HW-7-SECURITY

Questions:

Design and build a PKI infrastructure that includes Root CA, Signing CA, and TLS Certificate, E.g., as described here: http Links to an external site.://pki-tutorial.readthedocs.io/en/latest/simple Links to an external site./Links to an external site. Use the TLS certificate to install a web server, e.g. tomcat, https:// Links to an external site.tomcat.apache.org/tomcat-9.0-doc/ssl-howto.html

Group Name: Sankalp

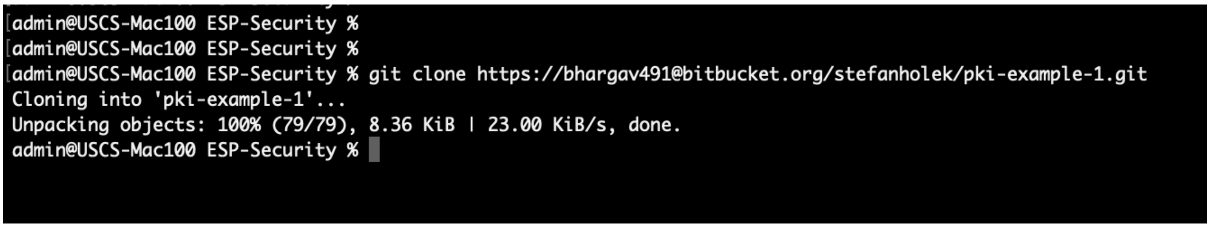
Team members:

- Bhargav Krishna Mullapudi
- Shireesh Vennamaneni
- Satya Ashish Veda
- Mohith Girigowdara Girish

Github Repository: https://github.com/bkrish111/hw-security.git

Answer:

Step 1: Clone the github repository https://bitbucket.org/stefanholek/pki-example-1. Proceed with the instructions given in: https://pki-tutorial.readthedocs.io/en/latest/simple/ to construct the PKI.

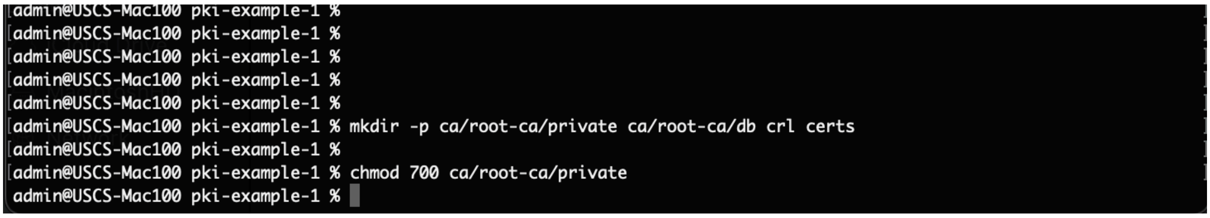


```
[admin@USCS-Mac100 ESP-Security %
[admin@USCS-Mac100 ESP-Security %
[admin@USCS-Mac100 ESP-Security % git clone https://bhargav491@bitbucket.org/stefanholek/pki-example-1.git
 Cloning into 'pki-example-1'...
 Unpacking objects: 100% (79/79), 8.36 KiB | 23.00 KiB/s, done.
 admin@USCS-Mac100 ESP-Security %
```

Step 2: Configure Root CA

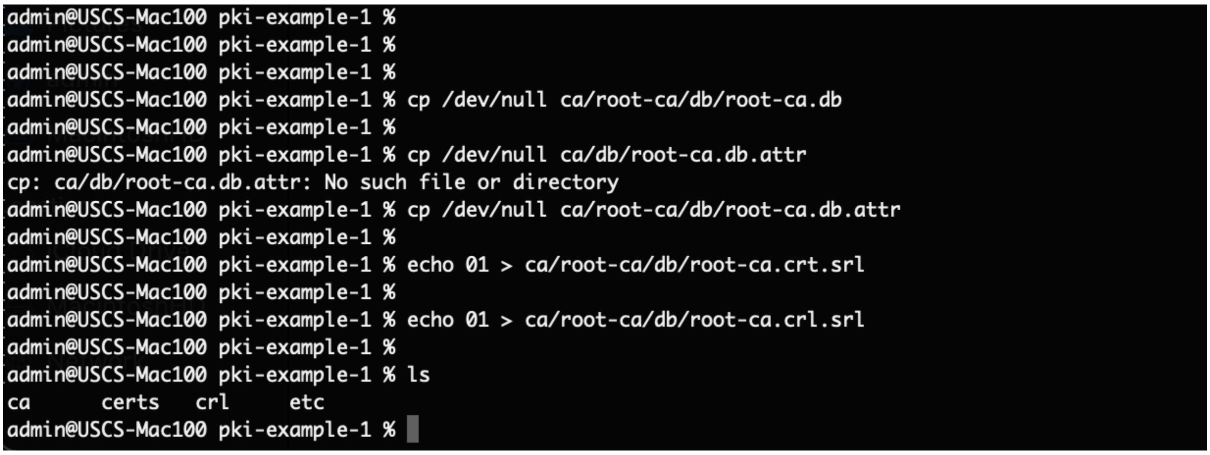
1.1 Configure Directories type, below mentioned commands:

The ‘ca’ directory holds CA resources, the ‘crl’ directory holds CRLs, and the ‘certs’ directory holds user certificates



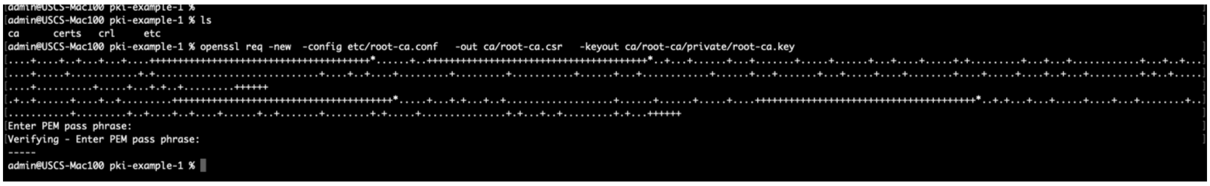
```
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 % mkdir -p ca/root-ca/private ca/root-ca/db crl certs
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 % chmod 700 ca/root-ca/private
admin@USCS-Mac100 pki-example-1 %
```

1.2 Configure Database, type below mentioned commands:



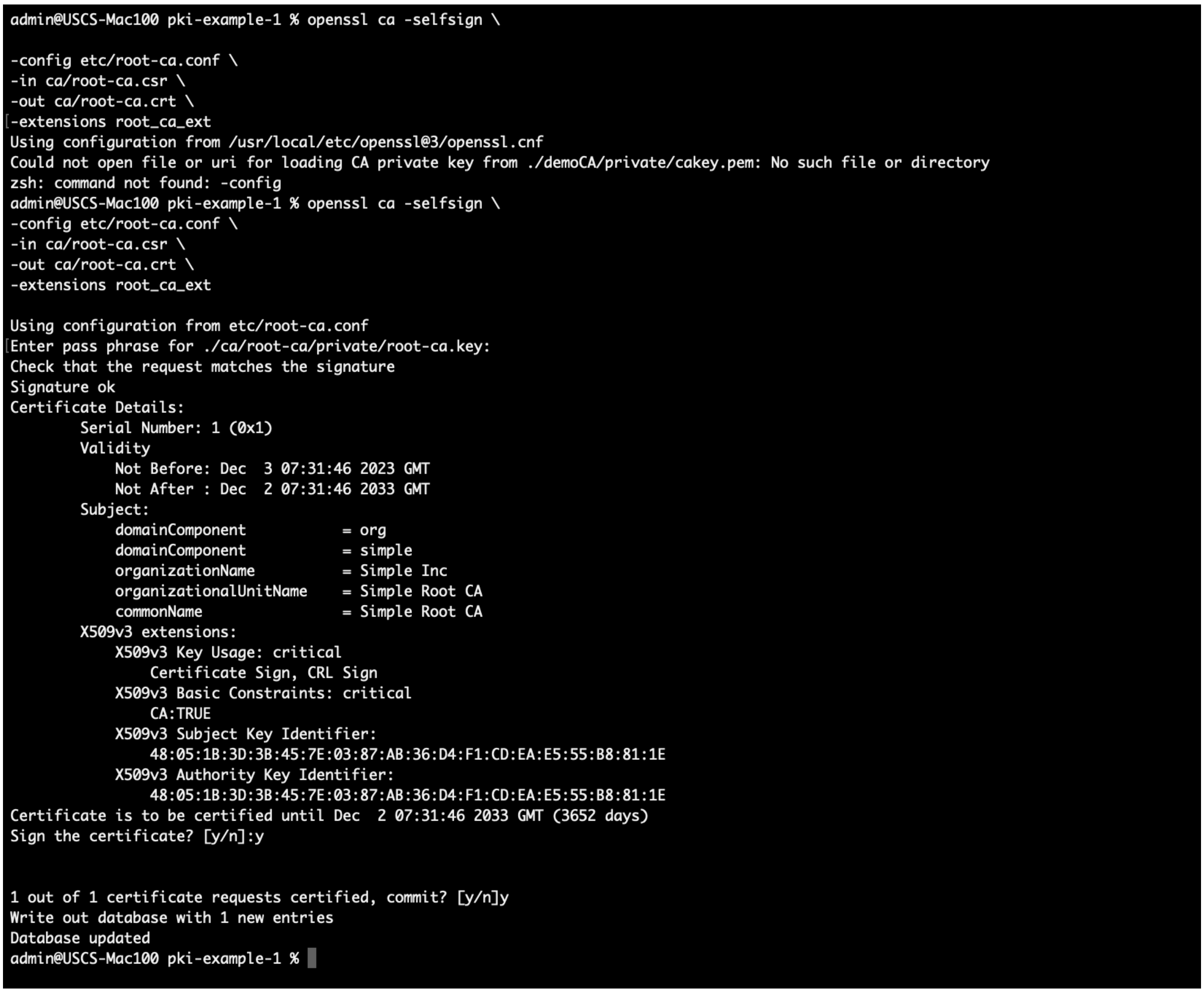
```
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 % cp /dev/null ca/root-ca/db/root-ca.db
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 % cp /dev/null ca/db/root-ca.db.attr
cp: ca/db/root-ca.db.attr: No such file or directory
admin@USCS-Mac100 pki-example-1 % cp /dev/null ca/root-ca/db/root-ca.db.attr
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 % echo 01 > ca/root-ca/db/root-ca.crt.srl
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 % echo 01 > ca/root-ca/db/root-ca.crl.srl
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 % ls
ca      certs   crl     etc
admin@USCS-Mac100 pki-example-1 %
```

