Comodo Korea
국제표준인증 제휴기관

Apache 웹서버(2.x.xx) CSR(Certificate Signing Request) 생성

Apache 웹서버를 사용하시는 경우에는 Apache 웹서버에 SSL 를 적용하는데에 몇 가지 확인해 보아야 할 부분이 있습니다.
openssl 암호화 라이브러리 설치 여부와 Apache 웹서버에 mod_ssl 모듈이 설치되어있어야 합니다.
다음으로 서버 개인키(비밀키)를 생성하고, 생성된 개인키를 토대로 CSR(Certificate Signing Request)을 생성합니다.
생성된 CSR 파일을 코모도코리아로 보내주시면, 루트기관에서 발행하는 정식인증서 발급 절차를 밟게됩니다.
그 후에 정식 인증서가 발급되고 웹서버에 설치되면 웹서버 SSL 설정은 마쳐지게 됩니다.

※ CSR(Certificate Signing Request) 생성 순서

1. openssl 설치 확인
2. Apache 웹서버 mod_ssl 모듈 설치 확인
3. 개인키(비밀키) 생성
4. 개인키 확인
5. CSR 생성
6. CSR 확인
7. 개인키 백업
8. 애니서트에 CSR 접수
9. 네트워크 확인 사항 - SSL 적용에 따른 방화벽, L4 switch 설정 확인
10. 코모도코리아 CSR 파일 답신 확인

1. openssl 설치 확인

먼저 openssl 라이브러리가 설치되어 있어야 합니다.

```
[root@web1 root]# find / -name
openssl
...
/usr/bin/openssl
...
/usr/local/openssl/bin/openssl
[root@web1 root]#
```

이상), /usr/local/openssl/bin/openssl 은 openssl 소스 설치된 것입니다. openssl 이 rpm 설치된 것이라면, openssl-devel 라이브러리도 rpm 설치되어있는지 확인합니다.

```
[root@web1 root]# rpm -q openssl
openssl-0.9.7a-2
[root@web1 root]# rpm -q openssl-
devel
openssl-devel-0.9.7a-2
[root@web1 root]#
```

참고적으로 openssl 모듈은 암호화처리 독립 모듈로 최신버젼을 따로 설치하는 것을 추천해 드립니다.
openssl 설치되지 않으셨다면, openssl 설치 가이드를 참고해 주시기 바랍니다.
(openssl 설치 가이드 보기)

2. Apache 웹서버 mod_ssl 모듈 설치 확인

Apache 2.x.xx 웹서버에 mod_ssl 모듈 설치 확인합니다.
Apache 웹서버는 두가지 방식의 모듈 설치를 지원하므로 statically linking module, DSO(Dynamic Shared Objects) module 로 설치된 모듈을 확인할 수 있습니다.
- $HTTPD 변수는 아파치 설치 디렉토리를 가르킵니다.

1. statically linking module 로 설치된 mod_ssl 모듈확인

```
[root@web1 root]# $HTTPD/bin/httpd -l
Compiled-in modules:
 ...
 mod_ssl.c
 ...
[root@web1 root]#
```

웹서버에 설치된 모듈중에 mod_ssl.c 을 확인합니다.

2. DSO module 로 설치된 mod_ssl 모듈확인

```
[root@web1 root]# $HTTPD/bin/httpd -l
```

```
Compiled-in modules:
 ...
 mod_so.c
 ...
[root@web1 root]# ls $HTTPD/module
mod_ssl.so ...
[root@web1 root]#
```

웹서버에 설치된 모듈중에 mod_so.c 을 먼저 확인합니다. 그리고 DSO module 로 설치된 모듈중에 mod_ssl.so 을 확인합니다.

만약에 mod_ssl 모듈이 설치되어있지 않다면, Apache 2.x.xx enable-ssl 옵션 설치 가이드 참고하시고 Apache 웹서버 mod_ssl 모듈을 설치해 주시면 됩니다. (Apache 2.x.xx enable-ssl 옵션 설치 가이드 보기)

모듈 설치 확인이 되었으면, 다음으로 CSR 파일을 생성합니다.
CSR 파일 생성과정에는 Apache 웹서버 SSL 모듈 설치 여부와는 관계없이, openssl 설치된 것으로 생성하실 수 있습니다.
하지만, 인증서가 발행된 다음에 설치에서 문제가 되기 때문에 사전에 웹서버의 SSL 암호화 모듈을 확인해 두는 것입니다.

