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

CHIEF INFORMATION OFFICER

MAY 0 6 2015

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
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
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: DoD Interim Guidance for Implementing Derived Public Key Infrastructure Credentials on Unclassified Commercial Mobile Devices

Reference: DoD CIO 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

The DoD CIO issued interim guidance permitting the use of derived Public Key Infrastructure (PKI) credentials on Commercial Mobile Devices in September 2014. The Defense Information Systems Agency (DISA) is currently developing a secure, scalable, and automated issuance capability for derived credentials for multiple devices. Until the automated provisioning is available later in 2015, components are authorized to issue derived PKI credentials in accordance with the procedures published and maintained on the DoD Information Assurance Support Environment (IASE) web site. (http://iase.disa.mil/stigs/Pages/index.aspx)

The Office of the DoD Chief Information Office point of contact for this matter is Mr. Mitchell Komaroff at email: mitchell.komaroff.civ@mail.mil, 703-697-3314.

Terry A. Halvorsen

DOD INTERIM CREDENTIAL IMPLEMENTATION INSTRUCTIONS
BlackBerry Devices

A. INTRODUCTION

1. The objective of this document is to provide an outline of the technical and administrative process necessary to establish and use derived PKI credentials on a BlackBerry smartphone.

2. The process outlined in the following steps will generate a key pair and an associated email signing certificate and recover the user's private email encryption certificate and associated private key (used to decrypt emails). Additionally, these steps will provide instructions for loading the certificates and private keys onto a BlackBerry.

3. These instructions are written and intended to be used only by DoD information technology (IT) personnel in direct support of the DoD service/agency they are supporting.

4. These instructions are only applicable to the BlackBerry smartphone operating system versions 7.X.X and newer and 10.2.X and newer.

B. TECHNICAL APPROACH

1. A DoD IT Professional will perform these steps with the user present.

2. The DoD IT professional will use a properly configured workstation with two CAC readers in the support area to perform this operation.

Encryption credential

1. To recover the email encryption credential, use Microsoft Internet Explorer 10 or newer and navigate to one of the following sites:

   a. https://ara-3.csd.disa.mil/ara/Key

      Or

   b. https://ara-4.csd.disa.mil/ara/Key

2. Authenticate to the site using the user’s identity certificate (certificate without Email in the display name). The user will enter their PIN. Make sure you chose the user’s certificate and not your own or you may lock out the CAC.

3. Identify the user’s current encryption certificate and choose “Recover.” The site will display a link to download the certificate and display the password to be used when importing the certificate. Create a folder on the local drive to temporarily store the certificate (e.g. c:\PKI). Click the download link and save the certificate in the

designated location for certificates on the local hard drive. The location shall not be a network or shared drive.

4. Document the password displayed in the above step. Do not save the password electronically on the same system as the certificates.

Signature Certificate

5. To generate the derived email signature certificate, use Mozilla Firefox version 32.0 configured in accordance with the Security Technical Implementation Guide (STIG). Note: newer versions do not work at this time.

6. Firefox has to be configured with a software security device to perform this operation. Follow the steps under, “Using Common Access Card (CAC) certificates in Firefox” at this site: http://iase.disa.mil/pki-pke/getting_started/Pages/firefox.aspx.

7. Once you verify Firefox is configured appropriately, navigate to the following site: https://email-ca-28.csd.disa.mil/ca/emailauth.html or https://email-ca-27.csd.disa.mil/ca/emailauth.html.

8. Set the certificate key length to 2048 and choose: “Signature Certificate only” from the dropdown.

9. Type the user’s email address that matches their email address on their CAC (enter twice). (NOTE: Verify their email address on their CAC before proceeding. If the email address is incorrect, it must be fixed prior to proceeding. For more details: https://www.dmdc.osd.mil/self_service/help/RAPIDS_Self_Service_Help.htm#Introduction.htm). When you select “Get Certificate,” you will be prompted to choose a token. If Firefox is configured correctly, the dialog box will show “FIPS Module.” Choose OK. When prompted for a PIN, make sure the user enters their PIN. Be careful to choose the correct authentication certificate or you may lock one of both CACs.

