

## **CAC for a Mac**

### **Using an Intel-based Apple OS X System to Access NMCI Outlook Web Access (OWA)**

## Change History

<b>Date Published/ Revised</b>	<b>Version No.</b>	<b>Author or Point of Contact</b>	<b>Section / Description of Change</b>
09/17/08	1.0	Tom Garity	Initial version.
10/08/08	1.1	Tom Garity	Corrected typographical and formatting errors.
10/23/08	1.2	Tom Garity	Updated for OS X 10.5.5 and Smart Card Services Update 1.2.

## Contents

<b>1. INTRODUCTION .....</b>	<b>1</b>
1.1 Use at Your Own Risk .....	1
1.2 Required Items and Software .....	1
<b>2. INSTALLATION PREPARATION.....</b>	<b>3</b>
2.1 Verify OS X Version .....	4
2.2 Verify SCR331 Firmware Version .....	5
<b>3. INSTALLATION PROCEDURES .....</b>	<b>7</b>
3.1 Install Apple Smart Card Services Update .....	7
3.2 Import CAC Intermediate Certificates.....	10
3.3 Determine Correct Link Based on Domain .....	15
3.4 Create an Identity Preference.....	16
<b>APPENDIX A: SCR331 FIRMWARE UPDATE PROCEDURE .....</b>	<b>19</b>
<b>APPENDIX B: UNINSTALL SMART CARD SERVICES UPDATE .....</b>	<b>29</b>
<b>APPENDIX C: DETERMINE DOMAIN AND URL.....</b>	<b>30</b>
<b>APPENDIX D: FREQUENTLY ASKED QUESTIONS .....</b>	<b>36</b>

## Tables

Table 1: Preparation Instructions .....	3
Table 2: Verify OS X Version .....	4
Table 3: Verify SCR331 Firmware Version .....	5
Table 4: Install Apple Smart Card Services.....	7
Table 5: Import CAC Intermediate Certificates.....	10
Table 6: NMCI Outlook Web Access URL Links.....	15
Table 7: Create an Identity Preference.....	16
Table 8: Download Drivers and Firmware .....	19
Table 9: Install SCR331 Drivers.....	20
Table 10: Update SCR331 Firmware.....	23
Table 11: Uninstall Smart Card Services Update .....	29
Table 12: NMCI Domains .....	30
Table 13: Determining User's Domain on Windows 2000 .....	31
Table 14: Determine My NMCI Domain in Windows XP .....	32
Table 15: NMCI Outlook Web Access URL Links.....	34

## 1. INTRODUCTION

CAC for a Mac is the ability to use a Department of Defense (DoD) common access card (CAC) on Apple Macintosh computers to access Web sites that require DoD certificate authentication. It was written to allow Navy Marine Corps Intranet (NMCI) users to access their NMCI e-mail using the NMCI Microsoft Outlook Web Access (OWA) portal. Access to other sites is possible; however, the required steps are not addressed in this document.

### 1.1 Use at Your Own Risk

These instructions comprise several steps, which are described in sufficient detail to be understandable by a casual user. EDS is not responsible for any loss of use as a result of installing the software or making the configuration changes discussed in this document.

### 1.2 Required Items and Software

This section describes the hardware and software needed to access NMCI Exchange e-mail via OWA with a Macintosh operating system (OS) X system.

- An Intel-based Apple Macintosh computer running OS X 10.5.1 or higher. (See Note 1.)
- Apple Smart Card Services Update, version 1.2. (See Note 2.) It can be downloaded from the following location:  
<http://idisk.mac.com/dp.hayes-Public/Smart Card Services Update v1.2.pkg.zip>
- A valid DoD CAC.
- An SCM Micro Model SCR331 universal serial bus (USB) Smart Card Reader with Firmware, version 5.25 or later. (See Note 3.)
- Administrative access to a computer running Microsoft Windows XP (WXP) OS is required if the SCR331 USB Smart Card Reader Firmware requires updating.

**Note: 1.** This document has been tested only on Intel-based systems running Apple OS X version 10.5.4 and 10.5.5 however it should be applicable to G4 and G5 PPC-based Apple systems. Steps to update the OS X OS are included in this document.

**Note: 2.** Apple Smart Card Services Update, version 1.2 is for PPC and Intel-based Apple computers running Mac OS X version 10.5.4 or 10.5.5. The Smart Card Services Update, version 1.2 package is an update of the version 1.1 Intel-only patch which contained some components that were not universal and were *only* valid for Intel-based systems. This means that anyone with a PowerPC (PPC)-based system or an Intel-based Apple running Mac OS X 10.5.5 should not install version 1.1 of the Smart Card Services Update. Appendix B, Uninstall Smart Card Services Update, provides the uninstall procedure to remove Smart Card Services Update version 1.1, if necessary.

**Note: 3.** This document was written using the SCR331 USB Smart Card Reader. Several other brands and models of Smart Card Readers are supported by Apple, however they have not been tested using this procedure. SCR331 USB Smart Card Readers with Firmware version of 2.00 or higher can be updated to version 5.25. Steps for updating the SCR331 USB Smart Card Reader Firmware are provided in Appendix A,

**Note:** This completes the setup procedure.

**Note:** SCR331 Firmware Update Procedure.

## 2. INSTALLATION PREPARATION

Table 1 lists the steps to prepare to install this solution.



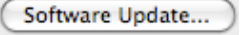
**Table 1: Preparation Instructions**

	<b>Step No.</b>	<b>Action</b>
	1.	Ensure the SCR331 USB Smart Card Reader is connected to the Macintosh.
	2.	Power on the Macintosh computer and log in with an account that has administrative privileges.

## 2.1 Verify OS X Version

Table 2 lists the steps to verify the Macintosh computer’s OS is at the required patch level.



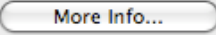
**Table 2: Verify OS X Version**

Step No.	Action
1.	<p>From the Apple  Menu, click <b>About This Mac</b>. The <b>About This Mac</b> window appears:</p>  <p>The second line displays the OS version number. Verify it is <b>10.5.4 or higher</b>.</p>
2.	<p>If not, update the OS by clicking  and follow the prompts. Note that some OS patches may require restarting the computer.</p>
3.	<p>Repeat as required to bring the OS version up to 10.5.4 or higher. Version 10.5.5 is preferred do to other updates provided.</p>

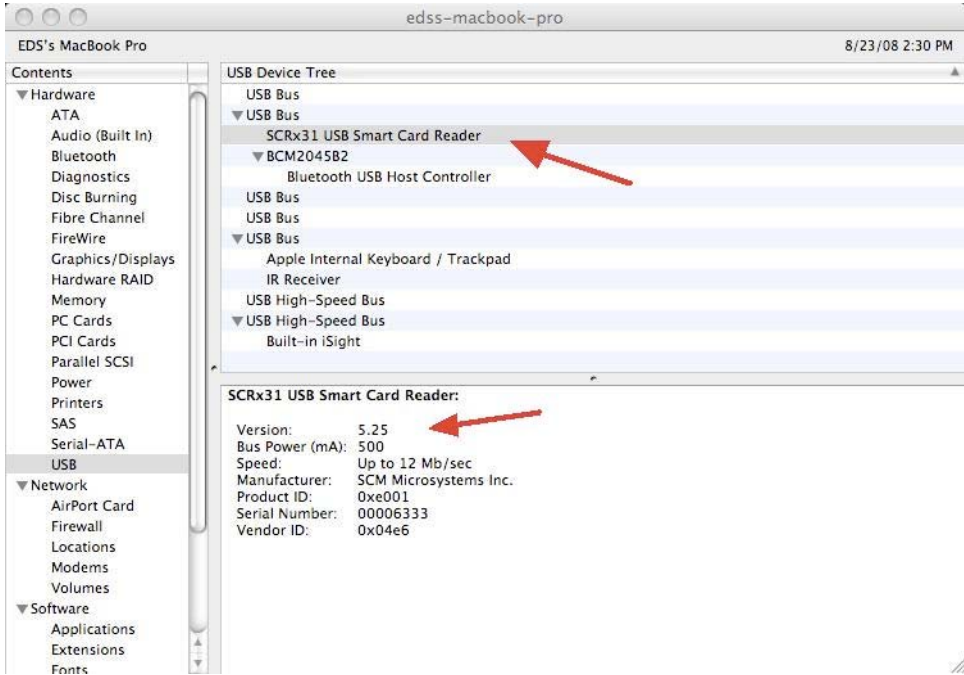
## 2.2 Verify SCR331 Firmware Version

Table 3 lists the steps to verify the SCR331 USB Smart Card Reader Firmware version.

**Table 3: Verify SCR331 Firmware Version**

Step No.	Action
1.	<p>If required, from the Apple  Menu, click <b>About This Mac</b>. The <b>About This Mac</b> window appears:</p> 
2.	<p>Click . The <b>System Profiler</b> window appears.</p>



Step No.	Action
3.	<p>In the left pane, under <b>Hardware</b>, click <b>USB</b>.</p>  <p><b>Note:</b> If the version displayed is not <b>5.25 or higher</b>, use the procedure in Appendix A,</p> <p><b>Note:</b> This completes the setup procedure.</p> <p><b>Note:</b> SCR331 Firmware Update Procedure, to upgrade the SCR331 USB Smart Card Reader's Firmware.</p>
4.	Close the System Profiler by clicking <b>System Profiler – Quit</b> in the Main Menu.

### 3. INSTALLATION PROCEDURES


This section describes the installations procedures.

