



CAC Reader End-User Set-Up Guide

Overview

This document will explain how to set-up your Common Access Card (CAC) to work within the Coast Guard's Standard Image.

CAC's will be used by the Coast Guard and DOD entities to ensure secure access to web pages, verify user credentials for message drafting and release, and possibly eventually sign-on access to your workstation. CAC Cards are replacing old style Military ID cards as the primary means of personnel identification. When the CAC Card is issued it comes with 3 Certificates. An Identification Certificate, an Encryption Certificate and a Signature Certificate are loaded on your CAC Card. These Certificates must be known to your system and properly set up to be used.

Before you can proceed you will need a personal CAC Card and a Standard Coast Guard CAC Card Reader attached to your workstation (either a stand-alone reader or an integrated keyboard reader). Your ESU or supporting IT Staff will also need to install some software on your workstation to enable the CAC Card Reader hardware to be recognized by your computer. Once this is accomplished you may proceed with this document. **The procedures in this document do not require administrative privileges.**

Section 1 - Registering Your Certificates

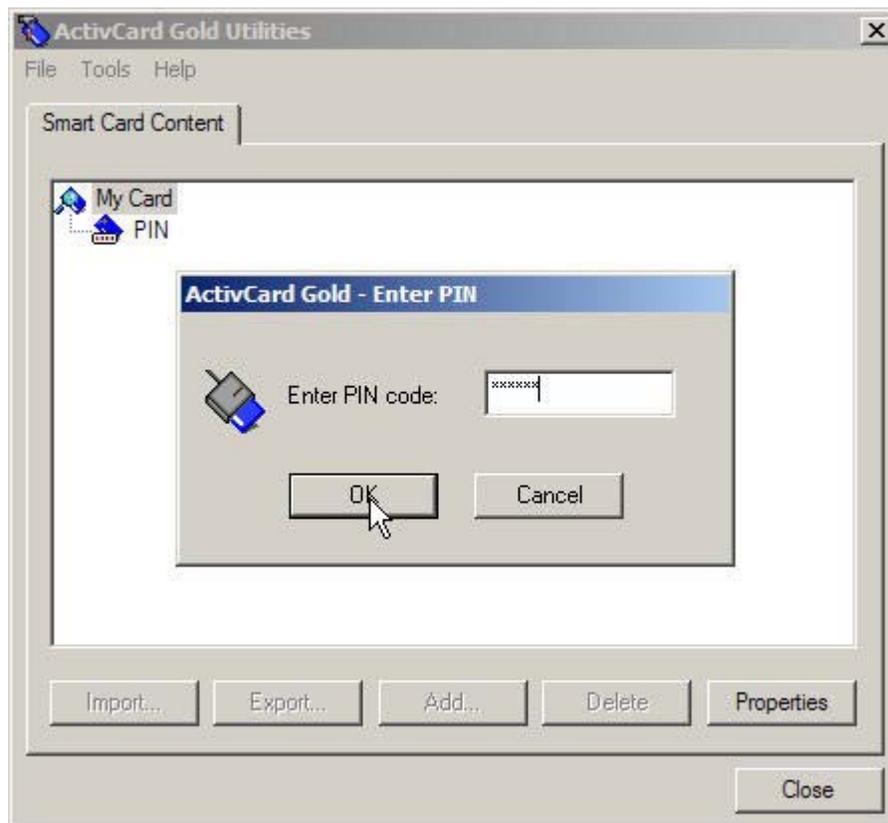
In order for the system to recognize your CAC Card and correctly access you certificates you must do the following.

1. Double-click on the ActivCard icon. (Lower right hand corner of your Desktop next to the clock).
2. Place your CAC into your reader.



