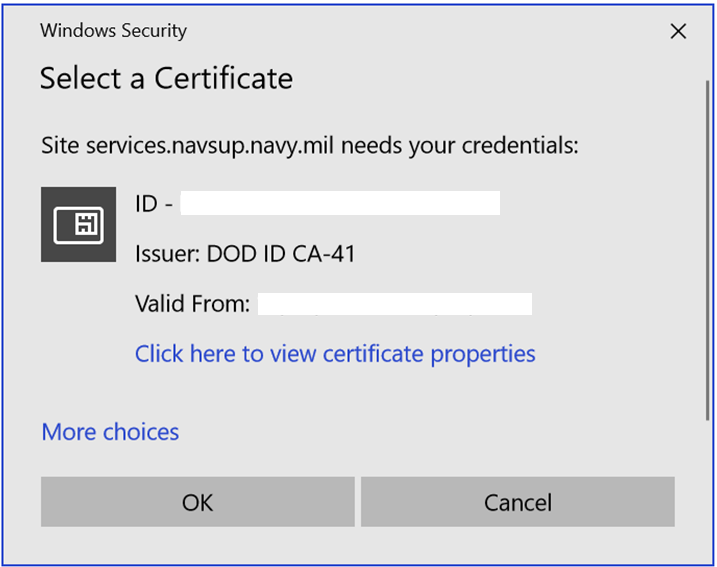
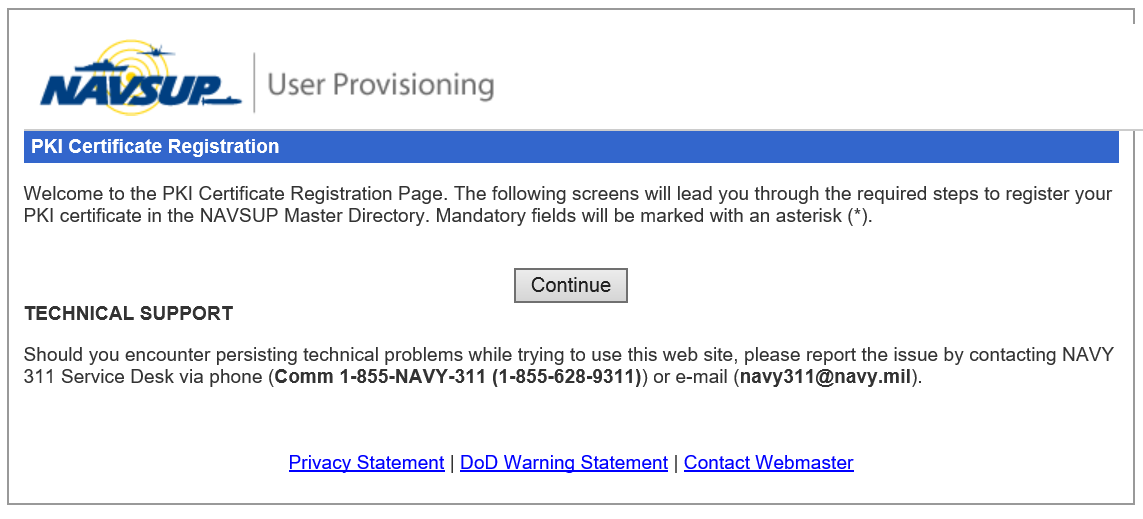
**Registration Steps with Screen Shots:**

Access Registration at <https://www.navsup.navy.mil/registration>



**Note:** If you do not see ID as part of the name displayed in your ‘Issuer’ field, click on ‘More Choices’ to allow you to see all of your associated certificates, and select your ID certificate.

