



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

**CAC on a MAC: Setting up a DOD Common Access Card
Reader on the Macintosh OS X Operating System**

by

Phil Hopfner

March 2006

Approved for public release; distribution is unlimited

This page is intentionally blank.

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

RADM Richard H. Wells, USN
President

Richard Elster
Provost

This report was conducted under sponsored research supported by the National Security Agency under the High Assurance Platform Security Support - Phase II project.

Reproduction of all or part of this report is authorized.

This report was prepared by:

Phil Hopfner
Research Associate

Reviewed by:

Released by:

Peter Denning
Department of Computer Science

Leonard A. Ferrari, Ph.D.
Associate Provost and
Dean of Research

This page is intentionally blank.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

| | | | |
|---|---|---|---|
| 1. AGENCY USE ONLY (Leave blank) | 2. REPORT DATE March 2006 | 3. REPORT TYPE AND DATES COVERED Technical Report | |
| 4. TITLE AND SUBTITLE: Title (Mix case letters) CAC on a MAC: Setting up a DOD Common Access Card Reader on the Macintosh OS X Operating System | | 5. FUNDING NUMBERS | |
| 6. AUTHOR(S) | | 8. PERFORMING ORGANIZATION REPORT NUMBER NPS-CS-06-009 | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000 | | 10. SPONSORING / MONITORING AGENCY REPORT NUMBER | |
| 9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A | | 11. SUPPLEMENTARY NOTES This work was conducted under sponsored research supported by the National Security Agency under the High Assurance Platform Security Support - Phase II project. Any findings, conclusions or recommendations expressed in this material are those of the author and do not reflect the official policy or position of the Department of Defense, the National Security Agency, or the U.S. Government. | |
| 12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; Distribution is unlimited | | 12b. DISTRIBUTION CODE | |
| 13. ABSTRACT (maximum 200 words) The Naval Postgraduate School, along with many other Department of Defense (DOD) organizations, utilizes the ActivCard USB Common Access Card (CAC) readers. The CAC readers in conjunction with the user's Smart Card enables access to DOD PKI-enabled websites and allows the user to send signed and encrypted email utilizing the DOD Public Key Infrastructure (PKI). Microsoft Windows systems utilize the ActivCard Gold middleware software to enable CAC reader functionality. This software package is well integrated and documented in the Microsoft Windows environment. Starting with Macintosh OS X 10.4.x, there was no need to install any middle-ware software as all of the support for the US Federal Smart Cards is built in. This document details how to update the ActivCard readers to make them fully compliant with OS X 10.4.x and then details the steps necessary to setup the system in order to use the CAC readers under the Macintosh OS X 10.4.x operating system. | | | |
| 14. SUBJECT TERMS | | 15. NUMBER OF PAGES 21 | |
| | | 16. PRICE CODE | |
| 17. SECURITY CLASSIFICATION OF REPORT Unclassified | 18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified | 19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified | 20. LIMITATION OF ABSTRACT UL |

This page is intentionally blank.



The Center for Information Systems
Security Studies and Research

Technical Report NPS-CS-06-009

CAC on a MAC

Setting up a DOD Common Access Card Reader on the Macintosh OS X
Operating System

Phil Hopfner
March 2006

Center for Information Systems Security Studies and Research
Computer Science Department
Naval Postgraduate School
Monterey, California 93943

CAC on a MAC: Setting up a DOD Common Access Card Reader on the Macintosh OS X Operating System

Phil Hopfner
Naval Postgraduate School
Monterey, CA

Abstract

The Naval Postgraduate School, along with many other Department of Defense (DOD) organizations, utilizes the ActivCard USB Common Access Card (CAC) readers. The CAC readers in conjunction with the user's Smart Card enables access to DOD PKI-enabled websites and allows the user to send signed and encrypted email utilizing the DOD Public Key Infrastructure (PKI). Microsoft Windows systems utilize the ActivCard Gold middleware software to enable CAC reader functionality. This software package is well integrated and documented in the Microsoft Windows environment. Starting with Macintosh OS X 10.4.x, there was no need to install any middle-ware software as all of the support for the US Federal Smart Cards is built in. This document details how to update the ActivCard readers to make them fully compliant with OS X 10.4.x and then details the steps necessary to setup the system in order to use the CAC readers under the Macintosh OS X 10.4.x operating system.

