**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

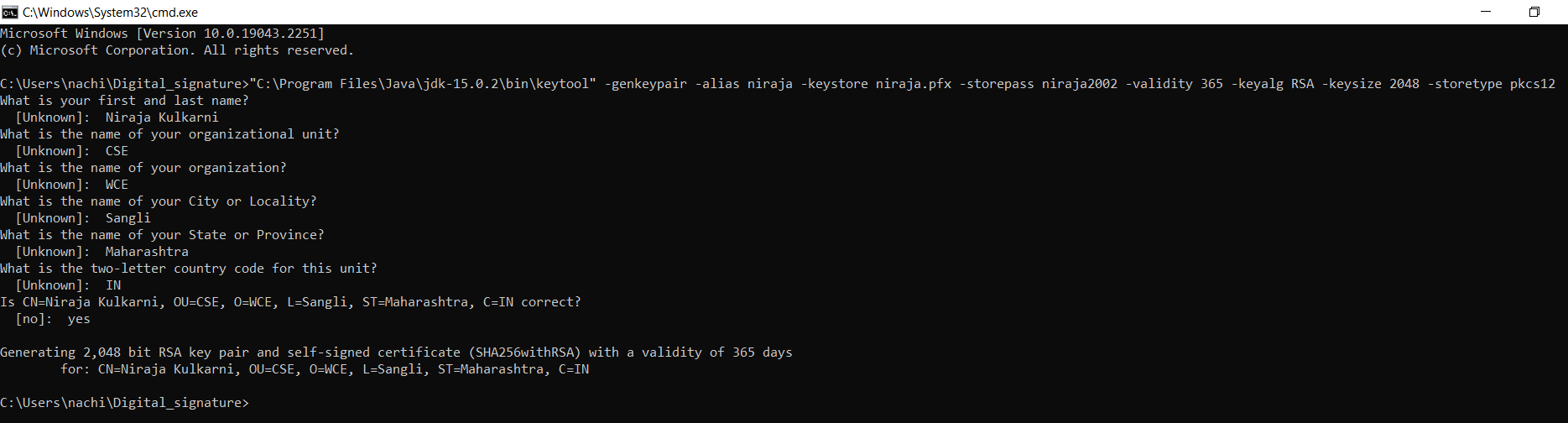
**Theory:**

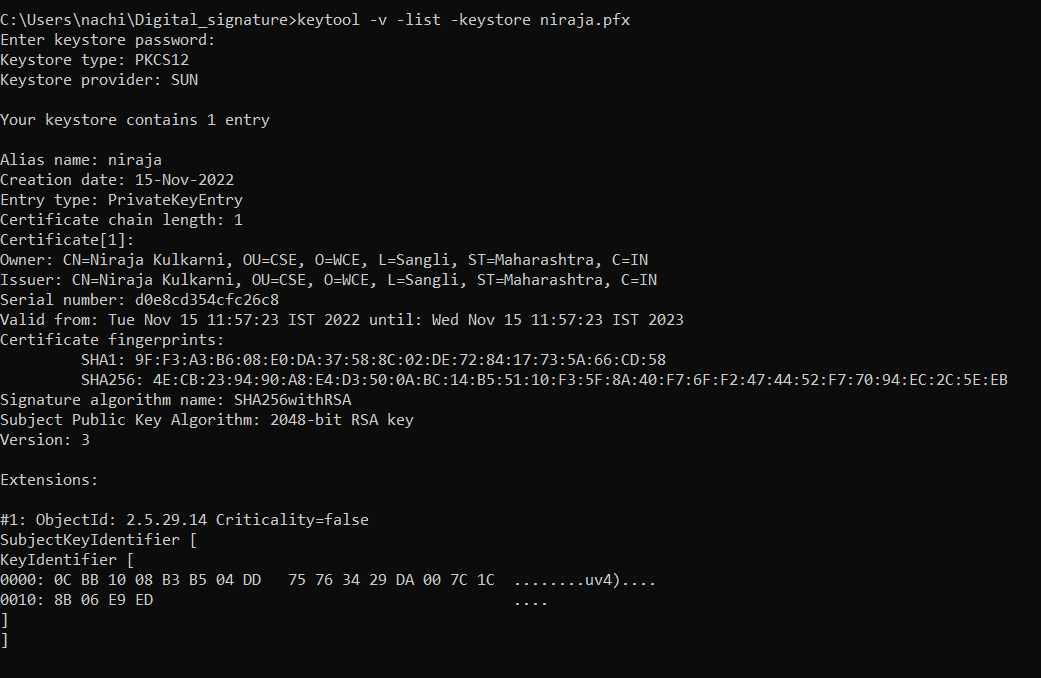
Digital certificate is issued by a trusted third party which proves sender’s identity to the receiver and receiver’s identity to the sender. A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. The CA issues an encrypted digital 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.

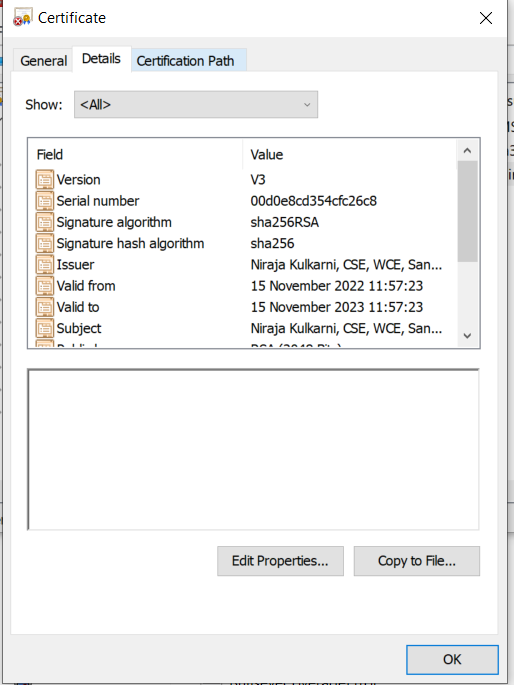
**Digital certificate contains:-**

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:







**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.