CMPE 272

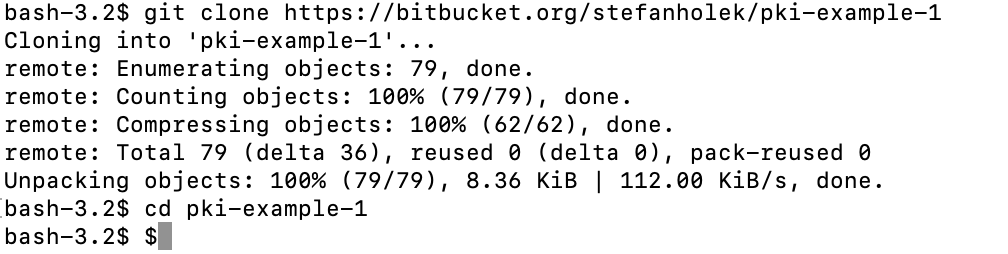
PKI INFRASTRUCTURE

-by CodeOurSouls

Step 1. Clone the Simple PKI example files and change directory:

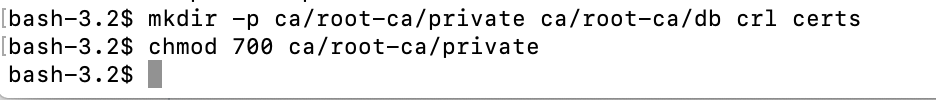
git clone https://bitbucket.org/stefanholek/pki-example-1

cd pki-example-1

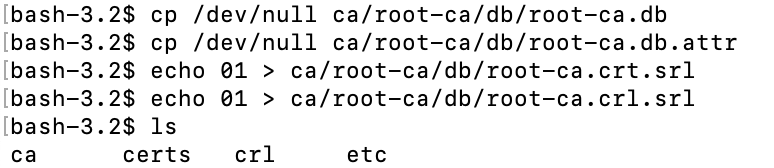


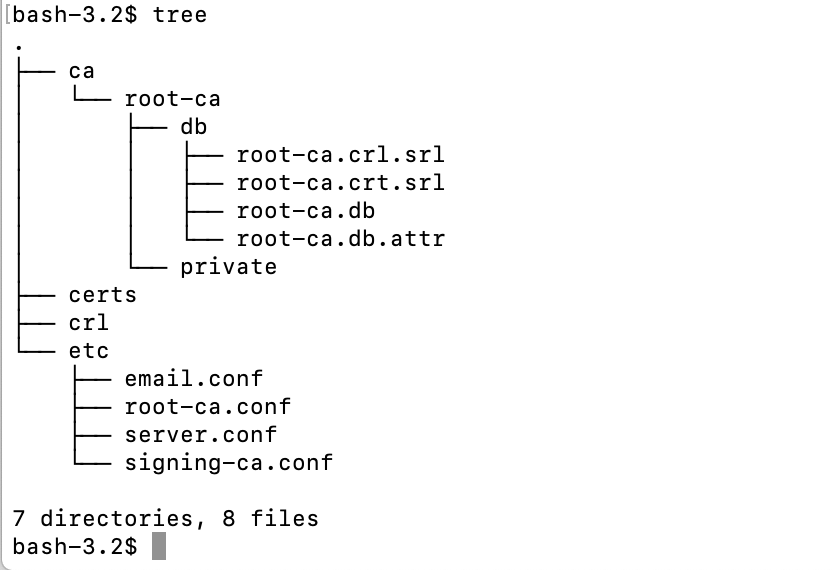
Step 2: Create Root CA:

Create the directories to hold the CA resources, CRLs and certificates:



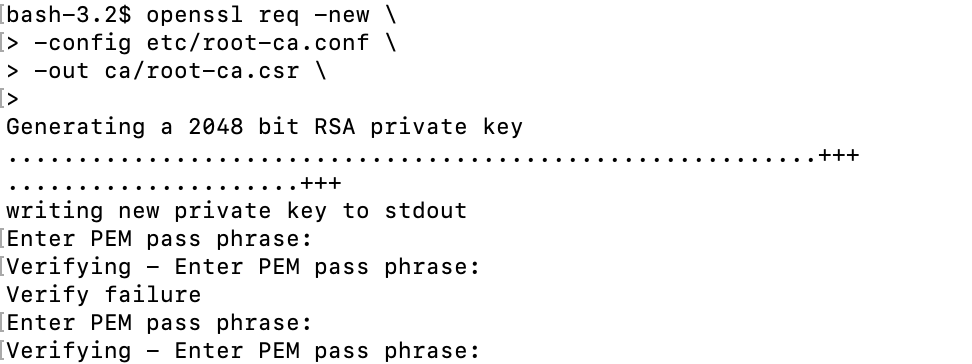
Step 3: Create the database:

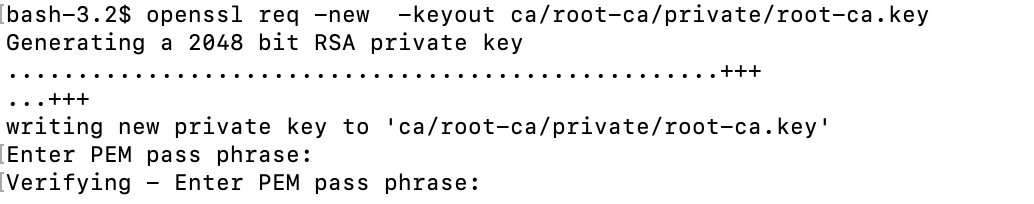


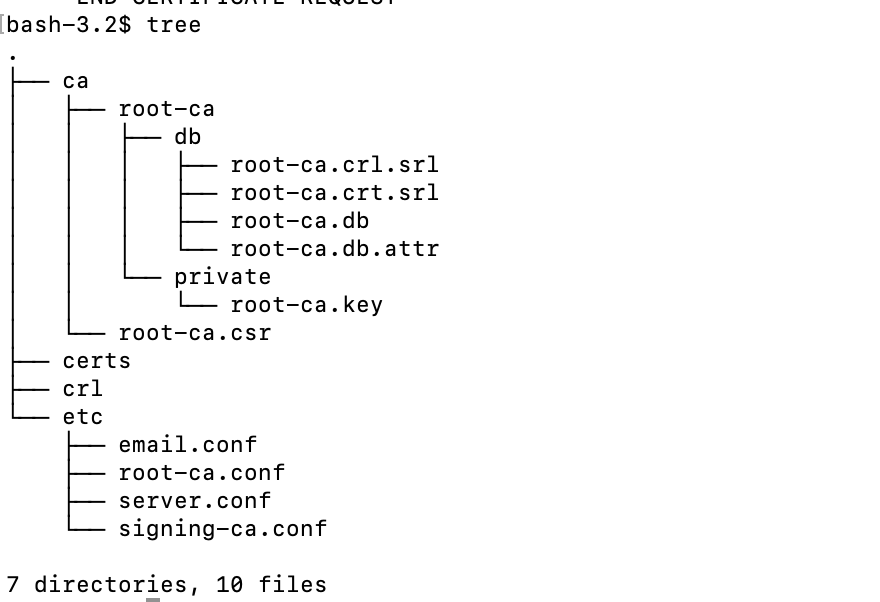


Step 3: Create the root CA request:

Using the “openssl req -new” command as given below to create a private key and a certificate signing request for the root CA.