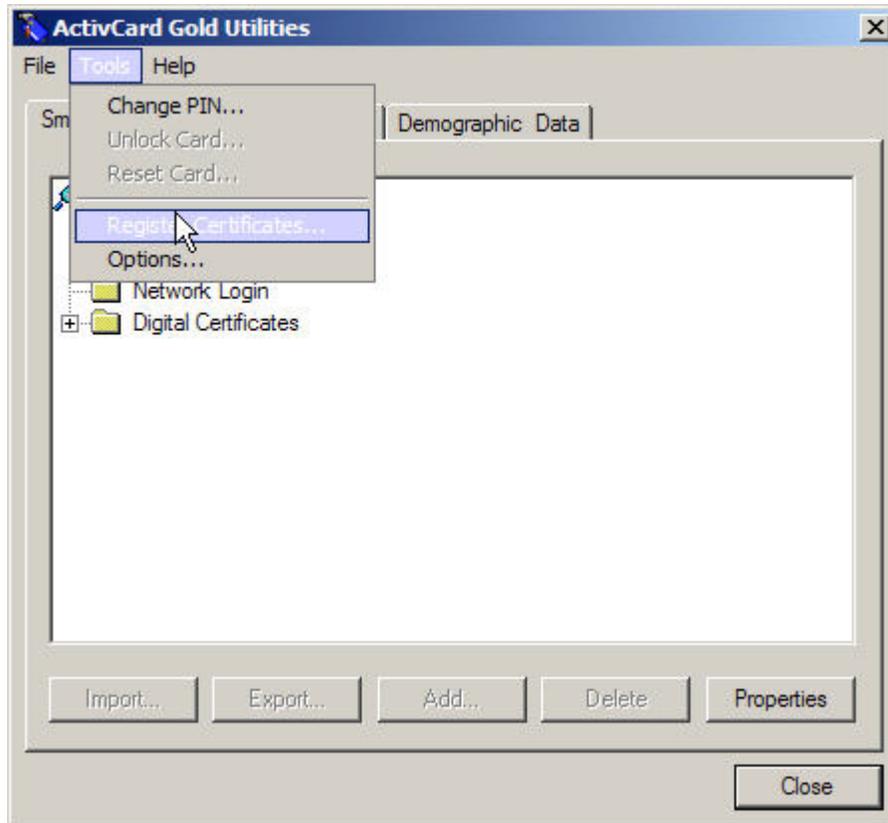
NOTE: If you do not see the icon pointed out in #2 above, your system may have minimized or hidden it to present a more User friendly visual experience. Look to the left side of the system tray box for a set of double arrows (<<). Clicking on that will reveal all icons/services running on your system. If the icon is still not present you should contact your ESU/Admin support. It is likely the proper software has not been loaded on your system.

3. After Double-Clicking on the icon, the following window will appear, enter the PIN that you selected when you received your CAC.

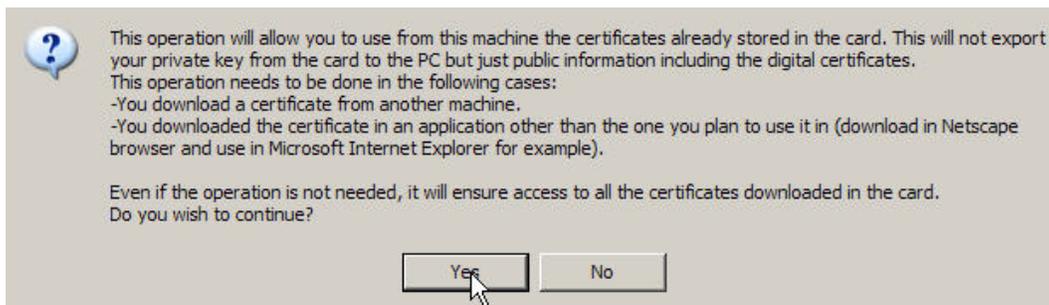


NOTE: BE VERY CAREFUL WHEN ENTERING YOUR PIN!! If you enter an incorrect PIN 3 times, your CAC will lock you out and **you will have return to the facility that issued you your CAC or another Verification Officer (VO) in order to regain access to your CAC.**

4. After correctly entering you PIN, you will see the following **ActiveCard Gold Utilities** window. From the menu at the top, click on **Tools** then **Register Certificates...**

