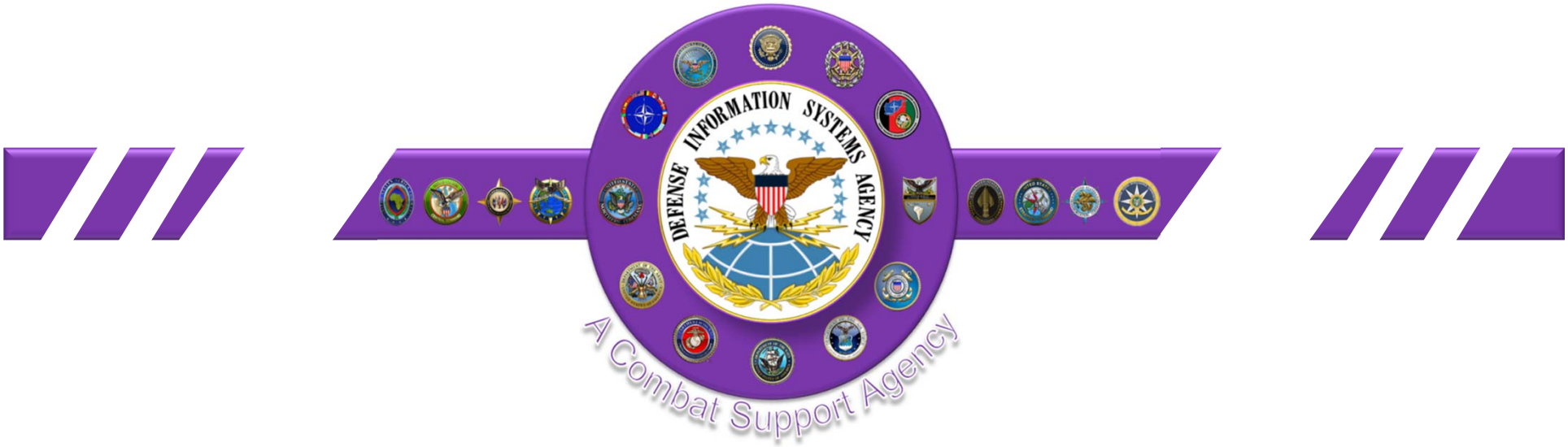

DoD iOS Soft Certificate Pilot

Greg Youst

DISA Chief Mobility Engineer

4 March 2015

Agenda

- Derived Credentials for Mobile Devices
- Pilot Approval
- Pilot Scope
- Phased Approach
- Provisioning Process
- Key Dependencies
- Required SOPs/TTPs
- Over-the-Air (OTA) PKI Provisioning Effort

Derived Credentials for Mobile Devices

- **Link to Common Access Card**
- **Eliminate smartcard readers**
- **Simplify credential management**
  - Authentication
  - Signature
  - Encryption certificates
- **DoD CIO Interim Guidance on Derived Credentials, released 23 Sep 2014**
  - *"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)"*
  - Signatory: Terry Halvorsen, Acting DoD CIO

DoD CIO Pilot Approval

- **DoD CIO Memorandum to Defense Information Systems Agency for exception to DoD PKI policy, released on 18 August 2014**
  - **"Request for Approval to pilot software Public Key Infrastructure Credentials on Unclassified Defense Information Systems Commercial Mobile Devices"**
- **Authorized for 1 year duration**
- **Authorized up to 500 devices**
- **Pilot only authorized on the unclassified network (NIPRNet)**
- **DoD PKI Medium assurance software certificates used will be Alternate Token (ALT) Certificates which is the exception to policy requested.**
- **All devices used must be FIPS 140-2 Level 1 certified and completed or have submitted an evaluation package to the National Information Assurance Partnership (NIAP) for certification against the Mobile Device Fundamentals Protection Profile within 4 months of the start of the pilot.**

Pilot Scope

Conduct pilot to test iOS 8 integration with user soft certificates to offer following capabilities:

- **Native signing/encryption**
- **Native browser authentication to PKI Enterprise Services**
- **Exchange ActiveSync**
- **User Authentication for VPN**

Phased Approach

- **14 select personnel were identified to participate in the pilot from the following groups:**
  - **Phase I (PMO Internal)**
  - **Phase II (DISA Non-VIPs)**
  - **Phase III (DISA VIPs)**

Provisioning Process

Below table outlines key steps required to provision an iOS device with soft certs, and MDM

Key Steps	Performed By
Identify Test Users	Mobility PMO
Generate Soft Certs & Load them on CDs	NIPRNet RAs
Update/Apply MDM Configurations/Policy (Exchange settings/Password)	Mobility PMO
Collect Devices	Tier I Support Operations
Load Latest iOS 8 OS	Tier III Support Engineers
Build Configuration Profile via Apple Configurator Tool and integrate user cert	Tier III Support Engineer/RAs
Push Configuration Profile to the device and issue MDM Provisioning PIN	Tier III Support Engineer/RAs
Provision Device with User and Conduct Preliminary Testing	Tier I Operations/User
Begin User Acceptance Testing	User/Tier 1/Tier II/Tier III Support
End User Acceptance Testing	Mobility PMO
Capture Feedback	Mobility PMO

RA: Registration Authority

Key Dependencies

- DAA Approval to generate and load soft certs
- Update MDM Policy/Configuration to have device password in accordance with DoD PKI Policy of at least 8 numeric and alphabetic characters
- Process RA/LRA Nomination Letters
- Train RAs to create and install PKI certificates
- Obtain and deploy RA Equipment
  - Workstation to generate user certificates
  - Standalone iMac Computer to create ACT profiles and push to device

Required SOPs/TTPs

Following is the list of SOPs/TTPs needed to perform this pilot

1. **Soft Cert Generation SOPs**
2. **Install beta iOS SOPs**
3. **Setup iMAC Computer SOPs**
4. **Setup/Use Apple Configurator Tool SOPs**
5. **User Acceptance Test TTPs**
6. **User feedback data collection**

SOP: Standard Operating Procedure

TTP: Tactics, Techniques and Procedures

Over-the-Air (OTA) PKI Provisioning Effort

- Developed a basic generic OTA PKI provisioning flow
- Currently working on an iOS approach
- Working prototype planned for mid-March
- Operational OTA PKI provisioning system planned for FY15
- Other mobile OS OTA PKI provisioning process to follow

Questions