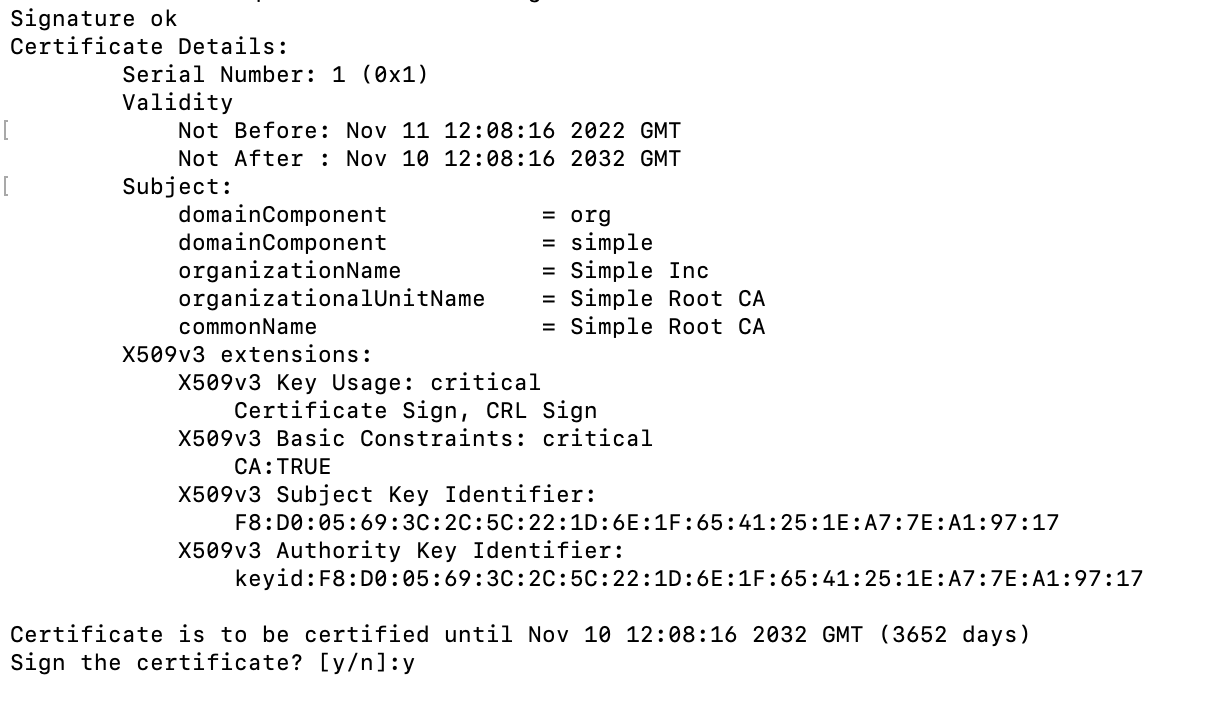


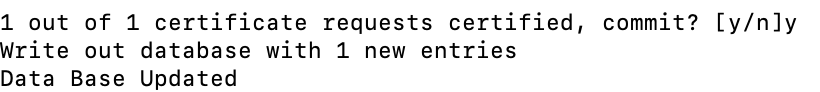




Step 4: **Create the root CA certificate:**

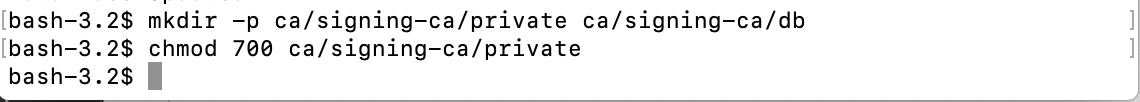




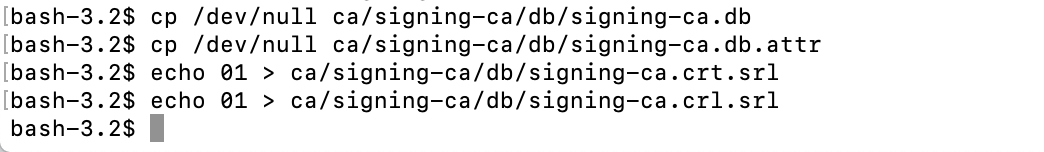