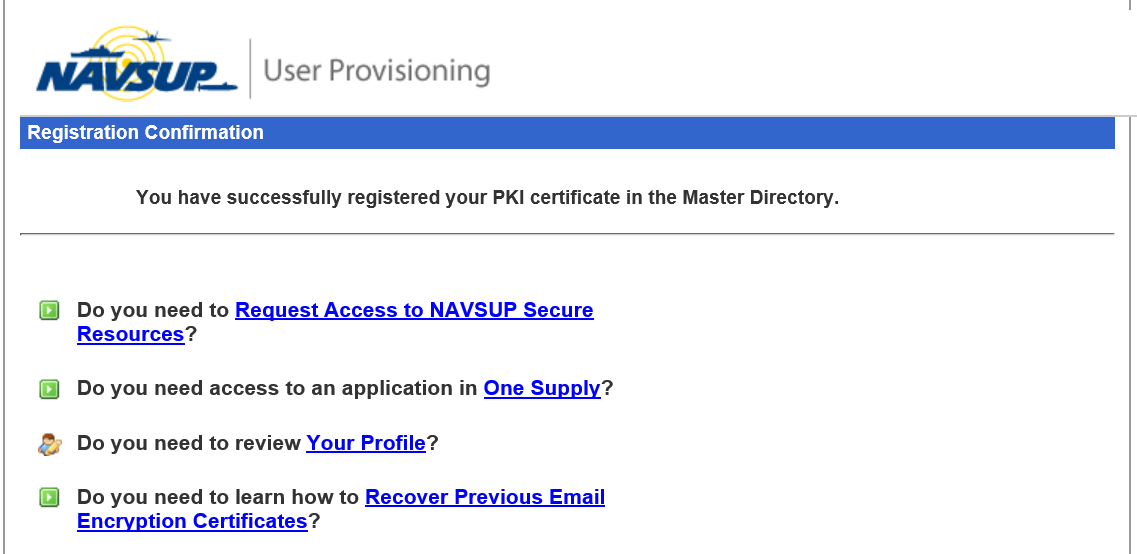
After clicking ‘OK’, you will see the following screen:



Click the ‘Continue’ button

Continue through each step, clicking ‘Next’ until you get to the end of the process and ensure that you select ‘Finish’ on the last step to complete the Registration Process.

At this point, you will see:



At this point, you have completed the Registration Process (notice the Successful Registration message).

Unless you need to Request Additional Access, you can close this window and now access any NAVSUP Secure site that you have access to.

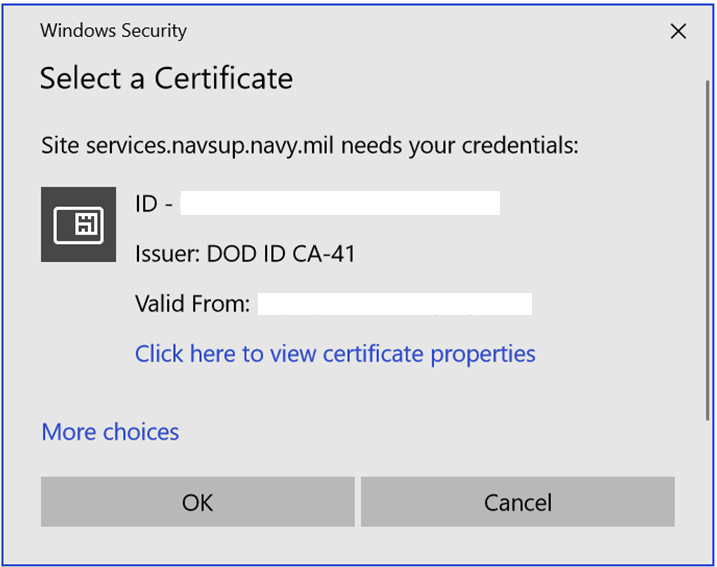
**Certificate You Presented was issued by an Unknown Certificate Authority (CA):**

User is trying to register their certificate and is receiving the following:

"This application has experienced an unexpected fatal error. The details of the error are as follows:

The certificate you presented was issued by an unknown Certificate Authority (CA). Only certificates that have been issued by a trusted CA can be registered in this directory. If you know for certain that you have presented a valid DoD PKI or IECA/ECA certificate, please report this issue by contacting the NAVSUP Consolidated Helpdesk."

