



DEPARTMENT OF DEFENSE

6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

DEC 20 2019

CHIEF INFORMATION OFFICER

MEMORANDUM FOR CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE

SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEFS OF THE 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

**CLEARED
For Open Publication**

Feb 07, 2020

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

SUBJECT: DoD Mobile Public Key Infrastructure (PKI) Credentials

- References: (a) Department of Defense Chief Information Officer Memorandum, "DoD Interim Guidance on the Use of DoD Personal Identity Verification Derived Public Key Infrastructure Credentials on Unclassified Commercial Mobile Devices," September 24, 2014 (hereby cancelled)
(b) Department of Defense Chief Information Officer Memorandum, "DoD Interim Guidance for Implementing Derived Public Key Infrastructure," May 6, 2015 (hereby cancelled)
(c) Department of Defense Chief Information Officer Memorandum, "Interim Digital Authentication Guidelines for Unclassified and Secret Classified DoD Networks and Information Systems," August 20, 2018

This memorandum approves Purebred, the Defense Information Systems Agency's (DISA) government developed solution, as an enterprise capability for issuing Department of Defense (DoD) Mobile PKI Credentials (previously referred to as derived credentials). Purebred is the only DoD approved capability for deploying DoD Mobile PKI Credentials to DoD mobile endpoints and approved authenticators.

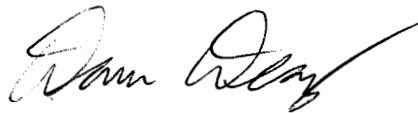
This memorandum also supersedes and cancels references (a) and (b) and prohibits the use of all other non-DoD Chief Information Officer (CIO) approved DoD mobile PKI credential issuance solutions or methods (e.g., side loading) for user/person-entity certificates. The attachment to this memorandum provides the technical and security requirements for the

issuance, use, and storage of DoD Mobile PKI Credentials and support, maintenance, and reporting requirements for Purebred. Additionally, the attachment establishes requirements for the issuance of DoD Mobile PKI credentials to DoD approved authenticators.

DoD approved alternative (non-PKI) Multi-Factor Authentication solutions may be implemented on DoD mobile endpoints to authenticate to unclassified DoD information systems in accordance with reference (c).

DoD Components pursuing alternative approaches or solutions to deploy DoD Mobile PKI Credentials or authenticators must request DoD CIO approval prior to demonstrations, testing, procurement, fielding, or use.

The point of contact for this matter is COL Thomas Clancy, (571) 372-4594, thomas.j.clancy2.mil@mail.mil.

A handwritten signature in black ink, appearing to read "Dana Deasy", with a stylized flourish extending to the right.

Dana Deasy

Attachments:
As stated

ATTACHMENT 1

- References:
- (a) National Security Agency (NSA) Technical Brief “Protecting Credentials in Current and Emerging Endpoint Devices for Access to Unclassified National Security Systems”, June 19, 2017
 - (b) DoD Instruction 8520.03, “Identity Authentication for Information Systems,” May 13, 2011, as amended
 - (c) DoD Manual 1000.13, “DoD Identification (ID) Cards: ID Card Life-Cycle”, January 23, 2014
 - (d) National Institute of Standards and Technology Special Publication 800-63-3, “Digital Identity Guidelines,” current edition
 - (e) National Institute of Standards and Technology Special Publication 800-88, “Guidelines for Media Sanitization,” current edition
 - (f) DoD CIO Memorandum, “Mobile Application Security Requirements,” October 6, 2017

This attachment provides updated technical and security requirements for the issuance, use, and storage of DoD Mobile PKI Credentials and support, maintenance, and reporting requirements for Purebred.

A. Scope

For the purpose of this attachment, DoD managed (regardless of ownership) Commercial Mobile Devices (CMD), Portable Electronic Devices (PED), and laptops are DoD mobile endpoints. DoD authenticators include DoD CIO approved authentication devices, which can generate and store DoD Mobile PKI credentials (regardless of ownership).

