01/08 Apache2 Certification (아파치 인증서)

제목

기관에서 인증서 요청하고 인증 받은 요청서를 웹 사이트에 등록해서 신뢰할 수 있도록 한 거

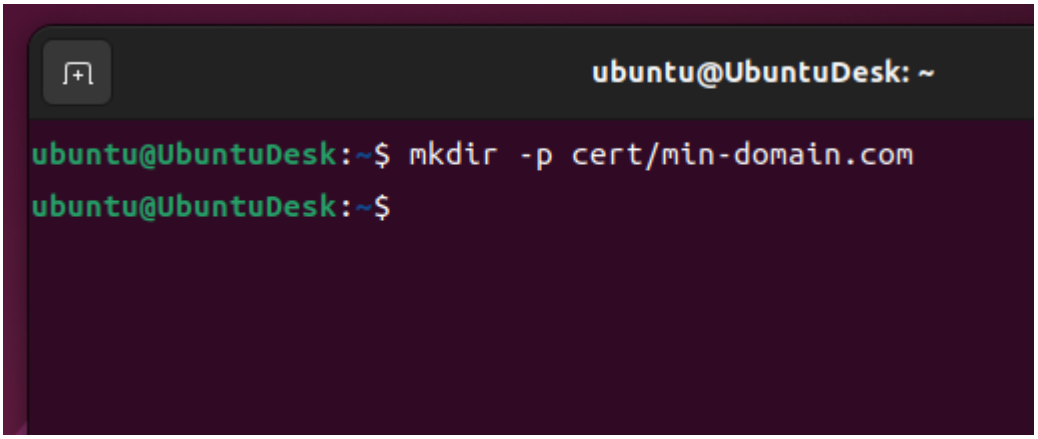
인증서 자체가 잘 동작이 되는지

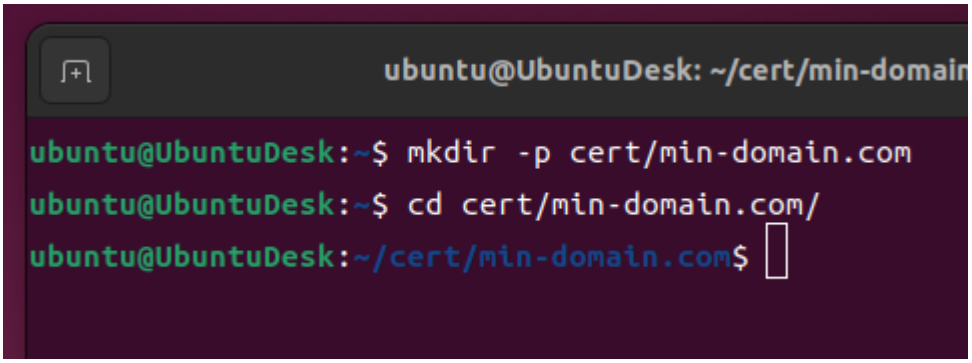
암호화 통신이 잘 되는 지 확인해보는 거

셀프 SIGN 은 기관서에서 해 준것이 아니니까 신뢰할 수 있는지 없는지 확실하지 않기 때문에 경고 표시가 뜨는 거

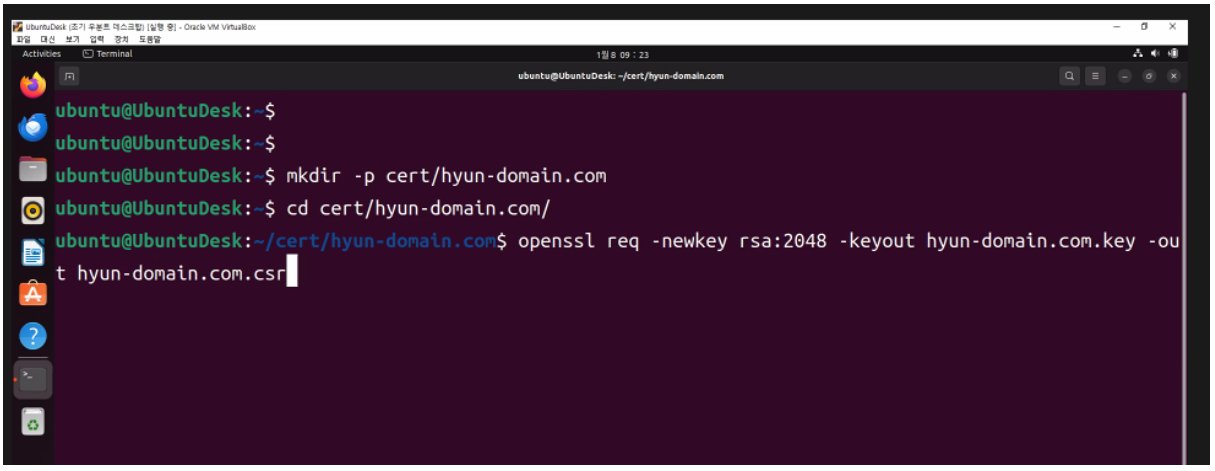
인증서 자체가 나의 서버에서 잘 작동하는지 알고 싶으면 셀프 사인만으로도 충분해

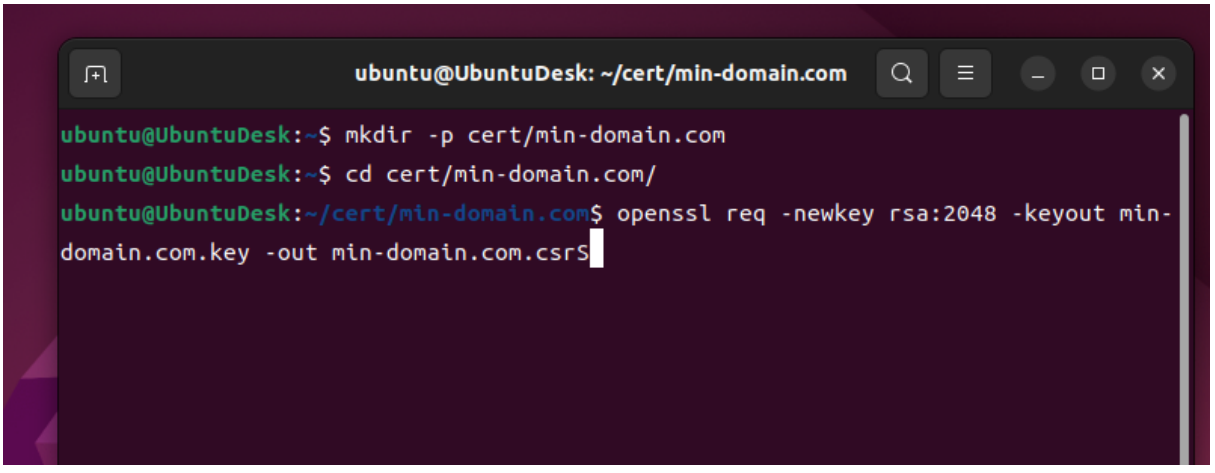
우분투에서 어떻게 하는 거

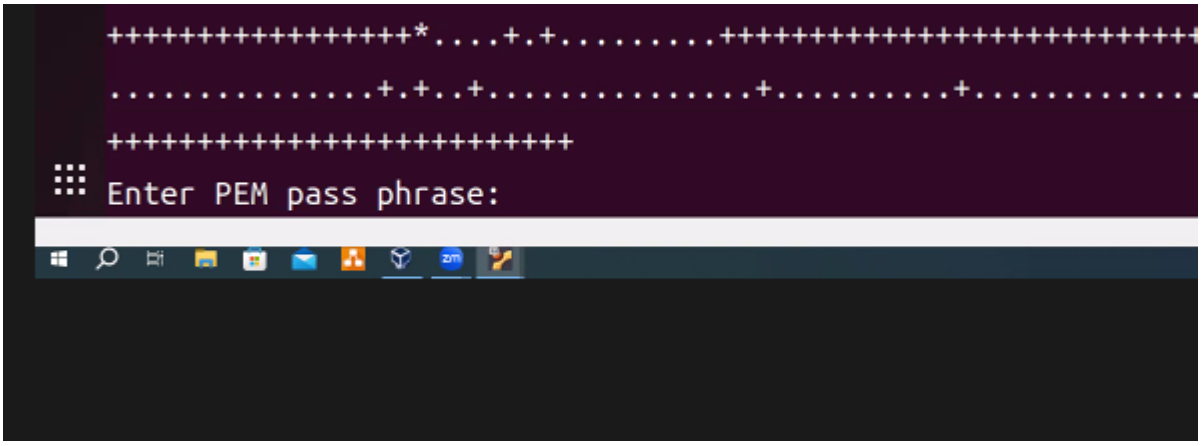



ubuntu@UbuntuDesk: ~/cert/min-domain
ubuntu@UbuntuDesk:~$ mkdir -p cert/min-domain.com
ubuntu@UbuntuDesk:~$ cd cert/min-domain.com/
ubuntu@UbuntuDesk:~/cert/min-domain.com$

‘

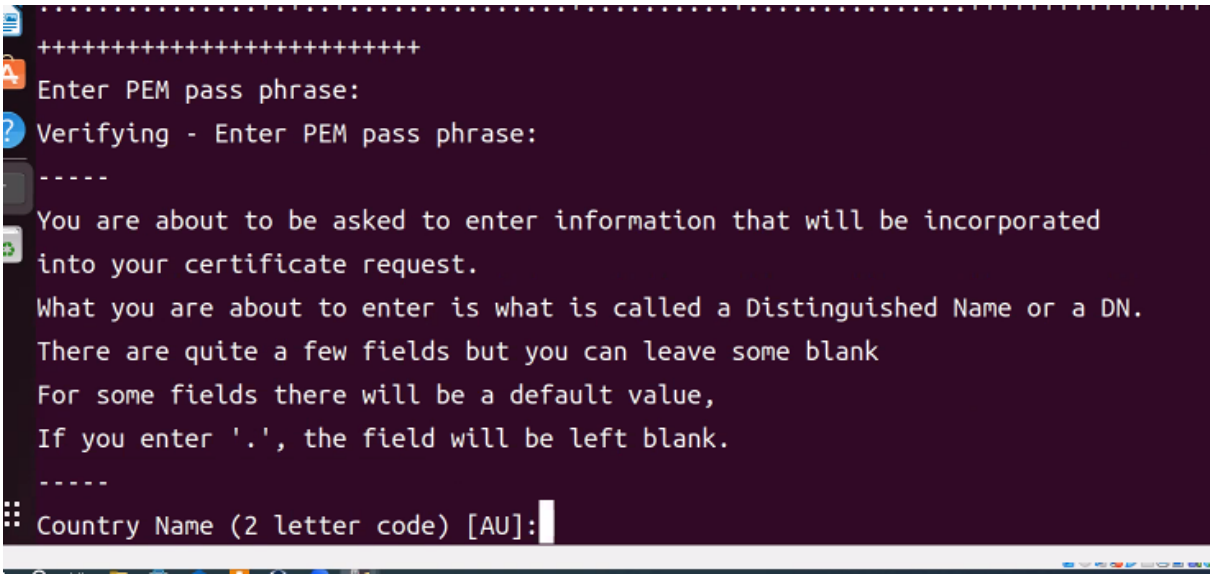

Activities
Terminal
ubuntu@UbuntuDesk: ~/cert/hyun-domain.com
ubuntu@UbuntuDesk:~$
ubuntu@UbuntuDesk:~$
ubuntu@UbuntuDesk:~$ mkdir -p cert/hyun-domain.com
ubuntu@UbuntuDesk:~$ cd cert/hyun-domain.com/
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ openssl req -newkey rsa:2048 -keyout hyun-domain.com.key -ou
t hyun-domain.com.csr


ubuntu@UbuntuDesk: ~/cert/min-domain.com
ubuntu@UbuntuDesk:~$ mkdir -p cert/min-domain.com
ubuntu@UbuntuDesk:~$ cd cert/min-domain.com/
ubuntu@UbuntuDesk:~/cert/min-domain.com$ openssl req -newkey rsa:2048 -keyout min-
domain.com.key -out min-domain.com.csr$



