

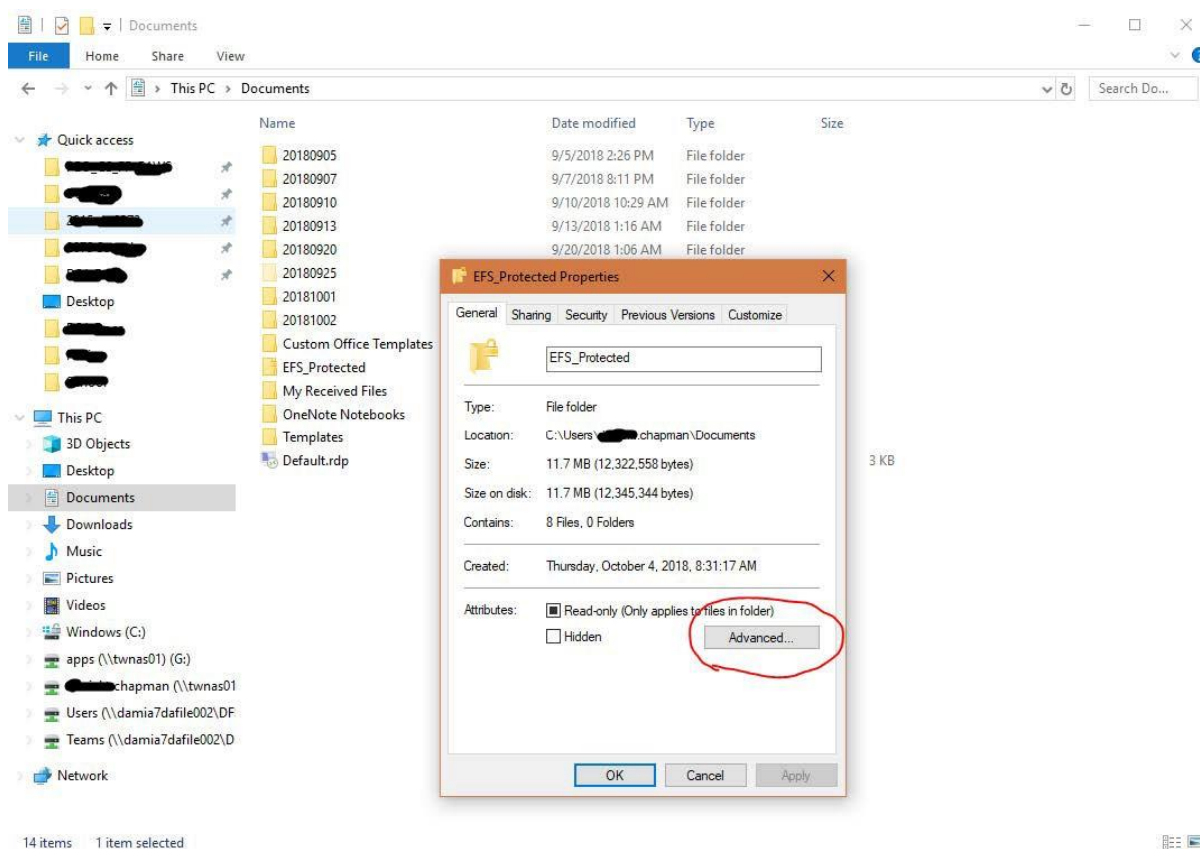
New CAC Procedure

Updated: 15 April 2019

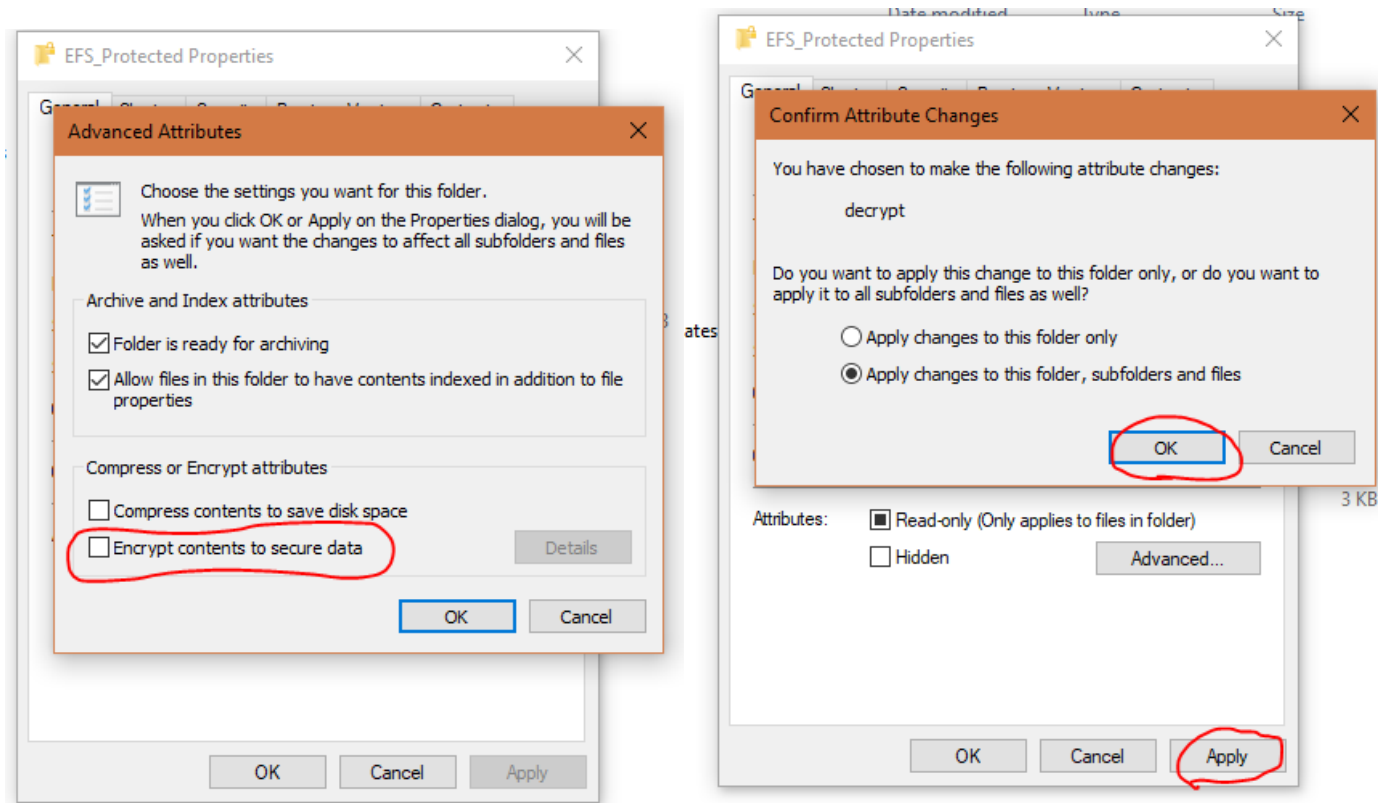
Part 1

- **Decrypt all encrypted files – THIS IS DONE BEFORE YOU RECEIVE YOUR NEW CAC.** This process is done to the encrypted folder that contains your encrypted documents. The reverse action will encrypt them once you have renewed your CAC. This process also works the same way for individual files.