B. DoD Mobile PKI Credentials Issuance, Usage, and Policy Mapping

1. Issuance of DoD Mobile PKI Credentials is dependent upon the requestor possessing a valid Common Access Card (CAC) or other authenticator at Authenticator Assurance Level (AAL) 3, in accordance with reference (d), which is bound to an identity proofed in accordance with reference (c). Verification of the requestor must be performed through a PKI authentication.
 - a. Authentication using an AAL 3 authenticator, which is bound to an identity proofed in accordance with reference (c), provides proof that face-to-face in person-verification was completed prior to the issuance of the requestor’s CAC or other authenticator. DoD Mobile PKI Credentials will identify the possessor by asserting the same Common Name (CN) as the PKI certification on the AAL 3 authenticator.
2. DoD Mobile PKI Credentials can be issued at two Assurance Levels:
 - a. DoD **Medium** Mobile PKI Credentials – AAL 2
 - i. Issued remotely or in person without a biometric comparison
 - ii. Assert Medium PKI policy object identifier (OID)

- b. DoD **Medium-Hardware** Mobile PKI Credentials – AAL 3
 - i. Issued remotely or in person without a biometric comparison
 - ii. Assert Medium-Hardware PKI policy OID
 - iii. Issued in accordance with paragraph C.3 of this memorandum.
3. Approved uses for DoD Mobile PKI Credentials:
- a. DoD **Medium** Mobile PKI Credentials – AAL 2
 - i. Authentication to information systems rated Sensitivity Level 3 and below in accordance with reference (b)
 - ii. DoD NIPR WiFi Authentication
 - iii. DoD NIPRNet VPN Authentication
 - iv. Digitally signing/encrypting emails and documents
 - b. DoD **Medium-Hardware** Mobile PKI Credentials – AAL 3
 - i. All DoD Medium Mobile PKI Credentials capabilities
 - ii. Authentication to information systems rated Sensitivity Level 4 and below (including unclassified National Security Systems) in accordance with reference (b)
 - iii. DoD network logon (e.g., Windows Logon)

	DoD PKI Policy Identifier (OID)	Credential Strength (Per DoDI 8520.03)	AAL (NIST 800-63-3)	Issuance	Approved Uses
Medium Mobile PKI Credentials	Medium	C	AAL 2	Remote or in person Issuance via PKI authentication without a biometric comparison	<ul style="list-style-type: none"> • Authentication to Sensitivity Level 3 & below • DoD NIPR WiFi & VPN Auth • Encryption/Digital Signature
Medium-Hardware Mobile PKI Credentials	Medium-Hardware	E	AAL 3	Remote or in person Issuance via PKI authentication without a biometric comparison	<ul style="list-style-type: none"> • All Medium capabilities plus: • Access to Sensitivity Level 4 and below (including NSS) • Networks Logon (including Windows Logon)

Table 1 - Issuance and Policy Mapping for DoD Mobile PKI Credentials

C. DoD Mobile PKI Credentials Storage, Protection, and Lifecycle Management

- 1. All mobile endpoints which are issued and store DoD Mobile PKI Credentials must be:
 - a. Validated against a relevant National Information Assurance Partnership (NIAP) protection profile, or
 - b. Validated by the National Institute of Standards and Technology (NIST) Crypto Module Validation Program (CMVP) as meeting Federal Information Processing Standards (FIPS) 140-2 Level Security Level 2 overall and Level 3 for Physical Security.

