Cryptography and Network Security

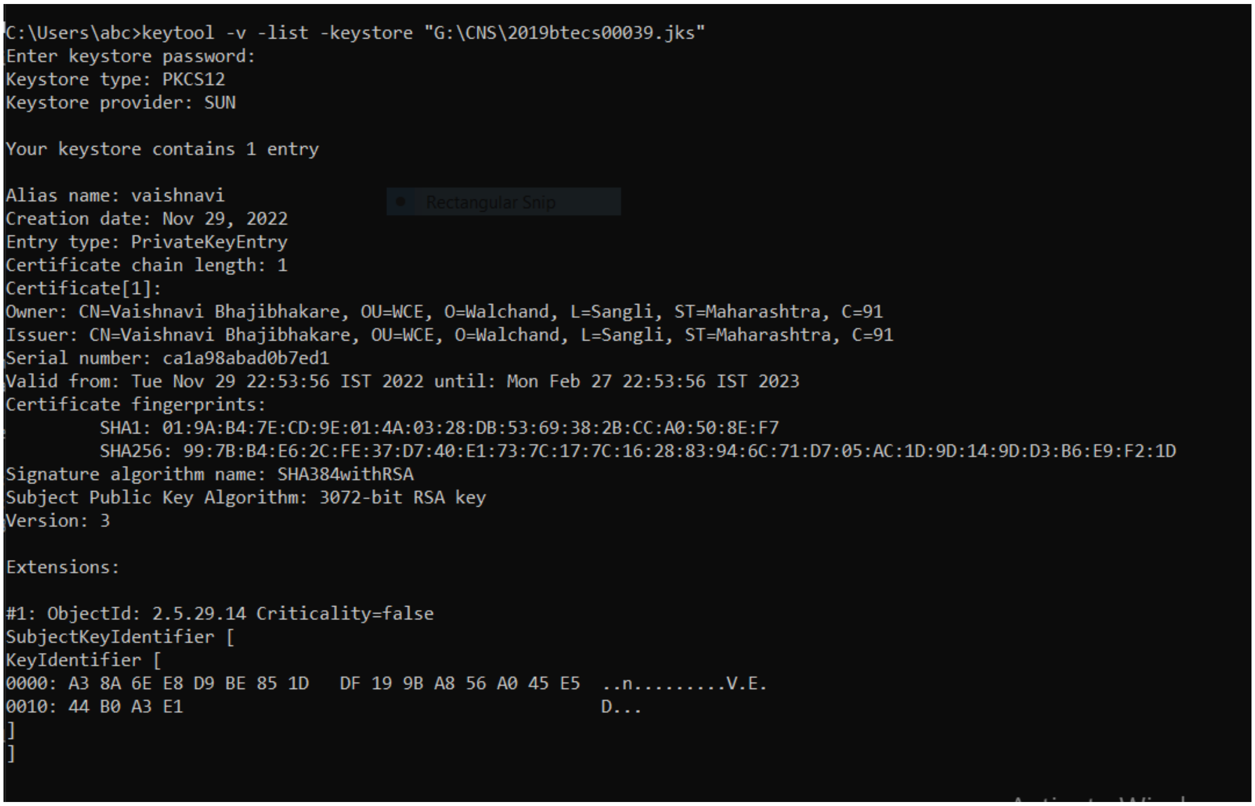
Assignment 14 – Generation of digital Certificate

