CS-305-J7997 Software Security

Module Five – Certificate Generation

Computer Science Department

Southern New Hampshire University

Eric Farkas

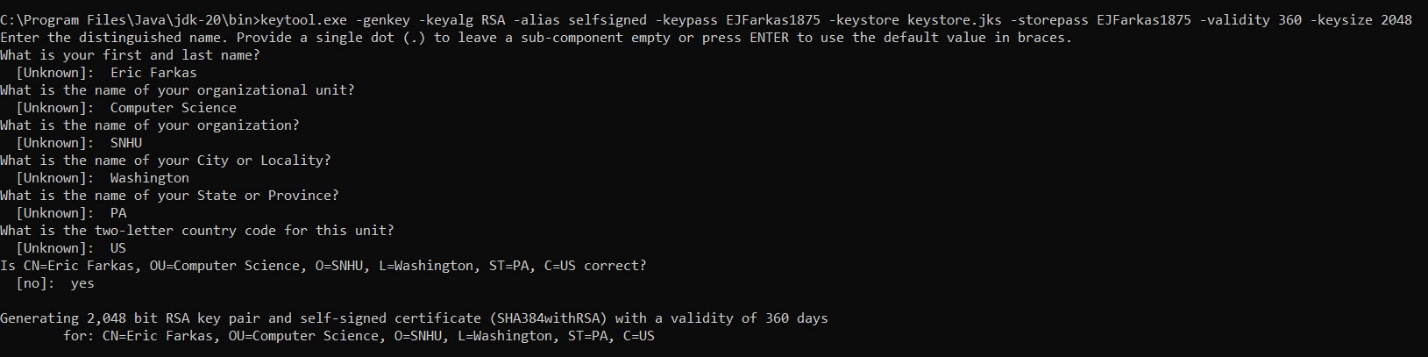
4/2/2023

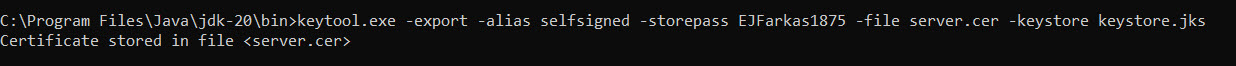
**Certificate Authorities:**

Certificate authorities, often referenced as CAs, ensure that entities dealing with sensitive data are legitimate. They do this through several methods designed to ensure the entity is authentic and that sensitive data is not being transmitted to a third party. Digital certificates are the primary method. These certificates are generated and placed on the public-facing side of systems. There is an exchange of information before any sensitive data is transmitted. This exchange ensures that both ends of the data channel are capable and compatible with communicating securely. The server then issues a key and waits for the client to respond with its key. Many certificates currently in use are held locally in systems and are called root certificates. These may be issued by a certificate authority or created locally depending on the application. System-to-system certificates are often generated locally as there is no reason to pay a certificate authority for entity validation and registration. User-to-system certificates almost always come from a certificate authority. Occasionally, an additional layer of protection must be placed in front of the root certificate. Intermediate certificates are built from the root certificate but hosted independently. An intermediate can be more easily replaced or deactivated than a root certificate.

In addition to certificate generation, certificate authorities verify entities, domains and registration information. This practice ensures the entity and its resource information is up to date and readily contactable should there be any question regarding authenticity or any suspicion that spoofing may have occurred. This practice also allows certificates to be quickly revoked in case of a breach. Certificates are not limited to transactional data connections. Certificate authorities also help to ensure the integrity of applications installed on a computer by validating and signing the code itself. The application provider information is shown during the installation process, and the user can proceed or stop based on this disclosure. Certificate authorities focus on security, authenticity and the chain of custody for data. This is expertise many entities do not have in house which makes the services CAs provide very valuable.

**Certificate Generation:**

****

****