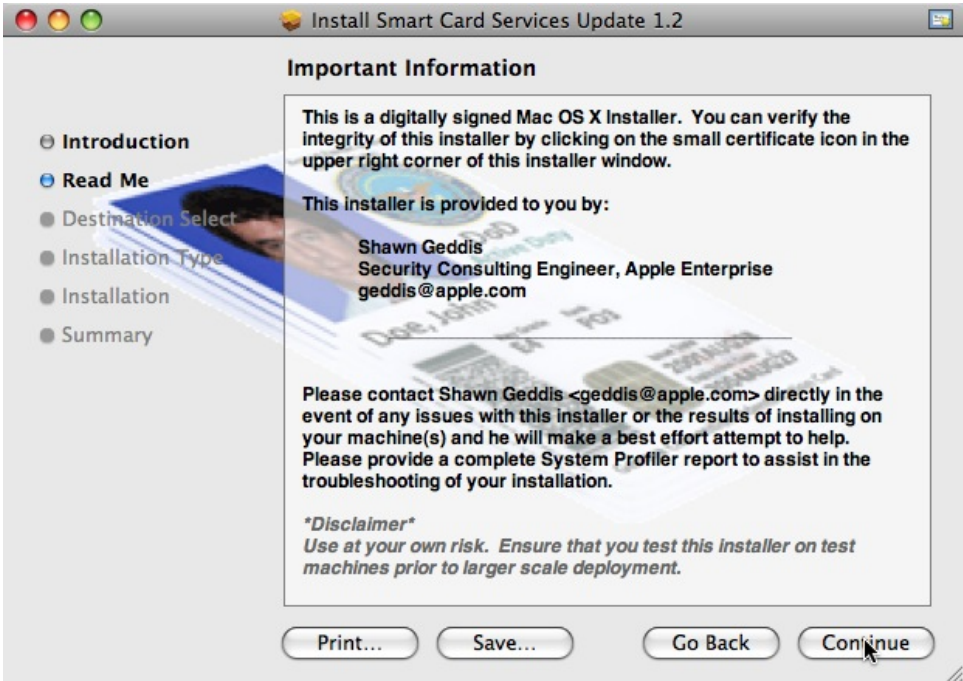
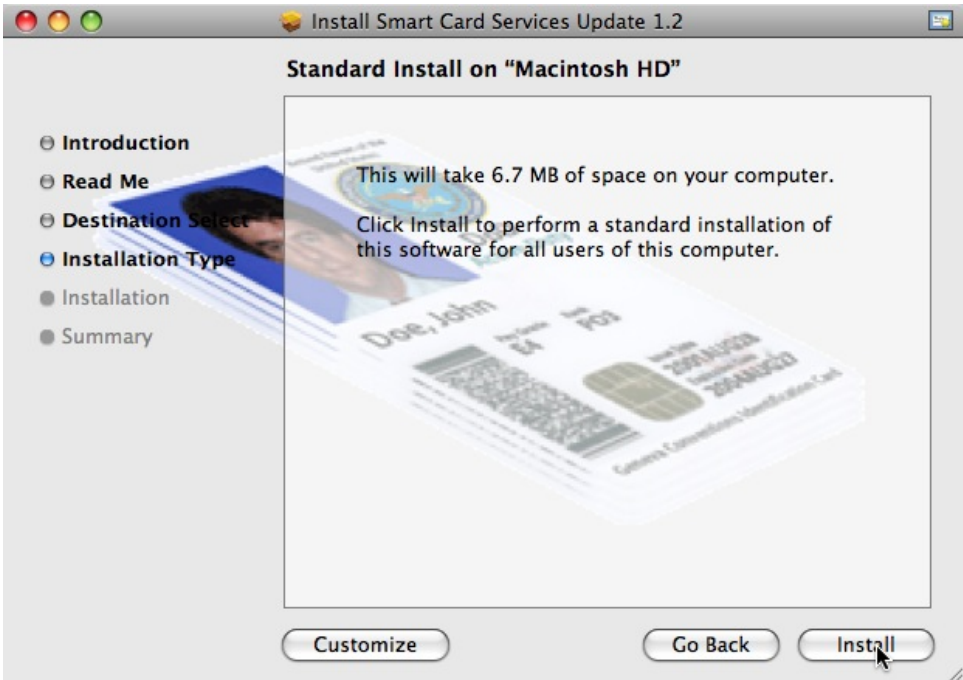
#### 3.1 Install Apple Smart Card Services Update

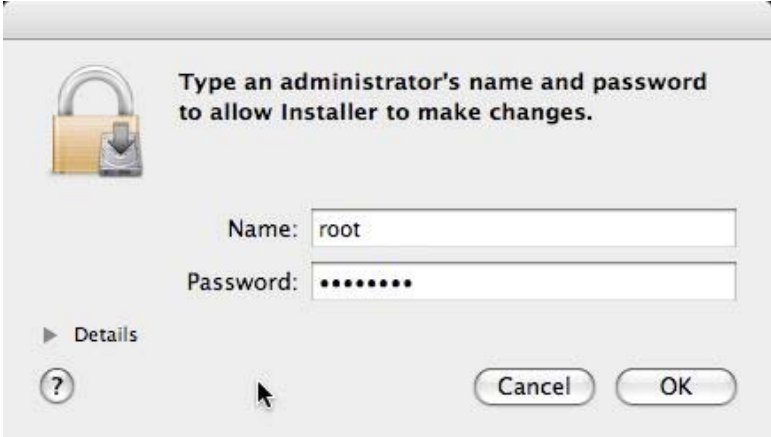

An update to the Apple OS X OS is required to allow DoD CAC certificates to function correctly. Table 4 lists the steps to install this solution.



**Note:** The Apple Smart Card Services Update v1.2 can be applied before or after upgrading to Mac OS X 10.5.5, however the OS must be at version 10.5.4 for it to install successfully.

**Table 4: Install Apple Smart Card Services**

No.	Prerequisite
1.	Download the Apple Smart Card Services Update from the following Uniform Resource Locator (URL): <a href="http://idisk.mac.com/dp.hayes-Public/Smart Card Services Update v1.2.pkg.zip">http://idisk.mac.com/dp.hayes-Public/Smart Card Services Update v1.2.pkg.zip</a>
2.	The patch should automatically run. If it does not, open the <b>Downloads</b> folder and double-click the file.
3.	<p>The <b>Welcome to the Smart Card Services Update 1.2 Installer</b> window appears:</p> 

No.	Prerequisite
4.	<p>Click <b>Continue</b>. The <b>Important Information</b> window appears:</p> 
5.	<p>Click <b>Continue</b>. The <b>Standard Install on Macintosh HD</b> window appears:  <b>Note:</b> If more than one OS X drive exists, an additional step may be required to select the Install drive.</p> 
6.	Click <b>Install</b> .

No.	Prerequisite
7.	<p>The <b>Administrative Permissions Request</b> window appears: Administrative permissions are required to install the update.</p> 
8.	<p>Enter an administrator user name and password and click <b>OK</b>. A <b>Restart Warning</b> window appears:</p> 
9.	<p>Click <b>Continue Installation</b>. The <b>Installation completed successfully</b> window appears:</p>


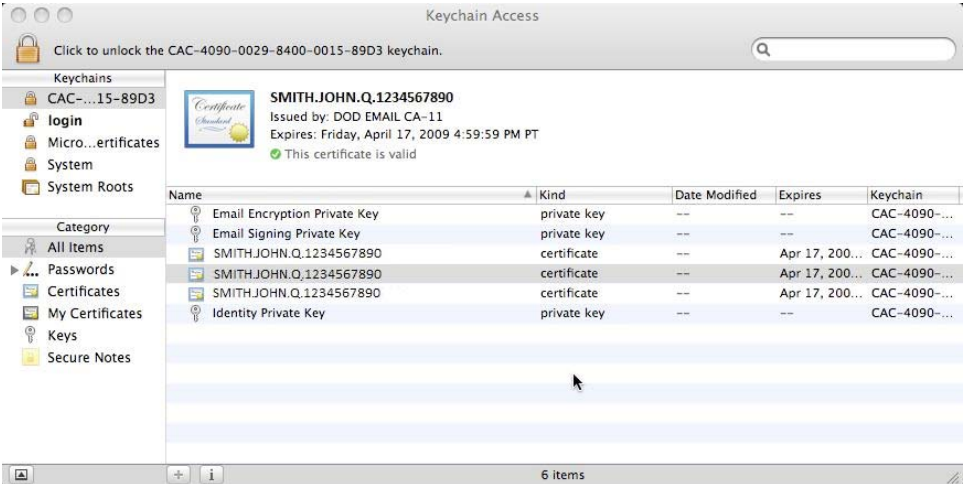
No.	Prerequisite
	
10.	<p>Save any work in progress and restart the computer by clicking <b>Restart</b>. After the computer restarts, log back in with the same username. There should be a new folder on the desktop named <b>SmartCardServices-Backup-[9E17]</b> (if OS version is 10.5.4) or <b>SmartCardServices-Backup-[9F33]</b> (if OS version is 10.5.5).</p> <div style="text-align: center;">  <p>SmartCardServices-Backup-[9E17]      or      SmartCardServices-Backup-[9F33]</p> </div> <p><b>Note:</b> The four characters between the square brackets may be different if the OS is patched higher than 10.5.4 or 10.5.5.</p>

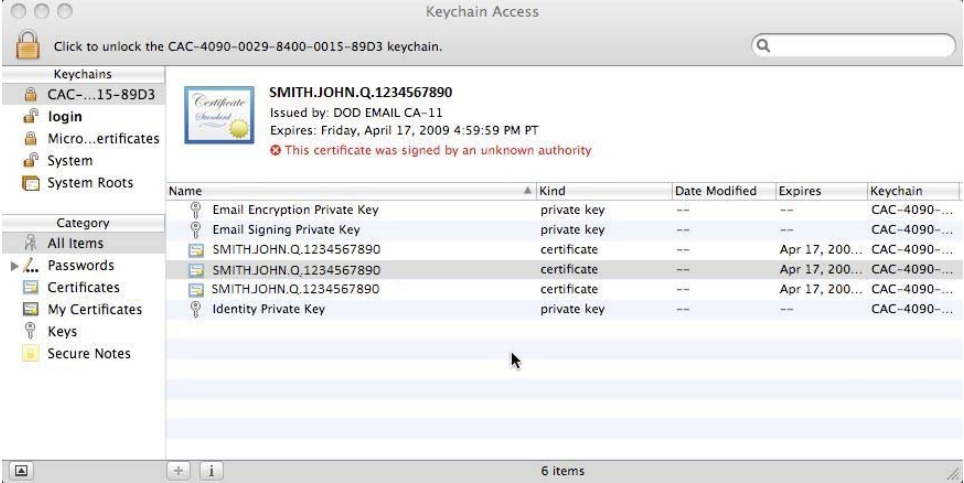

### 3.2 Import CAC Intermediate Certificates


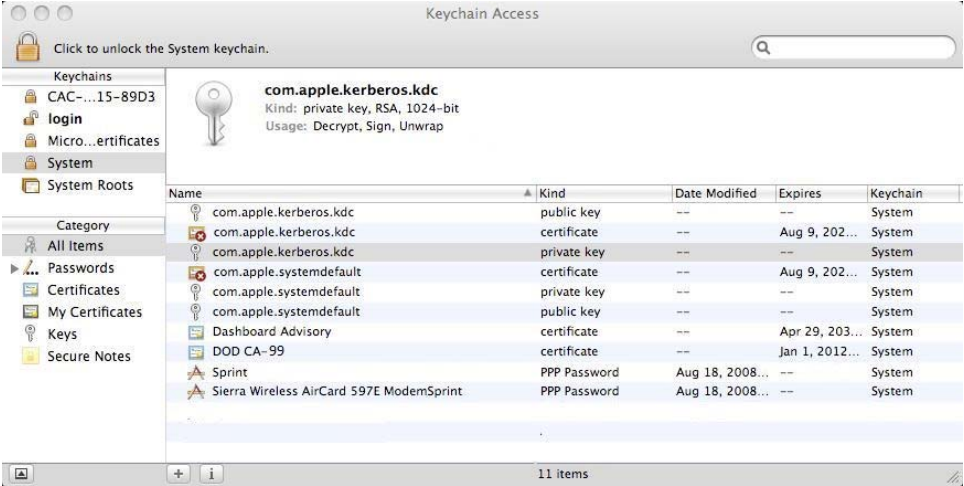
Table 5 lists the steps to import the required DoD intermediate certificates and validate the CAC certificates.

**Table 5: Import CAC Intermediate Certificates**


Step No.	Action
1.	Open the <b>Utilities</b> folder and double-click <b>Keychain Access</b> .

