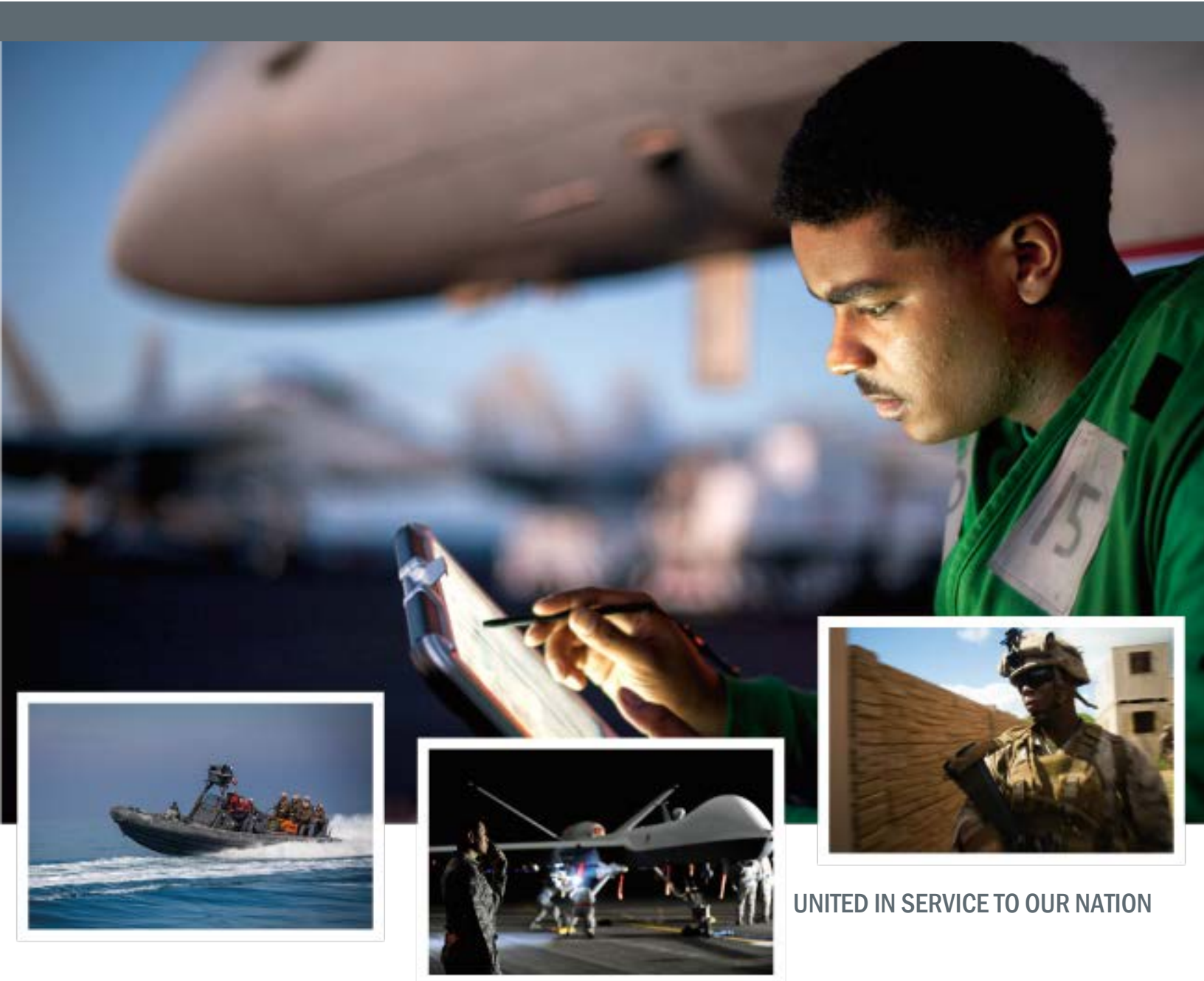




DEFENSE INFORMATION SYSTEMS AGENCY
A COMBAT SUPPORT AGENCY

Department of Defense Enterprise Email (DEE) Guide:
MANAGING DUAL-PERSONA CERTIFICATES

v1.0 September 26, 2016



UNITED IN SERVICE TO OUR NATION

UNCLASSIFIED // FOR OFFICIAL USE ONLY

DEE Guide: Managing Dual Persona Certificates v2
September 2016

Document Approval

Version	Document Approved By	Date Approved
1.0	Rodney Saxon, Chief, User Applications Branch (SE34)/ Program Manager, DoD Enterprise Email	20160926

Revision History

VERSION	DATE	PRIMARY AUTHOR(S)	REVISION/CHANGE	PAGES AFFECTED
1.0	20161223	DEE Team-Steve Spector IdSS-Ted Dressell DMDC/RAPIDS- Sangeeta Ryan	This is an update of the DEE Onboarding End-user Guide, first produced in 2013 and updated in 2014, which has been included in a packet distributed directly to Mission Partner Onboarding Program Managers/Teams.	All

Table of Contents

1	Overview: Dual-Persona Management	4
1.1	Introduction	4
1.2	Purpose	4
1.2.1	Who is Dual-Persona?	5
1.2.2	PIV Auth cert and the Federal Agency Smart Credential Number (FASC-N)	6
2	Dual-Persona DEE Setup	7
2.1	DMDC ID Card Office Online and Activating PIV Auth cert	8
2.2	Resetting the state of your cards in ActivClient	14
3	Getting Your DEE Email Address	16
4	Updating Email Encryption and Signing Certificates: FOR DUAL CAC HOLDERS ONLY	18
	Appendix 1: Troubleshooting Dual-Persona PIV Auth Cert Process	23
	Abbreviations, Acronyms, and Definitions	24

Figures

Figure 1.	PIV Auth cert – 16 digits	6
Figure 1.	Welcome to RAPIDS ID Card Office Online	8
Figure 2.	DEERS	8
Figure 3.	Login with CAC	9
Figure 4.	Select certificate	9
Figure 5.	Select Activate PIV	10
Figure 6.	Proceed Reading CAC	10
Figure 7.	Reading data progress	11
Figure 8.	Run this Application?	11
Figure 9.	Update CAC	12

UNCLASSIFIED // FOR OFFICIAL USE ONLY

DEE Guide: Managing Dual Persona Certificates v2

September 2016

Figure 10.	PIV is active	12
Figure 11.	Progress Bar	13
Figure 12.	Successful Update	13
Figure 13.	ActivClient	14
Figure 14.	Open ActivClient	14
Figure 15.	Forget state for all cards	15
Figure 16.	View my Certificates.....	15
Figure 17.	Certificates	15
Figure 18.	Select a Certificate	16
Figure 19.	Find the PIV Auth cert.....	16
Figure 20.	Outlook Web App	17
Figure 21.	OWA About	17
Figure 22.	Email address	17
Figure 23.	Change CAC Email.....	18
Figure 24.	–Proceed to Read CAC	19
Figure 25.	Reading CAC Progress Bar	19
Figure 26.	Client Authentication	20
Figure 27.	Always trust content.....	20
Figure 28.	New e-mail Address	21
Figure 29.	Change Email - Yes	21
Figure 30.	Progress of update.....	22
Figure 31.	CAC is successfully updated.	22

1 Overview: Dual-Persona Management

1.1 Introduction

As part of DISA's implementation of DEE, every end-user's Outlook mailbox is associated with an account. Each account must have a specified Common Access Card (CAC) assigned to it. This is accomplished via the *signature* certificate.