1.3 Create CA Request



```
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 % ls
ca      certs   crl     etc
admin@USCS-Mac100 pki-example-1 % openssl req -new  -config etc/root-ca.conf   -out ca/root-ca.csr   -keyout ca/root-ca/private/root-ca.key
....+....+..+...+...+....++++++++++++++++++++++++++++++++++++++++*......+..++++++++++++++++++++++++++++++++++++++++*..+...+......+...+.......+.....+......+...+....+.....+.+.........+...+...+............+...+..+...
....+.....+............+.+...........................+....+..+....+.........+.........+...........+......+..+............+......+...+.......+...+.....+...+........+....+.....+....+.+...+.........+.+..+....
....+..........+.....+...+.+..+.........++++++
.+..+......+....+..+.........++++++++++++++++++++++++++++++++++++++++*.....+...+.+...+..+...................+......+......+.....+....++++++++++++++++++++++++++++++++++++++++*..+.+...+...+.....+....+...+........+..
..........+.........+..+....+..+....+......+..+.......+........+.+.....+...............+.+...+..+.........+.+...++++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
admin@USCS-Mac100 pki-example-1 %
```

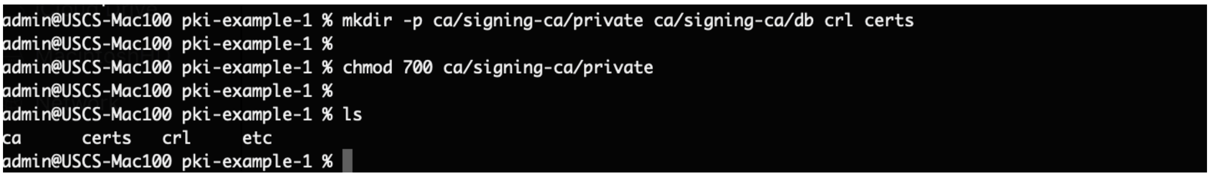
1.4 Create CA Certificate



```
admin@USCS-Mac100 pki-example-1 % openssl ca -selfsign \

-config etc/root-ca.conf \
-in ca/root-ca.csr \
-out ca/root-ca.crt \
[-extensions root_ca_ext
Using configuration from /usr/local/etc/openssl@3/openssl.cnf
Could not open file or uri for loading CA private key from ./demoCA/private/cakey.pem: No such file or directory
zsh: command not found: -config
admin@USCS-Mac100 pki-example-1 % openssl ca -selfsign \
-config etc/root-ca.conf \
-in ca/root-ca.csr \
-out ca/root-ca.crt \
-extensions root_ca_ext

Using configuration from etc/root-ca.conf
[Enter pass phrase for ./ca/root-ca/private/root-ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Dec  3 07:31:46 2023 GMT
            Not After : Dec  2 07:31:46 2033 GMT
        Subject:
            domainComponent           = org
            domainComponent           = simple
            organizationName          = Simple Inc
            organizationalUnitName    = Simple Root CA
            commonName                = Simple Root CA
        X509v3 extensions:
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                48:05:1B:3D:3B:45:7E:03:87:AB:36:D4:F1:CD:EA:E5:55:B8:81:1E
            X509v3 Authority Key Identifier:
                48:05:1B:3D:3B:45:7E:03:87:AB:36:D4:F1:CD:EA:E5:55:B8:81:1E
Certificate is to be certified until Dec  2 07:31:46 2033 GMT (3652 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Database updated
admin@USCS-Mac100 pki-example-1 %
```

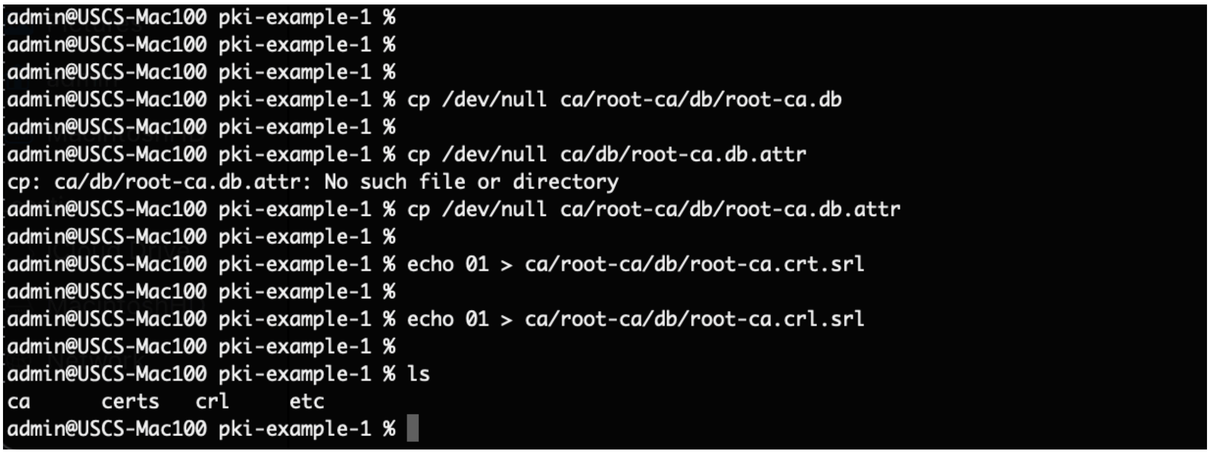
Step 3: Create Signing CA

3.1 Create Directories



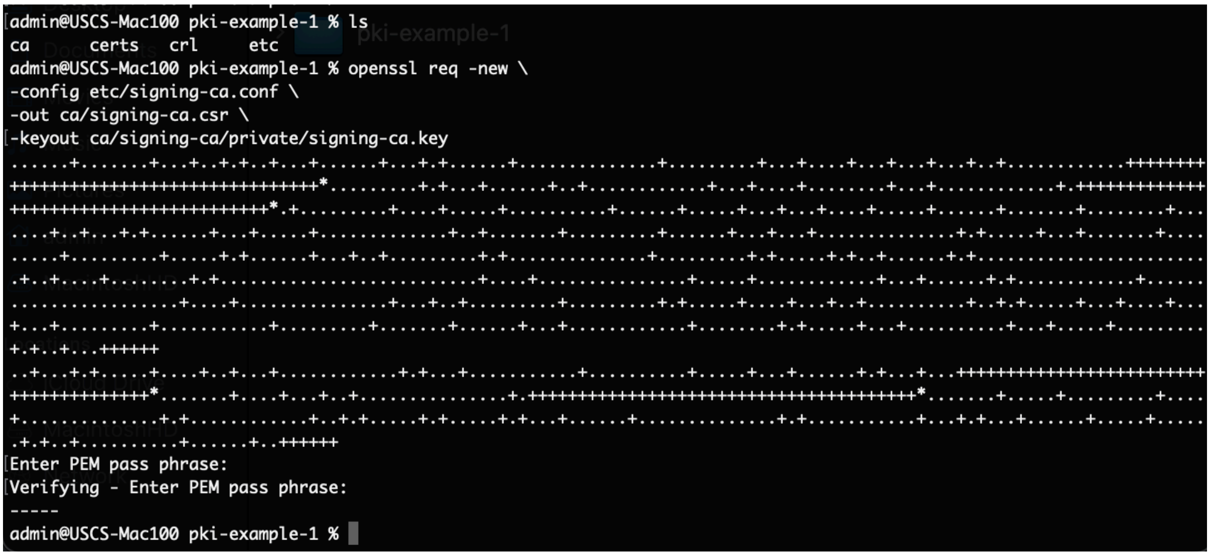
```
admin@USCS-Mac100 pki-example-1 % mkdir -p ca/signing-ca/private ca/signing-ca/db crl certs
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 % chmod 700 ca/signing-ca/private
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 % ls
ca      certs   crl     etc
admin@USCS-Mac100 pki-example-1 %
```

