

## Common Access Card (CAC) Modernization

What is CAC Modernization, and why do I need to take action?

The Coast Guard will transition to a new authentication method for the Common Access Card (CAC), to align with the rest of the federal government. To prepare for this transition, all personnel must have the new “Authentication” certificate on their CAC, so if you were notified, you must follow this guidance. On 02 April 2020, CG-6 released ALCOAST 119/20 - COMMON ACCESS CARD (CAC) MODERNIZATION – CAC HOLDER GUIDANCE, to provide guidance and directions for logging into CG workstations, systems, and applications using the new authentication certificate. The CAC is the Coast Guard’s primary means for authentication to access unclassified networks, information systems, and applications.

### Activating the PIV-Auth (“Authentication”) Certificate (Adding the Certificate to the CAC)

#### **IMPORTANT NOTICE:**

- 1.) It is **HIGHLY** preferred to access the website below using Internet Explorer from a Coast Guard workstation.
- 2.) If you receive an error stating JAVA needs to be installed, submit a ticket to CGFIXIT requesting JAVA be repaired and/or attempt these steps from another workstation.
- 3.) If adding the certificate to your CAC from a remote location, the following computer configurations are required; (Coast Guard laptops should already be properly configured)
  - ✓ CAC reader with ActivClient 7.1 or higher
  - ✓ Java 8 - Update 144 or higher
  - ✓ Internet Explorer 7 or higher

Updating CAC certificates does **NOT** work with Virtual Desktop Infrastructure (VDI). If using a Coast Guard issued laptop, ensure laptop is connected to the Internet, and do NOT sign into Virtual Private Network (VPN) before attempting to update CAC certificates. Personal computers must have the configurations noted above.

If unable to update your CAC online with the instructions provided below, you will need to schedule an appointment at the nearest available RAPIDS/DEERS (ID office) to complete this action. The RAPIDS Appointment Scheduler is located at <https://rapids-appointments.dmdc.osd.mil/>

- 1) Highlight the link below, copy and paste into another window (Internet Explorer) to be directed to the DMDC site:

[https://www.dmdc.osd.mil/self\\_service/rapids/unauthenticated?execution=e1s1](https://www.dmdc.osd.mil/self_service/rapids/unauthenticated?execution=e1s1)

2) Click **Sign In**

**milConnect** RAPIDS Self-Service  
**ID Card Office Online**

**Notice:**  
Any Operations that update your CAC or require digital signing of requests (nominating family members, creating Form DD1172-2, reissuance of family update 144 or higher, and Internet Explorer version 7 or higher. Please ensure your computer meets these minimum requirements before performing activities.

## Sign In

**Renew/Replace Family ID Cards**  
Renew/Replace Family ID Cards  
Update Your Contact Information  
Update a Family Member's Contact Information  
Add a Family Member

**CAC Maintenance**  
Update Your Email Address  
Download Applications  
Activate the PIV Authentication Certificate  
**ADD PCC TO UPN**

**2**

**Need Assistance?**  
For issues with your ID card or problems with sponsor or family member data, please contact a local ID card office.  
  
If you are having problems with this website please contact us.

Contact DMDC || Accessibility/Section 508 || USA.gov || No Fear Act Notice || Privacy and Security Notice

3) The *DEERS Self-Service Consent to Monitor* window appears. Click **OK**.

**DMDC** Serving Those Who Serve Our Country  
**ID Card Office Online**

### Self-Service Consent to Monitor

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG beneficiary self-service-authorized use only.

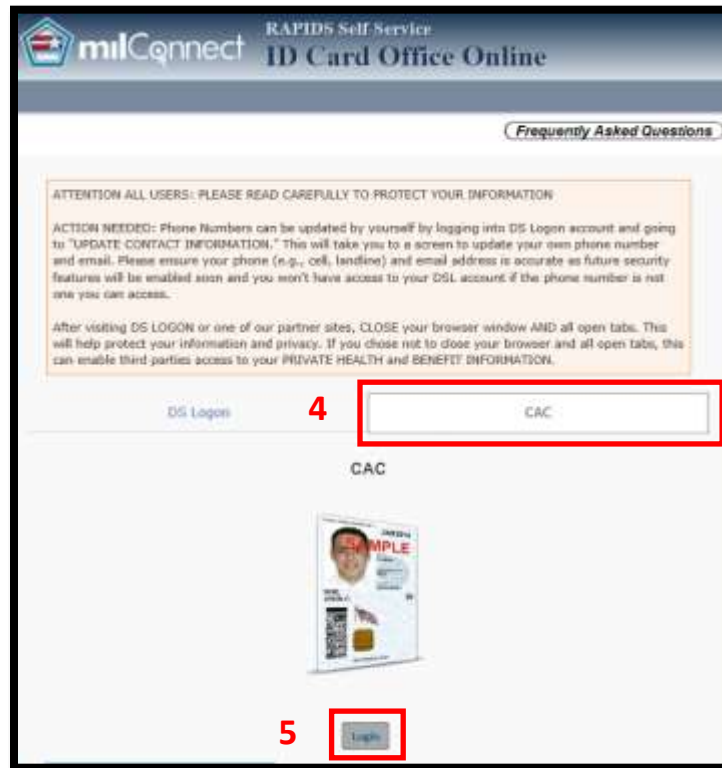
By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- While all personal identifying information (PII) data stored on this IS is protected under the Privacy Act of 1974, all communications using this IS, and the data contained therein, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications or information, or the content of confidential business communications or information, or the content of confidential communications or information of representatives of the news media, or the content of confidential communications or information of religious, labor, or other groups. Such communications and work product are private and confidential. See 5 U.S.C. 552a.

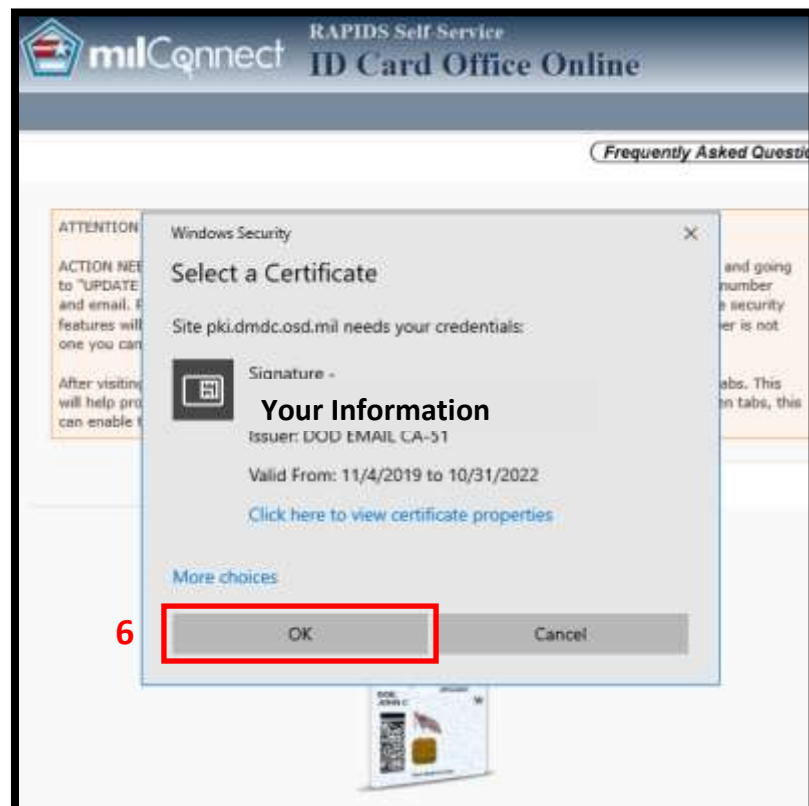
**3**

Contact DMDC || Accessibility/Section 508 || USA.gov || No Fear Act Notice

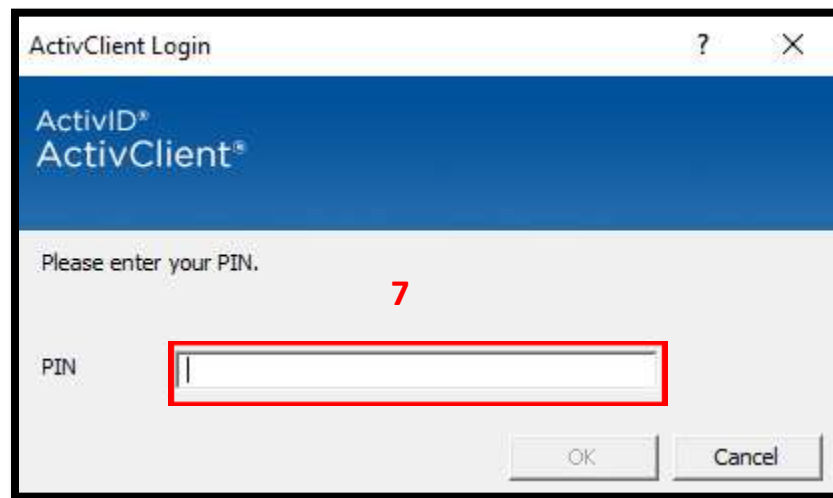
- 4) Click the **CAC** tab.
- 5) The Common Access Card (CAC) window appears. Click **Login**.



- 6) The *Select a Certificate* window appears. Select the 'DOD email' certificate which is the current authentication certificate accepted. Select **OK**.



7) Enter your PIN



ActivClient Login

ActivID®  
ActivClient®

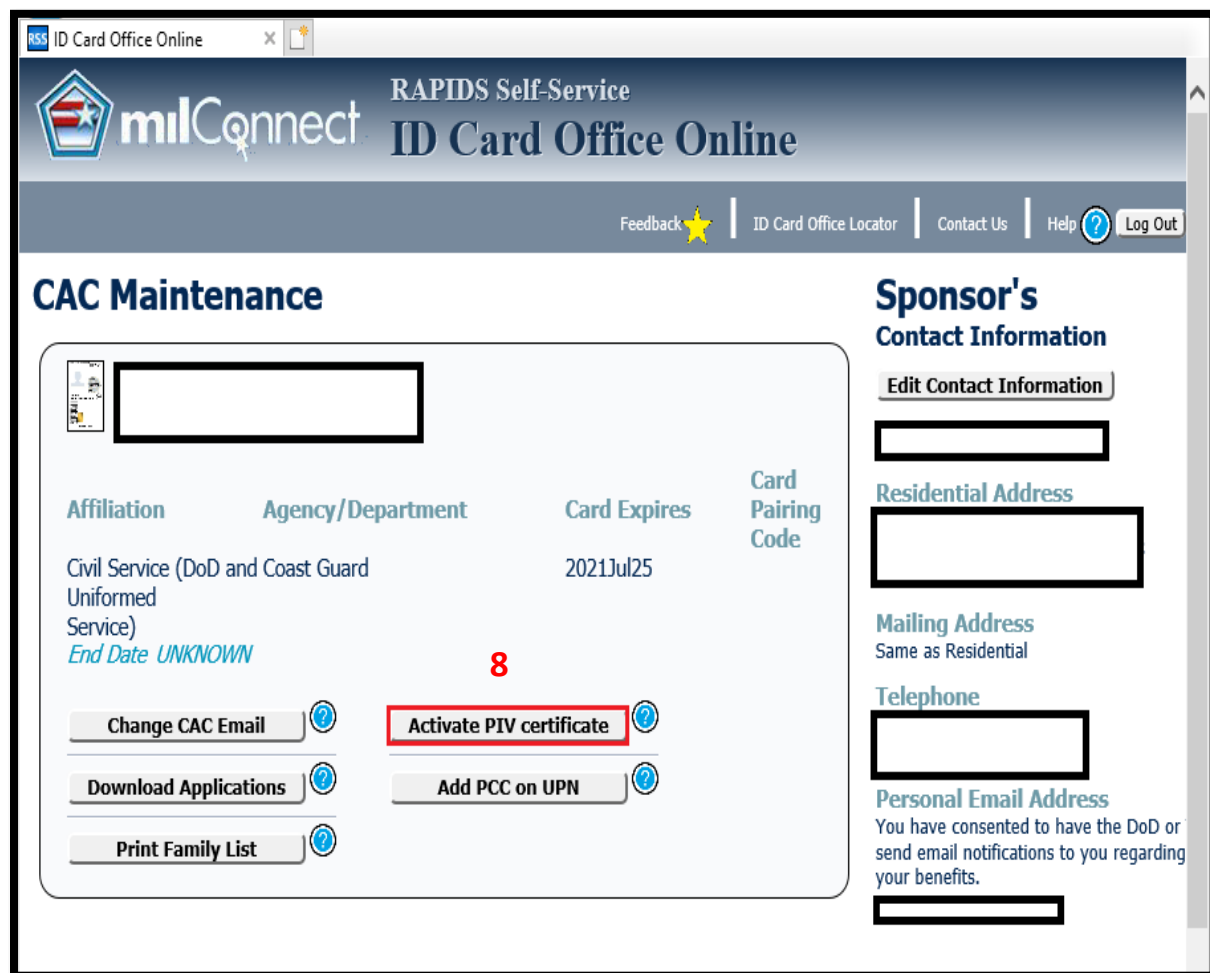
Please enter your PIN.

PIN

OK Cancel

A red box highlights the PIN input field, and a red number 7 is centered above it.

8) The RAPIDS Self Service window appears. Select Activate PIV Certificate.



RAPIDS Self-Service  
ID Card Office Online

Feedback ★ ID Card Office Locator Contact Us Help ? Log Out

### CAC Maintenance

Affiliation	Agency/Department	Card Expires	Card Pairing Code
Civil Service (DoD and Coast Guard Uniformed Service)		2021Jul25	
End Date UNKNOWN			

8

Change CAC Email ?

Download Applications ?

Print Family List ?

Activate PIV certificate ?

Add PCC on UPN ?

### Sponsor's Contact Information

Edit Contact Information

### Residential Address

### Mailing Address

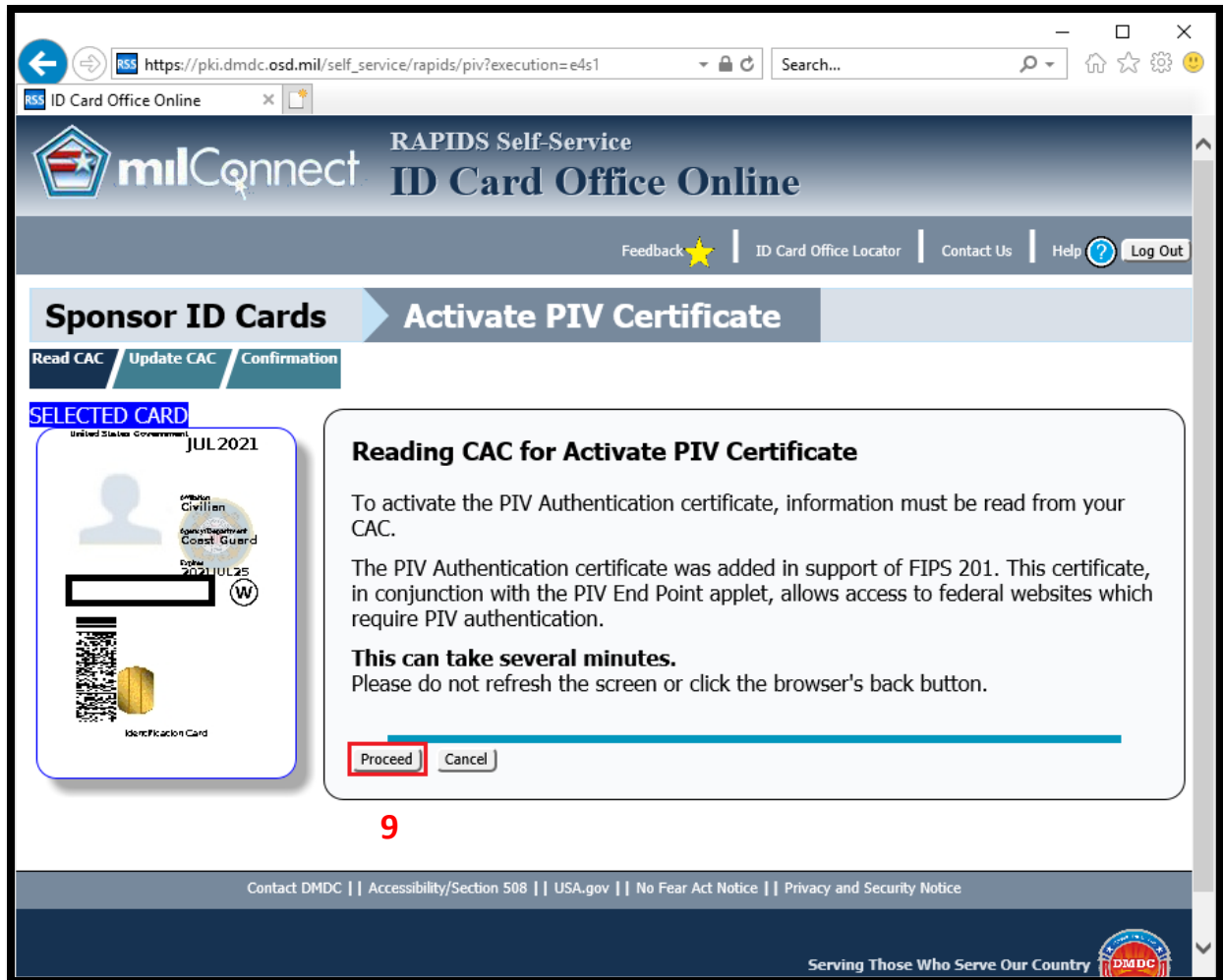
Same as Residential

### Telephone

### Personal Email Address

You have consented to have the DoD or send email notifications to you regarding your benefits.

9) The PIV Update window appears. In the PIV Information section, click **Proceed**.

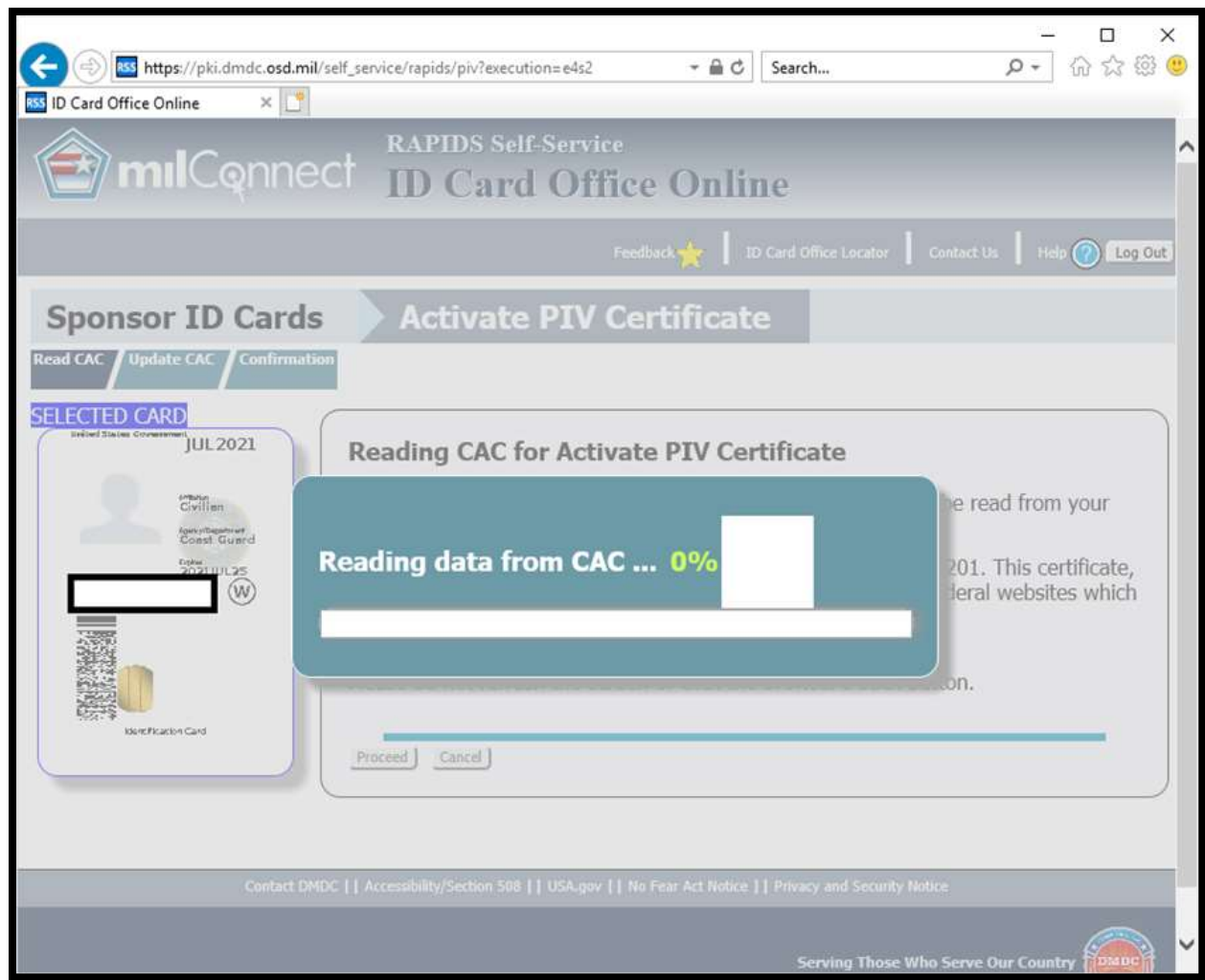


9

**NOTE:** If presented with the “Java Update Needed” window, click **Later** (Continue and you will be reminded to update again later.)



The Reading data from CAC Window appears.



**NOTE:** If your CAC has the PIV-Auth ("Authentication") certificate activated by default, or you have previously manually activated the PIV-Auth certificate, then you will receive the following: If you don't receive the following screen, proceed to **10**.

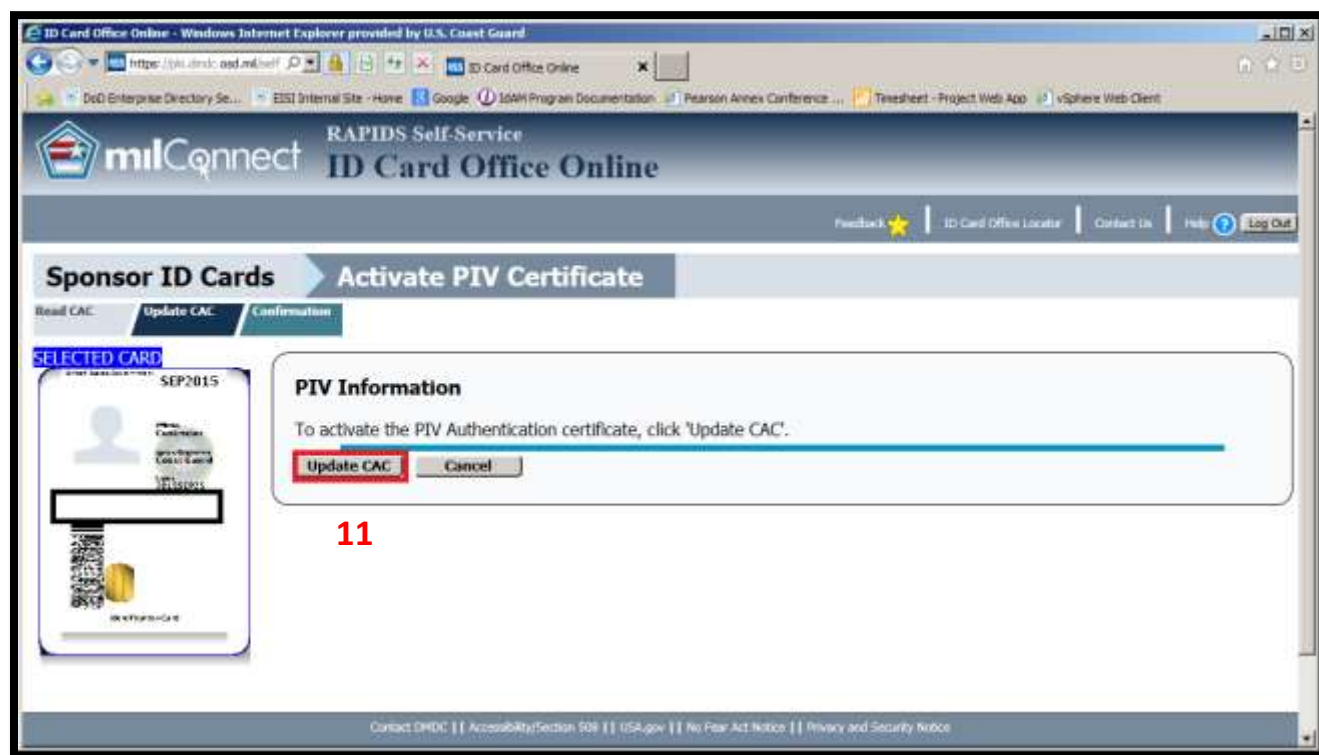




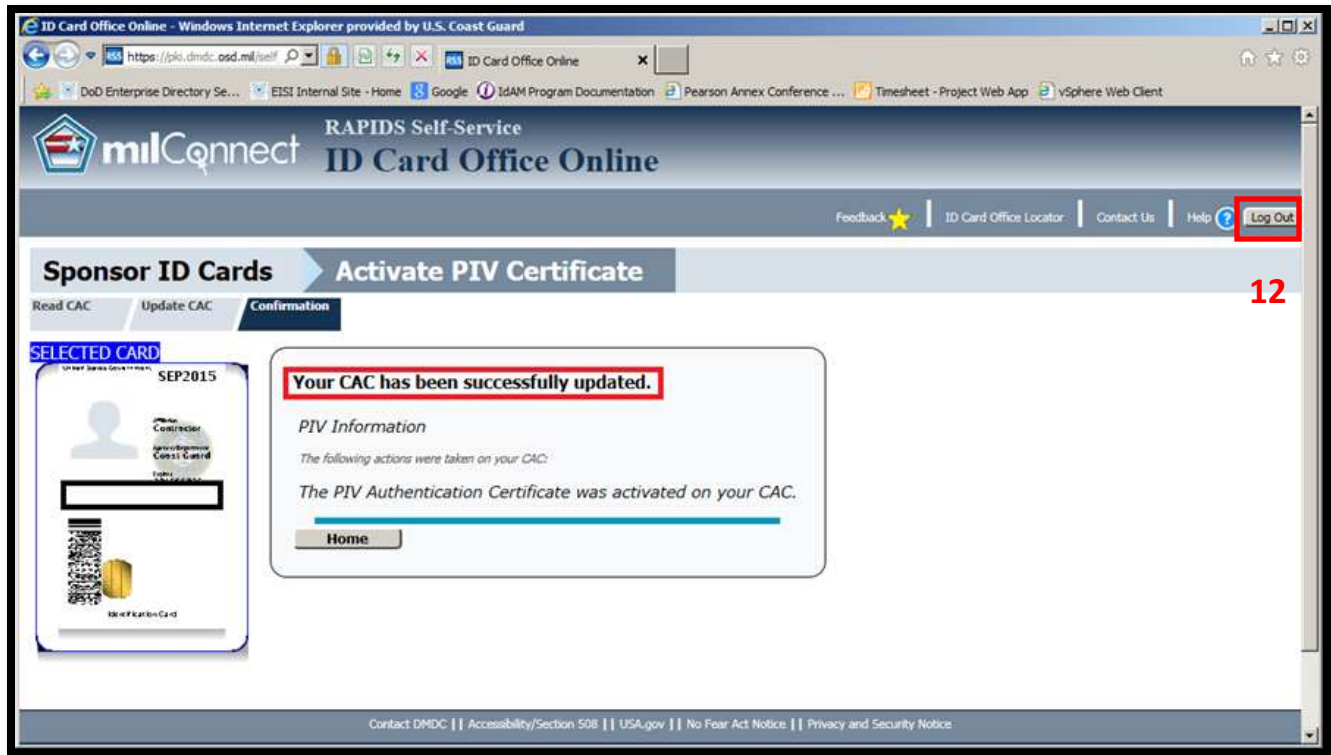
10) The *ID Card Office Online Applet* window appears. Click **Run**.



11) The PIV Update window appears. Click **Update CAC**.



12) The PIV Update window displays “Your CAC has been successfully updated”. Click **Log Out**.



Great, your PIV-Auth (Authentication) Certificate is now activated (added to your CAC)!

**No further action is required at this time.**

Thank you for your cooperation!

### Experiencing Issues Updating your CAC?

If you have any questions throughout this process, you should submit a CGFIXIT request via the CGFIXIT icon on your desktop and proceed to:

I NEED HELP WITH > MY CAC OR LOGIN > REQUEST NOW > I AM HAVING OTHER CAC ISSUES NOT IDENTIFIED ABOVE.

If unable to log in to a Coast Guard workstation contact the Centralized Service Desk Branch (CSDB) at 1-855-CG-Fixit (1-855-243-4948) (option 1, 1, 3).

Do you have questions about CAC Modernization? Please refer to the Frequently Asked Questions (FAQ's) at <https://www.dcms.uscg.mil/CAC/>