When Dual Persona individuals are onboarded to DoD Enterprise Email (DEE), they must activate their Personal Identity Verification Authentication certificate (PIV Auth cert), which is embedded in their Common Access Cards (CACs), in order to login with the certificate that matches their new DEE mailbox.

This guide provides instructions on how Dual-Persona end-users can use the DMDC ID Card Office Online (IDCO) web application to update (activate) the firmware on their CAC to display the PIV Auth cert and use it to access DEE. While, in most cases, the affected end-users know they are Dual-Persona, it may come as a surprise to some people; nonetheless, during the onboarding process all Dual-Personas should be informed by their migration team that the PIV Auth cert needs to be activated. This should happen no later than the day before migration.

Most problems with starting DEE accounts will occur when someone is unaware of his or her Dual-Persona status. The key here is to:

- Be aware of the possibility.
- A Dual-Persona list can be generated, using DEPO, by the Mission Partner DEE migration team. This can be checked to verify Dual-Persona status among onboarding end-users.

1.2 Purpose

The reason for activation of this certificate is to support **multiple persona end-users** in the DEE Domain with a simplified CAC login (once properly set up) to DEE.

Certificates and logging into DEE

DEE is a persona-based messaging solution that requires the end-user's proper certificate. Personal Identity Verification (PIV)-based authentication is how authorized end-users are able to login to their designated Mission Partner information technology networks and services, such as DEE.

When the end-user's CAC is inserted into their computer, it provides the information used to match the end-user to their appropriate Outlook service. The end-user selects the correct certificate and enters their password to complete access.

1.2.1 Who is Dual-Persona?

Dual Persona refers to individuals who have two or more personas (active identities) in the Defense Manpower Data Center (DMDC) database, each with its own CAC (such as someone who is a DoD civilian employee or contractor *and* in the Reserves); this group is well aware of this status. However, some individuals may be surprised to find out that they have been designated as Dual-Persona,

which can happen when someone has transitioned from one DoD role to another (for instance, when they retire from active service or civilian employment to become a consultant).

For DoD personnel with one persona — e.g., one of the following: Military (.mil); Civilian (.civ); or Contractor (.ctr) — the login token is their Common Access Card Email Signing Certificate.

Users with multiple personas (e.g., civilian employee and reservist) have a CAC for each persona, **however the multiple CACs all have the same signing certificate**, consequently, a method is required so DEE can recognize the appropriate persona during login. By activating the PIV Auth cert, which has a differently formatted SAN from that in the email signing certificate, the differentiating certificate number for each CAC can be matched to its appropriate account/service. Of course, the end-user must use the correct CAC and select the appropriate certificate for the desired service.

When being Dual Persona is a surprise?

When a DoD employee or contractor is in transition, they may show up in DMDC in two different contexts. This is because there is a grace period that keeps the person's old CAC recognized: if this overlaps with the new active role, a Dual Persona situation will occur. Consequently, someone retiring from active service and returning as a contractor may, unexpectedly, show up as Dual Persona.

1.2.2 PIV Auth cert and the Federal Agency Smart Credential Number (FASC-N)

CACs do not, by default, display the PIV Auth cert. Even when activated they will still look like other (non-email) certificates until you roll the cursor over your name. A regular cert will display 10 numbers; the PIV Auth cert will show 16 numbers, as shown in Fig. 1.

In previous environments (prior to DEE), users with two or more personas typically had only one email account. The new DEE system splits these two personas out into separate mailboxes. But only one digital identity is recognized until an individual who has two CACs activates the PIV Auth cert on both cards. The PIV Auth certificates have a field that is unique for the CAC-holder called the Federal Agency Smart Credential Number (FASC-N).



Figure 1. PIV Auth cert – 16 digits

The FASC-N is comprised of 36 digits of which 16 are placed into the PIV Auth cert and these let a Dual-Persona utilize the PIV Auth cert to login with the CAC that matches the desired mailbox. The last digit designates which type of persona the certificate is associated with in the end-user DEE mailbox: “2” for civilian; “4” for military; and “5” for contractor. So, when logging into the mailbox, the Outlook Client (the version in the end-user’s workstation) or the Outlook Web App (OWA) passes the unique number from the PIV Auth cert and matches it to the correct account and authenticates the end-user.

IMPORTANT: The end user will need to ensure the correct CAC is used for the particular account he or she wants to access.

NOTE: DISA has prepared a UPN white paper, *The Generation and Use of the userPrincipalName (UPN) attribute within IdSS and EASF*, to help explain how this works. It can be downloaded at: https://disa.deps.mil/ext/cop/iase/idam/downloads/20150727-unclass-fouo-upn_whitepaper_v1.pdf

2 Dual-Persona DEE Setup

In order to update your CAC, your laptop or work station must be CAC-enabled (a DEE requirement) and connected to the DoD network.

WARNING—Only people with Dual-Personas should proceed with these steps; those who aren't sure, but think they may qualify, should check with their migration manager who will have a list of Dual-Persona personnel. While it is not a terrible problem for a non-Dual-Persona end-user to activate the PIV Auth cert, they will be annoyed by having to select which certificate to use when accessing DEE. Also, once the PIV Auth cert is activated it cannot be deactivated.

Setting up your Dual-Persona PIV Auth cert requires a number of steps:

1. Connecting to DMDC ID Card Office Online.
2. Activating each CAC's PIV Auth cert.
3. Having the system "forget" your individual certificates.
4. Resetting your CAC identities in ActivClient.
5. Updating to your new DEE addresses (one associated with each CAC).

2.1 DMDC ID Card Office Online and Activating PIV Auth cert

In order to start your DEE service, you need to activate your PIV authentication certificate for each CAC and then have ActivClient forget the previous state of all your CACs. This section provides the steps for how to do that.

NOTE: In order to utilize the ID Card Office Online Portal, you must have the matching Architecture Browser and JAVA version as your Operating System (i.e. If running Windows 7 64-Bit, you must have Internet Explorer # 64-Bit and JAVA # 64-bit). Please see Appendix 1 – A.1 for further details.

