Date:11.11.2022

Final Year B. Tech., Sem VII 2022-23

Cryptography And Network Security Lab

Assignment submission

PRN No: 2019BTECS00077

Full name: Avinash Vishnu Biradar

Batch: B7

Assignment: 14

Title of assignment: Generation of Digital Certificate

Title:

Generation of Digital Certificate using Java KeyTool and Key Store Utilities

Aim:

Generation of Digital Certificate using Java KeyTool and Key Store Utilities

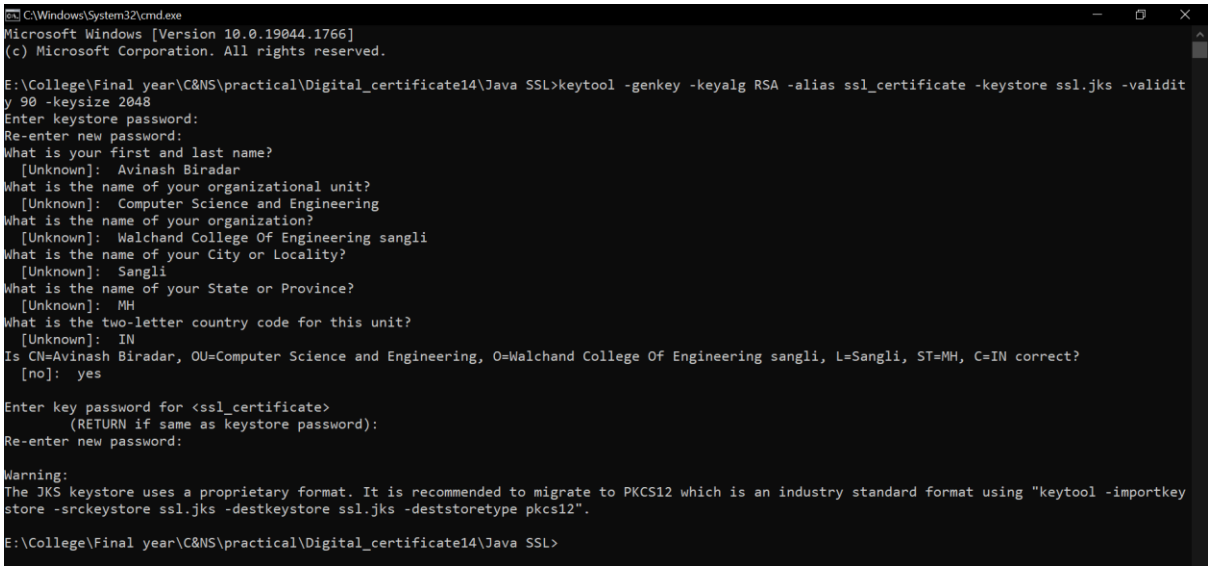
Theory:

- A digital certificate is a file or electronic password that proves the authenticity of a device, server, or user through the use of cryptography and the public key infrastructure (PKI).
- Digital certificate authentication helps organizations ensure that only trusted devices and users can connect to their networks. Another common use of digital certificates is to confirm the authenticity of a

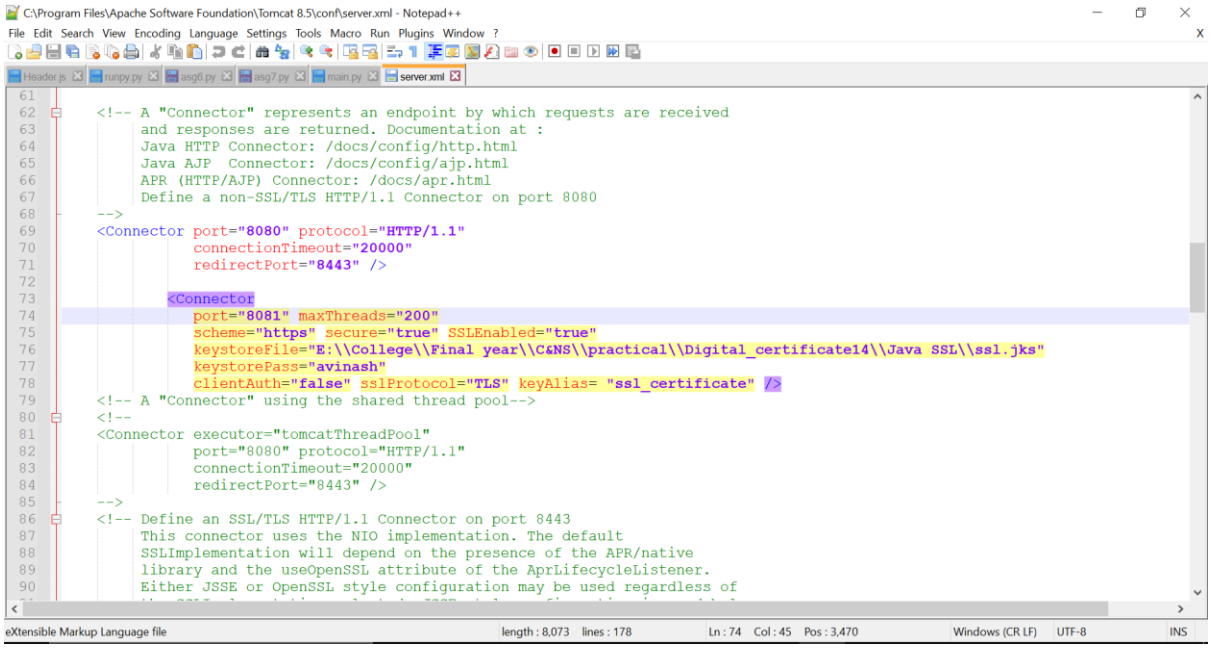
website to a web browser, which is also known as a secure sockets layer or SSL certificate.

