



## CYB 300 5-1 Lab Worksheet: Implementing a Public Key Infrastructure Lab Worksheet

**Andree Salvo**

**Southern New Hampshire University**

**CYB 300-14668**

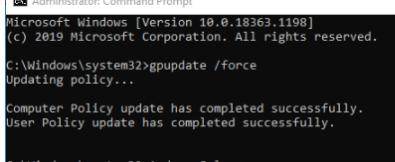
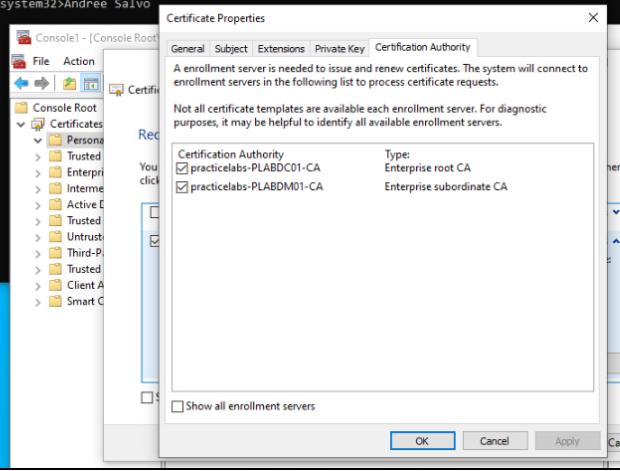
**Instructor: Jason Keltner**

### Lab: Implementing a Public Key Infrastructure

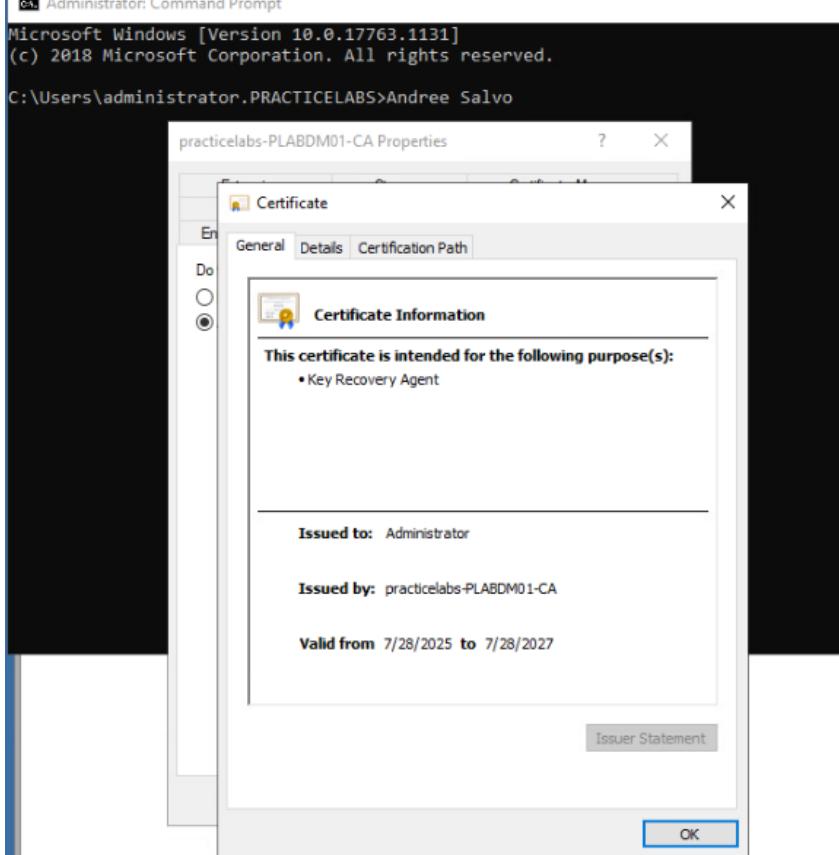
#### Exercise 2: Create a Self-Signed Certificate

Prompt	Response
Task 1: Take a screenshot of <b>Step 37</b> showing the successful creation of the certificate file. Add your name in the command line.	A screenshot of a terminal window titled "root@PLABKALI:/etc/ssl/private/plab". The window has a standard Linux desktop interface with a title bar, menu bar, and scroll bars. The terminal content shows the command "openssl x509 -in plab.csr -out plab.cer -req -signkey plab.key -days 3650" being run by root. The output shows the certificate details: "Signature ok", "subject=C = US, ST = New Jersey, L = Princeton, O = Practice Labs, OU = IT, CN = PLAB", and "emailAddress = admin@practice-labs.com". The command "Getting Private key" is also visible. The final line shows "root@PLABKALI:/etc/ssl/private/plab# Andree Salvo", where "Andree Salvo" is added to the command line. The terminal window is set against a dark background with a faint watermark of a person's face.

#### Exercise 4: Configure Certificate Revocation Lists (CRLs)

Prompt	Response
<p>Task 1: Take a screenshot of <b>Step 12</b> showing the presence of both the root CA and the subordinate CAs. Add your name in the command line.</p>	 
<p>What would be the purpose of creating a subordinate certificate authority?</p>	<p>The purpose of creating a subordinate certificate authority is to issue certificates while keeping the root CA secure and offline.</p>

### Exercise 7: Implement Key Archival

Prompt	Response
<p>Task 4: Take a screenshot of <b>Step 4</b> showing the recovery key certificate issued to the administrator. Add your name in the command line.</p>	 <pre data-bbox="608 274 1447 1129"> Administrator: Command Prompt Microsoft Windows [Version 10.0.17763.1131] (c) 2018 Microsoft Corporation. All rights reserved.  C:\Users\administrator.PRACTICELABS&gt;Andree Salvo  practicelabs-PLABDM01-CA Properties  Certificate General Details Certification Path  This certificate is intended for the following purpose(s): • Key Recovery Agent  Issued to: Administrator Issued by: practicelabs-PLABDM01-CA Valid from 7/28/2025 to 7/28/2027 Issuer Statement OK </pre>
<p>What is the importance of issuing a recovery key certificate to a restricted number of individuals?</p>	<p>Providing a recovery key certificate to a select few helps protect sensitive information by ensuring only highly trusted individuals have access to it, and also minimizing the risk of unauthorized exposure.</p>