Module Five Assignment:

Certificate Generation

Elizabeth Marticello

Southern New Hampshire University

CS 305-11883-M01 Software Security 2025 C-4

Professor Albanie Bolton

Due Date: August 3rd, 2025

Role and Value of Certificates

A Certificate Authority (CA) is a trusted third party that issues digital certificates to verify the identity of websites. The value of a CA is enabling secure communications online by confirming that a public key belongs to the entity it claims to. This helps prevent impersonation, fraud, and man-in-the-middle attacks. This way a user can trust the websites they visit, especially while shopping or banking (HashedOut, 2020).

Third Party Vendors for CA

It’s best to have a third-party vendor generate certificates for you because it is already recognized and trusted by browsers and applications. This means that any certificate they issue will automatically be accepted without additional setup. However, creating one in house could save on monetary cost, but could cause more risk if done improperly.

Using CA for Security

Utilizing a CA strengthens security because it ensures that when you connect to a site or a service, you’re talking to the right one. A certificate issued by a CA secures your data through encryption and confirms the identity of the other party, helping prevent interception or fraudulent activity.

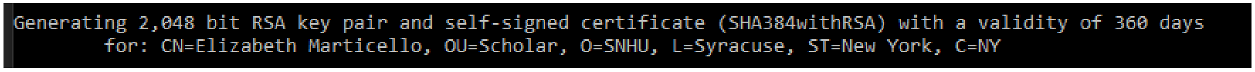
Advantages of Using a CA

Using a CA offers several advantages. Their certificates are automatically trusted by most browsers and applications providing a reliable way to verify identities online. They enable encryption through HTTPS, ensuring that data is protected during transfer. CA can also authenticate servers to confirm they are who they claim to be. Additionally, a third-party CA can make the process easier by having trust already established, removing the need for manual configurations (Manico & Detlefsen, 2024).

Screenshots

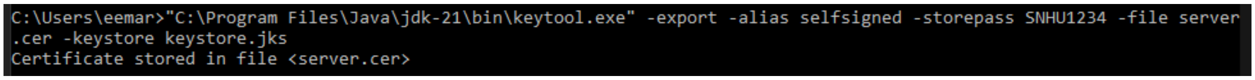
1. Certificate Generation: Use the Java Keytool to generate a self-signed certificate. (find keytool.exe)

   a. Genkey



```
Generating 2,048 bit RSA key pair and self-signed certificate (SHA384withRSA) with a validity of 360 days
        for: CN=Elizabeth Marticello, OU=Scholar, O=SNHU, L=Syracuse, ST=New York, C=NY
```

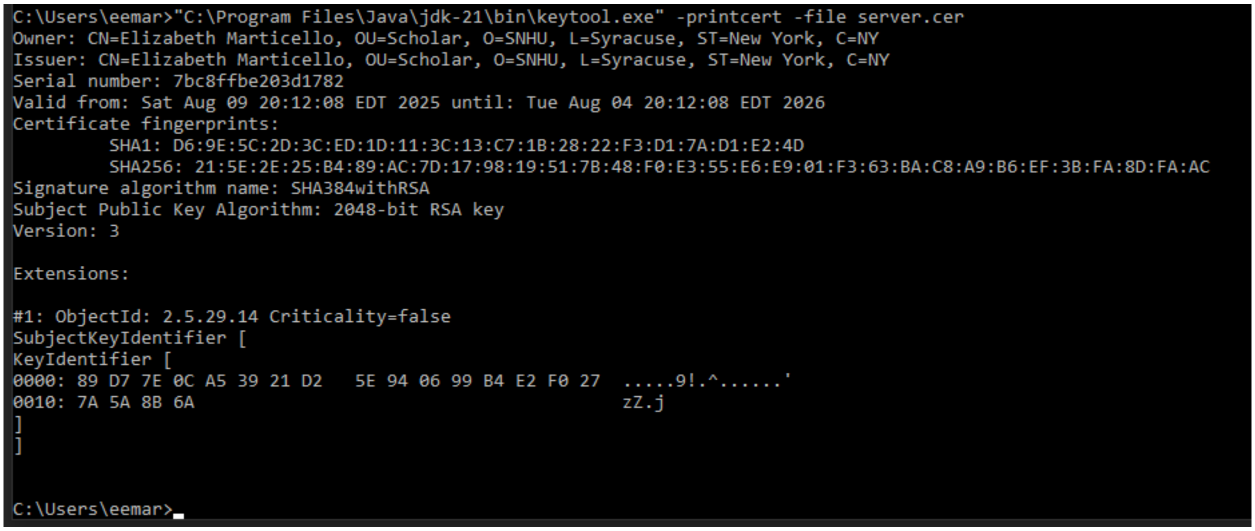
   b. Password for keystone



```
C:\Users\eemar>"C:\Program Files\Java\jdk-21\bin\keytool.exe" -export -alias selfsigned -storepass SNHU1234 -file server
.cer -keystore keystore.jks
Certificate stored in file <server.cer>
```