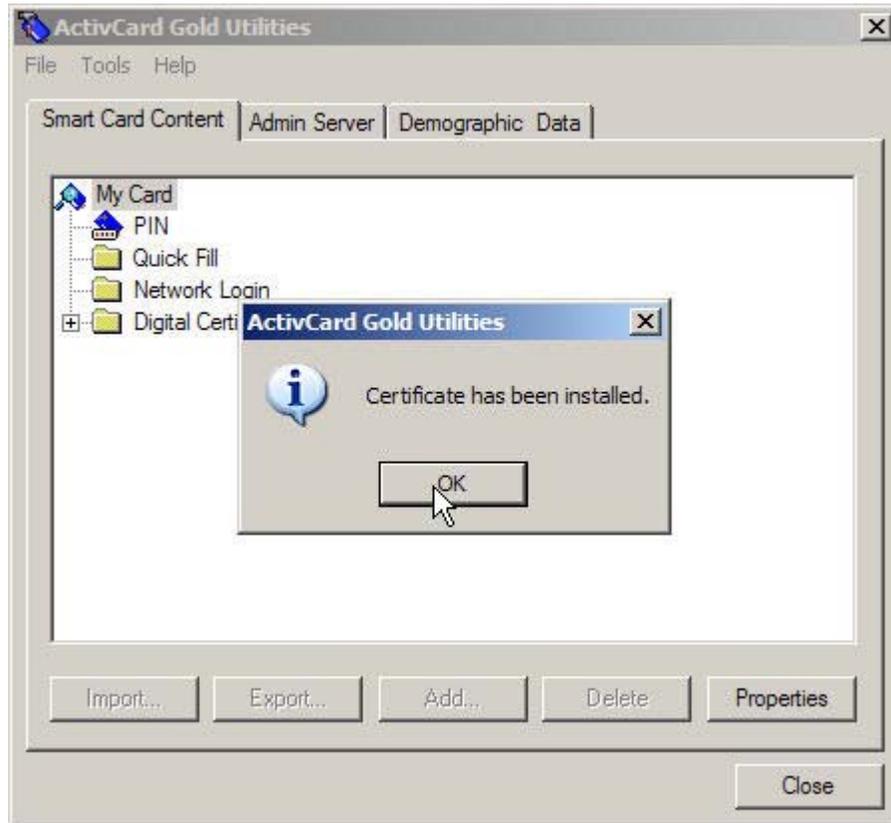


5. When you see the following information screen, read it and then click **Yes**.

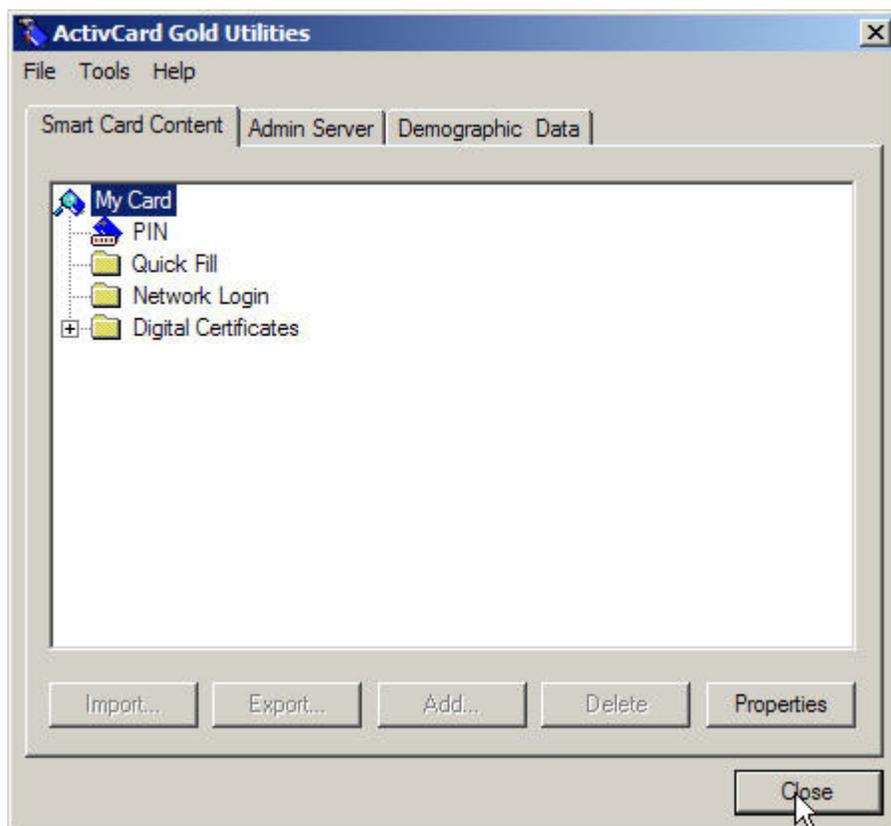


NOTE: This will place a shortcut in your Personal Certificate Store which points to the certificates embedded on your CAC card. If you do not complete this step, no programs in windows will know how to get to your certificates.

6. After the Certificates have been loaded, you will see the window below confirming that they have been installed. Click **OK**.



