgYJKoZIhvcNAQkB  
FgFgMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAL6nPTy3avNgbubx+ ESmD4LV1LQG  
fcSh8nehEOIxGwmCPlrhTP87PaA0XvGpvRQUjCGStrlQsd8lcYVVkOaytNUCAwEA  
AaAAMA0GCSqGSIb3DQEBAUAA0EAXcMsa8eXgbG2ZhVyFkRVrI4vT8haN39/QJc9  
BrRh2nOTKgfMcT9h+ 1Xx0wNRQ9/SIGV1y3+ 3abNiJmJBWnJ8Bg==  
-----END CERTIFICATE REQUEST-----
```

이 CSR의 전체 내용(-----BEGIN CERTIFICATE REQUEST 및 END CERTIFICATE REQUEST-----행 포함)을 복사하여 등록 폼에 붙여 넣는다.