SSL/TLS Web Server

Generate Certificates

Method 1: ??? CA ???

```
mkdir /etc/apache2/certs
cd /etc/apache2/certs
openssl genrsa -out myhomepbx.key 2048
openssl req -new -key myhomepbx.key -out myhomepbx.csr
openssl x509 -req -days 3650 -in myhomepbx.csr -signkey myhomepbx.key -out myhomepbx.crt
```

Method 2: ?? CA ???

```
# generate CA
# organizationName = HomePBX
# commName = HomePBX CA
# Enter PEM pass phrase: set new password that is used to sign the certicficate.
cd /etc/ssl/homepbxCA
openssl req -new -x509 -extensions v3_ca -keyout ca.key -out ca.crt -days 3650

# prerequisites
# Edit the openssl.homepbx.cnf as required
cp /etc/ssl/openssl.conf ./openssl.homepbx.cnf
touch index.txt
echo '01' > serial
mkdir newcerts

# generate Server certificates
# organizationName = HomePBX (it must be the same as CA, otherwise it cannot be signed by the CA)
# commName = FQDN of website or *
# Enter PEM pass phrase: It's not required, enter to skip it if wanted.
openssl req -config openssl.homepbx.cnf -new -nodes -keyout server.key -out server.csr
openssl ca -config openssl.homepbx.cnf -days 3650 -in server.csr -out server.crt

# generate PKCS12 for client authentication
```

```
# NOTE: you can create PKCS12 file by either server certificate or CA certificate.
# Enter Export Password: set new pasword that is used for importing the PKCS12
openssl pkcs12 -export -clcerts -in ca.crt -inkey ca.key -out homepbx_2021y.p12
# Alternatively
openssl pkcs12 -export -clcerts -in server.crt -inkey server.key -out homepbx_2021y.p12
```

openssl.homepbx.cnf

```
...
[ CA_default ]

dir         = .          # Where everything is kept  <== Here
certs       = $dir/certs        # Where the issued certs are kept
crl_dir     = $dir/crl          # Where the issued crl are kept
database    = $dir/index.txt    # database index file.
#unique_subject = no            # Set to 'no' to allow creation of
                                # several certs with same subject.
new_certs_dir  = $dir/newcerts      # default place for new certs.

certificate    = $dir/ca.crt   # The CA certificate <== Here
serial         = $dir/serial        # The current serial number
crlnumber      = $dir/crlnumber     # the current crl number
                                # must be commented out to leave a V1 CRL
crl            = $dir/crl.pem        # The current CRL
private_key    = $dir/ca.key# The private key  <== Here

x509_extensions = usr_cert          # The extensions to add to the cert
...
```