

**Final Year B. Tech., Sem VII 2022-23**  
**Cryptography & Network Security Lab**  
**PRN: 2020BTECS00205**  
**Full Name: Monika .V. Chitrakathi**  
**Batch: B8**

## Assignment - Digital Certificate

### Instructions

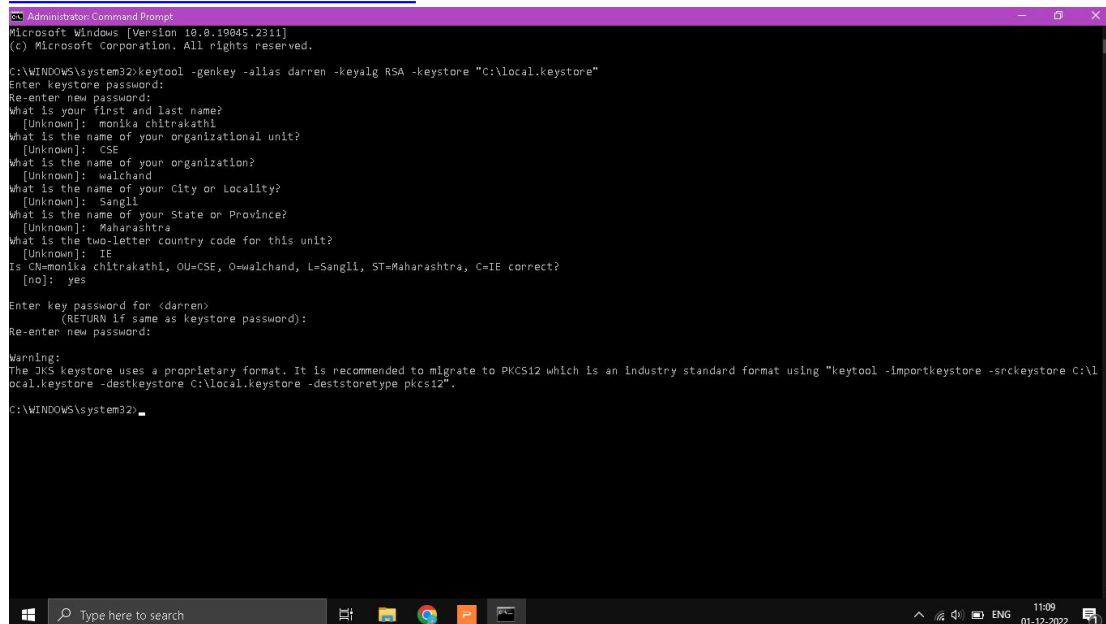
Creating a Self-Signed Digital Certificate

### To generate a certificate using the keytool utility

Use keytool to generate, import, and export certificates. By default, keytool creates a keystore file in the directory where it is run.

1. Change to the directory where the certificate is to be run.

Always generate the certificate in the directory containing the keystore and truststore files, by default domain-dir/config. For information on changing the location of these files, see [To change the location of certificate files](#).



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.2311]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>keytool -genkey -alias darren -keyalg RSA -keystore "C:\local.keystore"
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: monika chitrakathi
What is the name of your organizational unit?
[Unknown]: CSE
What is the name of your organization?
[Unknown]: walchand
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=monika chitrakathi, OU=CSE, O=Walchand, L=Sangli, ST=Maharashtra, C=IN correct?
[no]: yes
Enter key password for <darwin>
(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 -importkeystore -srckeystore C:\l
ocal.keystore -destkeystore C:\local.keystore -deststoretype pkcs12".

C:\WINDOWS\system32>
```

```
Administrator: Command Prompt
Enter keystore password:
keystore type: jks
keystore provider: SUN

Your keystore contains 1 entry

Alias name: darren
Creation date: 1 Dec, 2022
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=monika chitrakathi, OU=CSE, O=walchand, L=Sangli, ST=Maharashtra, C=IE
Issuer: CN=monika chitrakathi, OU=CSE, O=walchand, L=Sangli, ST=Maharashtra, C=IE
Serial number: 37c9f4b0
Valid from: Thu Dec 01 11:09:27 IST 2022 until: Wed Mar 01 11:09:27 IST 2023
Certificate fingerprints:
    SHA1: 3C:FC:91:D7:56:FB:6A:D2:9A:6C:75:01:81:25:A5:16:F5:C1:EE:45
    SHA256: 02:65:C2:70:7E:57:F2:65:36:47:1E:71:B8:4C:20:B7:23:FA:7E:67:C3:52:6C:95:43:F9:69:37:5F:56:17:DB
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: B5 24 22 61 03 18 CF C0 16 DC 16 11 F9 36 E6 BC .5*a.....6..
0010: 99 C5 F9 F4 ....
]
]