Introduction

Many Department of Defense (DOD) facilities use Smart Cards in combination with Common Access Card readers to provide security for transactions like logging into a system, digitally signing email and documents, encrypting email, accessing protected websites, etc. Information can be protected using the DOD Public Key Infrastructure (PKI) and access granted to those individuals using CAC readers and Smart Cards. [4]

The Microsoft Windows environment comprises the bulk of the end-user computing base in the DOD. Third-party software (like ActivCard Gold) integrates with the Microsoft Windows environment and provides the end user with seamless access to use their Smart cards in conjunction with CAC readers.

The DOD also has a large Macintosh-based user community. As of Macintosh OS X 10.4, the Macintosh operating system "...has built-in support for use with the U.S. Federal Government's Smart Cards which adhere to one of the approved specifications: CAC (Common Access Card), GSCIS (Government Smart Card Interoperability Specification), PIV (Personal ID Verification). Mac OS X also supports a wide variety of Smart Card Readers on all Apple systems running Mac OS X." [3].

However, getting the CAC readers to work properly under OS X 10.4 was somewhat problematic. The issue of getting everything properly setup was not published in any Apple documentation that could be located. There was a fair amount of information published by Shawn Geddis [1,2] and others on the Apple "Fed-Talk" Mailing list [5], but no comprehensive or step-by-step guide on how to get it working.

To that end, the Center for Information Systems Security Studies and Research (CISR) conducted tests, pulled all the available information together and produced a step-by-step guide which is detailed in the Appendix of this document. This guide steps the user through the following processes:

- Flash the Firmware in the USB CAC Reader.
- Enable DOD Certificates in KeyChain.
- Delete old Keychain Certificates and CAC cache.
- Copy new Certificates from CAC in KeyChain.
- Ensure Email address matches what's on the CAC.
- Specific Email setup information:
 - Setting up Mac Mail
 - Setting up Thunderbird

It should be possible to setup additional email clients based on the principles reflected in the documentation. The procedure has been tested by several individuals outside of the CISR organization and has been found to work well in all cases.

Acknowledgements

The author would like to extend his appreciation to the following individuals for their help and collaboration in the creation of this procedure.

Richard Scott Coté is a Lecturer at the Naval Postgraduate School

Shawn Geddis is a Security Consulting Engineer, Apple Computer

References

1. Shawn Geddis' home page, <http://homepage.mac.com/geddis/smartcards/FileSharing24.html>
2. Shawn Geddis, Smart Card Setup and Configuration Guide v1.0, 2004
3. Apple IT Pro Federal Government web site, <http://www.apple.com/itpro/federal>
4. Federal Government Smart Card web site, <http://www.smartcard.gov>
5. Apple Mailing Lists, <http://lists.apple.com/mailman/listinfo/fed-talk>

Appendix A: Detailed Procedures

Description:

This procedure details the steps necessary to get a USB CAC card reader working with email on a Mac running OS X 10.4.3 and above. Versions of Mac OS X prior to 10.4.3 have not been tested and may not work with this procedure.

WARNING:

This procedure has been tested on several systems. However, the author is providing this information "as-is" with no guarantees and cannot be held responsible for any misconfigurations or problems as a result of this procedure.

This procedure involves updating the firmware of an ActivCard USB reader. Once the firmware is updated, the USB reader can only be used on a PC that has had the SCR33x driver installed (in addition to the ActivCard Gold software).

