Final Year B. Tech, Sem VII 2022-23
PRN – 2020BTECS00211
Name – Aashita Narendra Gupta
Cryptography And Network Security Lab
Batch: B4
Practical No – 13

Title: To generate a digital certificate.

Theory:
Asymmetric encryption algorithms are based on the sharing of a public key between different users. Generally, the sharing of this key is done through an electronic directory (generally in LDAP format) or a website.

However, this method of sharing has a major weakness: there is no guarantee that the key is really the same as the user to whom it is associated. Indeed, a hacker can corrupt the public key present in the directory by replacing it with his public key. Thus, the hacker will be able to decrypt all the messages that have been encrypted with the key present in the directory.

Thus a digital certificate makes it possible to associate a public key with an entity (a person, a machine, …) in order to ensure its validity. The digital certificate is the identity card of the public key, issued by an organization called a certification authority (often noted CA for Certification Authority).
The certification authority is in charge of issuing digital certificates, assigning them a validity date (equivalent to the expiration date), as well as possibly revoking certificates before this date in case of compromise of the key (or the owner).

❖ **Structure of a certificate** :
Digital certificates are small files divided into two parts:

- The part containing the information
- The part containing the signature of the certification authority

The structure of digital certificates is standardized by the ITU X.509 standard (more precisely X.509v3), which defines the information contained in the digital certificate:

- The version of X.509 to which the digital certificate corresponds;
- The serial number of the digital certificate;
- The encryption algorithm used to sign the digital certificate;

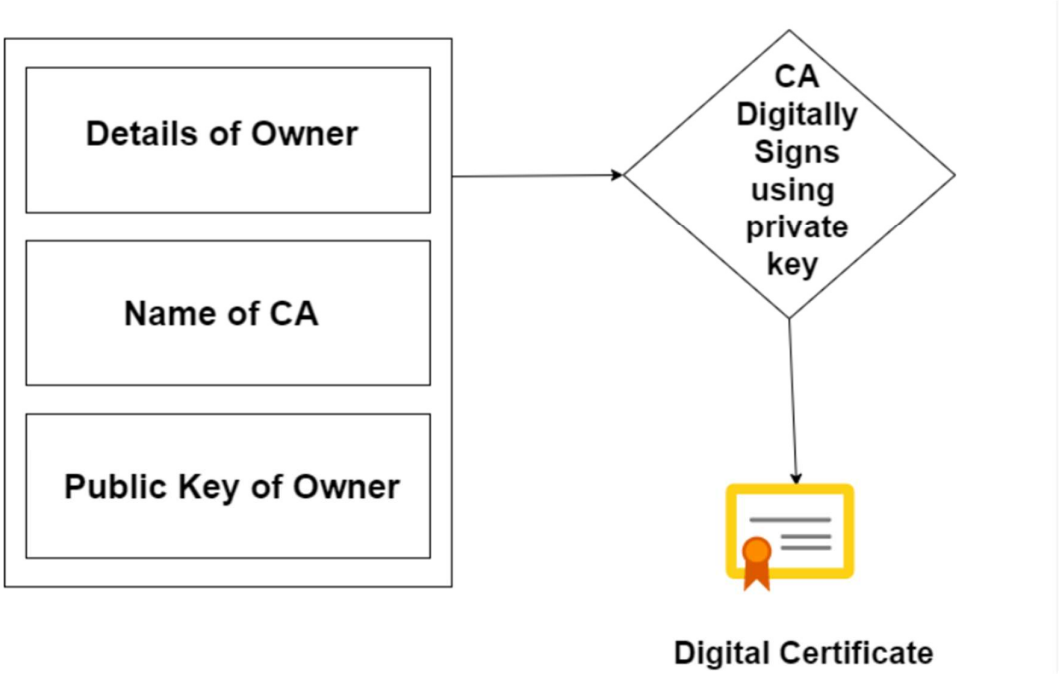
- The name (DN, for Distinguished Name) of the issuing Certification Authority(CA);
- The validity start date of the digital certificate;
- The digital certificate's expiry date;
- The purpose of the public key use;
- The public key of the digital certificate owner;
- The signature of the digital certificate issuer (thumbprint).