1. Go to **ID Card Office Online** at https://www.dmdc.osd.mil/self_service.

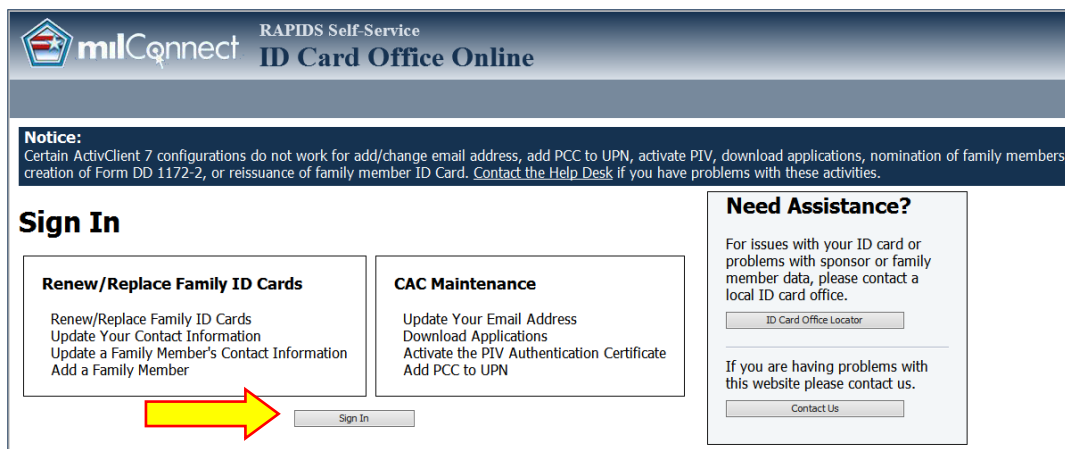


Figure 1. Welcome to RAPIDS ID Card Office Online

2. Click **OK**.

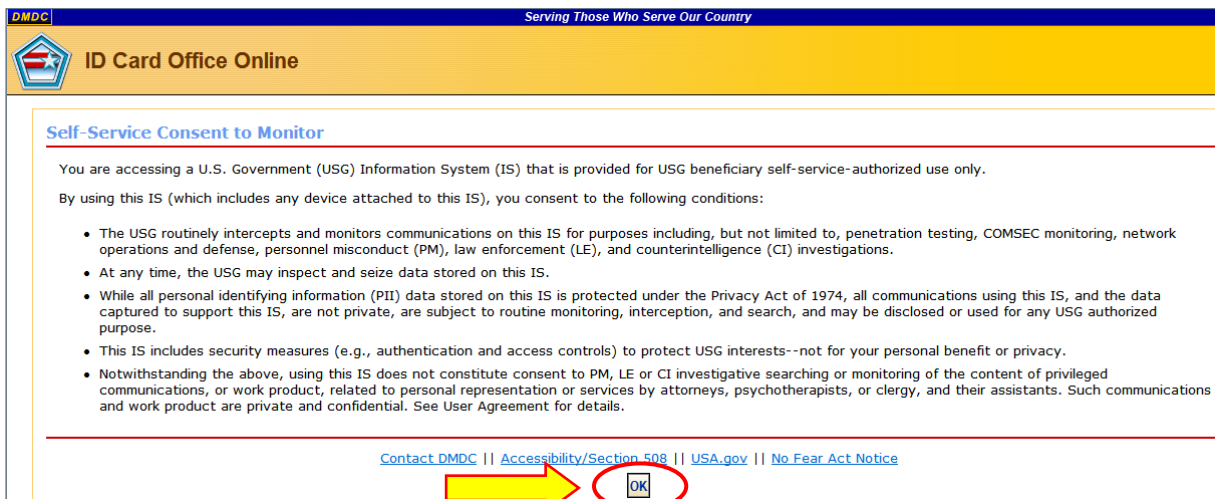


Figure 2. DEERS

3. Log in with your CAC.

Figure 3. Login with CAC

4. Select your identity certificate (**NOT** the email certificate), enter your PIN if asked, and click **OK**.
NOTE: When you complete activation for one CAC, insert the other CAC(s) and repeat the process.

