Department of Computer Science & Engineering

Cryptography & Network Security Lab

Assignment No. 14

PRN: 2019BTECS00017

Name: Muskan Raju Attar

Batch: B5

Title: Digital Certificate Generation

Aim: To Demonstrate Digital Certificate Generation using keytool

Theory:

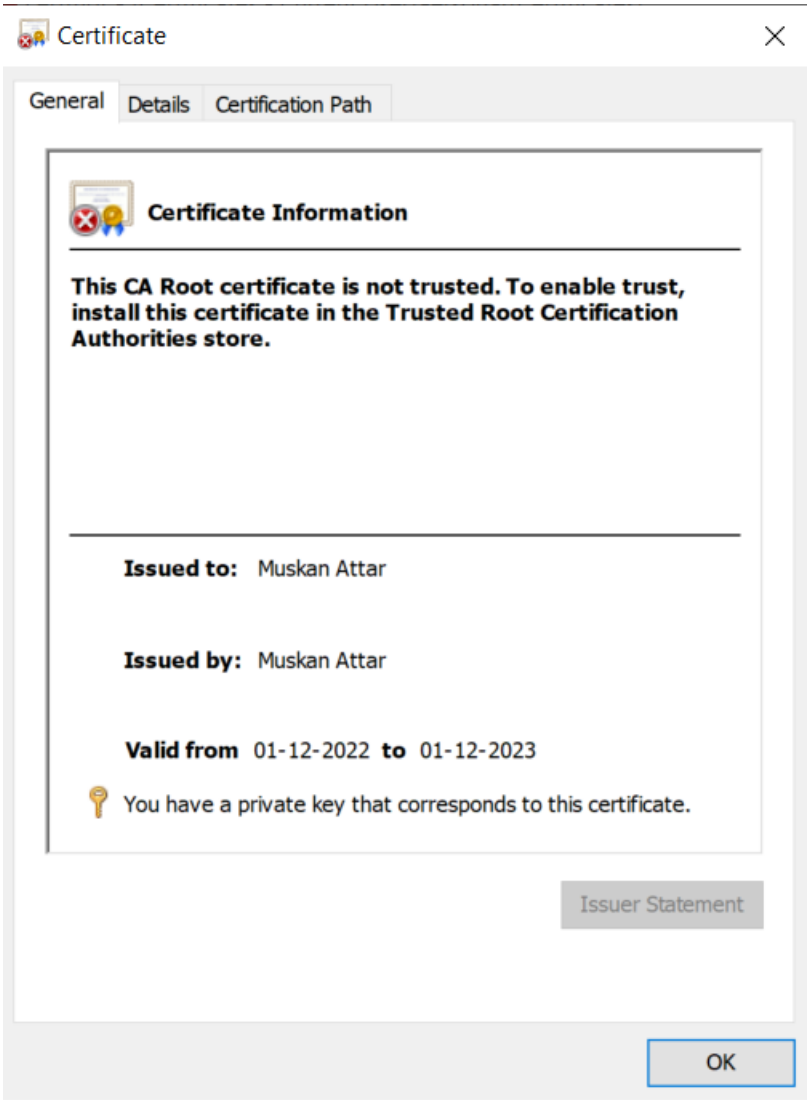
Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender. A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. The CA issues an encrypted digital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

Command Used:

-genkeypair -alias my_certificate -keystore my_keystore.pfx -storepass my_password -validity 365 -keyalg RSA -keysize 2048 -storetype pkcs12



Conclusion:

Performed digital signature creation and understood the importance of digital certificate.