- A digital certificate contains identifiable information, such as a user's name, company, or department and a device's Internet Protocol (IP) address or serial number. Digital certificates contain a copy of a public key from the certificate holder, which needs to be matched to a corresponding private key to verify it is real.
- A public key certificate is issued by certificate authorities (CAs), which sign certificates to verify the identity of the requesting device or user.
- Digital certificates can be requested by individuals, organizations, and websites. To do so, they provide the information to be validated and a public key through a certificate signing request. The information is validated by a publicly trusted CA, which signs it with a key that provides a chain of trust to the certificate.
- There are three different types of public key certificates:
    - A transport layer security (TLS)/SSL certificate
    - A code signing certificate
    - A client certificate.

Implementation of SSL Certification using Java Keytool



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19044.1766]
(c) Microsoft Corporation. All rights reserved.

E:\College\Final year\C&NS\practical\Digital_certificate14\Java SSL>keytool -genkey -keyalg RSA -alias ssl_certificate -keystore ssl.jks -validit
y 90 -keysize 2048
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  Avinash Biradar
What is the name of your organizational unit?
  [Unknown]:  Computer Science and Engineering
What is the name of your organization?
  [Unknown]:  Walchand College Of Engineering sangli
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=Avinash Biradar, OU=Computer Science and Engineering, O=Walchand College Of Engineering sangli, L=Sangli, ST=MH, C=IN correct?
  [no]:  yes

Enter key password for <ssl_certificate>
        (RETURN if same as keystore password):
Re-enter new password:

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkey
store -srckeystore ssl.jks -destkeystore ssl.jks -deststoretype pkcs12".

E:\College\Final year\C&NS\practical\Digital_certificate14\Java SSL>
```



C:\Program Files\Apache Software Foundation\Tomcat 8.5\conf\server.xml - Notepad++

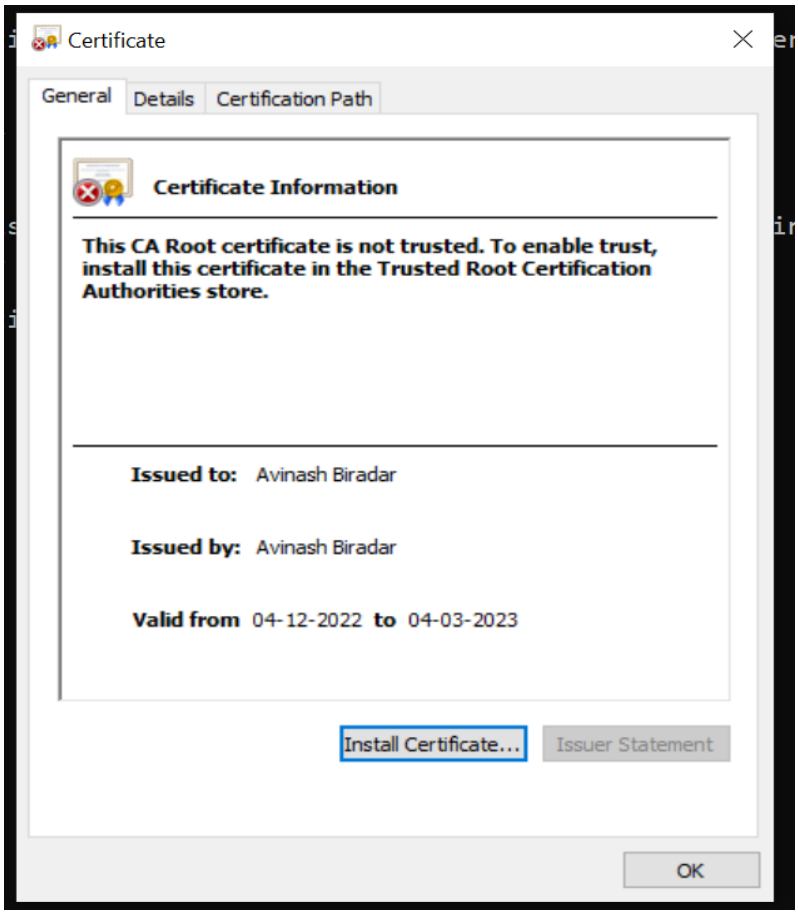
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

Header.js | runpy.py | asg6.py | asg7.py | main.py | server.xml