키에 대한 암호

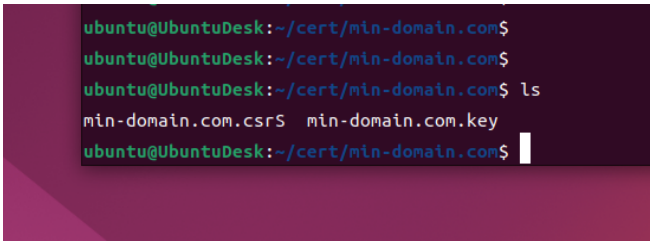
기억하기 쉬운 걸로

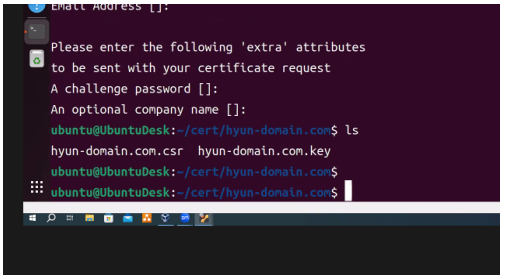


P@ssw0rd

```
+++++++++++++++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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) [AU]:kr
State or Province Name (full name) [Some-State]:seoul
Locality Name (eg, city) []:kangnam
Organization Name (eg, company) [Internet Widgits Pty Ltd]:min-domain
Organizational Unit Name (eg, section) []:web
Common Name (e.g. server FQDN or YOUR name) []:min-domain.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
ubuntu@UbuntuDesk:~/cert/min-domain.com$
```

