DISA
A Combat Support Agency

Side Loading Software Certificates on CMDs

Considerations for Pilot Planning

This briefing is UNCLASSIFIED

William MacLeod

2 February 2015

Version 1.0

DISA
A Combat Support Agency

Problem Statement

CC/S/As piloting software certificates on Commercial Mobile Devices within the scope of the *DoD Interim Guidance on the Use of DoD Personal Identity Verification Derived Public Key Infrastructure Credentials on Unclassified Commercial Mobile Devices* Memorandum, must distribute DoD PKI credentials as .P12 files until an enterprise over-the-air enrollment capability is available. Provisioning procedures for these pilots must be carefully planned to ensure DoD CIO's risk acceptance of storing PKI credentials in the hardware-backed keystores of NIAP certified CMDs does not necessitate storing credentials in unprotected states.

DISA
A Combat Support Agency

Notional End State for Ideal Pilot

1. DoD PKI subscriber has access to PK-Enabled services from their CMD
2. DoD PKI credentials are accessible to all approved applications that require them, but not accessible to unapproved applications
3. DoD PKI credentials on the CMD are protected from export by the secure key storage mechanisms described in the Mobile Device Fundamentals Protection Profile
4. No P12 files remain as artifacts of the transfer of the keys from the RA workstation to the CMD's secure storage

DISA
A Combat Support Agency

Planning Phases for Soft Cert Pilot

PKE recommends pilot planning address five stages in the life of the certificate.

Establish Scope	Generate PKI Credentials	Install PKI Credentials on CMD	Monitor CMD Health	Credential End-of-Life
• Certificate requirements will be driven by the scope of the pilot. Consider what services need to be PK-Enabled.	• Identify the RA/LRA CPS processes for generating and transferring credentials	• Identify what tools are available to make keys accessible to applications • Clean up P12s	• Ensure handset remains in the intended configuration for protecting keys	• Plan for revoking and destroying keys when appropriate

DISA
A Combat Support Agency

What Do You Want to Pilot?

1. Identify the capability being piloted
   - What handset? For this presentation, we'll assume all four major platforms are being piloted.
   - What applications? For this presentation, we'll assume a VPN client, an email client, a web browser, and a non-specific PK-Enabled COTS or GOTS application.
2. Identify the types of certificates that are needed for the applications being piloted.
   - Authenticating the user many servers may require a certificate with a UPN
   - To support S/MIME Email Encryption, it makes sense to recover the existing credential instead of generating a new one.
3. Identify the policy coverage for the pilot.
   - Does the pilot comply with the scope of *DoD Interim Guidance on the Use of DoD Personal Identity Verification Derived Public Key Infrastructure Credentials on Unclassified Commercial Mobile Devices*?
   - Is the pilot platform certified by NIAP and is it configured to comply with the MDF PP?
   - How are gaps in coverage addressed?

DISA
A Combat Support Agency

PKI Credentials Generated through Existing Processes

1. Identify the TAs, LRAs, RAs and KRAs that will be supporting the pilot.
   - DISA found the workload necessitated dedicated staff to fill these roles for its software certificate pilots
   - Coordinate training and credentialing as necessary
2. Identify the RA portals that will support provide these certificates
   - Existing RA processes should be sufficient to generate P12s of all necessary DoD PKI certificates
   - DISA used Alternate Login Token (ALT) Profile* on software CA-27, the EmailAuth Portal and the KRA portal
3. Identify the RA Workstations being used
   - At DISA, RA's were not permitted to install Configurator or connect microSDs to the RA Workstation
4. Ensure pilot participants provide:
   - Digitally signed email to KRA authorizing recovery of their keys for this purpose
   - Signed DD Form 2842 acknowledging receipt of credentials and responsibilities
   - End user agreement may require update

* The DoD PKI RA/LRA CPS requires this certificate be issued into hardware. DoD CIO is the approval authority to diverge from this requirement.

DISA
A Combat Support Agency

Resources for Certificate Generation

- DoD X.509 Certificate Policy and DoD PKI RA/LRA Certificate Practice Statement provides guidance on what certificates can be issued and requirements for their issuance
- DoD PKE hosts training decks for LRA, RA, and KRAs on IASE
  - http://iase.disa.mil/pki-pke/Pages/rlts.aspx
- DoD CIO Memo *DoD Interim Guidance on the Use of DoD Personal Identity Verification Derived Public Key Infrastructure Credentials on Unclassified Commercial Mobile Devices* provides guidance on limits of software certificate risk acceptance