Prerequisites:

- USB ActivCard Reader
- PC with Windows XP and ActivCard Gold 2.2 installed.
- From: <http://homepage.mac.com/geddis/smartcards/FileSharing24.html>
 - SCR33xx_inst_English_V8.11.zip
(adds the SCR33x drivers to recognize the updated CAC card reader)
 - SCR31CCID_FW_V5.18.zip
(to flash the firmware)

Overview:

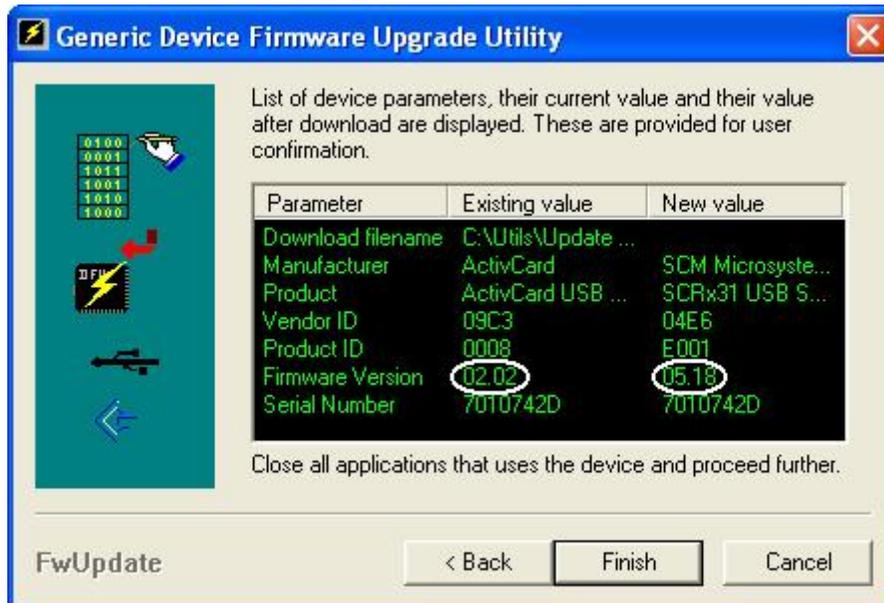
1. [Flash the Firmware in the USB CAC Reader.](#)
2. [Enable DOD Certificates in KeyChain.](#)
3. [Delete old Keychain Certificates and CAC cache.](#)
4. [Copy new Certificates from CAC in KeyChain.](#)
5. [Ensure Email address matches what's on the CAC.](#)
6. Specific Email setup information:
 - [Setting up Mac Mail](#)
 - [Setting up Thunderbird](#)

Flash the Firmware in the USB CAC Reader

Perform these steps on a Windows XP system with local Administrator authority.

Step 1: Flash the Reader

- a) Plug the “unflashed” ActivCard USB reader into a USB port.
- b) Launch the ActivCard Gold Utilities (in the system tray) and insert a CAC card to make sure the reader functions correctly.
- c) Go to **Start | Settings | Control Panel | Administrative Tools | Services**.
- d) Stop the following services:
 - ActivCard Gold AutoRegister
 - ActivCard Gold Service
 - Smart Card Service
- e) Extract the SCR33xx_inst_English_V8.11.zip contents into a folder. Do the same for the SCRx31CCID_FW_V5.18.zip file.
- f) From the extracted SCRx31CCID_FW_V5.18.zip folder, run **fwupdate.exe**.
- g) On the FwUpdate screen, click **OK**.
- h) Click Browse, select the SCR531_V518.bin file (from the extracted SCRx31CCID_FW_V5.18.zip folder) and click **Open**.
- i) Click **Next**.
- j) Verify that the Firmware “New Value” is version 05.18.



- k) Click **Finish**.
- l) Click **Close**.
- m) Unplug the USB CAC card reader.

Step 2: Load New CAC Drivers

- a) On the Windows PC, go to the extracted SCR33xx_inst_English_V8.11.zip folder and run **setup.exe**.
- b) Step through and complete the Installation Wizard and accept all the default settings.
- c) When the software is installed, plug the "flashed" CAC card reader into the system. It should be recognized as an "SCR33x USB Smart Card Reader".