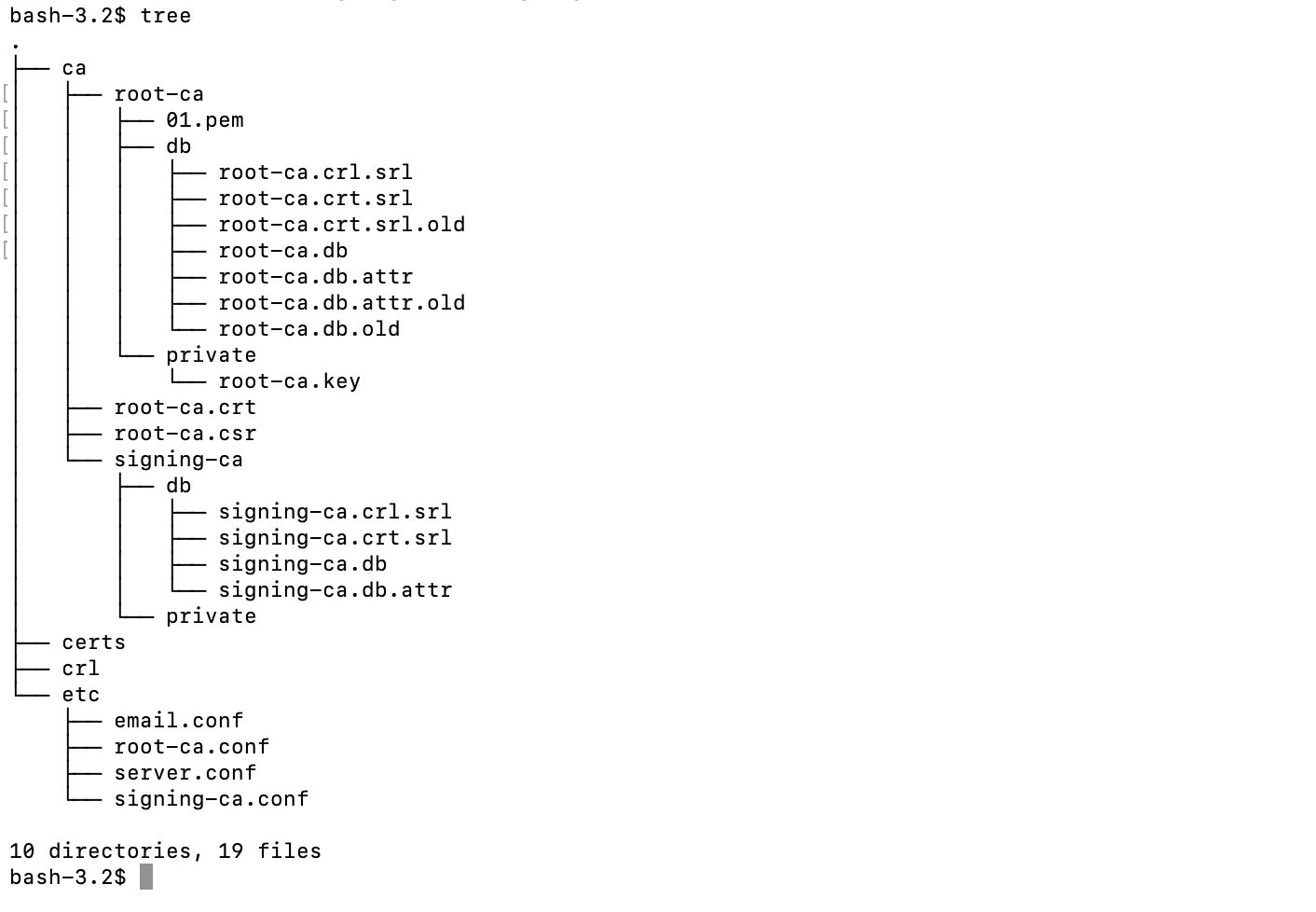
Step 5: **Create Signing CA:**

1. Create the directories to hold the signing CA resources:



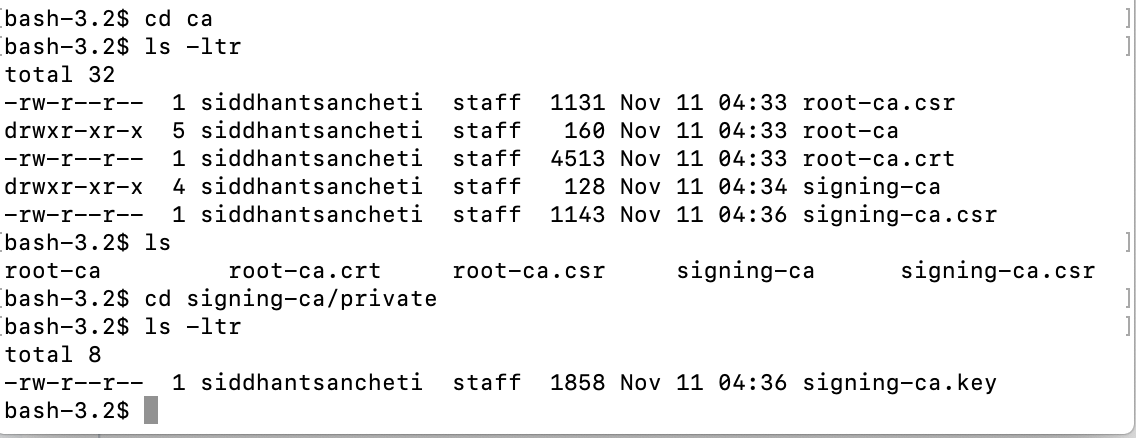
1. Create the database for signing CA:





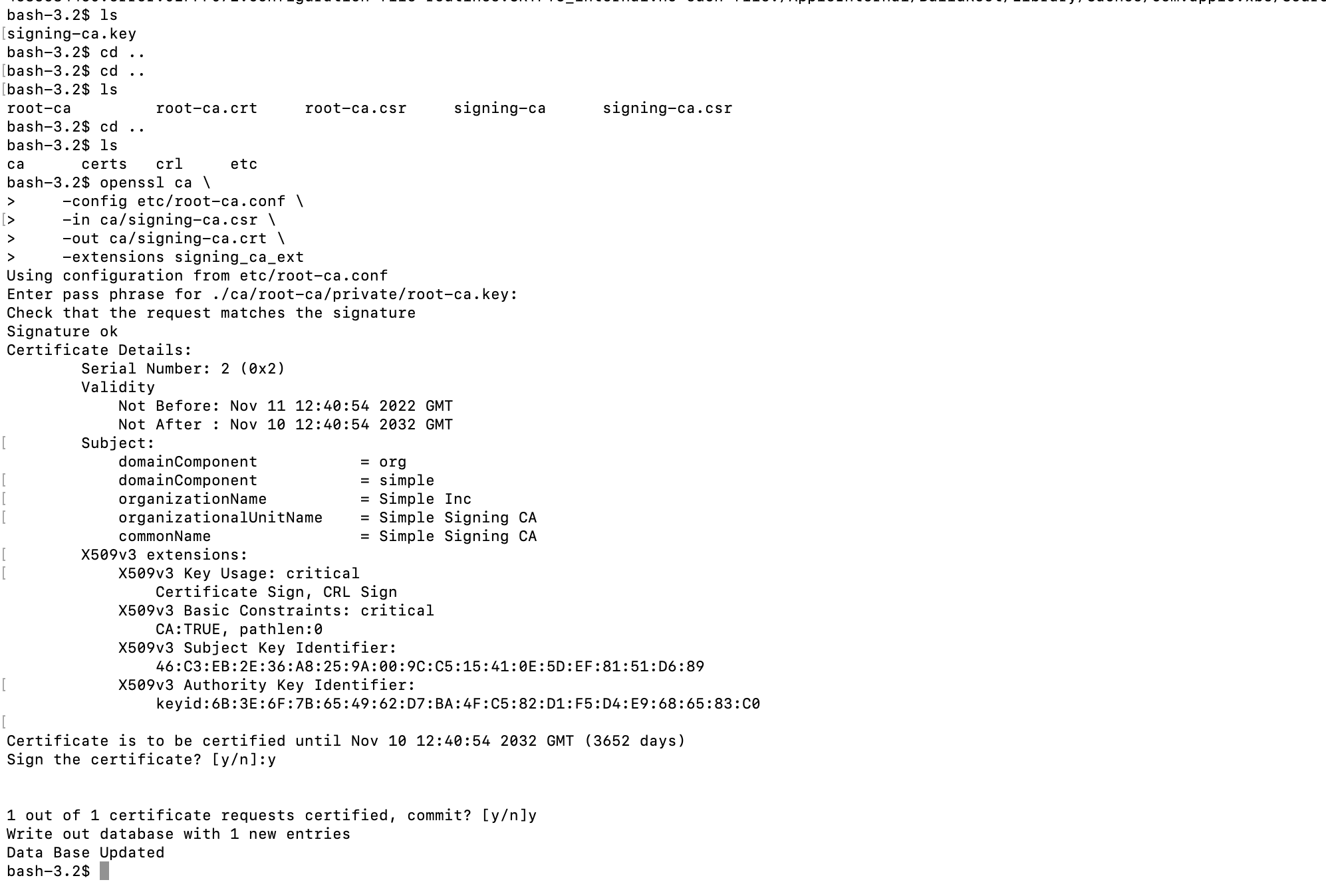
1. Create the signing CA request:

Use the “openssl req -new” command as given below to create a private key and a certificate signing request for the signing CA.



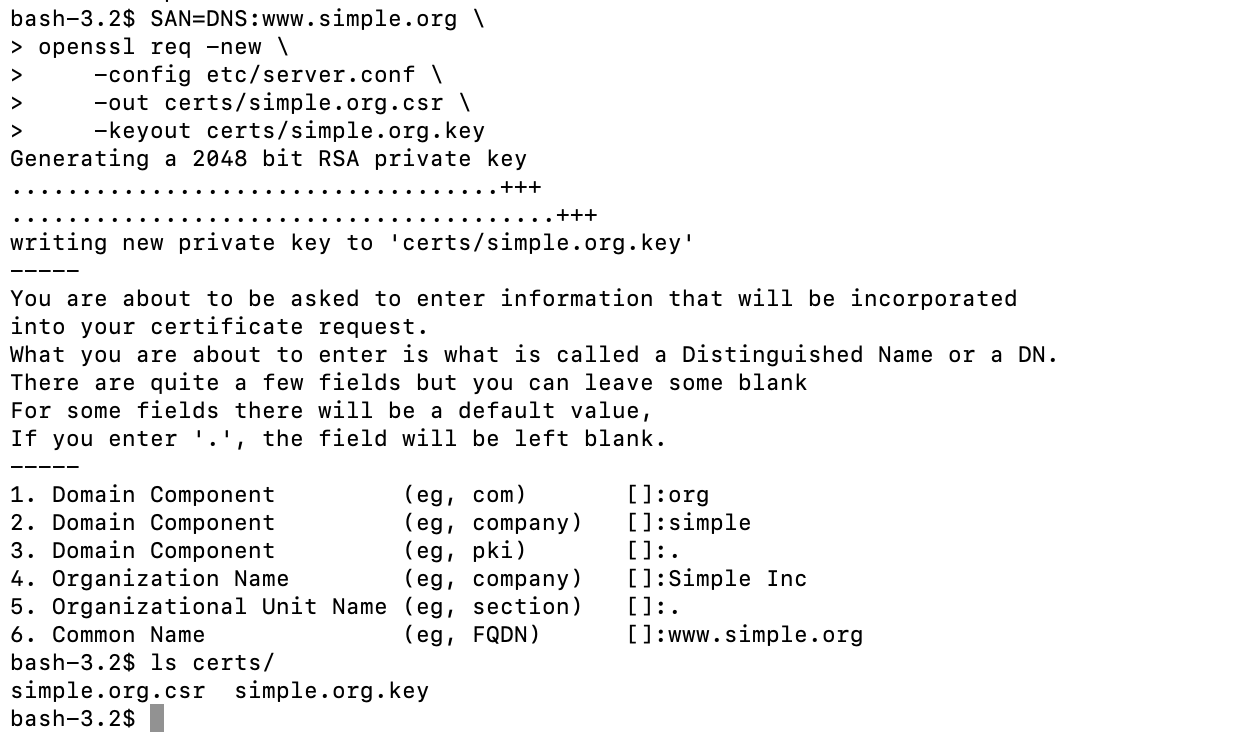
1. Create the signing CA certificate:

Next we will use the “openssl ca” command to issue a signing CA certificate based on the certificate signing request(CSR) created in the previous step.

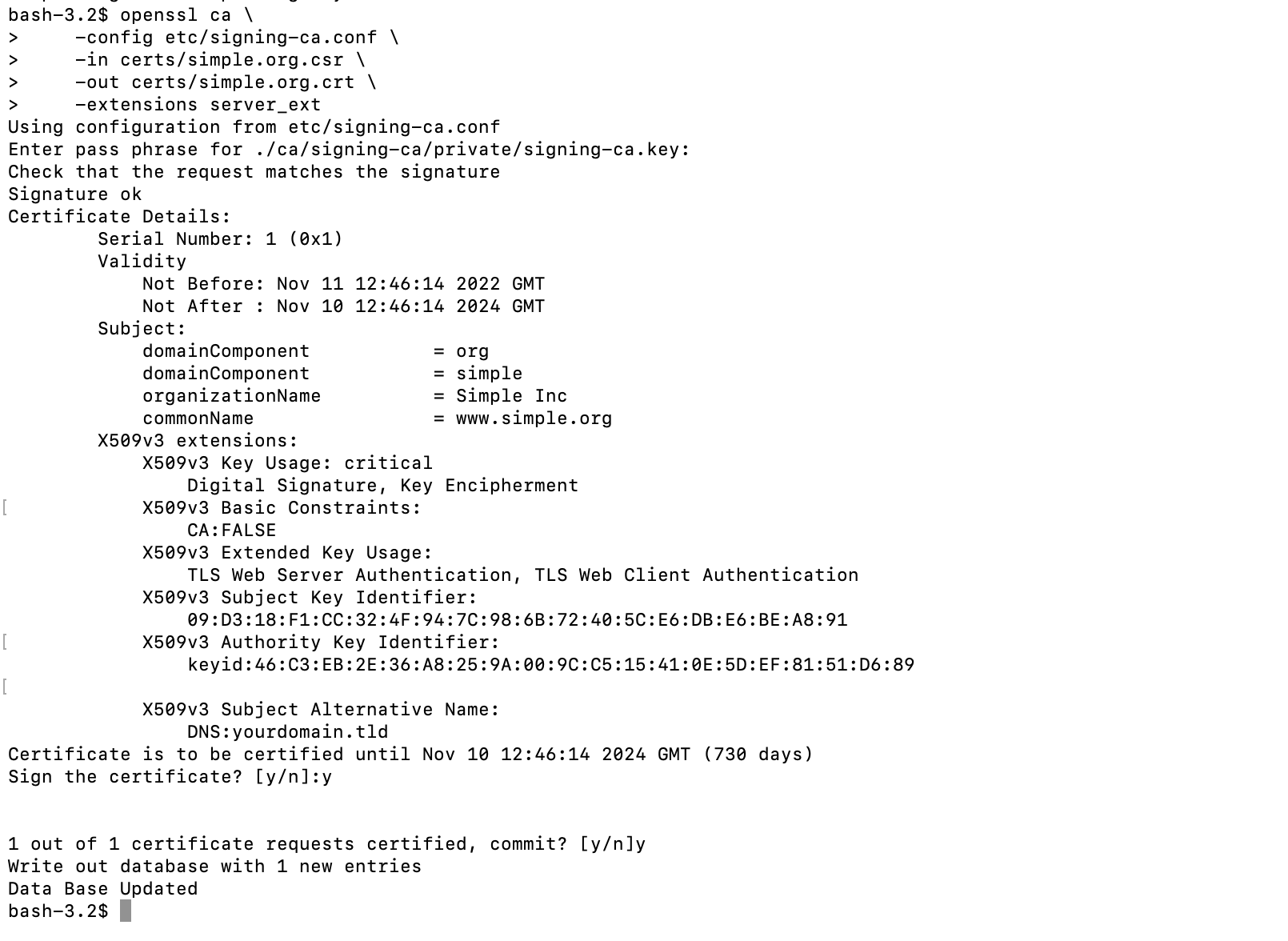


Step 6: **Create TLS server certificate:**

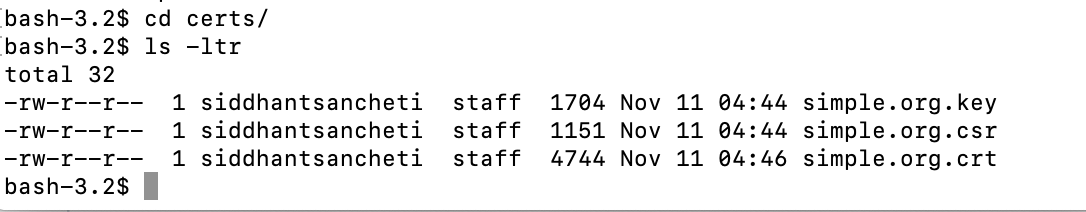
To create the TLS server certificate first we need to create the TLS server request using the command below. This will create a private key and a certificate signing request for the TLS server certificate.



Using the signing CA and the CSR created from the previous step, a server certificate can be issued with the following command.



The TLS certificate created in the certs folder:



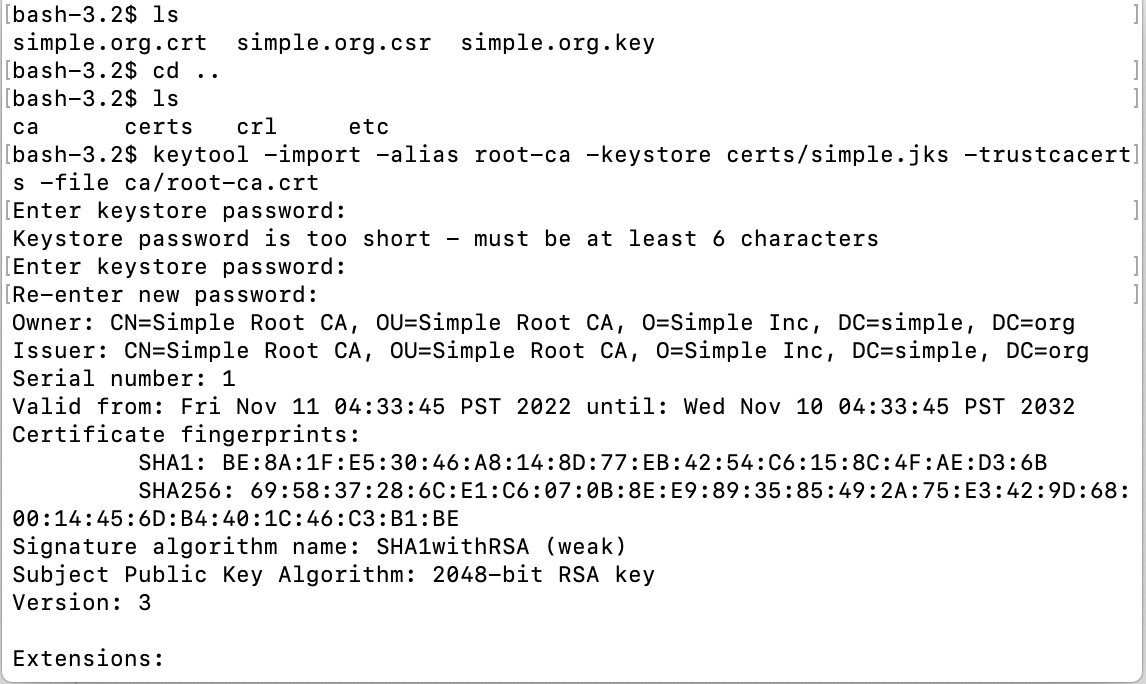


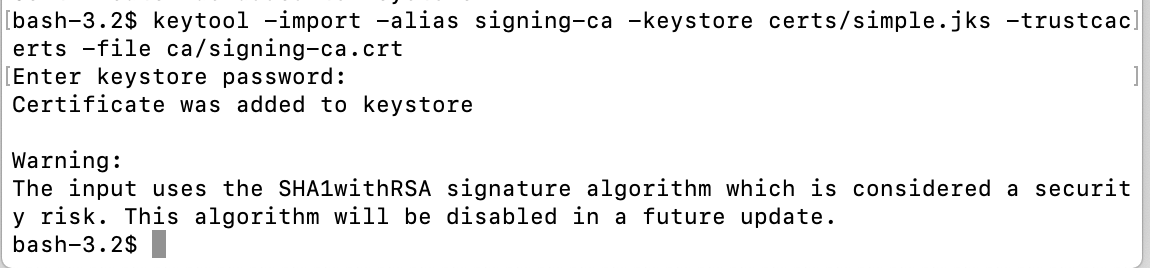


Step 7: **Install TLS server certificate on Tomcat:**

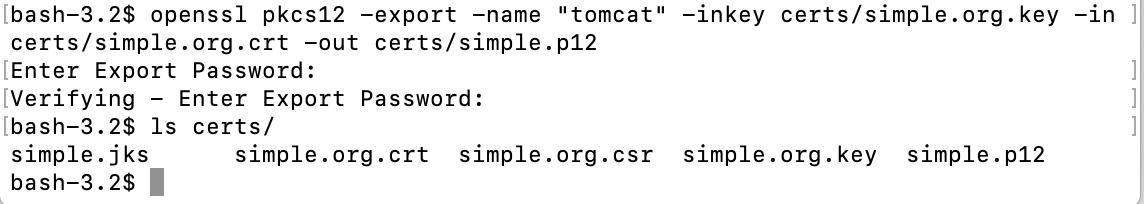
We will use the generated TLS certificate above to configure Tomcat to work with SSL. For that , we need to generate a keystore which has the complete certificate chain beginning from the root and up until the server.