Step 1: Right click on your encrypted folder. Open the properties and then the advanced options.



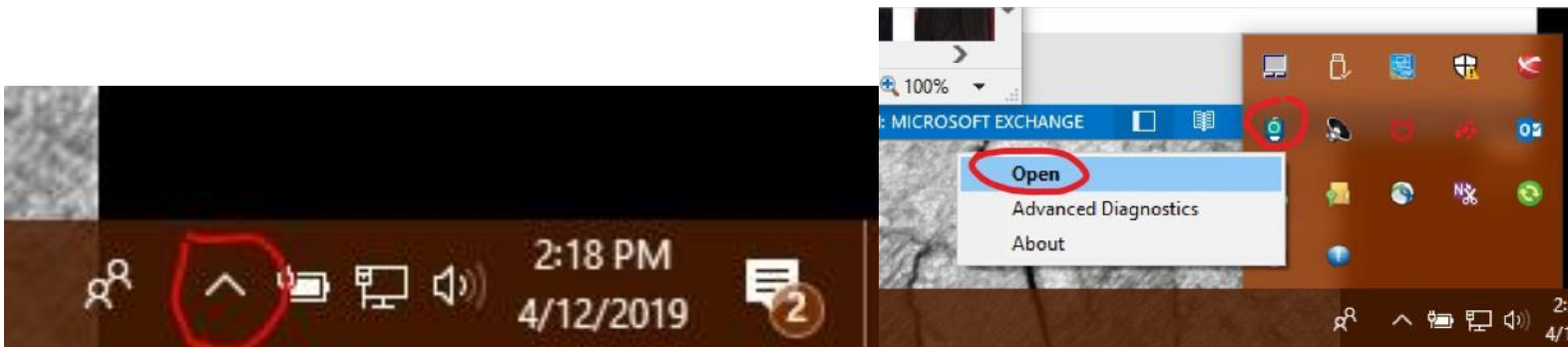
Step 2: Deselect the box, “Encrypt contents to secure data.” Click “OK”, click “Apply”, you will then be prompted with a “Confirm Attribute Changes” dialogue box, and click “OK”. You have now un-encrypted your files.



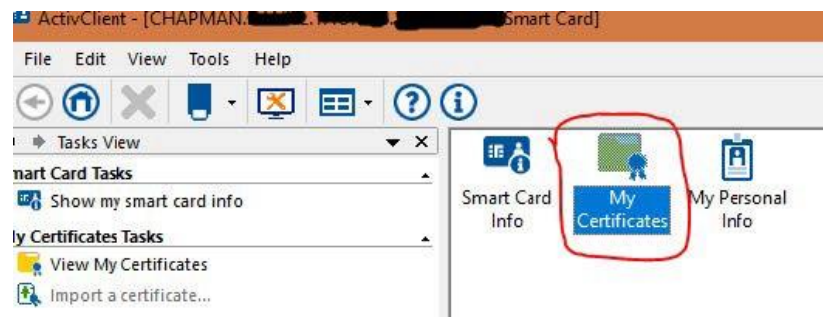
Part 2

- After receiving your new CAC, confirm your CAC CA Number.

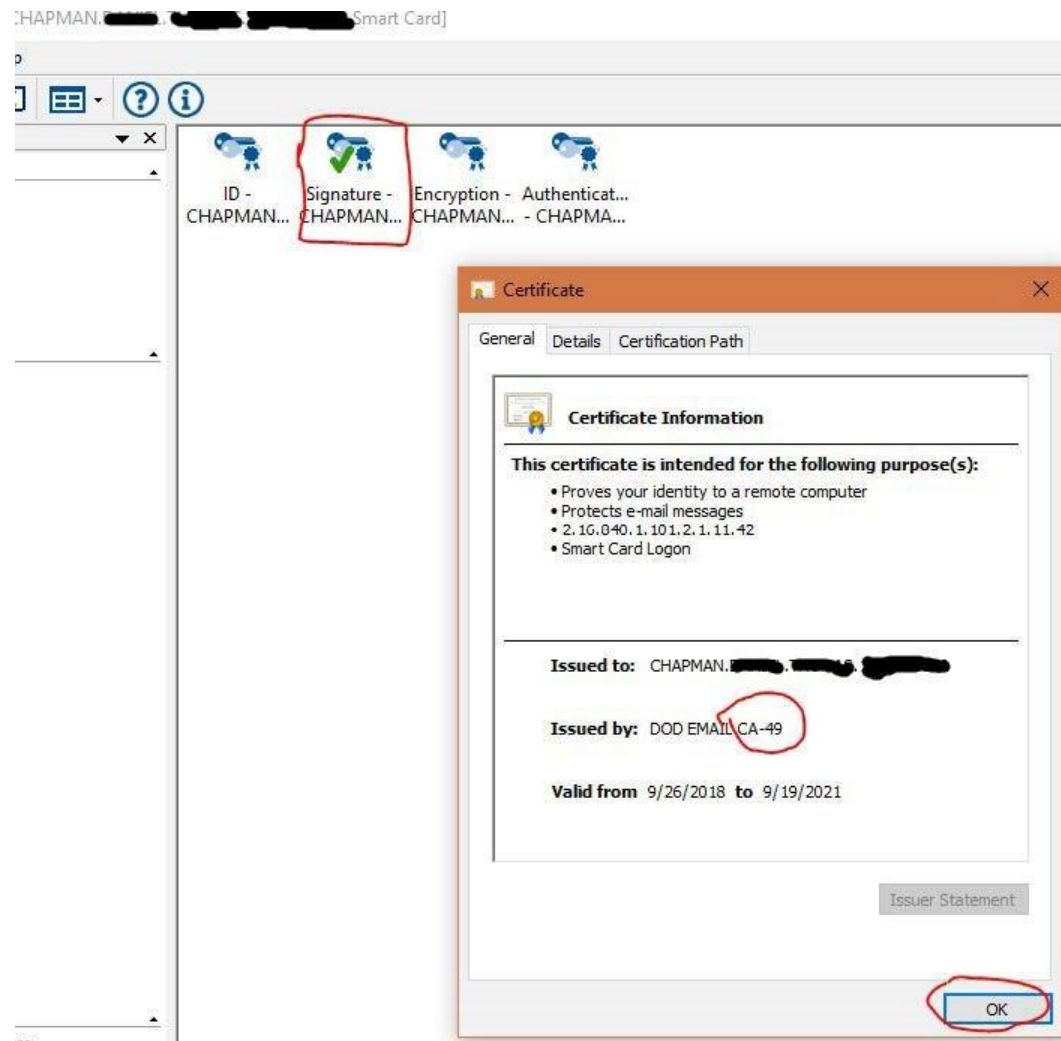
Step 1: Click the hidden icons tab. Locate the blue ActivClient Agent icon, right click and select open.