3. 개인키(비밀키) 생성

Solaris 8 Release 12/02 이하 버전에서 Apache 웹서버를 운영하신다면, [random 옵션사용]을 선택해 주시기 바랍니다.
1. 일반적인 키 생성(random 장치사용)
- $SSL_KEY_STORE 변수는 ssl 개인키를 보관하는 디렉토리를 가르킵니다.

```
▣
[root@web1 root]# cd $SSL_KEY_STORE
[root@web1 ssl]# openssl genrsa -des3 -out
ssl2007.key 2048
Generating RSA private key, 2048 bit long modulus
.............++++++
...++++++
e is 65537 (0x10001)
Enter pass phrase for ssl2007.key: ******
Verifying - Enter pass phrase for ssl2007.key:
******
[root@web1 ssl]#
```

패스워드를 설정하라는 메시지가 나오면 원하는 패스워드를 입력합니다. 이 패스

`

Comodo Korea
국제표준인증 제휴기관

워드는 나중에 인증서를 설치할 때 필요하므로 반드시 기억해두셔야 합니다.
입력을 마치면 2048 비트 RSA 키가 생성되어 ssl2007.key 라는 이름으로 저장됩니다. ssl2007.key 는 다른 적당한 이름으로 바꾸어도 무방합니다.

2. random 옵션사용
솔라리스의 경우에는 Solaris 8 Release 12/02 이하 버전에서 /dev/random 장치가 구성되지 않습니다.

Document ID	**ID27606**
Synopsis	**Differing /dev/random support requirements within Solaris[TM] Operating Environments**
Date	**27 Jan 2004**

[솔라리스 고객지원의 랜덤 device 안내문서]

openssl 유틸리티는 /dev/random 장치를 이용해서 개인키(비밀키) 생성하게 되므로,
/dev/random 장치를 이용할 수 없는 Solaris 8 Release 12/02 이하 버전에서는 다음과 같은 openssl rand 옵션으로
/dev/random 장치를 대신하는 랜덤데이타를 입력합니다.
- rand.dat 파일은 [랜덤데이타 seed] 파일로 서버상의 로그파일 복사본으로 만드시면 됩니다.
- $SSL_KEY_STORE 변수는 ssl 개인키를 보관하는 디렉토리를 가르킵니다.

```
[root@web1 root]# cd $SSL_KEY_STORE
[root@web1 ssl]# cp
[서버로그파일저장경로]/error_log rand.dat
[root@web1 ssl]# openssl genrsa -rand rand.dat -
des3 -out ssl2007.key 2048
34523 semi-random bytes loaded
Generating RSA private key, 2048 bit long modulus
.................................++++++
.......++++++
e is 65537 (0x10001)
Enter pass phrase for ssl2007.key: ******
Verifying - Enter pass phrase for ssl2007.key:
******
[root@web1 ssl]#
```

패스워드를 설정하라는 메시지가 나오면 원하는 패스워드를 입력합니다. 이 패스워드는 나중에 인증서를 설치할 때 필요하므로 반드시 기억해두셔야 합니다.

입력을 마치면 2048 비트 RSA 키가 생성되어 ssl2007.key 라는 이름으로 저장됩니다.
ssl2007.key 는 다른 적당한 이름으로 바꾸어도 무방합니다.

4. 개인키 확인

- 위의 작업과 계속 연관된 작업을 진행합니다.

```
[root@web1 ssl]# openssl rsa -noout -text -in
ssl2007.key
Enter pass phrase for ssl.key: ******
Private-Key: (2048 bit)
modulus:
    00:da:bf:f3:39:d7:c6:1f:bd:6f:a7:b8:aa:67:f2:
...
coefficient:
    6b:26:51:9e:fb:77:cf:7e:d4:2a:a6:d2:7f:21:fa:
    42:e4:7c:54:2e:5e:e9:fb:03:a6:25:d0:6a:fc:e9:
    e1:1b:45:82:61:c0:35:a9:50:25:0a:75:2a:f8:cc:
    87:10:30:9d:bd:36:8e:4b:f6:55:0d:08:30:e8:55:
    e4:00:3b:ec
[root@web1 ssl]#
```

패스워드를 입력하라는 메시지가 나오면 개인키에 설정한 패스워드를 입력합니다.
그러면 위와 같이 생성된 개인키를 확인할 수 있습니다.

5. CSR 생성

인증서를 신청하기 위한 정보를 입력합니다.
<주의사항>과 <입력예>를 반드시 읽어주시고 이에 따라서 정보를 입력하시기 바랍니다.

<주의사항>

1. Organization(영문회사명)에는 < > ~ ! @ # $ % ^ * / \ ( ) ? 등의 특수 문자를 넣을 수 없습니다. 사업자 등록증에 기재된 회사명과 일치하는 영문회사명을 넣어 주시기 바랍니다. (예: 사업자 등록증에 '코모도 코리아'이면 comodo korea 으로 넣어주셔야 합니다. comodo 만 넣으시면 않됩니다.) 또한, 인증서를 설치할 Common Name(인증 받을 도메인 주소)에 해당하는
도메인의 등록정보를 반드시 참조하셔서 해당 등록정보에 기재된 회사명을 참고 하실 수 있겠습니다.
영문 회사명은 소유하고 계신 도메인이 com/net/org 인 경우에는 Network Solutions 에서, kr 인 경우에는 KRNIC 에서 확인할 수 있습니다.

