# My sample caconfig.cnf file.

#

# Default configuration to use when one is not provided on the command line.

#

[ ca ]

default\_ca = local\_ca

#

#

# Default location of directories and files needed to generate certificates.

#

[ local\_ca ]

dir = /home/<username>/ourCA

certificate = $dir/cacert.pem

database = $dir/index.txt

new\_certs\_dir = $dir/signedcerts

private\_key = $dir/private/cakey.pem

serial = $dir/serial

#

#

# Default expiration and encryption policies for certificates.

#

default\_crl\_days = 365

default\_days = 1825

default\_md = sha1

#

policy = local\_ca\_policy

x509\_extensions = local\_ca\_extensions

#

#

# Copy extensions specified in the certificate request

#

copy\_extensions = copy

#

#

# Default policy to use when generating server certificates. The following

# fields must be defined in the server certificate.

#

[ local\_ca\_policy ]

commonName = supplied

stateOrProvinceName = supplied

countryName = supplied

emailAddress = supplied

organizationName = supplied

organizationalUnitName = supplied

#

#

# x509 extensions to use when generating server certificates.

#

[ local\_ca\_extensions ]

basicConstraints = CA:false

#

#

# The default root certificate generation policy.

#

[ req ]

default\_bits = 2048

default\_keyfile = /home/<username>/ourCA/private/cakey.pem

default\_md = sha1

#

prompt = no

distinguished\_name = root\_ca\_distinguished\_name

x509\_extensions = root\_ca\_extensions

#

#

# Root Certificate Authority distinguished name. Change these fields to match

# your local environment!

#

[ root\_ca\_distinguished\_name ]

commonName = MyOwn Root Certificate Authority

stateOrProvinceName = NC

countryName = US

emailAddress = root@tradeshowhell.com

organizationName = Trade Show Hell

organizationalUnitName = IT Department

#

[ root\_ca\_extensions ]

basicConstraints = CA:true