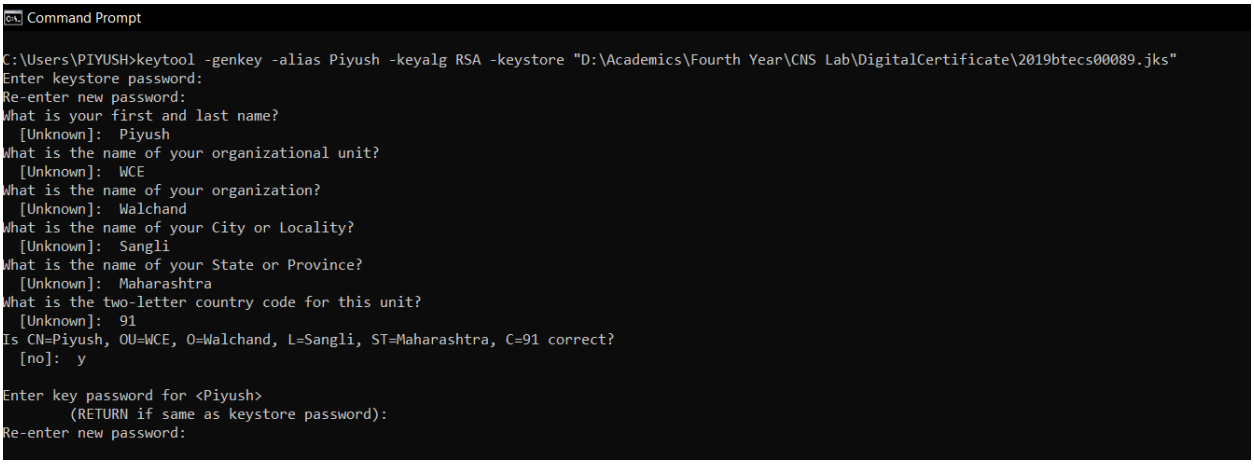
Cryptography and Network Security

Name: Piyush Mhaske Batch: B3
PRN : 2019BTECS00089

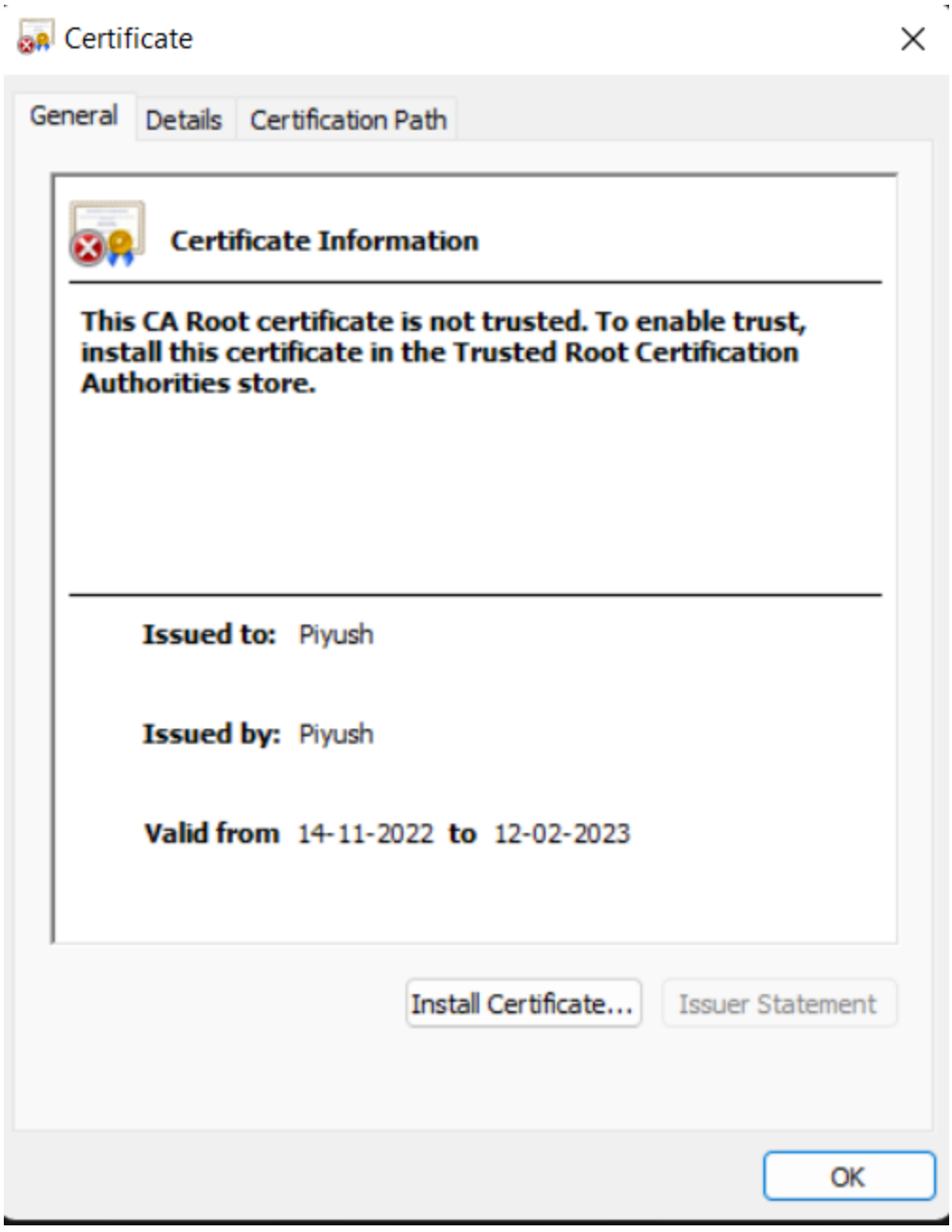
Generation of digital Certificate

Generation of digital certificate using **java key tool and key store utilities or by using open SSL**



```
C:\Users\PIYUSH>keytool -v -list -keystore "D:\Academics\Fourth Year\CNS Lab\DigitalCertificate\2019btecs00089.jks"
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: piyush
Creation date: 14 Nov, 2022
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=Piyush, OU=WCE, O=Walchand, L=Sangli, ST=Maharashtra, C=91
Issuer: CN=Piyush, OU=WCE, O=Walchand, L=Sangli, ST=Maharashtra, C=91
Serial number: 5425e0d3
Valid from: Mon Nov 14 15:00:21 IST 2022 until: Sun Feb 12 15:00:21 IST 2023
Certificate fingerprints:
         MD5:  FA:1A:F2:B7:4E:39:CE:93:E3:20:52:0A:84:42:31:30
         SHA1: 54:F7:3F:9D:D8:09:02:DC:5D:63:B1:70:1C:9A:58:E1:7B:2D:A9:22
         SHA256: D1:AF:25:CA:69:93:75:6C:95:9E:56:6E:89:E7:D3:EC:D2:5C:E9:A3:71:C3:E8:0F:82:8A:34:C3:F5:7C:98:37
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: D1 38 AF 41 68 59 26 0A   88 29 41 B1 25 EF 56 19  .8.AhY&..)A.%.V.
0010: DD 0F F2 41                                        ...A
]
]



*******************************************
*******************************************
```

```
C:\Users\PIYUSH>keytool -export -alias piyush -file "D:\Academics\Fourth Year\CNS Lab\DigitalCertificate\2019btecs00089_public_cert.cer" -keystore "D:\Academics\Fourth Year\CNS Lab\DigitalCertificate\2019btecs00
089.jks"
Enter keystore password:
Certificate stored in file <D:\Academics\Fourth Year\CNS Lab\DigitalCertificate\2019btecs00089_public_cert.cer>

C:\Users\PIYUSH>
```



Applications :

- Digital certificates are used for to secure email to identify one user to another
- It may also used for electronic document signing.