Common Access Cards (CACs) and Certificate Recovery Frequently Asked Questions

NETWORKS AND INFORMATION INTEGRATION

ASSISTANT SECRETARY OF DEFENSE

DOD CIO

May 26, 2010

Table of Contents

FAQs

Q1. What are the requirements of reissuing CACs in a Joint Base environment?

Under the joint base construct, some DoD civilian employees will be transferring from their current Service employer (supported Component) to another Service employer (supporting Component). Per the current CAC policy, DTM-08-003, the CAC must be reissued when employees will no longer be employed by their original Service or Agency as identified on their existing CAC.

Civilian Guidance

When the parent service organization of a DoD civilian employee changes from one Service to another due to joint basing activities, that employee's CAC must be reissued. For example, if the Army is the supported Component and the Air Force is the supporting Component, then any Army employees transferring to the Air Force must be issued a new CAC.

Military Guidance

Military members will not require reissuance of a CAC based on joint basing activities.

Contractor Guidance

Contractors are affected only if the Service sponsoring the contract will change as a result of joint base alignment. For contracts that will be changing Service sponsorship, the Contractor Verification System (CVS) trusted agent (TA) administering personnel under the contract should directly coordinate with the supporting Service to ensure that proper contract "handoff" activities are accomplished.

Back to Table of Contents

Q2. When do I get my new supporting agency CAC?

The civilians will be contacted by their Human Resources office. They will be required to visit the ID card office twice; once to pre-process their supporting Component CAC prior to the transition date, and once to turn in their supported Component CAC and receive their supporting Component CAC after the transition date.

They will not be able register and use the new, supporting Component CAC until after their official transfer date. Non-appropriated civilian employees transfer on 1 October 2010; appropriated civilians transfer on 10 October 2010.

Back to Table of Contents

Q3. What steps do I need to take to complete initial set-up of my new CAC and certificates on my computer?

To use the PKI certificates on the CAC, the user needs to complete the initial set-up of the CAC and the certificates with the user's computer. Typically, the CAC middleware application will read information from the CAC to import PKI certificate information to the user's computer. Insert the CAC into the CAC reader and allow the middleware application to read the CAC. The certificates from the CAC should automatically import to the operating system and Microsoft Outlook.

Importing Certificates into Microsoft Outlook

The steps below provide instructions on how to import and configure Microsoft Outlook 2007 Client for use with the email certificates on the newly issued CAC.

- Insert the CAC into the card reader.
- Open Microsoft Outlook.
- In the Tools pull-down menu, select "Trust Center".
- In the Trust Center window click the "E-mail Security tab"
- Under Encrypted e-mail, ensure that your Default Setting shows ActivClient Certificates. Then select the "Settings" button.
- The Change Security Settings window will be displayed. Outlook may automatically populate all of the required Security Settings. If not, enter a name

to label your “Security Settings Name”. Ensure “S/MIME is selected as the Cryptography Format.

- Check the boxes for Default Security Setting for this cryptographic message format, Default Security Setting for all cryptographic messages, and Send these certificates with signed messages.
- Click on the “Choose” button for the Signing Certificate field.
- In the Select Certificate window, expand Issued by to view the entire contents of the certificate. Select the certificate that indicates “DOD EMAIL CA”. Click “OK” to continue.
- You will return to the Change Security Settings window. The signing certificate you selected is inserted into the Signing Certificate field.
- Select “SHA-1” as the Hash Algorithm.
- Click on the “Choose” button and select Encryption certificate you wish to use.
- Select “3DES” as the Encryption Algorithm.
- Click “OK” to continue.
- Click the “Publish to GAL” button.
- Click “OK” button when done.

The steps below provide instructions on how to import and configure Microsoft Outlook 2003 Client for use with the email certificates on the newly issued CAC.

- Insert the CAC into the card reader.
- Open Microsoft Outlook.
- Click on “Tools”, select the “Options” menu
- Select the “Security” tab. Ensure that the CAC certificates are selected in the Default Settings box. Then select the “Settings” button.
- The Change Security Settings window will be displayed. Outlook 2003 may automatically populate all of the required Security Settings after click the “Settings” button from above. If not, continue by entering a name to label your “Security Settings Name.”
- Ensure “S/MIME” is selected as the Cryptography Format.
- Check the boxes for “Default Security Setting for this cryptographic message format”, “Default Security Setting for all cryptographic messages” and “Send these certificates with signed messages.”
- Click on the “Choose” button for the Signing Certificate field.
- In the Select Certificate window, expand “Issued by” to view the entire contents of the certificate. Select the certificate that indicates “DOD EMAIL CA”
- Click “OK” to continue
- You will return to the Change Security Settings window. The signing certificate you selected is inserted into the Signing Certificate field.
- Select “SHA-1” as the Hash Algorithm.

- Click on the “Choose” button and select Encryption certificate you wish to use.
- Select “3DES” as the Encryption Algorithm.
- Click “OK” to continue.
- You will be returned to the Options window.
- Click the “Publish to GAL” button.
- Click “OK” button when done.