Types of digital certificates

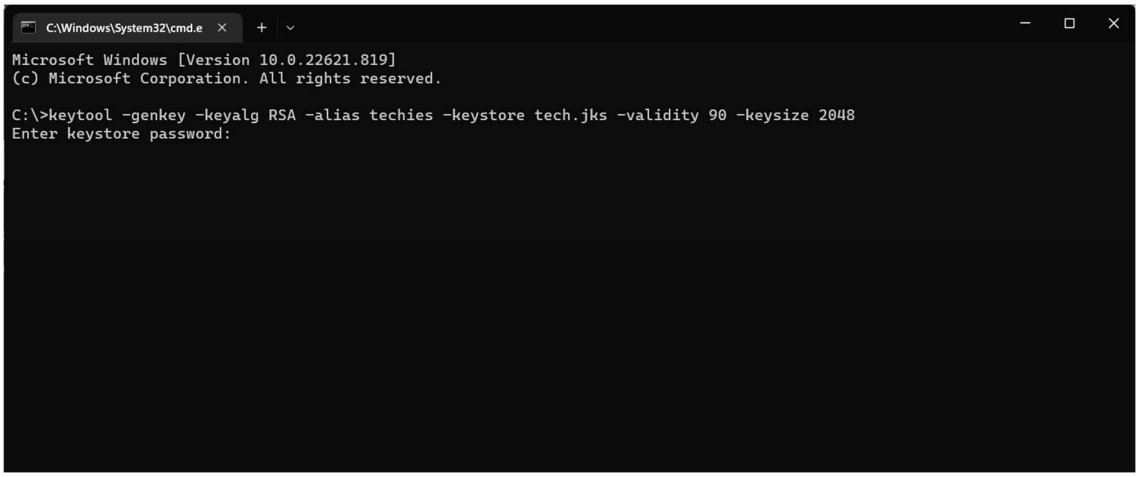
There are different types of digital certificates depending on the signature level:

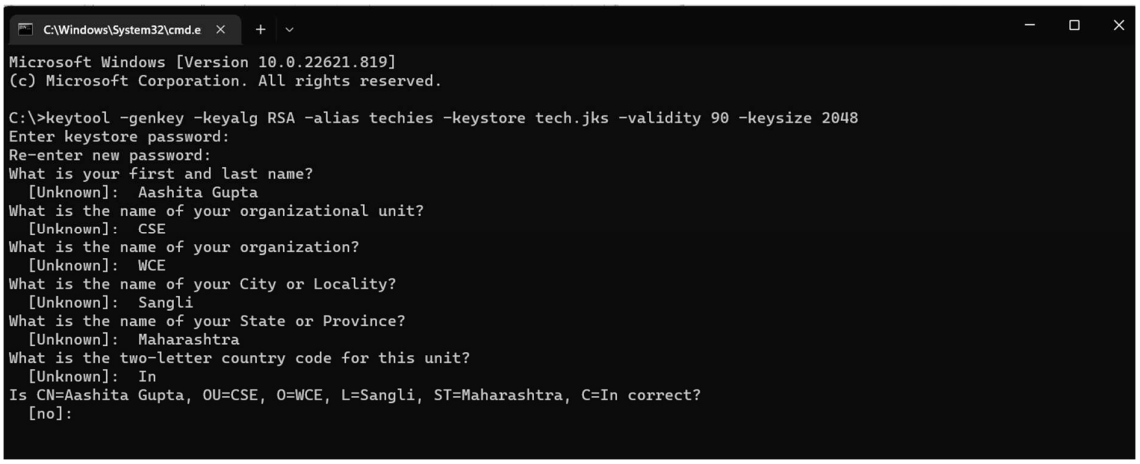
Self-signed certificates are certificates for internal use. Signed by a local server, this type of certificate guarantees the confidentiality of exchanges within an organization, for example for the needs of an intranet. It is thus possible to authenticate users using self-signed certificates.