Name: Vaishnavi Santosh Bhajibhakare

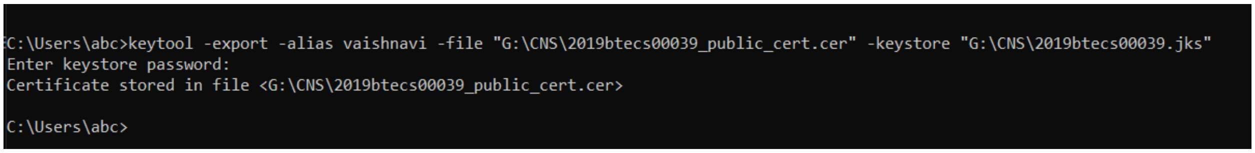
PRN: 2019BTECS00039

Batch: B2

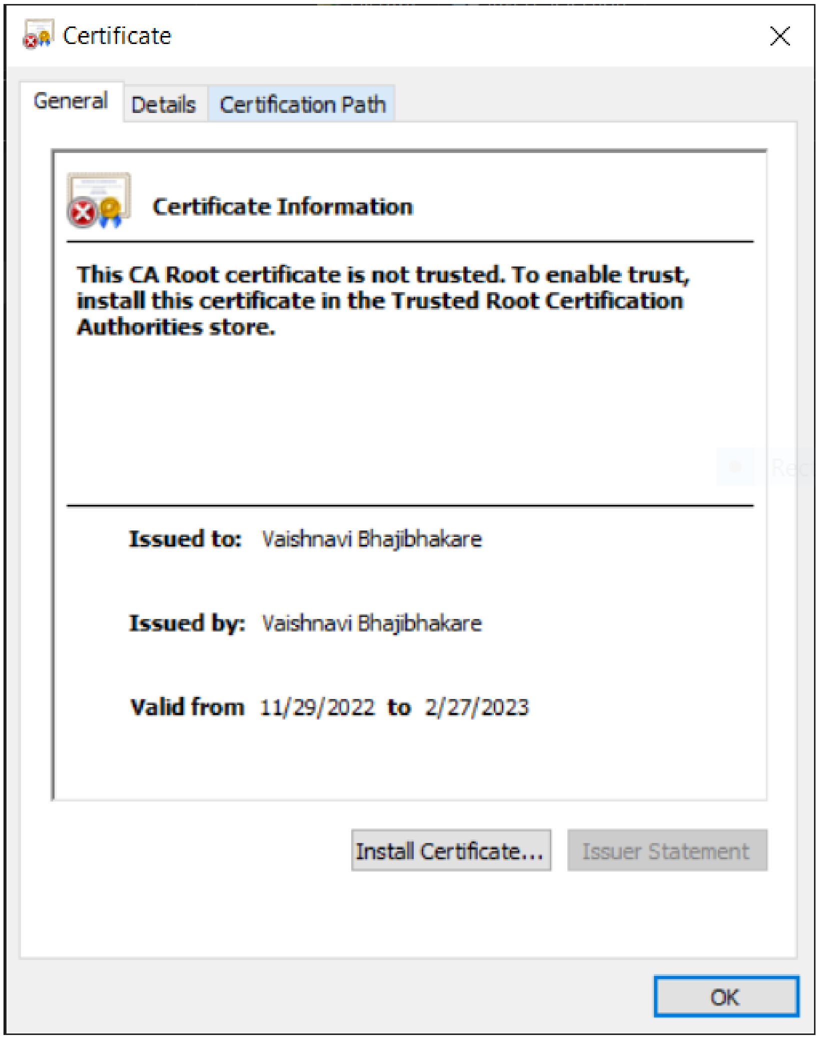
Problem statement : Generation of digital certificate using java key tool and key store utilities or by using open SSL



```
C:\Users\abc>keytool -v -list -keystore "G:\CNS\2019btecs00039.jks"
Enter keystore password:
Keystore type: PKCS12
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: vaishnavi
Creation date: Nov 29, 2022
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=Vaishnavi Bhajibhakare, OU=WCE, O=Walchand, L=Sangli, ST=Maharashtra, C=91
Issuer: CN=Vaishnavi Bhajibhakare, OU=WCE, O=Walchand, L=Sangli, ST=Maharashtra, C=91
Serial number: ca1a98abad0b7ed1
Valid from: Tue Nov 29 22:53:56 IST 2022 until: Mon Feb 27 22:53:56 IST 2023
Certificate fingerprints:
         SHA1: 01:9A:B4:7E:CD:9E:01:4A:03:28:DB:53:69:38:2B:CC:A0:50:8E:F7
         SHA256: 99:7B:B4:E6:2C:FE:37:D7:40:E1:73:7C:17:7C:16:28:83:94:6C:71:D7:05:AC:1D:9D:14:9D:D3:B6:E9:F2:1D
Signature algorithm name: SHA384withRSA
Subject Public Key Algorithm: 3072-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: A3 8A 6E E8 D9 BE 85 1D   DF 19 9B A8 56 A0 45 E5  ..n.........V.E.
0010: 44 B0 A3 E1                                        D...
]
]
```



```
C:\Users\abc>keytool -export -alias vaishnavi -file "G:\CNS\2019btecs00039_public_cert.cer" -keystore "G:\CNS\2019btecs00039.jks"
Enter keystore password:
Certificate stored in file <G:\CNS\2019btecs00039_public_cert.cer>

C:\Users\abc>
```



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: Vaishnavi Bhajibhakare

Issued by: Vaishnavi Bhajibhakare

Valid from 11/29/2022 to 2/27/2023

Applications :

- Digital certificates are used for to secure email to identify one user to another

- It may also used for electronic document signing.