CS 305 Software Security  
5-2 Certificate Generation

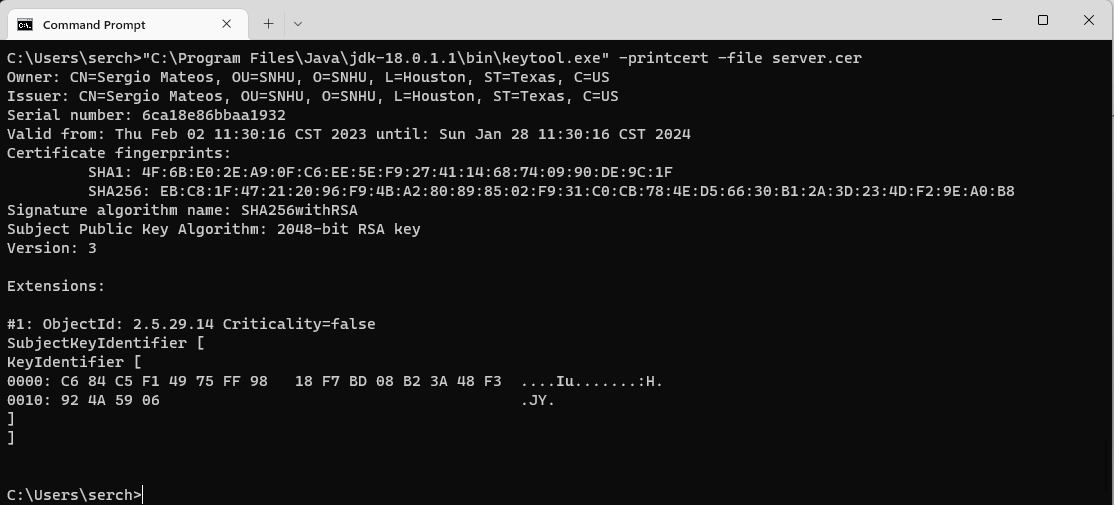
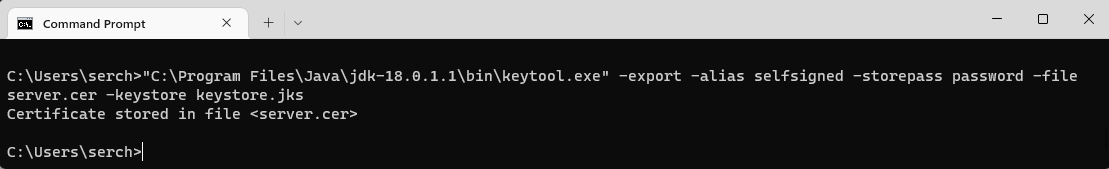
Sergio Mateos

Southern New Hampshire University

Certification Generation

1. Certificate Authorities:
   1. Why would you want to use CA for security?
      1. Certificate Authority (CA) is a trusted entity issued Secure Socket Layer (SSL) certificates, in other words, verify websites and other entities to ensure the users who they are communicating with. These certificates are encrypted and linked to a public key, and web browsers use them to authenticate the content. CA makes the internet more secure playing a role as pivotal role. The Secure Sockets Layer (SSL) or Transport Layer Security (TLS) ensures that communication is secure when communicating. The best way to describe is mentioned by TechTarget, a tech website, “The main goal of a CA is to verify the authenticity, and trustworthiness of a website, domain and organization so users know exactly who they're communicating with online and whether that entity can be trusted with their data.” (Loshin, 2021).
   2. What are the advantages of using CA?
      1. The main advantage is that it provides trust and certainty to the user of access to the authentic source. Ensuring that the user is accessing to authentic source provides security that the data is being transmitted and secured.
2. Certificate Generation
   1. Located JavaKeytool: "C:\Program Files\Java\jdk-18.0.1.1\bin\keytool.exe"
   2. Text

      Description automatically generatedCopy and Paste command: -genkey - keyalg RSA -alias selfsigned -keypass password -keystore keystore.jks -storepass password -validity 360 -keysize 2048
   3. Text

      Description automatically generatedSecure password for the keystore: -export -alias selfsigned -storepass password -file server.cer -keystore keystore.jks
   4. Demonstrate the certificate was effectively generated: -printcert -file server.cer
   5. Accessing to key store -export -alias selfsigned -storepass **changeme(password)** -file server.cer -keystore keystore.jks

Reference

Awati, R., & Loshin, P. (2021, September 1). *What is a Certificate Authority (CA)?* Security. Retrieved February 2, 2023, from https://www.techtarget.com/searchsecurity/definition/certificate-authority#:~:text=A%20certificate%20authority%20%28CA%29%20is%20a%20trusted%20entity,web%20servers%2C%20ensuring%20trust%20in%20content%20delivered%20online.

Admin. (2020, February 3). *4 benefits of certificate-based authentication*. GlobalSign. Retrieved February 2, 2023, from https://www.globalsign.com/en/blog/4-benefits-of-certificate-based-authentication