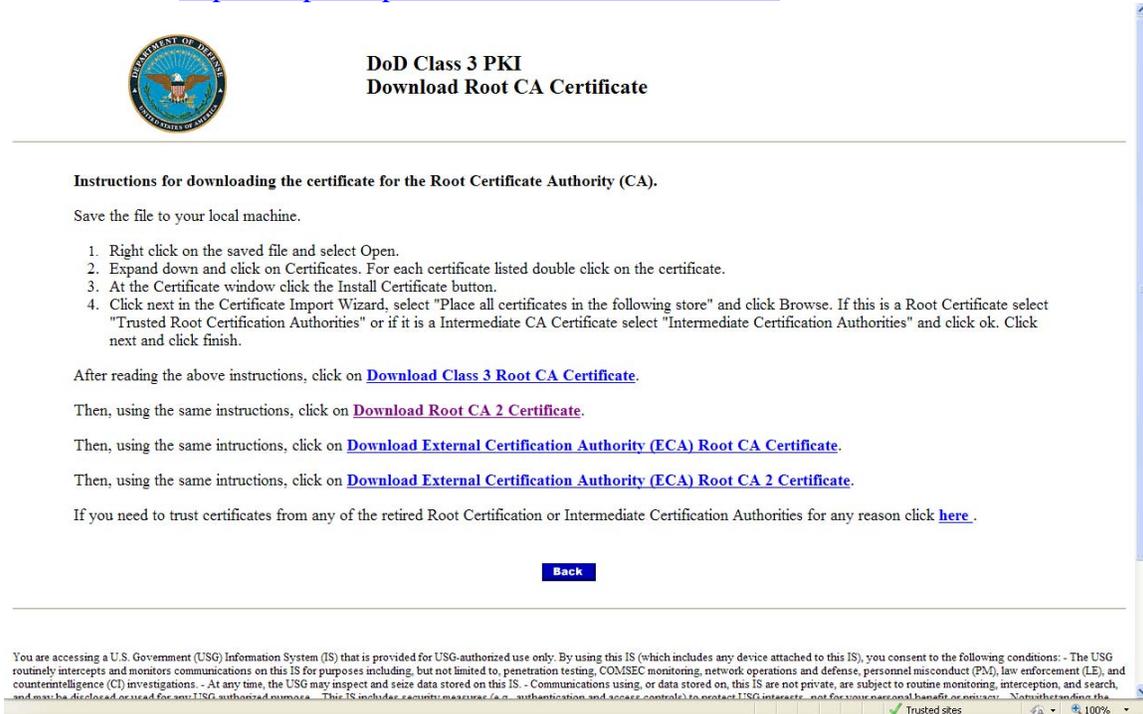


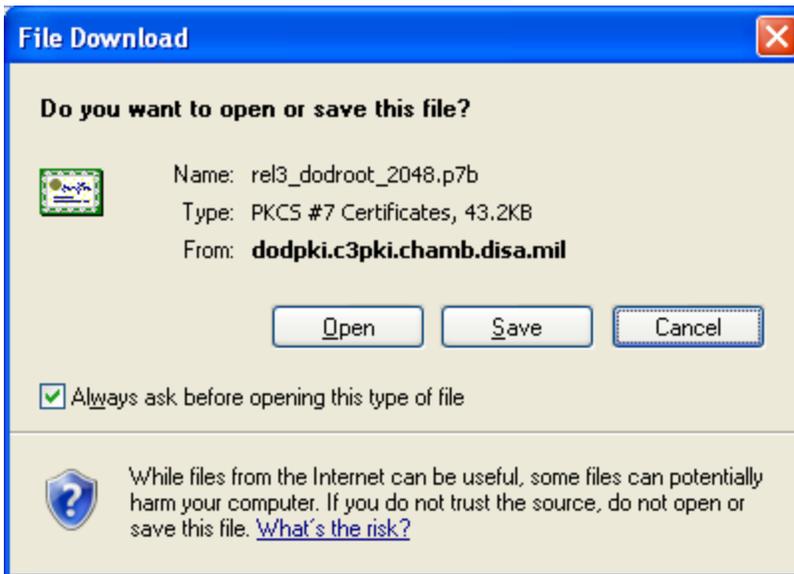
To Install the ENROL Security Certificate, please do the following:

1. Go to <http://dodpki.c3pki.chamb.disa.mil/rootca.html>



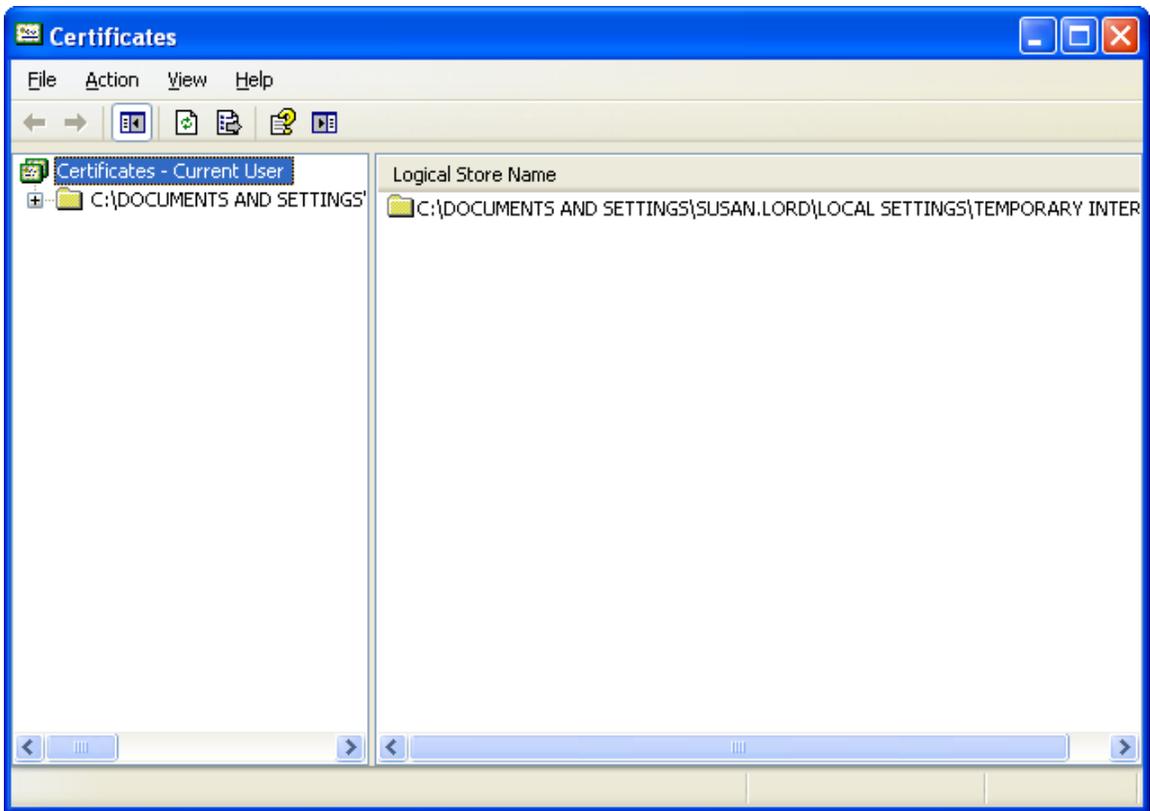
The screenshot shows a web page titled "DoD Class 3 PKI Download Root CA Certificate". On the left is the Department of Defense seal. The main content area contains instructions for downloading the certificate for the Root Certificate Authority (CA). The instructions include: "Save the file to your local machine.", a numbered list of steps (1. Right click on the saved file and select Open. 2. Expand down and click on Certificates. For each certificate listed double click on the certificate. 3. At the Certificate window click the Install Certificate button. 4. Click next in the Certificate Import Wizard, select "Place all certificates in the following store" and click Browse. If this is a Root Certificate select "Trusted Root Certification Authorities" or if it is a Intermediate CA Certificate select "Intermediate Certification Authorities" and click ok. Click next and click finish.), and several download links: "Download Class 3 Root CA Certificate", "Download Root CA 2 Certificate", "Download External Certification Authority (ECA) Root CA Certificate", and "Download External Certification Authority (ECA) Root CA 2 Certificate". There is also a link "here" for retired Root Certification or Intermediate Certification Authorities. A "Back" button is located at the bottom of the instructions. At the very bottom of the page, there is a disclaimer: "You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: - The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. - At any time, the USG may inspect and seize data stored on this IS. - Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose. - This IS includes certain measures (e.g., authentication and access controls) to protect USG interests, not for your personal benefit or privacy. - No other terms apply." The browser status bar shows "Trusted sites" and "100%" zoom.