Step 2: Double click the “My Certificates” folder.



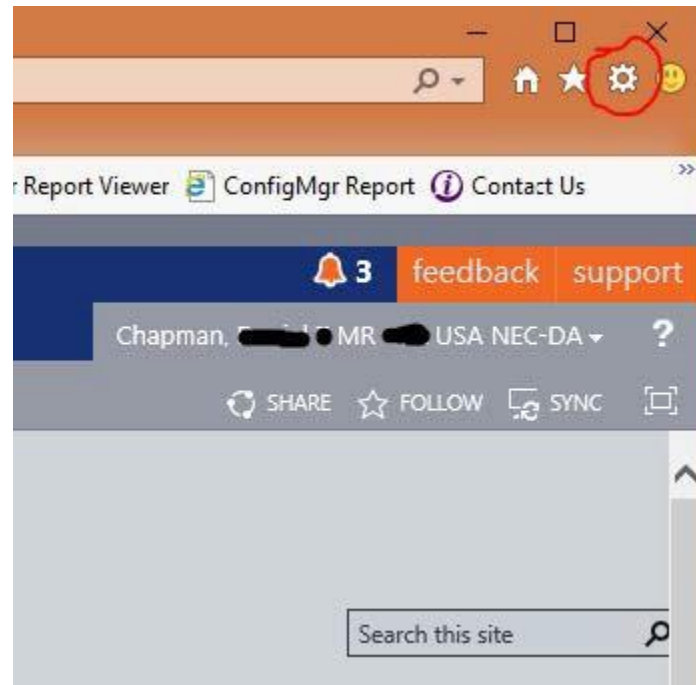
Step 3: Double click each certificate, identify the CA number, and click OK. Check each one so you are sure of each certificates number.



Part 3

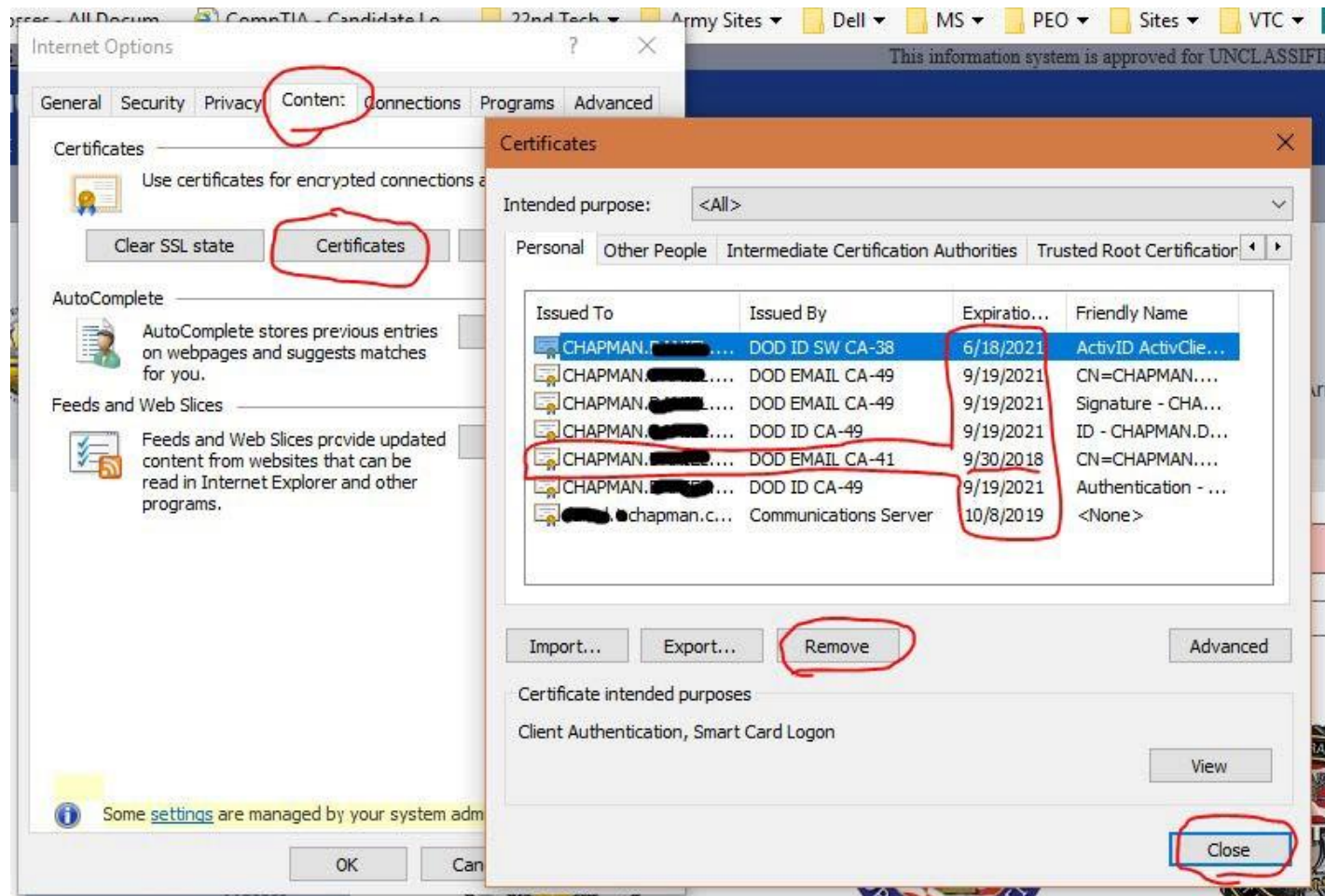
- Delete your old certificates.

Step 1: Open internet explorer, go to the gear button aka internet options and open that. Then click on “Internet Options.”



Step 2: Under “Internet Options”, open the “Content” tab and open the “Certificates.”

Next to your new CAC certificates, such as CA-49 for my example, you see the new expiration date in 2021. Identify the old certificates such as CA-41. Select each old certificate and remove them. Do not remove your new certificates, the Communications Server Certificate or the “DOD ID SW” Certificate for ActivClient. You have now cleared your old certificates.



Part 4

- Recover your old Certificates.

Step 1: Determine which link you will use based on your CA number.


