Lab 9
Request for a certificate

Objective: To learn how to implement a certificate request in java

Task: Execute a request to create a certificate

Work order:

1. Create certificate
2. Generate a request
3. Import file to keystore
4. View certificate information

Progress:

Generating keys.

Use this method to support HTTPS (HTTP over TLS). The following shows how to create a new key pair in a new or existing Java key store, which can be used to create a Certificate Signing Request (CSR) or obtain an SSL certificate from a CA.

This command will generate a 2048-bit RSA key pair under the specified alias (in this case, domain) in the specified storage file (keystore.jks).

```
keytool -genkeypair \
-alias domain \
-keyalg RSA \
-keystore keystore.jks
```

Generating a request for an existing private key.

To generate a certificate signing request that can be sent to the CA to obtain a trusted SSL certificate, you will need an existing keystore and alias.

This command will create a CSR (domain.csr) signed with a private key alias domain in keystore.jks:

```
keytool -certreq \
-alias domain \
-file domain.csr \
-keystore keystore.jks
```

Enter the keystore password, after which the request will be generated.

Importing Signed/Root/Intermediate Certificate.

How to import certificates (for example, a CA-signed certificate) into a keystore. It must match a private key with a specific alias. Alternatively, this command can be used to import a root or

intermediate certificate, which may be required by the CA to complete the chain of trust. Just provide a unique alias (for example, root instead of domain) and the certificate you want to import.

The following command will import the certificate (domain.crt) into the keystore (keystore.jks) under the specified alias (domain). The signed certificate, when imported, must match the private key with the specified alias:

```
keytool -importcert \
-trustcacerts -file domain.crt \
-alias domain \
-keystore keystore.jks
```

At this point, you will be prompted to enter your keystore password and then confirm the import.

Using Keytool to View Certificate Information.

This command will display detailed information about the certificate file (certificate.crt), including the checksum, distinguished name of the owner and its expiration date:

```
keytool -printcert \
-file domain.crt
```