2. Click "Download Root CA 2 Certificate."

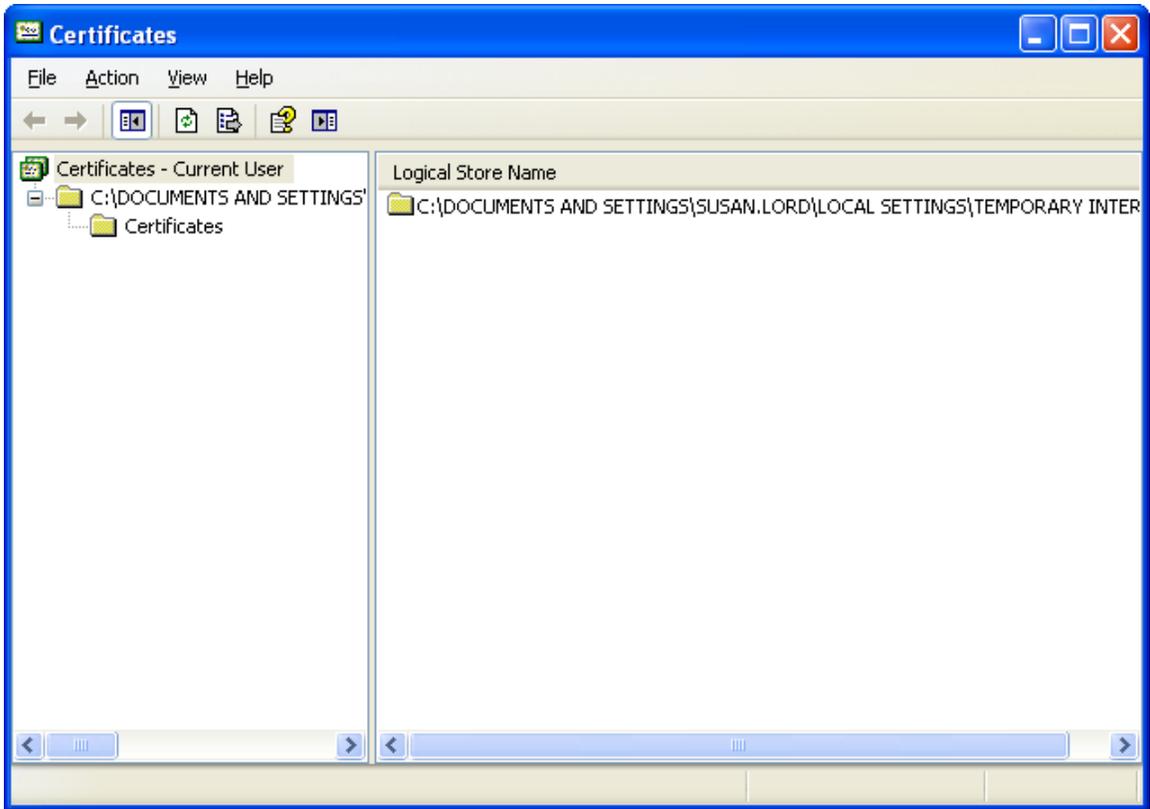


The screenshot shows a "File Download" dialog box. The title bar says "File Download" with a close button. The main text asks "Do you want to open or save this file?". Below this, there is a small icon of a certificate, the file name "rel3_dodroot_2048.p7b", the type "PKCS #7 Certificates, 43.2KB", and the source "From: dodpki.c3pki.chamb.disa.mil". At the bottom, there are three buttons: "Open", "Save", and "Cancel". Below the buttons, there is a checkbox labeled "Always ask before opening this type of file" which is checked. At the very bottom, there is a warning icon (a question mark in a shield) and the text: "While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. [What's the risk?](#)"