<https://ara-5.csd.disa.mil/ara/ss> Odd CA numbers

<https://ara-6.csd.disa.mil/ara/ss> Even CA numbers

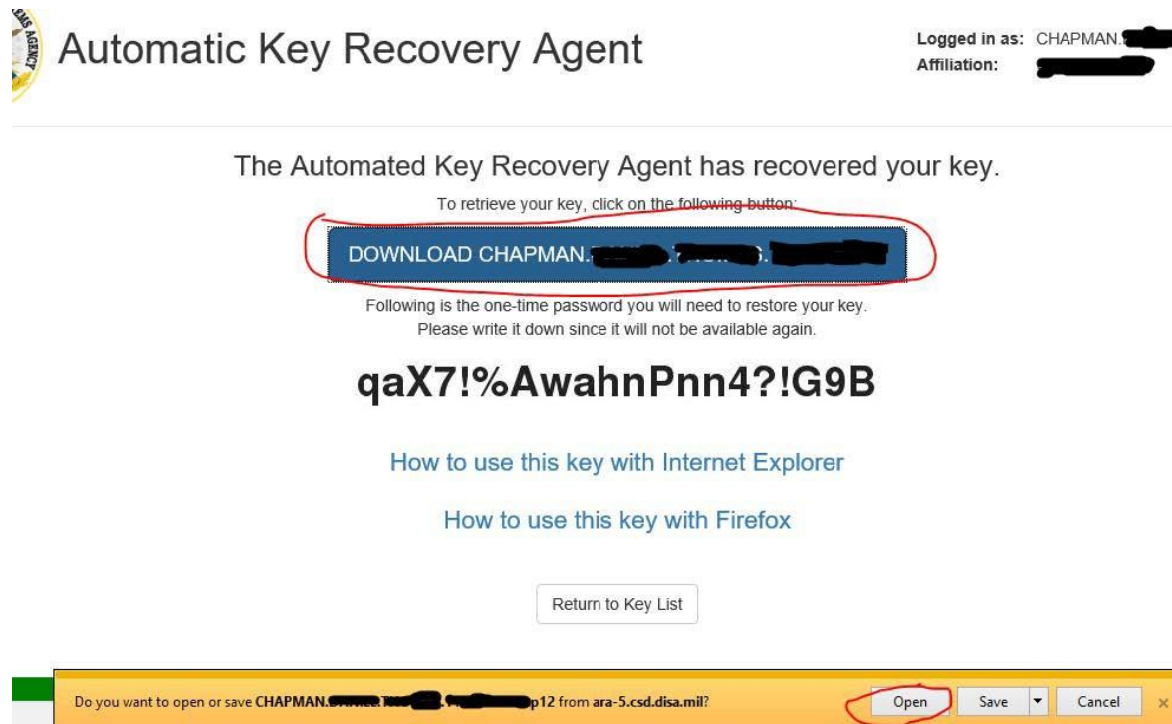
Copy and paste the link into the browser and use your Authentication certificate when prompted.

Step 2: Select the “Recover” option.

The following Encryption Keys can be recovered:

Common Name:	[REDACTED]	
Organization Affiliation:	[REDACTED]	
Not Valid Before:	2018-09-27 00:00:00 GMT	
Not Valid After:	2021-09-19 23:59:59 GMT	
Email:	[REDACTED].chapman.ctr@mail.mil	
Issuer:	DOD EMAIL CA-49	
Serial Number:	0x2D893	
Key Usage:	keyEncipherment	

Step 3: Select the Download option with your name listed. Click “Open” when prompted to open or save.



The screenshot displays the 'Automatic Key Recovery Agent' web interface. At the top left is a circular logo with 'DISA' and 'AGENCY' text. The title 'Automatic Key Recovery Agent' is centered at the top. On the top right, it shows 'Logged in as: CHAPMAN [redacted]' and 'Affiliation: [redacted]'. The main content area states 'The Automated Key Recovery Agent has recovered your key.' followed by 'To retrieve your key, click on the following button:'. A blue button labeled 'DOWNLOAD CHAPMAN: [redacted]' is highlighted with a red circle. Below the button, it says 'Following is the one-time password you will need to restore your key. Please write it down since it will not be available again.' The password 'qaX7!%AwahnPnn4?!G9B' is displayed in large, bold, black font. Underneath the password are two links: 'How to use this key with Internet Explorer' and 'How to use this key with Firefox'. A 'Return to Key List' button is located below the links. At the bottom of the page, a yellow download bar from Internet Explorer is visible, showing the file name 'CHAPMAN: [redacted].p12 from ara-5.csd.disa.mil?' and the 'Open' button is circled in red.

Automatic Key Recovery Agent

Logged in as: CHAPMAN [redacted]
Affiliation: [redacted]

The Automated Key Recovery Agent has recovered your key.

To retrieve your key, click on the following button:

DOWNLOAD CHAPMAN: [redacted]

Following is the one-time password you will need to restore your key.
Please write it down since it will not be available again.

