CS 594—Enterprise and Cloud Security
Assignment Three—Certificate Manager—Rubric

Testing (demonstrated via videos) should use the showcerts command to show the contents of the keystores and truststores after running each of the commands.

For the off-line root certificate authority, the manager provides these commands:

1. ☐ (10 points) `gencaroot`: Initialize the off-line keystore with the self-signed certificate for the root CA.
2. ☐ (10 points) exportcaroot --cert *cert-file*: Export an X509 certificate for the root CA, as a PEM file.

For managing online keystores, the manager provides these commands:

1. ☐ (10 points) genservercert --dns *server-domain-name*: Generate an SSL certificate for the server, signed by the root CA, that clients can use to authenticate the server, and stored in the application server keystore.
2. ☐ (10 points) genonlinecacert: Generate a certificate for the online CA, signed by the offline CA, and stored in the online keystore.
3. ☐ (10 points) exportonlinecacert --cert *cert-file*: Export an X509 certificate for the online CA, as a PEM file.

For now, we manage client certificates using the certificate manager:

1. ☐ (10 points) genclientroot --clientdn *client-dist-name* --duration *cert-duration* --keystore *client-keystore* --storepass *keystore- password* --keypass *key-password*: Initialize the client keystore with a self- signed v1 certificate.
2. ☐ (10 points) genclientcsr --keystore *client-keystore* --storepass *keystore-password* --keypass *key-password* --csr *csr-file* [--dns *client-domain-name*]: Generate a certificate signing request with the client keystore, outputting the result as a PEM file. The CSR is signed by the self-signed root certificate for the client, stored in the specified client keystore. Optionally the CSR may include a DNS domain name for the client.
3. ☐ (10 points) genclientcert --csr *csr-file* --cert *cert-file*: Generate a client certificate from the certificate signing request (CSR). The client certificate is signed by the online CA. Both the input CSR and the output certificate are PEM files.
4. ☐ (10 points) importclientcert --keystore *client-keystore* --storepass *keystore-password* --keypass *key-password* --cert *cert-file*: Import the client certificate into the specified client keystore. The certificate is provided as a PEM file.

☐ (5 points) Deployment: Show the certificate that the Web server provides.

Rubric: 5 points ☐

Total: _____