# CS 305 Module Five Coding Assignment Certificate Generation Guidelines and Rubric

**Certificate Authorities**

A certificate authority (CA) is a trusted third party that issues digital certificates to verify the identity of websites or organizations. Using a CA ensures authentication and encryption. For example, when you connect to a bank’s site, your browser checks its certificate against a CA, confirming it’s legitimate. CAs add trust and are standard for production environments.

**Certificate Generation**

On macOS, I used the built-in Java Keytool command to create a self-signed certificate. After generating a new keystore, I exported the certificate to a .cer file and verified its contents. This confirmed the certificate was valid and included a 2048-bit RSA key with SHA-256 signature.

keytool -genkey -keyalg RSA -alias selfsigned -keypass cs305snhu -keystore keystore.jks -storepass cs305snhu -validity 360 -keysize 2048

A black screen with white text

AI-generated content may be incorrect.

keytool -export -alias selfsigned -storepass cs305snhu -file server.cer -keystore keystore.jks

keytool -printcert -file server.cer

A computer screen shot of a black screen

AI-generated content may be incorrect.

Proof of exported .cer

A screenshot of a black box

AI-generated content may be incorrect.

**References**

Oracle. (n.d.). *Keytool – key and certificate management tool*. Oracle Documentation. https://docs.oracle.com/en/java/

Rescorla, E. (2018). *SSL and TLS: Designing and building secure systems*. Addison-Wesley.