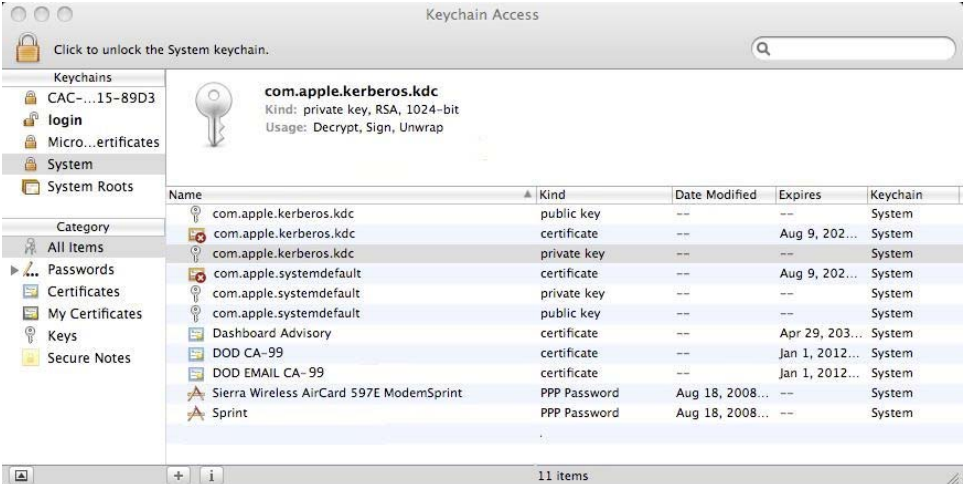
Step No.	Action
2.	Insert the CAC into the SCR331.
3.	In the <b>Keychains</b> (upper-left) panel of the Keychain Access utility, a new entry appears labeled <b>CAC-####-####-####-####-####</b> , where <b>####-####-####-####-####</b> is a unique number. Select this Keychain.
4.	<p>The contents of the CAC keychain display. Three certificates appear, one issued from a DOD Certificate Authority (CA) and two issued from a DOD E-MAIL CA:</p> 
5.	<p>In the right pane, click the first DoD certificate. The certificate Name, Issuer, and Expiration Date displays at the top in the right pane. If <b>This certificate is valid</b> displays in green, proceed to step 12.</p> 

Step No.	Action																																			
6.	<p>If <b>This certificate</b> was signed by an unknown authority displays in red, double-click it (or click <b>File - Get Info</b>).</p>  <p>The screenshot shows the Keychain Access application window. The left sidebar shows a tree view with 'Certificates' selected. The main pane displays a list of items in a table:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Kind</th> <th>Date Modified</th> <th>Expires</th> <th>Keychain</th> </tr> </thead> <tbody> <tr> <td>Email Encryption Private Key</td> <td>private key</td> <td>--</td> <td>--</td> <td>CAC-4090-...</td> </tr> <tr> <td>Email Signing Private Key</td> <td>private key</td> <td>--</td> <td>--</td> <td>CAC-4090-...</td> </tr> <tr> <td>SMITH.JOHN.Q.1234567890</td> <td>certificate</td> <td>--</td> <td>Apr 17, 200...</td> <td>CAC-4090-...</td> </tr> <tr> <td>SMITH.JOHN.Q.1234567890</td> <td>certificate</td> <td>--</td> <td>Apr 17, 200...</td> <td>CAC-4090-...</td> </tr> <tr> <td>SMITH.JOHN.Q.1234567890</td> <td>certificate</td> <td>--</td> <td>Apr 17, 200...</td> <td>CAC-4090-...</td> </tr> <tr> <td>Identity Private Key</td> <td>private key</td> <td>--</td> <td>--</td> <td>CAC-4090-...</td> </tr> </tbody> </table>	Name	Kind	Date Modified	Expires	Keychain	Email Encryption Private Key	private key	--	--	CAC-4090-...	Email Signing Private Key	private key	--	--	CAC-4090-...	SMITH.JOHN.Q.1234567890	certificate	--	Apr 17, 200...	CAC-4090-...	SMITH.JOHN.Q.1234567890	certificate	--	Apr 17, 200...	CAC-4090-...	SMITH.JOHN.Q.1234567890	certificate	--	Apr 17, 200...	CAC-4090-...	Identity Private Key	private key	--	--	CAC-4090-...
Name	Kind	Date Modified	Expires	Keychain																																
Email Encryption Private Key	private key	--	--	CAC-4090-...																																
Email Signing Private Key	private key	--	--	CAC-4090-...																																
SMITH.JOHN.Q.1234567890	certificate	--	Apr 17, 200...	CAC-4090-...																																
SMITH.JOHN.Q.1234567890	certificate	--	Apr 17, 200...	CAC-4090-...																																
SMITH.JOHN.Q.1234567890	certificate	--	Apr 17, 200...	CAC-4090-...																																
Identity Private Key	private key	--	--	CAC-4090-...																																
7.	<p>The <b>Certificate Information</b> window appears:</p>  <p>The Certificate Information window displays the following details:</p> <ul style="list-style-type: none"> <li><b>Trust</b> (expanded)</li> <li><b>Details</b> (expanded)             <ul style="list-style-type: none"> <li>Subject Name: _____</li> <li>Country: US</li> <li>Organization: U.S. Government</li> <li>Organizational Unit: DoD</li> <li>Extension: Certificate Authority Information Access ( 1 3 6 1 5 5 7 1 1 )</li> <li>Critical: NO</li> <li>Method #1: CA Issuers ( 1 3 6 1 5 5 7 4 8 2 )                     <ul style="list-style-type: none"> <li>URI: <a href="http://crl.chamb.disa.mil/getsig?DOD EMAIL CA-99">http://crl.chamb.disa.mil/getsig?DOD EMAIL CA-99</a></li> </ul> </li> <li>Method #2: Online Certificate Status Protocol ( 1 3 6 1 5 5 7 4 8 1 )                     <ul style="list-style-type: none"> <li>URI: <a href="http://ocsp.disa.mil">http://ocsp.disa.mil</a></li> </ul> </li> <li>Fingerprints:                     <ul style="list-style-type: none"> <li>SHA1: A4 A4 E1 C7 11 E1 78 DC 8C B9 19 0B ED AD 54 03 69 4A 0B 45</li> <li>MD5: EE F8 E7 42 BB 8D 3A 45 50 52 E0 9A 88 88 E7 00</li> </ul> </li> </ul> </li> </ul>																																			

Step No.	Action																																																							
8.	<p>Scroll down to the Extension section labeled <b>Certificate Authority Information Access</b> and click the link just below <b>Method #1</b> (Example: <a href="http://crl.chamb.disa.mil/getsign?DOD%20CA-99">http://crl.chamb.disa.mil/getsign?DOD%20CA-99</a>). The CA certificate downloads to the <b>Downloads</b> folder.</p> <p><b>Note:</b> Throughout this document, CA-99 is used to identify the specific CA the CAC was issued from. Replace CA-99 with the appropriate number for your CAC when following these instructions.</p>																																																							
9.	Close the <b>Certificate Information</b> window.																																																							
10.	<p>Open the <b>Downloads</b> folder and double-click the <b>DODCA-99.cer</b> file. The <b>Add Certificates</b> window appears:</p> 																																																							
11.	<p>Set the Keychain field to <b>System</b> and click <b>OK</b>. If required, enter the administrator user name and password and click <b>OK</b>. The <b>DOD CA-99</b> certificate appears under <b>System</b> in the <b>Keychain Access</b> window.</p>  <table border="1" data-bbox="570 1549 1365 1766"> <thead> <tr> <th>Name</th> <th>Kind</th> <th>Date Modified</th> <th>Expires</th> <th>Keychain</th> </tr> </thead> <tbody> <tr> <td>com.apple.kerberos.kdc</td> <td>public key</td> <td>--</td> <td>--</td> <td>System</td> </tr> <tr> <td>com.apple.kerberos.kdc</td> <td>certificate</td> <td>--</td> <td>Aug 9, 202...</td> <td>System</td> </tr> <tr> <td>com.apple.kerberos.kdc</td> <td>private key</td> <td>--</td> <td>--</td> <td>System</td> </tr> <tr> <td>com.apple.systemdefault</td> <td>certificate</td> <td>--</td> <td>Aug 9, 202...</td> <td>System</td> </tr> <tr> <td>com.apple.systemdefault</td> <td>private key</td> <td>--</td> <td>--</td> <td>System</td> </tr> <tr> <td>com.apple.systemdefault</td> <td>public key</td> <td>--</td> <td>--</td> <td>System</td> </tr> <tr> <td>Dashboard Advisory</td> <td>certificate</td> <td>--</td> <td>Apr 29, 203...</td> <td>System</td> </tr> <tr> <td>DOD CA-99</td> <td>certificate</td> <td>--</td> <td>Jan 1, 2012...</td> <td>System</td> </tr> <tr> <td>Sprint</td> <td>PPP Password</td> <td>Aug 18, 2008...</td> <td>--</td> <td>System</td> </tr> <tr> <td>Sierra Wireless AirCard 597E ModemSprint</td> <td>PPP Password</td> <td>Aug 18, 2008...</td> <td>--</td> <td>System</td> </tr> </tbody> </table>	Name	Kind	Date Modified	Expires	Keychain	com.apple.kerberos.kdc	public key	--	--	System	com.apple.kerberos.kdc	certificate	--	Aug 9, 202...	System	com.apple.kerberos.kdc	private key	--	--	System	com.apple.systemdefault	certificate	--	Aug 9, 202...	System	com.apple.systemdefault	private key	--	--	System	com.apple.systemdefault	public key	--	--	System	Dashboard Advisory	certificate	--	Apr 29, 203...	System	DOD CA-99	certificate	--	Jan 1, 2012...	System	Sprint	PPP Password	Aug 18, 2008...	--	System	Sierra Wireless AirCard 597E ModemSprint	PPP Password	Aug 18, 2008...	--	System
Name	Kind	Date Modified	Expires	Keychain																																																				
com.apple.kerberos.kdc	public key	--	--	System																																																				
com.apple.kerberos.kdc	certificate	--	Aug 9, 202...	System																																																				
com.apple.kerberos.kdc	private key	--	--	System																																																				
com.apple.systemdefault	certificate	--	Aug 9, 202...	System																																																				
com.apple.systemdefault	private key	--	--	System																																																				
com.apple.systemdefault	public key	--	--	System																																																				
Dashboard Advisory	certificate	--	Apr 29, 203...	System																																																				
DOD CA-99	certificate	--	Jan 1, 2012...	System																																																				
Sprint	PPP Password	Aug 18, 2008...	--	System																																																				
Sierra Wireless AirCard 597E ModemSprint	PPP Password	Aug 18, 2008...	--	System																																																				



Step No.	Action
12.	In the right pane, select the second (DOD E-MAIL) certificate. The certificate Name, Issuer, and Expiration Date displays at the top in the right pane.
13.	If <b>This certificate is valid</b> displays in green, proceed to Section 3.3 Determine Correct Link Based on Domain.
14.	If <b>This certificate was signed by an unknown authority</b> displays in red, double-click it (or click <b>File - Get Info</b> ). The <b>Certificate Information</b> window appears.
15.	Scroll down to the Extension Section labeled <b>Certificate Authority Information Access</b> and click the link just below <b>Method #1</b> (Example: <i>http://crl.chamb.disa.mil/getsig?DOD%20EMAIL%20CA-99</i> ). The CA certificate downloads to the Download folder.
16.	Close the <b>Certificate Information</b> window.
17.	<p>Open the <b>Downloads</b> folder and double-click the <b>DOD EMAIL CA-99.cer</b> file. The <b>Add Certificates</b> window displays.</p> 

Step No.	Action
18.	<p>Set the Keychain field to <b>System</b> and click <b>OK</b>. If required, enter an administrator user name and password and click <b>OK</b>. The <b>DOD EMAIL CA-99</b> certificate appears under <b>System</b> in the <b>Keychain Access</b> window.</p> 

### 3.3 Determine Correct Link Based on Domain

There are different Uniform Resource Locator (URL) entries for accessing NMCI Outlook Web Access depending on the user’s Active Directory domain. The correct URL to use is based on the user’s domain and whether the user is exempted from Cryptographic Log On (CLO). You need to know the domain your user account is located in to determine the correct URL to use. See APPENDIX C: Determine Domain if you do not know how to determine the domain of your user account.