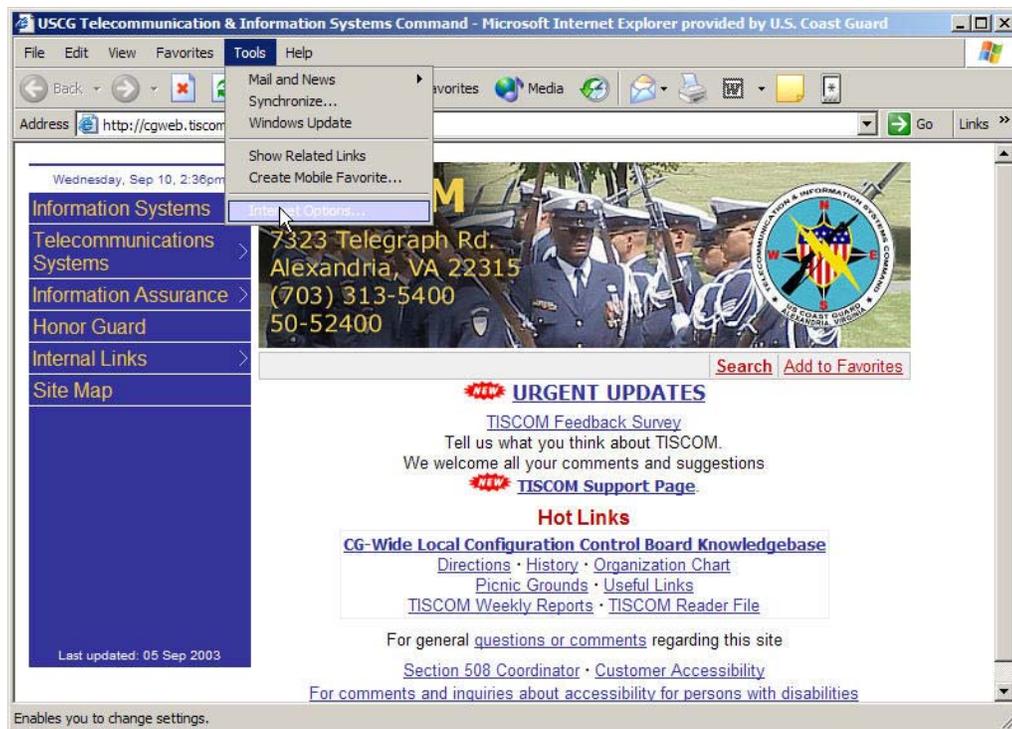
You will then see the window below. You have completed installing your Certificates. Click **Close**.



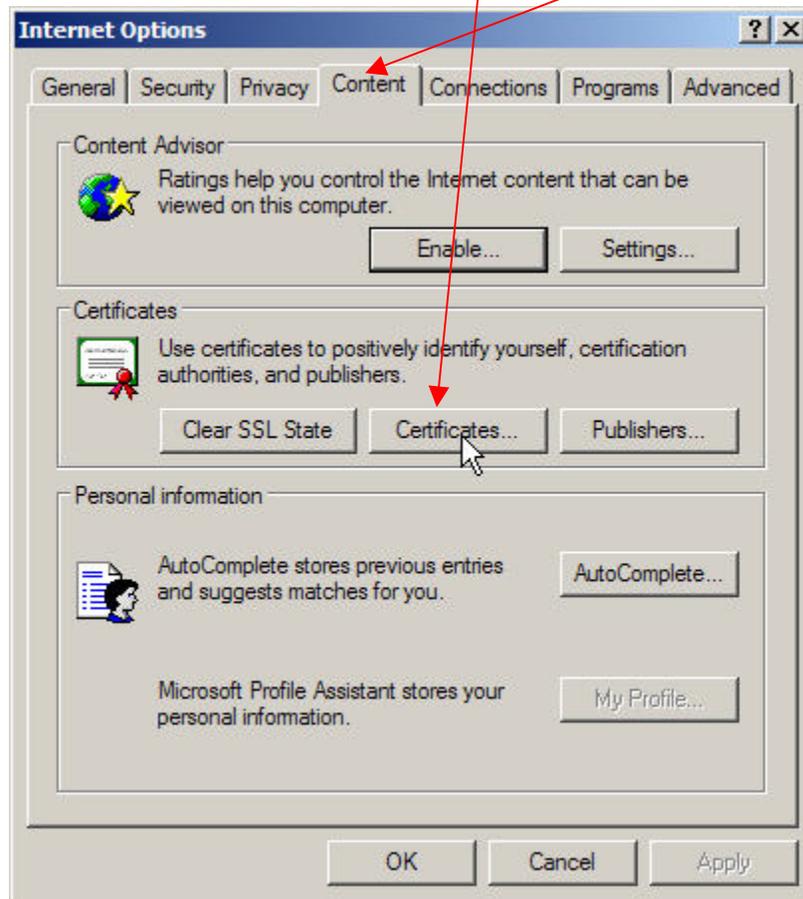
Section 2 - Enabling Client authentication Within Internet Explorer

In order to gain access to PKI protected web sites, client authentication must be enabled within Internet Explorer (IE). Enabling this feature allows you to use your CAC to authenticate and gain access to a PKI enabled web site. If this feature remains disabled, you will be unable to gain access to PKI protected sites.

1. First we will verify your Certificates are registered. Start Microsoft Internet Explorer
2. From the menu along the top, Click **Tools** then **Internet Options**.