2. All authenticators must be:
 - a. Validated by the NIST CMVP as meeting FIPS 140-2 Security Level 2 overall and Level 3 for Physical Security, or
 - b. Validated against a NIAP protection profile, where DoD CIO has deemed the protection profile is equivalent to or stronger than the FIPS requirements.
3. In order to be issued Medium-Hardware DoD Mobile PKI Credentials, the mobile endpoint or authenticator must provide a verifiable attestation to the issuance system ensuring that the PKI private keys are generated, stored, and protected in hardware validated in accordance with C.1 or C.2.
4. The Privilege User Working Group (PUWG) will evaluate endpoints/authenticators in accordance with C.1 or C.2 prior to issuance of DoD Mobile PKI Credentials and provide approval recommendations and accompanying assurance levels to the DoD Deputy CIO for Cybersecurity (DCIO-CS).
 - a. A list of approved mobile endpoints/authenticators and accompanying assurance levels will be maintained on the DoD Cyber Exchange (<https://cyber.mil>).
5. Mobile endpoints and authenticators must be configured in accordance with applicable DoD Security Technical Implementation Guides (STIGs).
 - a. Mobile endpoints and authenticators must be configured with an activation factor (something you know or something you are) which meets one of the following requirements:
 - i. Memorized secret of at least 6 decimal digits in length (e.g., PIN)
 1. Mobile endpoint passcodes meet this requirement
 - ii. Biometrics (e.g., a fingerprint or other biometric data).
 1. Biometrics as a second factor must be used in accordance with the device STIG (i.e., the biometric is acceptable if the STIG approves the biometric sensor for device unlock) or NIST Special Publication (SP) 800-63B.
 - b. DoD endpoint STIGs and monitoring tools should recognize and allow the use of DoD approved authenticators.
6. Mobile endpoints with DoD Mobile PKI Credentials must be managed and controlled by a DoD enterprise management system (e.g. Mobile Device Management, Enterprise Mobility Management, Active Directory, etc.).
 - a. DoD enterprise management system owners/ Authorizing Officials (AOs) must ensure a documented process is in place to validate a user's identity prior to unlocking/resetting the passcode of mobile endpoints with DoD Mobile PKI Credentials.
7. Mobile endpoints with DoD Mobile PKI Credentials must be updated to the most recent operating system (OS), security patch level, and firmware versions within 30 days of being made publically available by the manufacturer/vendor or carrier.

- a. Mobile endpoints should be configured to enable automatic updates to the greatest extent possible.
 - b. DoD enterprise management system must enforce compliance monitoring to ensure the mobile endpoints configuration settings do not deviate from AO approved configuration baseline (e.g., STIG configurations, AO approved OS versions, rooted/jailbroken devices, etc.).
 - i. Mobile endpoints out of compliance must have automated remediation actions performed on a graduated scale (e.g., restrict access to enterprise resources, revoke DoD Mobile PKI Credentials issued to the mobile endpoint, remotely wipe DoD information from the mobile endpoint, etc.)
 - c. Mobile endpoints that no longer receive the latest patches/updates from the vendor/carrier should be considered end-of-life, and be retired from service and wiped of DoD information.
 - d. Mobile endpoints which enable patches to be applied separate from device OS updates may delay OS updates if all patches have been applied.
8. Mobile endpoints and authenticators with DoD Mobile PKI Credentials must be treated the same as a CAC. Users must maintain positive control and report tamper, damage, or loss immediately.
- a. DoD enterprise management system owners/AOs must have a documented process in place to ensure Mobile endpoints are remotely wiped and the DoD Mobile PKI Credentials are revoked in the event the device is tampered, damaged, or lost.
9. Mobile endpoints with DoD Mobile PKI Credentials must be factory restored (e.g., all information deleted and reset) in accordance with NIST SP 800-88 before being re-provisioned to a new user.
10. DoD Mobile PKI Credentials must be stored in and protected by either an approved mobile endpoint's native hardware/hardware-backed keystore, a Trusted Platform Module (TPM), or the authenticator's crypto module.
11. Private keys must be generated either within a native hardware/hardware-backed keystore of an approved mobile endpoint, in the authenticator's approved crypto module, or in a hardware security module (HSM) within the issuance infrastructure that meets FIPS 140-2 Security Level 2 overall and Level 3 for Physical Security. Private keys must also be securely imported into an approved storage mechanism per paragraph C.10 of this memorandum.
- a. Encryption keys may be recovered from escrow and transferred to the mobile endpoint or authenticator via an assured channel and stored in an approved storage mechanism per C.10.
12. Credentials must be non-exportable from the mobile endpoint or authenticator's key storage mechanism.
- a. NOTE: The Purebred Key Sharing mechanism is exempted from this requirement (See paragraph D.1).