qaX7!%AwahnPnn4?!G9B

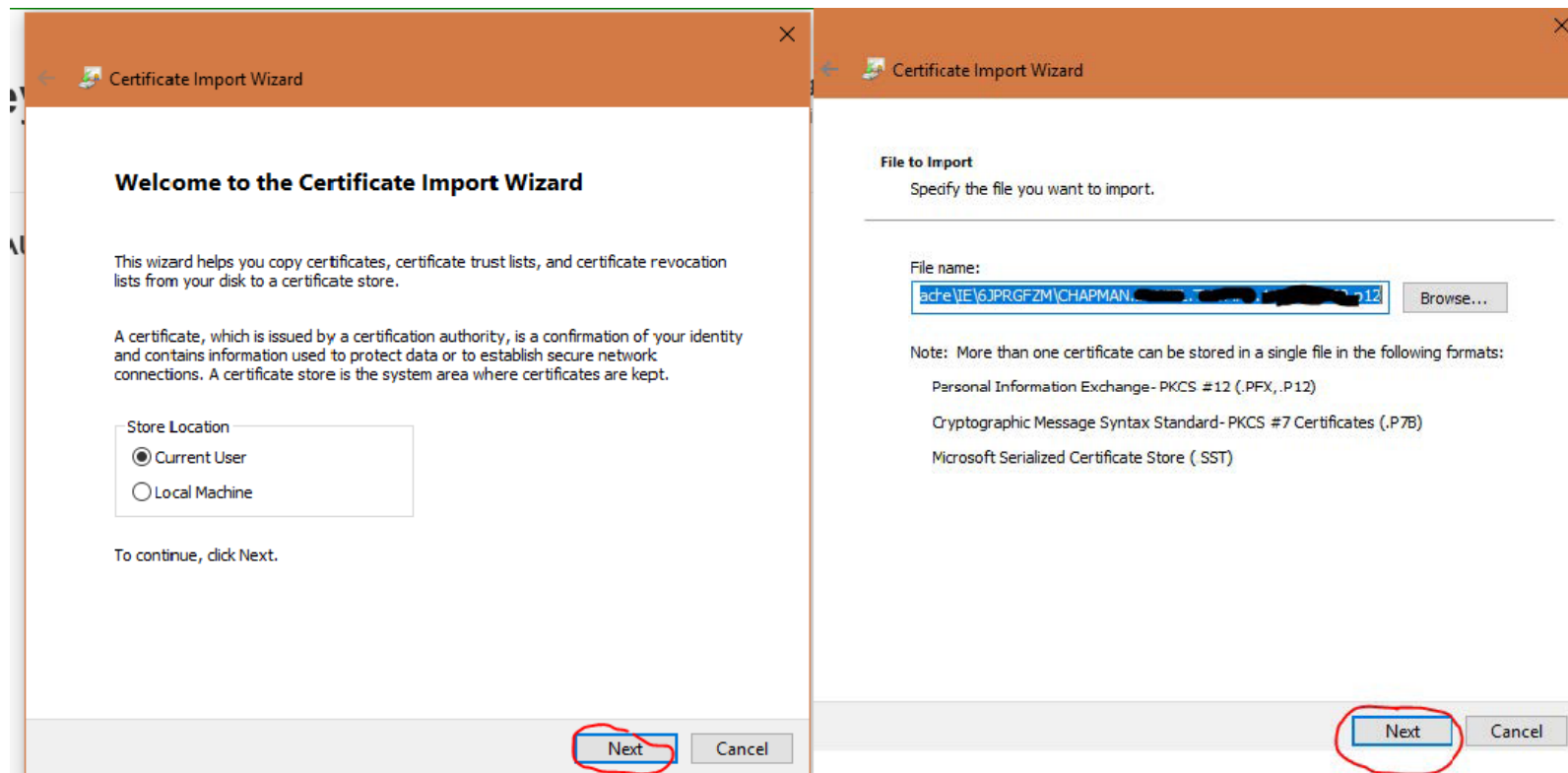
[How to use this key with Internet Explorer](#)

[How to use this key with Firefox](#)

[Return to Key List](#)

Do you want to open or save CHAPMAN: [redacted].p12 from ara-5.csd.disa.mil? **Open** Save Cancel

Step 4: Click “Next” on both dialogue boxes as they appear.



Step 5: Enter the password to recover your certificate. You can display the password to ensure you have typed it correctly, then click “Next.”

The screenshot shows the 'Automatic Key Recovery Agent' web interface. At the top, a green banner reads 'UNCLASSIFIED // FOR OFFICIAL USE ONLY'. The page title is 'Automatic Key Recovery Agent'. Below the title, it states 'The Automated Key Recovery Agent has recovered your key'. A button labeled 'DOWNLOAD CHAPMAN...' is visible. Below this, a message says 'Following is the one-time password you will need to restore your key. Please write it down since it will not be available again.' The password 'qaX7!%AwahnPnn4?!G9B' is displayed in large, bold text. Below the password, there are two links: 'How to use this key with Internet Explorer' and 'How to use this key with Firefox'. At the bottom of the page, there is a 'Return to Key List' button. Overlaid on the right side of the page is the 'Certificate Import Wizard' dialog box. The dialog box has an orange title bar and a close button (X). It contains the following sections: 'Private key protection' with the text 'To maintain security, the private key was protected with a password.' and 'Type the password for the private key.'; a 'Password:' text box with a red circle around it; a 'Display Password' checkbox; and 'Import options' with four checkboxes: 'Enable strong private key protection...' (unchecked), 'Mark this key as exportable...' (unchecked), 'Protect private key using virtualized-based security(Non-exportable)' (unchecked), and 'Include all extended properties.' (checked). At the bottom of the dialog box, there are 'Next' and 'Cancel' buttons, with the 'Next' button circled in red.

UNCLASSIFIED // FOR OFFICIAL USE ONLY

Automatic Key Recovery Agent

Logged in as: CHAPMAN. [REDACTED] Logout

The Automated Key Recovery Agent has recovered your key.

To retrieve your key, click on the following button:

DOWNLOAD CHAPMAN. [REDACTED]

Following is the one-time password you will need to restore your key.
Please write it down since it will not be available again.

qaX7!%AwahnPnn4?!G9B

[How to use this key with Internet Explorer](#)

[How to use this key with Firefox](#)

[Return to Key List](#)

Certificate Import Wizard

Private key protection
To maintain security, the private key was protected with a password.

Type the password for the private key.

Password: [REDACTED]

