**How to setup PKI Infrastructure?**

**Setting up root CA**

* sudo su –
* mkdir /pki
* cd /pki
* mkdir rootca
* cd rootca
* mkdir private
* opnessl genrsa –aes256 –out private/root-ca.key 4096
* yum install openssl-libs
* cp /etc/pki/tls/openssl.cnf /pki/rootca/ ( Change openssl.cnf according to configuration)
* mkdir certs newcerts
* touch index.txt
* echo 01 > serial
* creating csr and signed by self rootca
* openssl req –config openssl.cnf –key private/root-ca.key –new –days 3650 –sha256 –x509 –extension v3\_ca –out certs/root-ca.crt
* cd certs
* openssl x509 –in root-ca.crt –text

**Setting up Intermediate CA**

* cd /pki
* mkdir subca
* cd subca
* mkdir private
* cd private
* openssl genrsa –aes256 –out subca.key 4096
* cd ..
* cp /etc/pki/tls/openssl.cnf .
* openssl req –new –key private/subca.key –sha256 –out subca.csr ( CSR Created )
* openssl req –in subca.csr –text –noout ( To See what csr contains )
* cd ../rootca
* create custom extension look like

[ v3\_intermediate\_ca ]

subjectKeyIdentifier=hash

authorityKeyIdentifier=keyid:always,issuer

basicConstraints = CA:true,pathlen:0

Path len =0 means intermediate cannot create more CA it can sign only server certificates

* from rootca we sign intermediate CA certificate
* openssl ca –config openssl.cnf –extension v3\_intermediate\_ca –in pki/subca/subca/csr –out /pki/subca/subca.crt –days 3650
* now got subca folder
* chaned his configuration file to sign server certificate

**Setting up Server Certificate**

* cd /pki
* mkdir server
* cd server
* mkdir private
* cd private
* openssl genrsa –out server.key 4096
* openssl req –key private/server.key –new –sha256 –out server.csr
* CN == your domain name
* Go to intermediate CA to sign server certificate
* openssl ca –config openssl.cnf –extensions v3\_req –days 365 –in /pki/server/server.csr –out /pki/server/server.crt