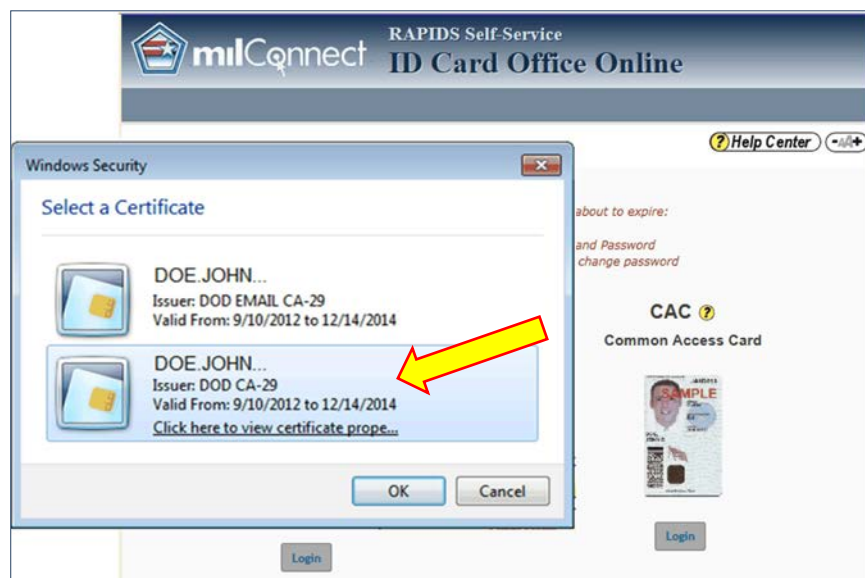


Figure 4. Select certificate

5. Select **Activate PIV certificate**.

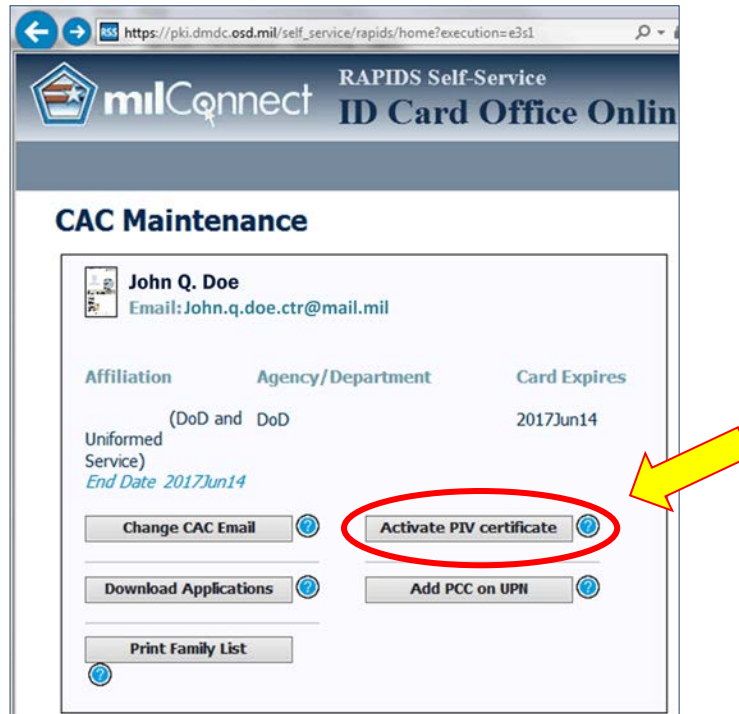


Figure 5. Select Activate PIV

6. Click **Proceed** to begin the process of reading the CAC data.

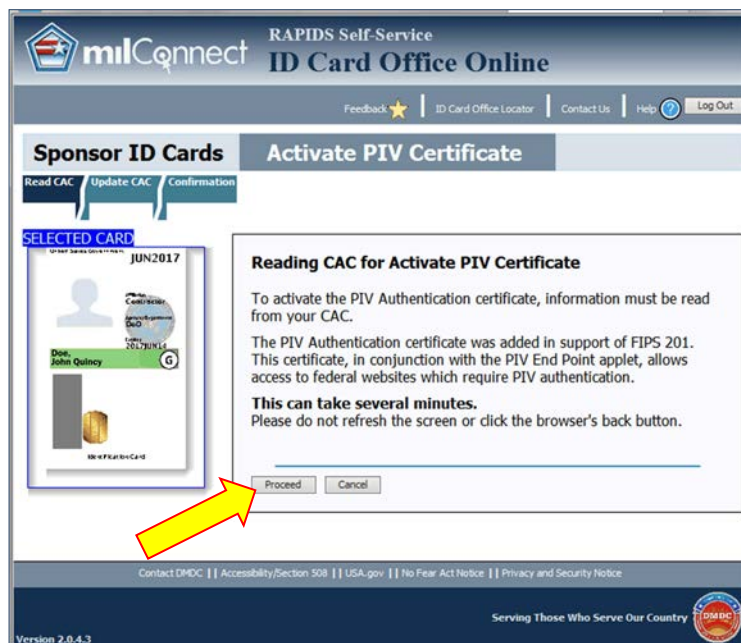


Figure 6. Proceed Reading CAC

7. A progress bar will track the CAC-reading phase.

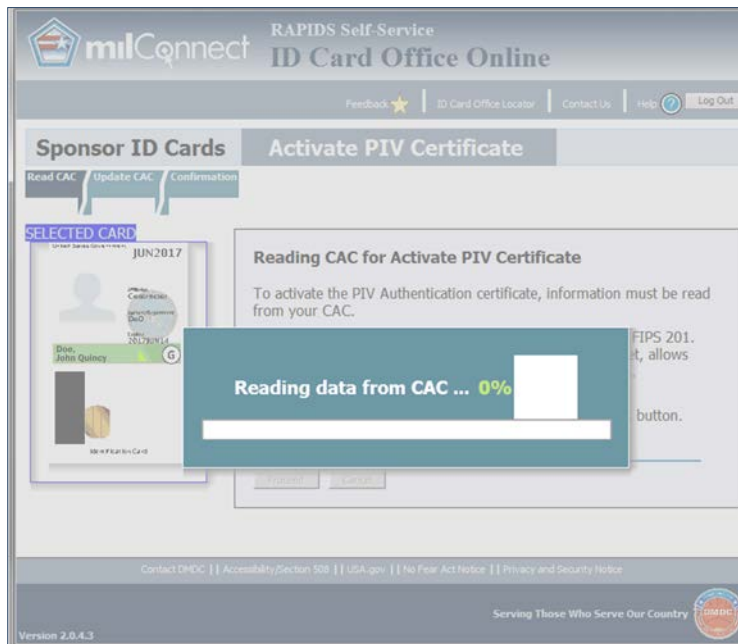


Figure 7. Reading data progress

8. The process runs on Java, which will periodically ask for confirmation. Click **Run** for all Java related prompts.



Figure 8. Run this Application?

9. The process advances to the **Update CAC** tab. Click **Update CAC** to activate the PIV Auth cert.



Figure 9. Update CAC

10. Java asks, "Do you want to run this application?" Click **Run**.

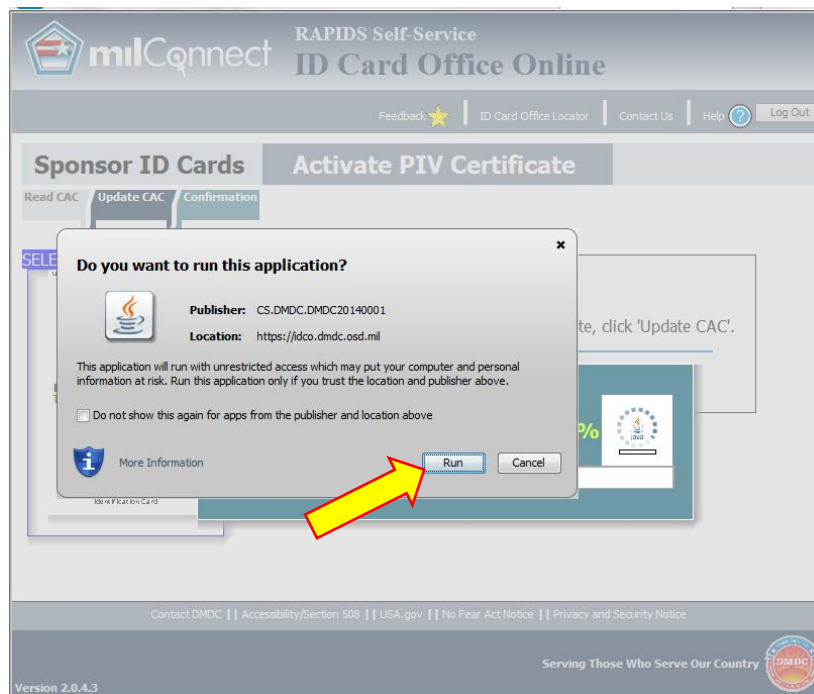


Figure 10. PIV is active

11. A progress bar appears.

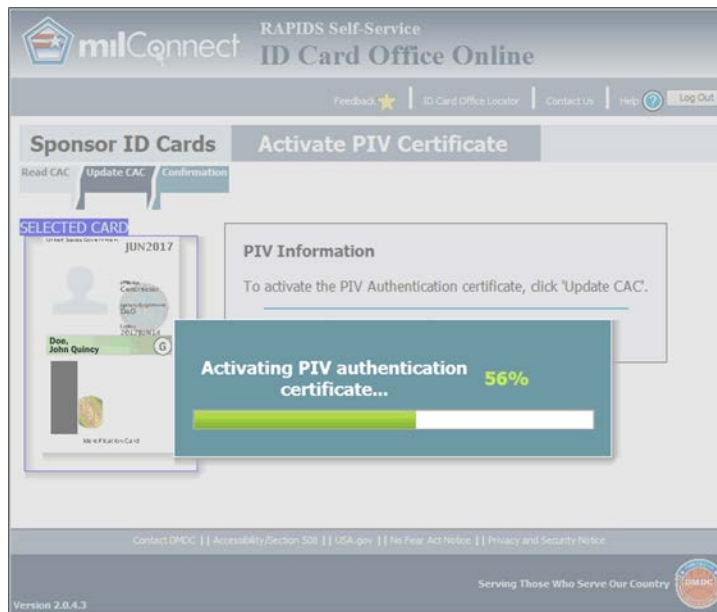


Figure 11. Progress Bar

12. The process shifts to the **Confirmation** tab, indicating the CAC has been updated. Click **Home**, then logout.

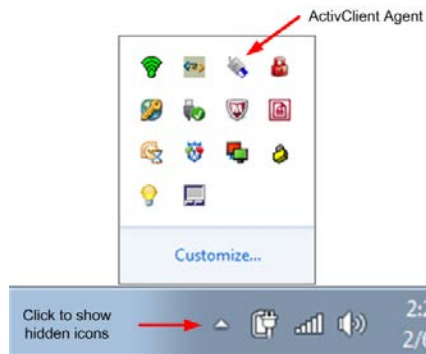


Figure 12. Successful Update

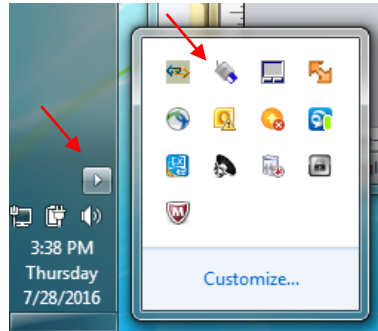
2.2 Resetting the state of your cards in ActivClient

Now that your PIV cert is active you need to tell the system to reset (forget) the state of all cards in ActivClient; it also lets you see the properties associated with your CAC and certificates. The ActivClient Agent is accessed from the System Tray (usually at the bottom of the computer display, though the exact location may vary); below are three examples of where it can be found

1. In the example below, the System Tray is on the bottom of the display. ActivClient is in a group of hidden icons that are visible when you click on the triangle.