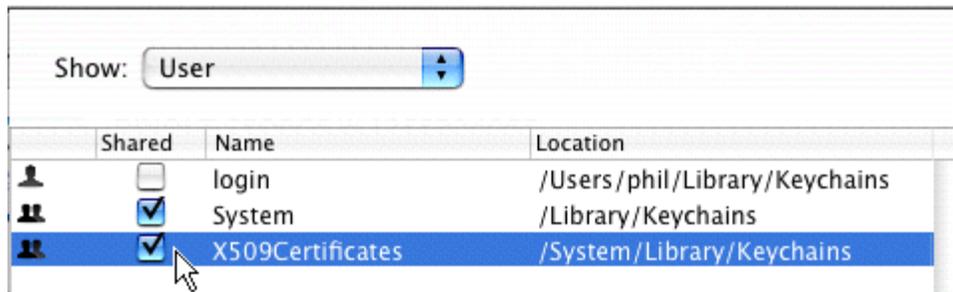
Step 3: (Optional) Verify New CAC Drivers

- a) Click on **Start | Programs | SCM Microsystems Tools | Installation Test**.
- b) Select **SCR33xx** and click **Test**.
- c) Click English and scroll down. The "Result:" should be "The installation test is completed successfully".
- d) Click Close.
- e) Remove the "flashed" USB card reader and label it with the following: **SCR33x USB Smart Card Reader Firmware: 05.18**

Add the DOD Intermediate CAs to the Keychain

These steps are performed on a Mac with OS X 10.4.3 or better.

- a) Logon to the Mac with your normal user ID.
- b) Launch Keychain Access (**Go | Utilities | Keychain Access**).
- c) Select **Edit | Keychain List**.
- d) Under Show, select: **Mac OS X (System)**.
- e) Check "Shared" checkbox for **X509Certificates (/System/Library/Keychains)**



- f) Click **OK**.
- g) Close Keychain Access.

At this point, you should now be able to send signed email. Any application that recognizes the Keychain should work with the CAC reader.

During testing it was noted that most applications require that the CAC card reader be plugged in and a CAC card inserted PRIOR to starting the application for the CAC Reader to work within the application.

Delete old Keychain Certificates and CAC cache (Optional):

If your CAC card has changed in any way (new email address, name change, etc) from the time you first used it on a specific system, you may have to clear out the cached CAC credentials and certificates.

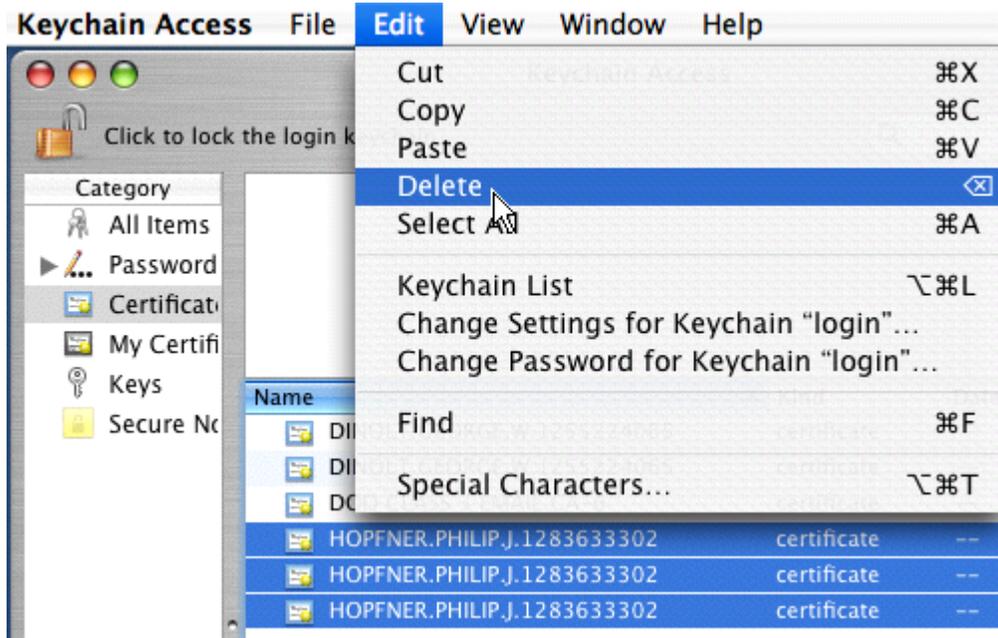
Step 1: Remove Cached CAC credentials

- a) Open a Terminal Session (**Go | Utilities | Terminal**)
- b) Type: `cd /private/var/db/TokenCache` and press <Enter>.
- c) Type: `sudo mv tokens tokens-old` and press <Enter>.
- d) Type: `sudo mkdir tokens` and press <Enter>.
- e) Type: `sudo chmod 711 tokens` and press <Enter>.

Note that this will remove ALL CAC card credentials from the system. If you wish to remove just one, you must examine the TokenCache folder and determine which "com.apple.token.cac:CAC-xxxx-xxxx-xxxx-xxxx-xxxx" needs to be removed.

Step 2: Remove old Certificates

- a) Launch Keychain Access (**Go | Utilities | Keychain Access**)
- b) Click on Certificates.
- c) Use **Edit | Delete** to remove certificates with your name (Last.First.MI.xxx)



- d) Close Keychain Access.

[Return to Top](#)

Copy new Certificates from CAC to Login Keychain:

You must copy your CAC credentials from the CAC card to the login (default) keychain.

- a) Insert your USB CAC reader into the system
- b) Launch Keychain Access (**Go | Utilities | Keychain Access**)
- c) Click on **Show Keychains.**
- d) Insert your CAC into the reader.
Note that a new entry appears (*smart card #x*).
- e) Click on the *smart card #x* keychain.
- f) Select the certificates with your name (Last.First.MI.xxxxxxx) and click on **Edit | Copy.**
- g) Click on the login (default) keychain and click on **Edit | Paste.**
- h) Close Keychain Access.

[Return to Top](#)

Ensure Email address matches what's on the CAC:

In order to send email, the email address embedded within your CAC must match the email address set in the Preferences of the email program. The Macintosh OS is case-sensitive, so if your email address is all CAPS in your CAC, your email address in your Preferences should be all CAPS.

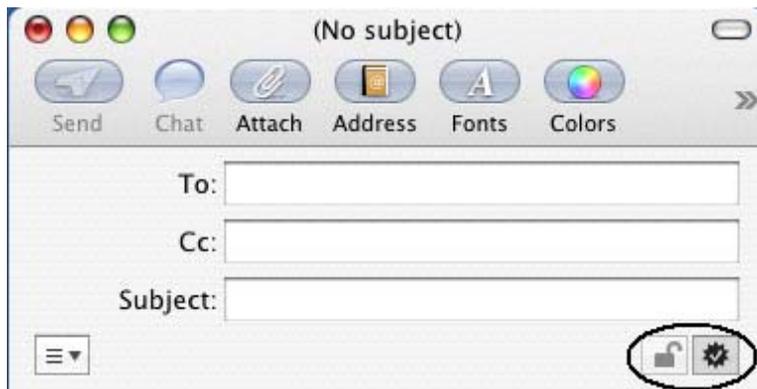
If there is a mismatch between the email program settings and your CAC, you will not see the icons for digitally signing/encrypting email in Mac Mail. Thunderbird will complain of "missing certificates" when trying to send mail.

Setting up Mac Mail:

This assumes that you already have setup Mac Mail for normal use.

- a) Logon to the Mac with your normal user ID.
- b) Plug a flashed USB CAC Card Reader into the USB port and insert your CAC card into the Reader.
- c) Start Mac Mail.
- d) Click New

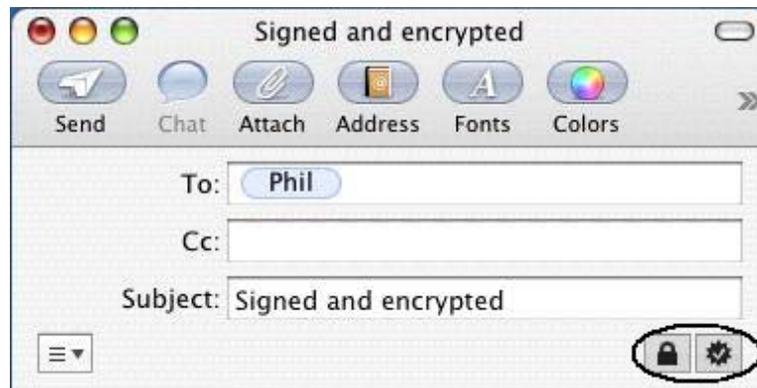
If the email address in your CAC card matches the email address in your **Preferences | Account**, you should see the icons for digitally-signed email appear when sending



New email.

Clicking the "starred" checkmark should allow you to select/deselect signed email.

Clicking the "padlock" should allow you to select/deselect encrypted email.



If you can't get the padlock to "shut", you don't have the public certificates for the person or person(s) you are trying to send to. If you are testing sending signed/encrypted email to yourself, see **Copy new Certificates from CAC to Login Keychain** above.

Setting Up Thunderbird:

This assumes that you already have setup Thunderbird for normal use.

- a) Logon to the Mac with your normal user ID.
- b) Plug a flashed USB CAC Card Reader into the USB port and insert your CAC card into the Reader.
- c) Open a Terminal session (**Go | Utilities | Terminal**).
- d) Type: "sudo pcsctool" and press <Enter>.
- e) Select: "1. commonAccessCard.bundle" and press <Enter>.
Verify the message "Token support updated successfully !" appears.

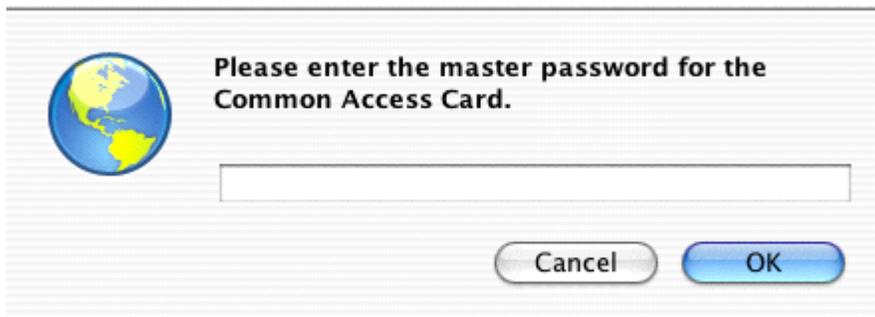
```
Select the appropriate token driver:
```

```
-----
1.      commonAccessCard.bundle
2.      GSCISPlugin.bundle
3.      mscMuscleCard.bundle
4.      slbCryptoflex.bundle
-----
```

```
Enter the number: 1
```

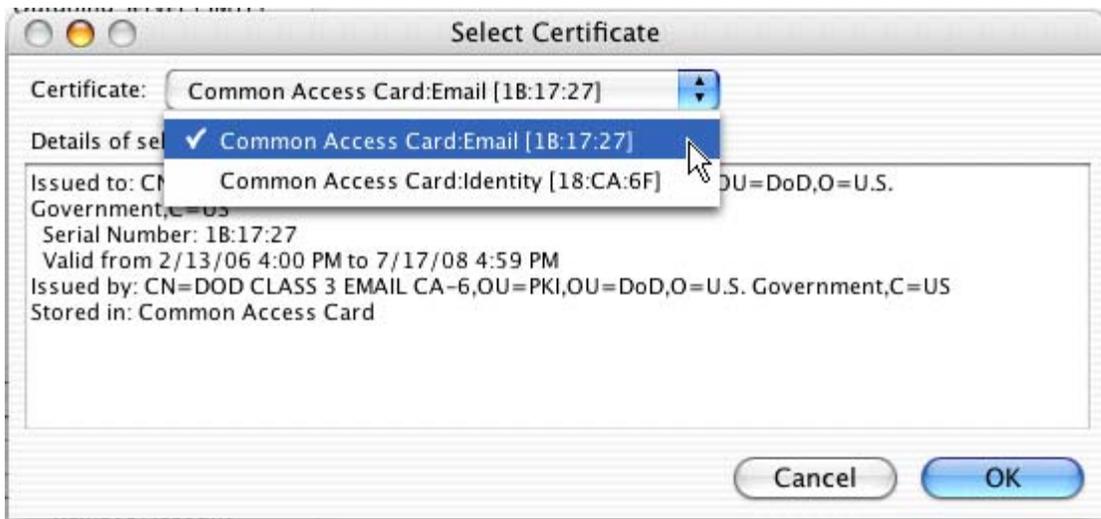
```
Insert your token in: CCID Smart Card Reader 0 0
Token support updated successfully !
```

- f) Start Thunderbird.
- g) Click on **Tools | Account Settings | Security**
- h) Click on **Manage Security Devices**.
- i) Click on **Load**.
- j) Under "Module filename" enter:
/usr/libexec/SmartCardServices/pkcs11/pkcs11.bundle/Contents/MacOS/pkcs11
- k) Click **OK**. Click **OK** to acknowledge that a new security module was added.
- l) Click **OK** to close the Manage Security Devices windows.
- m) Under Digital Signing, click on **Select...** The following should appear:



- n) Enter your CAC PIN.

o) Select the CAC:Email certificate and click **OK**.



p) Click **OK** to use the same certificate for encrypting/decrypting.

q) Click **OK** to close the Account settings window.

That's it. You should be able to send signed email using Thunderbird. Select the Security icon when sending new mail to select signed and/or encryption as an option.



If you get a warning because you don't have the proper certificates, you must import the proper DOD certificates into Thunderbird BEFORE you can send digitally signed email. See "[How to export/import DOD certificates](#)" in the **Notes** section below.

Notes

Test the CAC reader and Card on a Mac:

- a) Logon to the Mac with your normal user ID.
- b) insert a flashed USB CAC Card Reader into the USB port.
- c) Insert your CAC card into the Reader.
- d) Open a Terminal session (Go | Utilities | Terminal)
- e) Type: "pcsctest" and press <Enter>
- f) When prompted, type in the "reader number" displayed in the line above (e.g. 01) and press <Enter>.

The installation tests will run and the result should read

```
"PC/SC Test Completed Successfully!"
```

Using the "Flashed" CAC reader on Windows:

In addition to loading the ActivCard Gold software on a PC, you must load the SCR33xx_inst_English_V8.11.zip drivers on the PC in order for the PC to recognize and use the flashed CAC Reader.

Also note that the flashed CAC Reader will no longer be recognized as an ActivCard USB Reader V2, but will instead show up as an "SCR33X USB Smart Card Reader". The ActivCard Gold utility software will be able to operate with either a "flashed" or "unflashed" reader as long as both the ActivCard USB drivers and the SCR33X drivers have been installed.

How to export/import DOD certificates

This procedure allows you to export certificates from Internet Explorer and import them into Thunderbird one at a time.

