5-2 Coding Assignment: Certificate Generation

Sean M Jetté

CS-305

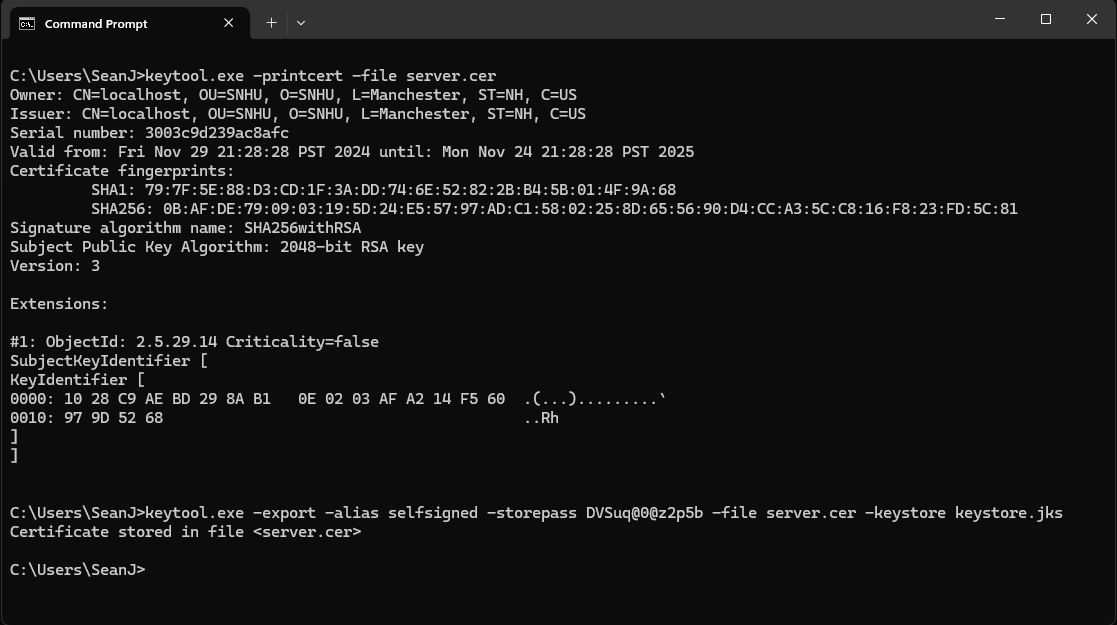
Professor Norman

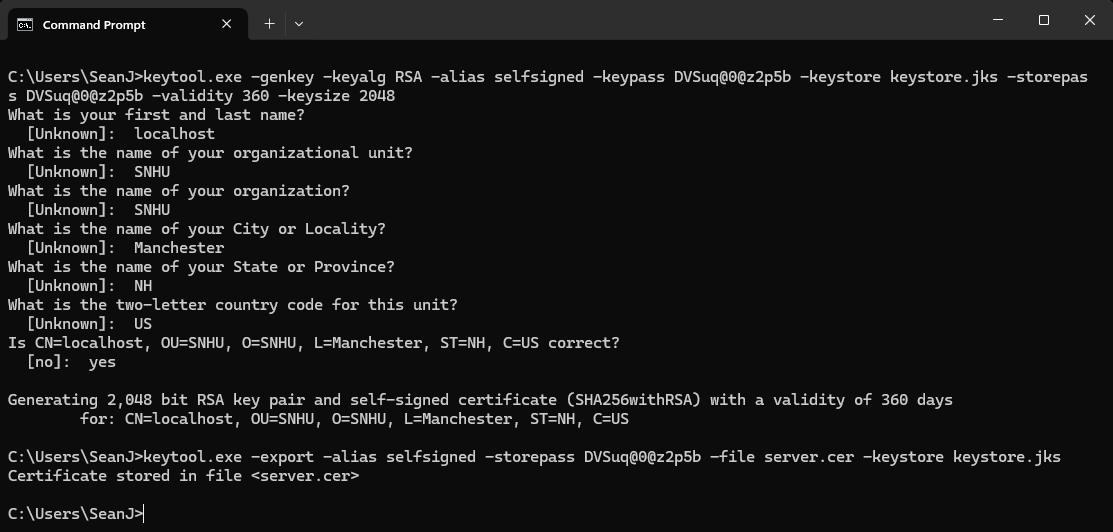
Certificate Authorities

Within the web security framework, there are many factors at play to ensure security is at the forefront of the user experience. As a function of that infrastructure, certificate authorities (CA)—a key component of the public key infrastructure (PKI)—play a crucial role in verifying the authenticity of websites and ensuring secure communications. When visiting a site labeled with a notification of “not secure,” this typically indicates that the site has not been validated by a CA or its certifricate has expired (Nelson, n.d.). This underscores the importance of needing a CA for security, with several critical factors to consider. One primary reason for relying on a CA is authentication. A CA verifies the legitimacy of a website or server through proper identifications, preventing potential man-in-the-middle attacks. Through the ensuring of authentication and data integrity, certificates enable HTTPS for data encryption and protection from eavesdropping (Gitlan, 2024).

There are several advantages to utilizing a CA-issued certificate over a self-signed certificate. Starting with the trust factor: where certificates generated by third-party CAs are automatically recognized and trusted by browsers, while self-signed certificates are not inherently trusted by other systems and require manual configuration to be accepted (Yitzhak, 2024). Additionally, CAs offer reliable and scalable systems for issuing and managing certificates; which is especially beneficial for larger organizations. They ensure that only legitimate organizations and individuals can obtain a TLS certificate, safeguarding trust and security throughout the web. While self-signed certificates might provide potential cost-effectiveness and greater control during development, they are insufficient for meeting extensive regulatory compliance requirements, such as those mandated by HIPAA. Regulatory frameworks often require trusted CA-issued certificates to ensure secure and compliant communications (SSL Corp, 2022).

Certificate Generation





References:

Gitlan, D. (2024, September 19). *How does TLS prevent Man-In-The-Middle attacks?* SSL Dragon. https://www.ssldragon.com/blog/ssl-prevent-mitm-attacks/

Nelson, M. (n.d.). *What is a CA? Certificate Authorities Explained*. https://www.digicert.com/blog/what-is-a-certificate-authority

SSL Corp. (2022, December 21). *Digital Certificates for HIPAA-Compliant Communication - SSL.com*. SSL.com. https://www.ssl.com/blogs/digital-certificates-for-hipaa-compliant-communication/

Yitzhak, T. (2024, November 21). Understanding Digital Certificates: Self-Signed vs. CA-Signed Certificates. *Medium*. https://medium.com/@talyitzhak/understanding-digital-certificates-and-self-signed-certificates-b1cdca759bbc