Openssl—CA

1. Creating directory

* pwd
* mkdir ca
* cd ca
* mkdir certs crl newcerts private
* chmod 700 private
* touch index.txt
* echo 1000 > serial

1. creating config file

* copy the conf file which is given
* and change the path and root key and root certificate
* save in ca

1. setting up root ca

* openssl genrsa -aes256 -out private/GBSRootCA.key 4069
* enter passward
* chmod 400 private/GBSRootCA.key
* pwd
* openssl req -config openssl.cnf -key private/GBSRootCA.key -new -x509 -days 7000 -sha256 -extensions v3 ca -out GBSRootCA.cert
* chmod 444 GBSRootCA.cert
* mv GBSRootCA.cert certs
* openssl x509 -noout -text -in certs/GBSRootCA.certs

1. creating certificate for intermideate CA

* pwd
* mkdir intermediate
* cd intermediate
* mkdir cert crl csr newcerts private
* chmod 700 private
* touch index.txt
* echo 1000 > serial
* echo 1000 > crlnumber
* copy the openssl.cnf file and change the path and root and privacy

1. creating public private key

* cd home/pranita/ca
* openssl genrsa -aes256 -out intermediate/private/GBSCSTCA.key 4096
* enter passward
* chmod 400 intermediate/private/GBSCSTCA.key
* openssl req -config intermediate/openssl.cnf -new -sha256 -key intermediate/private/GBSCSTCA.key -out intermediate/csr/GBSCSTCA.csr
* enter pass
* openssl ca -config openssl.cnf -extension v3\_intermediate\_ca -days 3650 -notext -md sha256 -in intermediate/csr/GBSCSTCA.csr -out intermediate/cert/GBSCST.cert
* enter pass
* cat index.txt
* cat serial

1. to look at content of openssl x509

* openssl x509 -noout -text -in intermediate/cert/GBSCST.cert

1. to verify the digital certificate

* openssl verify -CAfile certs/GBSRootCA.cert intermediate/cert/GBSCST.cert