Publishing Certificates to the GAL

The Publish to GAL feature publishes a user’s public key certificate to the GAL of the local Exchange server. If a user publishes the certificates to the GAL, other users accessing the same GAL can send encrypted email messages using the GAL entry.

The steps below provide instructions on how to publish certificates to the local Microsoft Exchange Server Global Address List (GAL) using Microsoft Outlook 2007.

- Insert your CAC into the card reader.
- Open Outlook.
- In the Tools pull-down menu, select “Trust Center”.
- In the Trust Center window click the “E-mail Security tab”
- Click the “Publish to GAL” button.
- Click “OK” to publish your certificates to the Global Address List.

The steps below provide instructions on how to publish certificates to the local Microsoft Exchange Server Global Address List (GAL) using Microsoft Outlook 2003.

- Insert your CAC into the card reader.
- Open Outlook.
- Click on “Tools”
- Select “Options” from the pull-down menu
- Select the “Security” tab on the Options window.
- In the Digital IDs (Certificates) section, click the “Publish to GAL” button to continue.
- Click “OK” to publish your certificates to the Global Address List.

Back to Table of Contents

Make certificates available to Windows and Internet Browser

The steps below provide instructions on how to make the new certificates available to Windows and the internet browser through the middleware on the user's computer.

If the IT environment is using ActivClient Software:

- Go to the Windows Start menu.
- Click on "Programs".
- Locate the "ActivIdentity" Folder.
- Highlight "Active Client", and then select "User Console".
- An ActivClient window will pop up.
- Go to the "Tools" pull down menu.
- Select "Advanced" and then select "Make Certificates Available to Windows".
- A screen should appear, informing the user that the certificates have been made available to Windows.
- Click on the "OK" button, and close out of the ActivClient window.

If you need further assistance with registering your certificates with Internet Explorer, please contact your local service desk for assistance.

Back to Table of Contents

Registering certificates with local service desks

Depending on the Joint Base process, users may have to register the new CAC certificates at the local service desk to ensure the electronic data interchange personal identifier (EDIPI) is populated within Active Directory (AD) for network accounts. For situations where the CAC is not authenticating to the network, users should contact the local joint base service desk for assistance.

Back to Table of Contents

Q4. How do I send a digitally signed email message?

Digitally signing a message applies the sender's certificate and public key to the message. The sender's certificate is sent with the message to help authenticate you to the recipient. To send digitally signed email, click on the Digitally Sign icon in the New Message window. This icon looks like a mail icon with a red ribbon.

The steps below provide instructions on how to digitally sign messages using Microsoft Outlook 2007.

- Insert your CAC into the card reader.
- Open Outlook.
- Address and compose a message
- Before sending, from the Options group, select the "Digitally Sign Message" button
- Click "Send"
- If prompted, enter your PIN and click "OK"

Back to Table of Contents

Q5. How do I send encrypted email messages?

Sending and viewing encrypted email messages requires both sender and receiver to share their certificate. Each must send the other a digitally signed message, which enables you to add the other person's certificate to your Contacts unless the sender and receiver have published their certificates to the GAL.

The steps below provide instructions on how to send encrypted messages using Microsoft Outlook 2007.

- Insert your CAC into the card reader.
- Open Outlook.
- Address and compose a message
- Before sending, from the Options group, select the "Encrypt Message Contents and Attachments" button.
- Click "Send"

Back to Table of Contents

Q6. How do I read archived encrypted e-mail after I get a new CAC?

When a user gets a new CAC, the user also gets new certificates. Any email that was encrypted with certificates from the previous CAC cannot be read using the new CAC. In order to read this encrypted email, users need to recover the private email encryption key associated with the user's old CAC. The Defense Information Systems Agency (DISA) provides automated and manual processes to assist with key recovery.

An ARA capability is provided by DISA to allow holders of new CACs to retrieve encryption keys and certificates from previous cards to permit decryption of old email.

Recovery of the old certificates is possible from the ARA website:

https://ara-1.c3pki.chamb.disa.mil/ara/Key

NOTE: The AR-1 URL is case sensitive. When you go to this link, you must identify yourself with PKI credentials. Use ONLY your identity certificate.

If the user experiences any issues connecting to the ARA 1 site listed above, use the following link to complete the recovery process using the secondary ARA site:

https://ara-2.c3pki.den.disa.mil/ara/Key

NOTE: The AR- 2 URL is case sensitive. When you go to this link, you must identify yourself with PKI credentials. Use ONLY your identity certificate.

Recovering a Certificate

The steps below provide instructions on how to use the Automated Key Recovery Agent (ARA) to recover certificates so users can decrypt old email messages.

- Launch Internet Explorer, insert your current CAC into the card reader and connect to one of the following sites:

  https://ara-1.c3pki.chamb.disa.mil/ara/Key

  https://ara-2.c3pki.den.disa.mil/ara/Key

- When prompted to select a certificate, select your CAC ID certificate. Click "OK"
- Enter your CAC Personal Identification Number (PIN) and click "OK"
- Read the warning and click "OK."

