Certificate Authorities (CA) are one of the most vital points of the Public Key Infrastructure (PKI). As defined in our module, CAs are trusted third-party entities that issue digital certificates in order to verify people, organizations and websites online, though developers oftentimes create their own self-signed CAs to skirt the cost and trouble of using a third party. The main reason you would want to use a CA is to reinforce the CIA triad; by using trusted certificates, we are able to know we are connecting to a legitimate website or system and that the data has not been altered, moreover, we can establish encrypted connections via HTTPS ( SSL/TLS) to prevent potential unwanted eavesdroppers(Awati & Loshin, 2025).

The main advantage of using CA is credibility and trust—certificates can become invalided if data changes, and CA’s maintain revocation lists which work to revoke compromised or expired certificates. On top of that, many industries and regulations require the use of CAs to meet security compliance standards like HIPAA for healthcare of PCI-DSS for credit cards—most federal systems are recommended for use of CA’s (McKay & Cooper, 2019). CAs allow users to know that the connection they are making is secure and with an authenticated individual / website / system, etc. and is safe from prying eyes. In the following screenshots, I show the generation of a self-signed certificate.

A screen shot of a computer

AI-generated content may be incorrect.

Figure - Screenshot with Certificate Information

A screenshot of a computer program

AI-generated content may be incorrect.

Figure - Screenshot showing certificate generation

References:

Awati, R., & Loshin, P. (2025, March 7). *What is a Certificate Authority (CA)?: Definition from TechTarget*. Search Security. https://www.techtarget.com/searchsecurity/definition/certificate-authority#:~:text=Key%20roles%20of%20a%20certificate,organizations%20to%20validate%20their%20identities.

Coclin, D. (2025). *What is a Ca? certificate authorities explained*. DigiCert. https://www.digicert.com/blog/what-is-a-certificate-authority

McKay, K., & Cooper, D. (2019, August 29). *Guidelines for the selection, configuration, and use of Transport Layer Security (TLS) implementations*. CSRC. https://csrc.nist.gov/pubs/sp/800/52/r2/final