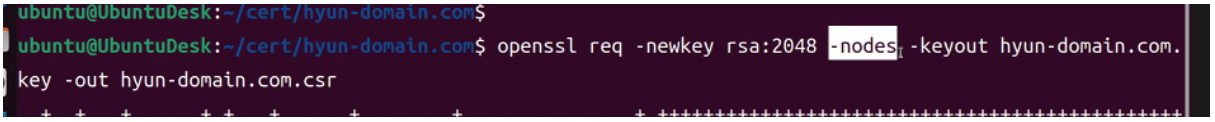
윈도우 서버에서 한 것 처럼 요청서를 만들어 볼게



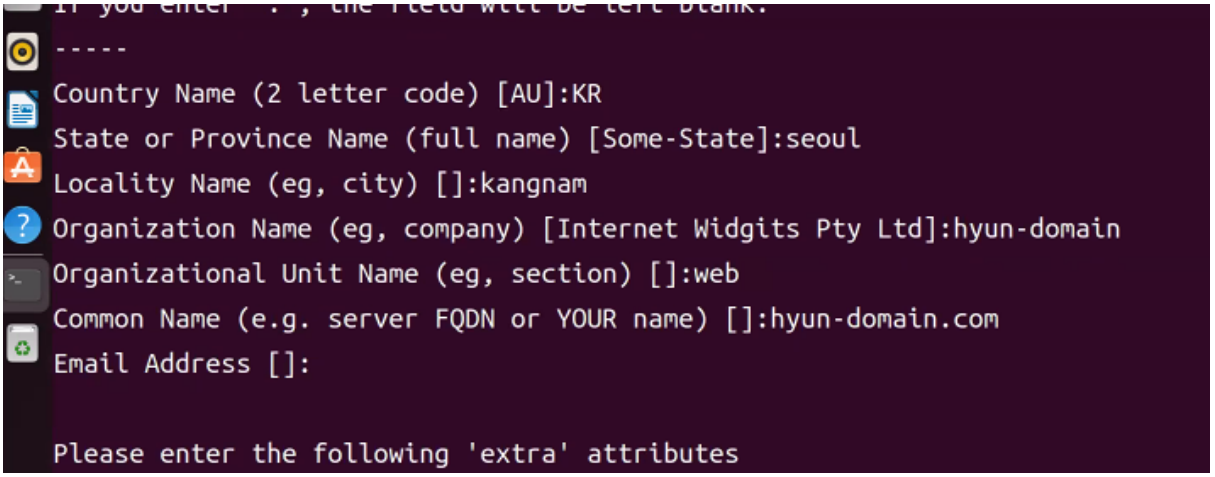


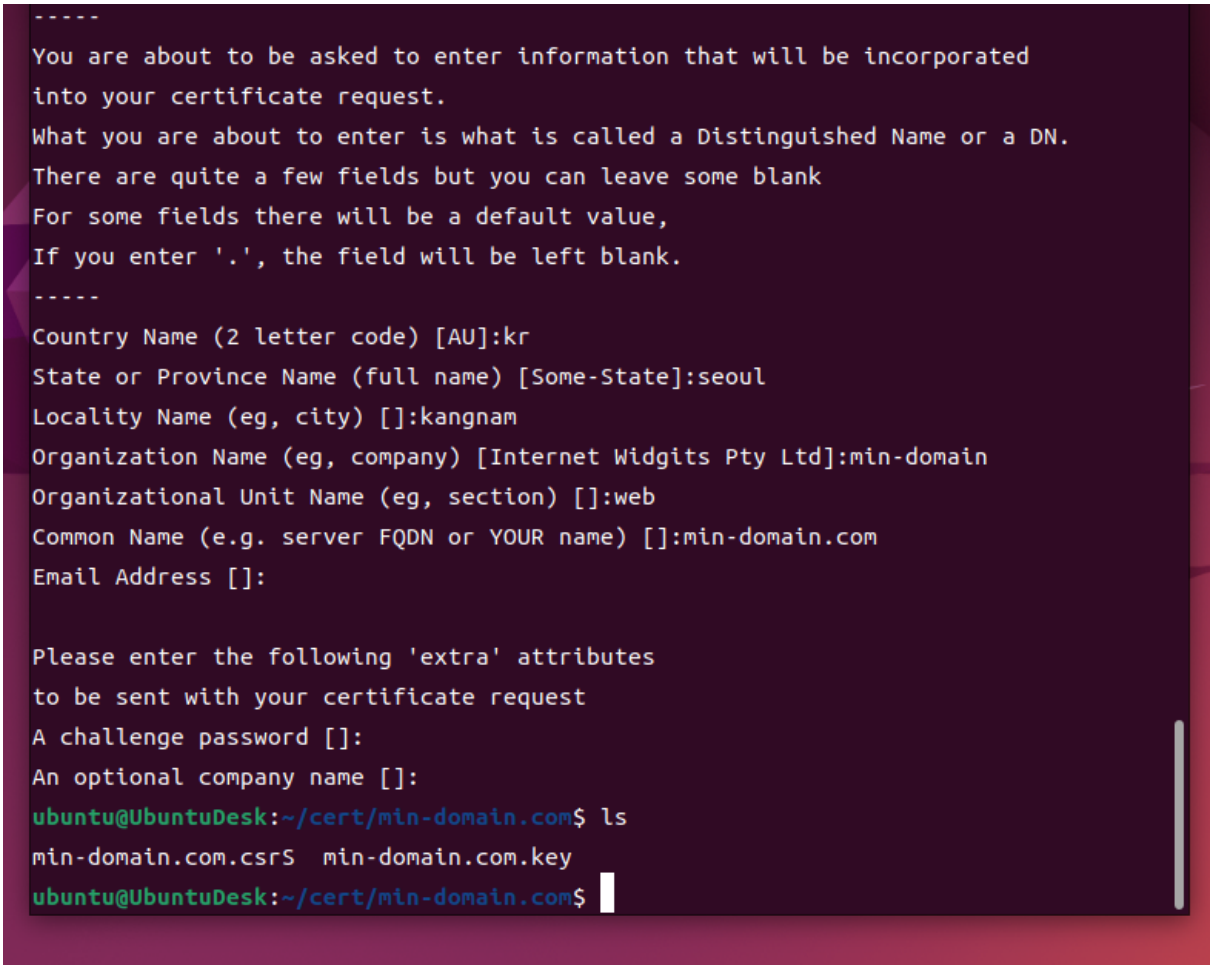
이렇게 디렉토리에 요청서가 들어가있다

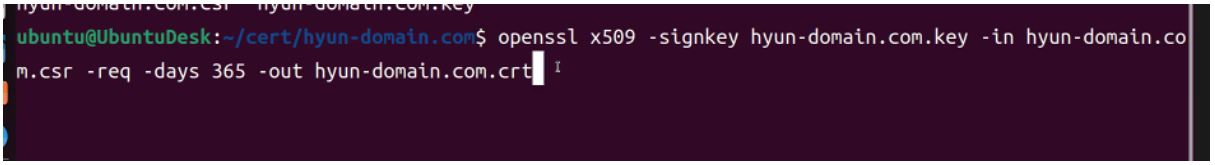
아까 pem pass 물어볼때 만들기 귀찮거나 그러면

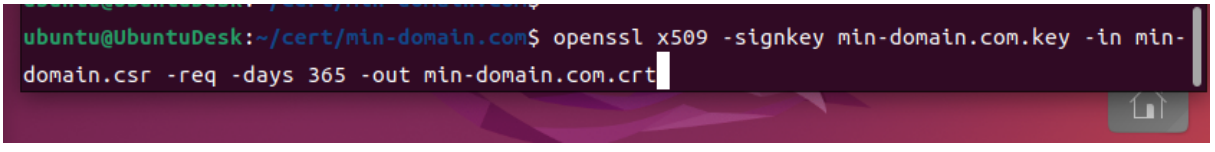


이렇게 -nodes 이렇게 넣으면 된다

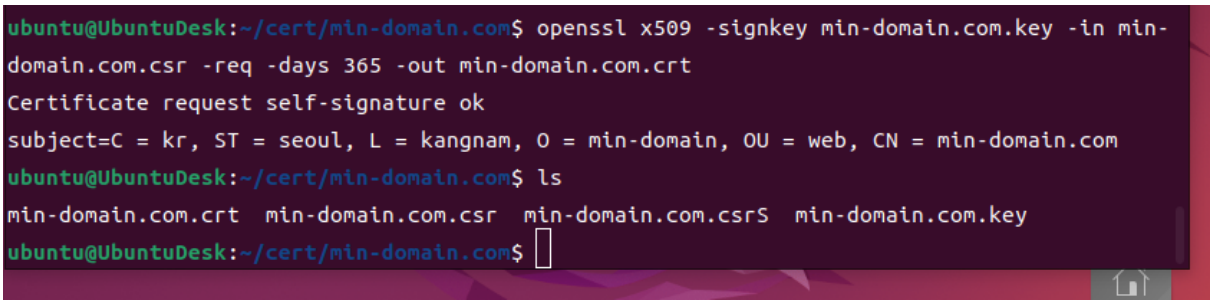


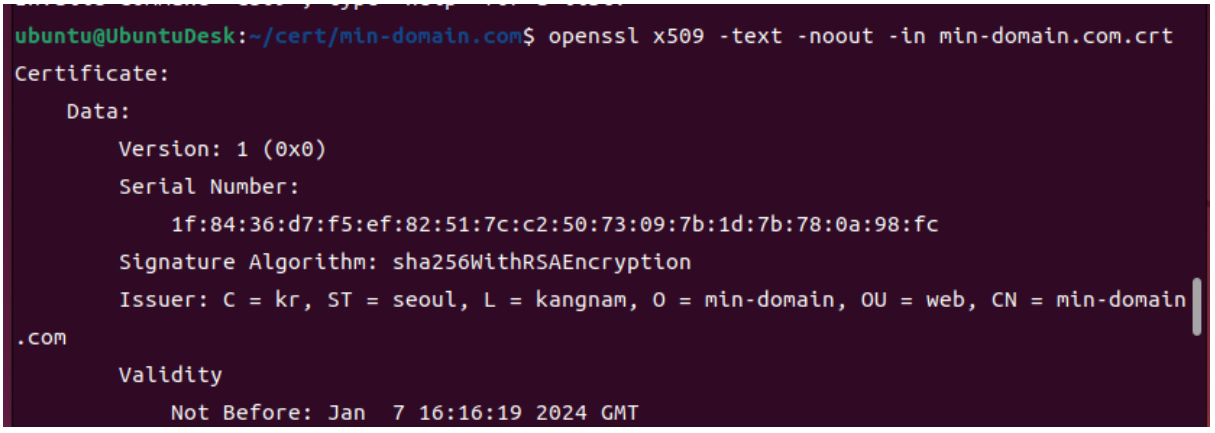






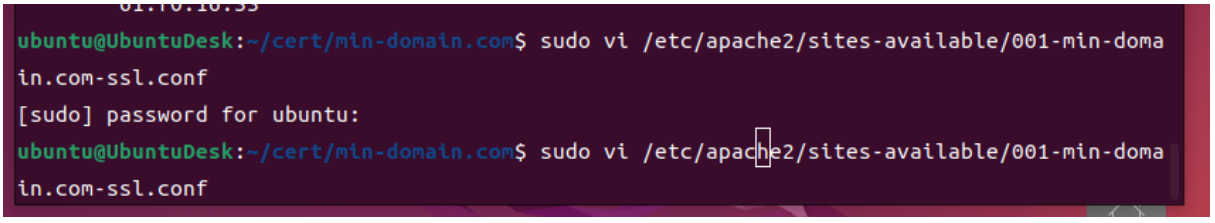
자체 서명된 인증서를 생성하거나, 인증 기관(Certificate Authority, CA)에게 CSR을 제출하여 서명된 인증서를 받아오는 등의 용도로 사용됩니다. 위 명령어를 사용하면 CSR 파일과 개인 키를 기반으로 유효 기간이 365일인 디지털 인증서가 생성

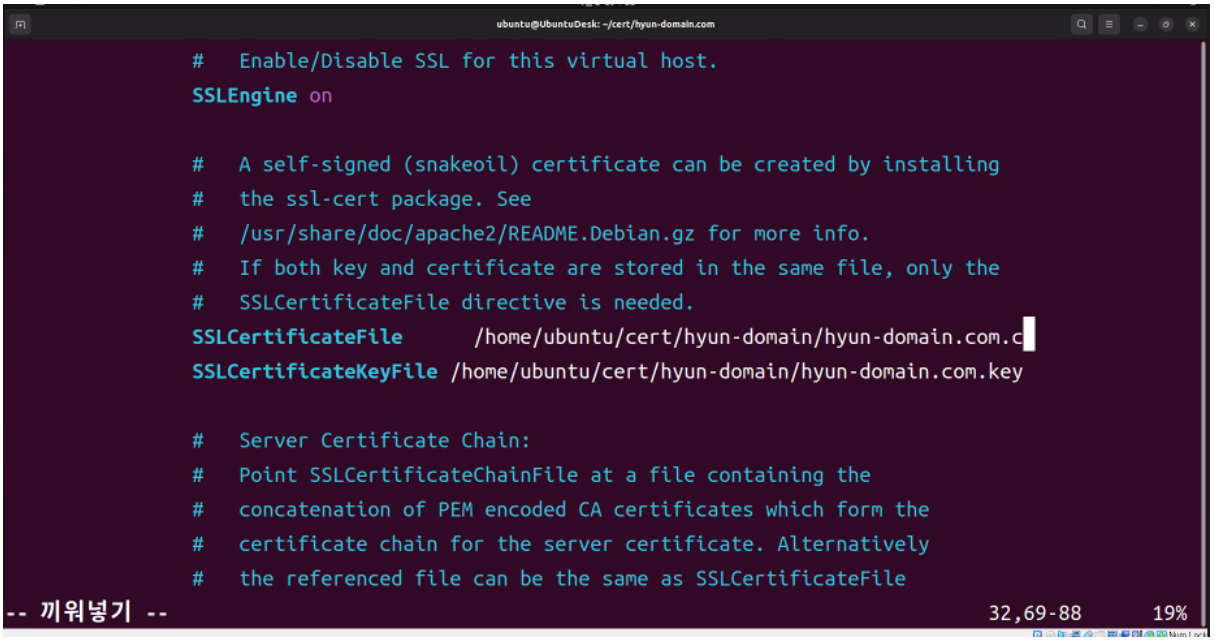





```
openssl x509 -text -noout - in min-domain.com.crt
```

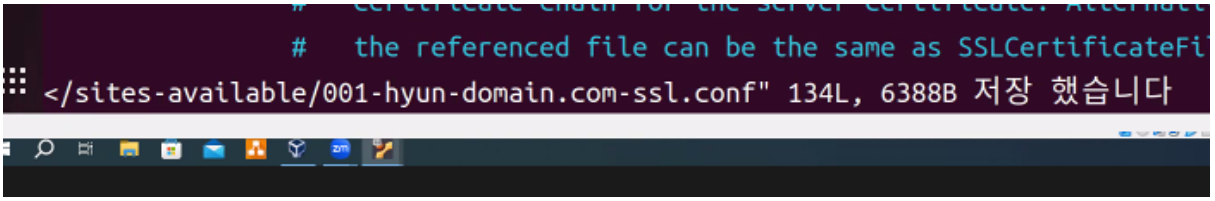
-> OpenSSL을 사용하여 X.509 형식의 SSL 인증서 파일의 내용을 텍스트로 표