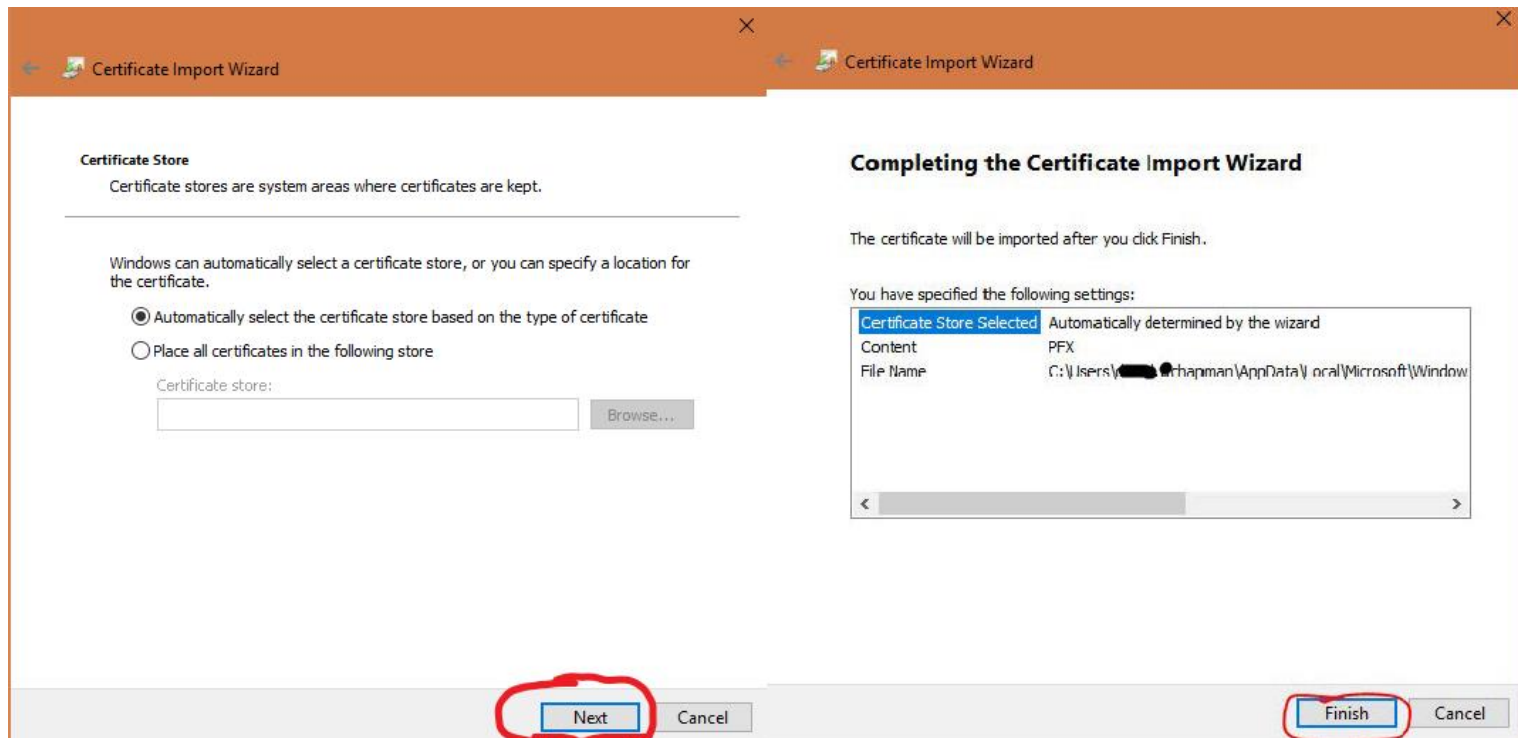
☐ Display Password

Import options:

- ☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
- ☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
- ☐ Protect private key using virtualized-based security(Non-exportable)
- ☒ Include all extended properties.

Next Cancel

Step 6: Click “Next.” Nothing needs to be changed. Click “Finish.”



Step 7: Click “Return to Key List.” You have successfully imported your certificate.

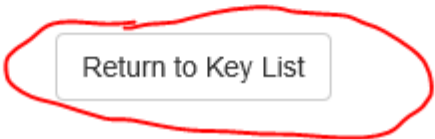
Now repeat the steps until you have recovered all of your certificates.

Following is the one-time password you will need to restore your key.
Please write it down since it will not be available again.

qaX7!%AwahnPnn4?!G9B

[How to use this key with Internet Explorer](#)

[How to use this key with Firefox](#)