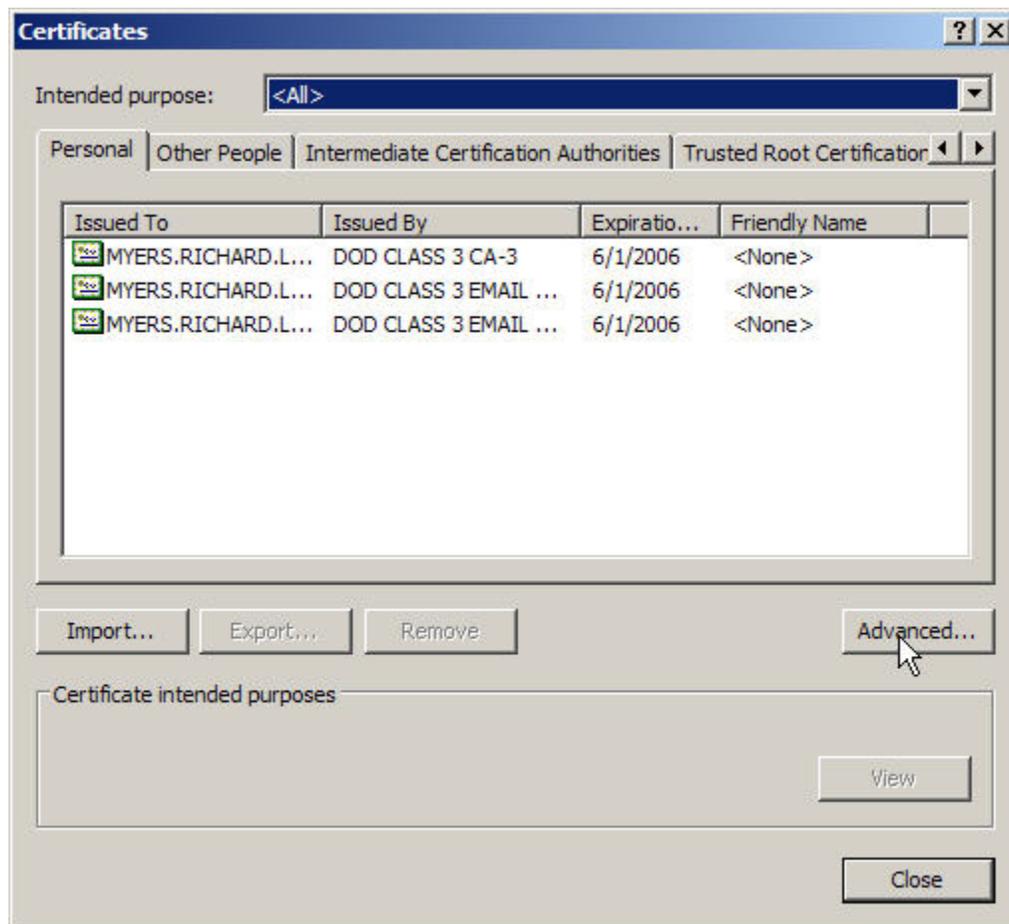


3. After clicking on **Internet Options**, you will see the window below. Click on the **Content** Tab at the top of the window, and then click the **Certificates** button in the middle of the window.