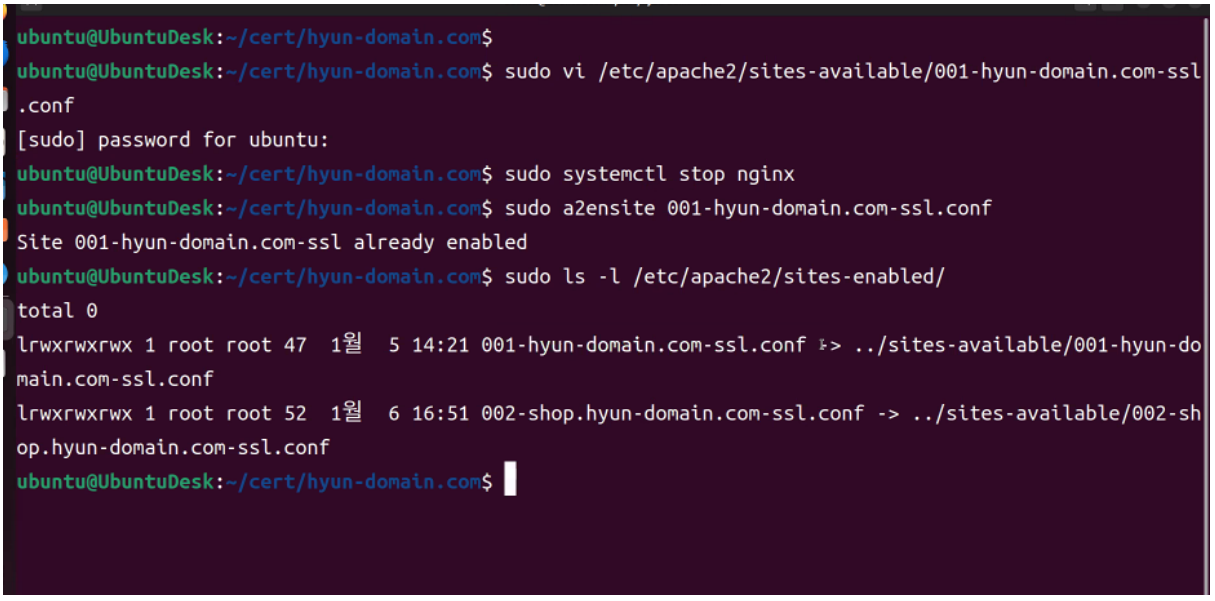


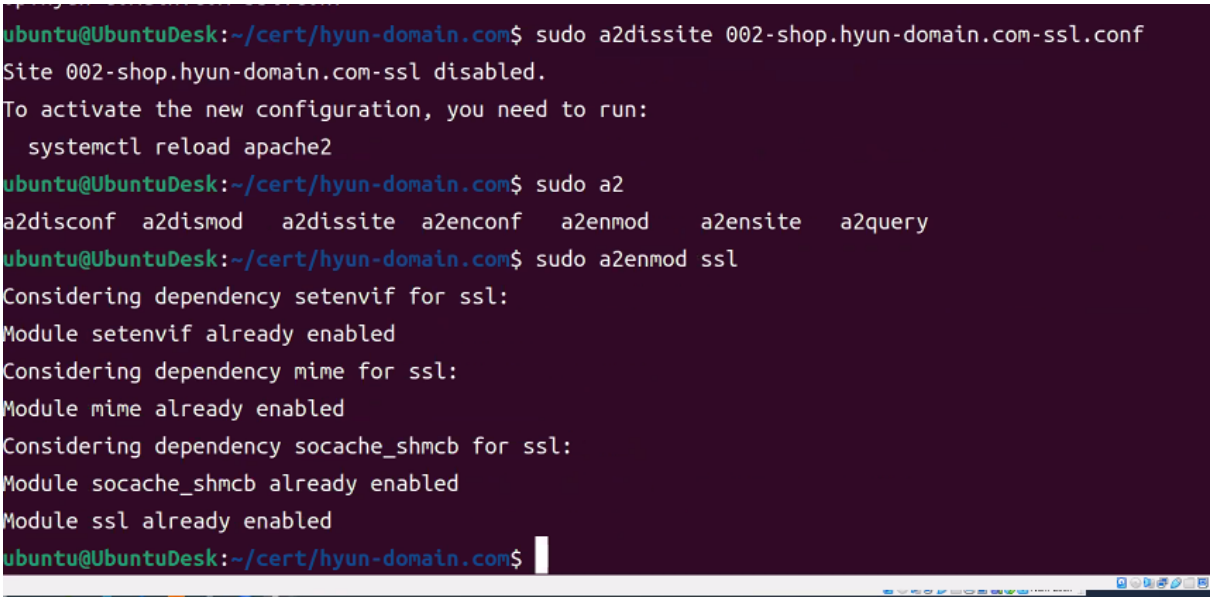


나는 이 파일이 없음

? 해결하셈

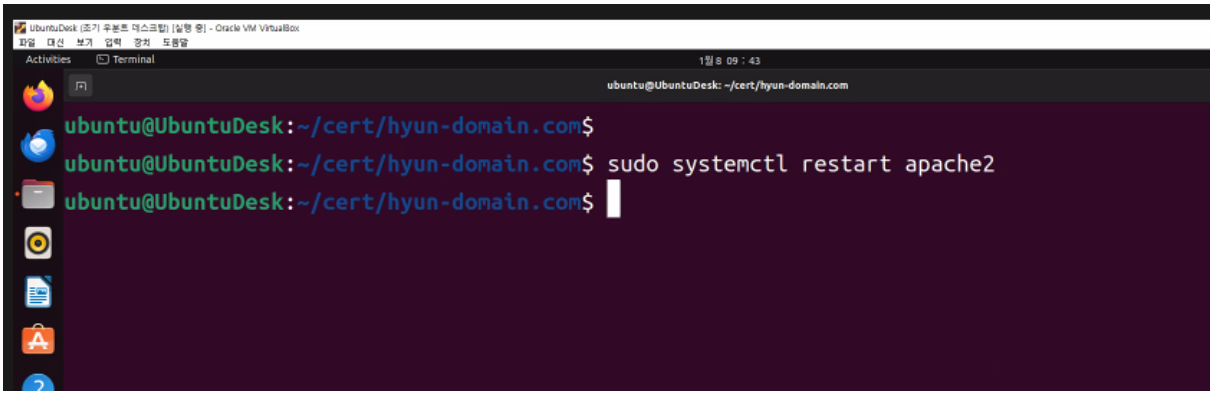


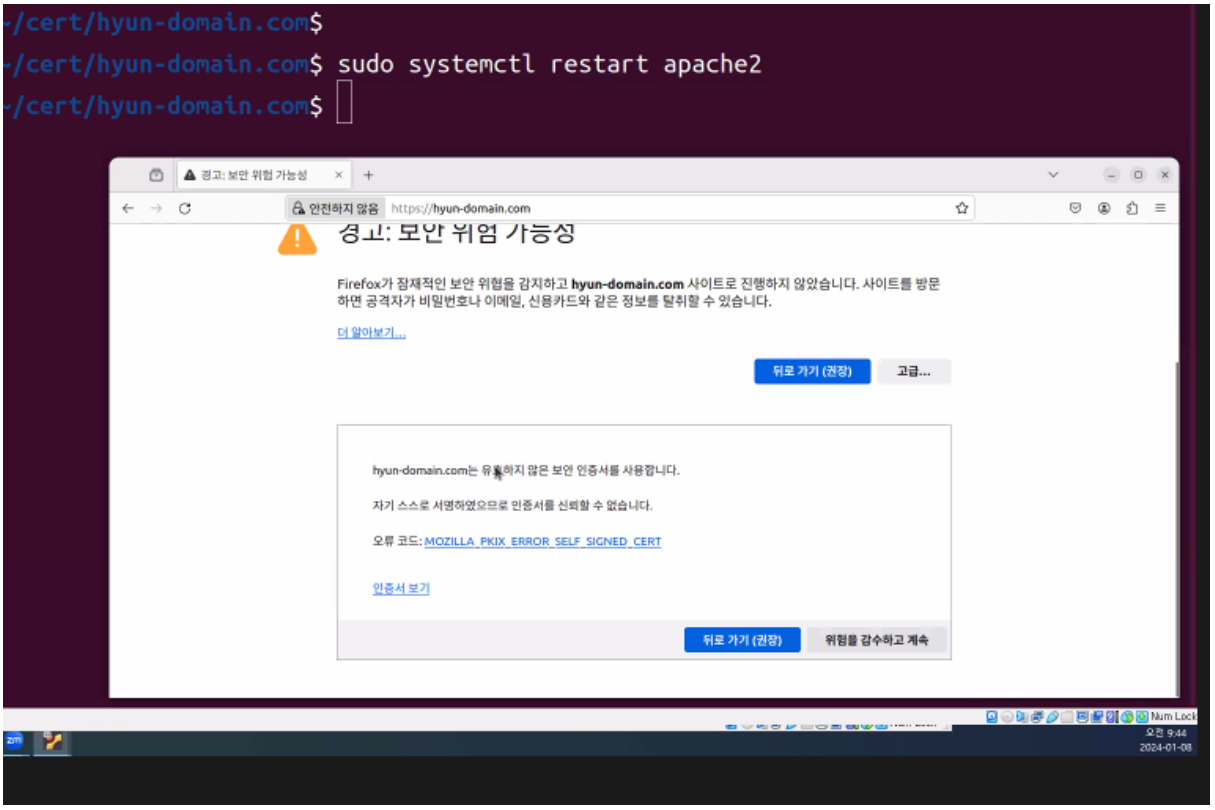

ubuntu@UbuntuDesk:~/cert/hyun-domain.com$
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ sudo vi /etc/apache2/sites-available/001-hyun-domain.com-ssl
.conf
[sudo] password for ubuntu:
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ sudo systemctl stop nginx
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ sudo a2ensite 001-hyun-domain.com-ssl.conf
Site 001-hyun-domain.com-ssl already enabled
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ sudo ls -l /etc/apache2/sites-enabled/
total 0
lrwxrwxrwx 1 root root 47 1월 5 14:21 001-hyun-domain.com-ssl.conf -> ../sites-available/001-hyun-do
main.com-ssl.conf
lrwxrwxrwx 1 root root 52 1월 6 16:51 002-shop.hyun-domain.com-ssl.conf -> ../sites-available/002-sh
op.hyun-domain.com-ssl.conf
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$


ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ sudo a2dissite 002-shop.hyun-domain.com-ssl.conf
Site 002-shop.hyun-domain.com-ssl disabled.
To activate the new configuration, you need to run:
systemctl reload apache2
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ sudo a2
a2disconf a2dismod a2dissite a2enconf a2enmod a2ensite a2query
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$

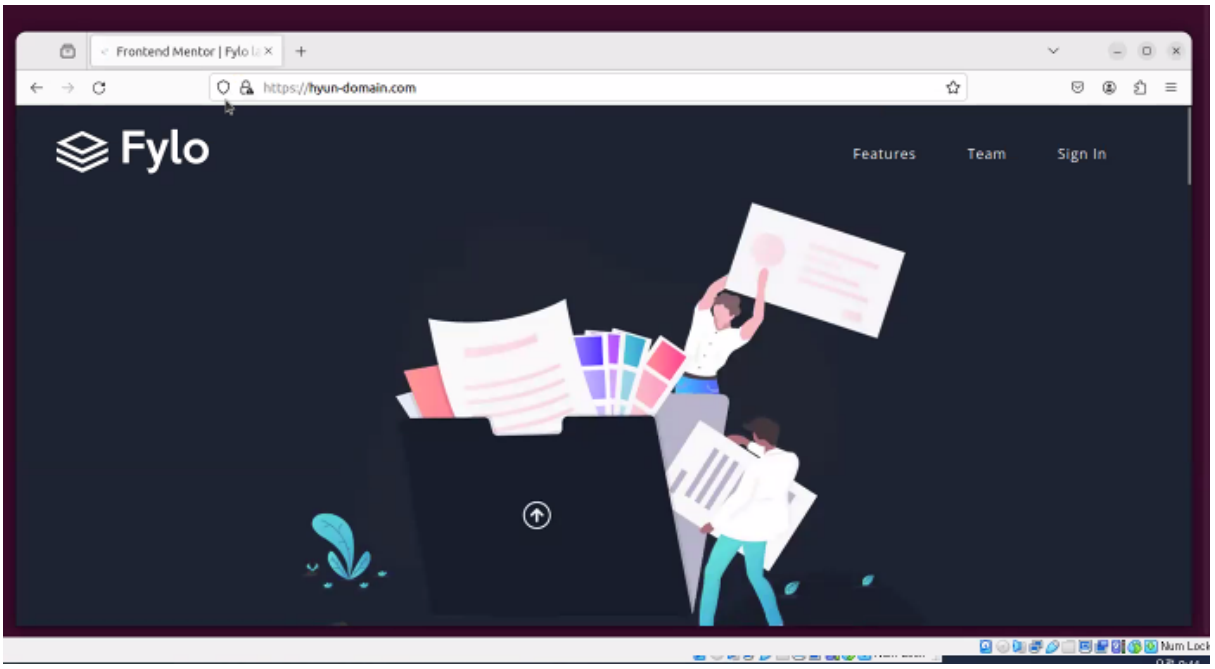
```
#   A self-signed (snakeoil) certificate can be created by installing
#   the ssl-cert package. See
#   /usr/share/doc/apache2/README.Debian.gz for more info.
#   If both key and certificate are stored in the same file, only the
#   SSLCertificateFile directive is needed.
SSLCertificateFile      /home/ubuntu/cert/hyun-domain.com/hyun-domain.com.crt
SSLCertificateKeyFile   /home/ubuntu/cert/hyun-domain.com/hyun-domain.com.key

#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
#   concatenation of PEM encoded CA certificates which form the
#   certificate chain for the server certificate. Alternatively
#   the referenced file can be the same as SSLCertificateFile
#   when the CA certificates are directly appended to the server
#   certificate for convinience.
```

