Coding Assignment 5-2: Certificate Generation

Dhiraj Gurung

Southern New Hampshire University

CS305

Wayne Morris

April 3, 2025

**Certificate Generation**

* 1. You would want to use a Certificate Authority (CA) for security because a CA is a trusted third-party entity that helps verify and authenticate the connection between two parties. To become a CA the CA must go through a very rigorous process and as a result there are not many Certificate Authorities out there. This process is one of the reasons that we can trust a CA. The CA uses both the server’s public key and the CA’s private key to create an encrypted public server key, also known as a signature. The encrypted public server key is then sent to the browser and then the browser will use the CA’s public key and the encrypted server public key to verify if it matches the server’s public key. This process utilizes both digital certificates and cryptographic keys which provide security for data while in transit.
  2. The first advantage of using a Certificate Authority is that it provides an added layer of security to the verification process. This is because if we are trying to communicate to another server without a CA to sign and authenticate our server certificate, we are vulnerable to a man in the middle attack. However, if we use a CA to sign our server certificate then we can rest assured that communication between the two servers are secure unless the whole CA is compromised. Certificate Authorities also have another advantage which is that they can provide trust to two parties. The Cas are created through a tough process that not just anyone can pass. As a result, they are widely trusted by major companies and used industry wide. While CA’s are not invulnerable entities, they make secure communication between two parties possible “without either having to

know or trust the other party” (Al-Janabi, 2012).

**Commands Used:**

keytool.exe -genkey -keyalg RSA -alias selfsigned -keypass passcs305 -keystore keystore.jks -storepass passcs305 -validity 360 -keysize 2048

keytool.exe -export -alias selfsigned -storepass passcs305 -file server.cer -keystore keystore.jks

keytool.exe -printcert -file server.cer

keytool.exe -export -alias selfsigned -storepass passcs305 -file server.cer -keystore keystore.jks

**Screenshot of Questions and Answers:**

A screenshot of a computer program

AI-generated content may be incorrect.

**Screenshot of Server.cer file:**

A screenshot of a computer

AI-generated content may be incorrect.

**Citations:**

*Al-Janabi, S. F., & Obaid, A. K. (2012, April). Development of certificate authority services for web applications. In 2012 International Conference on Future Communication Networks (pp. 135-140). IEEE.*

*Defining certificate authority and how it works*. Okta. (n.d.). https://www.okta.com/identity-101/certificate-authority/

*Laiture.* (n.d.). HTTPS, SSL, TLS & Certificate Authority Explained. YouTube. https://www.youtube.com/watch?v=EnY6fSng3Ew