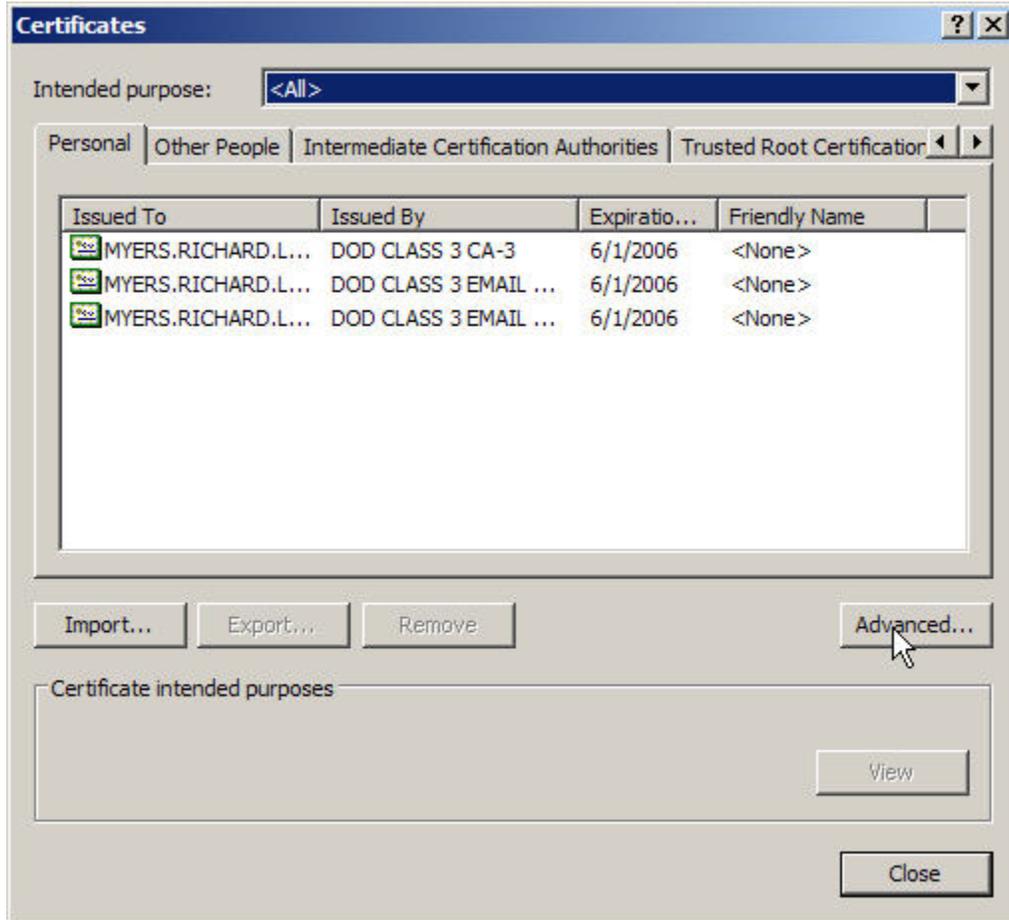


4. If you properly completed the **Section 1 - Registering your Certificates** procedure, then you will see your three certificates as on this screen below.

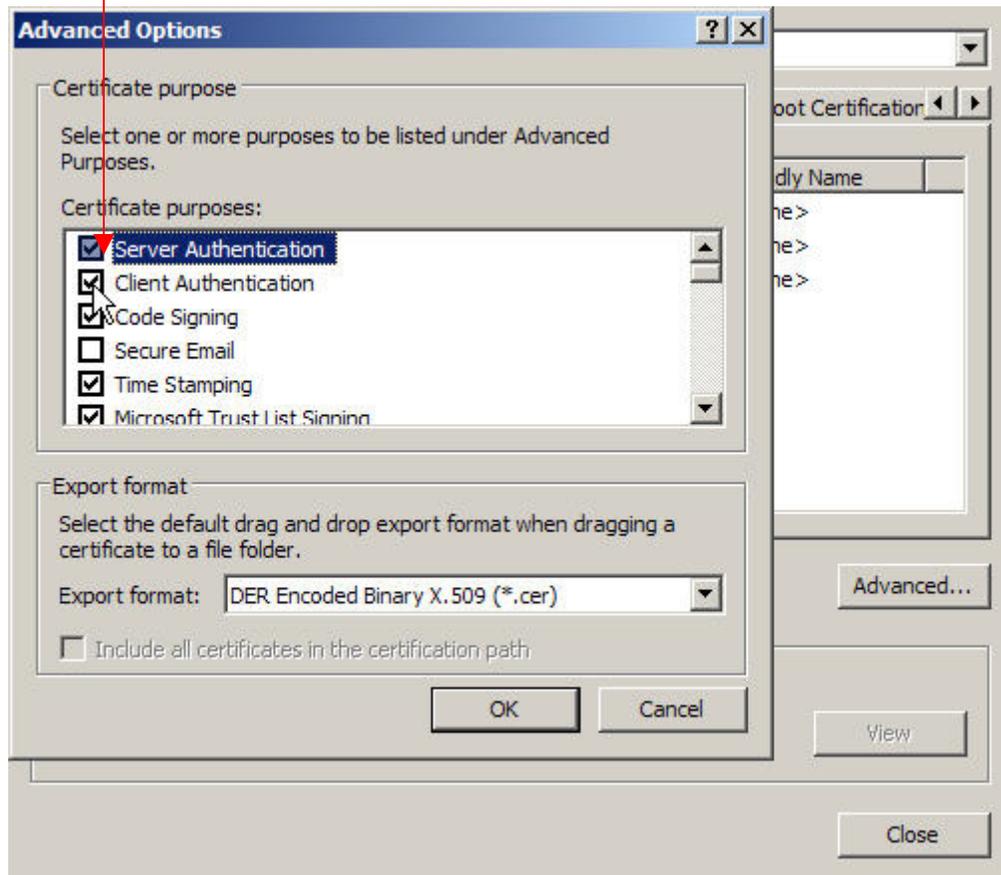
NOTE: If you do not see all 3 Certificates on this screen you will need to revisit a DEERS/RAPIDS issuance office and have your CAC updated. Inform the Yeoman at the office that your CAC has been incorrectly issued and needs to be updated with all three PKI Certificates. They will know how to proceed. (It usually means an E-Mail address was not registered in the original application.)