아까 이거 이렇게 수정





이렇게 해서 웹 사이트 들어가 보고 확인하기

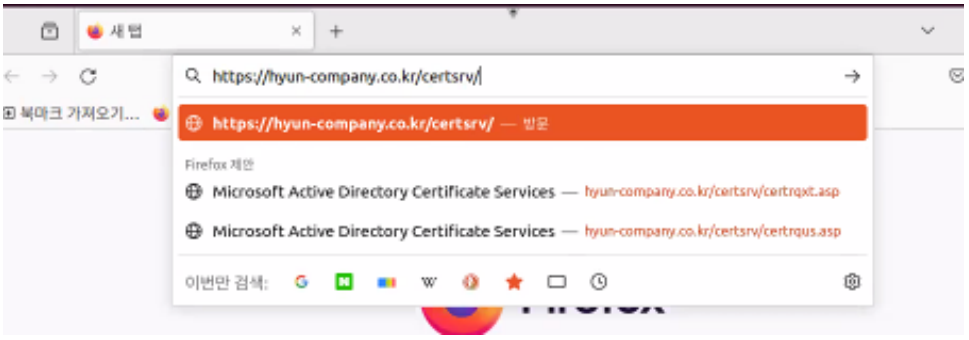


→ 이거 그때 민정님 블로그 보면서 다시 DNS 구성 다시 해보고 이거 해야 함

여기까지가 셀프사인하고 인증서 등록하고 적용하는 거

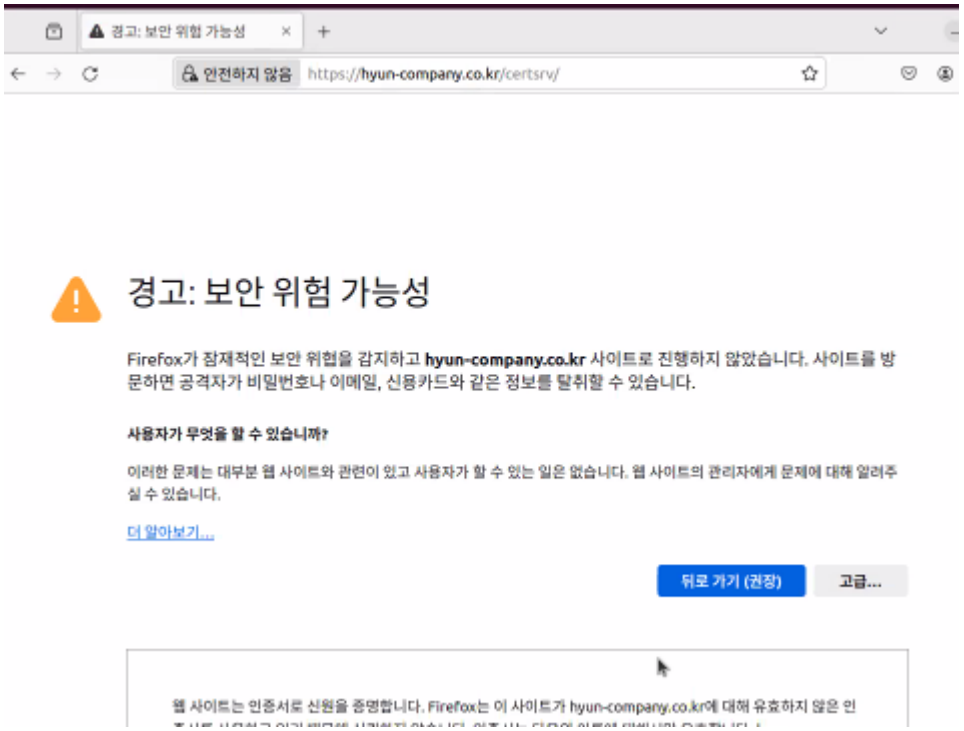
아파치 기준으로 해본 것

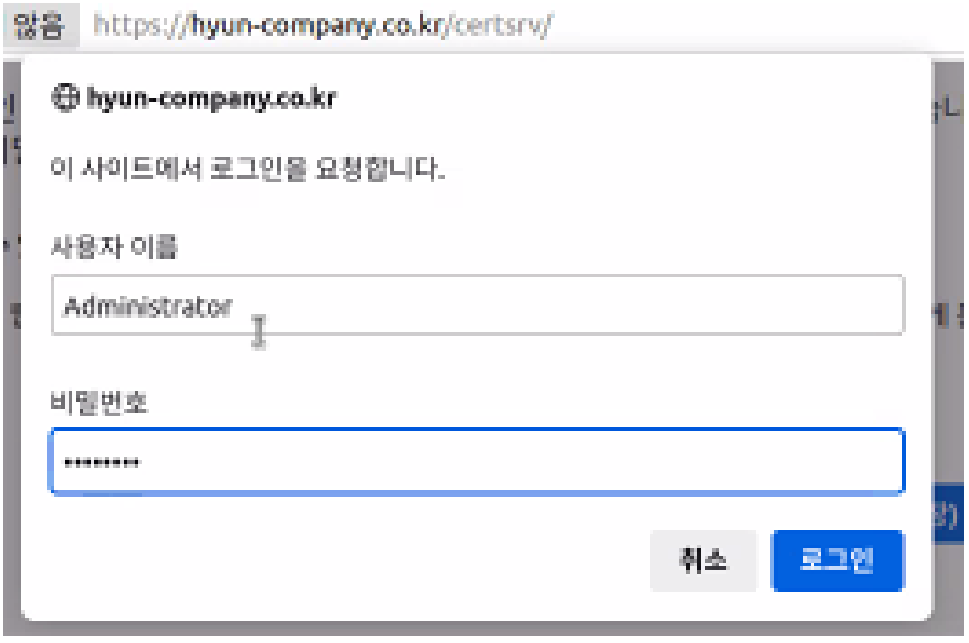
인증 기관을 구성했으니까 요청을 할려고 하면



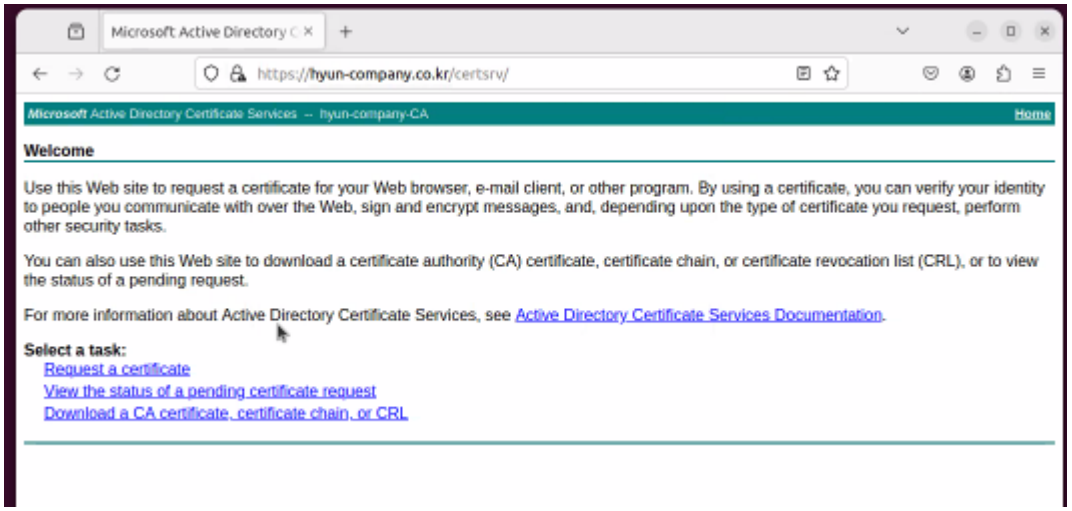
이 주소를 통해서 요청서 전송 가능

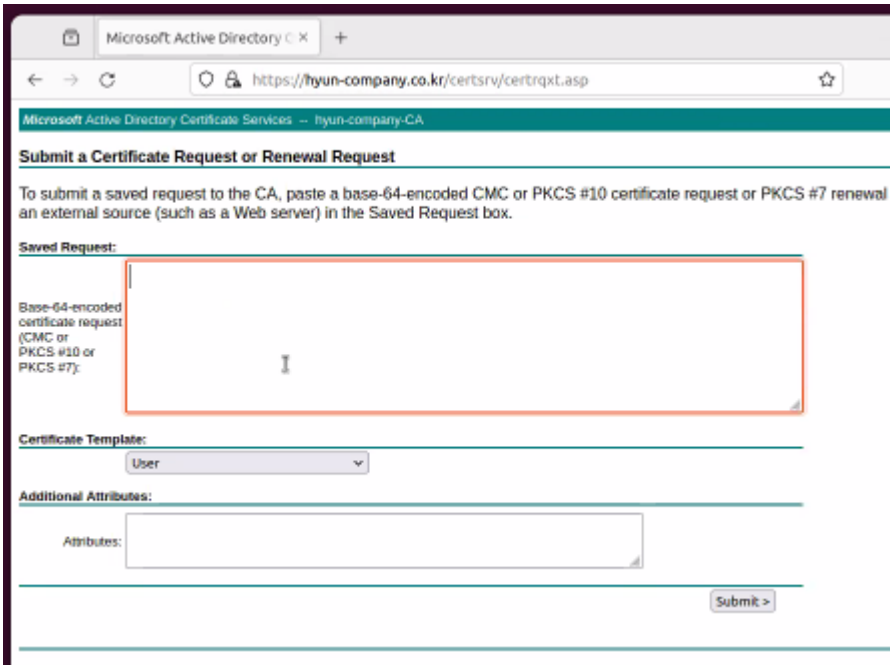
이 앞에 있는 주소는 CA 가 구성되어 있는 주소


경고: 보안 위험 가능성
안전하지 않음
https://hyun-company.co.kr/certsrv/
경고: 보안 위험 가능성
Firefox가 잠재적인 보안 위협을 감지하고 hyun-company.co.kr 사이트로 진행하지 않았습니다. 사이트를 방문하면 공격자가 비밀번호나 이메일, 신용카드와 같은 정보를 탈취할 수 있습니다.
사용자가 무엇을 할 수 있습니까?
이러한 문제는 대부분 웹 사이트와 관련이 있고 사용자가 할 수 있는 일은 없습니다. 웹 사이트의 관리자에게 문제에 대해 알려주실 수 있습니다.
더 알아보기...
뒤로 가기 (권장)
고급...
웹 사이트는 인증서로 신원을 증명합니다. Firefox는 이 사이트가 hyun-company.co.kr에 대해 유효하지 않은 인


않음
https://hyun-company.co.kr/certsrv/
hyun-company.co.kr
이 사이트에서 로그인을 요청합니다.
사용자 이름
Administrator
비밀번호
취소
로그인

→ 인증서 발급 계정

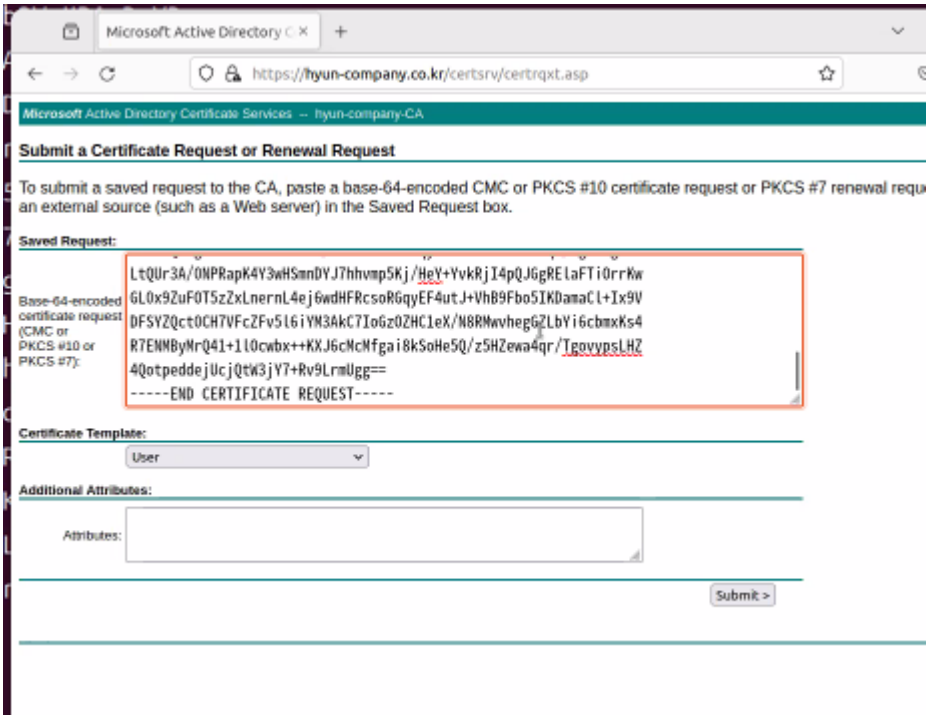

Microsoft Active Directory
https://hyun-company.co.kr/certsrv/
Microsoft Active Directory Certificate Services -- hyun-company-CA
Home
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.
Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL


Microsoft Active Directory
https://hyun-company.co.kr/certsrv/certrqxt.asp
Microsoft Active Directory Certificate Services -- hyun-company-CA
Submit a Certificate Request or Renewal Request
To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal an external source (such as a Web server) in the Saved Request box.
Saved Request:
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):
Certificate Template:
User
Additional Attributes:
Attributes:
Submit >

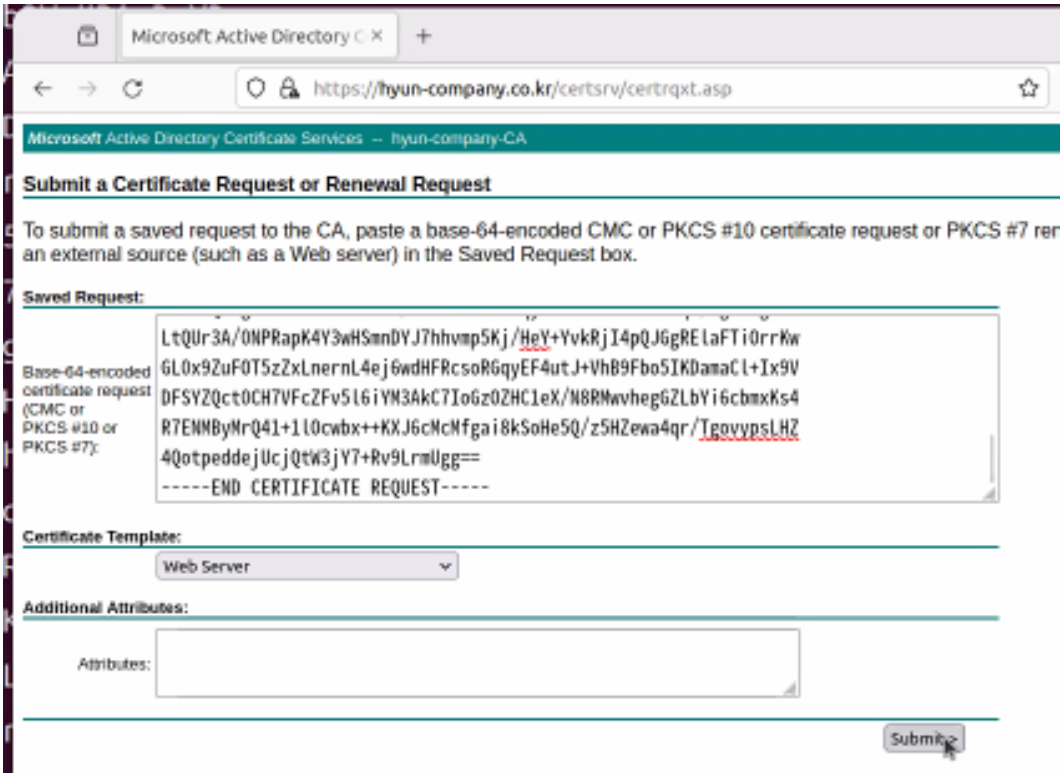
생성한 요청서 인증 파일

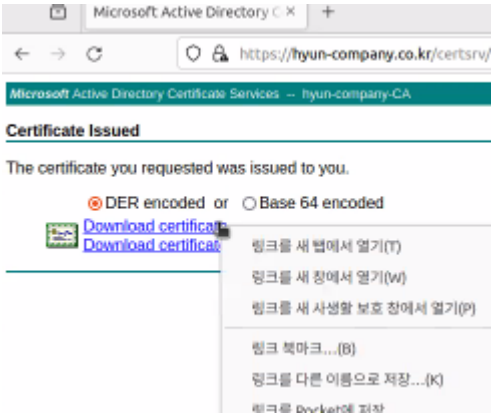
```
ubuntu@UbuntuDesk:~/cert/min-domain.com$ cat min-domain.com.csr
-----BEGIN CERTIFICATE REQUEST-----
MIICsDCCAZgCAQAwazELMAkGA1UEBhMCa3IxDjAMBgNVBAgMBXNlb3VsMRAwDgYD
VQQHDAdrYW5nbmFtMRMwEQYDVQQKDAptaW4tZG9tYWluMQwwCgYDVQQLDAN3ZWIx
FzAVBgNVBAMMDm1pbi1kb21haW4uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA1cNP7lxo8eBqVVbV62F1RVRAWiTba8l4wp/6uwUQU/8VTXBEZ//Z
ijTo0M+by5Gnk56mPEox8psFSAScij3Mpy67o7i8M8jeFVKhJRA3ny2DV0WKCe2m
wFeI73ZhR9RJIK+z7fTY3t1Jn8O/cJ3zlaYoc2dDg5QSyG5bIIwI8VdoA+LDwnza
Vz7l5NdgCTpn7gOVW7dFT56vYcl5L5h7aRzZl1S5yGdY9MA7DUkZDel5zE+mKH81
m3fflGKHmYegeMqjfppYy0645R9cfMh4Lyo6a4ZsOGibUsrmeFVUNUQcq8raUkv0
E8boMKfhf0ttPqM3qKiIq/5dmd0o+CyDowIDAQABoAAwDQYJKoZIhvcNAQELBQAD
ggEBAEgdibDg3t7iHFogQ7Y+z5Cx96lvhOZVRlNMcvPbkgyxHEO15vNcgx6UJ27W
n2nyNimhx7a7hRzTc5CDGSn9IBreu58xD/LINu0N4b2AJbbWLEdB194mr+jNbqzP
EDpkYsFBVyP1A8K+b7JV3PrKsmbOOVKCy+nBTTVZotG+caC+ZN2JF6MjSPy6qoXB
agtwDZv/A5MOSTctf9aVKVWWv6yRhsDac0p6MNm1OO6ZHxMwYnCpCyAw/Y6SqQdH
J2ezl7zO6U+8ipDuG/fPE0gQXl0dynAa1oIIsboDWZ/ZRCncpg3OslzW3jXH+Wgv
6pIV5j6LEjphCkWW6osu+6nXIyw=
-----END CERTIFICATE REQUEST-----
ubuntu@UbuntuDesk:~/cert/min-domain.com$
```

이 내용 전체 복붙해서



여기에 넣으면 되는 거

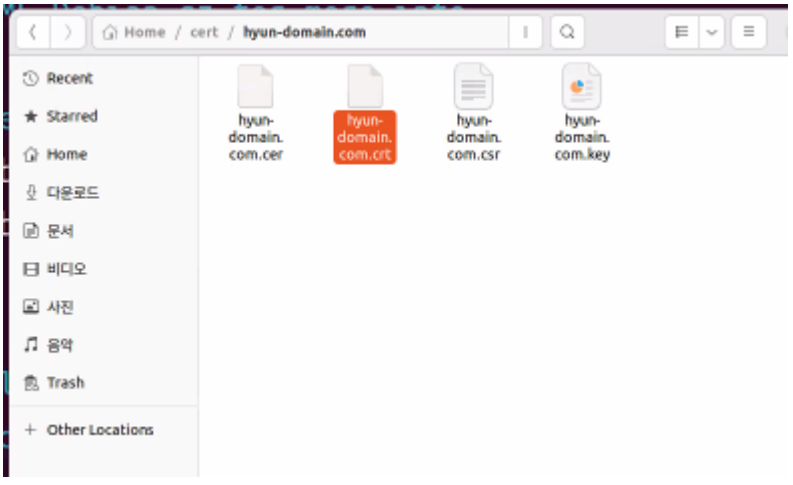

Microsoft Active Directory
https://hyun-company.co.kr/certsrv/certrqxt.asp
Microsoft Active Directory Certificate Services -- hyun-company-CA
Submit a Certificate Request or Renewal Request
To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 ren
an external source (such as a Web server) in the Saved Request box.
Saved Request:
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):
LtQUr3A/ONPRapK4Y3wHSmnDYJ7hhvmp5Kj/HeY+YvkRjI4pQJGgRElaFTiOrrKw
GLOx9ZuFOT5zZxLnernL4ej6wdHFRcsoRGqyEF4utJ+VhB9Fbo5IKDamaCl+Ix9V
DFSYZQctOCH7VFcZFv5l6iYN3AkC7IoGzOZHC1eX/N8RMwvhegGZLbYi6cbmxKs4
R7ENMByMrQ41+1lOcwbx++KXJ6cMcNfgai8kSoHe5Q/z5HZewa4qr/TgovypsLHZ
4QotpeddejUcjQtW3jY7+Rv9LrmUgg==
-----END CERTIFICATE REQUEST-----
Certificate Template:
Web Server
Additional Attributes:
Attributes:
Submit

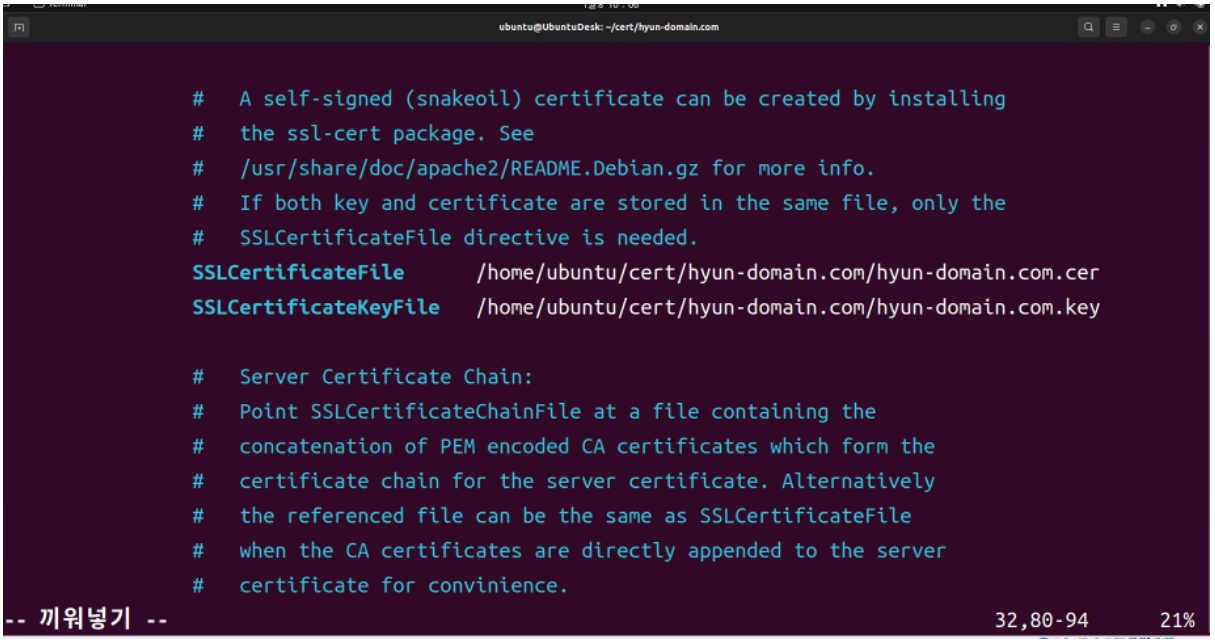

Microsoft Active Directory
https://hyun-company.co.kr/certsrv/
Microsoft Active Directory Certificate Services -- hyun-company-CA
Certificate Issued
The certificate you requested was issued to you.
DER encoded or Base 64 encoded
Download certificate
Download certificate
링크를 새 탭에서 열기(T)
링크를 새 창에서 열기(W)
링크를 새 사생활 보호 창에서 열기(P)
링크 북마크...(B)
링크를 다른 이름으로 저장...(K)

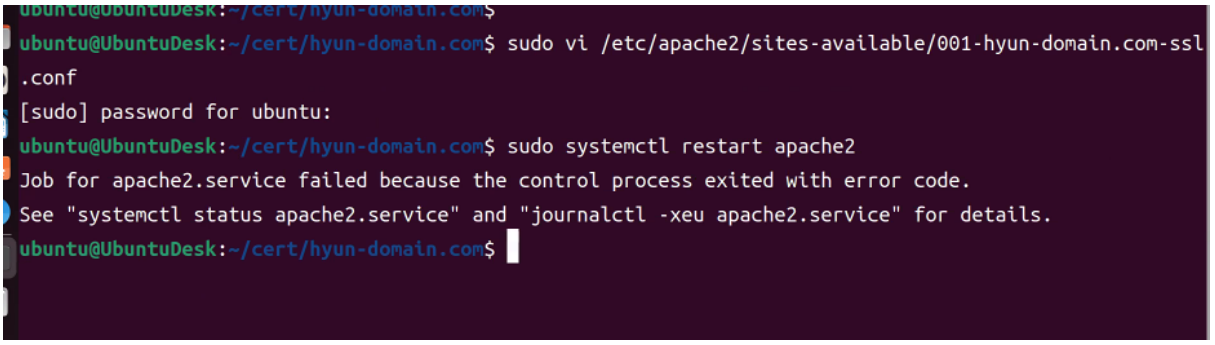
```
ory
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ mv ~/다운로드/certnew.cer ./hyun-domain.com.cer
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$
```

```
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ mv ~/다운로드/certnew.cer ./hyun-domain.com.cer
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ ls
hyun-domain.com.cer  hyun-domain.com.crt  hyun-domain.com.csr  hyun-domain.com.key
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ openssl x509 -text -noout -in hyun-domain.com.cer
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            12:00:00:00:07:53:fb:56:90:29:10:b8:da:00:00:00:00:00:07
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC = kr, DC = co, DC = hyun-company, CN = hyun-company-CA
        Validity
```

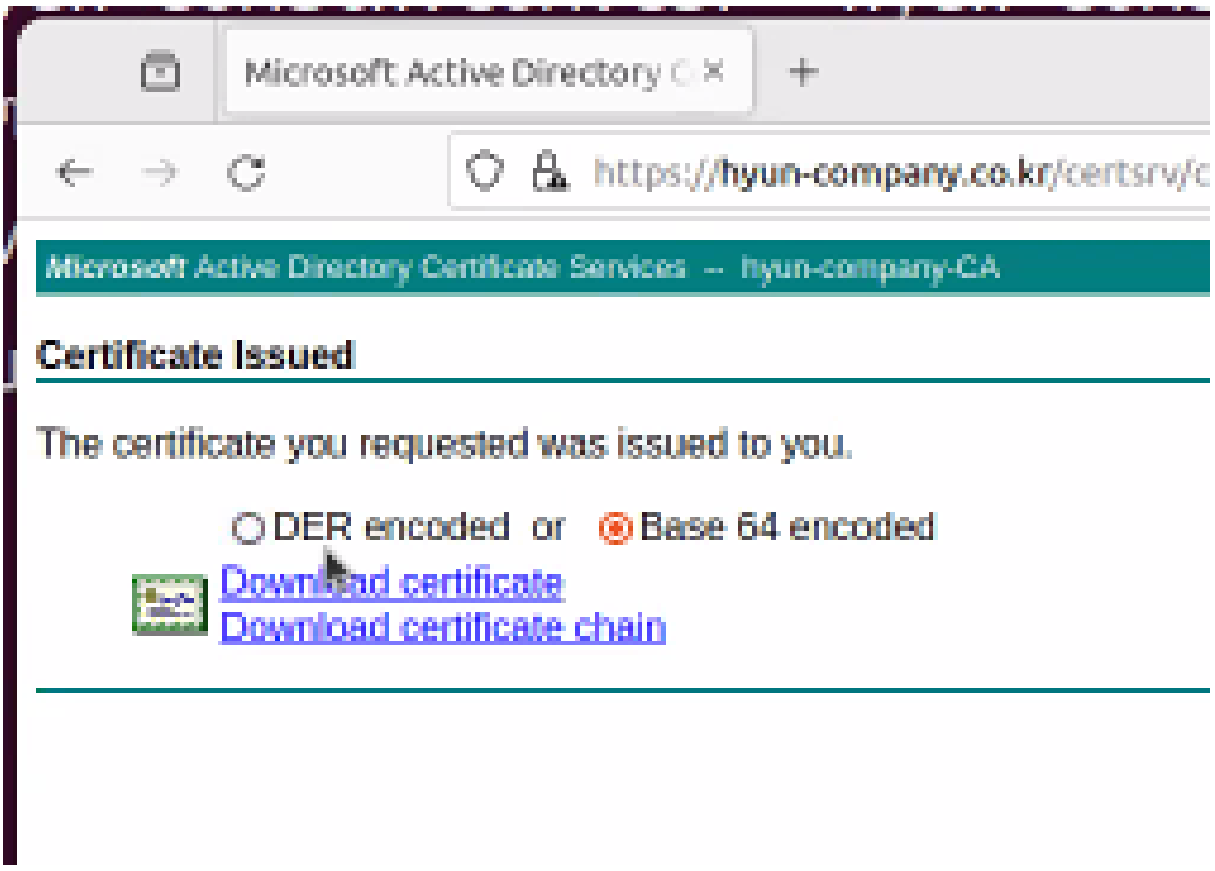
issuer 발급자 정보도 보임




ubuntu@UbuntuDesk: ~/cert/hyun-domain.com
A self-signed (snakeoil) certificate can be created by installing
the ssl-cert package. See
/usr/share/doc/apache2/README.Debian.gz for more info.
If both key and certificate are stored in the same file, only the
SSLCertificateFile directive is needed.
SSLCertificateFile   /home/ubuntu/cert/hyun-domain.com/hyun-domain.com.cer
SSLCertificateKeyFile   /home/ubuntu/cert/hyun-domain.com/hyun-domain.com.key
Server Certificate Chain:
Point SSLCertificateChainFile at a file containing the
concatenation of PEM encoded CA certificates which form the
certificate chain for the server certificate. Alternatively
the referenced file can be the same as SSLCertificateFile
when the CA certificates are directly appended to the server
certificate for convinience.
-- 끼워넣기 --
32,80-94
21%

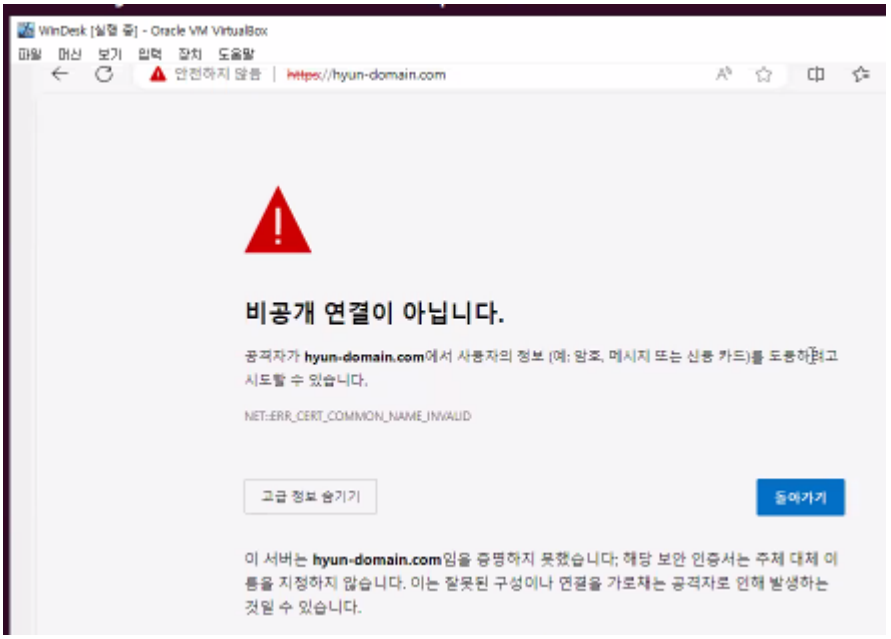

ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ sudo vi /etc/apache2/sites-available/001-hyun-domain.com-ssl
.conf
[sudo] password for ubuntu:
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ sudo systemctl restart apache2
Job for apache2.service failed because the control process exited with error code.
See "systemctl status apache2.service" and "journalctl -xeu apache2.service" for details.
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$


hyun-domain.com.cer hyun-domain.com.crt hyun-domain.com.csr hyun-domain.com.key
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ rm hyun-domain.com.cer
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ mv ~/다운로드/certnew.cer ./hyun-domain.com.cer
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ sudo systemctl restart apache2
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$