2/ Common Name(인증 받을 도메인 주소)에는 IP 주소, 포트번호, 경로명,

http:// 등을 포함할 수 없습니다.
③ 정보입력 과정에서 마지막에 나오는 Extra Attributes, 즉 A challenge password 와 An optional company name 은 입력하지 마시고 Enter 키만 눌러주셔야 합니다. 두 항목에 내용을 입력하실 경우 잘못된 CSR 이 생성될 수 있습니다.

<입력 예>

Country Name (국가코드) : KR
State or Province Name (시/도) : Seoul
Locality Name (구/군) : Songpa
Organization Name (회사명) : comodokor
Organizational Unit Name (부서명) : Digital Certificate Team
Common Name (인증 받을 도메인 주소) : 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 : Comodokorea

- 위의 작업과 계속 연관된 작업을 진행합니다.

```
[root@web1 ssl]# openssl req -new -key
ssl2007.key -out ssl2007.csr
Enter pass phrase for ssl.key: ******
...
Country Name (2 letter code) [KR]:kr
State or Province Name (full name)
[Berkshire]:Seoul
Locality Name (eg, city) [Newbury]:Songpa
Organization Name (eg, company) [My Company
Ltd]:Comodo Korea
Organizational Unit Name (eg, section) []:Digital
Certificate Team
Common Name (eg, your name or your server's
hostname) []: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 []:comodo
[root@web1 ssl]#
```

(개인키 파일인 ssl2007.key 로부터 CSR 파일인 ssl2007.csr 이 생성됩니다. ssl2007.csr 은 다른 이름으로 바꾸어도 됩니다.)

6. CSR 확인

- 위의 작업과 계속 연관된 작업을 진행합니다.

```
▣
[root@web1 ssl]# openssl req -noout -text -in
ssl2007.csr
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=kr, ST=Seoul, L=Songpa,
O=Company name,
        OU=Digital Certificate Team,
CN=www.comodokorea.co.kr
...
[root@web1 ssl]#
```

생성된 CSR 파일을 확인해 볼 수 있습니다.

7. 개인키 백업

- 위의 작업과 계속 연관된 작업을 진행합니다.

```
▣
[root@web1 ssl]# cp ssl2007.key /root/ssl2007.key
[root@web1 ssl]# sftp xxx.xx.xx.xx
> put ssl2007.key
```

안전한 곳에 개인키를 백업 복사를 해 놓습니다.
※ 개인키(ssl.key)파일과 패스워드는 결코 잃어버리시면 안 됩니다. 안전한 장소 에 백업해두시기 바랍니다.

8. 코모도코리아에 CSR 접수

생성된 CSR 파일을 출력해보면 다음과 같은 base64 형식의 문서를 볼 수 있습니다.
- 위의 작업과 계속 연관된 작업을 진행합니다.

```
[root@web1 ssl]# cat ssl2007.csr
-----BEGIN NEW CERTIFICATE REQUEST-----
MIISDOIUlkmlsRRlkSllskjauASKJlalOSISLKjwBgNV
BAgTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBU
b3duMRQwEgYDVQQKEwtPcHBvcnR1bmlOaTEYMBYGA1UE
CxMPT25saW5lIFNlcnZpY2VzMRowGAYDVQQDExF3d3cu
Zm9yd2FyZC5jby56YTBaMA0GCSqGSIb3DQEBAQUAAAkl
mLKSuljSOIjsfBWu5WLHD/G4BJ+PobiC9d7S6pDvAjuy
C+dPAnLOd91tXdm2j19OD1kgDoSp5ZyGSgwJh2V7diuu
PlHDAgEDoAAwDQYJKoZIhvcNAQEEBQADQQBf8LSLKknl
sklSSLlworrr334ZmXD1AvUjuDPCWzFupReiq7UR8ZOw
JUUsllkfq/IuuIlz6oCq6htdH7/tvKhh
-----END NEW CERTIFICATE REQUEST-----
[root@web1 ssl]#
```

이 CSR 문서를 반드시 첫줄(-----BEGIN CERTIFICATE REQUEST-----)과 끝줄(-----END CERTIFICATE REQUEST-----)이 포함되도록 복사하여 메모장에 붙여넣기 합니다.
이 CSR 을 코모도코리아 메일로 첨부해 주시기 바랍니다.

9. 네트웍 확인 사항 – SSL 적용에 따른 방화벽, L4 switch 설정 확인

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

10. 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 안내해드립니다.