Table 6 identifies the domains and Uniform Resource Locator (URL) link a user of that domain must use to access NMCI Outlook Web Access.

**Note:** Users who are CLO Exempt access NMCI Outlook Web Access using a different URL than others in the same domain.

**Table 6: NMCI Outlook Web Access URL Links**

Domain	URL Link
<b>NMCI Navy Users</b>	
NADSUSEA	<a href="https://webmail.east.nmci.navy.mil">https://webmail.east.nmci.navy.mil</a>
NADSUSWE	<a href="https://webmail.west.nmci.navy.mil">https://webmail.west.nmci.navy.mil</a>
NMCI-ISF	<a href="https://webmail.isf.nmci.navy.mil">https://webmail.isf.nmci.navy.mil</a>
NADSUSEA/NADSUSWE/NMCI-ISF	<a href="https://webmail.exceptions.nmci.navy.mil">https://webmail.exceptions.nmci.navy.mil</a>

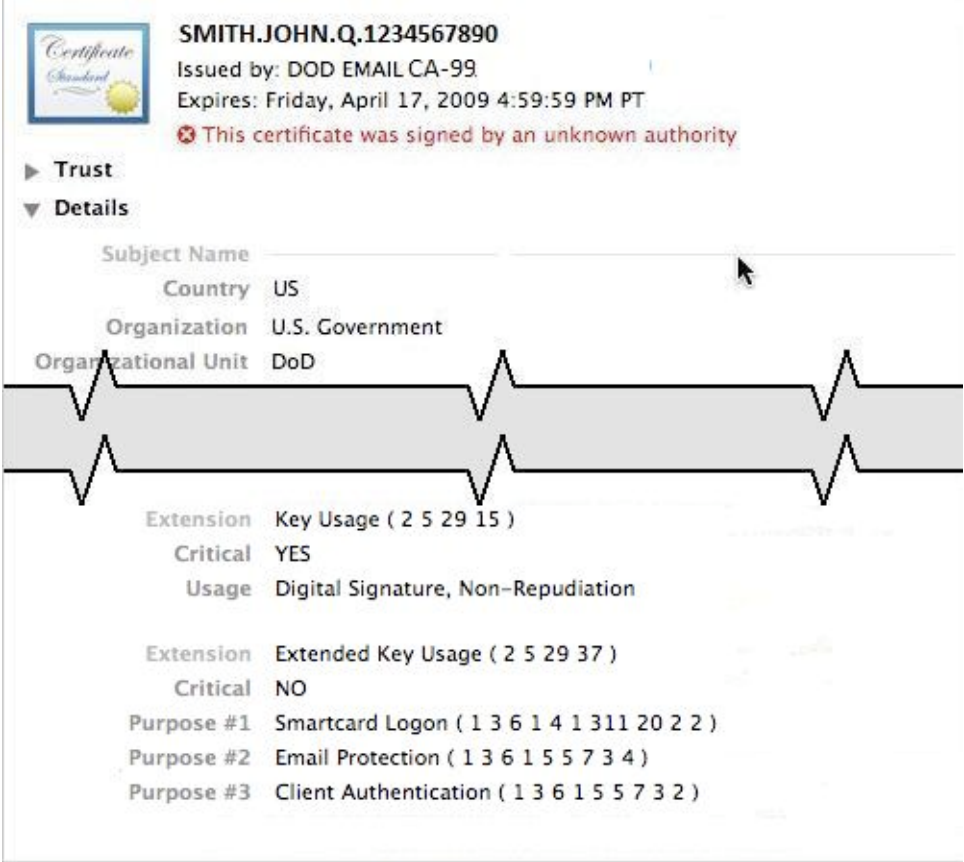
Domain	URL Link
(CLO Exception users)	
NADSUSEA NCIS COI	<a href="https://webmail.nmci.nmci.navy.mil">https://webmail.nmci.nmci.navy.mil</a>
NADSUSEA NCIS COI (CLO Exception users)	<a href="https://webmail.exceptions.ncis.nmci.navy.mil">https://webmail.exceptions.ncis.nmci.navy.mil</a>
PADS	<a href="https://webmail.pacom.mil">https://webmail.pacom.mil</a>
PADS (PACOM Single Mailbox Restore users and CLO Exception users)	<a href="https://webmail.exceptions.pacom.mil">https://webmail.exceptions.pacom.mil</a>
<b>NMCI Marine Corps Users</b>	
MCDSUS, MCDSJP and NMCI	<a href="https://webmail.nmci.usmc.mil">https://webmail.nmci.usmc.mil</a>

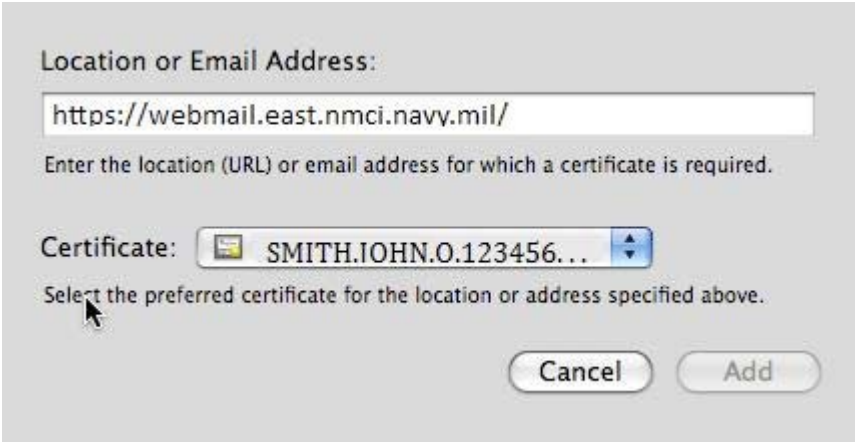
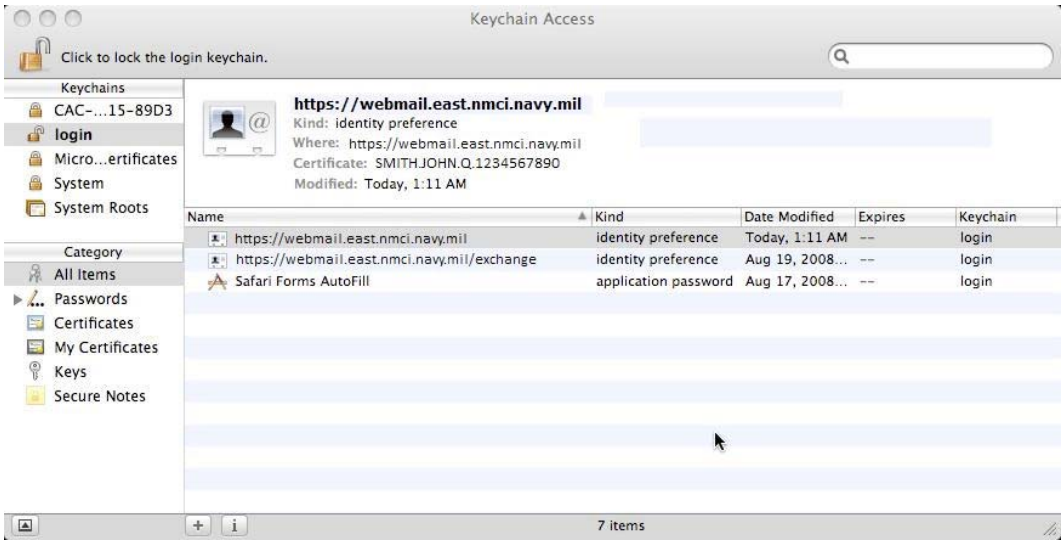
### 3.4 Create an Identity Preference

Table 7 lists the steps to create an Identity Preference. An Identity Preference is required when a Web server's security is set to optional, even if the Web site is set to required.

**Table 7: Create an Identity Preference**

Step No.	Action
1.	Click <b>CAC Keychain</b> under Keychains in the <b>Keychain Access</b> window.

Step No.	Action
2.	<p>Select the correct DOD E-MAIL certificate. The certificate that has a Key Usage of <b>Digital Signature, Non-Repudiation</b> (not Key Encipherment) and an Extended Key Usage of <b>Smartcard Logon, Email Protection, and Client Authentication</b> is required.</p>  <p><b>SMITH.JOHN.Q.1234567890</b>      Issued by: DOD EMAIL CA-99      Expires: Friday, April 17, 2009 4:59:59 PM PT      ⚠ This certificate was signed by an unknown authority</p> <p>► Trust      ▼ Details</p> <p>Subject Name _____      Country US      Organization U.S. Government      Organizational Unit DoD</p> <hr/> <p>Extension Key Usage ( 2 5 29 15 )      Critical YES      Usage Digital Signature, Non-Repudiation</p> <p>Extension Extended Key Usage ( 2 5 29 37 )      Critical NO      Purpose #1 Smartcard Logon ( 1 3 6 1 4 1 311 20 2 2 )      Purpose #2 Email Protection ( 1 3 6 1 5 5 7 3 4 )      Purpose #3 Client Authentication ( 1 3 6 1 5 5 7 3 2 )</p>

Step No.	Action																				
3.	<p>Use <b>Ctrl + click</b> to select <b>New Identity Presence</b>. Enter the appropriate URL determined in Section 3.3 above. In the case of the NADSUSEA user shown in the example below, the correct URL would be: <a href="https://webmail.east.nmci.navy.mil">https://webmail.east.nmci.navy.mil</a>.</p> 																				
4.	Click <b>Add</b> .																				
5.	<p>Select <b>login</b> under Keychains. The Identity Preference just created displays:</p>  <table border="1" data-bbox="537 1184 1409 1276"> <thead> <tr> <th>Name</th> <th>Kind</th> <th>Date Modified</th> <th>Expires</th> <th>Keychain</th> </tr> </thead> <tbody> <tr> <td>https://webmail.east.nmci.navy.mil</td> <td>identity preference</td> <td>Today, 1:11 AM</td> <td>--</td> <td>login</td> </tr> <tr> <td>https://webmail.east.nmci.navy.mil/exchange</td> <td>identity preference</td> <td>Aug 19, 2008...</td> <td>--</td> <td>login</td> </tr> <tr> <td>Safari Forms AutoFill</td> <td>application password</td> <td>Aug 17, 2008...</td> <td>--</td> <td>login</td> </tr> </tbody> </table>	Name	Kind	Date Modified	Expires	Keychain	https://webmail.east.nmci.navy.mil	identity preference	Today, 1:11 AM	--	login	https://webmail.east.nmci.navy.mil/exchange	identity preference	Aug 19, 2008...	--	login	Safari Forms AutoFill	application password	Aug 17, 2008...	--	login
Name	Kind	Date Modified	Expires	Keychain																	
https://webmail.east.nmci.navy.mil	identity preference	Today, 1:11 AM	--	login																	
https://webmail.east.nmci.navy.mil/exchange	identity preference	Aug 19, 2008...	--	login																	
Safari Forms AutoFill	application password	Aug 17, 2008...	--	login																	
6.	Repeat Steps 3 thru 5 using the same URL but adding <b>/exchange</b> to it. In the example above, it is shown as <a href="https://webmail.east.nmci.navy.mil/exchange">https://webmail.east.nmci.navy.mil/exchange</a> .																				