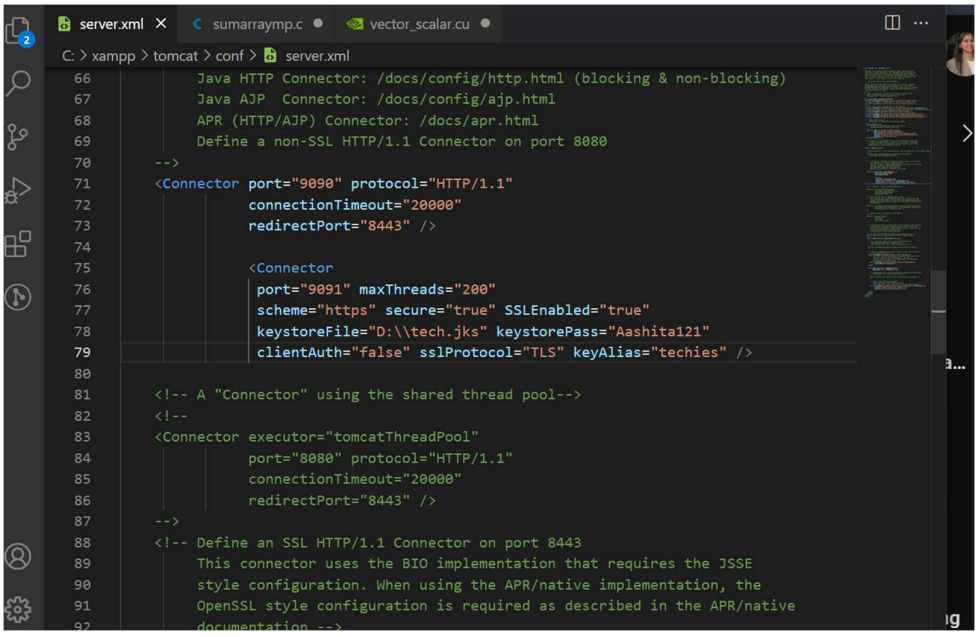
Certificates signed by a certification authority are necessary to ensure the security of exchanges with anonymous users, for example for a secure website accessible to the general public. The third-party certifier assures the user that the certificate belongs to the same organization to which it is claimed to belong.



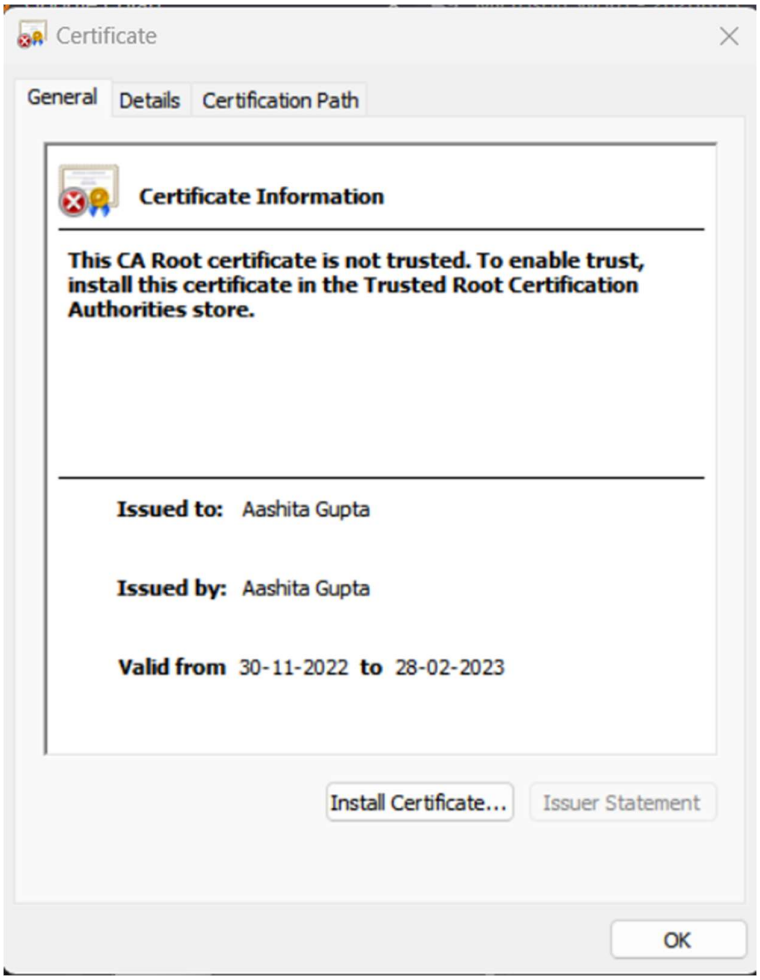
Snapshots:

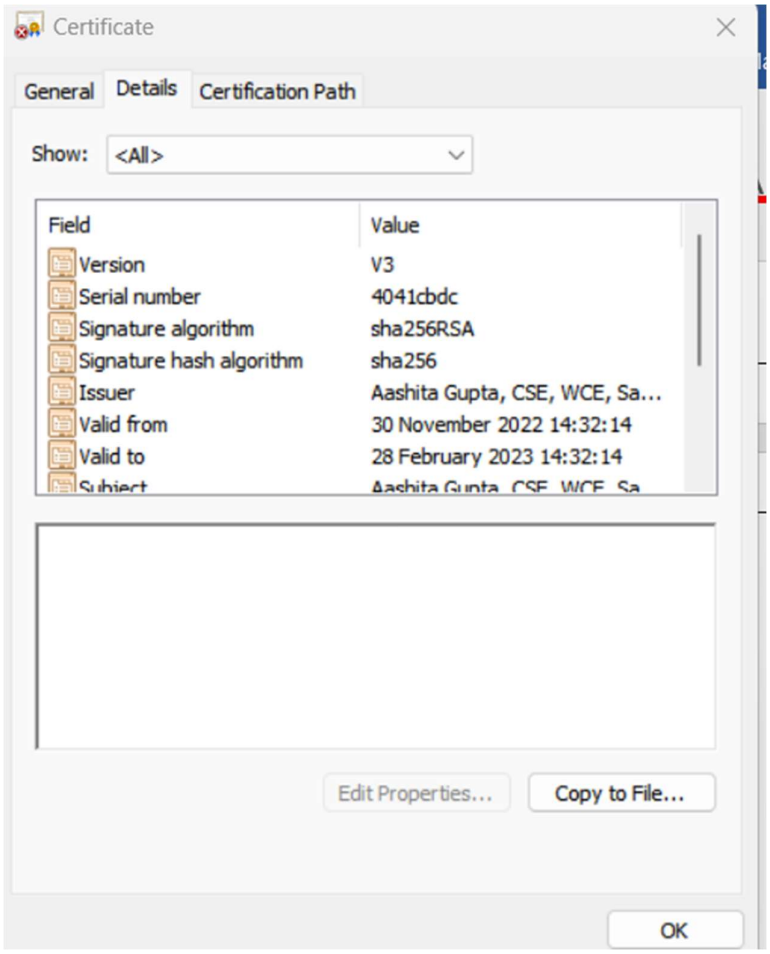

C:\Windows\System32\cmd.e
Microsoft Windows [Version 10.0.22621.819]
(c) Microsoft Corporation. All rights reserved.
C:\>keytool -genkey -keyalg RSA -alias techies -keystore tech.jks -validity 90 -keysize 2048
Enter keystore password:


C:\Windows\System32\cmd.e
Microsoft Windows [Version 10.0.22621.819]
(c) Microsoft Corporation. All rights reserved.
C:\>keytool -genkey -keyalg RSA -alias techies -keystore tech.jks -validity 90 -keysize 2048
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: Aashita Gupta
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=Aashita Gupta, OU=CSE, O=WCE, L=Sangli, ST=Maharashtra, C=In correct?
[no]:


server.xml
sumarraymp.c
vector_scalar.cu
C: > xampp > tomcat > conf > server.xml
Java HTTP Connector: /docs/config/http.html (blocking & non-blocking)
Java AJP Connector: /docs/config/ajp.html
APR (HTTP/AJP) Connector: /docs/apr.html
Define a non-SSL HTTP/1.1 Connector on port 8080
<Connector port="9090" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443" />
<Connector
port="9091" maxThreads="200"
scheme="https" secure="true" SSLEnabled="true"
keystoreFile="D:\\tech.jks" keystorePass="Aashita121"
clientAuth="false" sslProtocol="TLS" keyAlias="techies" />
<!-- A "Connector" using the shared thread pool-->
<!--
<Connector executor="tomcatThreadPool"
port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443" />
-->
<!-- Define an SSL HTTP/1.1 Connector on port 8443
This connector uses the BIO implementation that requires the JSSE
style configuration. When using the APR/native implementation, the
OpenSSL style configuration is required as described in the APR/native

```
C:\Windows\System32\cmd.e
operable program or batch file.

D:\>RSA -alias techies -keystore tech.jks -validity 90 -keysize 2048
'RSA' is not recognized as an internal or external command,
operable program or batch file.

D:\>keytool -genkey -keyalg RSA -alias techies -keystore tech.jks -validity 90 -keysize 2048
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  Aashita Gupta
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=Aashita Gupta, OU=CSE, O=WCE, L=Sangli, ST=Maharashtra, C=In correct?
  [no]:  yes


D:\>keytool -export -alias techies -file "D:\tech_cert.cer" -keystore "D:\tech.jks"
Enter keystore password:
Certificate stored in file <D:\tech_cert.cer>

D:\>
```





Conclusion: The digital certificate is the identity card of the public key, issued by an organization called a certification authority (often noted CA for Certification Authority).