

Use of Common Access Cards (CACs) from Home on Windows 7 without Middleware

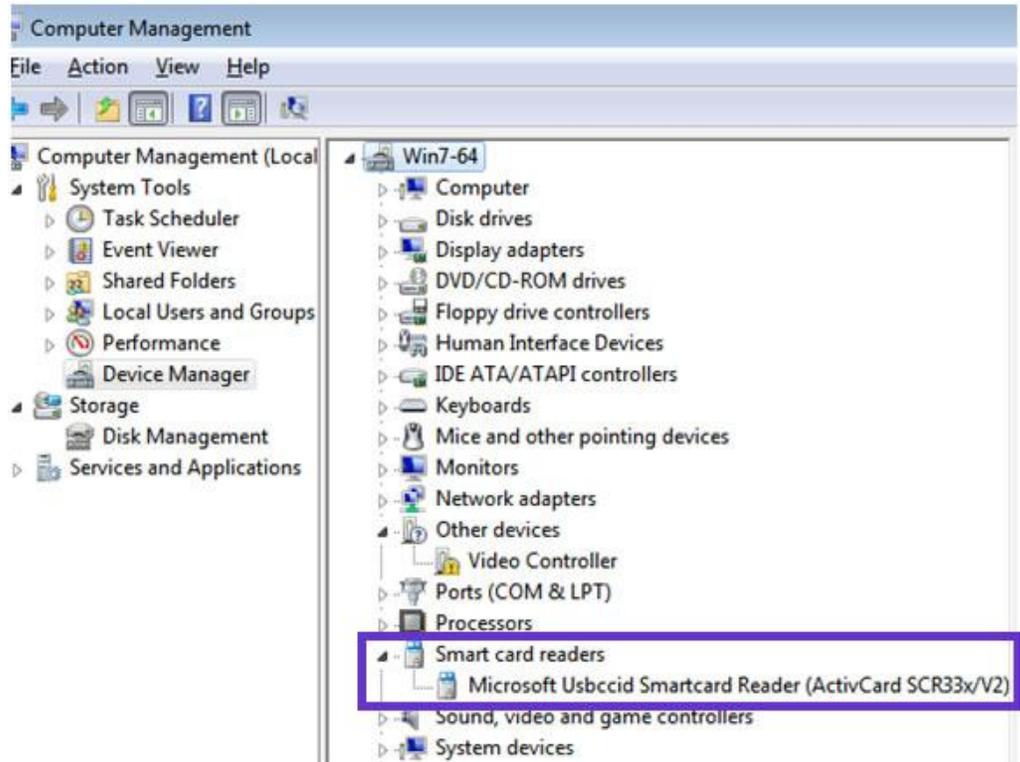
Problem:

Microsoft Windows 7 includes a native capability to read and use the newest CAC-based PKI certificates without installing smart card middleware such as ActivClient (AC). If you have a fully Personal Identity Verification (PIV) II-compliant CAC, you may be able to use your CAC on Windows 7 home machines, to access web sites, without having to install middleware. The following instructions will help you to configure Windows 7 to use a CAC without additional middleware in some cases. **These instructions are not applicable if you already have middleware installed.**

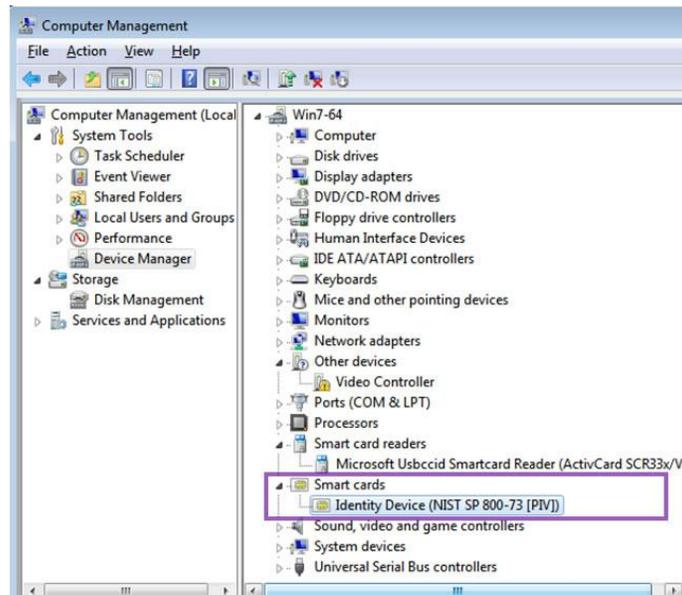
Solution:

NOTE: These instructions are provided as general guidance for home use only. The AF PKI SPO cannot support help desk calls concerning use of CACs on home machines. If these instructions do not work on your system, contact your Client Support Administrator (CSA) to obtain a copy of the ActivClient Home Use Middleware package. The Windows 7 version of home use middleware is estimated to be available February 2010.