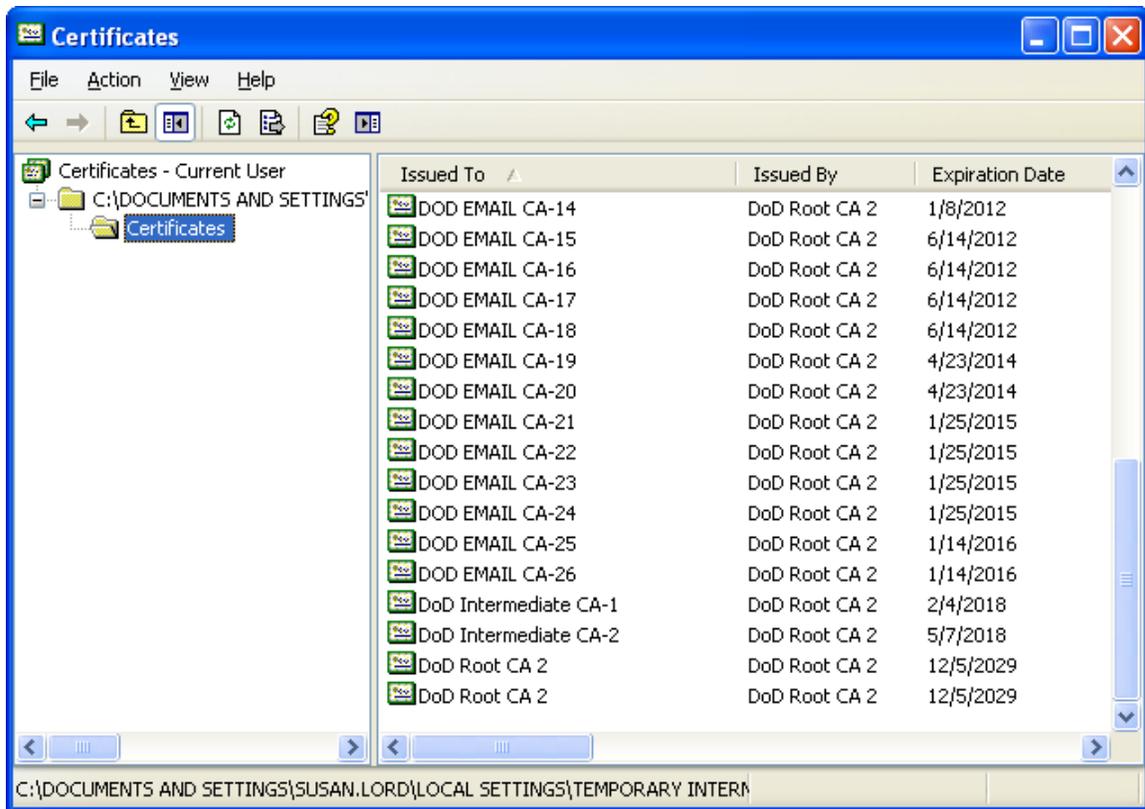
3. Click **Open**. The below screen will display:



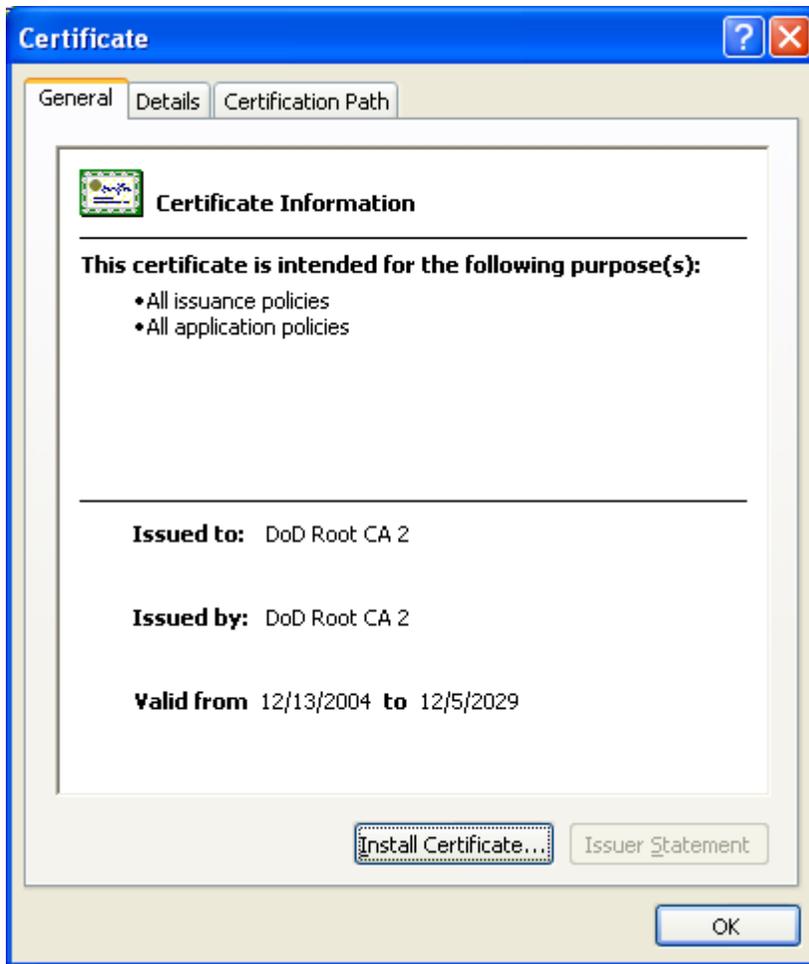
4. Click the plus sign to open the “C:\Documents and Settings...” folder.



5. Click “Certificates.”



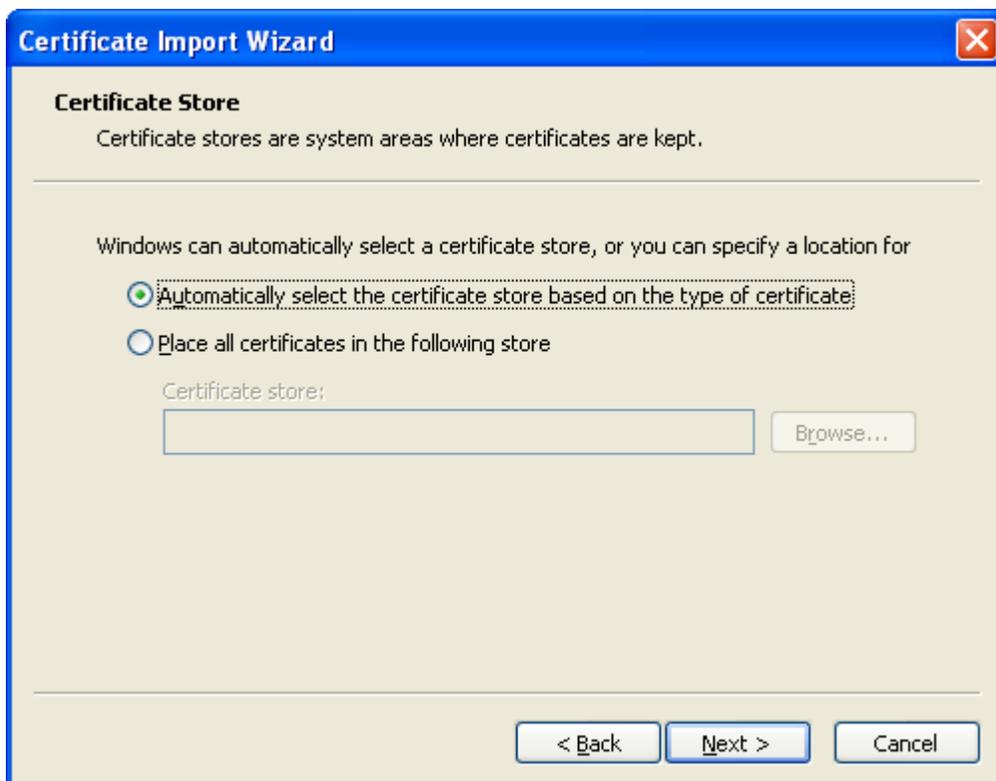
6. Scroll to the bottom of the list and you will see “DoD Root CA2.” Double click this certificate.



