White Paper

Common Access Card Joint Base Guidance

June 2010

OASD NII/DoD CIO
201 12th Street South
Crystal Gateway North, Ste 501
Arlington, VA 22202-4301

Contents

Introduction

This white paper provides joint bases the guidance for issuing Common Access Cards (CACs) as it applies to those employees aligning under a joint base construct.

This paper will be followed by a frequently asked question (FAQ) document which will provide commonly asked questions and answers as it pertains to reissuance of CACs and certificate recovery that the joint bases will be able to leverage as the transition period occurs.

A collaborative effort with the Defense Manpower Data Center (DMDC), Defense Information Systems Agency (DISA), Public Key Enabled (PKE) Support Desks, OASD NII and Booz Allen Hamilton contributed to the development of this whitepaper.

Purpose

The Department of Defense (DoD) issues CACs as the standard identification (ID) card for DoD civilian employees, active duty military, and eligible contractor personnel who need access to DoD facilities or DoD computer network systems. The CAC contains a computer chip, barcode, and a magnetic stripe which provides the following baseline functionalities:

- Logical access to computer systems
- Personnel identification
- Physical access to buildings
- Public key infrastructure (PKI) for signing and encryption

Following the January 2010 Implementation Review Conference (IRC), an action item was documented to review regulatory guidance for issuing CACs. 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. If the affiliation and agency/department fields on the CAC change in the joint base environment, a CAC must be reissued.

One important consequence of reissuing CACs to personnel affected by a joint basing transfer is a new encryption certificate will be issued on the new CAC. The encryption certificate stored on the CAC is used to decrypt encrypted email. When the old CAC is turned in, as required by the reissuance procedures, the cardholder loses access to the encryption certificate on that CAC. There are methods for ensuring continued access to

encrypted emails following the receipt of a new CAC. One method is to decrypt all email prior to receiving the new CAC. The second method is to request recovery of the certificate. Recovering the certificate from the old CAC provides the user the ability to read those emails encrypted with that corresponding certificate which is no longer available on the new CAC.

CAC Reissuance

Under the Joint Basing Base Realignment and Closure (BRAC) 2005 Recommendation 146, Phase II Joint Bases are scheduled to meet Full Operational Capability (FOC) on 1 October 2010. 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). The general rule is: if the parent Service affiliation changes, a new CAC is required.

According to DoD policy, a CAC must be reissued when the printed information on the CAC changes (e.g., pay grade, rank, and Service affiliation), when any of the media becomes unreadable or inoperable and/or if the CAC is reported lost or stolen.

Three categories of personnel eligible for the CAC could be impacted by the BRAC 2005 Recommendation 146 Joint Basing construct:

Reissuance Categories and Guidance

Employee	Reissue Guidance
Civilian	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	Military members will not require reissuance of a CAC based on joint basing activities.

Employee	Reissue Guidance
Contractor	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.

Physical and Logical Access

The CAC is the primary identification credential within the Department of Defense to access computer networks, information systems, military installations, and other DoD facilities. The CAC and the PKI certificates on the card act as the cardholder's electronic identity. The cardholder may use the digital certificates on the CAC to access secured applications, authenticate to unclassified DoD networks, digitally sign documents, and to encrypt and decrypt information.

During the reissuance of CACs within the joint basing environment, most system access should not be affected. However, case by case disruption may occur. For situations where the CAC is not visually damaged but still does not authenticate to the network, users should contact their joint base service desk to determine if the card or the computer is the problem.

Publishing and Registering Certificates

The identity certificate, email signature, and email encryption certificates should be issued on the CAC at the time of reissuance for joint base employees. If the user receiving a CAC does not have an organization e-mail address assigned, the user may return to a Real-time Automated Personnel Identification System (RAPIDS) terminal at a CAC issuance facility or the user maintenance portal web site to receive an e-mail certificate when the e-mail address has been assigned.

- RAPIDS site locator—http://www.dmdc.osd.mil/rsl/owa/home
- User maintenance portal—https://www.dmdc.osd.mil/ump/

The user maintenance portal is designed to process requests to update e-mail addresses and e-mail certificates on a user's CAC. There are circumstances, defined below, in a

joint base environment which may require a user to update the CAC email address and certificates.

- A user does not have an organization e-mail assigned at time of issuance
- Update an email address that was incorrectly entered
- Email address changed since being issued the CAC

When a user is issued a CAC, email certificates are generated on the CAC containing one email address provided by the user. Throughout the DoD community, some users may have email certificates on their CAC that do not match the email address. Reasons may include the following:

- Supported Component military personnel have a specific email address (i.e., Air Force E-Mail For Life, AKO) while stationed at a joint base with a different supporting Component
- Civilian personnel from other agencies may be temporarily assigned while maintaining their original agency affiliation
- An individual may have more than one email account and must be able to send digitally signed email and receive encrypted email using the same certificates

To ensure users with multiple email addresses working in a joint base environment have the ability to work across the DoD community without having to change email addresses, the service representatives agreed in 2005 to implement Name Check Suppression on the Microsoft Exchange servers at DoD installations to facilitate digital signing email.

The CAC reader and middleware is used to read and install PKI certificates making them available to sign and encrypt email messages and assist with registering the certificates to Microsoft Windows and the internet browser. The user must publish certificates to the Global Address List (GAL) to make it convenient for others to find and use the public encryption certificate.

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

Key Recovery

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.

It is recommended that prior to FOC, users complete the encryption key recovery process for their current encryption certificates to a disc or CD before their CAC is reissued because of a joint basing transfer. Completing a pre-recovery process will alleviate the need for DoD civilians that are transitioning from one Service to another to complete the manual recovery process.

Automated Key Recovery Agent (ARA)

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.

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 office for assistance.

Once the user has successfully downloaded and recovered the keys, the recovered key needs to be installed on the computer that will be used to open the older encrypted emails. Local help desks should be able to provide support for recovering encryption certificates using the ARA.

Key Recovery Agent (KRA)

Occasionally there are circumstances where the ARA recovery site cannot be used. The DISA KRA will be able to recover the certificates manually if either of the following situations exists:

- The DoD civilian changes from one Service to another
- Contractor on-boards as a DoD civilian

Contact the KRA at kra@disa.mil to recover certificates in both of the instances listed above.

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, "Suppress Name Checking for Outlook XP, 2003, and 2007"