3.2 Create Database

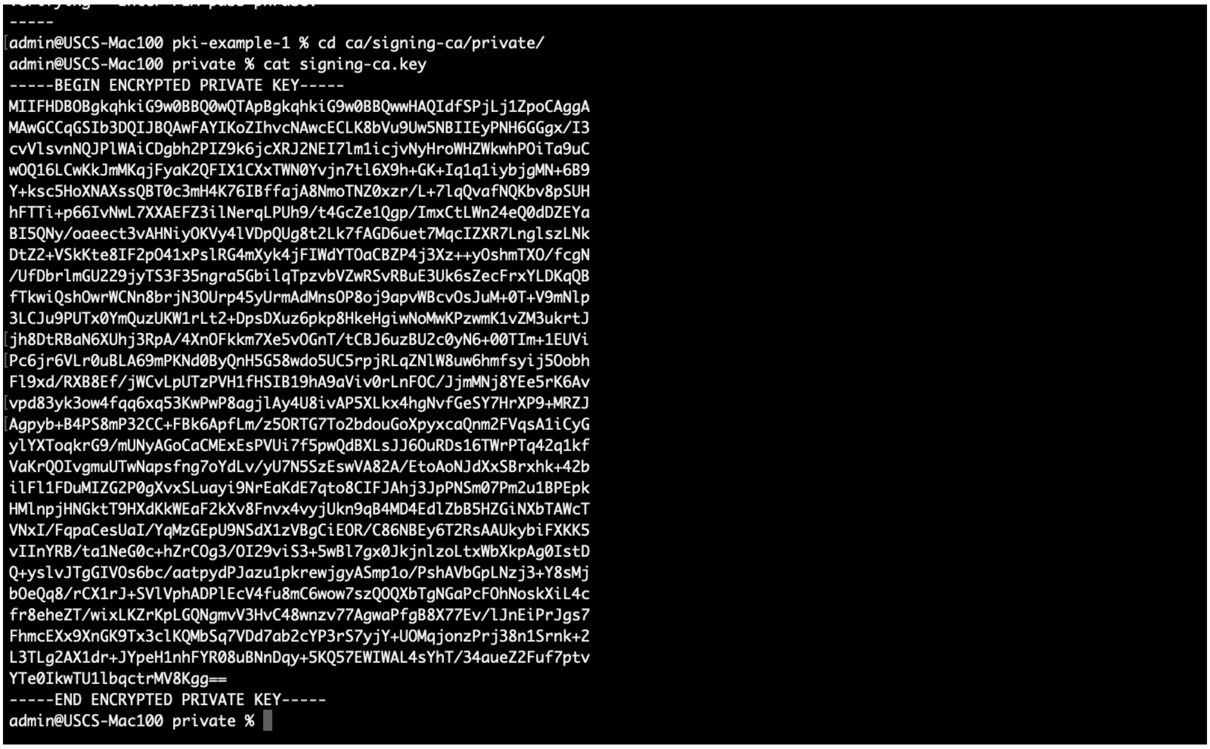


```
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 % cp /dev/null ca/root-ca/db/root-ca.db
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 % cp /dev/null ca/db/root-ca.db.attr
cp: ca/db/root-ca.db.attr: No such file or directory
admin@USCS-Mac100 pki-example-1 % cp /dev/null ca/root-ca/db/root-ca.db.attr
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 % echo 01 > ca/root-ca/db/root-ca.crt.srl
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 % echo 01 > ca/root-ca/db/root-ca.crl.srl
admin@USCS-Mac100 pki-example-1 %
admin@USCS-Mac100 pki-example-1 % ls
ca      certs   crl     etc
admin@USCS-Mac100 pki-example-1 %
```

3.3 Create CA Request

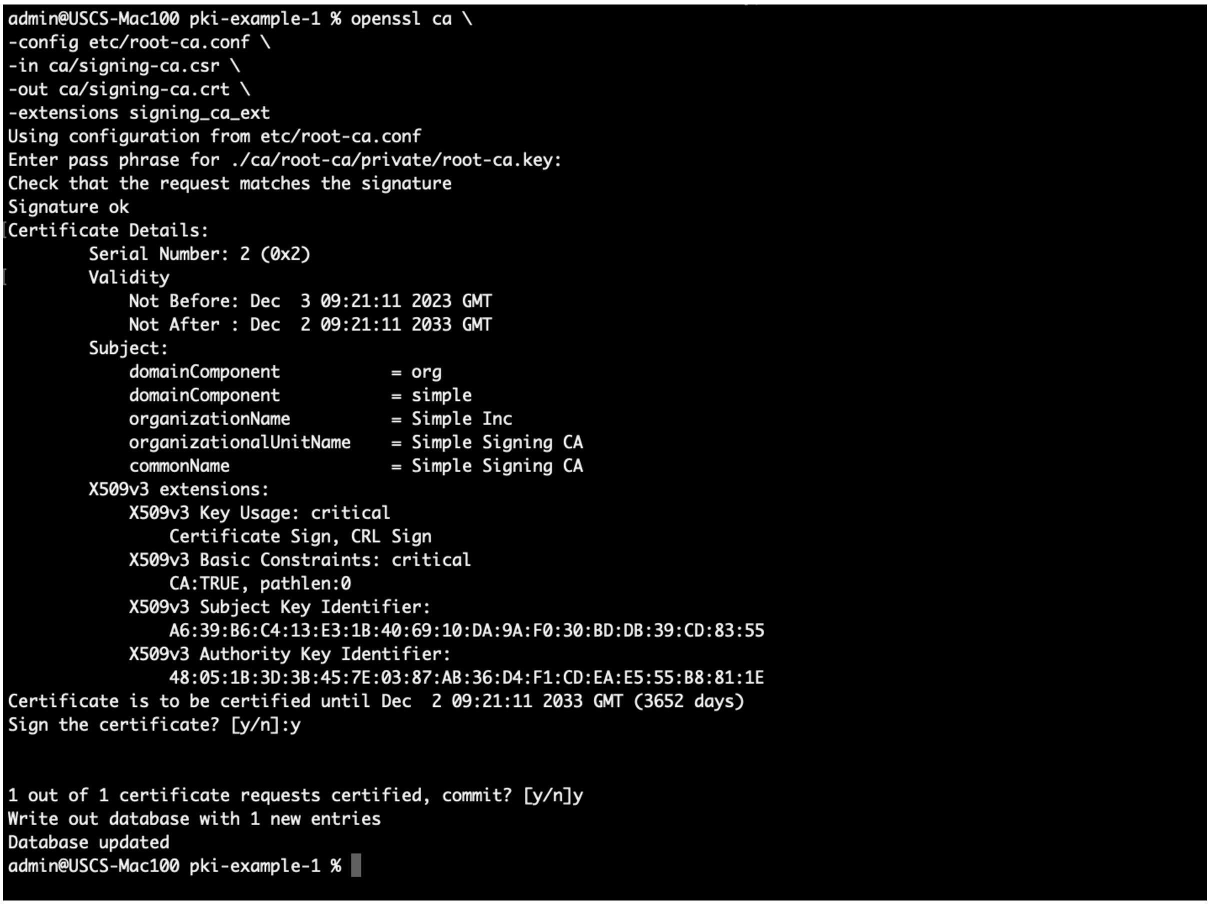


```
admin@USCS-Mac100 pki-example-1 % ls
ca      certs  crl     etc
admin@USCS-Mac100 pki-example-1 % openssl req -new \
-config etc/signing-ca.conf \
-out ca/signing-ca.csr \
-keyout ca/signing-ca/private/signing-ca.key
......+.......+...+..+.+..+...+......+...+.+......+.............+.........+...+....+...+...+...+..+............++++++++
+++++++++++++++++++++++++++++++*.........+.+...+......+..+............+...+....+........+...+............+.+++++++++++++
+++++++++++++++++++++++++*.+.........+....+.....+..........+......+.....+...+...+....+.....+......+.......+........+...
....+..+...+.+......+...+.....+.............+..+.......+.........+......+...+...+.............+.+.....+...+.......+....
.....+.........+.....+.+......+...+..+.........+.+.............+.........+.+.....+.+..+.+.......................
.+..+...+.....+.+.........................+....+.............+.....+............+...+......+.+............+......
.................+....+................+...+..+.........+..........+.+.....+....+...+..+..........+..+.+.....+....+....
+...+.........+..........+.........+.......+......+...+.............+........+.+.....+...+..........+...+.....+.........
+.+..+...++++++
..+...+.+.....+....+..+...+............+.+...+...........+..........+.....+...+......+.+...+...++++++++++++++++++++++++
++++++++++++++*.......+....+...+..+...............+.++++++++++++++++++++++++++++++++++++++++*.......+......+.........+....
+..............+.+............+..+.+.....+.+.....+.+...+......+.............+.+...........+...+.+...+......+.....+.....
.+.+..+..........+......+..++++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
admin@USCS-Mac100 pki-example-1 %
```



```
Verifying - Enter PEM pass phrase:
-----
admin@USCS-Mac100 pki-example-1 % cd ca/signing-ca/private/
admin@USCS-Mac100 private % cat signing-ca.key
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFHDBOBgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQwwHAQIdfSPjLj1ZpoCAggA
MAwGCCqGSIb3DQIJBQAwFAYIKoZIhvcNAwcECLK8bVu9Uw5NBIIEyPNH6GGgx/I3
cvVlsvnNQJPlWAiCDgbh2PIZ9k6jcXRJ2NEI7lm1icjvNyHroWHZWkwhPOiTa9uC
wOQ16LCwKkJmMKqjFyaK2QFIX1CXxTWN0Yvjn7tl6X9h+GK+Iq1q1iybjgMN+6B9
Y+ksc5HoXNAXssQBT0c3mH4K76IBffajA8NmoTNZ0xzr/L+7lqQvafNQKbv8pSUH
hFTTi+p66IvNwL7XXAEFZ3ilNerqLPUh9/t4GcZe1Qgp/ImxCtLWn24eQ0dDZEYa
BI5QNy/oaeect3vAHNiyOKVy4lVDpQUg8t2Lk7fAGD6uet7MqcIZXR7LnglszLNk
DtZ2+VSkKte8IF2pO41xPslRG4mXyk4jFIWdYTOaCBZP4j3Xz++yOshmTXO/fcgN
/UfDbrlmGU229jyTS3F35ngra5GbilqTpzvbVZwRSvRBuE3Uk6sZecFrxYLDKqQB
fTkwiQshOwrWCNn8brjN3OUrp45yUrmAdMnsOP8oj9apvWBcvOsJuM+0T+V9mNlp
3LCJu9PUTx0YmQuzUKW1rLt2+DpsDXuz6pkp8HkeHgiwNoMwKPzwmK1vZM3ukrtJ
jh8DtRBaN6XUhj3RpA/4XnOFkkm7Xe5vOGnT/tCBJ6uzBU2c0yN6+00TIm+1EUVi
Pc6jr6VLr0uBLA69mPKNd0ByQnH5G58wdo5UC5rpjRLqZNlW8uw6hmfsyij5Oobh
Fl9xd/RXB8Ef/jWCvLpUTzPVH1fHSIB19hA9aViv0rLnFOC/JjmMNj8YEe5rK6Av
vpd83yk3ow4fqq6xq53KwPwP8agjlAy4U8ivAP5XLkx4hgNvfGeSY7HrXP9+MRZJ
Agpyb+B4PS8mP32CC+FBk6ApfLm/z5ORTG7To2bdouGoXpyxcaQnm2FVqsA1iCyG
ylYXToqkrG9/mUNyAGoCaCMExEsPVUi7f5pwQdBXLsJJ6OuRDs16TWrPTq42q1kf
VaKrQOIvgmuUTwNapsfng7oYdLv/yU7N5SzEswVA82A/EtoAoNJdXxSBrxhk+42b
ilFl1FDuMIZG2P0gXvxSLuayi9NrEaKdE7qto8CIFJAhj3JpPNSm07Pm2u1BPEpk
HMlnpjHNGktT9HXdKkWEaF2kXv8Fnvx4vyjUkn9qB4MD4EdlZbB5HZGiNXbTAWcT
VNxI/FqpaCesUaI/YqMzGEpU9NSdX1zVBgCiEOR/C86NBEy6T2RsAAUkybiFXKK5
vIInYRB/ta1NeG0c+hZrCOg3/OI29viS3+5wBl7gx0JkjnlzoLtxWbXkpAg0IstD
Q+yslvJTgGIVOs6bc/aatpydPJazu1pkrewjgyASmp1o/PshAVbGpLNzj3+Y8sMj
bOeQq8/rCX1rJ+SVlVphADPlEcV4fu8mC6wow7szQOQXbTgNGaPcFOhNoskXiL4c
fr8eheZT/wixLKZrKpLGQNgmvV3HvC48wnzv77AgwaPfgB8X77Ev/lJnEiPrJgs7
FhmcEXx9XnGK9Tx3clKQMbSq7VDd7ab2cYP3rS7yjY+UOMqjonzPrj38n1Srnk+2
L3TLg2AX1dr+JYpeH1nhFYR08uBNnDqy+5KQ57EWIWAL4sYhT/34aueZ2Fuf7ptv
YTe0IkwTU1lbqctrMV8Kgg==
-----END ENCRYPTED PRIVATE KEY-----
admin@USCS-Mac100 private %
```

