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

CHIEF INFORMATION OFFICER

SEP 24 2014

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: DoD Interim Guidance on the Use of DoD Personal Identity Verification Derived Public Key Infrastructure Credentials on Unclassified Commercial Mobile Devices

Reference: NSA Memorandum, "Commercial Mobile Device (CMD) Public Key Infrastructure (PKI) for Unclassified National Security Systems (NSS) Way Forward-DECISION MEMORANDUM," July 31, 2014

The National Security Agency (NSA) Decision Memorandum recommends that DoD move to an approach to Public Key Infrastructure (PKI) credentials for Commercial Mobile Devices (CMDs) that improves performance and simplifies PKI operations for users of the devices. This new approach is based on deriving new PKI credentials from those stored on a Common Access Card (CAC) and then storing these new derived PKI credentials directly on the CMD. This will eliminate the need to buy and use external CAC readers for CMDs and will improve the overall user experience. Users will be able to operate CMDs more efficiently and will seamlessly integrate the use of important functions like encrypted or digitally signed email. Additional technical detail and implementation tasks for the derived PKI credential capability are provided in the attached Mobility Credential Guidance.

The DoD Chief Information Office point of contact for this matter is Mr. Mark Norton at email: mark.c.norton.civ@mail.mil, 571-372-4941.

Terry A. Halvorsen
Acting

Attachment:
As stated

ATTACHMENT

MOBILITY CREDENTIAL GUIDANCE

A. INTRODUCTION

1. The objective of this document is to outline the tasks necessary to establish a derived PKI credential capability for approved unclassified DoD Public Key Infrastructure (PKI) mobile implementations.
2. The document also provides interim guidance for the evaluation and application of Personal Identity Verification (PIV)-based PKI identity credentials used with unclassified DoD-issued Commercial Mobile Devices (CMD).
    a. The approach to deploying identity credentials on mobile devices is based on derived PKI credentials which, as the name implies, are derived from the PIV credentials that have been issued to appropriate personnel via their Common Access Card (CAC).
    b. A derived PKI credential differs from other PKI credentials in the manner in which identity verification is performed. Verification of the requester’s identity is performed through PKI authentication to the issuance infrastructure using the existing token, in this case the CAC, rather than in-person verification by a Registration Authority (RA) or Verifying Official (VO).
    c. Issuance of DoD derived PKI credentials is dependent upon the requestor possessing a valid CAC. Possession of a CAC provides proof that face-to-face in-person-verification was completed. Derived PKI credentials will identify the possessor of the CAC by asserting the same Common Name (CN) as the PKI certificates on the requestor’s CAC.
    d. For certain higher assurance derived PKI credentials, called Assurance Level 4 credentials, in person identity proofing is still required, e.g. physical inspection of the CAC at the user authentication station in accordance with NIST Special Publication 800-63 (Reference b).
3. PKI credential storage and use on classified CMDs is not addressed in this interim guidance. The roadmap for PKI credential storage on classified CMDs will be established by the National Manager for Classified Systems via the Committee for National Security Systems (CNSS).
4. Milestones are established from the memo signature date.

B. TECHNICAL APPROACH

1. The National Security Agency (NSA) has completed a risk analysis on the use of a CMD’s native key store and found it to be acceptable for the storage of National Security Systems (NSS) PKI credentials for unclassified NSS (Reference a).
2. For commercial mobile devices which are certified by the National Information Assurance Partnership (NIAP) Protection Profile for Mobile Device Fundamentals (MDFPP) (Reference c), derived PKI credentials will be permitted to be stored in the CMD’s native keystore. No additional protections or compliance requirements are recommended in the decision memorandum (Reference a).
3. Once derived PKI credentials are stored on a CMD, it shall be handled as if it were the CAC from which they were derived. Users must report it as missing immediately after it

is discovered as missing, the device shall not be loaned to other users, and users shall maintain positive control at all times.

4. For commercial mobile devices which have not been certified in accordance with the MDFPP, derived PKI credentials shall continue to be generated and stored in FIPS 140-2 level 2 validated cryptographic modules with FIPS 140-2 level 3 physical security in accordance with the DoD PKI Certificate Policy (CP) and SP 800-63-2.
5. The issuance infrastructure for the derived PKI credentials will provide one or more derived PKI credentials to enable client authentication and digital signature operations from an authorized CMD.
6. This issuance infrastructure shall copy the user's encryption certificate and recover the decryption key from escrow to enable client decryption from an authorized CMD.

