

Why would you want to use a CA for security?

In short, you would want to use a CA for security so it can't be faked. In longer terms, certificate authorities (CAs) are what make the internet secure and trustworthy. They sign digital certificates to show that a website's identity is who they say they are. This helps prevent phishing attempts and other malicious web fraud attempts. A third party verifying the authenticity of the site is the most secure way of verification.

What are the advantages of using a CA?

There are advantages to using a CA as opposed to other options like self-signed certificates or the Web of Trust option. Some of these include trusted authentication, the encryption they provide, and the standards they must uphold. Self-signed certificates still happen, but without a trusted certificate you get that "This site's security certificate is not trusted!" message. While you know that your site is trusted, others don't. It is the same kind of thing with Web of Trust Certificates, others may sign off on a certificate, but you might not trust those people. However, with enough people signing off on the certificate, that trust may begin to grow. I still think that a CA is the better option because of the benefits they offer.

Screenshot below.

```
Administrator: Windows Pow...
PS C:\Users\bryce\OneDrive - SNHU\CS-305\Module5\CS-305 5-2 Coding Assignment> keytool.exe -genkey -keyalg RSA -alias selfsigned -keystore keystore.jks -storepass Header-Dish-Radiated2 -validity 360 -keysize 2048
What is your first and last name?
[Unknown]: Bryce Jensen
What is the name of your organizational unit?
[Unknown]: Family
What is the name of your organization?
[Unknown]: Jensen Family
What is the name of your City or Locality?
[Unknown]: Expensiveville
What is the name of your State or Province?
[Unknown]: Utah
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=Bryce Jensen, OU=Family, O=Jensen Family, L=Expensiveville, ST=Utah, C=US correct?
[no]: yes

PS C:\Users\bryce\OneDrive - SNHU\CS-305\Module5\CS-305 5-2 Coding Assignment> keytool.exe -export -alias selfsigned -storepass Header-Dish-Radiated2 -file server.cer -keystore keystore.jks
Certificate stored in file <server.cer>
PS C:\Users\bryce\OneDrive - SNHU\CS-305\Module5\CS-305 5-2 Coding Assignment> keytool.exe -printcert -file server.cer

Owner: CN=Bryce Jensen, OU=Family, O=Jensen Family, L=Expensiveville, ST=Utah, C=US
Issuer: CN=Bryce Jensen, OU=Family, O=Jensen Family, L=Expensiveville, ST=Utah, C=US
Serial number: 16987c35
Valid from: Sat Nov 25 15:01:53 MST 2023 until: Tue Nov 19 15:01:53 MST 2024
Certificate fingerprints:
    SHA1: 09:F1:B6:9D:29:39:73:98:C8:07:61:42:0F:A0:A1:50:DD:78:99:5E
    SHA256: EE:D5:6D:1E:12:6E:A7:04:5B:1C:89:42:97:C8:D3:1F:B7:C6:C8:F6:AE:70:10:65:A5:57:D2:80:B3:06:F4:82
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: AC AF 69 B7 54 5D 75 27  45 4C F1 4E 06 CC F8 F6  ..i.T]u'EL.N....
0010: 13 15 2B CA                ..+.
]
]
```

Screenshot of both the certificate information form filled out with all fields completed and the screenshot of the printout of the server.cer file in one.