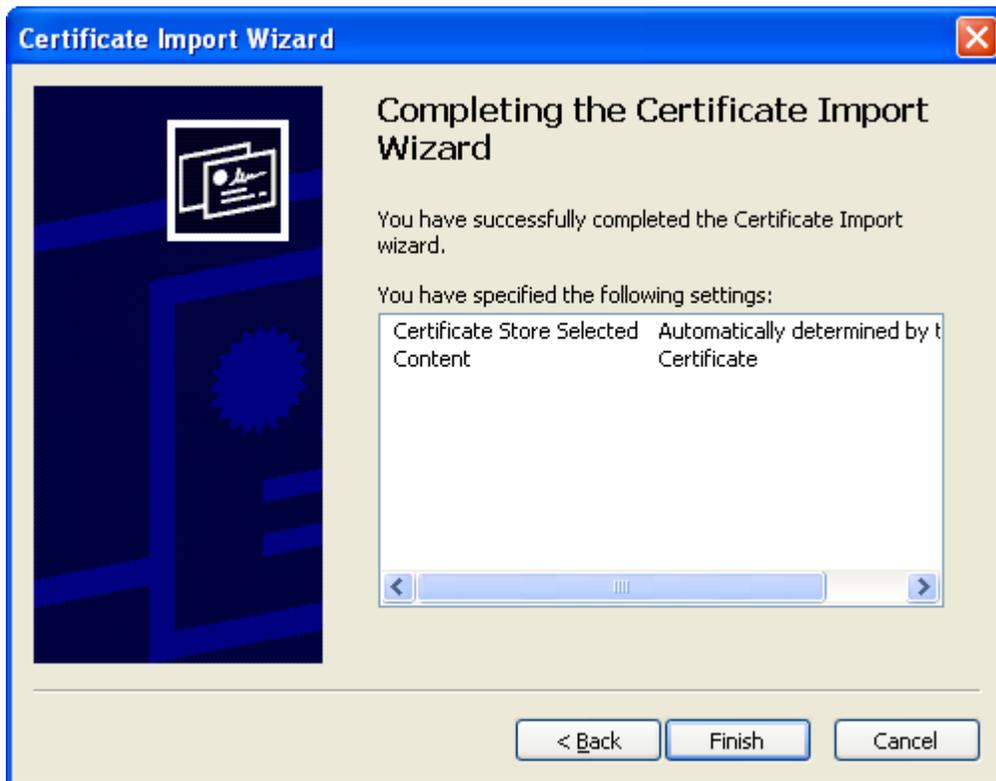
7. Click **Install Certificate**.



8. Click **Next**.



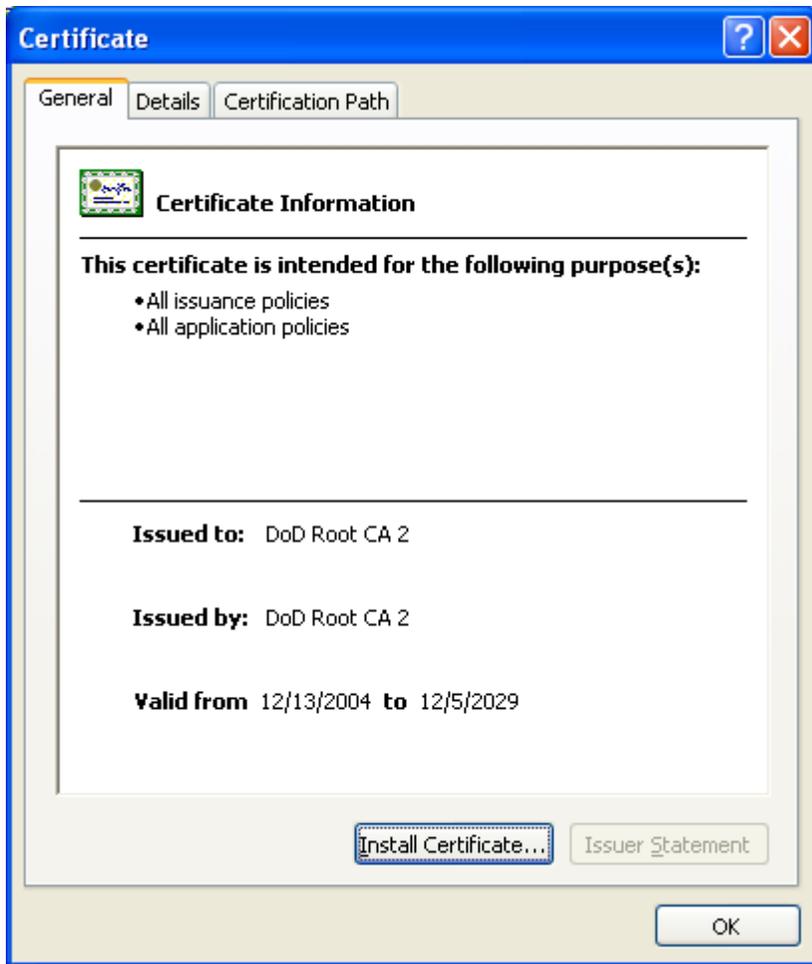
9. Select “Automatically select the certificate stored based on the type of certificate” and click **Next**.