2. When the System Tray is at the bottom of a vertical toolbar, click the triangle button.



3. In the example below, the ActivClient is on the left in the System Tray.



Figure 13. ActivClient

4. Locate the icon for your ActivClient Agent and click it, then click **Open**.

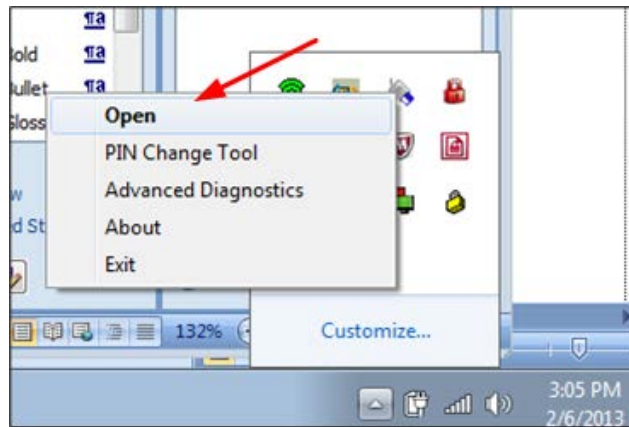


Figure 14. Open ActivClient

5. Select: **Tools>Advanced**; and then click **Forget state for all cards**.

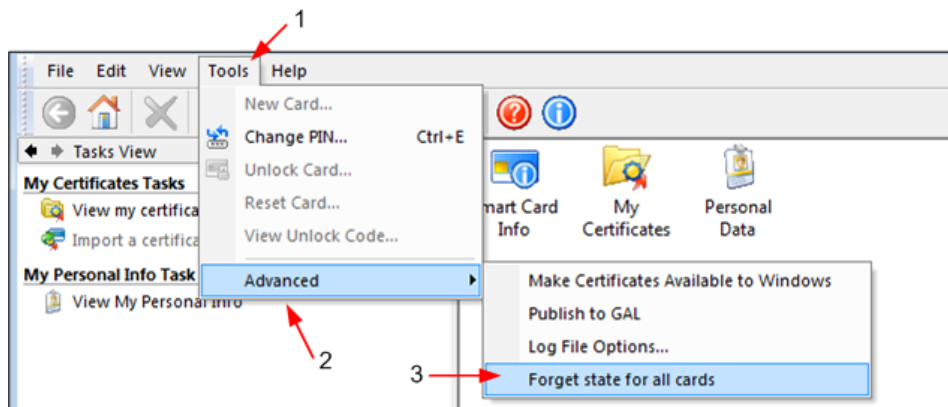


Figure 15. Forget state for all cards

6. Close ActivClient and then re-open it. Double-click the **My Certificates** icon.
Note: **Views** lets you select how you see the certificates—as icons, as a list, or as a detailed list.

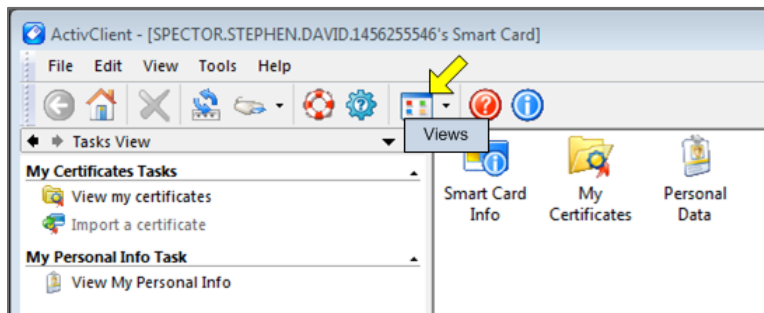


Figure 16. View my Certificates

7. Confirm that you see four certs. Click on **View** and select **Details** to understand which certs you have.

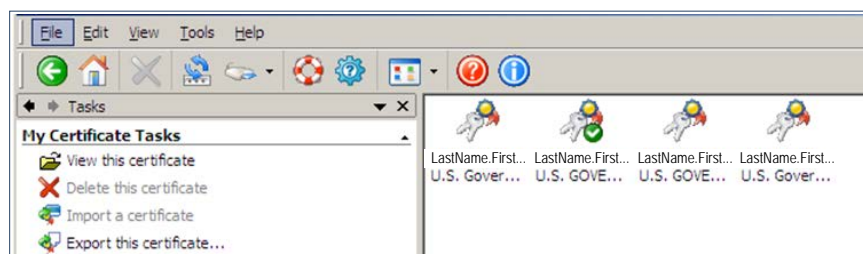


Figure 17. Certificates

NOTE: The reason for exposing the PIV Auth cert is that Dual-Persona users are now required to use it to authenticate to email. The email cert will be used only for signing and encrypting.

Now you need to update your Dual-Persona email certificates so you can access email from your different accounts. You need to know your DEE email address to complete that process. If you already know the address, go directly to Section 4.

3 Getting Your DEE Email Address

You will need to know your new email addresses to update your certificates and complete your migration to DEE (see Section 5). You will have a DEE email address for each CAC. These can be found in Outlook Web Access (OWA):

1. Open Internet Explorer and go to the following address: <https://web.mail.mil>. You will need to select your PIV Auth cert and click **OK**.

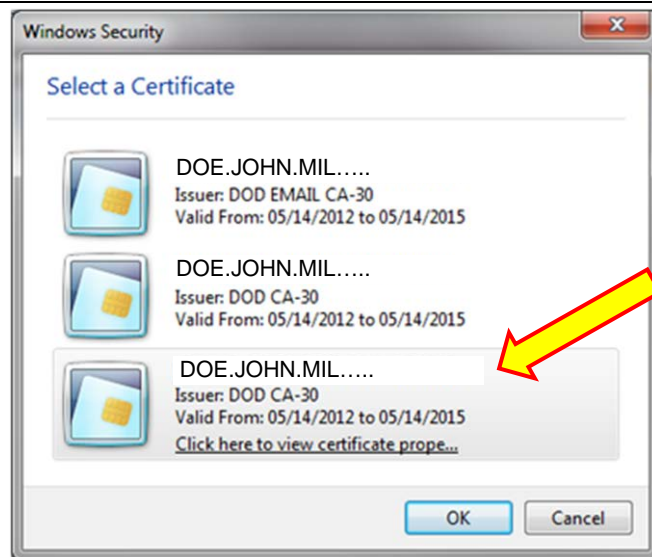


Figure 18. Select a Certificate

2. To verify which certificate is the PIV Auth cert simply highlight your name to reveal the ID number with 16 digits.

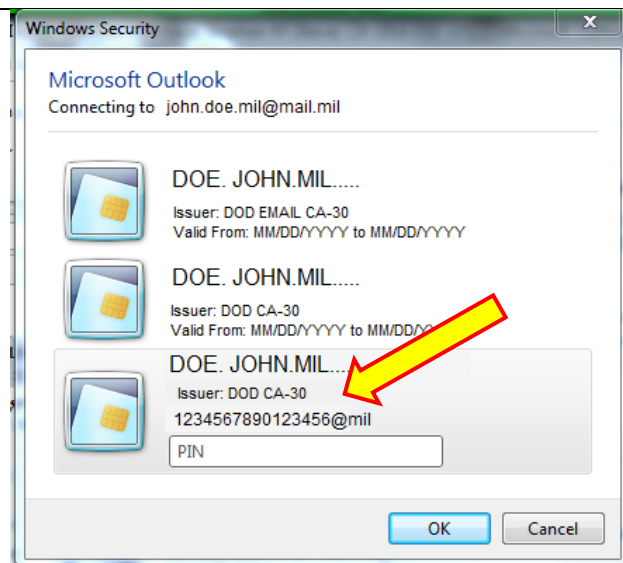


Figure 19. Find the PIV Auth cert

- After you've selected the PIV Auth cert, click **OK** to the **Terms of Use** screen. The Outlook Web App will direct you to the server that supports your DEE service—click on the link.

