Frequently Asked Questions

**Naval VAMOSC Public Key Infrastructure/
Common Access Card (PKI/CAC) Registration and Log in**

Please Note: A PKI-enabled browser is required for certificate registration and to log in to Naval VAMOSC System.

GENERAL INFORMATION

Q: What is a CAC and how does it relate to software certificates and PKI?

Q: Am I required to have a CAC?

Q: What is an External Certificate Authority (ECA)?

Q: Where can I get help regarding my Public Key Infrastructure (PKI)**?**

Q: Where can I obtain a CAC?

Q: Where are the nearest CAC / I.D. Card office locations in the Military District Washington area?

Q: Where can I get the Forms that I need to fill out?

Q: What information should you bring when obtaining a Common Access Card (CAC)?

Q: My certificate is expired. How do I receive a new one?

Q: My certificate is revoked. How do I receive a new one?

Q: If I don't have my CAC available, can I still log in to the Naval VAMOSC System?

CAC REGISTRATION

Q: How do I register a CAC?

Q: I am presented with more than one certificate in the Client Authentication window; which one do I select?

Q: My certificate does not show up in the Client Authentication window, what do I do?

Q: The Client Authentication window does not appear after clicking "Register Certificate." How do I resolve this?

CAC LOG-IN

Q: How do I log in using a CAC?

Q: Where do obtain all of the trusted DoD PKI and ECA PKI root and intermediate CA certificates?

Q: The Client Authentication window does not appear after clicking "Log in with CAC." How do I resolve this?

Q: I registered my CAC, but receive an error message when attempting to log in. What do I do?

ERROR MESSAGES

Q: I was redirected to a "Page cannot be displayed" URL. What could be the cause?

Q: I see an error page indicating that an error has occurred with my CAC log in. What does this mean?

Q: After placing my CAC in the reader, I get the following message: "You have three (3) attempts to correctly enter your Personal Identification Number for your CAC." Why am I receiving this message?

If your question is not included in this list of FAQs, please email *Naval VAMOSC Support at support@navyvamosc.com*.

GENERAL INFORMATION

What is a CAC and how does it relate to software certificates and PKI?
The Common Access Card (CAC) is a Department of Defense (DoD) smart card (credit card-size device that contains one or more integrated circuits) initiative currently underway across the Agency. The CAC will serve as the following: Standard ID card for active-duty military personnel (to include the Selected Reserve), DoD civilian employees, and eligible contractor personnel; principal card used to enable physical access to buildings and controlled spaces; principal card used to enable computer network and system access; and primary platform for the PKI authentication token. A CAC will contain a user's software certificate, which is a computer-generated record that ties the user's identification with the user's public key in a trusted bond. The certificate contains the following (at a minimum): Identity of the issuing Certification Authority, identity of the user, and the user's public key. A Public Key Infrastructure (PKI) provides an electronic framework (i.e., software and a set of rules and practices) for secure communication and transactions between organizations and individuals. A PKI is based on asymmetric encryption and digital signatures technologies.

Am I required to have a CAC?
DoD users and contractors that remotely access these sites will require the PKI certificate found on the Common Access Card (CAC). Non-DoD Federal Government users and contractors without the ability to use CAC will need to acquire an External Certificate Authority (ECA) certificate from an approved Certificate Authority for access.

All DoD employees (military and civilian), including DoD contractors, obtain certificates from DoD PKI via the CAC. This means that all DoD employees and contractors must have a CAC card.

To use your CAC, a CAC reader, Active Client software, and the DoD Root Certification Authorities are required. Root Certificates and installation instructions can be found on the following website: http://dodpki.c3pki.chamb.disa.mil.

As stated above, non-DoD Federal Government users will need to obtain an ECA certificate from an approved Certificate Authority to access these sites.

What is an External Certificate Authority (ECA)?
ECA's provide digital certificates to DoD private industry partners, contractors using their own equipment or working in non-government facilities, allied partners, and other agencies.

Approved ECA vendors:

- **IdenTrust, Inc. (formerly DST)**
  http://www.identrust.com/certificates/eca/index.html
- **Operational Research Consultants, Inc. (ORC)**
  http://www.eca.orc.com/
- **VeriSign, Inc.**
  http://www.verisign.com/verisign-business-solutions/public-sector-solutions/ieca-eca-certificates/index.html

Where can I get help regarding my Public Key Infrastructure (PKI)?
For information on your PKI please visit the following website: https://infosec.navy.mil/pki. This website requires a certificate to access it, so you may also call or email for information: SPAWAR Integrated Support Center Helpdesk 1-800-304-4636/DSN 588-4286 or itac@infosec.navy.mil

Where can I obtain a CAC?
See your Local Security Officer or if you are a contractor for DoD, then you should contact the DoD office you are supporting (your sponsor).

