SEM - VII - 2022-23
CNS Lab

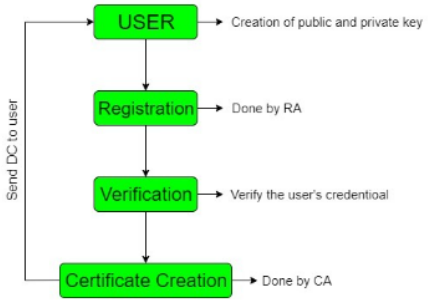
B3 - 2019BTECS00094 - Sweety Shrawan Gupta

Assignment 14

Digital Certificate Generation

Steps for Digital Certificate Creation:

- **Step-1:** Key generation is done by either user or registration authority. The public key which is generated is sent to the registration authority and private key is kept secret by user.
- **Step-2:** In the next step the registration authority registers the user.
- **Step-3:** Next step is verification which is done by registration authority in which the user's credentials are being verified by registration authority. It also checks that the user who send the public key have corresponding private key or not.
- **Step-4:** In this step the details and sent to certificate authority by registration authority who creates the digital certificate and give it to users and also keeps a copy to itself.



1. Generation of digital certificate using java key tool and key store utilities.

Creating a certificate:

```
C:\Users\SWEETY>keytool -genkey -alias priya -keyalg RSA -keystore "D:\local.keystore"
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  s g
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]:  mh
What is the two-letter country code for this unit?
  [Unknown]:  IN
Is CN=s g, OU=cse, O=wce, L=sangli, ST=mh, C=IN correct?
  [no]:  yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 90 days
        for: CN=s g, OU=cse, O=wce, L=sangli, ST=mh, C=IN
```

Displaying a certificate:

```
D:\>keytool -v -list -keystore local.keystore
Enter keystore password:
Keystore type: PKCS12
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: priya
Creation date: Nov 14, 2022
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=s g, OU=cse, O=wce, L=sangli, ST=mh, C=IN
Issuer: CN=s g, OU=cse, O=wce, L=sangli, ST=mh, C=IN
Serial number: 88fea0e2b145c2bf
Valid from: Mon Nov 14 14:56:47 IST 2022 until: Sun Feb 12 14:56:47 IST 2023Certificate fingerprints:
         SHA1: 91:BD:9F:AE:C8:19:7E:D4:7D:39:09:CB:74:F8:D9:75:F4:2C:AE:0E
         SHA256: AF:5C:45:AB:E8:67:FF:78:AA:8B:C0:11:20:06:CD:A2:D9:89:F4:90:73:65:C4:EA:B2:F7:43:37:3E:83:AC:5D
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: FD 3B DF FB 61 16 56 23   69 DF EB 19 1A 68 FD 6B  .;..a.V#i....h.k
0010: 7F 3A C7 8E                                        .:..
]
]



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