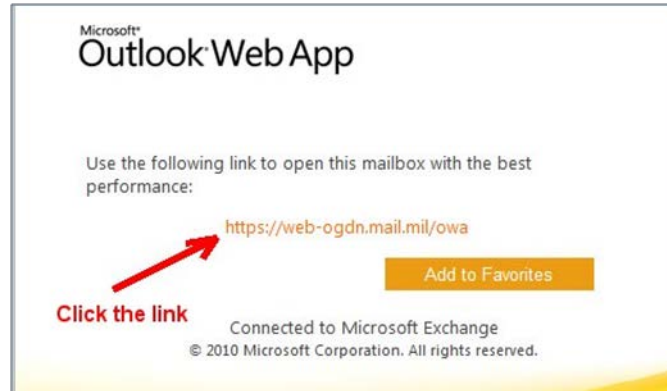


Figure 20. Outlook Web App

- Highlight your PIV certificate and click **OK**. Once in OWA, click the “?” below your name in the upper right-hand part of the OWA screen. Select **About** from the drop-down options.



Figure 21. OWA About

- Your email address is located in the **Mailbox owner** field of the **About** window. Write down or cut and paste your email address to notepad for future reference. This will be needed if you need to configure Outlook to connect to DEE.

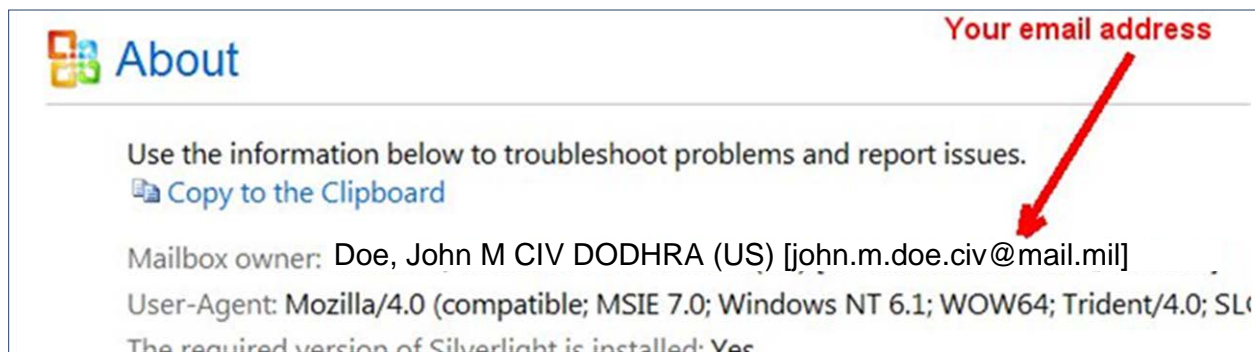


Figure 22. Email address

4 Updating Email Encryption and Signing Certificates: FOR DUAL CAC HOLDERS ONLY

NOTE: THE REASON FOR EXPOSING THE PIV AUTH CERT IS DUAL-PERSONA USERS ARE NOW REQUIRED TO USE IT TO AUTHENTICATE (SIGN ON) TO EMAIL. THE EMAIL CERT WILL BE USED ONLY FOR SIGNING AND ENCRYPTING.

The certificates on a CAC have an SMTP address associated with it. For most users, this certificate will match the legacy (pre-DEE) address, for instance First.Last@US.Army.Mil. Prior to DEE, the same address would exist on both CACs for users that have Dual-Personas.

In the DMDC database both personas can have the same SMTP address, however, in DEE it can only exist once, so there is a separate email address for each persona. To ensure proper functionality of both Outlook and OWA, users must change the SMTP address on their CACs to reflect each of their new DEE mailboxes. The following procedures outline the necessary steps to update the SMTP address on the CAC certificate.

NOTE: Do not proceed with this step unless you are sure you have a Dual-Persona AND have the same email address on both of your CACs.

1. Go to RAPIDS ID Card Office Online: https://www.dmdc.osd.mil/self_service/. Sign on as you did when you activated your PIV Auth cert.
2. At the Welcome to RAPIDS web page select **Change CAC Email**. **Each CAC requires updating. Pick one, update, complete the process, and repeat for all other CACs.**

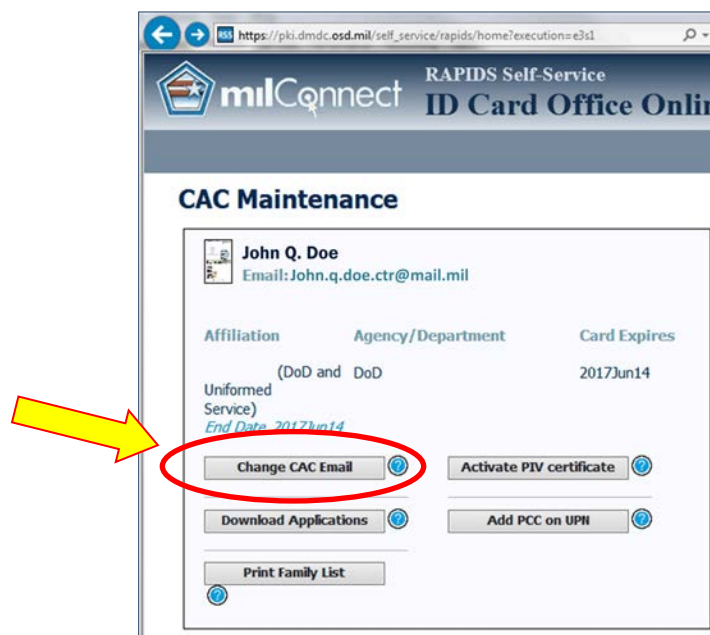


Figure 23. Change CAC Email

- The **Reading CAC** window shows a request to proceed. Click **Proceed** to continue.

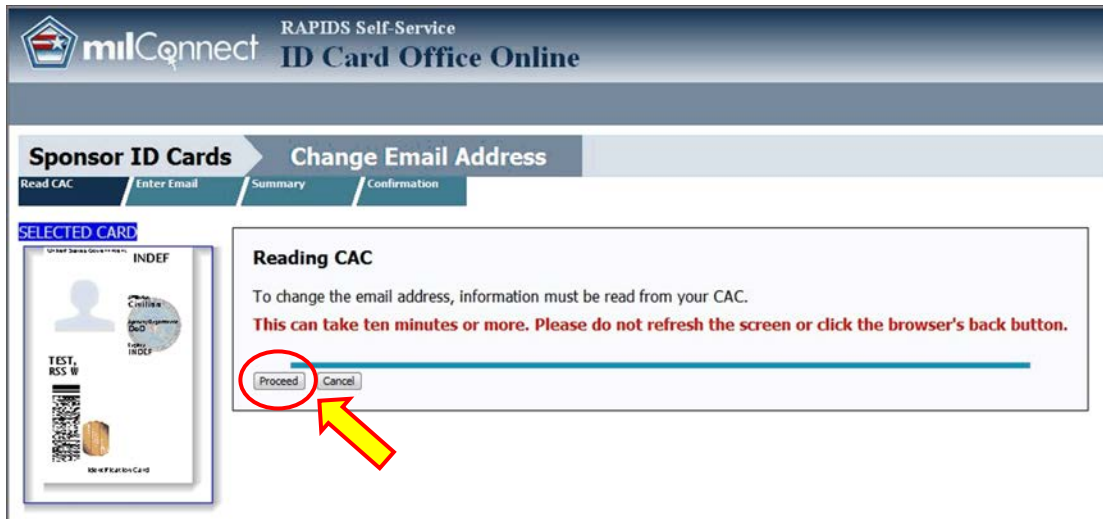


Figure 24. –Proceed to Read CAC

- The **Reading CAC** progress bar appears.

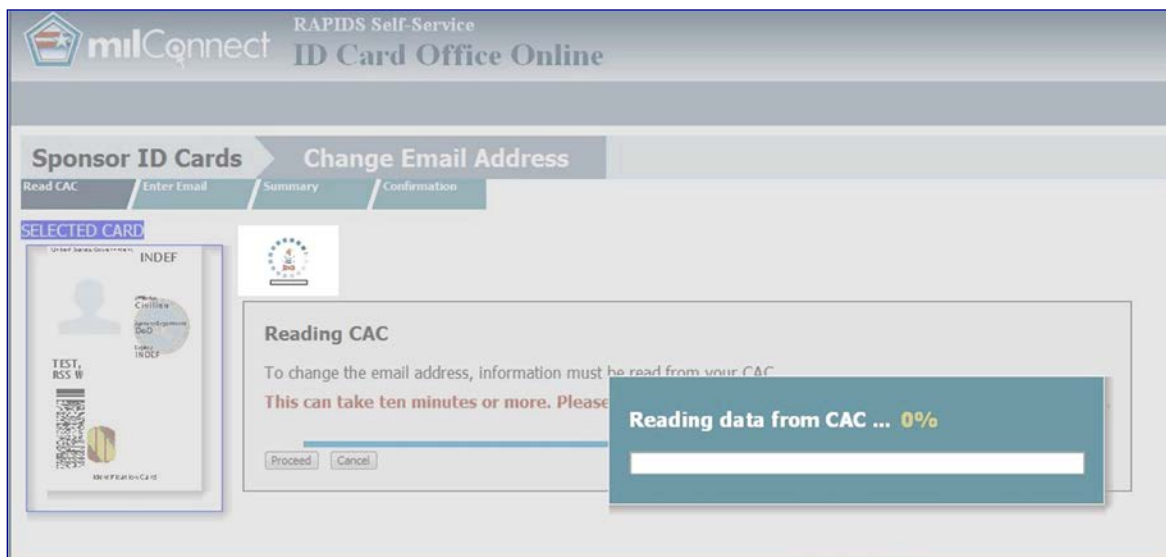


Figure 25. Reading CAC Progress Bar

5. A couple of Client Authentication windows may appear; if they do, select the certificate that you want to use to connect to RAPIDS Self Service ID Card Office Online and click **OK**.

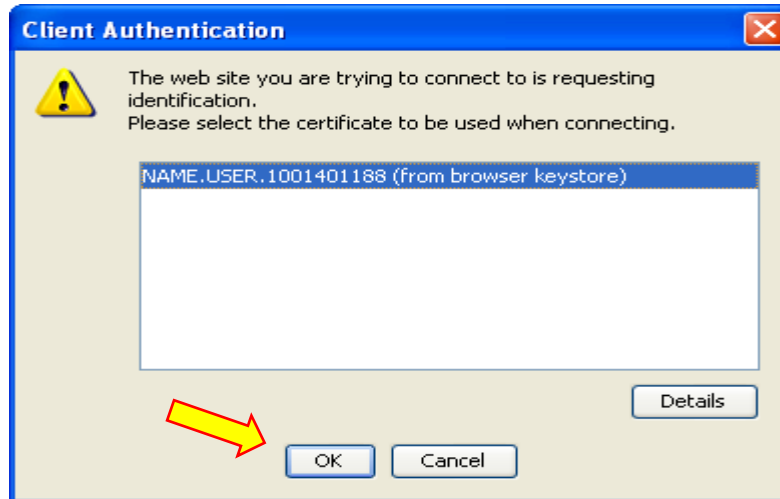


Figure 26. Client Authentication

6. A security warning will open. Click the checkbox to "**Always trust content from this publisher**" and click **Run** to continue.

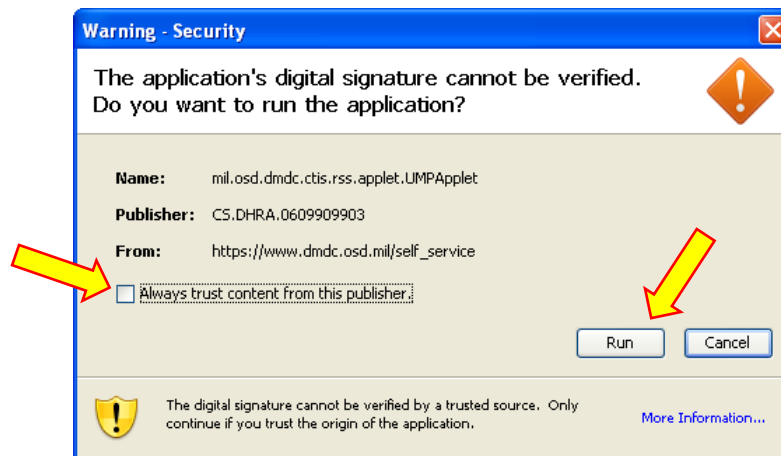


Figure 27. Always trust content

7. Enter and confirm your new DEE email address information in the provided text box. (**NOTE:** You have the option to check **Add PCC on UPN**. Selecting this option will modify your User Principal Name (UPN) to add a Personnel Category Code (PCC) to your email signature certificate. This option should be used if you have multiple CACs). Click **Next** and then click **Update**.

The screenshot shows the 'milConnect RAPIDS Self-Service ID Card Office Online' interface. The 'Sponsor ID Cards' section is active, with the 'Change Email Address' sub-section selected. The 'Enter Email' tab is highlighted. On the left, a 'SELECTED CARD' preview shows a sample ID card for 'TEST, RSS W'. The main area is titled 'Change Email' and displays the 'Current Email Address: test@test.mil'. Below this, there are two input fields for 'Enter new email address' and 'Confirm new email address', both containing 'rrs.test.civ@mail.mil'. A checkbox for 'Add Personnel Category Code to UPN' is present. At the bottom, there are 'Next' and 'Cancel' buttons. A yellow arrow points to the 'Next' button, and another yellow arrow points to the 'Enter new email address' input field.

Figure 28. New e-mail Address

8. The **Change Email Address** process requests confirmation. Click **Yes** to continue.

The screenshot shows the 'Confirmation' step of the 'Change Email Address' process. The 'Sponsor ID Cards' section is active, and the 'Change Email Address' sub-section is selected. The 'Confirmation' tab is highlighted. On the left, a 'SELECTED CARD' preview shows a sample ID card for 'TEST, RSS W'. The main area contains the following text: 'The following actions will be taken on your CAC: Your email address will be updated from test@test.mil to rrs.test.civ@mail.mil. Your email signature certificate will be replaced. The new certificate will have the email address of rrs.test.civ@mail.mil. Your email encryption certificate will be replaced. The new certificate will have the email address of rrs.test.civ@mail.mil. PLEASE READ CAREFULLY. Clicking "Yes" will begin the process that will change the email address on your CAC. Previous email certificates used for encryption and digital signatures will be revoked and replaced with new certificates. This action may require follow-up with your Systems Administration team for recovering old encryption certificate keys and publishing your new certificates. This update can take minutes or longer. Please do not refresh the page or click the back button.' Below this text, there is a question 'Do you want to continue?' with 'No' and 'Yes' buttons. A yellow arrow points to the 'Yes' button.

Figure 29. Change Email - Yes

9. **ID Card Office Online** displays the progress of your update.