13. DoD Mobile PKI Credentials must only be accessible to managed and native (e.g., mail client, browser) applications that have been evaluated and approved for use by the mobile endpoint's AO.
 - a. Managed mobile applications must be evaluated in accordance with reference (f).
14. The DoD Mobile PKI Credential's expiration date must be no greater than the primary authenticator they were derived from, and maintain the same Electronic Data Interchange Personal Identifier (EDIPI), email, and User Principal Name (UPN) as the principal authenticator from which they were derived.
 - a. DoD Mobile PKI Credentials must be bound to the user's Defense Enrollment Eligibility Reporting System identity and revoked if the user is no longer CAC eligible.
15. DoD Mobile PKI Credentials must be immediately flagged for revocation if the associated mobile endpoint or authenticator is reported as missing. Mobile endpoints must be flagged by the enterprise management system to be remotely wiped.
 - a. If a user loses their CAC, they can continue to use their DoD Mobile PKI Credentials on their mobile endpoint or authenticator.
 - i. Upon being issued a new CAC, the user will need to recover their new encryption keys.
 - b. If a user loses a mobile endpoint or authenticator with DoD Mobile PKI Credentials, they may be required to obtain new encryption keys.
16. Administrator credentials shall not be issued to mobile endpoints.
17. DoD Components shall not issue DoD Mobile PKI Credentials to devices that can practically support the use of a smart card and smart-card reader, such as DoD non-mobile traditional desktops (i.e., tower workstations).
 - a. DoD Components may, but are not required to, issue DoD mobile PKI credentials to laptops that support the use of a smartcard.

D. Purebred

1. The key sharing capability implemented by Purebred on iOS devices is authorized, provided that:
 - a. Keys consumed by applications must be stored per paragraph C.10 of this memorandum.
 - i. Keys must be encrypted when leaving the native hardware-backed keystore and remain encrypted until reintroduced into an approved storage mechanism per paragraph C.10 of this memorandum.
 - ii. Private keys must never exist in plaintext form outside the native hardware-backed keystore.
 - b. Credentials shared using this method may only assert the DoD PKI Medium OID

- c. Purebred application is deployed as an iOS Managed application and only other approved iOS Managed applications have access to the credentials.
 - d. iOS device has implemented STIG control to restrict data sharing from managed applications to unmanaged applications (via device management policy)
 - e. Once iOS provides a system mechanism for sharing of credentials, the custom key sharing feature will be deprecated.
2. Window's based mobile endpoints which implement a Trusted Platform Module in accordance with C.1 and provide a verifiable assertion may be issued Medium-Hardware DoD Mobile PKI Credentials via Purebred.
3. To facilitate enrollment in DISA's Purebred, trusted non-person entity/device certificates may be used to establish a secure connection to NIPRNet (with access limited to Purebred). Once a mobile endpoint is enrolled in Purebred, the use of these certificates should be discontinued and the user's DoD Mobile PKI Credentials should be used to the greatest extent possible.