Where are the nearest CAC / I.D. Card office locations in the Military District Washington area?
Additional information for obtaining a Command Access Card (CAC) can be found on HQDA Military Personnel Service Center website (http://www.hqda.army.mil/MPSC/alternate.htm).

Where can I get the Forms that I need to fill out?

http://www.hqda.army.mil/MPSC/forms.htm

Smart Card / DoD Common Access Card Request Form DD Form 1172-2

DD Form 577

What information should you bring when obtaining a Common Access Card (CAC)?

1. Update your DEERS contact information. (https://www.dmdc.osd.mil/appj/address/index.jsp)

2. Have a 6 to 8 digit (numerical) Personnel Identification Number (PIN) in mind as you will need to provide this when they are processing your action at the CAC Issuance Office.

3. Complete DD Form 1172-2

4. Military and Civil Service Employees (including appropriated and non-appropriated funded and direct and indirect hire foreign nationals)

   a. Two forms of identification; one must bear a picture, bring your current/expired government issued ID card.

   b. Social Security Card.

   c. Your Army Knowledge Online email address if you use a government computer (exceptions to AKO account are OJCS and OSD). Be sure to print clearly your full internet e-mail address (not your display name).

* If you don't have an AKO account you may obtain one by visiting the AKO Website: http://www.us.army.mil

* If you bring the wrong e-mail address and/or it is entered incorrectly, you will have to return later to correct it.

* Personal e-mail addresses (i.e., AOL, Hotmail, Yahoo accounts, etc.,) will not be accepted.

   d. Civil Service employees that are enrolled and inputted into DEERS, after In-processing with the Civilian Personnel Advisory Center (CPAC), can call to verify DEERS enrollment by calling (703)-602-0327 or 0349.

My certificate is expired. How do I receive a new one?
Each certificate has a validity period after which it expires. This period is set when the certificate is written to your CAC. Contact your local Security Officer or if you are a contractor for DoD, then you should contact the DoD office you are supporting (your sponsor).

My certificate is revoked. How do I receive a new one?
Your card may have been reported lost, stolen, or compromised. Contact your local Security Officer or if you are a contractor for DoD, then you should contact the DoD office you are supporting (your sponsor).

If I don't have my CAC available, can I still log in to the Naval VAMOSC?

You will not be able log in to the Naval VAMOSC using your Naval VAMOSC User ID and password without a CAC or ECA/PKI Certificate.

Note: If you do not have a User ID and password, select the Registration link on the Naval VAMOSC Home Page and sign up. For further questions email support@navyvamosc.com.

CAC REGISTRATION

How do I register my CAC/ECA with the Naval VAMOSC System?
Using a PKI-enabled browser, access the Naval VAMOSC Home Page (https://www.navyvamosc.com and select "Register Certificate" under the "Access the Database" Section.

I am presented with more than one certificate in the Client Authentication window; which one do I select?
Some users may find more than one certificate available for selection. This scenario may occur if a user's CAC or ECA has recently expired, and the user was issued an updated certificate. The expired certificate will remain stored in the browser's list of available certificates, and therefore, display in the Client Authentication window. To determine the validity of each certificate, highlight one of the certificates from the list displayed in the Client Authentication window (click on the certificate name) and click "View Certificate." The details of the certificate will include the expiration date. To remove a certificate from displaying in the Client Authentication window, go to Tools --> Internet Options --> Content --> Certificates, select the appropriate certificate, and click "Remove."

Note: If the incorrect certificate was inadvertently deleted, it will automatically re-install once the CAC is placed in the reader.

My certificate does not show up in the Client Authentication window, what do I do?
This may be due to one of the following reasons: your certificate is not installed/registered through the ActivCard Gold Utilities; your certificate has never been used with the web browser before; your certificate is un-trusted by the Naval VAMOSC Web Server; or your browser or CAC reader is configured incorrectly. If your certificate was not installed on this machine, please contact your local help desk support. If your certificate has not been used by a web browser on this machine, enter your CAC into the reader to import your software certificate into the browser. For the ECA, you must follow the instructions provided to you when you received your certificate. If your certificate is un-trusted by the Naval VAMOSC Web Server, contact the *Naval VAMOSC Team by email at support@navyvamosc.com*.