*****
*****

Warnings:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore local.keystore -destkeystore local.keystore -deststoretype pkcs12".

C:\>
```

2. Enter the following keytool command to generate the certificate in the keystore file, keystore.jks:

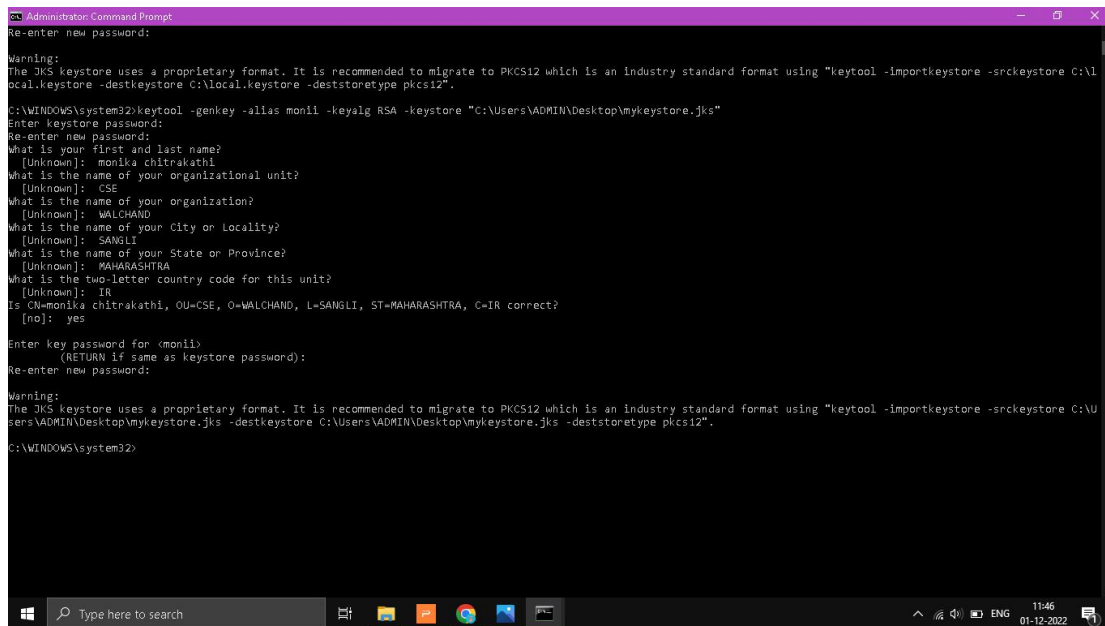
```
keytool -genkey -alias keyAlias-keyalg RSA -keypass
changeit -storepass changeit -keystore keystore.jks
```

Use any unique name as your keyAlias. If you have changed the keystore or private key password from their default, then substitute the new password for changeit in the above command.

A prompt appears that asks for your name, organization, and other information that keytool uses to generate the certificate.

3. Enter the following keytool command to export the generated certificate to the file server.cer (or client.cer if you prefer):

```
keytool -export -alias keyAlias-storepass changeit -file
server.cer -keystore keystore.jks
```



```
Administrator: Command Prompt
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 -importkeystore -srckeystore C:\local.keystore -destkeystore C:\local.keystore -deststoretype pkcs12".

C:\WINDOWS\system32>keytool -genkey -alias moni1 -keyalg RSA -keystore "C:\Users\ADMIN\Desktop\mykeystore.jks"
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: monika chitrakathi
What is the name of your organizational unit?
[Unknown]: CSE
What is the name of your organization?
[Unknown]: WALCHAND
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]: IR
Is CN=monika chitrakathi, OU=CSE, O=WALCHAND, L=SANGLI, ST=MAHARASHTRA, C=IR correct?
[no]: yes

Enter key password for <moni1>
(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 -importkeystore -srckeystore C:\Users\ADMIN\Desktop\mykeystore.jks -destkeystore C:\Users\ADMIN\Desktop\mykeystore.jks -deststoretype pkcs12".