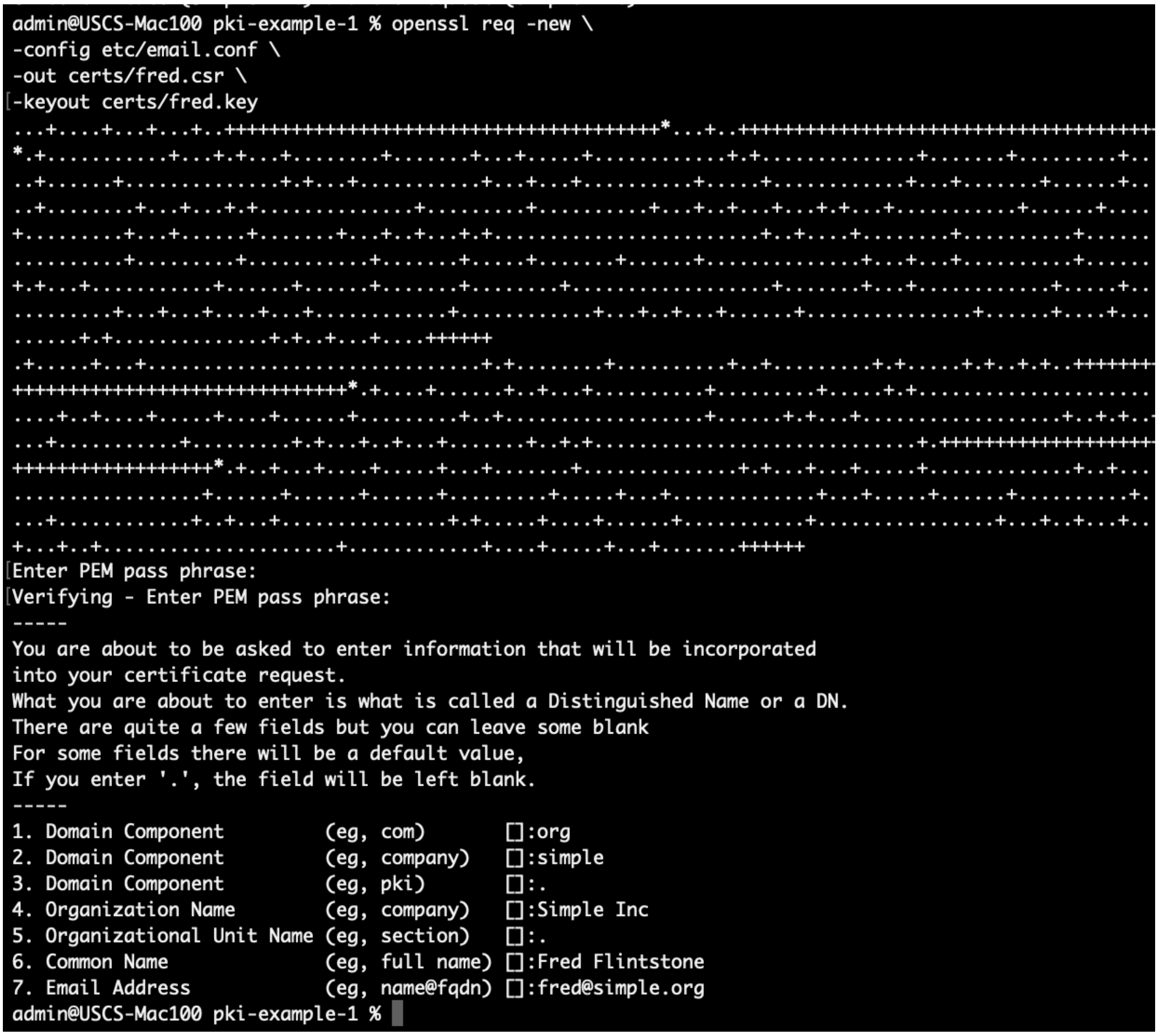
3.4 Create CA Certificate



```
admin@USCS-Mac100 pki-example-1 % openssl ca \
-config etc/root-ca.conf \
-in ca/signing-ca.csr \
-out ca/signing-ca.crt \
-extensions signing_ca_ext
Using configuration from etc/root-ca.conf
Enter pass phrase for ./ca/root-ca/private/root-ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 2 (0x2)
        Validity
            Not Before: Dec  3 09:21:11 2023 GMT
            Not After : Dec  2 09:21:11 2033 GMT
        Subject:
            domainComponent           = org
            domainComponent           = simple
            organizationName          = Simple Inc
            organizationalUnitName    = Simple Signing CA
            commonName                = Simple Signing CA
        X509v3 extensions:
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Subject Key Identifier:
                A6:39:B6:C4:13:E3:1B:40:69:10:DA:9A:F0:30:BD:DB:39:CD:83:55
            X509v3 Authority Key Identifier:
                48:05:1B:3D:3B:45:7E:03:87:AB:36:D4:F1:CD:EA:E5:55:B8:81:1E
Certificate is to be certified until Dec  2 09:21:11 2033 GMT (3652 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Database updated
admin@USCS-Mac100 pki-example-1 %
```