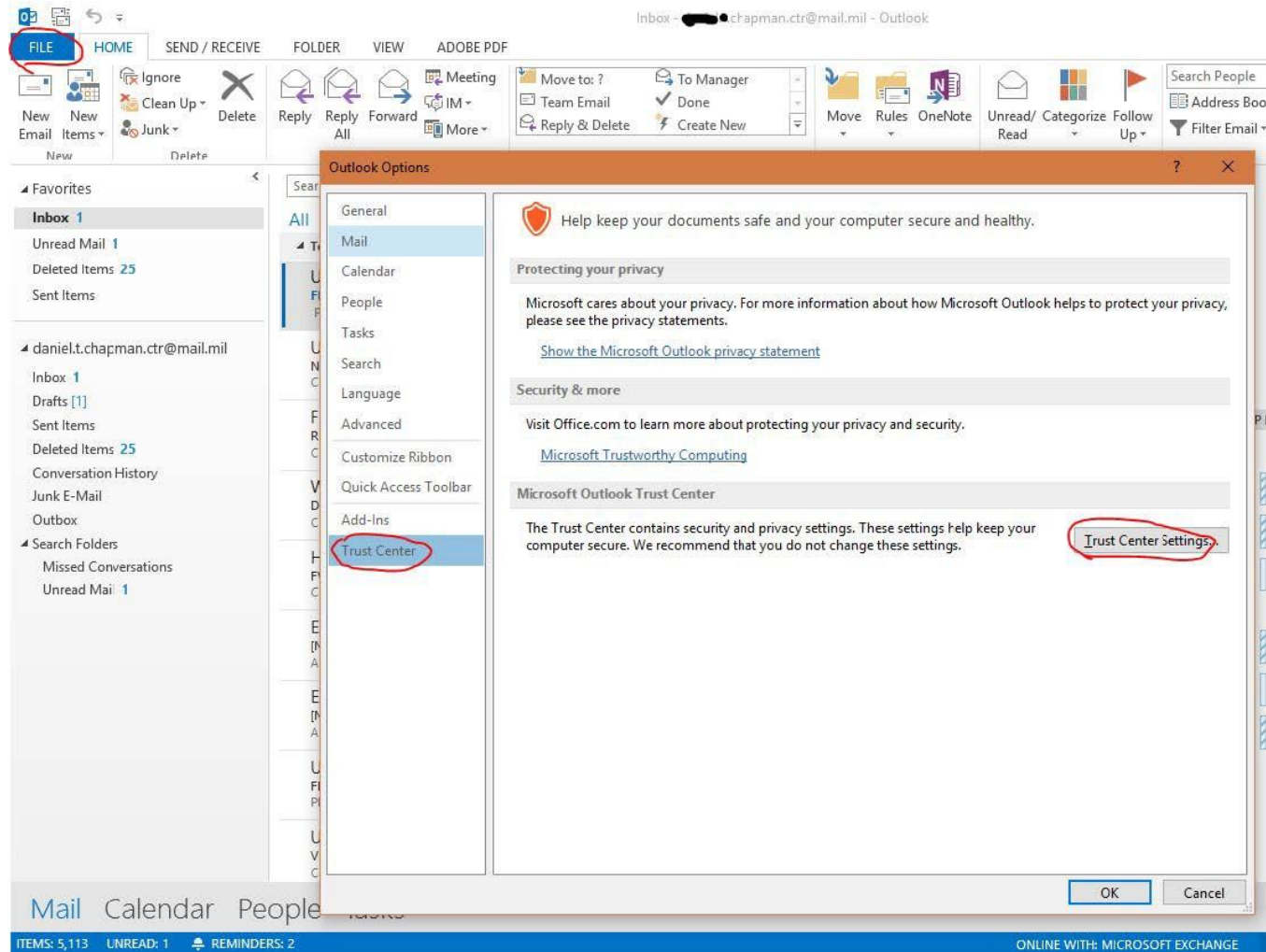


Return to Key List

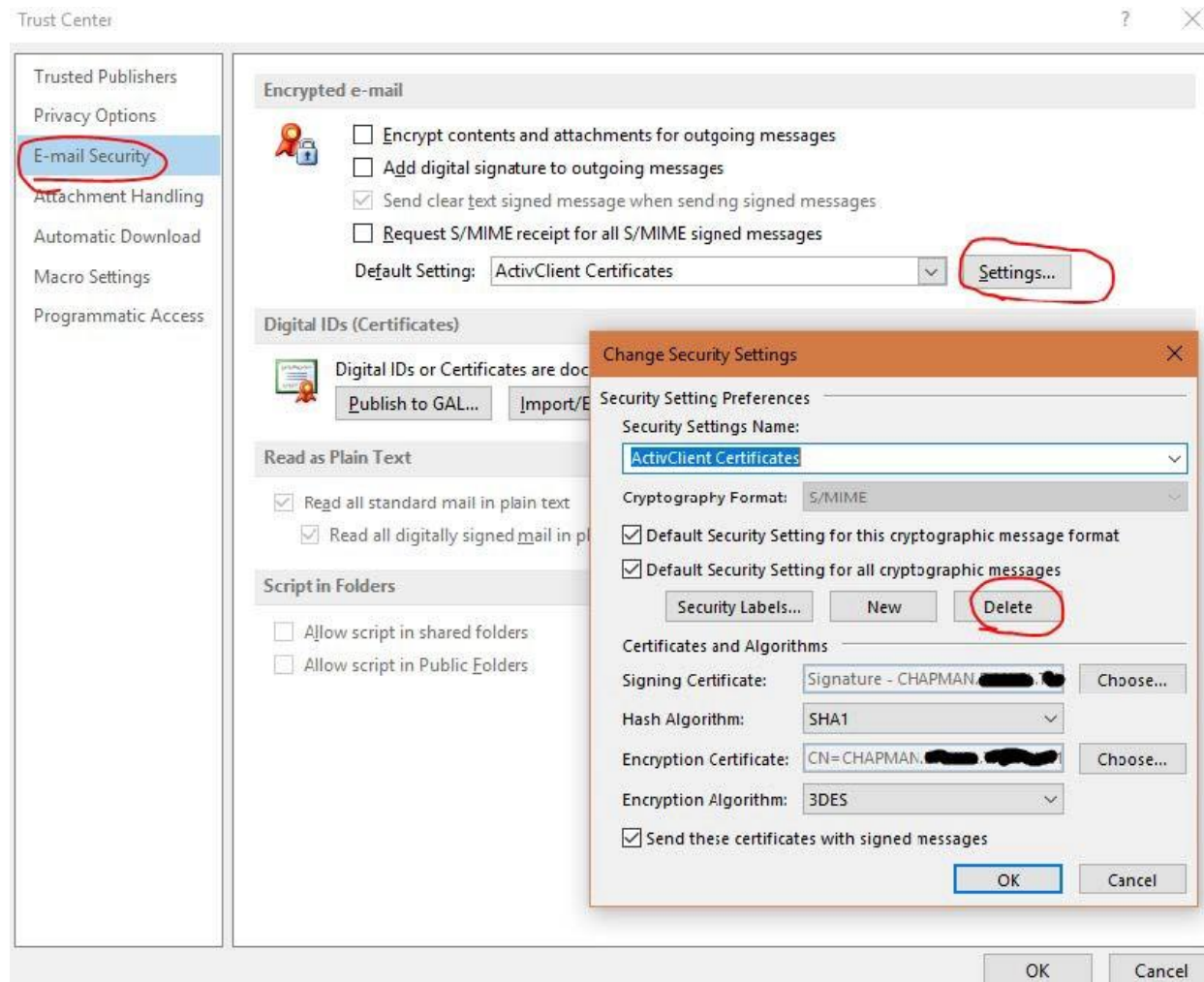
Part 5

- Publish your new certificates in outlook to the Gal.

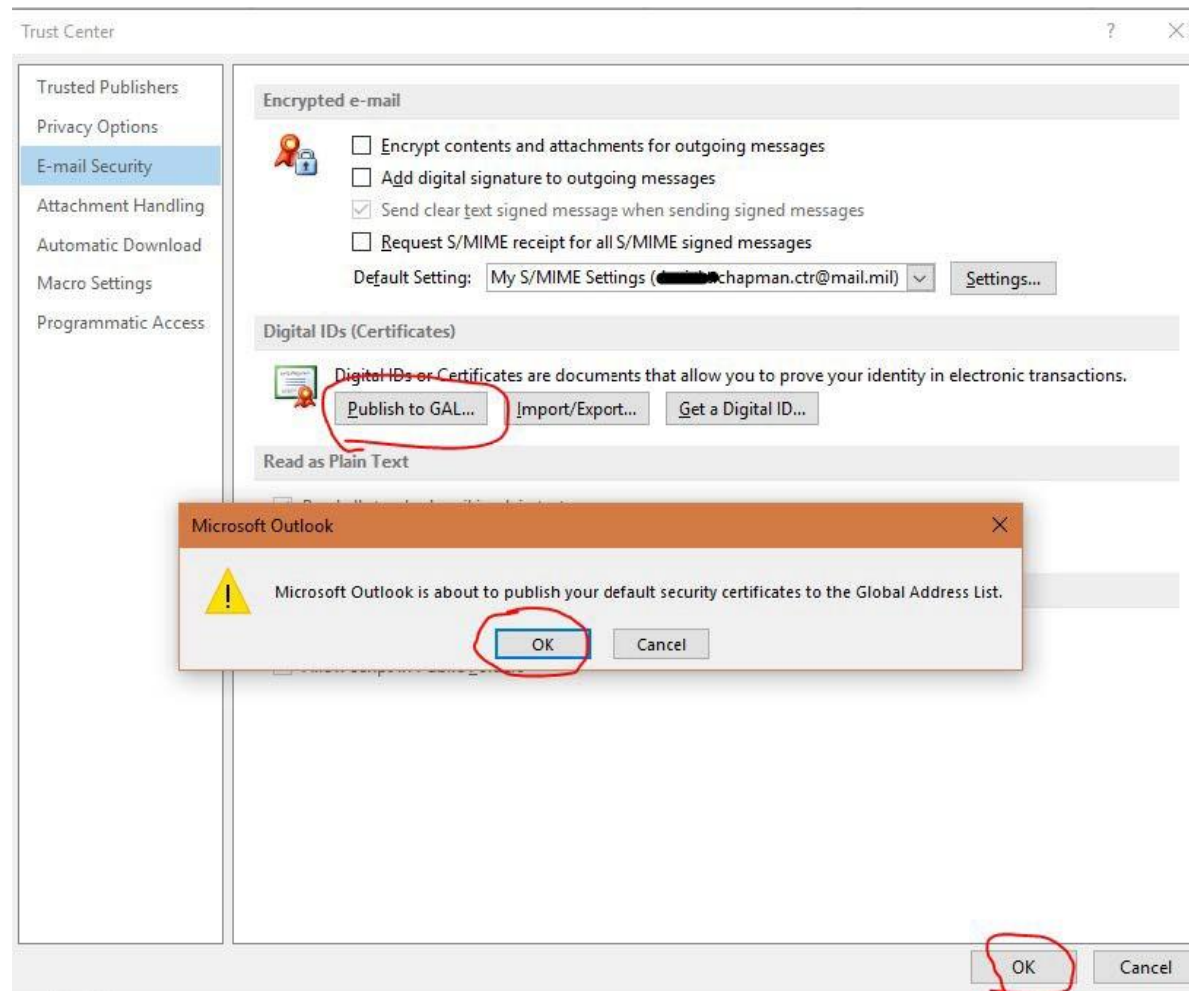
Step 1: Open Outlook, go to “File,” “Options,” select the “Trust Center” tab and then open “Trust Center.”



