Create an SSL Configuration File

While not actually required, it cuts down on the number of things you have to type. Creating this file allows you to use the -config parameter on many commands, with values drawn from here.

For example, everything in the **[req_distinguished_name]** is asked for every time you create a certificate, whether it be a CA or a Certificate Signing Request (csr), but must be different for each certificate created. By entering it once in the config file, you never have to type it again (see *prompt = no* in config). We will modify the CN to always be the name of the server to receive this, but we can leave everything else alons. Everything can be overridden by the command line.

This file is designed to be used several places, from creating the initial CA to creating a CSR, to creating the final Server Cert, so it is more complex than it needs to be.

When creating a Server Certificate, this file will be different for each one. Thus, I copy the entire file to a new file, specific to the Server Certificate being created and a .ext (for extension) suffix. While that is redundant, for small opeerations the simplicity outweighs the redundancy.

Copy the file to your SSL Creation directory and modify the **[req_distinguished_name]** section. Don't worry about the **[alt_names]** at this time.

Any number of spaces can be around the equals sign, or surrounding the name inside a section name (ie, [joe], [joe] and [joe] are all valid section names for the section *joe*).

A pound sign begins a comment, extending to the end of the line. There are a few places where comments can actually be (mis-)interpreted, according to the documentation, but I found no specifics.

openssl.cnf

```
[ req ]
default_bits        = 2048            # Size of keys
default_keyfile     = privkey.pem     # Default private key file
distinguished_name  = req_distinguished_name
prompt              = no
req_extensions      = req_ext          # Extensions to add to
certificate requests

[ req_distinguished_name ]
# Modify these for your network
C  = US
ST = Texas
L  = Dallas
O  = Example Corp
OU = Office
# CN should be different for all certs
CN = example.org
emailAddress = admin@example.org

[ req_ext ]
```

```
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names

# this section gets destroyed when creating server ext files
[alt_names]
DNS.1 = mydomain.com
DNS.2 = www.mydomain.com

# used when creating a CA
[ ca ]
default_ca = CA_default

# This is used when we create a CA
[ CA_default ]
keyUsage = critical, digitalSignature, keyEncipherment, cRLSign,
keyCertSign
extendedKeyUsage = serverAuth, clientAuth
basicConstraints = CA:TRUE

# used when creating a Server Cert
[ server ]
# Extensions for server certificates
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth
basicConstraints = CA:FALSE  # Specify that this is not a CA
```

You are now ready to Create an Internal CA