

# **Cryptography & Network Security**

**PRN - 2019BTECS00026**

**Name - Niraja Vasudev Kulkarni**

**Batch - B1**

## **Assignment - 14**

**Title:** Digital Certificate Generation

**Aim:** To Demonstrate Digital Certificate Generation using keytool

**Theory:**

Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender. A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. Digital certificate is used to attach public key with a particular individual or an entity.

**Digital certificate contains:-**

Name of certificate holder, Serial number which is used to uniquely identify a certificate, the individual or the entity identified by the certificate, Expiration dates, Copy of certificate holder's public key, Digital Signature of the certificate issuing authority.

**Screenshots:**

```

C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19043.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nachi\Digital_signature>"C:\Program Files\Java\jdk-15.0.2\bin\keytool" -genkeypair -alias niraja -keystore niraja.pfx -storepass niraja2002 -validity 365 -keyalg RSA -keysize 2048 -storetype pkcs12
What is your first and last name?
  [Unknown]: Niraja Kulkarni
What is the name of your organizational unit?
  [Unknown]: CSE
What is the name of your organization?
  [Unknown]: WCE
What is the name of your City or Locality?
  [Unknown]: Sangli
What is the name of your State or Province?
  [Unknown]: Maharashtra
What is the two-letter country code for this unit?
  [Unknown]: IN
Is CN=Niraja Kulkarni, OU=CSE, O=WCE, L=Sangli, ST=Maharashtra, C=IN correct?
  [no]: yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 365 days
    for: CN=Niraja Kulkarni, OU=CSE, O=WCE, L=Sangli, ST=Maharashtra, C=IN
C:\Users\nachi\Digital_signature>

```

```

C:\Users\nachi\Digital_signature>keytool -v -list -keystore niraja.pfx
Enter keystore password:
Keystore type: PKCS12
Keystore provider: SUN

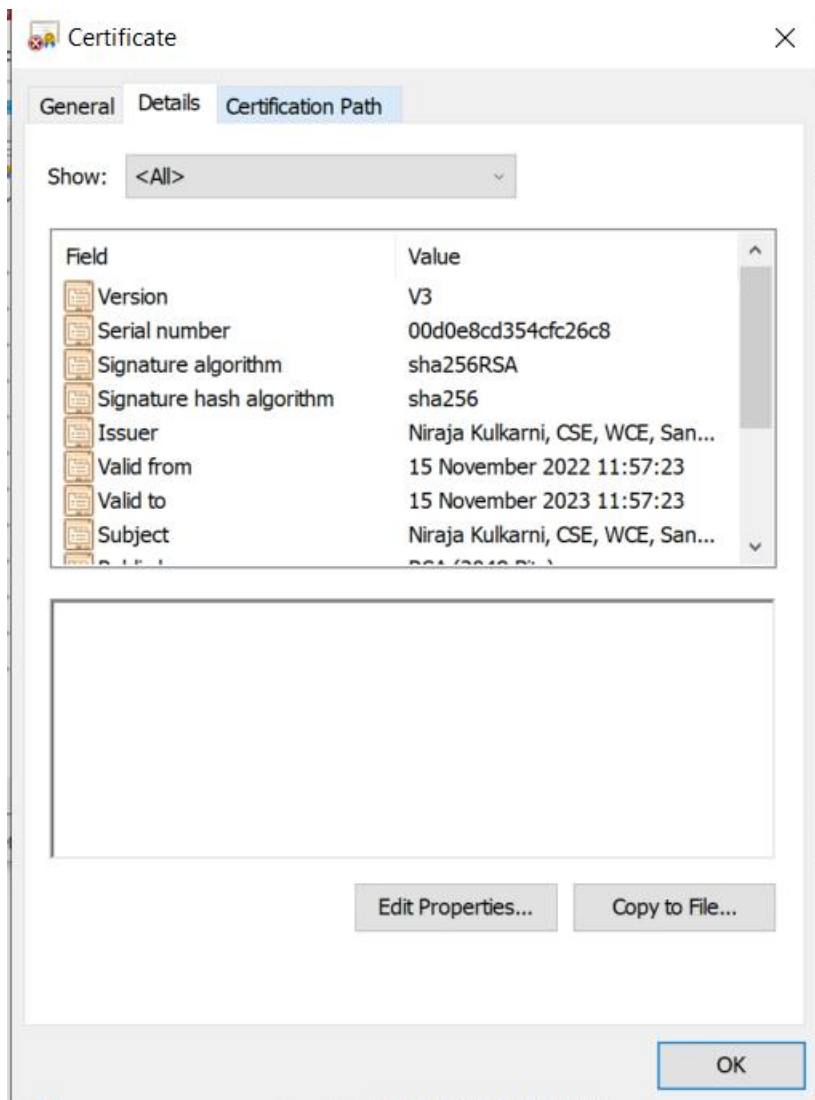
Your keystore contains 1 entry

Alias name: niraja
Creation date: 15-Nov-2022
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=Niraja Kulkarni, OU=CSE, O=WCE, L=Sangli, ST=Maharashtra, C=IN
Issuer: CN=Niraja Kulkarni, OU=CSE, O=WCE, L=Sangli, ST=Maharashtra, C=IN
Serial number: d0e8cd354cfc26c8
Valid from: Tue Nov 15 11:57:23 IST 2022 until: Wed Nov 15 11:57:23 IST 2023
Certificate fingerprints:
    SHA1: 9F:F3:A3:B6:08:E0:DA:37:58:8C:02:DE:72:84:17:73:5A:66:CD:58
    SHA256: 4E:CB:23:94:90:A8:E4:D3:50:0A:BC:14:B5:51:10:F3:5F:8A:40:F7:6F:F2:47:44:52:F7:70:94:EC:2C:5E:EB
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: 0C BB 10 08 B3 B5 04 DD   75 76 34 29 DA 00 7C 1C   .....uv4)....
0010: 8B 06 E9 ED               ....
]
]

```



### **Conclusion:**

Digital certificate is a file that ensures holder's identity and provides security. It is generated by CA (Certifying Authority) that involves four steps: Key Generation, Registration, Verification and Creation.