STEPS TO INSTALL THE SSL CERTIFICATE IN THE LINUX SERVER

STEPS TO INSTALL SSL CERTIFICATE

yum install openssl
yum install mod_ssl
openssl genrsa -out ca.key 2048
openssl req -new -key ca.key -out ca.csr
openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt
cp ca.crt /etc/pki/tls/certs
cp ca.key /etc/pki/tls/private
cp ca.csr /etc/pki/tls/private
vim /etc/httpd/conf.d/ssl.conf
we change the ssl ceerticate file location
————————EX————————————
Server Certificate:
Point SSLCertificateFile at a PEM encoded certificate. If
the certificate is encrypted, then you will be prompted for a
pass phrase. Note that a kill -HUP will prompt again. A new
certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/pki/tls/certs/ca.crt

Server Private Key:
If the key is not combined with the certificate, use this
directive to point at the key file. Keep in mind that if
you've both a RSA and a DSA private key you can configure
both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/pki/tls/private/ca.key
_____________EX_____________________

vi /etc/httpd/conf/httpd.conf
<VirtualHost *:443>
SSLEngine on
SSLCertificateFile /etc/pki/tls/certs/ca.crt
SSLCertificateKeyFile /etc/pki/tls/private/ca.key
servername 13.233.21.101
Documentroot /var/www/html
</VirtualHost>

RESTART THE HTTPD SERVice