



OFFICE OF THE SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-1000

DEC - 7 2018

CLEARED
For Open Publication

13
Feb 01, 2019

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Modernizing the Common Access Card - Streamlining Identity and Improving Operational Interoperability

Homeland Security Presidential Directive 12 (HSPD-12) requires Federal departments and agencies to use strong authentication credentials to access their networks and information systems. The Common Access Card (CAC) is the DoD's primary credential for fulfilling these requirements on the Non-Secure Internet Protocol Router Network (NIPRNet). Without adjustments to DoD's CAC implementation, the Department will continue to diverge from the Public Key Infrastructure (PKI) standards utilized by the rest of the Federal Government, mission partners, and industrial suppliers. This memorandum makes the DoD's Personal Identity Verification (PIV)-Authentication (Auth) certificate the standard for access to DoD information technology assets on the NIPRNet across the Department.

The United States warfighter's ability to interoperate with various mission partners is hampered by a lack of common identity standards. This memorandum directs the alignment of DoD's use of the CAC with the Federal PIV-Auth certificate to:

- Standardize implementations and reduce inefficiencies around secure information exchange with DoD, Federal, state, local, territorial, and tribal mission partners.
- Improve cybersecurity posture and simplify configuration and change management of Department network resource authentication, as well as the implementation and reporting of risk management controls, by using a common Department-wide PKI principal authenticator.
- Reduce costs associated with maintaining DoD-peculiar legacy authentication mechanisms, such as legacy CAC interfaces and certain smart card middleware.
- Allow the Department to use commercial products designed to read federal HSPD-12 PIV compliant PKI credentials.

By May 1, 2020, DoD will issue a new configuration of DoD PKI certificates on the CAC in which the number of certificates will be reduced from four to three. At the same time, DoD's unclassified network and secure web asset user accounts will use the DoD PIV-Auth certificate as the only PKI certificate on the CAC for authenticating users.

Accordingly, this memorandum directs:

- DoD Components to begin immediate planning and prioritizing for reconfiguring their network and web-application user accounts to support PIV-Auth authentication.

- The DoD Chief Information Officer (CIO) Cybersecurity Scorecard Team to document and track the progress of configuration changes to DoD unclassified network and web application user-accounts necessary to accommodate the use of the PIV-Auth certificate. The Scorecard Team will establish periodic reporting metrics for the DoD Components and share this information with the DoD Identity Protection and Management Senior Coordinating Group (IPMSCG). The DoD IPMSCG will monitor and oversee the following actions:

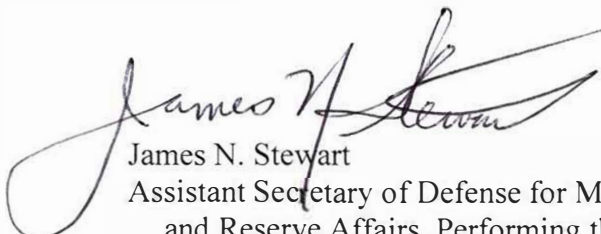
By May 1, 2019:


- DoD Components will provide their individual transition plans to the DoD CIO Cybersecurity Scorecard Team.
- The Defense Information Systems Agency (DISA) will develop education, outreach, and training materials on changes to the CAC and instructions for selecting the PIV-Auth certificate for authentication to NIPRNet systems.

By May 1, 2020:

- The National Security Agency, DISA, and the Defense Management Data Center will collaborate to create a new version of the CAC that contains certificates and attributes as outlined in Attachment 1.
- DoD Components will ensure unclassified network and secure web asset user accounts leveraging user principal names (UPNs) are required to use the DoD PIV-Auth certificate on the CAC for authenticating users. Particular attention should be placed on the activity identified in Attachment 2 (Certificate Reduction Transition Areas).
- DoD Components will complete re-provisioning all NIPRNet web application user accounts not using UPNs to map to DoD PIV-Auth certificate.