This completes the setup procedure.

## APPENDIX A: SCR331 FIRMWARE UPDATE PROCEDURE

The following three sections describe the procedure for downloading the drivers and firmware.

**Note:** The procedure must be performed on a computer running WXP or Windows 2000 (W2K) OS.

### Download Drivers and Firmware

Table 8 lists the steps to download the SCR331 USB Smart Card Reader drivers and Firmware update.

**Table 8: Download Drivers and Firmware**

Step No.	Action
1.	Create a folder on the desktop named <b>SCR331Temp</b> .
2.	Open a browser and go to <a href="http://www.scmmicro.com/support/pcs_downloads.php?lang=en">http://www.scmmicro.com/support/pcs_downloads.php?lang=en</a>
3.	In the middle of the window, click <b>Driver/Firmware</b> in the <b>Type</b> field.
4.	Click <b>SCR331/SCR531 CCID USB</b> in the <b>Smartcard Reader</b> field.
5.	Click <b>Windows(R) XP 32-bit</b> in the <b>OS</b> field.
6.	In the bottom of the window, ensure the <b>I read and accept the EULA</b> check box is selected and click <b>Next</b> .
7.	In the <b>SCR331/SCR531 CCID USB Firmware</b> section, download the <b>SCRx31CCID_fw525.zip</b> file by clicking <b>Download File</b> following the name. Save the file to the <b>SCR331Temp</b> folder just created on the Desktop.
8.	In the <b>SCR331/SCR531 CCID USB - Windows (R) XP 32-bit Driver/Installer</b> section, download the <b>SCR3xxx_4.31_4.41.zip</b> file by clicking <b>Download File</b> following the name. Save the file to the <b>SCR331Temp</b> folder just created on the Desktop.
9.	Close the browser.
10.	Expand <b>SCR331Temp\SCR3xxx_4.31_4.41.zip</b> and copy the <b>SCR3xxx_Drivers_Win2k_Win2003server_XP3264_Vista3264_V4.41</b> folder to the Desktop.
11.	Close <b>SCR3xxx_4.31_4.41.zip</b> .
12.	Expand <b>SCR331Temp\SCRx31CCID_fw5.25.zip</b> and copy the <b>SCRx31CCID_fw5.25</b> folder to the Desktop.
13.	Close <b>SCRx31CCID_fw5.25.zip</b> .
14.	Delete the <b>SCR331Temp</b> file.


### Install the SCR331 USB Smart Card Reader

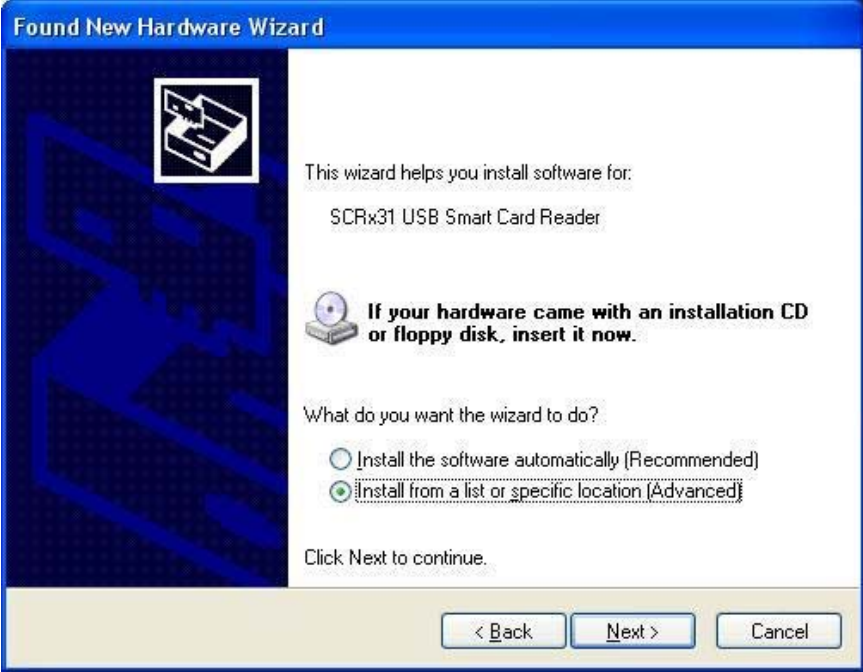
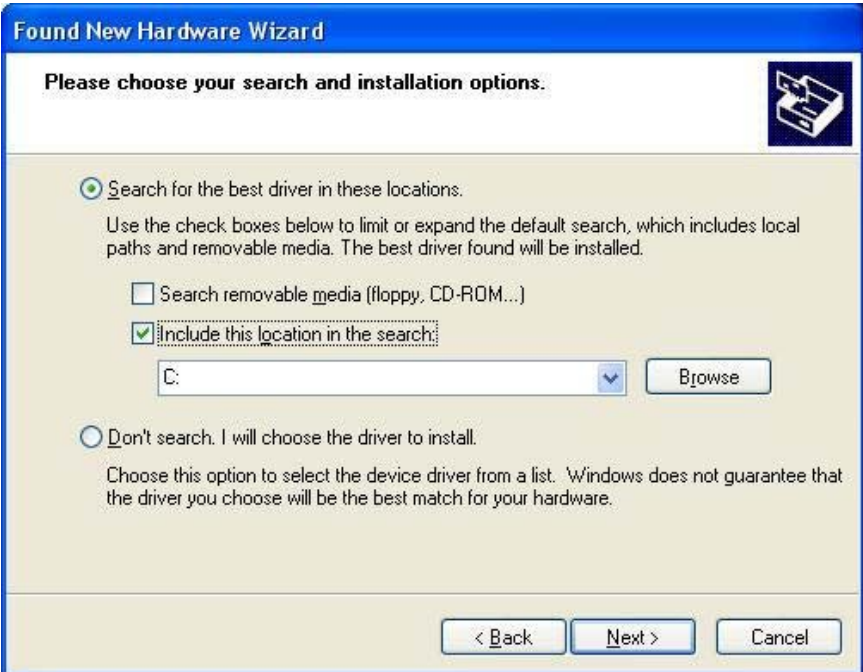
Table 9 lists the steps to install the SCR331 USB Smart Card Reader on a computer running WXP Professional or Home OS.

These steps only need to be completed *once*. If the SCR331 was previously installed on the Windows computer, proceed to Section 0,



**Note:** Update the Firmware.

**Table 9: Install SCR331 Drivers**

Step No.	Action
1.	<p>Plug the SCR331 reader into a USB port on the computer. The <b>New Hardware Wizard</b> starts if the device has not been connected before. Select the <b>No, not this time</b> option and click <b>Next</b>.</p> 

Step No.	Action
2.	<p>Ensure the <b>Install from a list or specific location (Advanced)</b> check box is selected and click <b>Next</b>.</p> 
3.	<p>Select the <b>Search for the best driver in these locations</b> option and check the <b>Include this location in the search box</b>. Click <b>Browse</b>.</p> 



Step No.	Action
4.	<p>Select the <b>SCR3xx_Drivers_Win2k_Win2003server_XP3264_Vista3264_v4.41</b> folder. Click <b>OK</b> to close the <b>Browse for Folder</b> window.</p> 
5.	<p>Click <b>Next</b>.</p> 

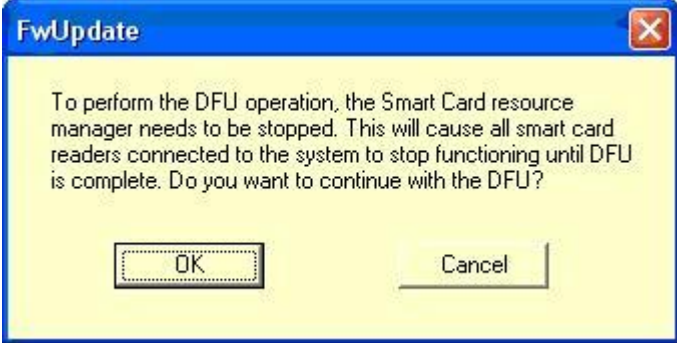
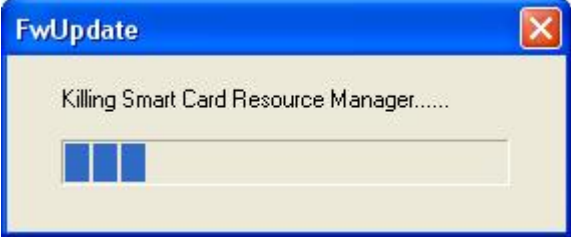
Step No.	Action
6.	<p>Click <b>Finish</b> to close the <b>New Hardware Wizard</b>.</p> 
7.	<p>The SCR331 drivers are now installed. Proceed to Section, 0, Update the Firmware.</p>