E. Responsibilities:

1. DoD CIO shall:
 - a. Review and approve alternative approaches to deploy DoD Mobile PKI Credentials;
 - b. In cooperation with the PUWG, review and approve mobile endpoints and authenticators that can be issued and store DoD Mobile PKI Credentials;
 - c. In cooperation with the PUWG, provide oversight and requirements to Purebred to guide future development efforts; and
 - d. Review and approve alternative Multi-Factor authentication solutions.
2. DISA shall:
 - a. Provide an information brief on Purebred to the Defense Security/Cybersecurity Authorization Working Group (DSAWG);
 - b. Annually evaluate the Purebred mobile application in accordance with reference (f) and provide evaluation results to DoD Components, as requested;
 - c. Ensure, via technical means, Purebred only deploys DoD Mobile PKI Credentials to DoD approved mobile endpoint or authenticators;
 - d. Clearly link a credential to the device to which it was issued;
 - e. Maintain and publish a list of Purebred supported mobile endpoints/authenticators and accompanying assurance levels on the DoD Cyber Exchange (<https://cyber.mil>);

- f. Review and update all mobile endpoint STIGs to support the use of DoD Mobile PKI Credentials and/or authenticators.
 - g. Work with the Defense Manpower Data Center (DMDC) to develop a mechanism to ensure when a user is no longer CAC eligible, all associated DoD Mobile PKI Credentials are revoked;
 - h. Brief DoD CIO & the PUWG semi-annually on the status of Purebred and the development roadmap; and
 - i. As needed, update the DoD Certificate Practice Statement to ensure alignment with Purebred capabilities.
3. DMDC shall:
- a. Support DISA in implementing a mechanism to ensure when a user is no longer CAC eligible, all associated DoD Mobile PKI Credentials are revoked; and
 - b. Enable automated processing of user's certificate histories in support of the deployment of DoD Mobile PKI Credentials (including but not limited to the elimination of ambiguous personas).
4. NSA shall:
- a. Continually evaluate the risks to DoD Mobile PKI Credentials on mobile endpoints/authenticators and update reference (a) as appropriate; and
 - b. Create and maintain a list of latest OS/Patch level for all NIAP validated mobile endpoints and OSs. This list should delineate the latest available OS/patch level by all major U.S. carriers currently used by the DoD.
5. Heads of DoD Components shall:
- a. Adopt Purebred as their DoD Mobile PKI Credentialing solution;
 - b. Provide feedback to DoD CIO and DISA regarding additional requirements for Purebred;
 - c. Seek DoD CIO approval prior to demonstrations, testing, procurement, and fielding of alternative approaches to deploy DoD Mobile PKI Credentials; and
 - d. Document processes for validating a user's identity prior to unlocking/resetting the passcode of mobile endpoints. Remotely wipe the mobile endpoint and revoke the DoD Mobile PKI Credentials if a user reports the mobile endpoint as missing or showing signs of tampering.

F. Definitions:

Authenticator. Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. In previous editions of NIST SP 800-63, this was referred to as a token.

Credential. An object or data structure that authoritatively binds an identity via an identifier or identifiers and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber.

Mobile Endpoint. A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with a self-contained power source. Mobile endpoints may also include voice communication capabilities, on board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include:

- Smartphones and Tablets (i.e., CMDs) running mobile Operating Systems (OS)
- Laptops, notebooks, 2-in-1 convertible laptops, netbooks, and ultra-mobile PCs running traditional non-mobile Oss

ATTACHMENT 2

This attachment provides a list of mobile endpoints & authenticators approved for the issuance of DoD Mobile PKI via approved issuance systems and the **maximum** accompanying assurance level suitable for each device based on the requirements of ATTACHMENT 1.

#	Approved Mobile Endpoints & Authenticators	Maximum Assurance Level
1	National Information Assurance Partnership (NIAP) Validated Mobile Devices ¹	Medium (AAL2) or MediumHardware (AAL3) ²
2	Windows 10 Mobile Endpoints with validated Trusted Platform Modules	MediumHardware (AAL3)
3	YubiKey Series 4 (FIPS Version Only)	MediumHardware (AAL3)

¹ NIAP Validated Mobile Devices <https://www.niap-ccevs.org/Product/PCL.cfm?ID624=69>

² NIAP Validated Mobile Devices which provided a verifiable attestation to the issuance system and store private keys in hardware may be issued MediumHardware (AAL3) credentials