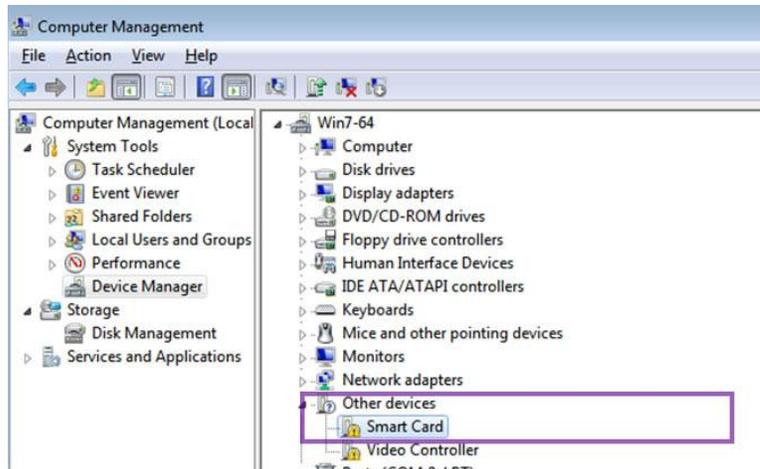
1. Verify that you have a fully PIV-II-compliant CAC. To determine if your card is compliant, check the card type printed on the back of your CAC. If the type is “Gemalto TOP DL GX4 144K” or “Oberthur ID One 128 v5.5 Dual” then the CAC is fully PIV-compliant. If the type is “Gemalto GCX4 72K DI” or “Oberthur ID One V5.2 Dual” then there is a POSSIBILITY that the CAC is fully PIV-II-compliant depending on when and where your CAC was issued. All other card types are not PIV-II-compliant and cannot be used with Windows 7 without additional middleware. To definitively determine if your CAC is PIV-II-compliant, use the following directions (**these directions assume you do NOT have middleware already installed on your machine**).
 - i. Install a card reader on your Windows 7 machine. Verify the card reader is properly installed by checking that a reader is listed in the Device Manager under “Smart card readers”. (The Device Manager can be accessed by opening the Start menu, right-clicking Computer {which may be listed as a computer name}, and selecting “Manage”.)



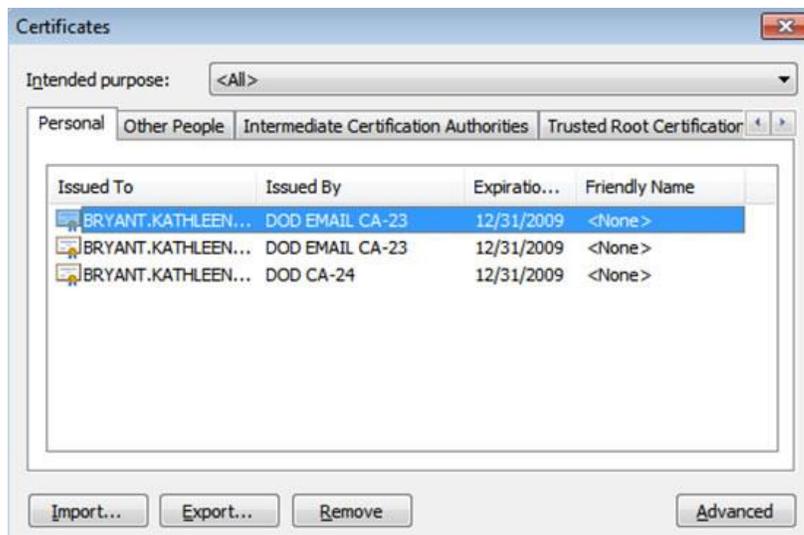
Insert the CAC in the reader. Verify the card reader is successfully recognizing the CAC by checking that an “Identity Device” is listed in the Device Manager under “Smart cards” as shown below. If it is, your CAC may be PIV-II compliant.



