XCA Digital Certificate

first install xca
in xca
file
new database

Now
create template
new template → empty (default)
internal name - address template
country name - in
state - mh
locality - pune
organization - Iacsd
(every certificate common name is diff so leave it empty)
then ok

Now create root ca private key
name → rootca (default algo RSA)
in certificate for root ca
New certificate
signing -
create a self signed
template for new certficate
address template

in subject tab
internal name - rootcacertificate
common name - rootca
check private key : rootca

Again in source tab
in template select CA template and apply
extension and verify in advance tab
then ok

(2)

subca's private key
new key → subca
* in certificate
new certificate
use this certificate for signing
check for rootcacertificate
template-
address template
apply subject
* in subject tab
internal name - subcacertificate
common name - subca
check for private key -
subca

Now again in source tab
select ca template
and apply extensions
and in extensions → years 5 → apply

create subca

webserver private key
create key
new key → webserver
* in certificate
new certificate
use this certificate → subca
template-
address template
apply subject
* in subject tab

(3)

Internal name - webservercertificate
Common name = www.webserver.com
check for private key
webserver
Now again in source tab
select TLS_client template
apply extensions
then ok

* Export private key of webserver
select webserver → export
select .pem private key (format)
ok

* Export certificate chain
select webserver → export →
pem chain → format

Now in debian
install apache2
change index.html (/var/www/html/index.html)
mkdir ~~/etc/www~~ /etc/apache2/ssl
cd /etc/apache2/ssl

* Copy the private key and certificate chain to the debian from base machine using ftp
apt-get install vsftpd
uncomment writeenable in vsftpd.conf
in base machine
cmd prompt - ftp ip
put filename

(4)

and move that both key file in
/etc/apache2/ssl/

sudo cp * /etc/apache2/ssl/

ls -l /etc/apache2/ssl/

sudo chmod 600 /etc/apache2/ssl/
sudo a2enmod ssl
sudo a2ensite default-ssl
sudo nano /etc/apache2/sites-available/
default-ssl.conf

ServerName . Webserver commonname:443
(www.ps.com)

Change
certificate file /etc/apache2/ssl/ .pem
certificatekeyfile /etc/apache2/ssl/keyfile.pem

save it

sudo systemctl reload apache2
restart
status

In windows (cmd run as administrator (c/sys32/drivers/etc
add www.ps.com in host file with
ip
save it
Now browse https://www.ps.com