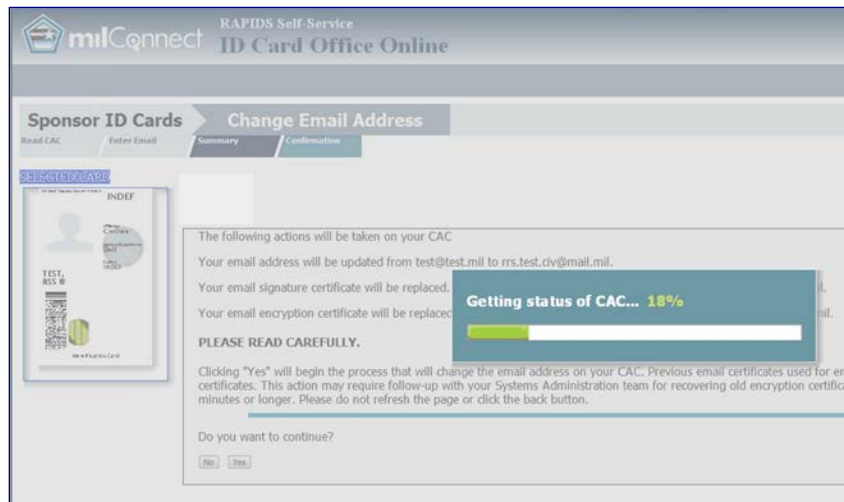


Figure 30. Progress of update

10. Once **ID Card Office Online** has completed processing, the screen will notify you of successful completion. Click the **Home** tab. To update other CACs, log off, remove the CAC you just updated, log in with the other CAC, and repeat the process to update it.

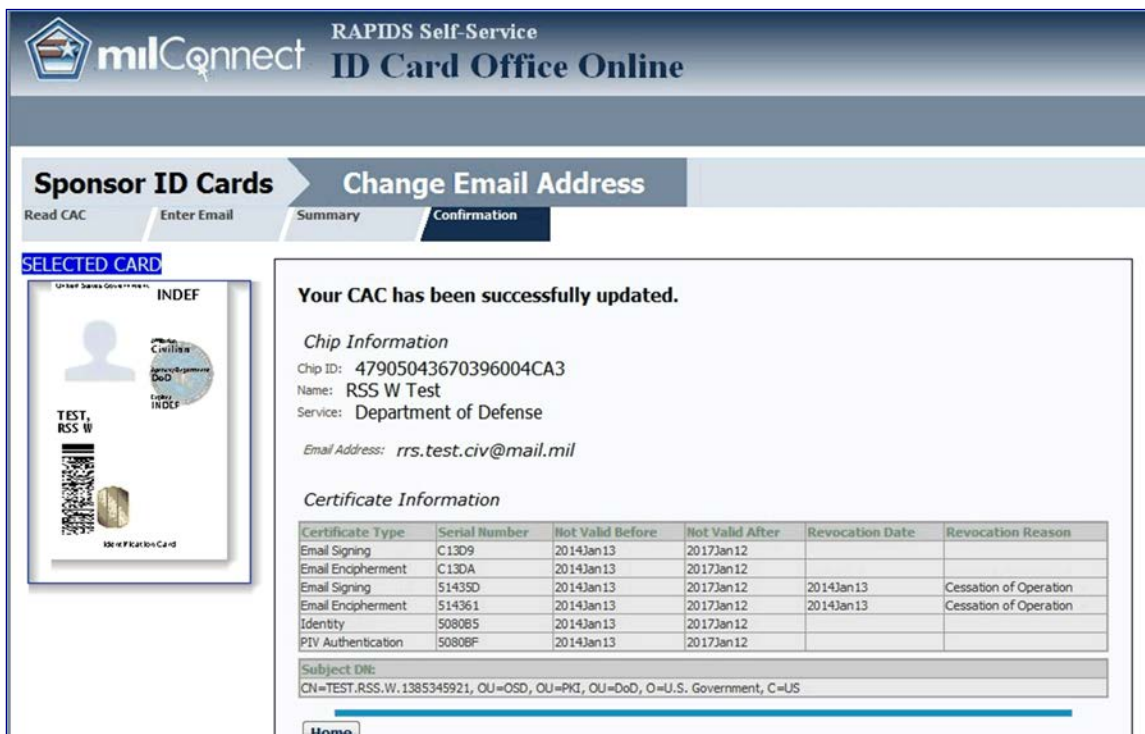


Figure 31. CAC is successfully updated.

Appendix 1: Troubleshooting Dual-Persona PIV Auth Cert Process

A.1 Compatibility Conflict: 32-bit vs. 64-bit settings

Some people receive a RAPIDS ID Card Office Online error message regarding a compatibility conflict that exists between settings related to 32-bit and 64-bit desktop installations. As more users upgrade their Operating System (OS) to 64-bit compatibility, issues may arise if using ActivClient, Internet Explorer (or other browsers), and JRE versions that are not the same bit level. Please confirm that your ActivClient Middleware, JRE, and browser (Internet Explorer or an alternative) are all set to the same bit:

- ActivClient (32-bit), JRE (32-bit), and Internet Explorer (32-bit) or
- ActivClient (64-bit), JRE (64-bit), and Internet Explorer (64-bit).

Any inconsistency among those three components means that you will not be able to use RSS and/or other smart card-enabled applications.

Another documented problem is where a mission partner's Outlook 2007 32Bit Mail Client that may not read Dual-Persona certificates managed on a 64Bit Windows 7 platform. A system patch has corrected the issue under most circumstances. If such a problem should occur for Dual-Persona individuals, check with your Service Desk and refer to this document:

"Windows 7 64x AGM and Dual-Persona's Outlook 2007, and 32Bit Client"

A.2 Problem accessing RAPIDS ID Card Office Online

If there is a problem accessing the RAPIDS Self Service web site, contact the DMDC Support Center (DSC) at 1-800-372-7437.

A.3 PIV Auth cert is enabled, problem accessing DEE

If someone's PIV Auth cert is enabled, but there are problems accessing DEE- for guidance or help checking their provisioned account try contacting:

- The appropriate Network Enterprise Center/CONUS-Theater Network Operations and Security Center (NEC/CTNOSC) or
- The DEE team via the Mission Partner local help desk.

A.4 Personnel data seems to be incorrect

If someone's personnel data seems to be incorrect and not reflect their affiliations correctly, try the DMDC Support Office at 1-800-538-9552.

Abbreviations, Acronyms, and Definitions

The following abbreviations, acronyms, and definitions aid in the understanding of this document.

Abbreviations and Acronyms	Description
CAC	Common Access Card – Identification and sometimes benefits and privilege card produced by the DoD, which contains an Integrated Circuit Chip (ICC) holding demographic data and digital certificates
DEE	DoD Enterprise Email
DISA	Defense Information Systems Agency
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DSC	DMDC Support Center
DSLogon	Unique Logon ID and Password given to DoD Beneficiaries to access DoD web applications in lieu of a CAC
EDIPI	Electronic Data Interchange Personal Identifier
FASC-N	Federal Agency Smart Credential Number
JRE	Java Runtime Environment
OWA	Outlook Web App (the application...not Outlook Web Access)
OWA	Outlook Web Access (the DEE Web-based email service)
PCC	Personnel Category Code
PIV Auth cert	Personal Identity Verification Authentication Certificate
RAPIDS	Real-time Automated Personnel Identification System – Application used to update data on the DEERS Person Data Repository (PDR) and create DoD Identification cards
RSS	RAPIDS Self Service
UPN	User Principal Name