DISA
A Combat Support Agency

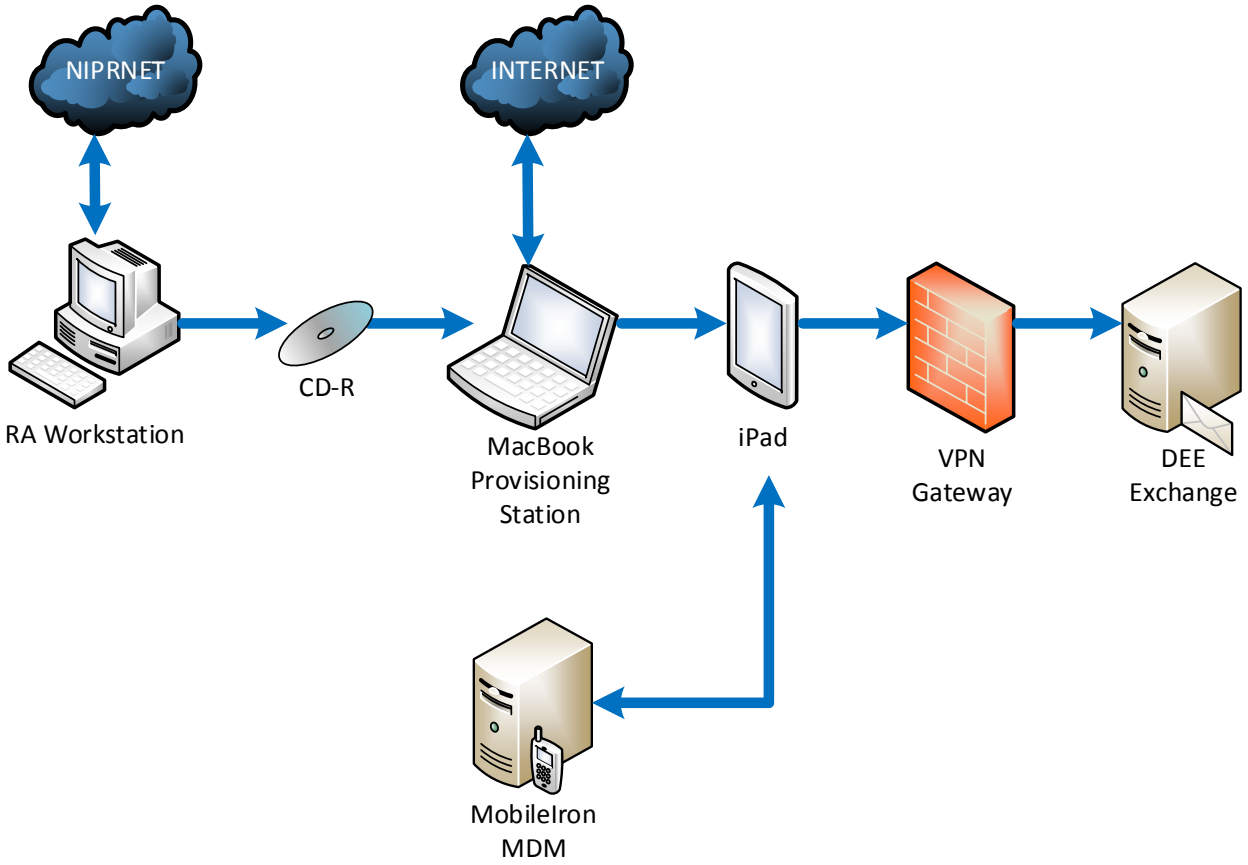
Goals for Installing PKI Credentials on CMD

1. Make keys accessible to the applications that require them
2. Place the keys in the secure storage of the CMD
3. Ensure keys do not exist anywhere except the intended mobile device
4. Destroy any copies of the keys that were necessary to complete installation

DISA
A Combat Support Agency

DISA's iOS Provisioning Model

1. Generate ALT, Signature, and Encryption Certs on RA Workstation as P12s
2. Burn P12s to CD
3. Provision device in MDM
4. Generate iOS Configuration Profiles on MacBook w/o copying P12s to file system
5. Push Configuration Profiles to iPad
6. Connect to VPN
7. Email profile should update
8. Destroy CD-R



Establish Scope | Generate PKI Credentials | **Install PKI Credentials on CMD** | Monitor CMD Health | Credential End-of-Life

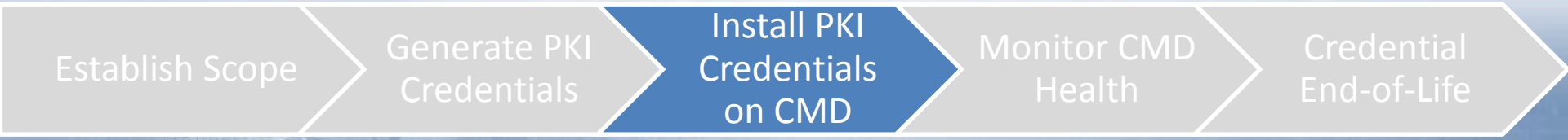
DISA
A Combat Support Agency

Transferring P12s into Secure Storage

Method for installing PKI credentials in secure storage vary by platform, but may include