If your CAC is not PIV-II-compliant, the smart card will show up under “Other devices” as shown below:



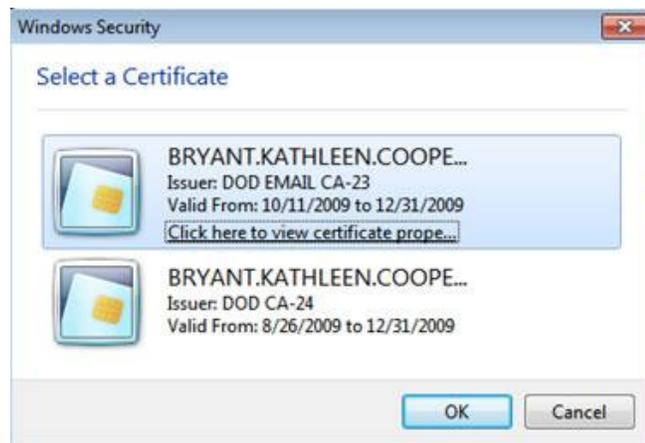
- ii. Open the Internet Explorer (IE) Certificate Store. If you think your CAC is PIV-II compliant, go into IE, select Tools\Internet Options\Content\Certificates. The Personal Tab should open by default. If your CAC is PIV-II-compliant, you should see 3 certificates issued to you by DoD as shown below:



Two of these certificates (the ones that have “EMAIL” in the “Issued By” field) are your standard DoD E-mail Signature and Encryption certificates. The third certificate is your PIV Identity certificate. This PIV Identity certificate is a different certificate than the DoD Identity certificate you normally see when using ActivClient middleware. This should not impact your Home Use operations. If your CAC is not PIV-II-compliant, no certificates will be listed in the Personal Tab. You will have to install the ActivClient 6.2 middleware Home Use Package (expected availability February 2010) in order to use your CAC with Windows 7.

NOTE: if you suspect you do not have a PIV-II compliant card DO NOT request a new card. Fully PIV compliant CACs will be issued via normal attrition. If your card type is “Gemalto GCX4 72K DI” or “Oberthur ID One V5.2 Dual” then there is a possibility that it can be made PIV-II compliant by using the User Maintenance Portal/Post Issuance Portal (UMP/PIP) and selecting the “[PIV Update](#)” option. UMP/PIP will tell you at that point if the card cannot be updated. See your CSA for assistance with UMP/PIP.

2. Install the DoD PKI Trust Chains. Access the DOD Root CA Download web page (<http://dodpki.c3pki.chamb.disa.mil/rootca.html>) and follow the directions on the page to install all of the trust chains on your Windows 7 machine.
3. Add Outlook Web Access (OWA) address to IE8 Trusted Sites (for OWA users only). The OWA website must be listed as a trusted site in order for the user to sign or decrypt email. Open IE8 and select Tools\Internet Options\Security. Select the Trusted Sites zone, then click on “Sites”. Type the address for your OWA website (for example: <https://lackland.mail.us.af.mil/owa>) in the box labeled “Add this website to the zone” and click Add. The site will be added to the list. Click Close and then OK to exit the Internet Options window.
4. Access web sites and authenticate with your CAC-based certificates in IE as usual. You will be prompted to select a certificate and enter your Personal Identification Number (PIN) as shown in the screenshots below. **IMPORTANT:** If you are accessing a web site that is linking back to your network account as Sharepoint or Outlook Web Access (OWA), you may need to select your E-mail Signature certificate (the one that has “EMAIL” in the Issued By field) in order to authenticate. The PIV Identity certificate (the one that does NOT have “EMAIL” in the “Issued By” field) will not work with your Active Directory account (any use that connects back to your work account, like Sharepoint or OWA) unless you have used LEAP with this particular CAC to populate your ID Certificate information. Your PIV Identity certificate can always be used to client authenticate to web sites that are not linking back to your network account.



5. If you are having issues accessing a web site with your CAC, try the following:
 - i. Add the web site to the IE "Trusted Sites" list (in IE under Tools\Internet Options\Security).
 - ii. Open the IE Certificate Store by selecting Tools\Internet Options\Content\Certificates. For each of your certificates in the Personal tab, highlight the certificate and click the "Advanced" button. From within the Advanced Options configuration window select the checkbox for "Client Authentication" then click OK. (These settings are normally NOT required to use the CAC certificates with Windows 7).
 - iii. In the IE Internet Options window select the Advanced tab. In the Settings box, scroll to the Security section and verify that the checkboxes for TLS 1.0 and SSL 3.0 are checked.

If, after following these instructions, you are unable to get your CAC to work, contact your CSA and request the ActivIdentity Home Use middleware package (estimated availability February 2010).