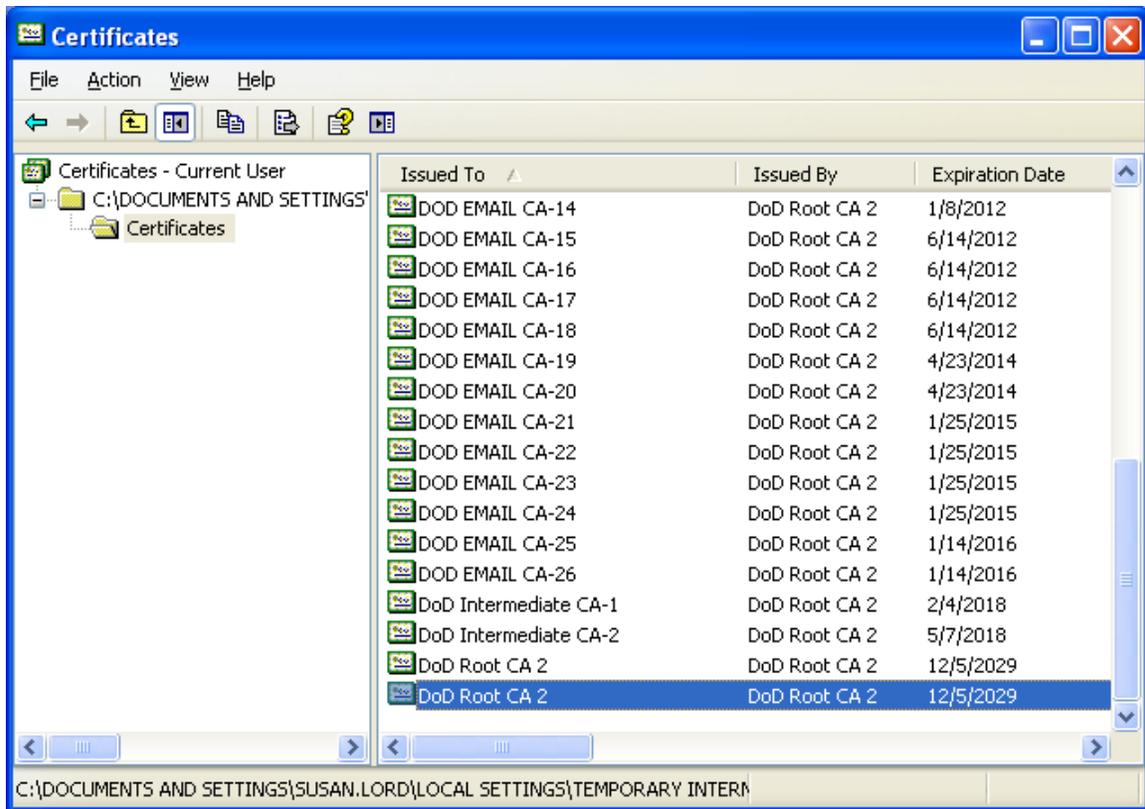
10. Click **Finish**.



11. Click **OK**.



12. Click **OK**.



13. Click the red **X** to close the Certificates window.

14. You should now be able to access [ENROL](#).