1. Ensure you have a registered certificate. If unsure, go to <https://www.navsup.navy.mil/registration> and when prompted, select your ID certificate and NOT your Email certificate.



**Note:** If you do not see your ID certificate populated in your certificate window, click on the ‘More Choices’ link to display all of your available certificates.

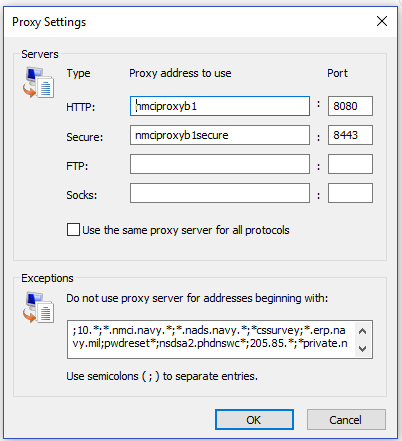
2. The error that you are reporting is the result of an incorrect certificate being selected when prompted, during the Registration process.

Please ensure that you select your ID certificate and NOT your Email certificate (which will give you the reported error).

**Going to Main page and not Being Prompted for Certificate:**

Modify Your Proxy Settings in IE:

Go to IE > Tools > Internet Options > Connections > LAN Settings > Advanced



Down in the Exception List area, we are suggesting that you copy all the sites that are listed in there into a word document, then go into that word document and look for my.navsup.navy.mil

and remove it from the list. Delete all entries out of your exception list so that it is empty and then take the list and copy it all back into your exception list area (without the my.navsup.navy.mil) in it.

Another way you can do this is to just look for my.navsup.navy.mil within the list in your exception list and carefully delete it, so whichever is easier for you.

**Note:** If you do not have the rights to make the above-mentioned modifications, you may need to have your Local Desktop Support Personnel to make them for you.

**If not being prompted for your certificate**, are your DOD ROOT Certificates loaded in your browser?

To verify, go to IE internet options>content>certificates>intermediate certificate authorities, do you have DoD CA-2 to DoD CA-3? You will need to scroll down through list since these are scattered.

If not, you will need to download the DoD PKI Root Certificates, see below.

\*\*\*Ensure that you see DOD Root CA 3 (expiration date 12/30/2029)

**To Download DoD PKI Root certificates**

Individuals who have a valid authorized need to access DoD Public Key Infrastructure (PKI)- protected information but do not have access to a government site or government-furnished equipment will need to configure their systems to access PKI-protected content.

Accessing DoD PKI-protected information is most commonly achieved using the PKI certificates stored on your Common Access Card (CAC). The certificates on your CAC can allow you to perform routine activities such as accessing OWA, signing documents, and viewing other PKI-protected information online. For more information about your CAC and the information stored on it, visit [http://www.cac.mil](http://www.cac.mil/).

Before you begin, make sure you know your organization’s policies regarding remote use.

For instructions on downloading the DoD Root Certificate, go to

<https://public.cyber.mil/pki-pke/end-users/getting-started/>

Click on the ‘Windows’ dropdown

Step 3 provides guidance on how to install the DoD Root Certificate by using an InstallRoot Setup Wizard.

**Note:** It is suggested that you select the ‘Non Administrator’ option

**Note:** If you do not have the rights to make the above-mentioned modifications, you may need to have your Local Desktop Support Personnel make them for you.

**Note:** There is also a link for the InstallRoot 5.2: User Guide further down on the page

Once installed:

Verify that at a minimum, DOD Root CA 2 and DOD Root CA 3 is installed on your Trusted Root Certification Authorities tab

(Go to IE>Settings>Internet Options>Content> Trusted Root Certification Authorities tab)

Close browser and try to access the website that you were having problems with.

**There is a problem with the website's security certificate" error Problem:**

You are receiving error that says "there is a problem with the website's security certificate" error accessing a NAVSUP webpage, or youi can't access the PKI registration site <https://www.navsup.navy.mil/registration> (at all).

