Plugins Required: PyOpenSSL

Python Version Used: 3.5.2

Usage:

1. Run ‘SelfSignedCertificate.py’
2. First create a root certificate by typing ‘r’
3. Enter the root certificate signing request details: Country: (Must be two characters), State, location, organization, organization unit and common name.
4. Program will then create the csrRequest, privateKey and X509RootCertificate files.
5. Now that these files have been generated, an you can type ‘e’ to create an end user certificate.
6. Enter the end user certificate signing request details: Country: (Must be two characters), State, location, organization, organization unit and common name.
7. Program will then create the endUserCertificate file
8. Now that a root certificate and end user certificate exists, the user can enter ‘v’ to validate the certificate of their choosing.
9. Enter the name of the certificate you wish to validate. E.g. ‘EndUserCertificate.crt’
10. The program will then perform a check to ensure the given certificate validates against the chain of certificates.