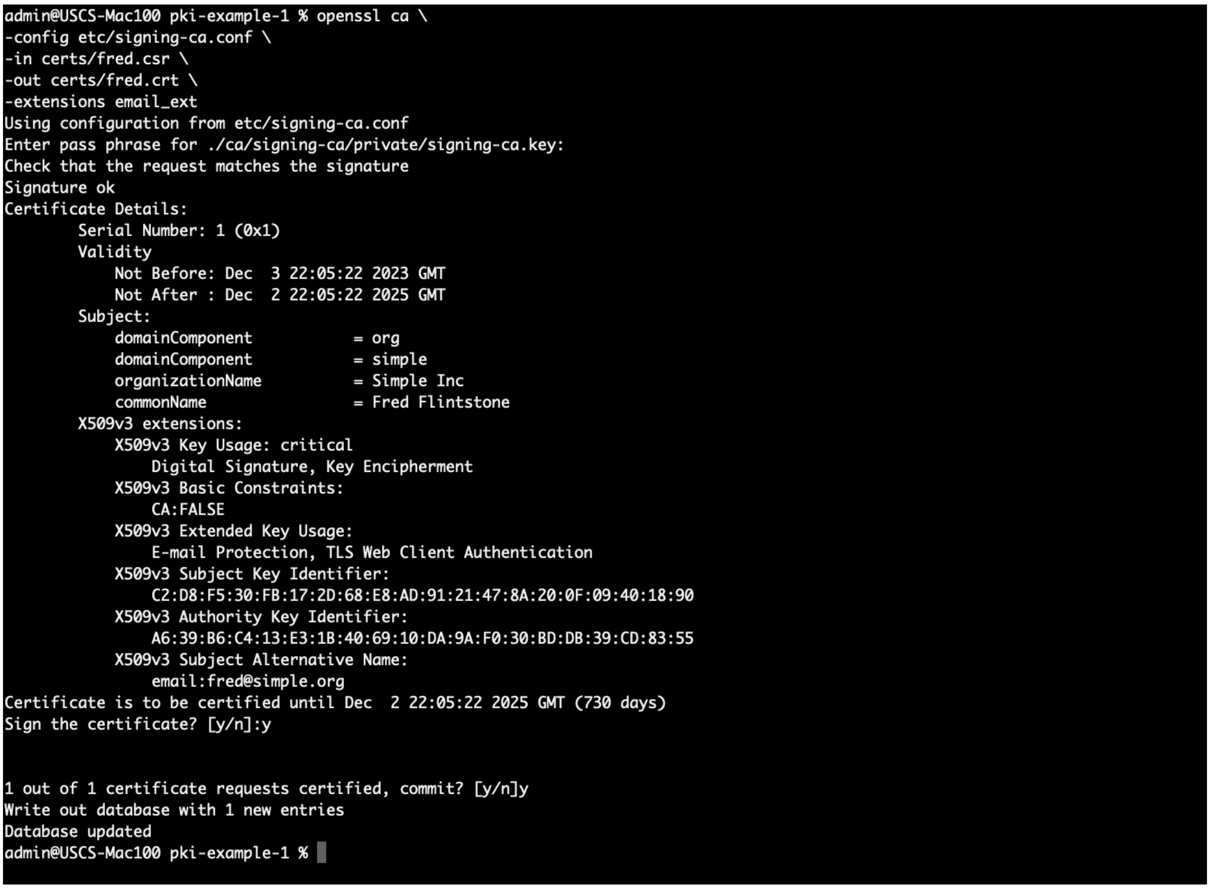
Step 4: Operate Signing CA

4.1 Create email Request



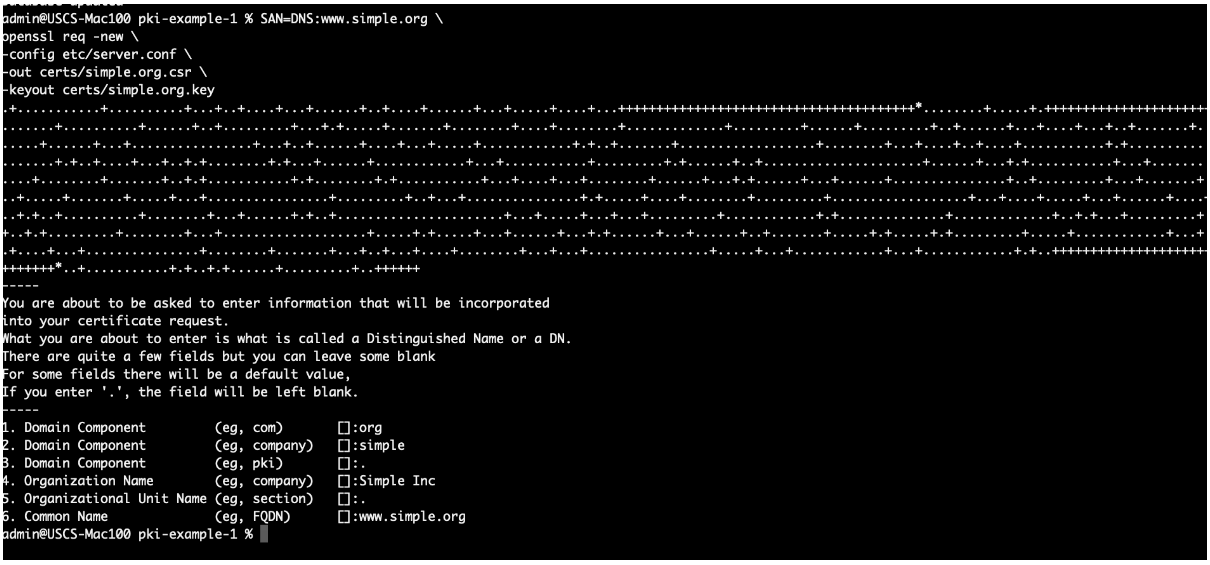
```
admin@USCS-Mac100 pki-example-1 % openssl req -new \
-config etc/email.conf \
-out certs/fred.csr \
[-keyout certs/fred.key
...+....+...+...+..++++++++++++++++++++++++++++++++++++++++*...+..++++++++++++++++++++++++++++++++++++++
*.+..........+...+.+...+........+.......+...+.....+...........+.+.............+.......+.........+..
..+......+.............+.+...+..........+...+...+.........+.....+...........+...+.......+......+..
..+........+...+...+.+.............+........+.........+...+..+...+...+.+...+..........+......+....
+.........+...+......+.......+...+..+...+.+.....................+..+....+.......+..........+......
..........+.........+...........+.......+.....+.......+......+.............+...+...+..........+......
+.+...+..........+......+......+.......+........+.................+.......+...+..........+.....+..
.........+...+...+....+...+...........+...........+...+..+...+......+..............+.......+....+...
......+.+.............+.+..+...+....++++++
.+.....+...+.........................+.+........+..........+..+.........+.+.....+.+..+.+..+++++++
+++++++++++++++++++++++++++++*.+....+......+..+...+.........+.........+.....+.+...................
....+..+....+.....+....+......+.........+..+................+......+.+...+..................+..+.+..
...+..........+.........+.+...+..+...+.......+..+.+..........................+.+++++++++++++++++++
+++++++++++++++++*.+..+...+....+.....+...+.......+.............+.+...+...+.....+...........+..+...
................+......+......+......+.........+.....+...+.............+...+.....+......+..........+.
...+...........+..+...+..............+.+.....+....+......+...........+...............+...+..+...+..
+...+..+....................+...........+....+.....+...+.......++++++
[Enter PEM pass phrase:
[Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
1. Domain Component         (eg, com)       □:org
2. Domain Component         (eg, company)   □:simple
3. Domain Component         (eg, pki)       □:.
4. Organization Name        (eg, company)   □:Simple Inc
5. Organizational Unit Name (eg, section)   □:.
6. Common Name              (eg, full name) □:Fred Flintstone
7. Email Address            (eg, name@fqdn) □:fred@simple.org
admin@USCS-Mac100 pki-example-1 %
```

4.2 Create email Certificate



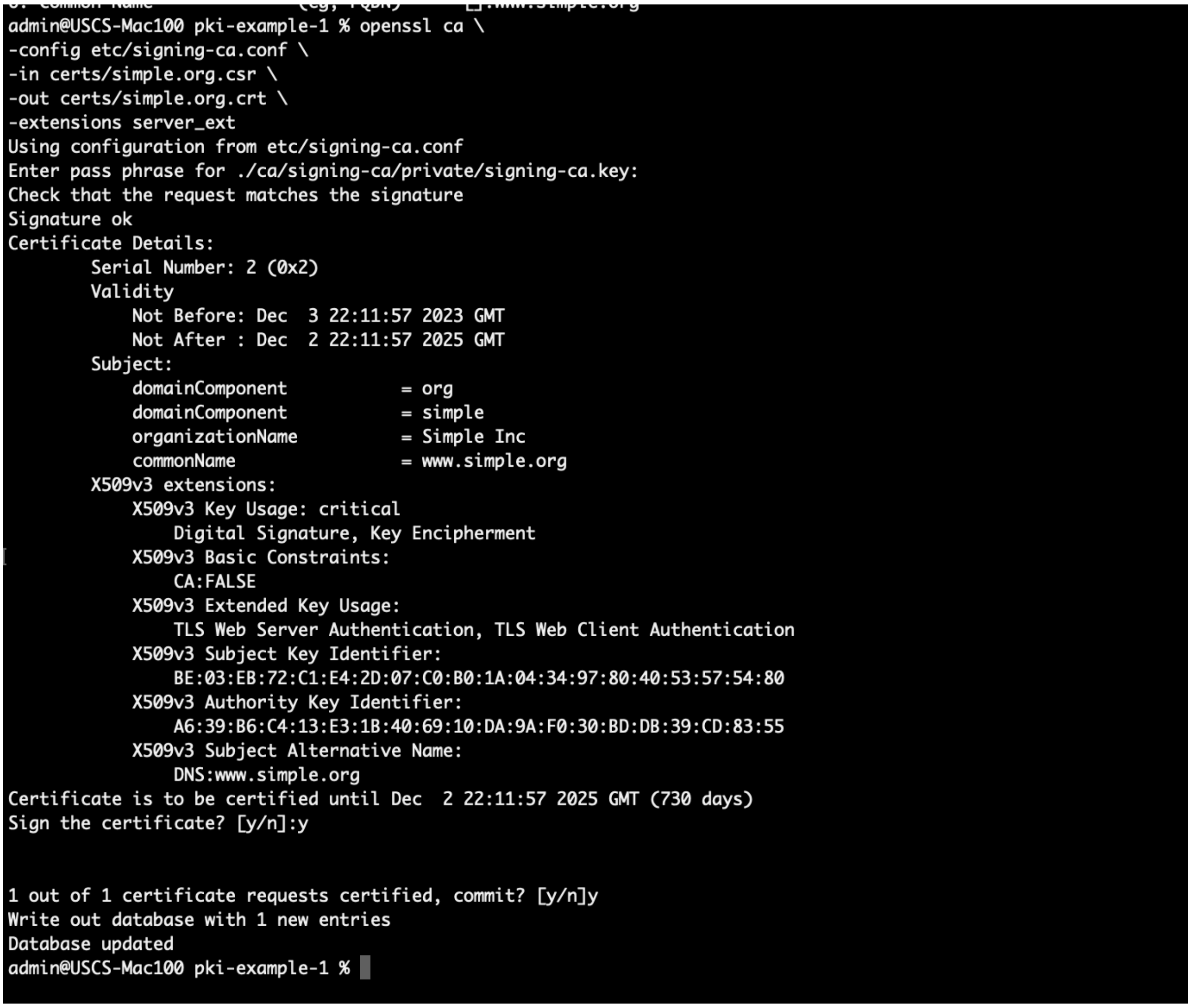
```
admin@USCS-Mac100 pki-example-1 % openssl ca \
-config etc/signing-ca.conf \
-in certs/fred.csr \
-out certs/fred.crt \
-extensions email_ext
Using configuration from etc/signing-ca.conf
Enter pass phrase for ./ca/signing-ca/private/signing-ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Dec  3 22:05:22 2023 GMT
            Not After : Dec  2 22:05:22 2025 GMT
        Subject:
            domainComponent           = org
            domainComponent           = simple
            organizationName          = Simple Inc
            commonName                = Fred Flintstone
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                E-mail Protection, TLS Web Client Authentication
            X509v3 Subject Key Identifier:
                C2:D8:F5:30:FB:17:2D:68:E8:AD:91:21:47:8A:20:0F:09:40:18:90
            X509v3 Authority Key Identifier:
                A6:39:B6:C4:13:E3:1B:40:69:10:DA:9A:F0:30:BD:DB:39:CD:83:55
            X509v3 Subject Alternative Name:
                email:fred@simple.org
Certificate is to be certified until Dec  2 22:05:22 2025 GMT (730 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Database updated
admin@USCS-Mac100 pki-example-1 %
```

