General

We have three users as shown below:

Delegate:	Derek
Helpdesk:	Harry (can assist in PIN resets)
Security Officer:	Susan (can request card renewals and card retire)

Exercise 1 – PIN Unblock

The scenario is that the user has successfully completed the issuance of their card and performed a PIN unblock as part of that exercise. Now that they have a smart card, we would expect "log on interactively with a smart card" to be enforced on the user account, meaning that their password is randomised and they can now only log on with a smart card.

However, the user has incorrectly entered the PIN four times and blocked the use of the smart card and cannot perform an unblock without help. We'll enlist the helpdesk and perform the unblock either from a colleague's PC or at a kiosk.

Task Setup	
Setup the Unblock Smart Card Workflow **a) Start CLM as adm** **b) Scroll down the home page and click on the Manage Profile Templates link** **c) Select the "CLM Sample Smart Card Logon" profile template to begin editing it** **d) Select the "Unblock Policy" in the left column** **e) Scroll down to the "Workflow: Initiate Unblock Requests" section** **f) Click add new principal...** **g) Click the lookup button** **h) Narrow the search for users only, then search for Harry (our helpdesk user)** **i) Select the Harry from the returned link and click the OK button** **j) Click on the "Change Password Provider settings" link in the One Time Passwords section** **k) Ensure the default password provider is selected, and a value of 1 is entered** **l) Click on the "Display on Screen" link in the passwords distribution section** **m) Observe that we could distribute a one time password in a number of manners, but for now leave it at "display on screen"** **n) Click the OK button** **That completes setting up the unblock workflow for exercise 1**	

Task Execution	
Blocking of Card **a) The user (Derek) first blocks their smart card PIN by entering the incorrect PIN four times whilst attempting to perform a smart card logon to Windows**	
Derek phones the helpdesk (Harry) who validates the user **a) Harry launches a session to CLM (runas)** **b) Harry clicks on the "Find a user to view or manage their information" link and then searches for "Derek"** **c) In the smart cards section, there is an icon representing Derek's permanent smart card; click on the GUID (link) adjacent to the icon** **d) Then click on the Unblock this smart card link** **e) Make a record of the One-time password displayed on the screen** **Note: if for some reason this is not correctly recorded, Harry can always retrieve this value by:** **1. Clicking on the approved requests link in the left column** **2. Selecting the Approved hyperlink corresponding to an unblock request for Derek** **3. Click on the Distribute button**	

Try it, you can't do any harm!	
a) Derek goes into CLM and clicks on the "Complete a request with one-time passwords" link **b) Derek types in the one-time password and clicks the Next button** **c) Derek is prompted to enter and confirm a new PIN for the smart card** **Note: Derek could have just as easily accomplished this task by clicking on the approved requests link in the left column, this would also have taken him to the screen prompting for a one-time password**	
Perform a smart card logon to prove all is well	

Exercise 2 – Certificate Renewal

Certificates have a finite lifetime, one year is typical, hence they need to be renewed. In CLM, the renewal process can be significantly streamlined whereby when CLM detects the certificate renewal threshold has been reached (say six weeks prior to expiry) and an email is automatically sent to the user with a link and one time password contained which the user would click on and use to be guided through a simple renewal process. In this lab, we'll *force* the renewal process by manually creating a renewal request, however, the email notification and auctioning will be just the same.

Task Setup	
Setup the Renew Smart Card Workflow **a) Start CLM as admin** **b) Scroll down the home page and click on the Manage Profile Templates link** **c) Select the "CLM Sample Smart Card Logon" profile template to begin editing it** **d) Select the "Renew Policy" in the left column** **e) Scroll down to the "Workflow: Initiate Renew Requests" section** **f) Click add new principal...** **g) Click the lookup button** **h) Narrow the search for users only, then search for Susan (our security officer)** **i) Select the Susan from the returned link and click the OK button** **j) Click on the "Change Password Provider settings" link in the One Time Passwords section** **k) Ensure the default password provider is selected, and a value of 1 is entered** **l) Click on the "Display on Screen" link in the passwords distribution section and change the distribution method to Email Subscriber** **m) Enter an email address (this is not going to be validated, it'll just appear in the sender field of the email)** **n) Enter the Mail Subject: "Certificate Renewal Ready"** **o) Enter the body text as below:** ***{User!givenName}*** ***Your smart card logon certificate is ready for renewal, please ensure that you have inserted your smart card into the reader attached to your computer.*** ***To execute the issuance (and get a new certificate) click on the following link: https://clm-vip/clm/content/sm/auth/authorization.Aspx?PasswordCount=1*** ***When prompted for one-time password 1, enter the following value: {Secret1}*** **p) Click the OK button** **That completes setting up the renewal workflow for exercise 2**	