10. The next dialog will ask you to choose the certificate to present to verify identification. Choose the identity certificate of the user and make sure you uncheck “Remember this decision.” You may receive two alerts and then a screen stating the certificate has been stored in your browser with instructions on how to recover the certificate; do not follow those instructions.

    NOTE: If you receive an “Authentication Error” message, you may not have deleted a previous certificate. To do this, navigate to options, advanced, certificates, and choose view certificates. Delete the certificate labeled “software security device” located in the tab labeled “your certificates” and try again.

11. Once this is successful and you receive the instruction page from step 10 above, navigate back to Your Certificates at the location in the NOTE from step 10, select the certificate, and choose backup.

12. You will be prompted for a location to save the certificate. Navigate to the same location you stored the email certificate, type a file name and choose save.

13. You will be prompted for a password. You MUST use a 16 character complex (i.e. uppercase, lowercase, numbers, and special characters) to protect this certificate.

14. For more information on protecting certificates, review the document at the following link:
http://iase.disa.mil/pki/eca/Documents/Protecting_ECA_Software_Certificates.doc

<u>Installing certificates on the BlackBerry</u>

15. Loading certificates shall be done at the same workstation on which the certificates were stored per paragraph B.3., above.

16. For legacy BlackBerry devices, only operating system 7.x.x and newer shall be used.
    a. The device should already have the key store password set and synchronized with the device password. Additionally, ensure the key store is configured in accordance with the latest STIG.

    b. Ensure the devices' key store settings on the BlackBerry Enterprise Server (BES) match the STIG required settings. The goal is to give the user the same experience as they have at their desktop with respect to the timeout period for entering their CAC PIN.

    c. Connect the user's device using a USB cable, and use desktop manager certificate sync to transfer the certificates to the device. NOTE: If you do not see "Certificates" as an option, go to tools, and look under the "General" tab and check the box "Use certificate synchronization."

    d. Certificates are not exportable once imported to the BlackBerry.

17. For BlackBerry 10 devices, operating system (OS) 10.2.1.x and newer shall be used.

    a. Connect the BlackBerry to the desktop. The BlackBerry should appear as an external drive on the computer. Drag both certificates to a folder on the device (not the micro SD card). This will place the certificates on the "Personal" side of the device.

    b. On the device, navigate to Certificates located in Settings under Security and Privacy. Select the "Import" button, then "Device-Personal, and navigate to the certificates file, select it, enter the password, then select import to work perimeter. Then repeat the import for the 2nd certificate. Be sure to enter the right password for each certificate. Once the import is completed, delete the certificate files in the file system on the personal side of the device.

c. On BlackBerry 10 OS devices, the work space timeout is what controls access to the certificates. This should be set in accordance with the latest STIG.
d. Certificates are not exportable from the BlackBerry once imported.

C. ADMINISTRATIVE TASKS

1. The DoD agency using these instructions shall create an addendum to the user agreement with the following language, at a minimum.

   a. The user understands there is additional risk in using derived PKI credentials on mobile devices.

   b. The user will treat the BlackBerry smartphone as if it were their Common Access Card (CAC) (e.g. report the card lost or stolen immediately). The user agreement will provide information on how to report a lost or stolen device.

   c. The user acknowledges they have been trained how to wipe the device in the event the device starts to operate abnormally.

   d. The user understands that if they lose their CAC, they also have to replace the credentials on their mobile devices. If the user loses their mobile device which contains their PKI credentials, they must also replace their CAC.

2. The DoD agency using these instructions shall keep a list of users and certificate information (e.g. types of certs, s/n's, etc.) which have PKI derived credentials on their BlackBerry smartphone. Tracking shall be done on a spreadsheet or in a ticket tracking system (e.g. Remedy) where reports can be easily created identifying who has derived PKI credentials on their BlackBerry.

3. The DoD IT personnel performing these steps shall ensure both credentials stored on the computer during the transfer process are deleted from the local storage and certificate stores on all browsers. Additionally, empty the trash or deleted files to ensure the files no longer resides on the system in any form. The paper the password(s) were written down on shall be shredded or placed in a burn bag.

4. DISA shall incorporate these procedures in the next revision of the BlackBerry STIG located here: http://iase.disa.mil/stigs/net_perimeter/wireless/Pages/smartphone.aspx.

5. These instructions are to be used as an interim step to provide the derived PKI capability and functionality until an approved scalable enterprise solution is available.