4.3 Create TLS Server Request



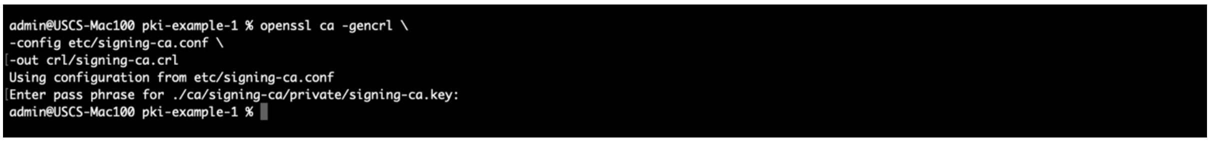
```
admin@USCS-Mac100 pki-example-1 % SAN=DNS:www.simple.org \
openssl req -new \
-config etc/server.conf \
-out certs/simple.org.csr \
-keyout certs/simple.org.key
.+..........+.........+...+..+....+...+......+..+....+......+...+.....+....+...++..+...++++++++++++++++++++++++++++++++++++++*........+.....+.++++++++++++++++++++++
........+..........+......+..+..........+...+.+.....+........+.........+.....+.........+........+..............+..........+......+..........+..+.......+...+....+...+..+........+.
......+......+...+................+...+..+.......+.....+...+......+..............+.+..+...+.+..+........+...................+.........+...+.....+..+.....+............+.+...........
........+.+..+....+...+..+.+.........+.+...+.......+.............+...+..........+........+..........+.+.......+..+.........................+.......+...+.+............+...+........
.....+........+.......+..+.+...........+.+.........+.+...........+...+....+...+.......+.........+.......+...+.+.......+...+.......+...................+..+...........+...+.........+
..+.....+.......+.....+...+.................+.........+..+...+............+.+.....+.+.....+....+.........+..........+...................+...+....+....+...+......+.....
..+.+..+..........+........+...+......+.+..+.........................+...+.....+...+...+...+...+..........+.............+.+.................+..............+..+.+...+..........+
+..+.+........+........+..+.................+.....+.+.....+...+......+...+.+......+.+.......+...+......+..+........+.....+.+.....+.+..........+.....+.............+...+
.+....+...+...............+.........+.......+...+..+...+....+........+...+...+.......+..................+......+...+..............+...+..............+.+..+++++++++++++++++++++
+++++++*..+..........+.+..+.+.....+.........+..++++++
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
1. Domain Component         (eg, com)       []:org
2. Domain Component         (eg, company)   []:simple
3. Domain Component         (eg, pki)       []:.
4. Organization Name        (eg, company)   []:Simple Inc
5. Organizational Unit Name (eg, section)   []:.
6. Common Name              (eg, FQDN)      []:www.simple.org
admin@USCS-Mac100 pki-example-1 %
```

4.4 Create TLS Service Certificate



```
6. Common Name              (eg, FQDN)       []:www.simple.org
admin@USCS-Mac100 pki-example-1 % openssl ca \
-config etc/signing-ca.conf \
-in certs/simple.org.csr \
-out certs/simple.org.crt \
-extensions server_ext
Using configuration from etc/signing-ca.conf
Enter pass phrase for ./ca/signing-ca/private/signing-ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 2 (0x2)
        Validity
            Not Before: Dec  3 22:11:57 2023 GMT
            Not After : Dec  2 22:11:57 2025 GMT
        Subject:
            domainComponent           = org
            domainComponent           = simple
            organizationName          = Simple Inc
            commonName                = www.simple.org
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Subject Key Identifier:
                BE:03:EB:72:C1:E4:2D:07:C0:B0:1A:04:34:97:80:40:53:57:54:80
            X509v3 Authority Key Identifier:
                A6:39:B6:C4:13:E3:1B:40:69:10:DA:9A:F0:30:BD:DB:39:CD:83:55
            X509v3 Subject Alternative Name:
                DNS:www.simple.org
Certificate is to be certified until Dec  2 22:11:57 2025 GMT (730 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Database updated
admin@USCS-Mac100 pki-example-1 %
```

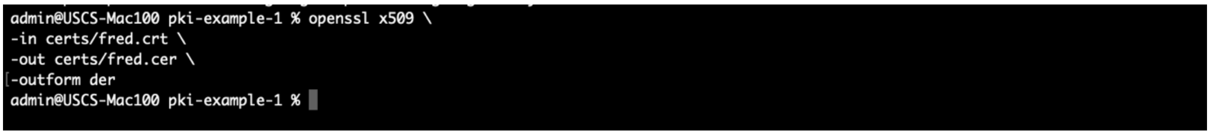
4.5 Create CRL



```
admin@USCS-Mac100 pki-example-1 % openssl ca -gencrl \
-config etc/signing-ca.conf \
-out crl/signing-ca.crl
Using configuration from etc/signing-ca.conf
Enter pass phrase for ./ca/signing-ca/private/signing-ca.key:
admin@USCS-Mac100 pki-example-1 %
```

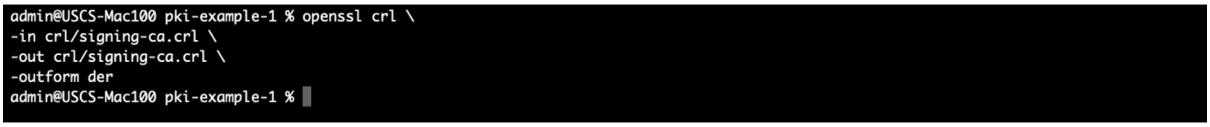
Step 5: Output Formats

5.1 Create DER Certificate



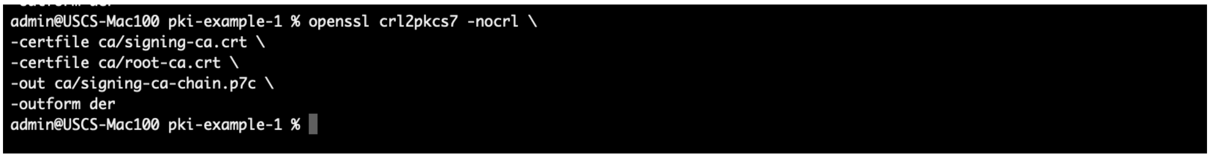
```
admin@USCS-Mac100 pki-example-1 % openssl x509 \
-in certs/fred.crt \
-out certs/fred.cer \
[-outform der
admin@USCS-Mac100 pki-example-1 % 
```

5.2 Create DER CRL



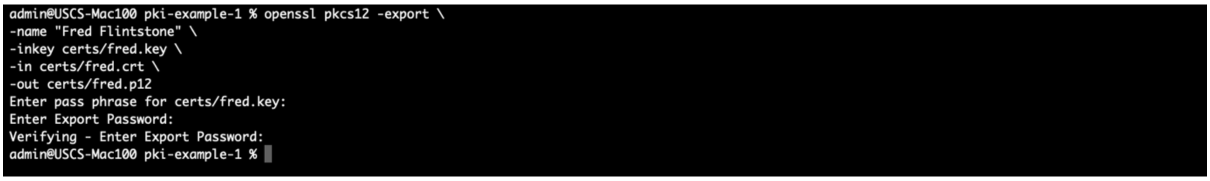
```
admin@USCS-Mac100 pki-example-1 % openssl crl \
-in crl/signing-ca.crl \
-out crl/signing-ca.crl \
-outform der
admin@USCS-Mac100 pki-example-1 % 
```

5.3 Create PKCS#7



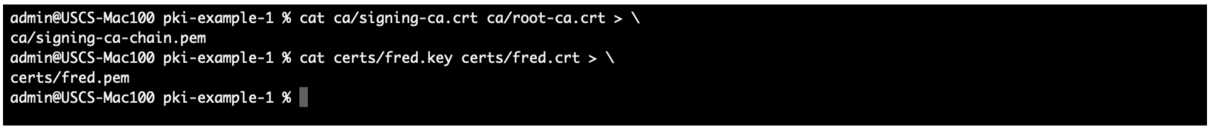
```
admin@USCS-Mac100 pki-example-1 % openssl crl2pkcs7 -nocrl \
-certfile ca/signing-ca.crt \
-certfile ca/root-ca.crt \
-out ca/signing-ca-chain.p7c \
-outform der
admin@USCS-Mac100 pki-example-1 % 
```

5.4 Create PKCS#12



```
admin@USCS-Mac100 pki-example-1 % openssl pkcs12 -export \
-name "Fred Flintstone" \
-inkey certs/fred.key \
-in certs/fred.crt \
-out certs/fred.p12
Enter pass phrase for certs/fred.key:
Enter Export Password:
Verifying - Enter Export Password:
admin@USCS-Mac100 pki-example-1 % 
```

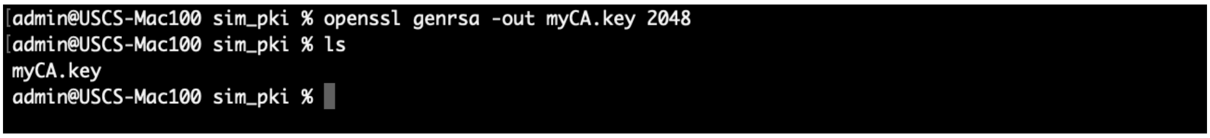
5.5 Create PEM Bundle



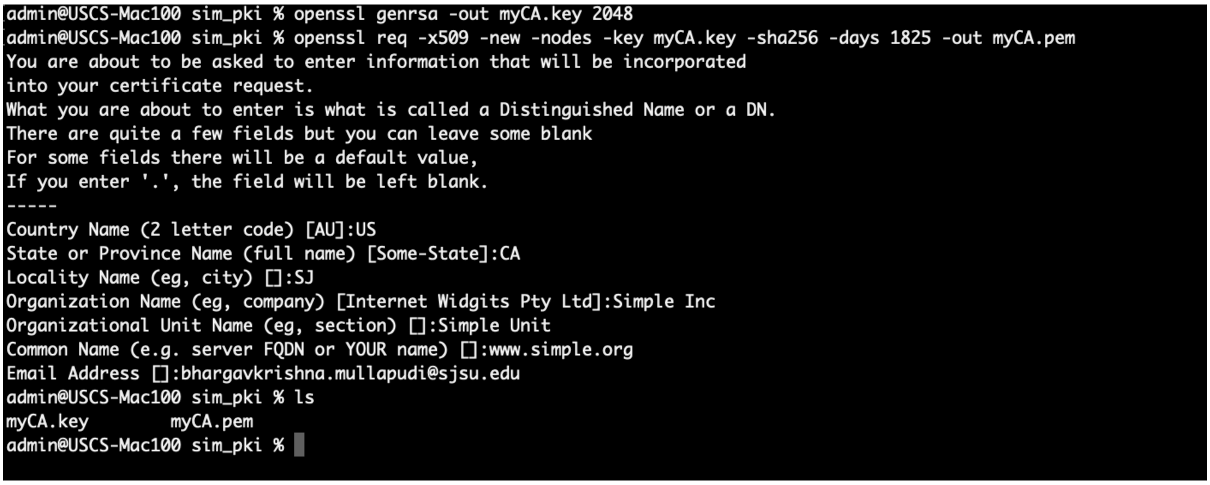
```
admin@USCS-Mac100 pki-example-1 % cat ca/signing-ca.crt ca/root-ca.crt > \
ca/signing-ca-chain.pem
admin@USCS-Mac100 pki-example-1 % cat certs/fred.key certs/fred.crt > \
certs/fred.pem
admin@USCS-Mac100 pki-example-1 % 
```

Step 6: Install the web server Tomcat through link: https://tomcat.apache.org/tomcat-9.0-doc/ssl-howto.html

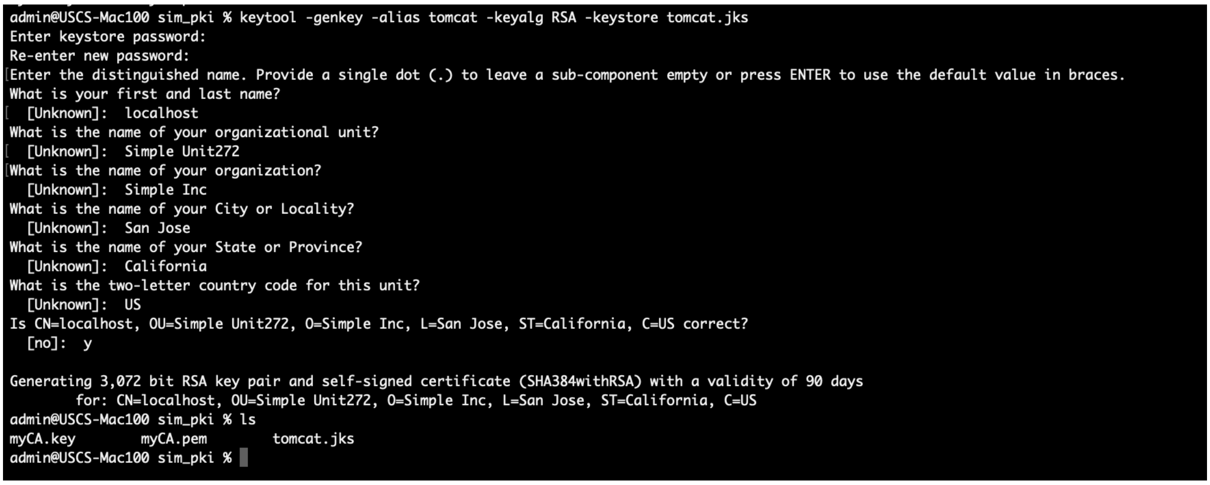
Follow the Below commands:



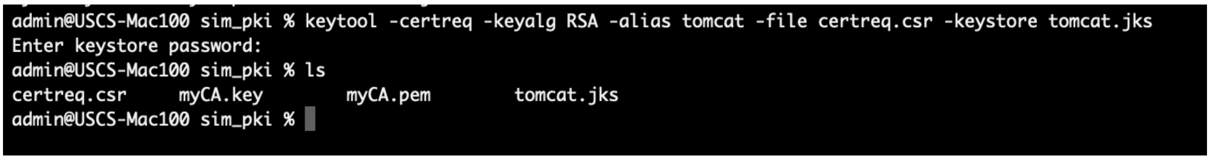
```
[admin@USCS-Mac100 sim_pki % openssl genrsa -out myCA.key 2048
[admin@USCS-Mac100 sim_pki % ls
myCA.key
admin@USCS-Mac100 sim_pki % 
```



```
admin@USCS-Mac100 sim_pki % openssl genrsa -out myCA.key 2048
admin@USCS-Mac100 sim_pki % openssl req -x509 -new -nodes -key myCA.key -sha256 -days 1825 -out myCA.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:SJ
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Simple Inc
Organizational Unit Name (eg, section) []:Simple Unit
Common Name (e.g. server FQDN or YOUR name) []:www.simple.org
Email Address []:bhargavkrishna.mullapudi@sjsu.edu
admin@USCS-Mac100 sim_pki % ls
myCA.key        myCA.pem
admin@USCS-Mac100 sim_pki % 
```

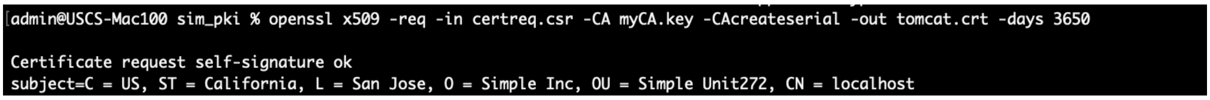


```
admin@USCS-Mac100 sim_pki % keytool -genkey -alias tomcat -keyalg RSA -keystore tomcat.jks
Enter keystore password:
Re-enter new password:
[Enter the distinguished name. Provide a single dot (.) to leave a sub-component empty or press ENTER to use the default value in braces.
What is your first and last name?
[  [Unknown]:  localhost
What is the name of your organizational unit?
[  [Unknown]:  Simple Unit272
[What is the name of your organization?
  [Unknown]:  Simple Inc
What is the name of your City or Locality?
  [Unknown]:  San Jose
What is the name of your State or Province?
  [Unknown]:  California
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=localhost, OU=Simple Unit272, O=Simple Inc, L=San Jose, ST=California, C=US correct?
  [no]:  y

Generating 3,072 bit RSA key pair and self-signed certificate (SHA384withRSA) with a validity of 90 days
        for: CN=localhost, OU=Simple Unit272, O=Simple Inc, L=San Jose, ST=California, C=US
admin@USCS-Mac100 sim_pki % ls
myCA.key        myCA.pem        tomcat.jks
admin@USCS-Mac100 sim_pki % 
```



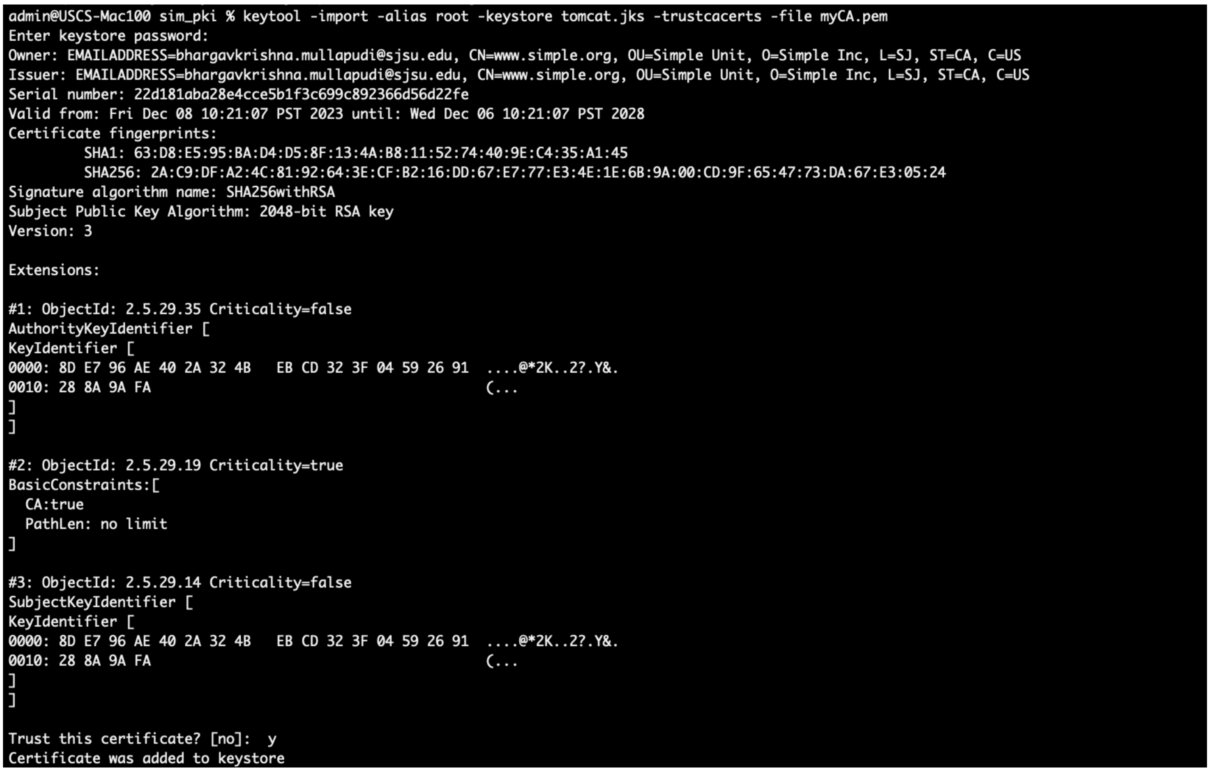
```
admin@USCS-Mac100 sim_pki % keytool -certreq -keyalg RSA -alias tomcat -file certreq.csr -keystore tomcat.jks
Enter keystore password:
admin@USCS-Mac100 sim_pki % ls
certreq.csr     myCA.key        myCA.pem        tomcat.jks
admin@USCS-Mac100 sim_pki % 
```

Using the root certificate, Sign the certificate for Tomcat:

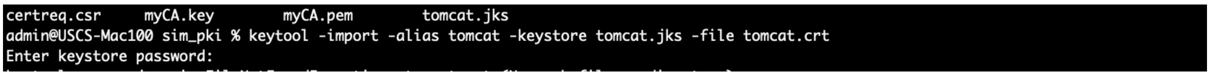


```
[admin@USCS-Mac100 sim_pki % openssl x509 -req -in certreq.csr -CA myCA.key -CAcreateserial -out tomcat.crt -days 3650

Certificate request self-signature ok
subject=C = US, ST = California, L = San Jose, O = Simple Inc, OU = Simple Unit272, CN = localhost
```

Import Tomcat certificate and Root certificate:

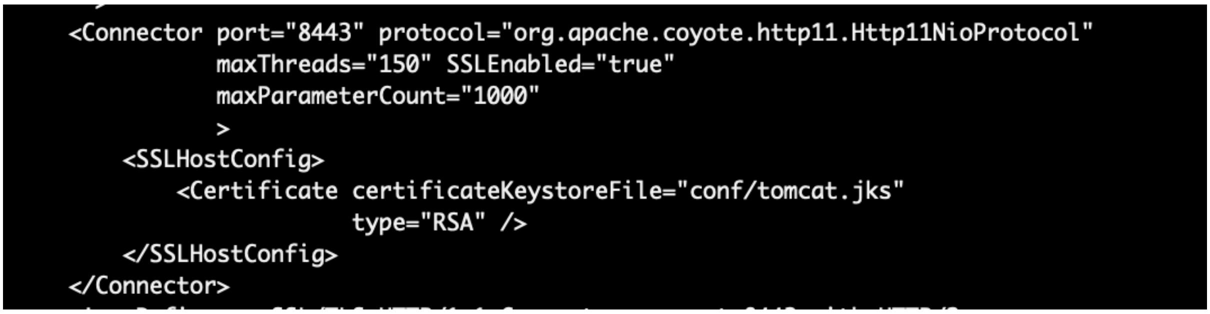


```
admin@USCS-Mac100 sim_pki % keytool -import -alias root -keystore tomcat.jks -trustcacerts -file myCA.pem
Enter keystore password:
Owner: EMAILADDRESS=bhargavkrishna.mullapudi@sjsu.edu, CN=www.simple.org, OU=Simple Unit, O=Simple Inc, L=SJ, ST=CA, C=US
Issuer: EMAILADDRESS=bhargavkrishna.mullapudi@sjsu.edu, CN=www.simple.org, OU=Simple Unit, O=Simple Inc, L=SJ, ST=CA, C=US
Serial number: 22d181aba28e4cce5b1f3c699c892366d56d22fe
Valid from: Fri Dec 08 10:21:07 PST 2023 until: Wed Dec 06 10:21:07 PST 2028
Certificate fingerprints:
         SHA1: 63:D8:E5:95:BA:D4:D5:8F:13:4A:B8:11:52:74:40:9E:C4:35:A1:45
         SHA256: 2A:C9:DF:A2:4C:81:92:64:3E:CF:B2:16:DD:67:E7:77:E3:4E:1E:6B:9A:00:CD:9F:65:47:73:DA:67:E3:05:24
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 8D E7 96 AE 40 2A 32 4B   EB CD 32 3F 04 59 26 91  ....@*2K..2?.Y&.
0010: 28 8A 9A FA                                        (...
]
]

#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen: no limit
]

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 8D E7 96 AE 40 2A 32 4B   EB CD 32 3F 04 59 26 91  ....@*2K..2?.Y&.
0010: 28 8A 9A FA                                        (...
]
]

Trust this certificate? [no]:  y
Certificate was added to keystore
```



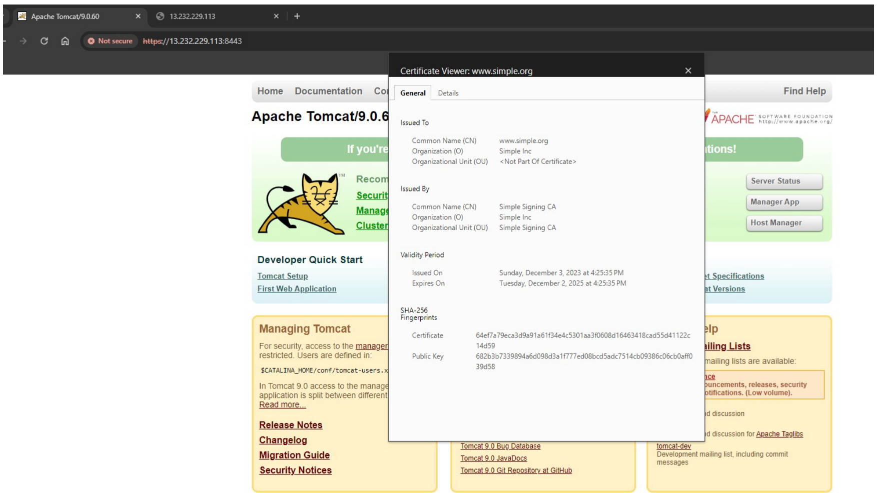
```
certreq.csr     myCA.key        myCA.pem        tomcat.jks
admin@USCS-Mac100 sim_pki % keytool -import -alias tomcat -keystore tomcat.jks -file tomcat.crt
Enter keystore password:
```

Update server.xml for the Tomcat Connector



```
    <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
               maxThreads="150" SSLEnabled="true"
               maxParameterCount="1000"
               >
        <SSLHostConfig>
            <Certificate certificateKeystoreFile="conf/tomcat.jks"
                         type="RSA" />
        </SSLHostConfig>
    </Connector>
```

Start-Up Tomcat



Certificate Viewer: www.simple.org

General | Details

Issued To

Common Name (CN)	www.simple.org
Organization (O)	Simple Inc
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

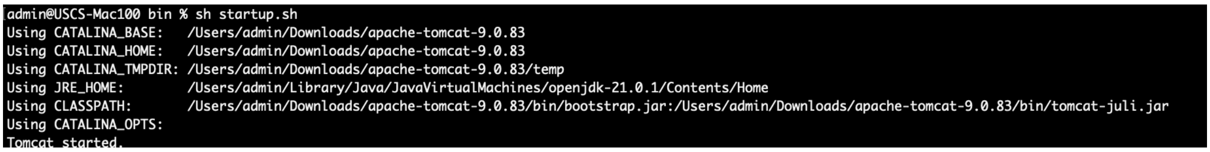
Common Name (CN)	Simple Signing CA
Organization (O)	Simple Inc
Organizational Unit (OU)	Simple Signing CA

Validity Period

Issued On	Sunday, December 3, 2023 at 4:25:35 PM
Expires On	Tuesday, December 2, 2025 at 4:25:35 PM

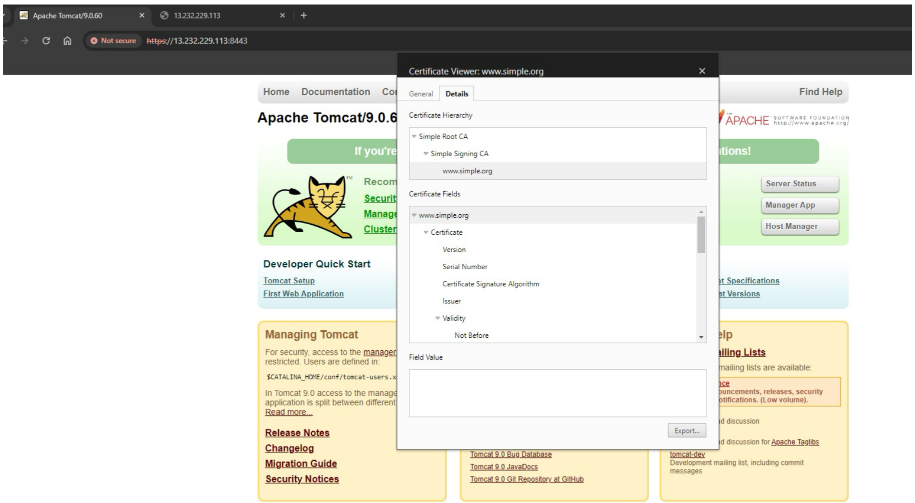
SHA-256 Fingerprints

Certificate	64ef7a79eca3d9a91a61f34e4c5301aa3f0608d16463418cad55d41122c14d59
Public Key	682b3b7339894a6d098d3a1f777ed08bcd5adc7514cb09386c06cb0aff039d58



```
admin@USCS-Mac100 bin % sh startup.sh
Using CATALINA_BASE:   /Users/admin/Downloads/apache-tomcat-9.0.83
Using CATALINA_HOME:   /Users/admin/Downloads/apache-tomcat-9.0.83
Using CATALINA_TMPDIR: /Users/admin/Downloads/apache-tomcat-9.0.83/temp
Using JRE_HOME:        /Users/admin/Library/Java/JavaVirtualMachines/openjdk-21.0.1/Contents/Home
Using CLASSPATH:       /Users/admin/Downloads/apache-tomcat-9.0.83/bin/bootstrap.jar:/Users/admin/Downloads/apache-tomcat-9.0.83/bin/tomcat-juli.jar
Using CATALINA_OPTS:
Tomcat started.
```

Validate TLS



Certificate Viewer: www.simple.org

General | Details

Certificate Hierarchy

- Simple Root CA
  - Simple Signing CA
    - www.simple.org

Certificate Fields

- www.simple.org
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity
      - Not Before

Field Value

Export...