MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Follow-on Guidance for the DoD CAC Certificate Reduction Realignment Plan – Personal Identity Verification Transition

1. References:


   c. Memorandum, Army CIO/G-6, 17 Apr 18, subject: Upcoming Changes to the DoD CAC.

2. Purpose. This memorandum notifies all Army activities to transition Public Key-enabled Information Technology (IT) resources (networks, systems, applications, workstations, and so forth) and personnel to use the Personal Identity Verification Authentication (PIV Auth) certificate.

3. Background. The Under Secretary of Defense for Personnel and Readiness and the DoD Chief Information Officer (CIO) will release a joint policy memorandum mandating that all DoD Components transition Non-Secure Internet Protocol Router Network (NIPRnet) Public Key-Enabled IT resources to use the PIV Auth certificate for authentication no later than 18 months from signature date of memorandum. Although the DoD Joint policy memorandum has been delayed, it will be published in the near future to allow the Department to meet Federal requirements.

4. Army’s Decision. The Army has decided to proceed with transitioning its IT resources to support the PIV Auth certificate ahead of the release of the DoD mandate. This will ensure the Army proactively prepares personnel and IT resources to support the DoD CAC Certificate Reduction Realignment Plan. Transitioning the CAC to use the PIV Auth certificate aligns with Federal guidelines, enhances interoperability with other Federal agencies, and ensures the CAC meets FIPS 201-2 requirements.
SAIS-CBM
SUBJECT: Follow-on Guidance for the DoD CAC Certificate Reduction Realignment Plan – Personal Identity Verification Transition

5. CAC Modernization Plan. The DoD CAC Certificate Reduction and Realignment Plan entails the following:

   a. All DoD Components transition NIPRnet IT resources to use the PIV Auth certificate vice the Identity or Email Signing certificates for authentication.

   b. Eliminate the Identity certificate from the CAC.

   c. Realign the Email Signing certificate to perform only signature operations, such as digitally signing emails and documents.

6. Army User Actions. All Army users with a CAC issued before 24 February 2018 that expires after 31 March 2019 must activate the PIV Auth certificate via the Defense Manpower Data Center (DMDC) Self Service portal (https://www.dmdc.osd.mil/self_service/) no later than 31 March 2019. Instructions to activate the PIV Auth certificate are provided on the DMDC website.

   a. All users with a CAC issued 24 February 2018 or later will already have an activated PIV Auth certificate, so no action is required from them.

   b. The Army must have all users with an activated PIV Auth Certificate no later than the 31 March 2019 deadline to allow Network Engineers to begin testing and transitioning all users NIPRNet accounts to use the PIV Auth Certificate.

   c. Users are not required to obtain a new CAC for the sole purpose of having an activated PIV Auth Certificate. CACs should only be replaced through the normal life cycle process. Existing CACs are still viable and simply need the PIV Auth Certificate activated as outlined above.

   d. Users will not be required to use the PIV Auth Certificate for Authentication until the Army’s PIV transition is completed. However, certain Army systems have the capability to process the PIV Auth Certificate today; users of these systems who have an activated PIV Auth Certificate will not see any disruption in service.

7. U.S. Army Cyber Command (ARCYBER). No later than 45 days from the signature date of this memorandum, ARCYBER will publish an Operations Order (OPORD) to direct Army organizations and system owners to transition systems to use the PIV Auth certificate for authentication. The OPORD will provide specific transition instructions to ensure the appropriate PK-enabled IT resources are configured to process CACs using the PIV Auth certificate.
SAIS-CBM

SUBJECT: Follow-on Guidance for the DoD CAC Certificate Reduction Realignment Plan – Personal Identity Verification Transition

8. Army IT System Owners Actions. System owners must configure Public Key-Enabled IT resources as described in the ARCYBER OPORD, when released, to meet the Army’s transition completion deadline of 31 December 2019.

9. Army Schedule. The Army’s plan is to be proactive and complete the transition ahead of the DoD timeline. As such:

   a. No later than 45 days from signature date of this memorandum, ARCYBER will publish an OPORD that provides implementation guidance.

   b. No later than 31 March 2019, all Army CAC users must have an activated PIV Auth certificate.

   c. No later than 31 December 2019, all Army NIPRnet PK-enabled IT resources will be configured to support the PIV Auth certificate.

   d. Effective 01 January 2020, all Army NIPRnet PK-enabled IT resources will use the PIV Auth certificate to perform all authentication functions.