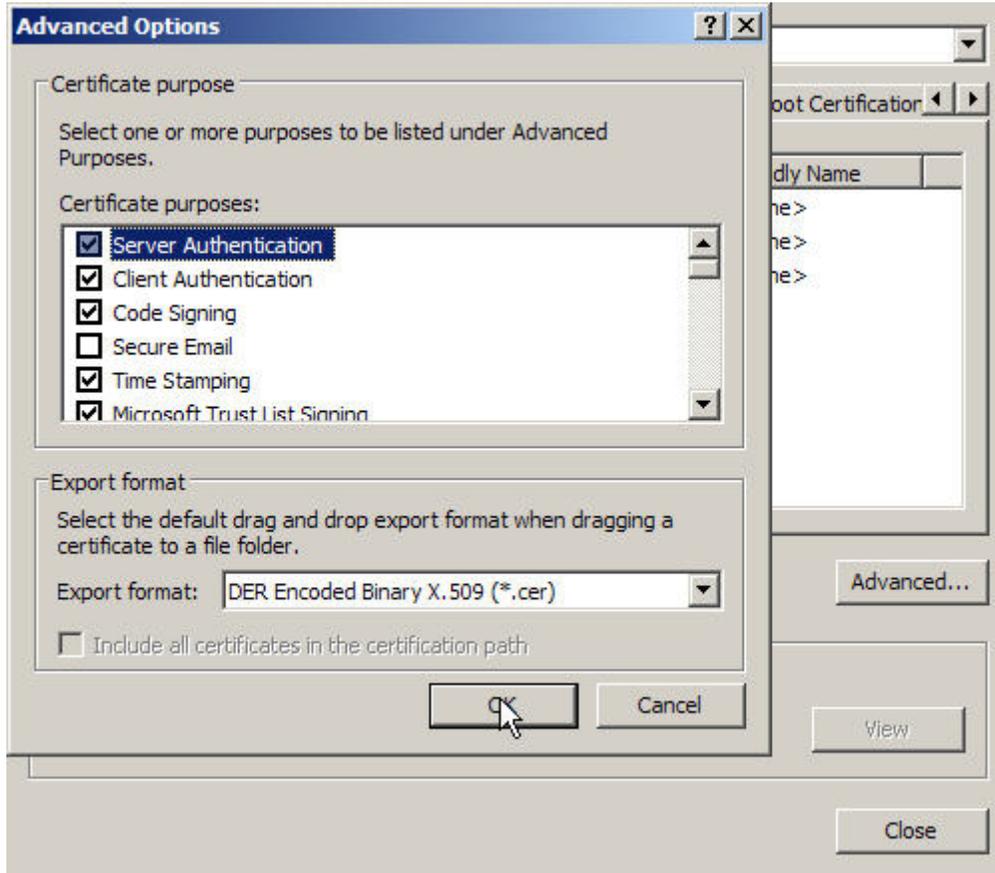
5. Click the **Advanced** Button.



