Preparation

====================

install openssl

(manually adjust system path or reboot to ensure openssl bin folder is in path)

Phase 1 - making the certificate request

================================================

create a config file (using a text editor)

contents should use a format like this...

------ START: DO NOT INCLUDE THIS LINE IN THE CONFIG FILE --------

[ req ]

default\_bits = 2048

distinguished\_name = req\_distinguished\_name

req\_extensions = req\_ext

prompt = no

[ req\_distinguished\_name ]

countryName = US

stateOrProvinceName = OHIO

localityName = Cincinnati

organizationalUnitName = NOC

organizationName = NNL

commonName = Gigaflow.nnl.com

[ req\_ext ]

subjectAltName = @alt\_names

[alt\_names]

DNS.1 = Gigaflow.nnl.com

------ END: DO NOT INCLUDE THIS LINE IN THE CONFIG FILE --------

save the config file (e.g. Gigaflow.nnl.com.cnf)

use openssl to generate a key file and CSR based on the config file

openssl req -new -newkey rsa:2048 -nodes -keyout Gigaflow.nnl.com.key.pem -out Gigaflow.nnl.com.csr -config Gigaflow.nnl.com.cnf

this will generate a new key file and a new csr file.

insert the CSR file (or its contents) into the CA that will be used to generate a cert

Phase 2 - Generate/Download the new certificate

=============================================

generate the cert. this may require assistance from the CA operator.

download the cert and all corresponding Certs from the CA.

"PEM" format with Full "certificate chain" is preferred.

PEM files are text files. they have sections that are started and ended with ----BEGIN---- and -----END----- respectively

if there is more than one section, this is because there is more than one item in the file (e.g. a certificate chain)

openssl x509 -text -inform=PEM -in=Gigaflow.nnl.com.cer.pem

this process assumes that PEM format with full chain has been used to generate the certificate file.

if you have a file named, Gigaflow.nnl.com.cer , you may wish to rename it Gigaflow.nnl.com.cer.pem

Phase 3 - Join Key and Cert material to generate P12 file for Gigaflow

=========================================================================

openssl pkcs12 -export -inkey Gigaflow.nnl.com.key.pem -in Gigaflow.nnl.com.cer.pem -name Gigaflow.nnl.com -out Gigaflow.nnl.com.p12

...verify the p12 file using the command...

openssl pkcs12 -in MYSTORE.p12 -nodes

NOTE1: the creation of key, csr and p12 files can be completed on any system that has openssl. in other words, it is not necessary to \*generate\* the key on the same system that will use the certificate. just make sure that each set of corresponding files (KEY, CSR, CER and P12) are not mixed up.

NOTE2: this process uses a keyphrase to protect the contents of the P12 file, including the private key for the certificate.

However, the key file itself is not protected and should probably be securely destroyed after the P12 has been generated.