

Kennedy Uzoho

CS 305

Module Five: Certificate Authority Generation

10/02/2022

- **Why would you want to use a CA for security?**

The Certificate Authority is an organization that provides secure encrypted communication between two parties over a network. CA ensures that a website is authenticated. A CA authenticates connections to ensure that website or a particular communication is authentic by verifying its SSL/TLS certificate. CA stores, issues, and signs a digital certificate access form. It is the root of trust that provides services that authenticate the identity of servers, computers, computer systems, websites, and other entities such as IoT.

- **What are the advantages of using a CA?**

CA provides trusted verification that ensures a system is securely connecting to another system by providing trust certificates. CA provides security for data in transit or between sources. A CA can help provide sensitive information about revoked or suspended certificates, helping users know which source to trust.

Certificate information form filled out with all fields completed

```
MINGW64/c/Users/Kenyk
$ keytool -genkeypair -alias KenDev -keyalg RSA -keysize 2048 -storetype PKCS12 -keystore KenDev.p12 -validity 365
0
Enter keystore password: password
Re-enter new password: password
What is your first and last name?
[Unknown]: Kennedy Uzoho
What is the name of your organizational unit?
[Unknown]: SNHU
What is the name of your organization?
[Unknown]: CS 305
What is the name of your City or Locality?
[Unknown]: PHILLY
What is the name of your State or Province?
[Unknown]: PA
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=Kennedy Uzoho, OU=SNHU, O=CS 305, L=PHILLY, ST=PA, C=US correct?
[no]: YES

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 3,650 days
for: CN=Kennedy Uzoho, OU=SNHU, O=CS 305, L=PHILLY, ST=PA, C=US

Kenyk@bigscreen MINGW64 ~
$
```

Command to export KenDev.p12 to certificate file server.cer

```
Kenyk@bigscreen MINGW64 ~  
$ keytool -export -alias KenDev -storepass password -file server.cer -keystore KenDev.p12  
Certificate stored in file <server.cer>
```

Screenshot of certificate file (server.cer) printed out

```
Kenyk@bigscreen MINGW64 ~  
$ keytool -printcert -file server.cer  
Owner: CN=Kennedy Uzoho, OU=SNHU, O=CS 305, L=PHILLY, ST=PA, C=US  
Issuer: CN=Kennedy Uzoho, OU=SNHU, O=CS 305, L=PHILLY, ST=PA, C=US  
Serial number: baddalebfce023e8  
Valid from: Sun Oct 02 22:47:11 EDT 2022 until: Wed Sep 29 22:47:11 EDT 2032  
Certificate fingerprints:  
  SHA1: 96:AA:0B:60:26:E2:6C:9B:BC:54:8F:6C:AD:AA:F2:3F:33:06:1D:19  
  SHA256: 35:49:BD:1A:B2:F8:FD:0C:BF:49:4D:BF:A2:54:6E:34:BB:7C:DE:FF:E2:69:1B:3D:B5:6A:C4:CC:7D:49:98:27  
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: 61 A4 97 AB 79 1A 89 55 7B 3C 9D 2C 14 39 B6 43 a...y..U.<.,.9.C  
0010: DD F5 47 EE ..G.  
]  
]  
]
```

## Reference

- Crane, C. (2021, June 10). *What Is a Certificate Authority (CA) and What Do They Do?* Hashed Out by The SSL Store™. <https://www.thesslstore.com/blog/what-is-a-certificate-authority-ca-and-what-do-they-do/#but-just-how-many-cas-are-there>
- IBM. (n.d.). *Benefits of Self-signed and CA-signed Digital Certificates*. IBM.Com. Retrieved October 2, 2021, from <https://www.ibm.com/docs/en/b2b-integrator/5.2?topic=certificates-benefits-self-signed-ca-signed-digital-certificates>
- SSLSTORE. (n.d.). *What is an SSL/TLS Certificate? Here's a Quick Overview*. SSLStore.Com. Retrieved October 2, 2021, from <https://www.thesslstore.com/new-to-ssl/what-is-ssl-tls.aspx>