Prepare the keystore file and add the root and signing certificate:

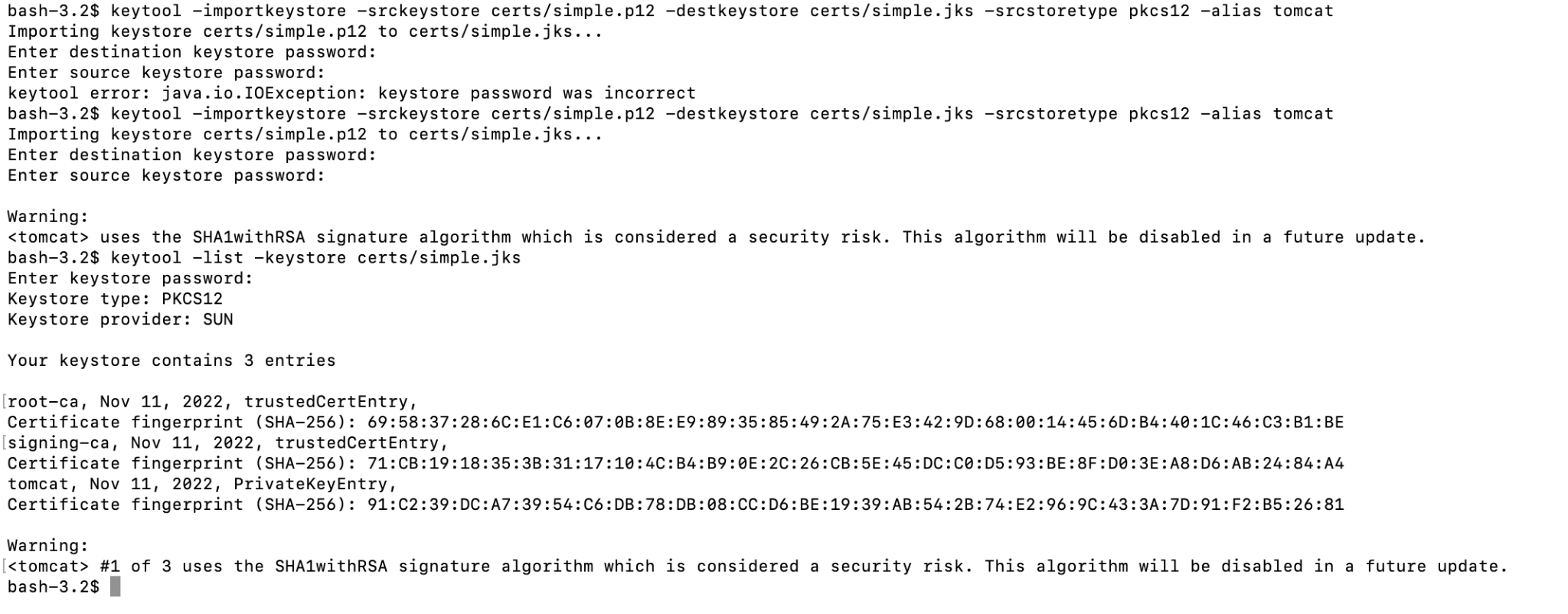




1. Generate the certificate-key pair for the server:



1. Import the certificate-key pair to the keystore:



Once the keystore is ready, then in Tomcat, the SSL configuration needs to be made in “server.xml” which is located in the “conf” directory of the Tomcat installation.

