ESERCITAZIONE 6 – Certificati Digitali

1. Verifica Certificati:

Spostiamo tutti i file ".pem" dalla cartella "LabAuthority" nella nostra cartella di lavoro.

openssl verify "cert.pem":

verifica del certificato con estensione ".pem";

openssl x509 -in "cert.pem" **-noout -text**:

mostra a schermo un certificato;

2. Self-Signed Certificate:

- Creiamo sul desktop la cartella "CA-Lab";
- In "CA-Lab" creiamo la cartella "demoCA";
- In "demoCA" creiamo le cartelle "certs", "crl", "newcerts";
- In "demoCA" creiamo 2 file attraverso TOUCH da terminale:

  touch index.txt

  touch serial
- In "serial" scriviamo un numero casuale (es. 1000), ovvero il numero seriale da cui partiranno i certificati.

Copiare nella cartella "CA-Lab" il file "**openssl.cnf"** che si trova in "/usr/lib/ssl".

openssl req -new -x509 -keyout my-ca.key **-out** my-ca.crt **-config openssl.cnf** (**inform DER** (?)):

genera il Self-Signed Certificate per farci diventare una CA root;
la password che verrà chiesta in questa fase servirà anche per generare la "chiave privata" nel file "my-ca.key";
il file "my-ca.crt" conterrà la CHIAVE PUBBLICA CERTIFICATA collegata alla chiave privata;

3. Certificate Signing Request per un server:

openssl genrsa -out server.key:

genera il file server.key contenente la chiave pubblica/privata del server;

openssl req -new -key server.key **-out** server.csr **-config** openssl.cnf:

genera la Certificate Signing Request dopo aver inserito alcuni valori:

- COMMON NAME: nome dell'organizzazione da certificare (inserire "CustomerServer.com");
- ORGANIZATION NAME: inseriamo il nome della nostra CA;
- Verrà creato il file "*server.csr*" in CA-Lab che conterrà la richiesta per ottenere il certificato per la chiave pubblica contenuta nel file stesso;

Nei panni della CA, generiamo il certificato:
openssl ca -in server.csr **-out** server.crt **-cert** my-ca.crt **-keyfile** my-ca.key **-config openssl.cnf**:

verrà creato il file "*server.crt*" che conterrà la chiave pubblica certificata;

Ora bisogna inserire il certificato nel Web Server aprendo il file "*hosts*" presente nella cartella *"etc":*
sudo open hosts:

inseriamo nel file una nuova riga ->
"127.0.0.1" "CustomerServer.com"

Combiniamo in un unico file la chiave segreta e il certificato:
cp server.key server.pem
cat server.crt **>>** server.pem

Lanciamo un web server usando "server.pem" per far si che questo server sia presente sul web:
openssl s_server -cert server.pem **-www**

Apriamo Firefox e digitiamo l'indirizzo:
http://CustomerServer.com:4433/

Se otteniamo un messaggio di errore, bisogna importare il certificato della nostra CA ("*my-ca.crt*") nel browser:
setting -> **privacy & security** -> **view certificates** -> **import** -> trovare e selezionare il nostro certificato, spuntando "Trust this CA to identify web sites.