6. The DoD CIO point of contact for the technical instructions is Will Alberts at william.r.alberts.ctr@mail.mil or 571-372-4727.

REFERENCES

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

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

(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

(e) “DoD CIO 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.

Frequently Asked Questions

DoD Interim Guidance for Implementing Derived Public Key Infrastructure
Credentials on Unclassified Commercial Mobile Devices, May 06, 2015.

Subject: DoD Interim Guidance for Implementing Derived Public Key Infrastructure Credentials on Unclassified Commercial Mobile Devices, May 06, 2015.

Overview

The intent of this Frequently Asked Questions (FAQ) document is to provide clarification of the subject memorandum based on inquires received from the DoD CIO.

The following is a list of questions with responses to provide clarification or updates to the subject memorandum.

Q1. Firefox version 32.0 has multiple vulnerabilities, can we use a newer version of Firefox to recover Signing Certificates?

A1. Response: No. Newer versions of Firefox after 32 are not compatible with the DoD PKI. The vulnerabilities associated with Firefox 32 can be mitigated on the system if its use is restricted to generating credentials for the purpose of this memo.

Q2. The links provided in the subject memorandum for recovering the email encryption certificate are not working.

A2. Response: DoD Public Key Enabling (PKE) Engineering Support has updated the auto recovery agents for recovering email encryption certificates:

Legacy CA (Below CA 33):

- https://ara-3.csd.disa.mil/ara/Key

CAs 33 and Above:

- https://ara-5.csd.disa.mil
- https://ara-6.csd.disa.mil

If you still have issues recovering your email encryption private key, please visit DISA Public Key Infrastructure (PKI)/PKE contact us page to locate your RA/RKA:

- http://iase.disa.mil/pki-pke/Pages/contact.aspx

Q3. What is Purebred and how does the subject memorandum relate to Purebred?

A3. Purebred is a DISA government off the shelf (GOTS) application built to meet the requirements of the DoD CIO 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. Which can be found at this site: http://iase.disa.mil/stigs/mobility/Pages/index.aspx

The subject memorandum was published as interim guidance until an enterprise Derived Credentials solution is developed (Purebred). DISA's Derived Credential solution, Purebred, is in the piloting phase. Purebred is being developed by DISA PKI Engineering to provide a secure, over the air, and scalable method of distributing DoD PKI certificates on commercial mobile devices (i.e., Blackberry, iOS, Android, Windows).

More information about Purebred can be found at the following locations:

- Website - http://iase.disa.mil/pki-pke/Pages/purebred.aspx
- Email - dodpke@mail.mil

Q4. Do users who lose their CAC or mobile device have to replace credentials on their mobile device and obtain a new CAC?

A4. The attachment to the memo currently states:
"C. 1. d. The user understands that if they lose their CAC, they also have to replace the credentials on their mobile devices. If the user loses their mobile device which contains their PKI credentials, they must also replace their CAC."

If the CAC is lost:
The user will replace the recovered private key on the mobile device used for reading encrypted email (key encipherment key).
FYI: The email signature key on the CAC and mobile device are not the same so the email signature certificate on the mobile device does not need to be replaced.

If the mobile device is lost:
The user shall leverage the PKI self-service portal to generate a new email key used for reading encrypted emails. The portal is located at: https://pki.dmdc.osd.mil/self_service/

Once you sign into the portal, select the "Change CAC email". Make sure you enter your CURRENT email address (unless it does need to be changed). This will generate a new key encipherment certificate (email decryption) on your CAC. You will then be able to recover this new certificate in accordance with the subject memorandum's instructions.

NOTE: This process requires a stable connection to the internet. In some cases, you may have to close and re-open your browser and start over if an error or the site times out.

Government POC's for the subject memorandum:
Mr. Komaroff, Mitchell at mitchell.komaroff.civ@mail.mil and 703-697-3314
Ms. Santos-Logan, Carmen J. carmen.j.santoslogan.civ@mail.mil and 571-372-4692

Technical POC's for this FAQ and subject memorandum:
Mr. Alberts, Will at william.r.alberts.ctr@mail.mil and 571-372-4727
Mr. Rossero, Stephen J at stephen.j.rossero.ctr@mail.mil and 571-372-4907