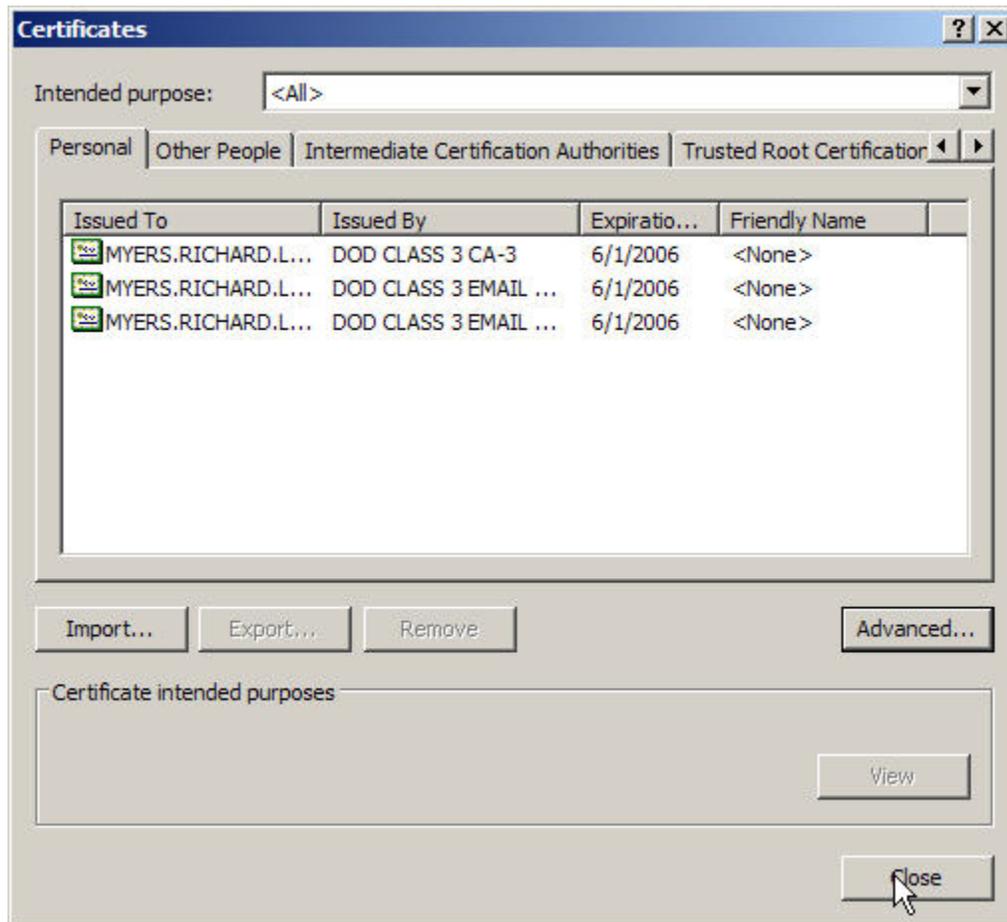
6. The **Advanced Options** window will appear. Check the box next to **Client Authentication**.



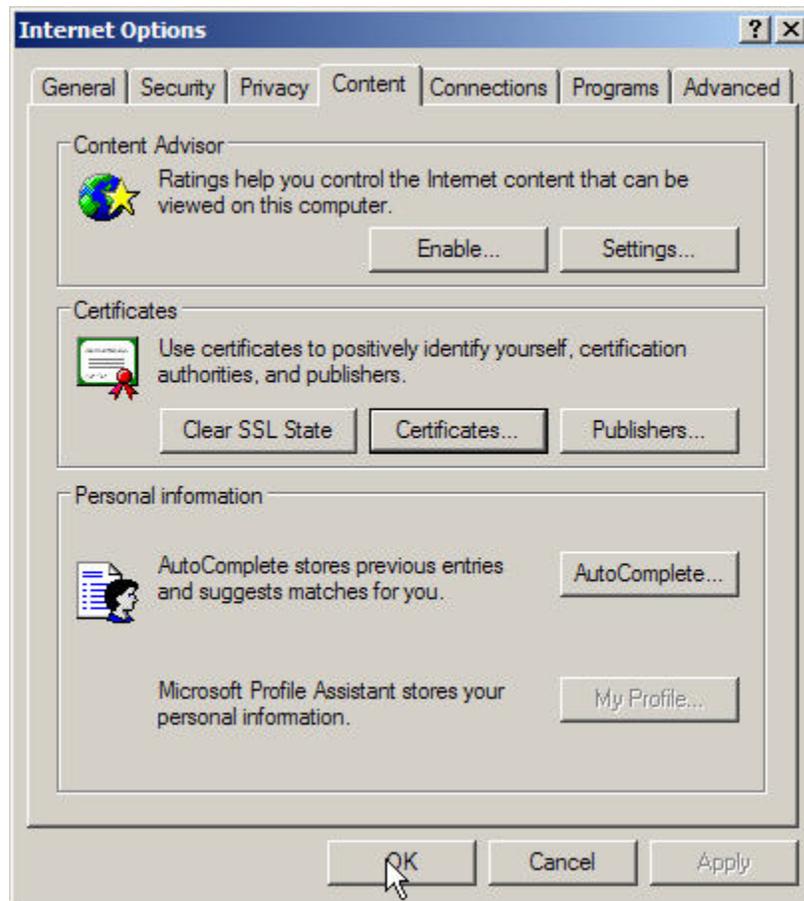
8. Click **OK**. This will take you back to the Certificates window.



9. Click **Close**. You will be back at the **Internet Options** window.



10. Click **OK**. You have enabled Client Authentication in Internet Explorer.



Section 3 - Enabling Digital Signatures within Outlook

Digital Signatures within Outlook should not be configured at this time. We will issue this procedure at a future date.

This completes the set-up of your Certificates (**Section 1**) and Configuration of Internet Explorer for Secure Web Page Access (**Section 2**).

--- End of Document ---