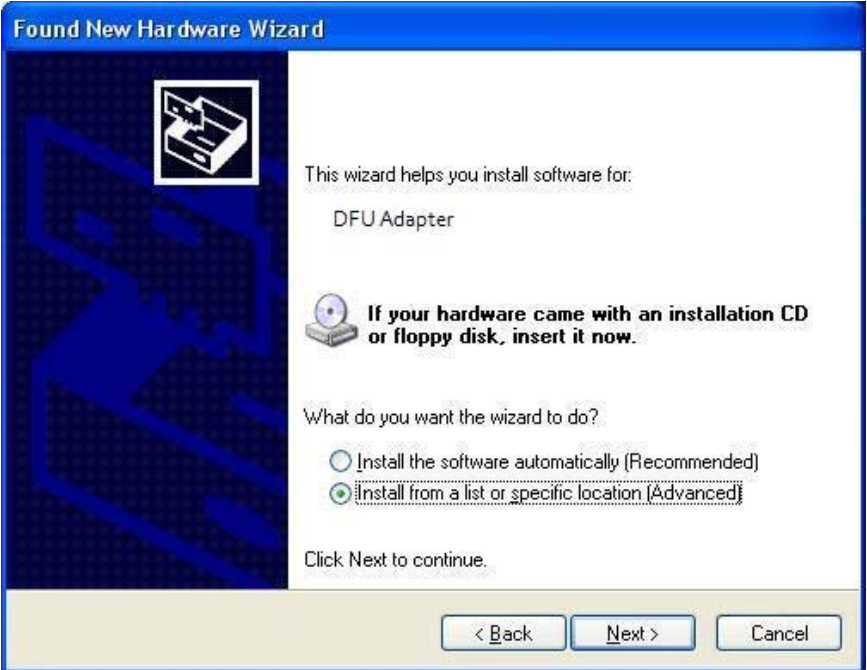
### Update the Firmware

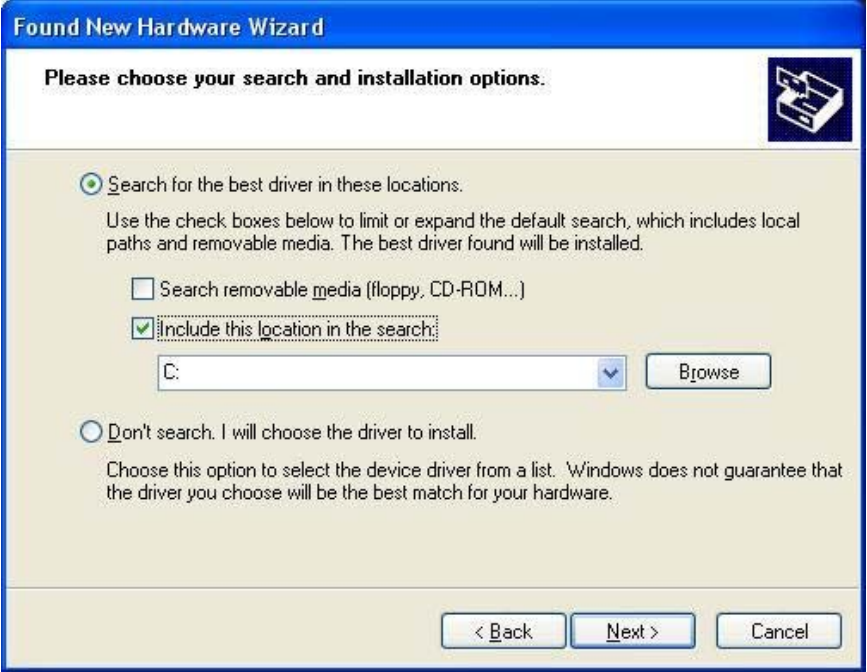
Table 10 lists the steps to update the SCR331 Firmware.



**Table 10: Update SCR331 Firmware**


Step No.	Action
1.	Open the <b>SCR331\FWUpdate</b> folder.

Step No.	Action
2.	<p>Run <b>FWUpdate.exe</b>. The <b>FwUpdate</b> window appears.</p> 
3.	<p>Click <b>OK</b>. A <b>Killing Smart Card Resource Manager</b> message appears showing that the Smart Card Resource Manager will be stopped.</p>  <p><b>Note:</b> This step may take a minute or more. When the Smart Card Resource Manager is stopped, a <b>New Hardware Found</b> message may appear. If it does not, proceed to step 9.</p>

Step No.	Action
4.	<p>The Found New Hardware Wizard will start if the Smart Card Device Firmware Update (DFU) Adapter drivers are not detected. If this occurs, select the <b>No, not this time</b> option and click <b>Next</b>.</p> 
5.	<p>Select the <b>Install from a list or specific location (Advanced)</b> option and click <b>Next</b>.</p> 

Step No.	Action
6.	<p>Select the <b>Search for the best driver in these locations</b> option and check the <b>Include this location in the search</b> box. Click <b>Browse</b>.</p> 

Step No.	Action
7.	<p>The <b>Browse for Folder</b> window appears, select the <b>SCRx31 CCID_fw5.25</b> folder. Click <b>OK</b> and <b>Next</b>.</p> 
8.	<p>Click <b>Finish</b> to close the <b>Found New Hardware Wizard</b> window.</p> 

Step No.	Action																								
9.	<p>The <b>Generic Device Firmware Upgrade Utility</b> window appears:</p>  <p>List of device parameters, their current value and their value after download are displayed. These are provided for user confirmation.</p> <table border="1" data-bbox="685 527 1279 783"> <thead> <tr> <th>Parameter</th> <th>Existing value</th> <th>New value</th> </tr> </thead> <tbody> <tr> <td>Download filename</td> <td>SCR531_V525...</td> <td></td> </tr> <tr> <td>Manufacturer</td> <td>SCM Microsysteme...</td> <td>SCM Microsysteme...</td> </tr> <tr> <td>Product</td> <td>SCRx31 USB S...</td> <td>SCRx31 USB S...</td> </tr> <tr> <td>Vendor ID</td> <td>04E6</td> <td>04E6</td> </tr> <tr> <td>Product ID</td> <td>E001</td> <td>E001</td> </tr> <tr> <td>Firmware Version</td> <td>04.13</td> <td>05.25</td> </tr> <tr> <td>Serial Number</td> <td>00006333</td> <td>00006333</td> </tr> </tbody> </table> <p>Close all applications that use the device and proceed further.</p> <p>FwUpdate <span style="float: right;">Finish Cancel</span></p>	Parameter	Existing value	New value	Download filename	SCR531_V525...		Manufacturer	SCM Microsysteme...	SCM Microsysteme...	Product	SCRx31 USB S...	SCRx31 USB S...	Vendor ID	04E6	04E6	Product ID	E001	E001	Firmware Version	04.13	05.25	Serial Number	00006333	00006333
Parameter	Existing value	New value																							
Download filename	SCR531_V525...																								
Manufacturer	SCM Microsysteme...	SCM Microsysteme...																							
Product	SCRx31 USB S...	SCRx31 USB S...																							
Vendor ID	04E6	04E6																							
Product ID	E001	E001																							
Firmware Version	04.13	05.25																							
Serial Number	00006333	00006333																							
10.	Click <b>Finish</b> .																								
11.	All steps requiring a computer running WXP OS have been completed. Shut down the computer and disconnect the SCR331.																								

## APPENDIX B: UNINSTALL SMART CARD SERVICES UPDATE

Table 11 lists the steps to uninstall Smart Card Services Update, version 1.1 from an Intel-based system running OS X version 10.5.4. The folder name in Step 4 and the version number in Step 5 may be different if uninstalling from a system running a higher version of OS X.

**Table 11: Uninstall Smart Card Services Update**

	<b>Step No.</b>	<b>Action</b>
	1.	Disconnect the Smart Card Reader from the Apple computer.
	2.	Restart the computer.
	3.	Log on to the computer with an administrative account.
	4.	Open the <b>SmartCardServices-Backup-[9E17]</b> folder and move the old components back to their respective locations.
	5.	Restart the computer. The system should be back to a working 10.5.4 configuration.



## APPENDIX C: DETERMINE DOMAIN AND URL

This appendix provides the steps necessary to determine the domain of your NMCI user account as well as the correct URL for accessing NMCI Outlook Web Access. Table 12 lists the domains and provides a brief description of them.

**Table 12: NMCI Domains**

Domain	Fully Qualified Domain Name (FQDN)	Description
<b>NMCI Navy Enclave</b>		
<b>NADSUSEA</b>	nadsusea.nads.navy.mil	(Naval Active Directory Services United States East) for Navy NMCI users east of the Mississippi River
<b>NADSUSWE</b>	nadsuswe.nads.navy.mil	(Naval Active Directory Services United States West) for Navy NMCI users west of the Mississippi River
<b>PACOM</b>	pacom.pads.navy.mil	(Pacific [Command] Active Directory Services) for Navy NMCI Pacific Command users
<b>NMCI-ISF</b>	nmci-isf.com	NMCI Administrative domain (Navy) for NMCI administrators in the Navy NMCI Active Directory forest
<b>NMCI Marine Corps Enclave</b>		
<b>MCDSUS</b>	mcdsus.mcds.usmc.mil	(Marine Corps Directory Services United States) for USMC NMCI users who are part of the continental United States and Hawaii
<b>MCDSJP</b>	mcdsjp.mcds.usmc.mil	(Marine Corps Directory Services Japan) for USmC NMCI users who are outside the continental United States
<b>NMCI</b>	nmci.mcds.usmc.mil	NMCI Administrative domain (USMC) for NMCI administrators in the USMC NMCI Active Directory forest

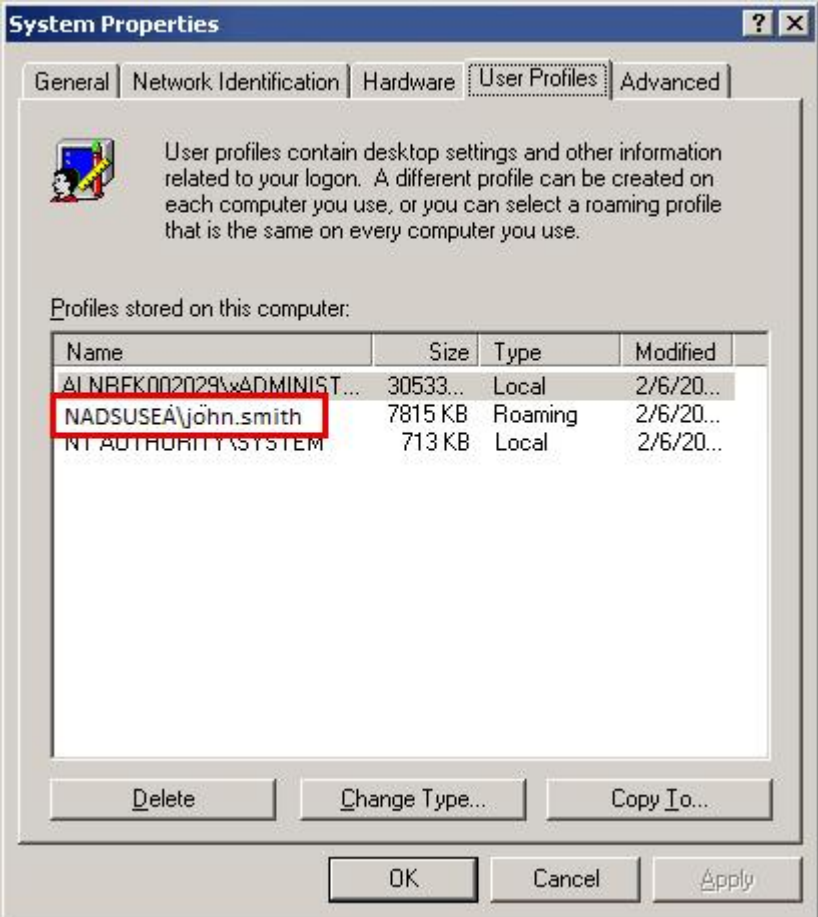
The procedure for determining your NMCI domain is slightly different depending on if you are using a NMCI Client Data seat running the Windows 2000 Professional Operating System or one running the Windows XP Professional Operating System.

### **Determine My NMCI Domain on a Windows 2000 NMCI Client Data seat**

Table 13 lists the steps to determine your User account's domain when logged onto a NMCI Client Data seat running the Windows 2000 Professional Operating System.