Note: If you are attempting to register a software certificate, your certificate must be imported into the browser. To enter a software certificate within IE, go to Tools --> Internet Options --> Content --> Certificates --> Import and follow the wizard to find and import your certificate. To enter a software certificate within Netscape (7.0 or later), go to Edit --> Preferences --> Privacy & Security --> Certificates --> Manage Certificates --> Import and follow the instructions to import your certificate. To download the Root CA Certificate into Netscape, visit the DoD Class 3 PKI website and follow the provided instructions: http://dodpki.c3pki.chamb.disa.mil/rootca.html.

The Client Authentication window does not appear after clicking "Register Certificate." How do I resolve this?
You may need to close the active browser window(s) and open a new one to attempt the process again. This scenario will occur when a user has cancelled out of a portion of the registration process. The browser will store a previous selection in its cache, which will require the user to clear the cache before making a different selection.

CAC LOG IN

How do I log in using a CAC/ECA?
Using a PKI-enabled browser, access the Naval VAMOSC Home Page at (https://www.navyvamosc.com). Click "Log In", then click "Log In with Certificate", then select the appropriate certificate from the Client Authentication window, and enter your PIN when prompted (if applicable).

> **Note**: If you are trying to register your certificate, please follow the directions under "How do I register a CAC?"

Where do obtain all of the trusted DoD PKI and ECA PKI root and intermediate CA certificates?
https://www.dodpke.com/InstallRoot/
Install and manage DoD authorized root and intermediate Certification Authorities (CAs) on Microsoft-based operating systems.
NOTE: This versions requires a Java Runtime Environment(JRE) to be installed.

The Client Authentication window does not appear after entering the Naval VAMOSC URL. How do I resolve this?
You may need to close the active browser window(s) and open a new one to attempt the process again. This scenario will occur when a user has cancelled out of a portion of the registration process. The browser will store a previous selection in its cache, which will require the user to clear the cache before making a different selection.

I registered my CAC, but receive an error message when attempting to log in. What do I do?
Previously, software certificates were stored directly in a user's web browser. The more recent DoD CAC initiative eliminates this need by providing the user with a mobile certificate stored directly on their Card. During this transition period, some users will find they have two separate certificates from which to choose. A user might inadvertently register their local certificate instead of their CAC certificate in Naval VAMOSC. However, Naval VAMOSC will allow a user to register only one certificate at a time; subsequent certificate registrations will preempt a previous registration. For example, if a user has an active software certificate stored in their browser and attempts to register it through Naval VAMOSC, they will not be able to register an additional certificate (i.e., their CAC) without overriding the previous certificate's registration. In order to avoid this scenario, it is suggested to use a CAC for all Naval VAMOSC access, but it is accessible through an ECA.

ERROR MESSAGES

I was redirected to a "Page cannot be displayed" URL. What could be the cause?
There are three known circumstances when this will apply: The user has attempted to log in or register an expired certificate, the user has canceled out of the PIN entry window for their CAC/ECA, or the user has logged out of Naval VAMOSC and attempted to log in using their CAC/ECA without closing the browser. To rectify this problem, close the existing browser window and open a new window; this will clear the cache and enable the user to continue.

Note: To verify the expiration on your certificate using IE, select your certificate from the Client Authentication window, highlight the correct certificate, and click "View Certificate." The certificate validity dates will be displayed at the bottom of the "General" tab. Your CAC also displays the expiration date in the bottom right corner on the face of the card. If you determine your card is valid, but are having trouble accessing Naval VAMOSC, please contact the *Naval VAMOSC Team by email at support@navyvamosc.com*.

I see an error page indicating that an error has occurred with my CAC/ECA log in. What does this mean?
This is likely due to an unavailable resource on Naval VAMOSC. If the problem persists, please contact the *Naval VAMOSC Team by email at support@navyvamosc.com*.

After placing my CAC in the reader, I get the following message: You have three (3) attempts to correctly enter your Personal Identification Number for your CAC. Why am I receiving this message?
After the third consecutive attempt, your CAC is locked and you will not have access to your PKI certificates. You MUST have your CAC unlocked at a CAC PIN Reset (CPR) workstation. The Naval VAMOSC Support team CANNOT unlock your CAC.