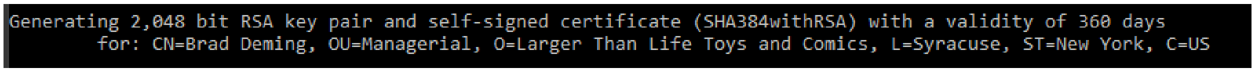
   c. Print out CER, and

   d. Show that certificate was generated.



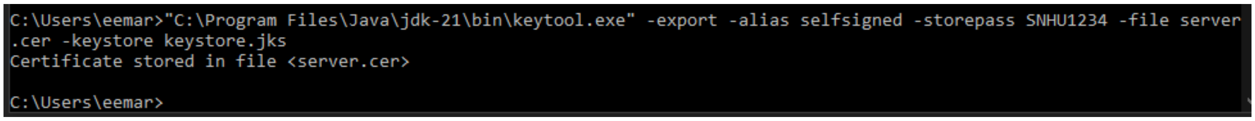
```
C:\Users\eemar>"C:\Program Files\Java\jdk-21\bin\keytool.exe" -printcert -file server.cer
Owner: CN=Elizabeth Marticello, OU=Scholar, O=SNHU, L=Syracuse, ST=New York, C=NY
Issuer: CN=Elizabeth Marticello, OU=Scholar, O=SNHU, L=Syracuse, ST=New York, C=NY
Serial number: 7bc8ffbe203d1782
Valid from: Sat Aug 09 20:12:08 EDT 2025 until: Tue Aug 04 20:12:08 EDT 2026
Certificate fingerprints:
         SHA1: D6:9E:5C:2D:3C:ED:1D:11:3C:13:C7:1B:28:22:F3:D1:7A:D1:E2:4D
         SHA256: 21:5E:2E:25:B4:89:AC:7D:17:98:19:51:7B:48:F0:E3:55:E6:E9:01:F3:63:BA:C8:A9:B6:EF:3B:FA:8D:FA:AC
Signature algorithm name: SHA384withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 89 D7 7E 0C A5 39 21 D2   5E 94 06 99 B4 E2 F0 27  .....9!.^......'
0010: 7A 5A 8B 6A                                        zZ.j
]
]


C:\Users\eemar>
```

   e. Answer series of questions with unique answers.



```
Generating 2,048 bit RSA key pair and self-signed certificate (SHA384withRSA) with a validity of 360 days
        for: CN=Brad Deming, OU=Managerial, O=Larger Than Life Toys and Comics, L=Syracuse, ST=New York, C=US
```

f. Export Certificate to CER file.



```
C:\Users\eemar>"C:\Program Files\Java\jdk-21\bin\keytool.exe" -export -alias selfsigned -storepass SNHU1234 -file server
.cer -keystore keystore.jks
Certificate stored in file <server.cer>

C:\Users\eemar>
```

Resources

(2020, August 10). *What Is a Certificate Authority (CA) and What Does It Do?* HashedOut by the SSL Store. https://www.thesslstore.com/blog/what-is-a-certificate-authority-ca-and-what-do-they-do/

Manico, J., & Detlefsen, A. (2024). *Iron-Clad Java: Building Secure Web Applications*. McGraw Hill Computing. https://learning.oreilly.com/library/view/iron-clad-java/9780071835886/ch06.html#ch06lev2sec7