**Table 13: Determining User's Domain on Windows 2000**

<b>Step No.</b>	<b>Action</b>
1.	From your NMCI seat, right-click the <b>My Computer</b> icon, then select <b>Properties</b> .
2.	In the <i>System Properties</i> window, select the <b>User Profiles</b> tab.

		 <p>The screenshot shows the 'System Properties' dialog box with the 'User Profiles' tab selected. Below the introductory text, there is a table titled 'Profiles stored on this computer:' with the following data:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Size</th> <th>Type</th> <th>Modified</th> </tr> </thead> <tbody> <tr> <td>ALNRFK002029\ADMINIST...</td> <td>30533...</td> <td>Local</td> <td>2/6/20...</td> </tr> <tr> <td>NADSUSEA\john.smith</td> <td>7815 KB</td> <td>Roaming</td> <td>2/6/20...</td> </tr> <tr> <td>NT AUTHORITY\SYSTEM</td> <td>713 KB</td> <td>Local</td> <td>2/6/20...</td> </tr> </tbody> </table> <p>The 'NADSUSEA\john.smith' entry is highlighted with a red rectangular box.</p>	Name	Size	Type	Modified	ALNRFK002029\ADMINIST...	30533...	Local	2/6/20...	NADSUSEA\john.smith	7815 KB	Roaming	2/6/20...	NT AUTHORITY\SYSTEM	713 KB	Local	2/6/20...
Name	Size	Type	Modified															
ALNRFK002029\ADMINIST...	30533...	Local	2/6/20...															
NADSUSEA\john.smith	7815 KB	Roaming	2/6/20...															
NT AUTHORITY\SYSTEM	713 KB	Local	2/6/20...															
3.		Your <i>Domain</i> is listed in front of your user name under the <i>Name</i> heading.																
4.		Using the domain from Step 3, locate the correct URL in Table 15. CLO Exemption users have a different URL than CAC enforced users.																


**Determine My NMCI Domain on a Windows XP NMCI Client Data seat**

Table 14 lists the steps to determine your User account’s domain when logged onto a NMCI Client Data seat running the Windows XP Professional Operating System.

**Table 14: Determine My NMCI Domain in Windows XP**

Step No.	Action
1.	From your NMCI seat, right-click the <b>My Computer</b> icon, then select <b>Properties</b> .

	2.	In the <i>System Properties</i> window, select the <b>Advanced</b> tab.
	3.	Click <b>Settings</b> in the <i>User Profiles</i> section.
	4.	Your <i>Domain</i> is listed in front of your user name under the <i>Name</i> heading.

	
5.	Using the domain from Step 4, locate the correct URL in Table 15. CLO Exemption users have a different URL than CAC enforced users.

**Determine Correct NMCI Outlook Web Access URL**

Table 15 identifies the domains and Uniform Resource Locator (URL) link a user of that domain must use to access NMCI Outlook Web Access.

**Note:** Users who are CLO Exempt access NMCI Outlook Web Access using a different URL than others in the same domain.

**Table 15: NMCI Outlook Web Access URL Links**

Domain	URL Link
NADSUSEA	<a href="https://webmail.east.nmci.navy.mil">https://webmail.east.nmci.navy.mil</a>
NADSUSWE	<a href="https://webmail.west.nmci.navy.mil">https://webmail.west.nmci.navy.mil</a>
NMCI-ISF	<a href="https://webmail.isf.nmci.navy.mil">https://webmail.isf.nmci.navy.mil</a>
NADSUSEA/NADSUSWE/NMCI-ISF (CLO Exception users)	<a href="https://webmail.exceptions.nmci.navy.mil">https://webmail.exceptions.nmci.navy.mil</a>

<b>Domain</b>	<b>URL Link</b>
NADSUSEA NCIS COI	<a href="https://webmail.nmci.nmci.navy.mil">https://webmail.nmci.nmci.navy.mil</a>
NADSUSEA NCIS COI (CLO Exception users)	<a href="https://webmail.exceptions.ncis.nmci.navy.mil">https://webmail.exceptions.ncis.nmci.navy.mil</a>
PADS	<a href="https://webmail.pacom.mil">https://webmail.pacom.mil</a>
PADS (PACOM Single Mailbox Restore users and CLO Exception users)	<a href="https://webmail.exceptions.pacom.mil">https://webmail.exceptions.pacom.mil</a>

## APPENDIX D: FREQUENTLY ASKED QUESTIONS

**Q: What is needed to use my DoD Common Access Card (CAC) on an Apple computer to access my NMCI email?**

**A:** The following items are required to allow Outlook Web Access (OWA) to your NMCI email from an Apple computer:

- Apple computer running OS X version 10.5.4 or higher (Note: PPC-based Apple computers have not been tested with this solution.)
- Apple Smart Card Services Update v1.2 patch (Available from: [http://idisk.mac.com/dp.hayes-Public/Smart Card Services Update v1.2.pkg.zip](http://idisk.mac.com/dp.hayes-Public/Smart_Card_Services_Update_v1.2.pkg.zip))
- CAC For A Mac – Setup Instructions (Latest version available from: [http://idisk.mac.com/dp.hayes-Public/CAC\\_for\\_a\\_Mac\\_v1.2.doc](http://idisk.mac.com/dp.hayes-Public/CAC_for_a_Mac_v1.2.doc))
- SCR331 USB Smart Card Reader with Firmware version 5.25 or higher (Readers with Firmware version of 2.0 or higher can be updated to 5.25. If updating is necessary, the following additional items are also required:
  - Administrator access to a computer running Windows XP (Home or Professional)
  - Windows XP drivers for the SCR331 USB Smart Card Reader SCR3xxx\_4.31\_4.41.zip (Available from: [http://idisk.mac.com/dp.hayes-Public/SCR3xxx\\_4.31\\_4.41.zip](http://idisk.mac.com/dp.hayes-Public/SCR3xxx_4.31_4.41.zip))
  - SCR331 Firmware update SCR331CCID\_fw5.25.zip (Available from: [http://idisk.mac.com/dp.hayes-Public/SCR331CCID\\_fw5.25.zip](http://idisk.mac.com/dp.hayes-Public/SCR331CCID_fw5.25.zip))

**Q: Where can I obtain the necessary files?**

**A:** The SCR331 drivers and Firmware can be obtained from the SCM Micro website at:

[http://www.scmmicro.com/support/pcs\\_downloads.php?lang=en](http://www.scmmicro.com/support/pcs_downloads.php?lang=en)

The Apple Smart Card Services Update v1.2 can be obtained from:

[http://idisk.mac.com/dp.hayes-Public/Smart Card Services Update v1.2.pkg.zip](http://idisk.mac.com/dp.hayes-Public/Smart_Card_Services_Update_v1.2.pkg.zip)

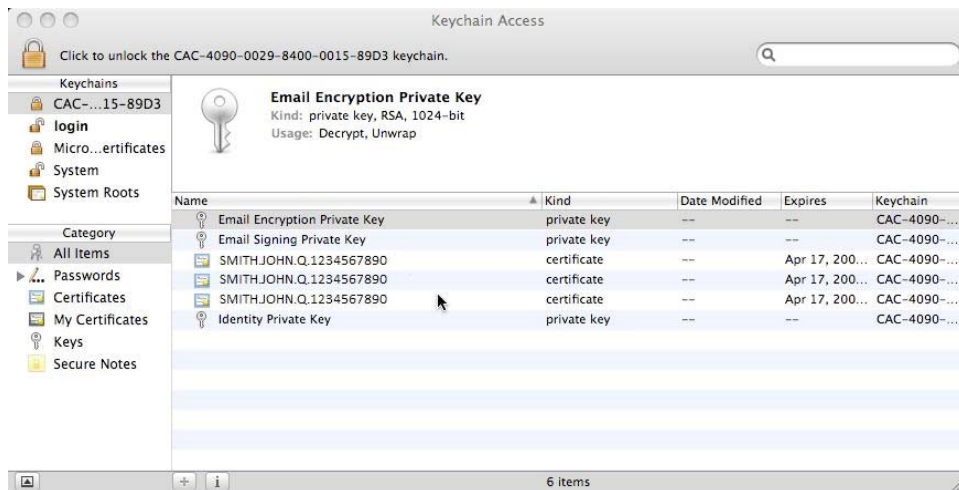
**Q: I get an error: "Safari was unable to open the page."**

**A:** There could be any number of causes for this error. First, try quitting Safari (From the Safari Main Menu, select Quit Safari (or use the Command-Q shortcut) and then restarting it. Alternately, restart the computer to clear any data cached in memory.

Verify connectivity to websites that do not require authentication to eliminate network issues. A system that is used on multiple networks (i.e. Home and Work) or different network connections (i.e. Wireless, CAT-5 Copper, AirCard, etc.) may need the Network Preferences modified, including proxy settings. Troubleshooting network issues is beyond the scope of this document.

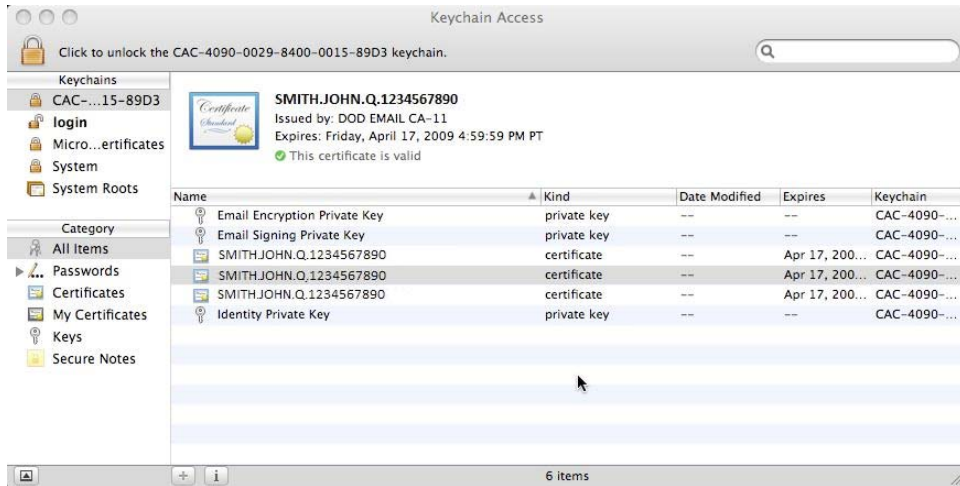
Another possible cause is missing Root or Intermediate Certificates. Ensure the Intermediate Certificates have been imported into the System Keychain of the Keychain Access utility. To download and install the Intermediate Certificates for your CAC, performing the following steps:

1. Open the Utilities folder, and double-click **Keychain Access**.
2. Insert your CAC into the SCR331.
3. In the Keychains (upper left) panel of the Keychain Access utility, a new entry will appear labeled **CAC-#####-#####-#####-#####-#####**, where **#####-#####-#####-#####-#####** is a unique number. Select this Keychain.
4. The contents of the CAC keychain will be displayed in the right panel. Three certificates will be displayed, one issued from a DOD CA and two issued from a DOD EMAIL CA.

