Name: Shaikh Amaan Shaikh Farooque PRN: 2019BTECS00076
Class: B.Tech CSE Batch: B3
CNS Lab (MKC) Assignment-14

Date: 30th Nov 2022 Page No. 1

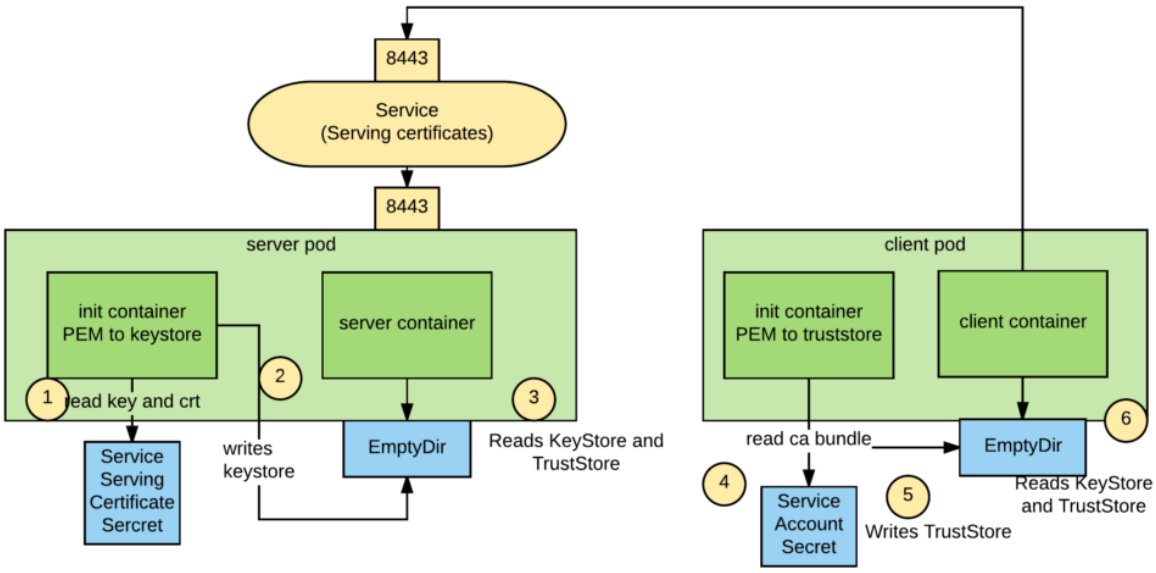
Title: Digital Certificate

Aim: To generate a digital certificate using keytool utility

Introduction:

keytool is a key and certificate management utility. It allows users to administer their own public/private key pairs and associated certificates for use in self-authentication (where the user authenticates himself/herself to other users/services) or data integrity and authentication services, using digital signatures.

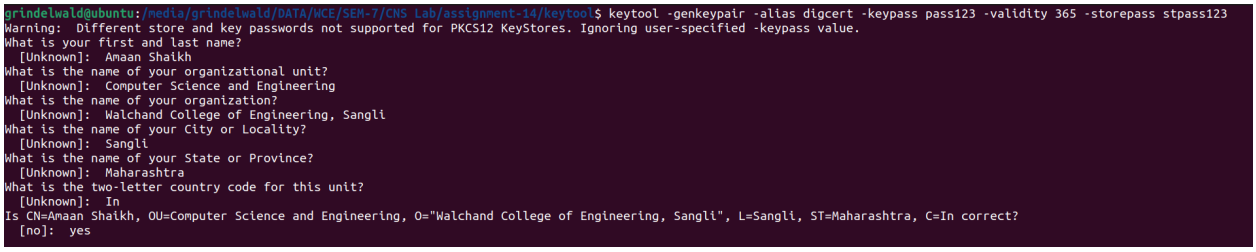
Theory:



Procedure:

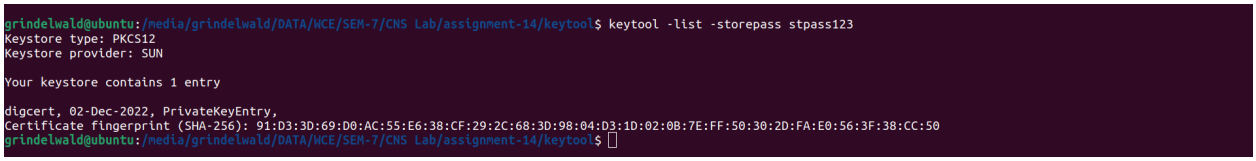
1. Creating a self signed certificate:

```
keytool -genkeypair -alias digcert -keypass pass123
-validity 365 -storepass stpass123
```