Step 2: Select the “E-mail Security” tab on the left, then open “Settings.” Click “Delete” twice, deleting your ActivClient and E-mail Certificate. Click “OK” to close the Security Settings box. Open “Settings.” again It will bring in your new certificates. Click “OK” to close the Security Settings box.



Step 3: Click “Publish to GAL,” then click “OK” in the dialogue box. You have now published your new certificates to the Gal.



Part 6

- Access AKO and enroll your new CAC. <https://amid.us.army.mil/>

Step 1: Ensure that your username and password are not expired. If it is, then change your password.

Last Password Change

Your last password change was on 17 May 2016

Your password will expire on **14 Dec 2018**

[Change Password](#)

*** Example of an expired password. The current date is April 2019.**

Step 2: Login to AKO with your username and password

Step 3: Select “My Account,” then click account information

Step 4: Click “CAC/Certificate Registration.”

Step 4: Click “Clear Registered Information.” If you receive an error stating you are currently logged in with a CAC, then make sure you log out of AKO, close all internet explorer browsers. Launch internet explorer and log in to AKO with your username and password. Make sure you click the “Login” button, not “CAC/PKI Login” after entering your username and password.

Registration

If you are currently logged in with CAC, you must log out and log back in to AKO with your username and password before you can clear your CAC information.

Current Registered Information

Current Registered Information

Cert Type:	DoD CAC certificates
Common Name:	CHAPMAN [REDACTED]
Distinguished Name:	CN=CHAPMAN [REDACTED], OU=CONTRACTOR, OU=PKI, OU=DOD, O=U.S. GOVERNMENT, C=US
Valid From:	Thu Sep 27 00:00:00 GMT 2018
Valid To:	Sun Sep 19 23:59:59 GMT 2021
Serial Number:	2e901
Issuer:	CN=DOD ID CA-49, OU=PKI, OU=DOD, O=U.S. GOVERNMENT, C=US

Clear Registered Information

- When done correctly you will receive the following message:

Your CAC information has been successfully cleared.

CAC/Certificate Registration

No CAC/Certificate is registered for your account. Follow the instructions below to register your CAC/Certificate.

If you do not know your CAC PIN or if you have locked out your CAC PIN (after three incorrect tries), DO NOT CALL THE AKO HELP DESK. The AKO Help Desk cannot assist you if you have locked your CAC. Instead, you should contact your local help desk to determine the location of the nearest CAC PIN Reset (CPR) station. You should go to an ID Card Issuance Facility (your central processing/badge office or Local Registration Authority) to have your PIN reset only if a CPR station is unavailable.

If you have any other issues, please visit the [AKO CAC Resource Center](#)

Note: Registration with a non-CAC X.509 certificate may not provide access to all sites and services authenticated by AKO.

Register

Step 5: After clicking “Register,” you will be prompted for a certificate, use your authentication certificate, then enter your AKO password into the dialogue box. Click, “Register My Certificate.”

https://certreg.us.army.mil/suite/pages/cac/prereg.none - Internet Explorer provi...

Register your CAC/Certificate

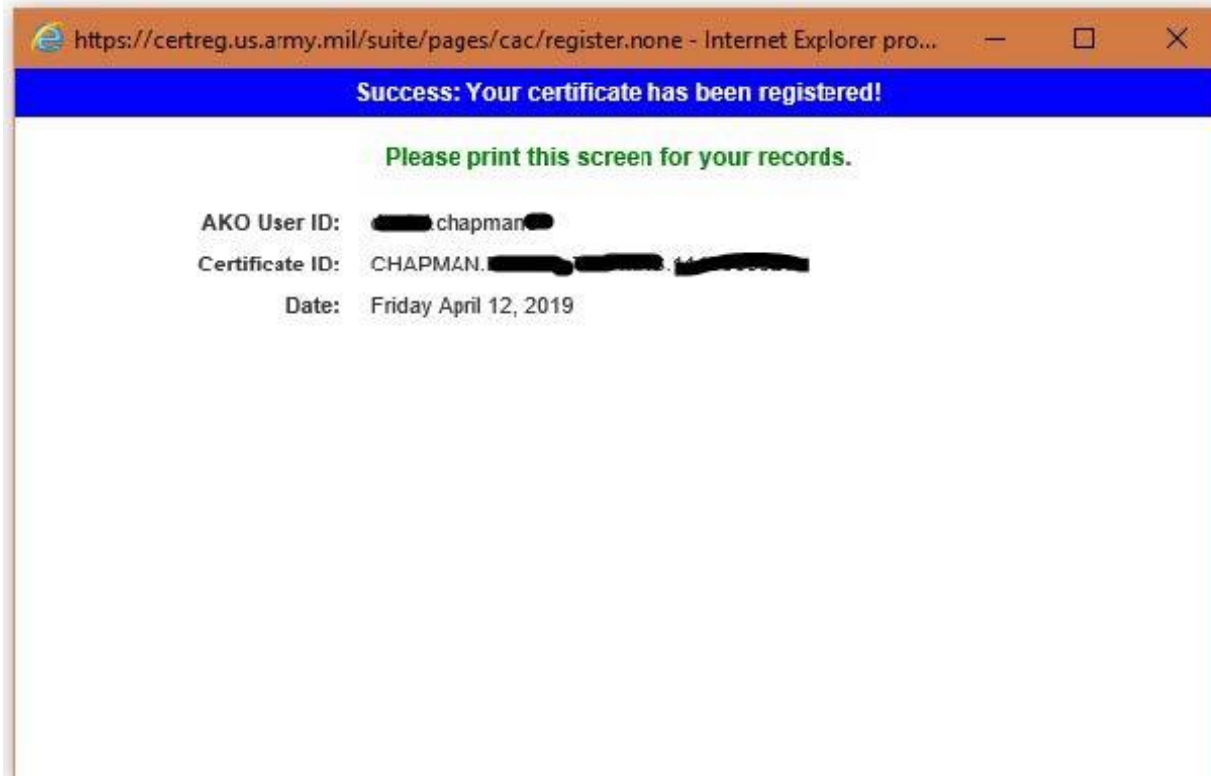
Enter your AKO password below to register your CAC/Certificate with your AKO account.

AKO Password:

Register My Certificate

[Click here for more help on registering your CAC.](#)

register



You have successfully registered your CAC information with AKO.

Congratulations – you are now ready to get back to work.