**Certificate Generation**

Justin Starr

Department of STEM

CS 305 – Software Security

Dr. Sarah North

October 1, 2023

**Certificate Generation**

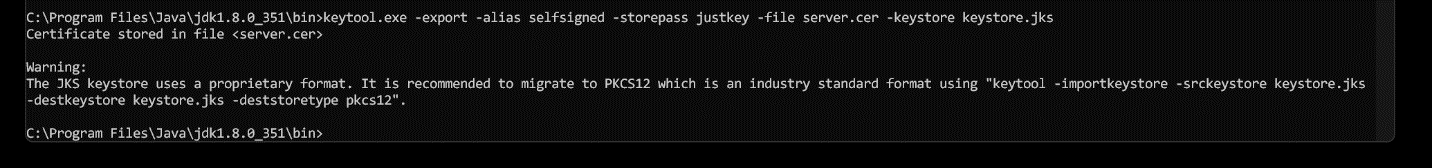
The following is a short analysis of why a person would want to use a CA (Certificate Authority) for security and its advantages. CAs are the backbone of Security protocols, such as SSL (Secure Sockets Layer) and TSL (Transport Security Layer) that provide a public key infrastructure, enabling people to trust servers that they have never had experience working with before (Manico & Detlefsen, 2014, Chapter 6). The reason why a person would want to use a CA for security is because it helps to establish a secure communication channel (Manico & Detlefsen, 2014, Chapter 6). When, for example, a TSL client connects to a server, the server sends its certificate to the client and the client then determines whether or not it trusts the CA that signed the certificate (Manico & Detlefsen, 2014, Chapter 6). If the client does in fact trust the CA that signed the certificate, they can choose to trust the server that the certificate came from once it has been verified that the certificate authority, did in fact, sign the certificate (Manico & Detlefsen, 2014, Chapter 6). It essentially establishes trust between the client and the server. Similar to how CAs can be used when helping to establish secure connections, they are also used to digitally sign data (Oracle, 2018). “When data is digitally signed, the signature can be verified to check the data integrity and authenticity”, (Oracle, 2018). When referring to the integrity of the data it means that the data has not been changed and its authenticity refers to the data coming from the person that says has created the data and signed it; that it did not come from somewhere else (Oracle, 2018).

An advantage of using a CA is that it takes away much of the burden of maintaining or managing your own certificates or private CAs (DigiCert, 2023). Public CAs have established themselves as trusted authorities that the public can rely on to ensure that the websites they visit or the data they obtain from various companies are in fact what they say they are (DigiCert, 2023). Additionally, utilizing such authorities helps remove further burdens such as CA compliance, technicalities, and additional security concerns (DigiCert. 2023).

The following are screenshots that include the certificate information form filled out with all fields completed and a screenshot of the server.cer file to demonstrate that the certificate has been effectively generated.

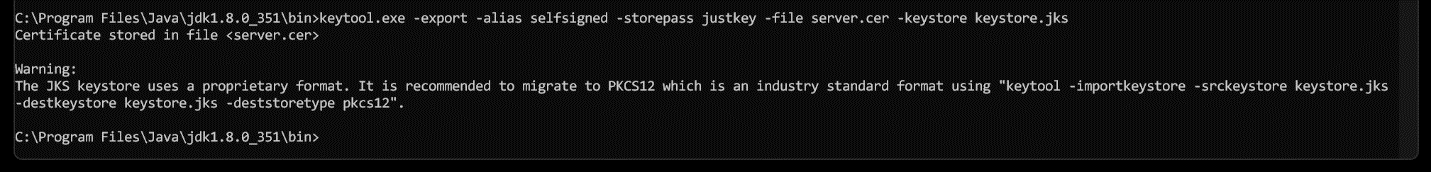
A computer screen with white text

Description automatically generated



A screenshot of a computer

Description automatically generated



**References**

DigiCert. (2023). *Benefits of Partnering with a Certificate Authority*. Benefits of Partnering

with a Certificate Authority | DigiCert.com. <https://www.digicert.com/blog/benefits-of-partnering-with-a-certificate-authority>

Manico, J., & Detlefsen, A. (2014). *Iron-Clad Java: Building Secure Web Applications*. McGraw

Hill Computing. <https://learning.oreilly.com/library/view/iron-clad-java/9780071835886/?sso_link=yes&sso_link_from=SNHU>

Oracle. (2018). *Keytool - Key and Certificate Management Tool*. keytool-Key and Certificate

Management Tool. <https://docs.oracle.com/javase/6/docs/technotes/tools/windows/keytool.html>