- The ARA will gather a list of all of the private certificates recoverable to the user.
- Choose the desired key to recover and click the "Recover" button.
- Click "OK" to confirm that you are the DoD subscriber for the key and wait while the key is being recovered
- Once the key is recovered, a page will display with a URL to download the key and a password. Write down or print the password. You will need this password to restore your key. Click the URL to download your key.
- Select "Save." Save the file to a CD or networked shared drive. Do not save the file to your local computer.
- Click the "Logout" button to end your session.
- The user will receive a notification email that the key has successfully been recovered.
- Install the recovered certificate on your workstation using the "Installation of Recovered Certificate" FAQ below.

Installation of a Recovered Certificate

The steps below provide instructions on how to install a recovered private encryption certificate.

- Locate the recovered key file from it saved location (CD or portable memory device is recommended).
- Right click the file and select "Install PFX."
- Click "Next" to continue.
- Verify the file name displayed and click "Next."
- Enter the password provided to you by the ARA website or the KRA.
- Check the box next to "Enable Strong Private Key Protection."
- Click "Next."
- Select the radio button next to "Place All Certificated in the Following Store."
- Click "Browse."
- Choose the "Personal" store and click "OK" to close the window.
- Click "Next" to continue.
- You have successfully installed the recovered certificate. Click "Finish" to close the Certificate Import Wizard window and automatically open the security settings window.
- Click the "Set Security Level" button.
- Click the radio button next to "High."
- Click "Next" to continue.

- Enter a new Password. Confirm the password. Click "Finish."
- Click "OK" to close the Import Wizard window.
- Click "OK" to close stating the import was successful.

Back to Table of Contents

Q7. What if I can't use the ARA site to recover an old certificate?

If the user encounters problems in recovering the key on either ARA site or if the certificate is not available on the recovery site, the user will need to contact the joint base organization's Registration Authority or Key Recovery Agent for assistance.

Registration Authority (RA)/Key Recovery Agent (KRA) Email Contacts

Service/Component	Email Address
Air Force	afpki.ra@us.af.mil
Army	army.ra@hgda.army.mil
DISA	kra@disa.mil
Marine Corps	raoperations@mcnosc.usmc.mil
Navy	jesus.a.gutierrez@navy.mil

Back to Table of Contents

Q8. Can I recover my current certificate prior to transitioning to another service Component in a Joint Base environment?

It is recommended that prior to FOC; users complete an **encryption key recovery process** for their current encryption certificate to a disc or CD before having a new CAC issued. For DoD civilians that are transitioning from one Service to another, completing a key recovery process prior to new CAC issuance will alleviate the need to complete the manual recovery process through the RA or KRA. Follow the "Recovering a Certificate" steps to complete the process prior to FOC.

Back to Table of Contents

Q9. I have received a new CAC and cannot login to the network?

The user should contact the Joint Base Service Desk for help in troubleshooting CAC logon problems. If users with new CACs cannot logon to the network, it is recommended that the System Administrators verify the domain controller's NTAuthCertificate store which contains the affected CACs issuing CA certificate.

Back to Table of Contents

Q10. How do I access secure websites with my CAC?

Secure websites may require different certificates for authentication and some may require you register your new CAC. If you receive an error after completing the steps outlined below; close Internet Explorer, access the site again selecting another one of your certificates.

- Ensure that the CAC is inserted into the smart card reader.
- Open Internet Explorer.
- Enter the URL of the secure website.
- The Choose a Digital Certificate window opens.
- Select your "Identity Certificate" from the list.

Back to Table of Contents

Resources Available

DMDC has volunteered to answer any questions for identification card reissuance at joint bases. Contact Cynthia Dengler (cynthia.dengler@osd.pentagon.mil) for questions on issuing CACs; contact Heidi Boyd (heidi.boyd@osd.pentagon.mil) or Sam Yousefzadeh (sam.yousefzadeh.ctr@osd.pentagon.mil) for questions on policy. Service personnel offices should also be involved in resolving issues as DMDC cannot resolve issues if there is no hire action or transfer action.

Visit the JBPMO Website to view a repository of guidance and troubleshooting assistance at the Defense Knowledge Online (DKO) portal https://www.us.army.mil/suite/page/560093. A DKO account is required to access this information.

References

1) USD P&R Directive-Type Memorandum (DTM) 08-003, "Next Generation Common Access Card (CAC) Implementation Guidance," 1 December 2008
2) DoD Public Key Enablement (PKE) Knowledge Base Article, "Importing DoD Class 3PKI Email Certificates into Microsoft Outlook 2003.pdf"
3) DoD Public Key Enablement (PKE) Knowledge Base Article, "Installing a Recovered Encryption Key.pdf"
4) DoD Public Key Enablement (PKE) Knowledge Base Article, "Publishing DoD Class 3PKI Certificates to the GAL.pdf"
5) DoD Public Key Enablement (PKE) Knowledge Base Article, "QRG Auto Key Recovery.pdf"
6) DoD Public Key Enablement (PKE) Knowledge Base Article, "User cannot logon to Network with New CAC"