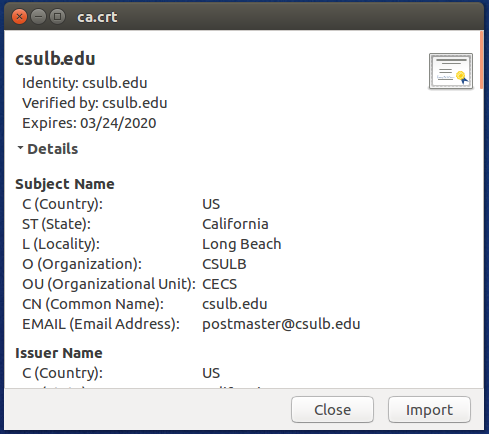
**Lab #3**

**CECS 378 – Spring 2021 Cappel**

**Due:** Wednesday, February 24th prior to lab (11:59 PM)

**Screen Shot 1)** Right-click on the *ca.crt* file and Open with View file. Expand the details section and take a snip (screen shot) of the contents of the file and then close the file.



**Question 1)** How long is the *ca.crt* valid? What RSA key size was used for the Public key found in *ca.crt*?

**Answer:** The ca.crt certificate is valid for one month. The RSA key size is 2048 bits.

**Question 2)** How many bits is the private key generated in the *server.key*?

**Answer:** The private key is 1024 bits.

**Question 3)** Who verified the *server.crt* certificate? How long is the *server.crt* valid?

**Answer:** The certificate was verified by csulb.edu. The certificate is valid for one year.

**Question 4)** Why do you think the web server failed to start when changing the certificate information but not the modulus information?

**Answer:** The modulus is not used to validate the certificate. It was only used in generating the public/private key pair. Changing the modulus will have no effect. However, changing the certificate information will affect the validity of the certificate and cause the web server to fail.

**Question 5)** Did your browser allow you to connect to the website? Why or why not?

**Answer:** The browser will NOT allow you to connect to the website because the URL (localhost) does not match the common name listed in the certificates in the certificate store of the browser.

**Question 6)** Did your browser allow you to connect to the website? Why or why not?

**Answer:** The browser will NOT allow you to connect to the website because the certificate is still leveraging a common name of SEEDPKILab2020.com. If the common name does not match the URL you are attempting to access, your browser should warn you.

**Question 7)** How important is it to protect the private key of your CA? Explain…

**Answer:** It is critical that the private key of the CA is kept confidential. If it is compromised an adversary can spoof the duties of the CA, publish malicious certificates, and ultimately impersonate any web site leveraging that CA in its certificate trust chain.

**Question 8)** What information is being stored in the index.txt file?

**Answer:** The index.txt file contains the certificate serial number, the serial count of each certificate, and the Owner and Common Name used for each certificate.

*V 210222030552Z 1000 unknown /C=US/ST=California/L=Long Beach/O=SEEDLabsInc./CN=SEEDPKILab2020.com*

*V 210222033342Z 1001 unknown /C=US/ST=California/L=Long Beach/O=Example Inc./CN=example.com*

**Screen Shot 2)** Take a snip (screen shot) of your SEEDUbuntu1 desktop showing *all* the files and folders you created during this lab. **Hint:** Your screen shot should have 1 folder and 10 files.