Your assistance and attention to detail in helping the Department make a seamless transition to better support interoperability with our mission partners are greatly appreciated. The points of contact for this effort are: Ms. Patricia Janssen for the Office of the DoD CIO, who may be reached at patricia.l.janssen.civ@mail.mil, or (571) 372-4221; and Mr. Alex Sedillos for Office of the Under Secretary of Defense for Personnel and Readiness, who may be reached at alex.a.sedillos.civ@mail.mil, or (831) 583-2400.


James N. Stewart
Assistant Secretary of Defense for Manpower
and Reserve Affairs, Performing the Duties
of the Under Secretary of Defense for
Personnel and Readines


Dana Deasy
DoD Chief Information Officer

Attachments:

As stated

cc:

Chair, DoD IPMSCG

DISTRIBUTION:

Chief Management Officer of the Department of Defense
Secretaries of the Military Departments
Chairman of the Joint Chief of Staff
Under Secretaries of Defense
Chiefs of Military Services
Chief of the National Guard Bureau
Commandant of the Coast Guard
Commanders of the Combatant Commands
General Counsel of the Department of Defense
Director of Cost Assessment and Program Evaluation
Inspector General of the Department of Defense
Director of Operational Test and Evaluation
Assistant Secretary of Defense for Legislative Affairs
Assistant to the Secretary of Defense for Public Affairs
Director of Net Assessment
Directors of Defense Agencies
Directors of DoD Field Activities

Attachment 1: Detail of Emerging Changes to Certificates on CAC

DoD PKI X.509 Certificates On CAC				
	DoD Identity	DoD PIV Authentication	DoD E-mail Signing	DoD E-mail Encryption
Current CAC	Key Usage (KU): <ul style="list-style-type: none"> • Digital signature • Non-repudiation 	KU: <ul style="list-style-type: none"> • Digital signature Extended Key Usage (EKU): <ul style="list-style-type: none"> • Smart Card Logon (SCL) • Client-Authentication Subject Alternate Name (SAN) Field: <ul style="list-style-type: none"> • Federal Derived User Principal Name (UPN) • Federal Agency Smart Credential Number 	KU: <ul style="list-style-type: none"> • Digital signature • Non-repudiation EKU: <ul style="list-style-type: none"> • SCL • Client-Authentication • Secure E-mail SAN Field: <ul style="list-style-type: none"> • DoD Derived UPN • Request For Comment (RFC) 822 name 	KU: <ul style="list-style-type: none"> • Key Encipherment SAN Field: RFC 822 name
Future CAC	Remove Certificate	Same as current.	Same as current except: <ul style="list-style-type: none"> • Remove SCL EKU • Remove Client-Authentication EKU • Add Microsoft document signing EKU • Remove DoD Derived UPN in SAN 	Same as current.

**CLEARED
For Open Publication**

Feb 01, 2019

Attachment 2: Certificate Realignment Transition Areas

When DoD IT assets encounter a CAC after May 1, 2020, the CAC holder's account is to be re-provisioned or updated so existing access is not disrupted. The following areas have been identified as priorities for the DoD Components to address and ensure:

1. Defense Information Systems Agency (DISA) Enterprise Application Services Forests (EASF) is modified to be able to provision user accounts/authenticate users to DoD enterprise web applications (e.g., Defense Collaboration Service, Defense Enterprise Portal, Defense Enterprise E-mail) for non-dual persona personnel with DoD PIV authentication certificate (and its 16-digit Federal derived User Principal Name (UPN)), rather than DoD E-mail signing certificate (and its DoD-derived 10 digit UPN, i.e., DoD ID Number).
2. Any DoD UNCLASSIFIED website using a DoD identity certificate is modified to provide user accounts/authenticate users with a DoD PIV authentication certificate rather than a DoD identity certificate.
3. Any DoD UNCLASSIFIED website requiring the DoD E-mail signing certificate is modified to be able to provision user accounts/authenticate users with DoD PIV authentication certificate.
4. All DoD UNCLASSIFIED network/Active Directory user accounts are modified/re-provisioned to use DoD PIV authentication certificate (and its Federal derived 16-digit UPN) rather than DoD E-mail signing certificate.

**CLEARED
For Open Publication**

13
Feb 01, 2019

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW