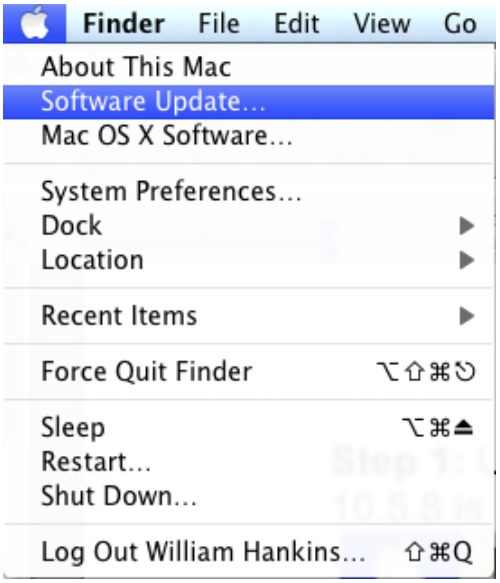
Updated on 18 June 2010

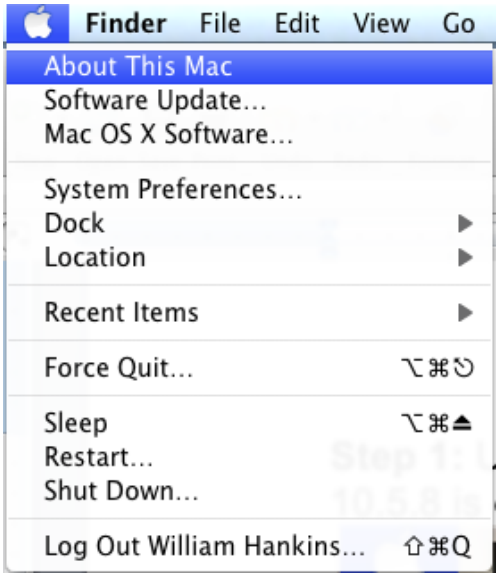
Setting up your CAC for use on your Macintosh (Visually):

Step 1: Update your system. (10.5.6 is the minimum required for Leopard, though 10.5.8 is currently available for Leopard, and 10.6.4 is available for Snow Leopard)



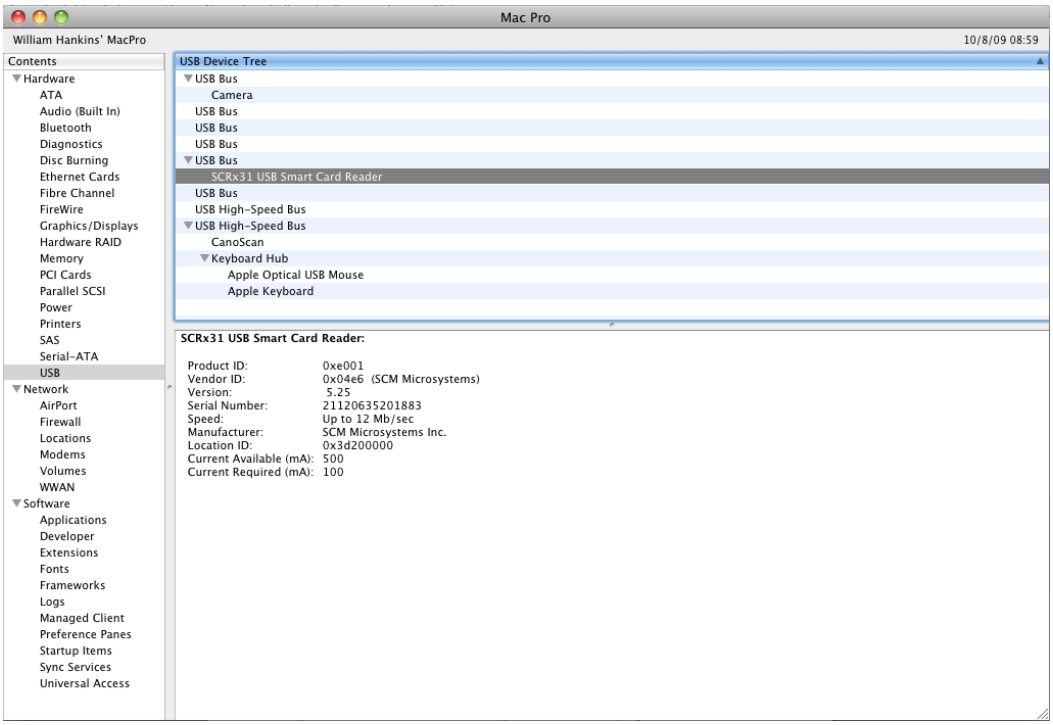
Step 2: Plug in your CAC Reader to an available USB Port

Step 3: Click the Apple Icon in the upper left corner of your desktop and select "About This Mac"



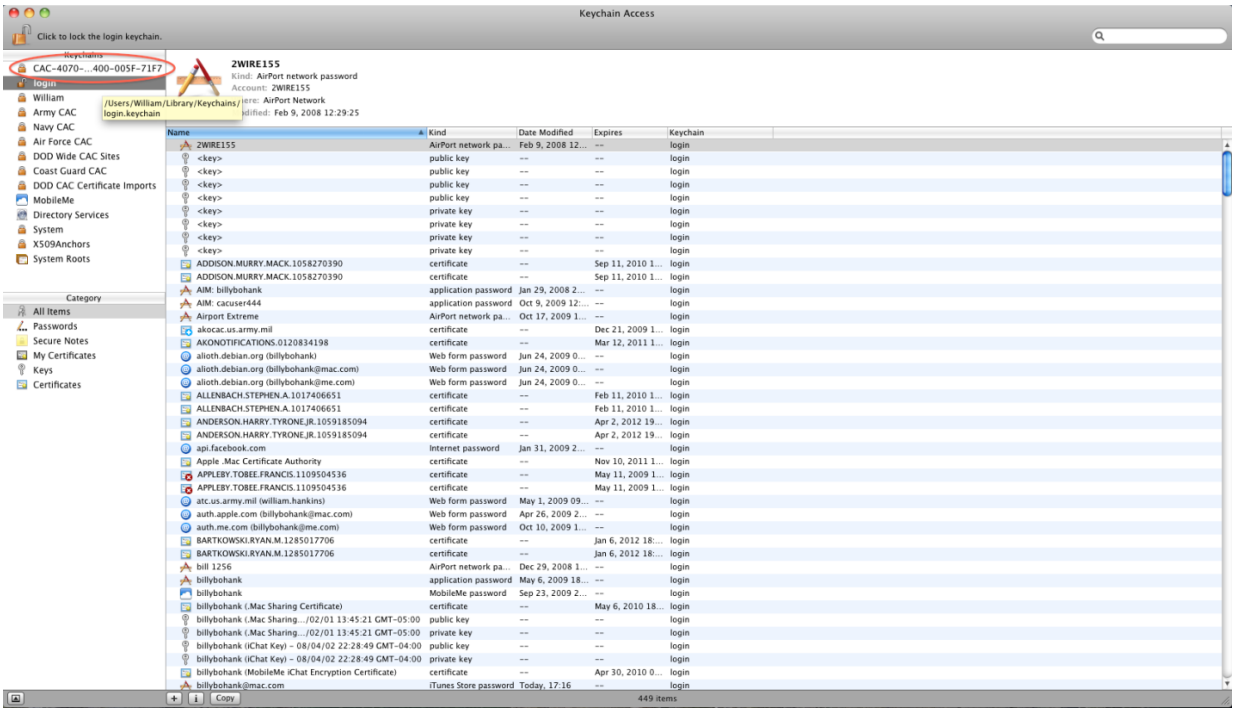
Step 4: Click the "More Info" Button within the window that pops up. (This opens System Profiler)

Step 5: Within the "*Hardware*" Category select "*USB*." On the right side of the screen the window will display all hardware plugged into the USB ports on your Mac. You should see "*Smart Card Reader*." If the Smart Card reader is present, it is installed on your system, and no further hardware changes are required, i.e. additional drivers / Firmware upgrades. You can now Quit System Profiler.



Step 6: Click: *Go, Applications,* scroll down to: *Utilities,* click the little triangle to open it up, double click *Keychain Access*"

Step 7: Insert your CAC into the CAC Reader. In the upper left of the Keychain Access window, under "Keychains" your CAC should show up (CAC XXXX-XXXX-XXXX-XXXX-XXXX), click it. In the right side you will see the certificates that are on your CAC. (If your CAC does not appear remove it from the reader, unplug the Reader, quit, and re-open Keychains Access, plug in the Card Reader, and insert your CAC)



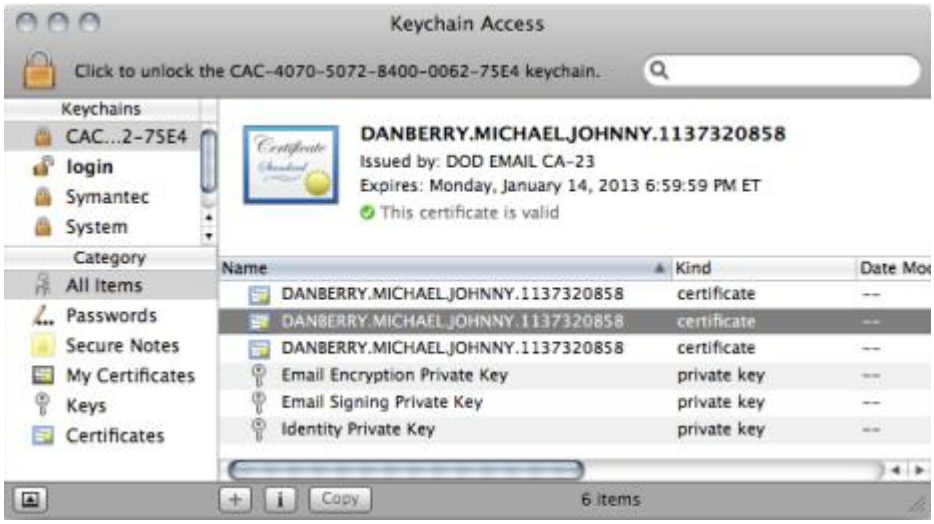
Step 8: Click the "Padlock" icon in the upper left corner of the program window, which will prompt you for your CAC PIN. Enter your PIN to unlock your CAC.

Step 9: Select the desired certificate, which will show DOD CA-XX or DOD EMAIL CA-XX in the upper window. Right Click (Control Click) and select "New Identity Preference"

Step 10: Enter the URL / website (choose from the below links) for the appropriate website you wish to access using your CAC, select the appropriate certificate and click “Add”:

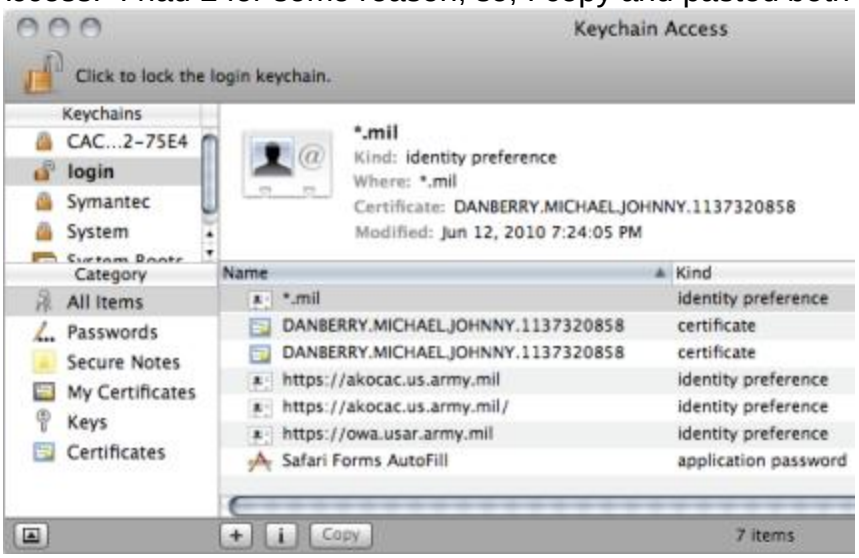
Step 10a: I was unable to save the email certificate for my OWA (it kept defaulting back to the non-email certificate)

Step 10b: I copied the email certificate(s) from the CAC...2-75E4 section.



Step 10c: I first verified it was the *email certificate* before pasting it into the login section

Step 10d: I pasted the above email certificate(s) into the login screen section of Keychain Access. I had 2 for some reason, so, I copy and pasted both of them.



Step 11: Quit Keychain Access (and Applications (if it is still open)), remove your CAC from the reader, and re-insert it. Open Safari and begin navigating to your CAC enabled site.

Examples of URLs to add to your Keychain Access

Army:
- AKO: https://akocac.us.army.mil/ (DOD CA-XX)
- AKO Webmail: https://wmcac.us.army.mil/ (DOD CA-XX)
- Fort Gordon OWA (NASE Email Access): https://rw3.army.mil/EXCHANGE (EMAIL CA-XX)
- Army Reserve OWA (USAR Email Access): https://owa.usar.army.mil/ (EMAIL CA-XX)
- Center for Army Lessons Learned (CALL): https://call3.leavenworth.army.mil (DOD CA-XX)
- CONUS AMEDD Exchange OWA: https://medmail-conus.amedd.army.mil/Exchange (EMAIL CA-XX)
- National Guard Knowledge Online: https://gkoportal.ngb.army.mil (DOD CA-XX)
- NORAD NORTHCOM CAC Registration Site: https://registration.noradnorthcom.mil/ (DOD CA-XX)
- NORAD NORTHCOM External Access Site: https://operations.noradnorthcom.mil (DOD CA_XX)
- Soldier Survey Site: https://fcportal.forscom.army.mil/ (EMAIL CA-XX)

Navy:
- Navy Knowledge Online (1 of 2): https://cac01.nko.navy.mil (DOD CA-XX)
- Navy Knowledge Online (2 of 2): https://cac01.nko.navy.mil:443/app1/index2.jsp (DOD CA-XX)
- Navy Webmail: https://webmail.nmci.navy.mil (DOD CA-XX)
- Reserve Portal: https://private.navyreserve.navy.mil/ (DOD CA-XX)
- NADSUSEA (Navy East OWA): https://webmail.east.nmci.navy.mil (EMAIL CA-XX)
- NADSUSWE (Navy West OWA): https://webmail.west.nmci.navy.mil (EMAIL CA-XX)
- NADSUSEA NCIS COI (Navy NCIS OWA): https://webmail.ncis.nmci.navy.mil (EMAIL CA-XX)
- NMCI-ISF (Navy ISF OWA): https://webmail.isf.nmci.navy.mil (EMAIL CA-XX)
- PADS (Navy PADS OWA): https://webmail.pacom.mil (EMAIL CA-XX)
- PADS (Navy PACOM SMR Users OWA): https://webmail.exceptions.pacom.mil (EMAIL CA-XX)
- IATS NMCI Webmail (1 of 3): https://iats.nmci.navy.mil (EMAIL CA-XX)
- IATS NMCI Webmail (2 of 3): https://iats.nmci.navy.mil/ (EMAIL CA-XX)
- IATS NMCI Webmail (3 of 3): https://iats.nmci.navy.mil/cas (EMAIL CA-XX)
- Marine Corps Webmail: https://webmail.us.nmci.usmc.mil/Exchange (EMAIL CA-XX)
- Navy InfoSec: https://infosec.navy.mil (DOD CA-XX)
- Navy Medical (1 of 3): www.med.navy.mil:80 (DOD CA-XX)
- Navy Medical (2 of 3): https://nmo.med.navy.mil/ (DOD CA-XX)
- Navy Medical (3 of 3): https://nmo.med.navy.mil/pki/default.cfm (DOD CA-XX)
- Navy Medical Outlook Web Access: https://sscc-fe-03.med.navy.mil/EXCHANGE (EMAIL CA-XX)
- JTF-GNO: https://www.jtfgno.mil (EMAIL CA-XX)
- BUPERS: https://pki.bol.navy.mil/ (DOD CA-XX)

- NSIPS (1 of 2); https://nsips.nmci.navy.mil (DOD CA-XX)
- NSIPS (2 of 2): https://nsipsweb.nmci.navy.mil/nsipsclo/logon (DOD CA-XX)
- NROWS: https://nrows.sscno.nmci.navy.mil (DOD CA-XX)
- Navy Reserve Portal (1 of 2): https://private.navyreserve.navy.mil/ (DOD CA-XX)
- Navy Reserve Portal (2 of 2): https://private.navyreserve.navy.mil/pages/default.aspx (DOD CA-XX)

Air Force: (There are currently issues with the AF Portal, the issues are being addressed and updates will be posted here when available)
- AF Portal (1 of 3): https://www.my.af.mil (DOD CA-XX)
- AF Portal (2 of 3): https://www.my.af.mil/EAI_JUNCTION/eai/ (DOD CA-XX)
- AF Portal (3 of 3): https://www.my.af.mil/EAI_JUNCTION/eai/auth (DOD CA-XX)
- Air Force Portal Virtual MPF Site: https://w20.afpc.randolph.af.mil/afpcsecurenet20/ (DOD CA-XX)
- Air Force Top Flite Website: https://logon.jag.af.mil (DOD CA-XX)
- Air Force Jag Site: https://aflsa.jag.af.mil/ (DOD CA-XX)
- Air Force Education Exchange: https://cacwebmail.afit.edu/Exchange (EMAIL CA-XX)
- AF AMC Exchange Email: https://mail.amc.af.mil/exchange (EMAIL CA-XX)

Coast Guard:
- Coast Guard Email: http://cgwebmail.uscg.mil/ (DOD CA-XX)

DoD:
- Defense Manpower Data Center: https://pki.dmdc.osd.mil (DOD CA-XX)
- DOD 411 Directory: https://jeds.gds.disa.mil (EMAIL CA-XX)
- Tricare Online: https://www.tricareonline.com/preloginHome.do (DOD CA-XX)
- Tricare (1 of 3): https://cac1.tricareonline.com/ (EMAIL CA-XX)
- Tricare (2 of 3): https://cac2.tricareonline.com/ (EMAIL CA-XX)
- Tricare (2 of 3): https://cac3.tricareonline.com/ (EMAIL CA-XX)
- Military Health System: https://mhssc.timpo.osd.mil (DOD CA-XX)

Note on URL's: It is important to understand that when entering URL's into an identity preference they must be precise. As you can see in the preceding references some end with a "/". Not all websites will have this. Every website that attempts to validate your CAC must search a database (Usually internal to the site) and the URL you enter is creating the link between that database and your CAC. As there is not a single database that all sites use for this purpose you will encounter sites that do not function properly initially. If you pay attention to the actions of the browser when you click the login button you will usually see where the browser is being pointed and can use that URL in your Identity Preference. For the most part you will not need to reference a specific site, i.e. ending in .html etc, but instead the will use the broad address as above.

Note on Certificate Selection: When creating Identity Preferences within Keychains it is important to understand the difference between your Certificates. I will not go into

great detail as to the differences here however I will give you the information you need to know. There are 3 certificates on your CAC:

- **DOD CA-XX**, used for identification verification, is the top most certificate shown in Keychains. This will be used when logging into AKO. This will show up with a red "x" beside it a majority of the time as "Unsigned".

- **DOD CA-XX EMAIL**, used for signatures, is the second in the list of certificates in the list. This certificate is used when you digitally sign an email, or document, and by some websites for verification of your identity, i.e. Outlook Web Access. When logging into a non-AKO site keep in mind that whatever certificate you used when logging on at your work computer will be required on your MAC.

- **DOD CA-XX EMAIL**, used for encryption, is the third in the list of certificates. This will not be used when accessing websites, and unless you are accustomed to encrypting your email, will not be used at all.

When creating Identity Preferences there will be some trial and error involved in selecting the correct URL/Certificate combination. If you create an Identity Preference and attempt to change the certificate it uses you may see more than 3 certificates when you open the drop down menu as below, they are grouped into their respective classes, the first pair being the DOD CA-XX, second pair EMAIL CA-XX (Signature) and the third pair EMAIL CA-XX (Encryption). Choose either of the first two if you want the DOD CA-XX and so forth. They point to the same certificate.

This should set you up to access sites that are authenticated with your CAC. Please let me know how this works out for you and what issues you have. Once again if you have additional sites you have found solutions for please let me know and I will include them in the list on this page. If you still have questions, feel free to contact me by visiting: https://militarycac.com/MACquestions.htm.

Current as of: 18 June 2010

Written by CPT Bill Hankins, Revised by CW3 Michael J. Danberry while following the instructions on my own iBook G4 & MacBook Mac laptops.