1. Installation from on-device disk or microSD
    1. This method may introduce risk if the P12 stays on the device after installation, because the P12 could be copied to another device
    2. Ensure the P12 is deleted after installation (not just the pointer) or the microSD is removed
2. Installation from email attachments
    1. This method introduces the risk that the certificate is installed on any device of the email recipient's choosing
    2. This method requires the recipient already have access to their email from the device
    3. Implementing this capability falls under over-the-air provisioning rather than side-loading
    4. DoD PKE recommends against this approach
3. Installation from web sites
    1. This method requires the user and device authenticate prior to receiving their credential
    2. Implementing this capability falls under over-the-air provisioning rather than side-loading
    3. DoD PKE recommends against this approach
4. Installation from configuration profile push
    1. This method can be implemented over USB or over-the-air
    2. Over USB requires a configuration utility installed on a provisioning workstation
    3. Over-the-air exposes the credential to intercept unless it is encrypted to the intended recipient's device (more to follow in PureBred presentation)

We will focus on options 1 and 4(USB) for this presentation



DISA
A Combat Support Agency

Option 1: Installation from Disk Space

- The general concept behind this approach is copying the P12 from the RA workstation onto the file system of the mobile device, then using the CMD's key installation process
  - P12s residing on the file system of a NIAP certified mobile device do not benefit from the full protections of the secure storage
  - Deleting P12s after installation may not be sufficient. Ensure handsets are destroying the key and not merely removing a pointer to the file
- Identify all logical locations in which the P12 file is saved during provisioning, so that they may be destroyed after provisioning

DISA
A Combat Support Agency

Option 4: Installation from Configuration Profile over USB

- DISA used the Apple Configurator on a Provisioning Workstation (Mac Mini) to generate Configuration Profiles and push P12s directly into iOS System KeyChain
  - Apple Configurator requires internet access to start, but not to run.
  - Apple configurator allowed P12s to be pushed to device without installing them on the workstation. iPhone Configuration Utility did not.
- Side-loaded and manually configured configuration profiles introduce new challenge of unmanaged profiles in iOS
  - MDM may not be able to remove side-loaded configuration profiles in the event of compromise
  - File sharing between managed and unmanaged applications may be disallowed

DISA
A Combat Support Agency

Consider Key Access Controls

- One of the security strengths of many modern CMDs is the use of application-specific keychains to prevent key access to unintended applications.
  - In iOS, keychains are separated by the app-signer, so if you want credentials for the native email client and a GOTS application, you need the keys in both keychains.
  - BlackBerry 10 handsets make keys in the Corporate side of BlackBerry Balance available to all apps
  - Android and Windows have similar key-chain concepts, but DoD PKE is unprepared to present on them at this point
- In order for an application to use DoD PKI credentials it must be written to use credentials correctly.
  - DoD PKE hosts DoD PKI Functional Interface Specification on IASE to assist developers in supporting DoD PKI. http://iase.disa.mil/pki-pke/Pages/admin.aspx

DISA
A Combat Support Agency

Deviations from the Configuration Baseline

1. At DISA, Soft Cert pilot on DMUC handsets necessitated new configuration profile push from MobileIron MDM
   - Removed the Email Profile from the MDM Configuration Profile
   - Increase device password complexity to minimum requirement for activation secret for user credentials

DISA
A Combat Support Agency

Resources for Certificate Transfer

- Vendor documentation is the most important
- Vendors generate “Security Target” documents as part of NIAP certification. These provide guidance on what they consider to be their secure storage.
  - https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm

DISA
A Combat Support Agency

Monitoring the Health of the CMD

- Throughout the lifecycle of the CMD events may impact certificates
  - Device is lost or stolen
  - Device is jailbroken or rooted
  - User removes configuration profiles
  - User removes certificate profiles
- Existing RA processes do not provided automated responses or alerts to these events
- User agreement for pilot participants should specify user responsibilities for protecting their device and notifying their LRA
- MDM can provide additional monitoring tools for LRAs to track the health and compliance of the devices that have DoD PKI credentials
- Coordination with Tier 1 help desks, helps prevent mistaken removal of pilot configuration profiles
- RAs should also track the user's CAC-eligibility over time to ensure their software certificate is revoked when they are no longer required

DISA
A Combat Support Agency

Credential End-of-Life

- DoD PKI permits issuing Software Certificates for up to three years, but the certificate should not be issued for longer than:
  - The date of expiration of the participant's CAC
  - The end of the software certificate pilot
- Plan for changing email encryption keys over time.
- Plan for rekeying devices if the pilot is expected to continue past the expiration of the certificate
- If an event necessitates revocation of the DoD PKI credentials, ensure notification channels are established to alert the RA
- Encryption keys are still valuable after their certificates expire or are revoked, so destroy expired/revoked keys on device whenever possible.

DISA
A Combat Support Agency

DoD PKE POCs

DoD PKE Help Desk

dodpke@mail.mil

Merkeshia Hines-McKnight

DoD PKE Project Lead

mcknight.m.hines.civ@mail.mil

William MacLeod

DoD PKE Mobile Lead

william.r.macleod.ctr@mail.mil

DISA
A Combat Support Agency

Questions

www.disa.mil