C. IMPLEMENTATION TASKS

1. The NSA NIAP office will facilitate certified test laboratories' evaluations of mobile devices against the MDFPP and add mobile devices which successfully complete evaluation to the Product Compliant List at https://www.niap-ccevs.org/CCEVS_Products.
2. DoD elements shall continue to comply with the key generation and storage requirements in the DoD PKI Certificate Policy, using only cryptographic modules that are either FIPS-validated or approved against an alternate standard published by the DoD PKI Project Management Office (PMO) for generating and storing DoD PKI private keys on unclassified CMDs.
3. Within 90 days, the DoD PKI PMO in conjunction with the DoD Public Key Enabling (PKE) and DoD PKI engineering teams shall design the approach for implementing an enterprise derived PKI credential issuance service for unclassified CMDs. This service shall be comprehensive, ensure interoperability with other Federal Departments and Agencies using a PKI, leverage available open standards, support commercial MDMs, and at a minimum include the following:
    a. Support for a use case specifying the requirements for the provisioning and use of both device credentials and user derived PKI credentials
    b. Identity verification using existing CAC certificates
    c. Secure generation of derived PKI credential keys on commercial mobile devices
    d. Secure generation or transfer of device keys to the commercial mobile device
    e. Secure certification of public keys
    f. Incorporation of an enrollment service and associated protocols into the relevant Certificate Authority (CA)
    g. Recovery of the user decryption key from the escrow system
    h. Secure destruction of any key transfer media for keys not generated on the CMD
    i. Certificate profile requirements
    j. Revocation relationships to the existing CAC certificates
    k. Ability to scale credential issuance and certificate management to the level required by the DoD
    l. Help desk support
    m. An estimation of costs associated with alternative issuance infrastructure approaches.

4. The DoD Mobility PMO shall integrate the recommended derived PKI credential issuance approach defined in section 3.3 into the Defense Mobile Unclassified Capability (DMUC) by July 2015.

D. PRIORITIZATION OF PKI PILOTS AND RELATED DEVELOPMENT

1. In order to prioritize resources for a derived PKI credential infrastructure development, technology evaluation in the following areas shall be discontinued:
    a. Universal Integrated Circuit Cards (UICC)
    b. Unauthorized microSD card pilots for storing DoD PKI credentials
2. Near Field Communications (NFC) for mobile devices shall be limited to the existing pilot. Activities investigating NFC for physical access and transit payments are authorized to continue.
3. All future activities involving access to DoD PKI private keys across an NFC interface or storage of derived PKI credentials using an approach not covered by this memo shall be coordinated with DoD CIO and the DoD PKI PMO.

E. POLICY ACTIONS

1. Within 15 days, DoD CIO shall request guidance from the Office of Management and Budget (OMB) with respect to M-06-16 and M-07-16 two factor authentication separation requirements.
2. Within 60 days the DoD Deputy CIO for CyberSecurity shall propose modifications to DoD Instruction 8520.03. The policy changes shall incorporate approved mobile storage options into the credential strength definitions and associated authorized data sensitivity levels.
3. Within 60 days DoD PKI Policy Management Authority (PMA) will approve the use of the recommended Object Identifier (OID) for user certificates on CMDs
4. Within 90 days DISA Field Security Operations shall modify the DISA Mobile Policy Security Requirements Guide (SRG) and any Security Technical Implementation Guides (STIGs) or DoD Annexes (Reference d) to mobile device protection profiles to permit the use of DoD PKI credentials stored within native keystores on CMDs certified in accordance with the MDFPP.
5. No administrative access to DoD systems from mobile devices is allowed at this time.
6. The use of hardware token PKI credentials on laptops and desktops is still required, and any policy changes made for mobile devices do not affect this requirement.

F. LONG TERM TASKS

1. NSA shall stay abreast of emerging technologies and ensure Information Assurance (IA) requirements are captured in Protection Profiles issued by NIAP. This shall include research and development in the following areas:
    a. Assess technologies such as Trusted Execution Environments (TEE) as these are employed by CMD vendors to augment protections provided by existing native key stores.

b. Coordinate the ongoing development of the Trusted Platform Module (TPM) Protection Profile to ensure consistency in the guidelines for hardware roots-of-trust on mobile devices.
c. Identify research and development requirements for improved derived PKI credential security, generation, implementation, and key management including revocation.

REFERENCES

(a) NSA Memorandum, “Commercial Mobile Device (CMD) Public Key Infrastructure (PKI) for Unclassified National Security Systems (NSS) Way Forward-DECISION MEMORANDUM,” July 31, 2014

(b) NIST Special Publication 800-63, “Electronic Authentication Guideline,” February, 2013

(c) National Information Assurance Partnership Protection Profile, “Protection Profile for Mobile Device Fundamentals,” February 12, 2014

(d) “DoD Annex for Mobile Device Fundamentals Protection Profile,” Version 1, Release 1, January 29, 2014