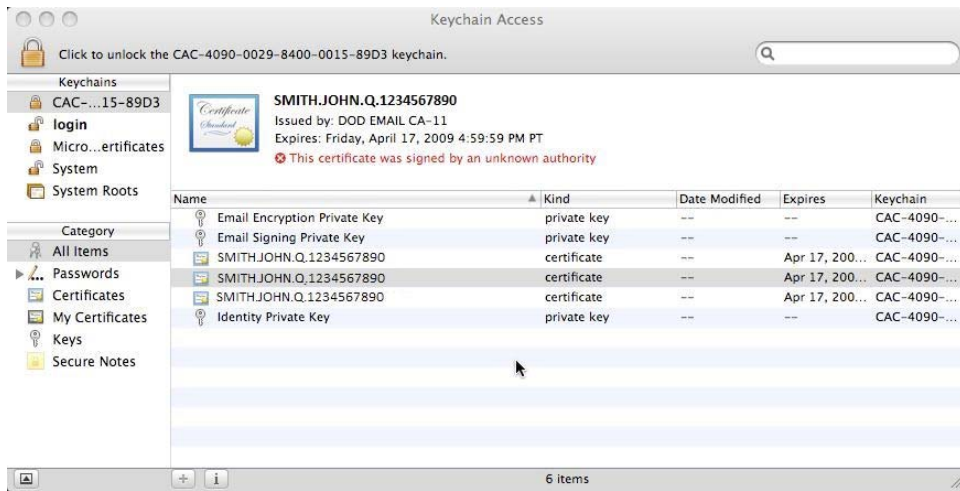


5. In the right panel, select the first (DoD) certificate. The certificate name, Issuer and Expiration Date will be displayed at the top of the right panel. If **“This certificate is valid”** is displayed in green, go to Step 11.

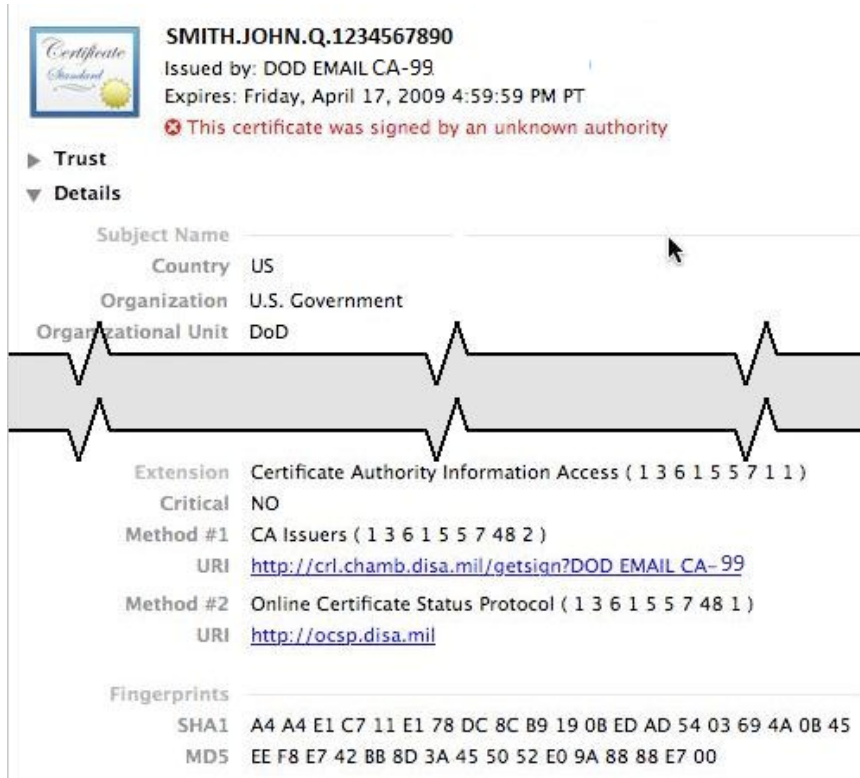




6. If "**This certificate was signed by an unknown authority**" is displayed in red, double-click it (or select File - Get Info).



7. The certificate Information window opens.



Scroll down to the Extension section labeled **Certificate Authority Information Access** and click on the link just below Method #1 (Example: <http://crl.chamb.disa.mil/getsign?DOD%20CA-99>). The Certificate Authority's certificate will be downloaded to your Downloads folder.

Throughout this document, CA-99 is used to identify the specific Certificate Authority the CAC was issued from. Replace CA-99 with the appropriate number for your CAC when following these instructions.

8. Close the Certificate Information window.
9. Open the Downloads folder and double-click on the **DODCA-99.cer** file. The Add Certificates window displays.



10. Set the Keychain field to **System** and click **OK**. If necessary, enter the administrator's name and password and click **OK**. The DOD CA-99 certificate will appear in the System section of Keychain Access.



11. In the right panel, select the second (DOD EMAIL) certificate. The certificate name, Issuer and Expiration Date will be displayed at the top of the right panel.
12. If **"This certificate is valid"** is displayed in green, go to next section (Import CAC Intermediate Certificates).
13. If **"This certificate was signed by an unknown authority"** is displayed, double-click it (or select File - Get Info). The Certificate Information window opens.
14. Scroll down to the Extension section labeled **Certificate Authority Information Access** and click on the link just below Method #1 (Example: <http://crl.chamb.disa.mil/getsign?DOD%20EMAIL%20CA-99>). The Certificate Authority's certificate will be downloaded to the Download folder.

15. Close the Certificate Information window.
16. Open the Downloads folder and double-click on the DOD EMAIL CA-99.cer file. The Add Certificates window displays.



17. Set the Keychain field to System and click OK. If necessary, enter administrator's name and password and click OK. The DOD EMAIL CA-99 certificate will appear in the System section of Keychain Access.



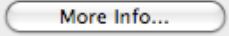
**Q: My CAC doesn't show up in the Keychain Access utility.**

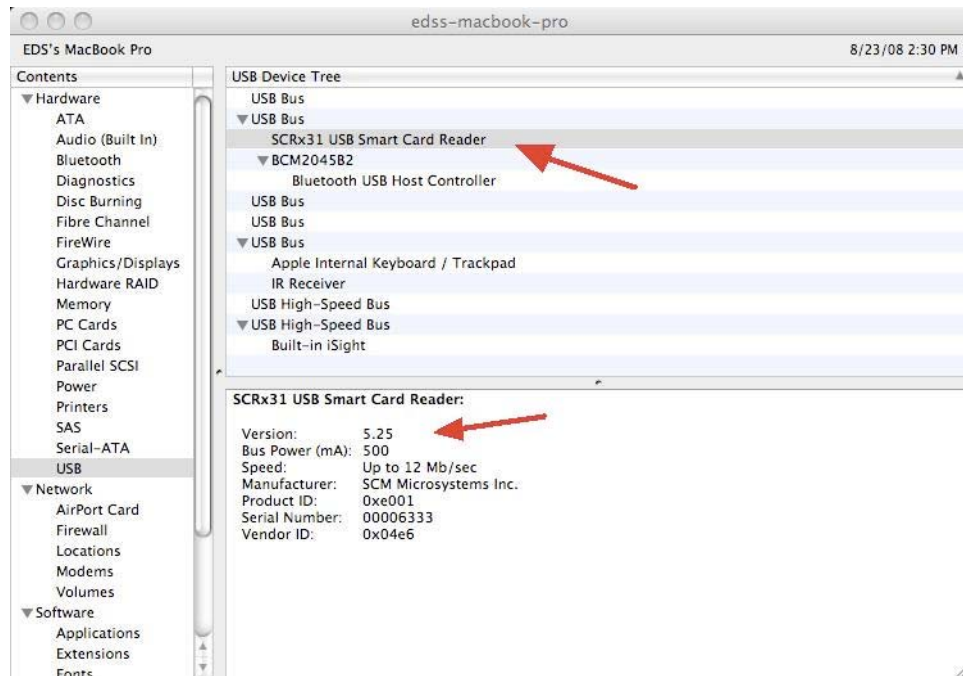
**A:** There are several possible reasons for this:

1. Verify the Firmware version of the SCR331 USB Smart Card Reader is correct. It must be 5.25 or higher. To verify the Firmware version, perform the following steps:
  - a. Connect the SCR331 USB Smart Card Reader to the Intel-based Apple computer and log in with an account having administrative privileges.

- b. From the Apple  Menu, select **About this Mac**. The About this Mac pop-up displays.



- c. Click the  button on the Information display. The System Profiler window opens.
- d. In the Left-hand pane, under the Hardware section, select USB.



- e. If the version displayed is not 5.25 or higher, use the procedures of Appendix A to upgrade the SCR331 USB Smart Card Reader's Firmware.
  - f. Close the System Profiler by selecting **System Profiler – Quit** from the Main Menu.
2. You have a new DoD Common Access Card that is not supported. New versions of CACs are issued as the current supply of cards is exhausted, and they occasionally provide additional capabilities that conflict with existing software. No issues with CACs issued prior to 15 August 2008 have been reported. If you have issues with a CAC issued after 15 August 2008, contact Apple Technical Support.
  3. You are using an unsupported Smart Card Reader. This process has only been verified using an SMC Micro SCR331 External USB Smart Card Reader. Other readers may work (either as is, or with the implementation of necessary drivers) however they have not been tested and are not included in these documents.

**Q: Some website links work but others don't.**

**A:** This solution has been verified for NMCI OWA only. Access to NMCI SharePoint or other CAC enabled sites has not been tested. Creating a separate Keychains Identity Preference may allow access to other sites. The steps of section 3.4 Create an Identity Preference can be used to create additional Identity Preference entries.

**Q: NMCI Outlook Web Access works fine for five to ten minutes and then Safari generates a "The page cannot be displayed" error. Additionally, Technical Information section of the page states "Error Code: 401 Unauthorized. This server requires authorization to fulfill the**

**request. Access to the Web server is denied. Contact the server administrator (12209).”  
When I attempt to reload the page, I get the same result. This doesn’t happen on a  
Windows machine using Internet Explorer. Why?**

**A:** This is due to the way Safari 3 handles client-side certificate authentication, by only prompting for when a Web page requires certificate authentication. The NMCI Outlook Web Access site is set for optional certificate authentication and the pages are set to time-out after a short period. This is to prevent a user from forgetting to log out and leaving their session open indefinitely. When the page times out, Safari doesn’t automatically resend the certificate authentication, which generates the 401 error.

The current work-around is to close out of Safari completely (not just the active window), re-start Safari and connect to NMCI Outlook Web Access again.

**Q: Why is a Windows machine required? Can a virtual machine be used?**

**A:** The Firmware update program is only written for the Windows Operating System. Yes, a Parallels or VMware Fusion virtual machine can be used to update the SCR331 Firmware, however using a physical Windows system is much simpler. One option is to use Boot Camp and install Windows XP on the Apple. If using a virtual machine, you will need to disconnect and connect the reader inside the virtual machine’s settings twice (once during the update, and again after it completes). This is because the configuration of the reader changes during the update. Steps to update the SCR331 using a virtual machine are beyond the scope of this document.

**Q: I don’t have a SCM Micro SCR-331 USB Smart Card Reader. Can other readers be used?**

**A:** Apple supports a number of different Smart Card readers, however the only model tested with this document is the SCM Micro SCR-331. A list of Apple supported readers can be found a <http://pcslite.alieth.debian.org/ccid.html> under the section “Supported CCID/ICCD Readers”.