Module 5: Certificate Generation

Software Security

Version 1.0

Ronny Z. Valtonen

Software Security

Certificate Authorities:

According to Iron-Clad Java, a CA acts as a trusted 3rd party that verifies a website's public key and matches it to a private key that only the CA holds.[1] This process ensures that a user is communicating with the legitimate entity and not a duplicated key. Furthermore, "Let's Encrypt" shows how a nonprofit CA can generate free certificates for communications over HTTPS.[2] This is a practical advantage of using a CA for ensuring data security and creating trust between the user and the website. Lastly, using a CA protects against man in the middle attacks by ensuring the key matches the hex message being sent. Another advantage of using a CA is that it provides the ability to remove certificates when needed, for example if a certificate was compromised, it can be revoked. If you didn't use a CA where a user self-signed certificates are used, if this certificate is compromised, a user may never know until it is too late. Like in our previous assignment, users will also see a warning about an "unsafe" website if the certificate is self-signed, due to the high risk of the website not actually being the true website. There is one disadvantage with using a CA, if an attacker somehow manages to compromise the CA, they can issue fraudulent certs to many domains - however, this risk outweighs the extreme risk of self-signed certs.

---

[1] Manico and Detlefsen, *Iron-Clad Java: Building Secure Web Applications (Oracle Press)*, 2014.
[2] "Let's Encrypt."

Certificate Generation:

Generate Key

```
C:\Windows\System32>"C:\Program Files\Java\jdk-23\bin\keytool.exe" -genkey -keyalg RSA -alias module5 -keypass password -keystore
 keystore.jks -storepass password -validity 360 -keysize 2048
Enter the distinguished name. Provide a single dot (.) to leave a sub-component empty or press ENTER to use the default value in
braces.
What is your first and last name?
  [Unknown]:  Ronny Valtonen
What is the name of your organizational unit?
  [Unknown]:  HP Spectre
What is the name of your organization?
  [Unknown]:  SNHU
What is the name of your City or Locality?
  [Unknown]:  Forest Grove
What is the name of your State or Province?
  [Unknown]:  Oregon
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=Ronny Valtonen, OU=HP Spectre, O=SNHU, L=Forest Grove, ST=Oregon, C=US correct?
  [no]:  yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA384withRSA) with a validity of 360 days
        for: CN=Ronny Valtonen, OU=HP Spectre, O=SNHU, L=Forest Grove, ST=Oregon, C=US

C:\Windows\System32>
```

Export CER file

```
C:\Windows\System32>"C:\Program Files\Java\jdk-23\bin\keytool.exe" -export -alias module5 -storepass password -file server.cer -k
eystore keystore.jks
Certificate stored in file <server.cer>

C:\Windows\System32>
```

Print cert

```
C:\Windows\System32>"C:\Program Files\Java\jdk-23\bin\keytool.exe" -printcert -file server.cer
Owner: CN=Ronny Valtonen, OU=HP Spectre, O=SNHU, L=Forest Grove, ST=Oregon, C=US
Issuer: CN=Ronny Valtonen, OU=HP Spectre, O=SNHU, L=Forest Grove, ST=Oregon, C=US
Serial number: e56f353b079dee39
Valid from: Sun Apr 06 22:37:40 PDT 2025 until: Wed Apr 01 22:37:40 PDT 2026
Certificate fingerprints:
         SHA1: E7:1D:C3:98:DB:E3:7D:7D:2F:5F:E2:2D:5A:C6:41:40:80:44:E3:CD
         SHA256: C1:14:5B:2A:A2:B4:56:81:DF:2D:25:7A:C7:18:20:90:7D:2A:03:39:75:62:F7:A9:03:B2:F1:FC:B0:FD:4A:F5
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: 56 8C 1A 47 E7 49 92 20   CF A4 31 45 3B 6F DE B3  V..G.I. ..1E;o..
0010: 14 90 CB F8                                        ....
]
]
```

Sources

Jim Manico and August Detlefsen, *Iron-Clad Java: Building Secure Web Applications (Oracle Press)*, 2014, http://dl.acm.org/citation.cfm?id=2826076.

"Let's Encrypt," March 18, 2025. https://letsencrypt.org/.