C:\WINDOWS\system32>
```

4.If a certificate signed by a certificate authority is required, see [To sign a digital certificate using the keytool utility](#).

5.To create the truststore file cacerts.jks and add the certificate to the truststore, enter the following keytool command:

```
keytool -import -v -trustcacerts -alias keyAlias -file server.cer  
-keystore cacerts.jks -keypass changeit
```

If you have changed the keystore or private key password from their default, then substitute the new password for changeit in the above command.

The tool displays information about the certificate and prompts whether you want to trust the certificate.

```
Administrator Command Prompt
keytool error: java.lang.Exception: Keystore file does not exist: truststore
java.lang.Exception: Keystore file does not exist: truststore
    at sun.security.tools.keytool.Main.doCommands(Main.java:783)
    at sun.security.tools.keytool.Main.run(Main.java:379)
    at sun.security.tools.keytool.Main.main(Main.java:372)

C:\>keytool -list -v -keystore trust
Enter keystore password:
Keystore type: jks
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: monil
Creation date: 1 Dec, 2022
Entry type: trustedCertEntry

Owner: CN=monika chitrakathi, OU=CSE, O=WALCHAND, L=SANGLI, ST=MAHARASHTRA, C=IR
Issuer: CN=monika chitrakathi, OU=CSE, O=WALCHAND, L=SANGLI, ST=MAHARASHTRA, C=IR
Serial number: 1c9c6532
Valid from: Thu Dec 01 11:46:18 IST 2022 until: Wed Mar 01 11:46:18 IST 2023
Certificate fingerprints:
    SHA1: DD:25:43:35:04:E0:1B:51:95:C0:1C:98:1B:31:3C:92:9E:ED:4A:56
    SHA256: 1E:0C:02:3C:56:5D:74:42:D3:E5:30:02:F7:CD:12:B0:A4:E9:09:02:E7:98:2F:2F:6C:1C:28:D9:02:4E:4F:0F
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: 14 13 00 F9 F4 F0 27 29  BD 7B 0C 62 5F 27 76 9F  .....')...b_v.
            0010: 3A C8 6A DE                  :.j.
        ]
    ]

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

6.Type yes, then press Enter.

Then keytool displays something like this:

Certificate was added to keystore [Saving cacerts.jks]

```
Administrator Command Prompt

-rfc                output in RFC style
-alias <alias>      alias name of the entry to process
-file <filename>     output file name
-keystore <keystore> keystore name
-storepass <arg>     keystore password
-storetype <storetype> keystore type
-providername <providername> provider name
-providerclass <providerclass> provider class name
-providerarg <arg>    provider argument
-providerpath <classpath> provider classpath
-v                 verbose output
-protected         password through protected mechanism

Use "keytool -help" for all available commands

C:\>
C:\>keytool -export -alias monl -file "C:\Users\ADMIN\Desktop\test.cer" -keystore "C:\Users\ADMIN\Desktop\mykeystore.jks"
Enter keystore password:
keytool error: java.lang.Exception: Alias <monl> does not exist

C:\>keytool -export -alias monil -file "C:\Users\ADMIN\Desktop\test.cer" -keystore "C:\Users\ADMIN\Desktop\mykeystore.jks"
Enter keystore password:
Certificate stored in file <C:\Users\ADMIN\Desktop\test.cer>

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore C:\Users\ADMIN\Desktop\mykeystore.jks -destkeystore C:\Users\ADMIN\Desktop\mykeystore.jks -deststoretype pkcs12".

C:\>
```

```
Administrator: Command Prompt

at sun.security.provider.KeyStoreDelegator.engineGetKey(KeyStoreDelegator.java:96)
at sun.security.provider.JavaKeyStore$DualFormatJKS.engineGetKey(JavaKeyStore.java:70)
at java.security.KeyStore.getKey(KeyStore.java:1829)
at sun.security.tools.keytool.Main.recoverKey(Main.java:3417)
at sun.security.tools.keytool.Main.installReply(Main.java:2847)
at sun.security.tools.keytool.Main.doCommands(Main.java:1854)
at sun.security.tools.keytool.Main.run(Main.java:379)
at sun.security.tools.keytool.Main.main(Main.java:372)

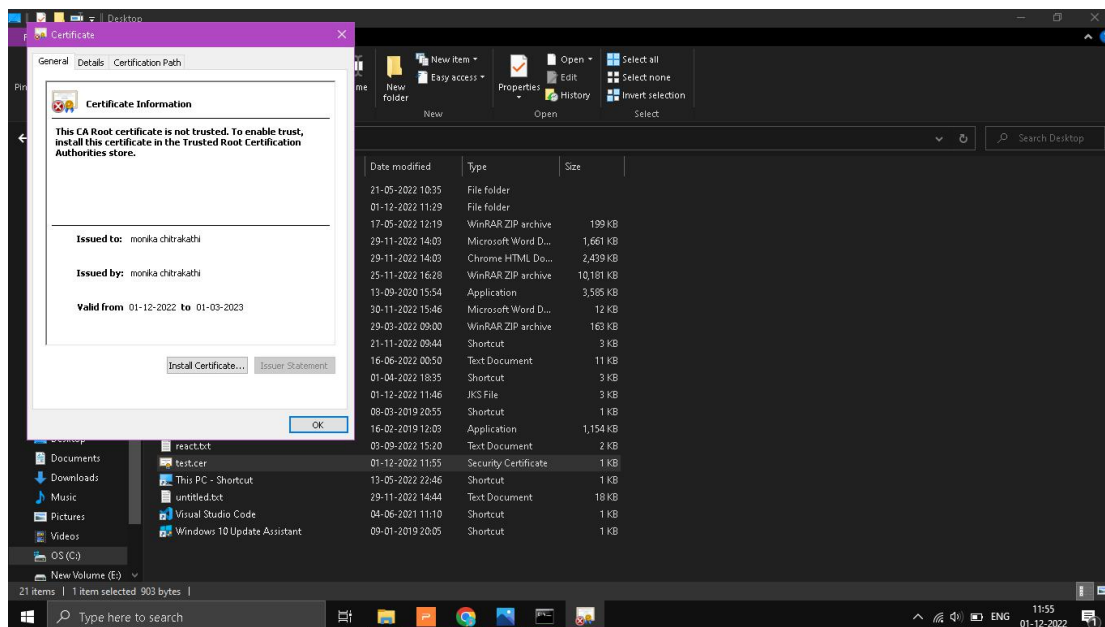
C:\>keytool -import -alias monil -file "C:\Users\ADMIN\Desktop\test.cer" -keystore "C:\Users\ADMIN\Desktop\mykeystore.jks"
Enter keystore password:
keytool error: java.lang.Exception: Certificate reply and certificate in keystore are identical

C:\>keytool -import -alias monil -file "C:\Users\ADMIN\Desktop\test.cer" -keystore trust
Enter keystore password:
Re-enter new password:
They don't match. Try again
Enter keystore password:
Re-enter new password:
Owner: CN=monika chitrakathi, OU=CSE, O=WALCHAND, L=SANGLI, ST=MAHARASHTRA, C=IR
Issuer: CN=monika chitrakathi, OU=CSE, O=WALCHAND, L=SANGLI, ST=MAHARASHTRA, C=IR
Serial number: 1c9c6532
Valid from: Thu Dec 01 11:46:18 IST 2022 until: Wed Mar 01 11:46:18 IST 2023
Certificate fingerprints:
    SHA1: 00:22:43:35:04:E0:1B:51:95:C8:1C:98:1B:31:3C:92:9E:ED:4A:56
    SHA256: 1E:0C:02:3C:56:5D:74:42:D3:E5:39:02:F7:CD:12:B0:A4:E9:69:82:E7:98:2F:2F:6C:1C:28:D9:82:4E:4F:8F
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: 14 13 90 F9 F4 F0 27 29 BD 7B 0C 62 5F 27 76 9F .....')...b'_v.
0010: 3A C8 6A DE :j.
]
]

Trust this certificate? [no]: yes
Certificate was added to keystore

C:\>
```



7.Restart the Application Server.