10. Points of contact are Mr. Jude Roeger, (703) 545-1749 (DSN 865) or jude.a.roeger2.civ@mail.mil; and Mr. Timothy Hiligh, (703) 545-1741 (DSN 865) or timothy.r.hiligh.ctr@mail.mil.

   BRUCE T. CRAWFORD
   Lieutenant General, GS
   Chief Information Officer/G-6

DISTRIBUTION:
Principal Officials of Headquarters, Department of the Army
Commander:
   U.S. Army Forces Command
   U.S. Army Training and Doctrine Command
   U.S. Army Material Command
   U.S. Army Futures Command
   U.S. Army Pacific
   U.S. Army Europe
   (CONT)
SAIS-CBM

SUBJECT: Follow-on Guidance for the DoD CAC Certificate Reduction Realignment Plan – Personal Identity Verification Transition

DISTRIBUTION: (CONT)
U.S. Army Central
U.S. Army North
U.S. Army South
U.S. Army Africa/Southern European Task Force
U.S. Army Special Operations Command
Military Surface Deployment and Distribution Command
U.S. Army Space and Missile Defense Command/Army Strategic Command
U.S. Army Cyber Command
U.S. Army Medical Command
U.S. Army Intelligence and Security Command
U.S. Army Criminal Investigation Command
U.S. Army Corps of Engineers
U.S. Army Military District of Washington
U.S. Army Test and Evaluation Command
U.S. Army Installation Management Command
U.S. Army Human Resources Command
U.S. Army Financial Management Command
U.S. Army Marketing and Engagement Brigade
Superintendent, United States Military Academy
Director, U.S. Army Acquisition Support Center
Superintendent, Arlington National Cemetery
Commandant, U.S. Army War College
Director, U.S. Army Civilian Human Resources Agency

CF:
Director, Army National Guard
Director of Business Transformation
Commander, Eighth Army
If you have a Common Access Card (CAC) issued prior to 24 February 2018 you will need to follow the instructions below for getting a Personal Identity Verification (PIV) loaded on your CAC. Army suspense for having all users with an activated PIV Authentication Certificate is NLT 31 March 2019.

STEP-BY-STEP PROCESS FOR ADDING A PIV TO YOUR CAC:

**Step 1:** On the Left bottom corner of your desktop, Left Click on the Windows symbol - then type JAVA -

**Step 2:** Now select CONFIGURE JAVA

**Step 3:** Select the security tab

**Step 4:** Select edit site list - and add this URL to the Exception site list (https://idco.dmdc.osd.mil) then select OK

**Step 5:** Now select OK again to close the JAVA control panel.

**Step 6:** Now restart your browser.

**Step 7:** Log into the milConnect Website (https://www.dmdc.osd.mil/self_service)

**Step 8:** Select "Sign In"

**Step 9:** New Window opens labeled ID Card Office Online - select "OK"

**Step 10:** Select "Login" with Common Access Card

**Step 11:** A Certificate Window pops-up - Choose your EMAIL certificate on your CAC - select more choices, then select the certificate where the issuer is DOD EMAIL.

**Step 12:** A Window will open asking for your PIN - enter pin and select OK

**Step 13:** Select Activate PIV Certificate

**Step 14:** A new window appears with a title "Reading CAC for Activate PIC Certificate" - select "Proceed"

**Step 15:** A window appears asking if you want to run this application? Select "RUN" - you will be prompted to enter your PIN number

**NOTE** Some users have to click inside the box after entering each number of the PIN (i.e. if your pin is 123456 you would have to click inside the box, then enter 1, then click inside the box, then enter 2...) Not everyone experiences this issue, but some do.

**Step 16:** DO NOT REFRESH THE SCREEN OR CLICK THE BROWSER'S BACK BUTTON during the process

**Step 17:** A window with PIV Information opens and you need to click "UPDATE CAC" then the system will post the information to the Issuance Portal

**Step 18:** Another JAVA window will appear, select RUN - you will be prompted to enter your PIN number once again, after entering your pin, select OK

**NOTE** Some users have to click inside the box after entering each number of the PIN (i.e. if your pin is 123456 you would have to click inside the box, then enter 1, then click inside the box, then enter 2...) Not everyone experiences this issue, but some do.

**Step 19:** Now you should see a message stating "Activating PIV authentication Certificate"

**Step 20:** Then you should get a message stating "YOUR CAC HAS BEEN SUCCESSFULLY UPDATED" - select HOME, then logout of milConnect.