2. Listing Certificates in the keystore

```
keytool -list -storepass stpass123
```



3. Listing the certificate

```
keytool -list -v -alias digcert -storepass stpass123
```

```
grindelwald@ubuntu:/media/grindelwald/DATA/WCE/SEM-7/CNS Lab/assignment-14/keytool$ keytool -list -v -alias digcert -storepass stpass123
Alias name: digcert
Creation date: 02-Dec-2022
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=Amaan Shaikh, OU=Computer Science and Engineering, O="Walchand College of Engineering, Sangli", L=Sangli, ST=Maharashtra, C=In
Issuer: CN=Amaan Shaikh, OU=Computer Science and Engineering, O="Walchand College of Engineering, Sangli", L=Sangli, ST=Maharashtra, C=In
Serial number: 336fef67
Valid from: Fri Dec 02 11:52:45 IST 2022 until: Sat Dec 02 11:52:45 IST 2023
Certificate fingerprints:
         SHA1: 52:40:AA:DF:82:0C:13:10:1F:04:59:29:F9:4D:BE:E4:9C:7E:C5:09
         SHA256: 91:D3:3D:69:D0:AC:55:E6:38:CF:29:2C:68:3D:98:04:D3:1D:02:0B:7E:FF:50:30:2D:FA:E0:56:3F:38:CC:50
Signature algorithm name: SHA256withDSA
Subject Public Key Algorithm: 2048-bit DSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 49 6B 5E E6 1A EF 34 CC   EE 6A 72 EB E7 0B 6B E4  Ih^...4..jr...k.
0010: 25 08 B9 DA                                        %...
]
]
```

4. Exporting certificate to file server.cer

```
keytool -export -alias digcert -storepass stpass123
-file server.cer -keystore keystore.jks
```

```
grindelwald@ubuntu:/media/grindelwald/DATA/WCE/SEM-7/CNS Lab/assignment-14/keytool$ keytool -export -alias digcert -storepass stpass123 -file server.cer -keystore keystore.j
ks
Certificate stored in file <server.cer>
```

5. Creating truststore and adding certificate to the it

```
keytool -import -v -trustcacerts -alias digcert
-file server.cer -keystore cacerts.jks -keypass
pass123
```

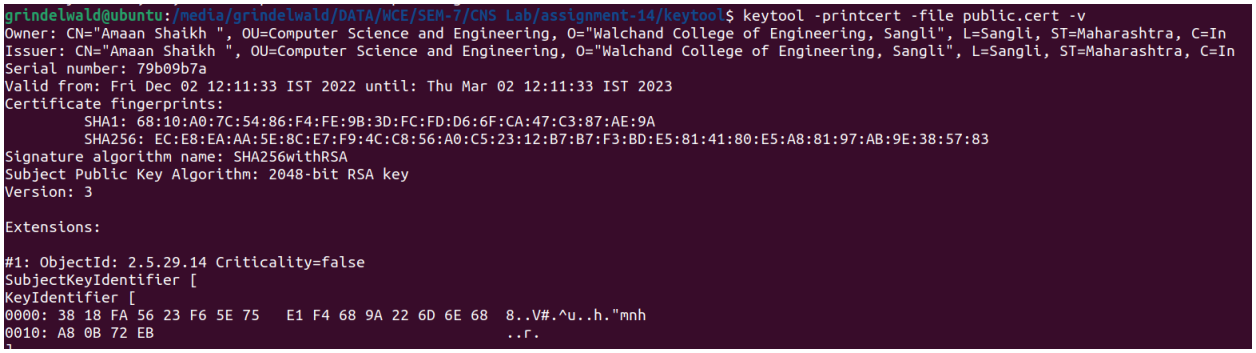
```
grindelwald@ubuntu:/media/grindelwald/DATA/WCE/SEM-7/CNS Lab/assignment-14/keytool$ keytool -import -v -trustcacerts -alias digcert -file server.cer -keystore cacerts.jks -k
eypass pass123
Enter keystore password:
Re-enter new password:
Owner: CN="Amaan Shaikh ", OU=Computer Science and Engineering, O="Walchand College of Engineering, Sangli", L=Sangli, ST=Maharashtra, C=In
Issuer: CN="Amaan Shaikh ", OU=Computer Science and Engineering, O="Walchand College of Engineering, Sangli", L=Sangli, ST=Maharashtra, C=In
Serial number: 79b09b7a
Valid from: Fri Dec 02 12:11:33 IST 2022 until: Thu Mar 02 12:11:33 IST 2023
Certificate fingerprints:
         SHA1: 68:10:A0:7C:54:86:F4:FE:9B:3D:FC:FD:D6:6F:CA:47:C3:87:AE:9A
         SHA256: EC:E8:EA:AA:5E:8C:E7:F9:4C:C8:56:A0:C5:23:12:B7:B7:F3:BD:E5:81:41:80:E5:A8:81:97:AB:9E:38:57:83
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 38 18 FA 56 23 F6 5E 75   E1 F4 68 9A 22 6D 6E 68  8..V#.^u..h."mnh
0010: A8 0B 72 EB                                        ..r.
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
[Storing cacerts.jks]
grindelwald@ubuntu:/media/grindelwald/DATA/WCE/SEM-7/CNS Lab/assignment-14/keytool$
```

6. Exporting certificate from keystore.jks to public.cert

```
keytool -export -alias digcert -keystore
keystore.jks -rfc -file public.cert
```

7. Printing the certificate

```
keytool -printcert -file public.cert -v
```



Conclusion: Generated digital certificate using java keytool utility successfully