5-2 Coding Assignment: Certificate Generation

Armon Wilson

SNHU CS-305

**Certificate Generation**

Why would you want to use a CA for security?

Certificate Authorities (CAs) are trusted third-party entities that play a crucial role in establishing trust and security in online communication (Manico & Detlefsen, 2015). They issue digital certificates that serve as electronic passports for websites, verifying their identity and enabling secure connections. These certificates bind a public key to a website's domain name, and when you visit a secure website (HTTPS), your browser checks the website's certificate against the CA's trusted list (Manico & Detlefsen, 2015).

What are the advantages of using a CA?

Using a CA offers several advantages for security. CAs are recognized and trusted by major web browsers and operating systems, so when a website presents a certificate issued by a trusted CA, your browser automatically establishes a secure connection (Manico & Detlefsen, 2015). This ensures that the data you exchange with the website is encrypted and protected from eavesdropping. Cas verify the identity of website owners before issuing certificates, helping to prevent impersonation attacks where malicious actors create fake websites to steal your information (Manico & Detlefsen, 2015). Digital certificates enable the use of HTTPS, which encrypts data transmitted between your browser and the website, protecting your sensitive information from being intercepted and misused (Manico & Detlefsen, 2015).

Certificate information form:

A screen shot of a computer

Description automatically generated

Certificate information found in the server.cer file:

A computer screen with white text

Description automatically generated

**References:**

Manico, J., & Detlefsen, A. (2015). Iron-Clad Java. McGraw Hill Computing.