Task Execution	
Security Officer Creates Renewal Request **a) The Security Officer (Susan) launches a session to CLM (runas)** **b) Susan clicks on the "Find a user to view or manage their information link" and then searches for Derek** **c) In the smart cards section, there is an icon representing Derek's permanent smart card; click on the GUID (link) adjacent to the icon** **d) Susan clicks on the "Renew this smart card" link** **e) Susan can observe that a renewal email has been sent to Derek**	
Derek Actions the Renewal **a) Derek opens his email and reads the message sent by the "Security Officer" via CLM** **b) Derek pastes the URL embedded in the message into his browser** **c) Derek pastes the one time password from email message into the CLM prompt, then clicks on the next button**	

d) **When prompted, Derek enters his existing PIN to enable CLM to write the new certificate onto his smart card**	
Perform a smart card logon to prove all is well	

Exercise 3 – Certificate Retirement

Derek has left the company and handed his smart card into the security officer. The security officer will retire the card which will perform the function of revoking any certificates on the card and then "reformatting" it for potential re-use.

Task Setup	
Setup the Retire Smart Card Workflow **a) Start CLM as admin** **b) Scroll down the home page and click on the Manage Profile Templates link** **c) Select the "CLM Sample Smart Card Logon" profile template to begin editing it** **d) Select the "Retire Policy" in the left column** **e) Scroll down and click on the "Change General settings" link in the Workflow: General section** **f) Ensure that "Erase user data from the smart card" is selected, then click the OK button** **g) Click on the "Change Revocation Settings" link in the Workflow: Revocation Settings section** **h) Change the fixed revocation delay to 0, then click the OK button** **i) Scroll down to the "Workflow: Initiate Retire Requests" section** **j) Click add new principal...** **k) Click the lookup button** **l) Narrow the search for users only, then search for Susan (our security officer)** **m) Select the Susan from the returned link and click the OK button** **That completes setting up the retire workflow for exercise 3**	

Task Execution	
Security Officer Inspects Card **a) The Security Officer (Susan) launches a session to CLM (runas)** **b) Susan clicks on the "Find a user to view or manage their information link" and then searches for Derek** **c) In the smart cards section, there is an icon representing Derek's permanent smart card** **d) We can see that this card has two certificates: one which is valid (the renewed one) and one which is revoked (the original certificate)** **e) Let's click on the GUID next to the smart card icon to see more information** **f) Click on the "Derek link" which corresponds to the valid (renewed) certificate** **g) Click on download certificate, then open – we can inspect the certificate which was issued to Derek** **h) Click on the Return quick link in the left column** **i) Observe the smart card operations performed on the card** **a. Enrol – this was originated by the CLM MA** **b. Unblock – originated by Derek in Lab1 straight after the card was issued** **c. Unblock – originated by Harry (after we blocked the PIN)** **d. Renew – originated by Susan** **j) We could click into any of these to learn more detail of each executed workflow**	
Susan Retires Derek's Smart Card **a) Susan clicks on the "Retire this smart card" link** **b) Click on the Next button** **c) Observe the retire confirmation then click on the main page button**	
Review **a) Susan clicks on the "Find a user to view or manage their information link" and then searches for Derek** **b) No smart card information is presented**	

c) Select Retired from the profile status left column **d) We can now see the operations which have been performed on the card and information about certificates which were installed during the card's lifetime**	