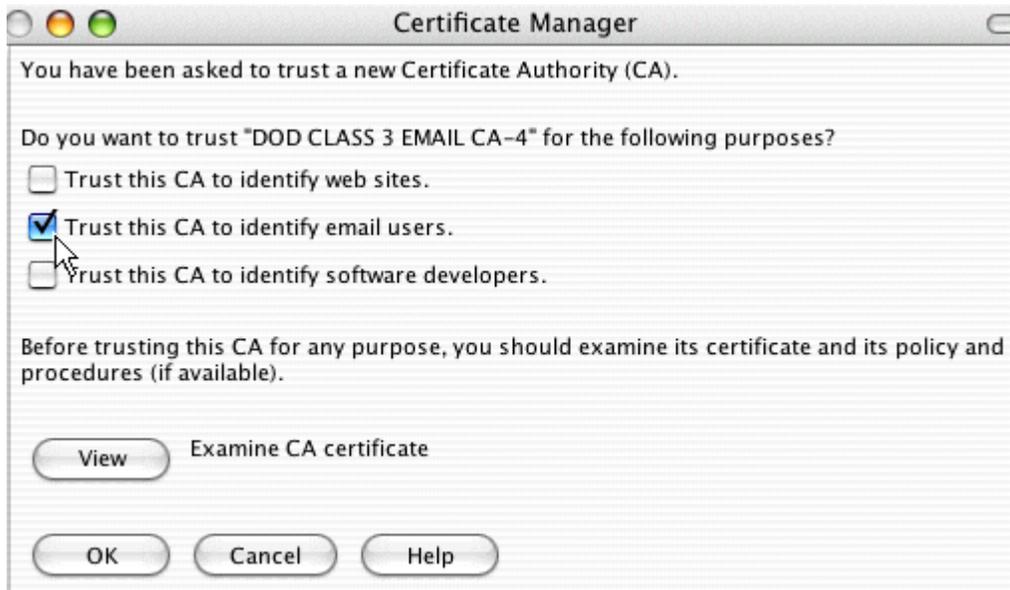
Export the certificate

- a) On a Windows PC, launch Internet Explorer.
- b) Click on **Tools | Internet Options.**
- c) Click on **Content.**
- d) Click on **Certificates.**
- e) Click on **Intermediate Certification Authorities.**
- f) Click on the first **DOD CLASS 3 EMAIL xxx** certificate in the list (scroll down a bit).
- g) Click on **Export.**

- h) Click **Next**.
- i) Click **Next**.
- j) Use the Browse button and place the file somewhere where you'll find it (e.g. Desktop) with a name you'll remember.
- k) Click **Next**.
- l) Click **Finish** and then **OK** (notice the .CER file has been created).
- m) Repeat for all **DOD CLASS 3 EMAIL xxx** certificates and save the files for later use.

Import the certificate

- a) Launch Thunderbird (Mac platform).
- b) Click on **Tools | Options**.
- c) Click on the **Security** tab.
- d) Click on View **Certificates**.
- e) Click on the **Authorities** tab.
- f) Click **Import**.
- g) Navigate to the folder (e.g. Desktop) where you saved the .CER files.
- h) Double-click the .CER file.



- i) Select "**Trust this CA to identify email users**" and click **OK**.

That's it....the certificate will appear under U.S. Government. Now – just repeat the above for each certificate.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
8725 John J. Kingman Rd., Ste. 0944
Ft. Belvoir, VA 22060-6218
2. Dudley Knox Library, Code 013 2
Naval Postgraduate School
Monterey, CA 93943-5100
3. Research Office, Code 09 1
Naval Postgraduate School
Monterey, CA 93943-5138
4. Christine Cermak 1
CIO, Naval Postgraduate School
Monterey, CA 93943-5138
5. David Wennergren 1
DoN CIO
1000 Navy Pentagon
Washington DC 20350-1000
6. Shawn Geddis 1
Security Consulting Engineer, Apple Computer
7. Dr. Cynthia Irvine 1
Naval Postgraduate School
Monterey, CA 93943-5100
8. Paul Clark 1
Naval Postgraduate School
Monterey, CA 93943-5100
9. Richard Scott Coté 1
Naval Postgraduate School
Monterey, CA 93943-5100
10. Phil Hopfner 1
Naval Postgraduate School
Monterey, CA 93943-5100
11. Cullen Jones 1
Naval Postgraduate School
Monterey, CA 93943-5100