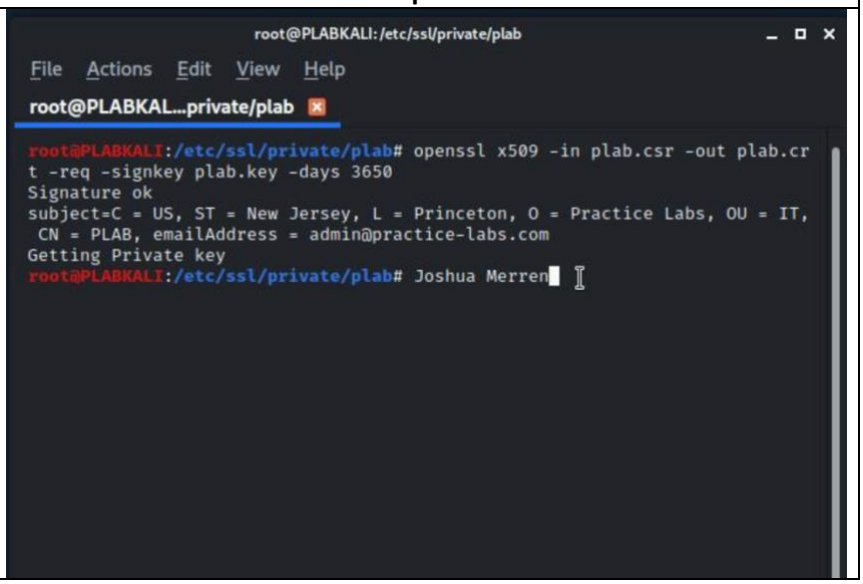
Southern New Hampshire University

CYB 300 Module Five Practice Lab Worksheet

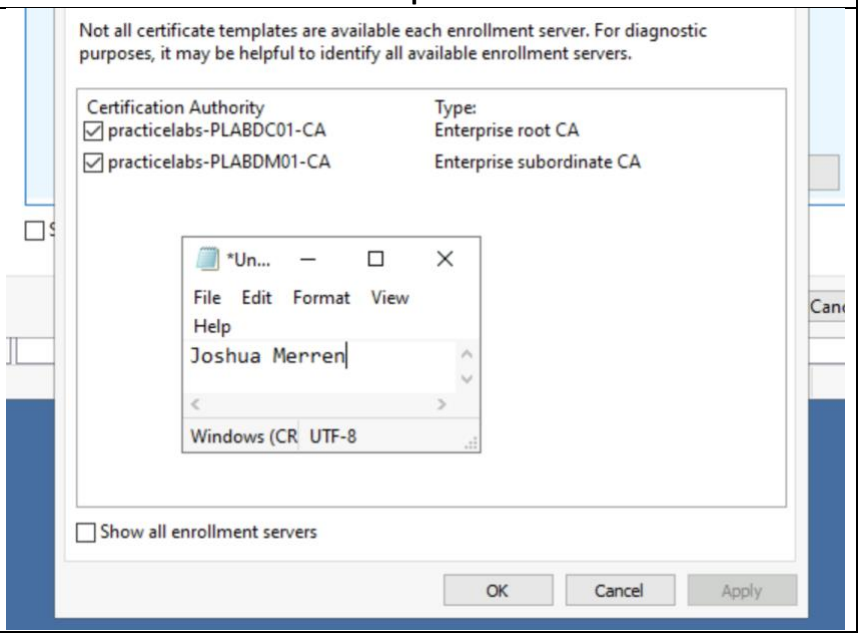
Complete this worksheet by replacing the bracketed phrases in the Response column with the relevant information. For all screenshots, include your name in the command line.

Lab: Implementing a Public Key Infrastructure

Exercise 2: Create a Self-Signed Certificate

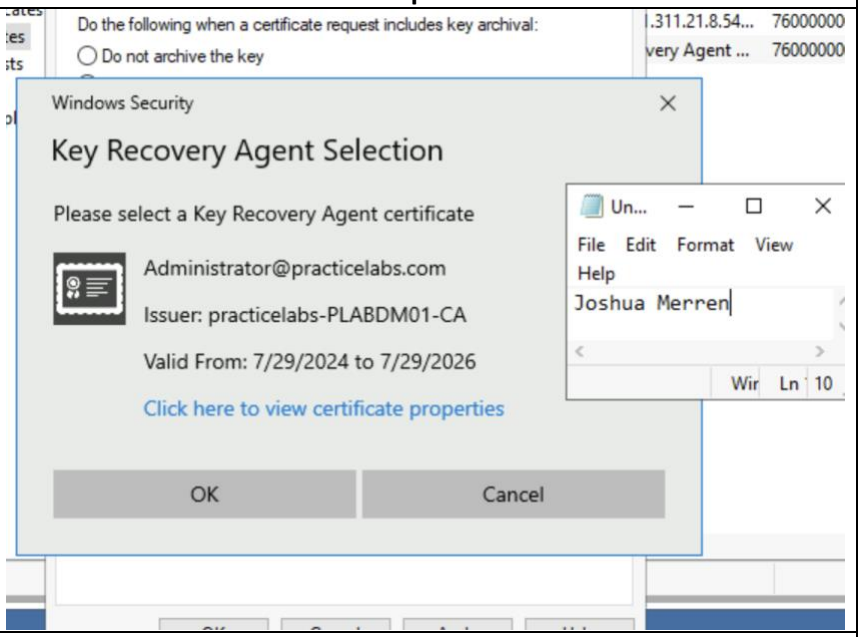
Prompt	Response
Task 1: Take a screenshot of **Step 37** showing the successful creation of the certificate file. Add your name in the command line.	

Exercise 4: Configure Certificate Revocation Lists (CRLs)

Prompt	Response
Task 1: Take a screenshot of **Step 12** showing the presence of both the root CA and the subordinate CAs. Add your name in the command line.	

Prompt	Response
What would be the purpose of creating a subordinate certificate authority?	A subordinate certificate authority (CA) allows for a more scalable and manageable public key infrastructure (PKI). It decentralizes the issuance of certificates to different departments or sectors within an organization, enhancing security by limiting the scope of each CA's authority and reducing the risk of a single point of failure.

Exercise 7: Implement Key Archival

Prompt	Response
Task 4: Take a screenshot of **Step 4** showing the recovery key certificate issued to the administrator. Add your name in the command line.	
What is the importance of issuing a recovery key certificate to a restricted number of individuals?	Issuing a recovery key certificate to a limited number of individuals is crucial for maintaining the security of encrypted data. This strategy ensures that only authorized personnel have access to recover keys, which are necessary for decrypting data if the original encryption keys are lost or compromised. It helps prevent unauthorized access and maintains the integrity and confidentiality of sensitive information.