

Name: Rutikesh Sawant

Batch: B2

Subject: CNS Lab

PRN: 2019BTECS00034

Assignment 15

Aim: Generation of digital certificate by using java keystore and keytool utilities.

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 a public key with a particular individual or an entity.

Output:

```
C:\Users\danaps>"C:\Program Files\Java\jdk1.8.0_202\bin\keytool" -genkeypair -alias RutikeshSawant -keystore RutikeshSawant.pfx -storepass Rutikesh -validity 365 -keyalg RSA -keysize 2048 -storetype pkcs12
What is your first and last name?
[Unknown]: Rutikesh Sawant
What is the name of your organizational unit?
[Unknown]: CSE
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]: Maharashtra
What is the two-letter country code for this unit?
[Unknown]: IN
Is CN=Rutikesh Sawant, OU=CSE, O=Walchand College of Engineering Sangli, L=Sangli, ST=Maharashtra, C=IN correct?
[No]: yes

C:\Users\danaps>
```

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

☒ Current User

☐ Local Machine

To continue, click Next.

Next

Cancel



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Users\danap\RutikeshSawant.pfx

Browse...

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Next

Cancel



←  Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

••••••••

☐ Display Password

Import options:

- ☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
- ☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
- ☐ Protect private key using virtualized-based security(Non-exportable)
- ☒ Include all extended properties.

Next

Cancel



←  Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

- ☐ Automatically select the certificate store based on the type of certificate
- ☒ Place all certificates in the following store

Certificate store:

Personal

[Browse...](#)

[Next](#)

[Cancel](#)



Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Personal
Content	PFX
File Name	C:\Users\danap\RutikeshSawant.pfx

Finish

Cancel



Certificate



General Details Certification Path



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: Rutikesh Sawant

Issued by: Rutikesh Sawant

Valid from 16-11-2022 **to** 16-11-2023



You have a private key that corresponds to this certificate.

Issuer Statement

OK