Normally the user is on a non-NMCI computer (such as a vendor).

**Solution:**

\*\*Someone with Admin rights may need to run this install\*\*

**To Download DoD PKI Root certificates**

Individuals who have a valid authorized need to access DoD Public Key Infrastructure (PKI)- protected information but do not have access to a government site or government-furnished equipment will need to configure their systems to access PKI-protected content.

Accessing DoD PKI-protected information is most commonly achieved using the PKI certificates stored on your Common Access Card (CAC). The certificates on your CAC can allow you to perform routine activities such as accessing OWA, signing documents, and viewing other PKI-protected information online. For more information about your CAC and the information stored on it, visit [http://www.cac.mil](http://www.cac.mil/).

Before you begin, make sure you know your organization’s policies regarding remote use.

For instructions on downloading the DoD Root Certificate, go to

<https://public.cyber.mil/pki-pke/end-users/getting-started/>

Click on the ‘Windows’ dropdown

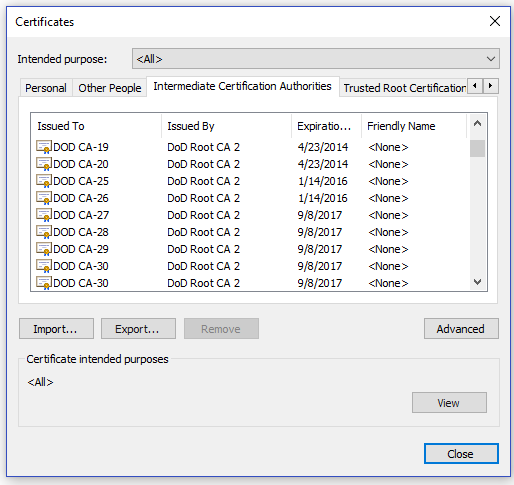
Step 3 provides guidance on how to install the DoD Root Certificate by using an InstallRoot Setup Wizard.

**Note:** It is suggested that you select the ‘Non Administrator’ option

Once installed:

Verify that at a minimum, DOD Root CA 2 and DOD Root CA 3 is installed on your Trusted Root Certification Authorities tab, see screenshot below:

(Go to IE>Settings>Internet Options>Content> Trusted Root Certification Authorities tab)



Close browser and try to access the website that you were having problems with.

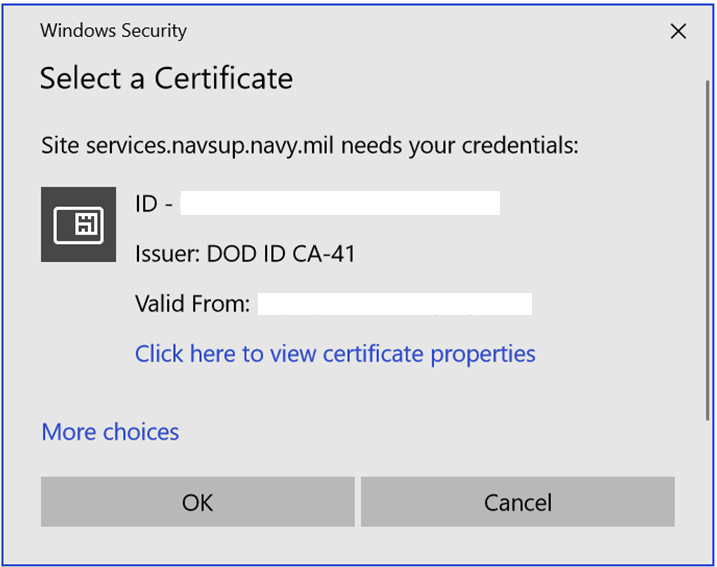
**Invalid PKI Certificate Error – When attempting to Register:**

Unable to register PKI certificate on NAVSUP Registry – Error- Invalid PKI Certificate

Ensure that you have a registered certificate.