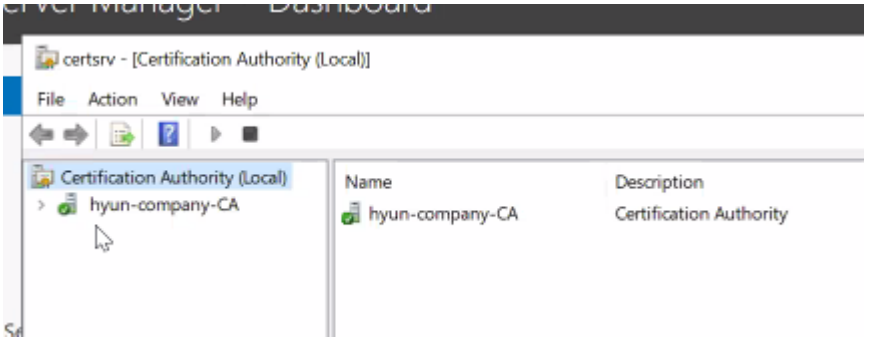


우분투에서 다운로드 받을 때에는 base 63 encoded 이걸로 받기

윈도우 데스크탑 가서 해보면 이렇게 떠야 함

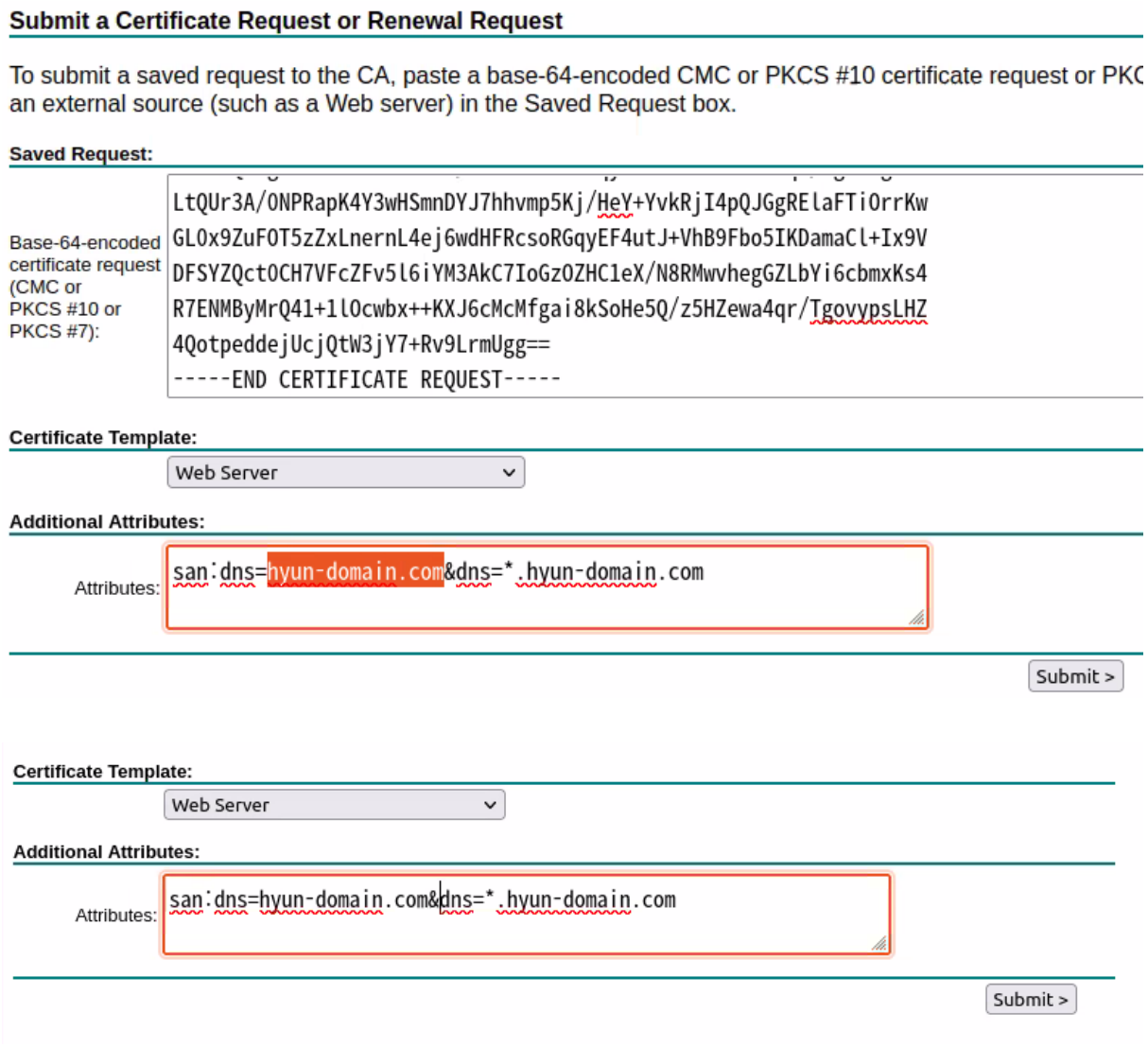


윈도우 서버에서 이거 해주고

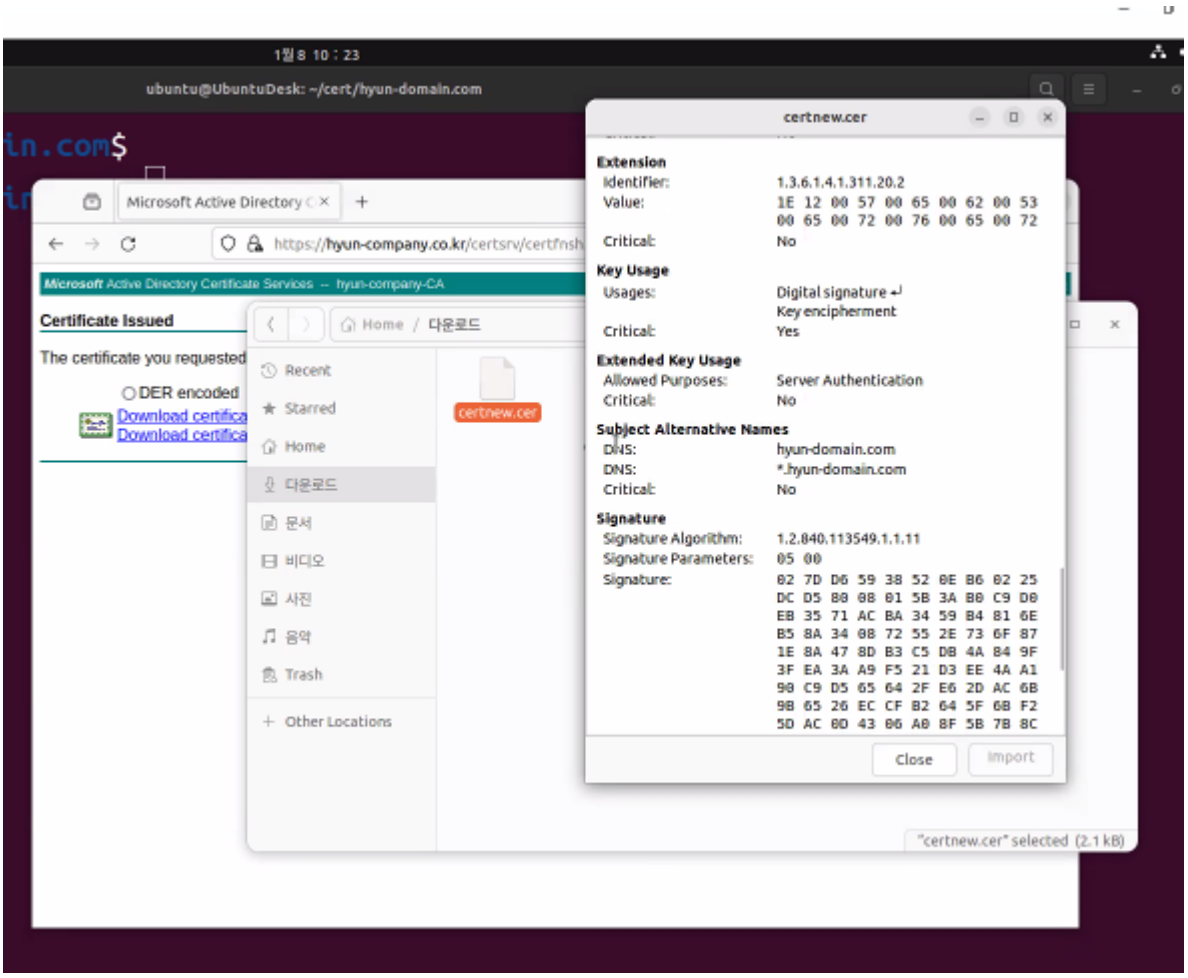


이거 재시작도 해줘야 함

```
PS C:\Users\Administrator> certutil -setreg policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\hyun-company-CA\Pol
icyModules\CertificateAuthority_MicrosoftDefault.Policy\EditFlags:
```



다시 우분투로 돌아와서 이렇게 대체 주체 설정해주고



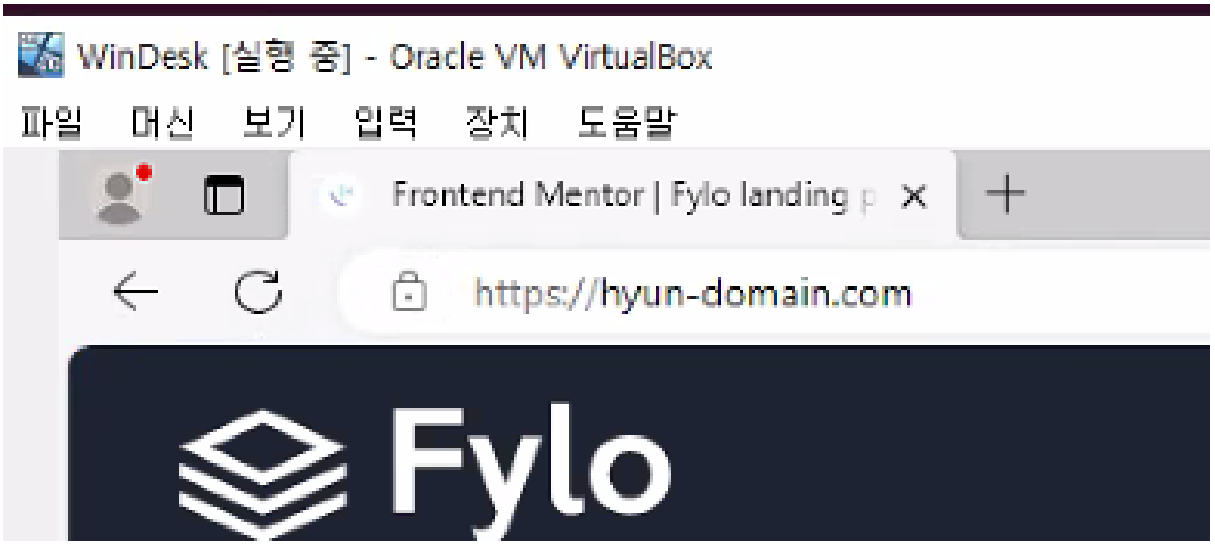
다운로드 디렉토리에서 확인해주기

```
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ mv ~/다운로드/certnew.cer ./hyun-domain.com.2.cer
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ sudo vi /etc/apache2/sites-available/001-hyun-domain.com-ssl
.conf
```

이름 바꾸고 나서 재시작

```
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ mv ~/다운로드/certnew.cer ./hyun-domain.com.2.cer
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ sudo vi /etc/apache2/sites-available/001-hyun-domain.com-ssl
.conf
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$ sudo systemctl restart apache2
ubuntu@UbuntuDesk:~/cert/hyun-domain.com$
```

이렇게 해준 닫음에 윈도우즈 데스크 가서 다시 열어보는 거



여기까지 하기