```
61
62      <!-- A "Connector" represents an endpoint by which requests are received
63           and responses are returned. Documentation at :
64           Java HTTP Connector: /docs/config/http.html
65           Java AJP  Connector: /docs/config/ajp.html
66           APR (HTTP/AJP) Connector: /docs/apr.html
67           Define a non-SSL/TLS HTTP/1.1 Connector on port 8080
68      -->
69      <Connector port="8080" protocol="HTTP/1.1"
70                 connectionTimeout="20000"
71                 redirectPort="8443" />
72
73                <Connector
74                 port="8081" maxThreads="200"
75                 scheme="https" secure="true" SSLEnabled="true"
76                 keystoreFile="E:\\College\\Final year\\C&NS\\practical\\Digital_certificate14\\Java SSL\\ssl.jks"
77                 keystorePass="avinash"
78                 clientAuth="false" sslProtocol="TLS" keyAlias= "ssl_certificate" />
79      <!-- A "Connector" using the shared thread pool-->
80      <!--
81      <Connector executor="tomcatThreadPool"
82                 port="8080" protocol="HTTP/1.1"
83                 connectionTimeout="20000"
84                 redirectPort="8443" />
85      -->
86      <!-- Define an SSL/TLS HTTP/1.1 Connector on port 8443
87           This connector uses the NIO implementation. The default
88           SSLImplementation will depend on the presence of the APR/native
89           library and the useOpenSSL attribute of the AprLifecycleListener.
90           Either JSSE or OpenSSL style configuration may be used regardless of
```

eXtensible Markup Language file | length : 8,073 | lines : 178 | Ln : 74 | Col : 45 | Pos : 3,470 | Windows (CR LF) | UTF-8 | INS

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19044.1766]
(c) Microsoft Corporation. All rights reserved.

E:\College\Final year\CNS\practical\Digital_certificate14\Java SSL>keytool -v -list -keystore  "ssl.jks"
Enter keystore password:
Keystore type: jks
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: ssl_certificate
Creation date: 4 Dec, 2022
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=Avinash Biradar, OU=Computer Science and Engineering, O=Walchand College Of Engineering sangli, L=Sangli, ST=MH, C=IN
Issuer: CN=Avinash Biradar, OU=Computer Science and Engineering, O=Walchand College Of Engineering sangli, L=Sangli, ST=MH, C=IN
Serial number: 67ec0984
Valid from: Sun Dec 04 17:13:28 IST 2022 until: Sat Mar 04 17:13:28 IST 2023
Certificate fingerprints:
         MD5:  98:CC:8C:90:49:FE:C5:42:4B:8B:EF:5C:D5:8F:D1:A1
         SHA1: 7B:8B:99:9B:39:07:08:DC:5B:39:57:E0:98:8C:A1:7F:97:DE:CB:70
         SHA256: B0:A8:E3:15:23:49:AE:11:7A:B5:E6:E0:8A:05:4B:3F:3C:33:FD:86:4A:36:EB:A3:28:47:AB:5F:4A:D0:79:31
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: E2 4F D1 20 BF 98 60 8F   3E AD 41 3D AA 92 79 2F  .O. ..`.>.A=..y/
0010: E1 68 F2 5A                                        .h.Z
]
]
```



Applications:

- Digital certificates are used for to secure email to identify one user to another
- It may also use for electronic document signing.