Matt Tranchina 11/26/2023

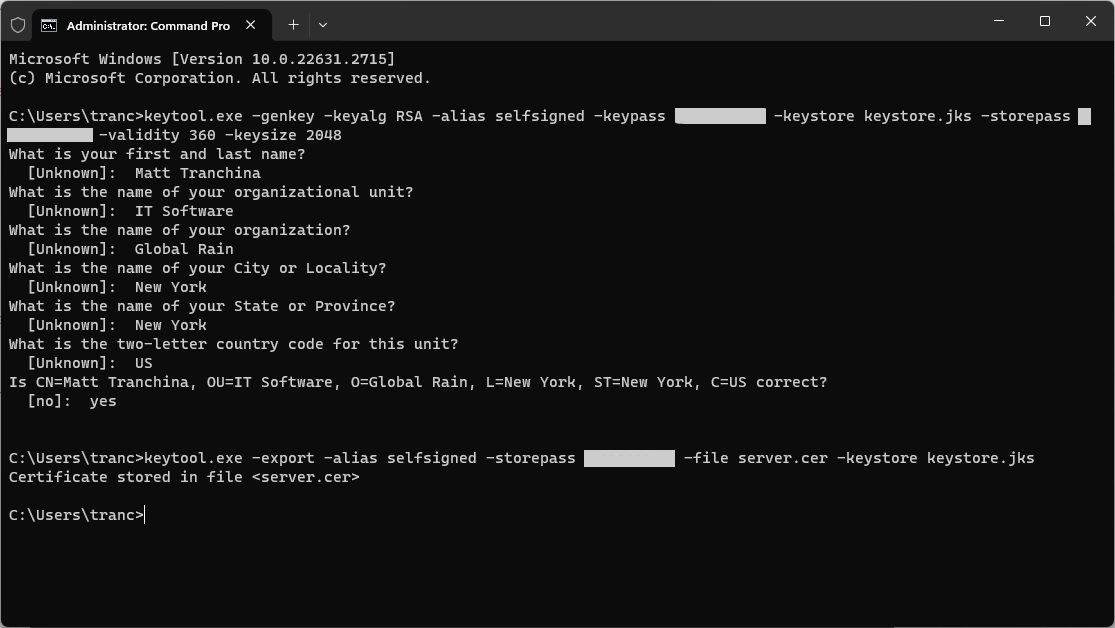
CS- 305 Software Security 5-2 Certificate Generation

In cryptography, a certificate authority or certification authority (CA) is an entity that stores, signs, and issues digital certificates ("Certificate authority", 2023). Essentially this means that a CA helps ensure the authenticity of a website. It creates a “digital fingerprint” to prove that the website that a person is dealing with is verified and true. Websites can be verified by trusted third party companies like IdenTrust, DigiCert, and Sectigo. Using a CA has multiple advantages, such as establishing a secure connection and preventing a “man-in-the-middle” attack.

When data is being transmitted, an attacker can place themselves between the two endpoints and intercept the data to either collect information or change the data completely. This is known as a man-in-the-middle attack. When entering a website for the first time, the server sends its public key along with a digital certificate that is signed by the CA. Once it establishes this trust with the client through a process known as an SSL/TLS handshake, then a secure, encrypted connection forms between them (Crane, 2020). Having a CA verifies the company, or server, before issuing a TLS certificate. Once the TLS handshake is established, a public key is used by the user’s browser to encrypt the data that is sent to the website, of which has a private key to decrypt the data. This ensures that the data in question is being transferred between two trusted parties and the data is being encrypted during transit.

When dealing with sensitive information, it is always reassuring that your information is kept confidential. Visiting a website using the HTTPS prefix ensures that the website is verified by a third party and can be trusted. Developers can generate self-signed certificates, which makes the developer the CA. Doing so avoids the costs and trouble of domain names and certificate authority interactions. The following screenshots show my certificate information form filled out with my information and a printout of the server certificate file.

**Certificate of Information**



**Printout of the Server.cer**

**A screenshot of a computer program

Description automatically generated**

**References**

Crane, C. (2020, August 11). What Is a Certificate Authority (CA) and What Do They Do? Security Boulevard. <https://securityboulevard.com/2020/08/what-is-a-certificate-authority-ca-and-what-do-they-do/>

Certificate authority. (2023, November 7). In Wikipedia. <https://en.wikipedia.org/wiki/Certificate_authority>