If unsure, go to register at https://www.navsup.navy.mil/registration

You should get prompted to select your certificate, make sure you select your ID certificate.



**Note:** If you are not prompted, the first certificate in the list will be used and that is the email certificate and this can cause this error.

**Note:** If you do not see ID as part of the name displayed in your ‘Issuer’ field, click on ‘More Choices’ to allow you to see all of your associated certificates, and select your ID certificate

If you are not getting prompted for your certificate, do the following:

* Open Internet Explorer
* Tools
* Internet Options
* Content
* Click on ‘SSL state’

Then retry accessing the registration site

**Locked Certificate:**

If you are reporting that you are getting a message that your certificate is locked, it probably happened because you entered the incorrect PIN number too many times.

Resolution: You will need to contact your CAC Office to have your PIN reset

**‘Account Disabled’ error:**

\*\* issue normally exists if user has multiple PKI certificates

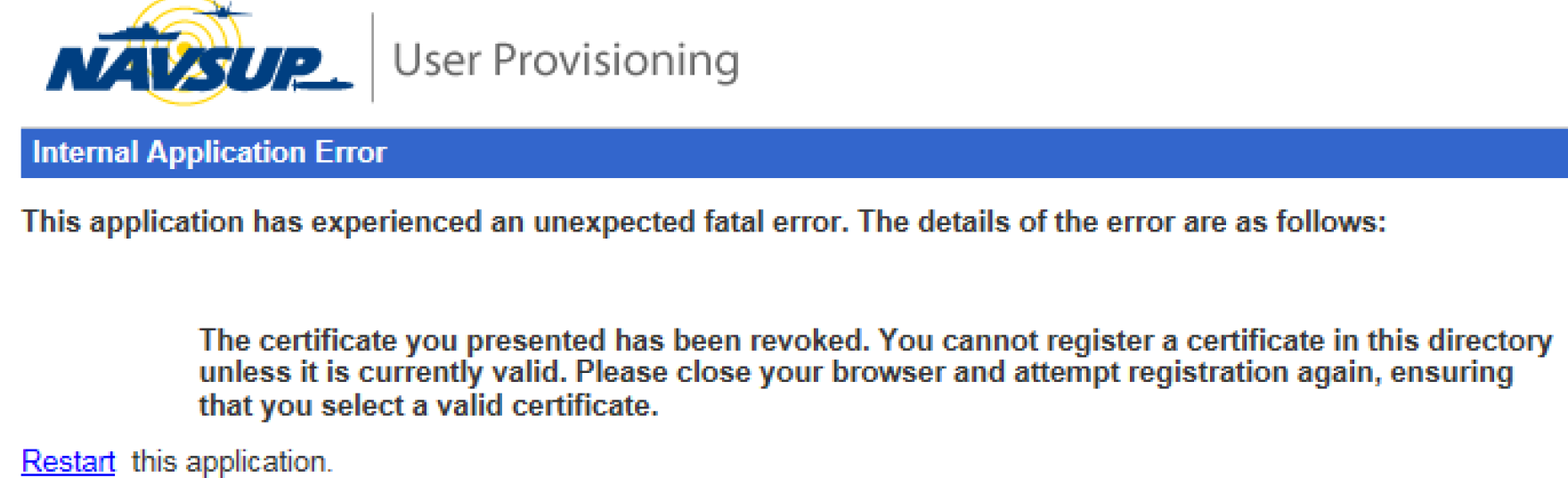
You will need to contact the NAVY311 helpdesk at 855-628-9311 or [navy311@navy.mil](mailto:navy311@navy.mil) and

ask them to request that your ticket be assigned to ORACLE\_SUPPORT\_MECH group

Request ORACLE support team remove the older PKI certificate from the NAVSUP Master directory

Once old certificate is removed, you should be able to access MyNAvsup

**‘Certificate has been Revoked’ error**



You will need to go to your CAC office and get a new CAC, and windows, re-register the NEW certificate at <https://www.navsup.navy.mil/registration> and try accessing site again.