CHAT QUESTIONS FROM 11/1/17 DERIVED PIV CREDENTIALS COI CALL

Thank you to those who partipated in the call. Below are the answers to the questions that were raised during our most recent Derived PIV call. Additional information about this project can be found on our website, including links to download the Derived PIV Credentials draft practice guide.

1. **Is the Entrust Datacard PKI CA really in the "cloud" or in their managed data center?**

   It is really in the cloud such that those with appropriate permissions are able to access it. In this case the cloud location is a managed data center. It is a test environment of the service at this site: https://www.idmanagement.gov/trust-services/

2. **How did you handle the issue of API between Entrust & MobileIron?**

   The NCCoE did not participate in the integration of the two solutions – the integration stems from a partnership that already existed.

3. **Can you talk about integration challenge between EMM and CMS?**

   There were numerous configuration items we needed to create within the MobileIron EMM to allow authorized mobile users to have DPC certificates from Entrust provisioned to their managed devices; that process was facilitated through vendor participation, and is fully documented in Volume C of our practice guide.

Key Storage

4. **Where are the private keys stored, and how are they generated. For those who are not familiar with MobileIron can you compare/contrast to local native device keystore, like the Apple keychain?**

   This build focused entirely on the software container provided by MobileIron. We may experiment on native keystore storate in the future. The private keys are generated on the device.

5. **Where is the credential stored on the device? MobileIron PIV-D Entrust app?**

   MobileIron software container.

6. **How is private key generated on mobile device? Are you copying over a p12? Or is private key generated using app on device? Does that mean you are generating private key on device or copying over a p12 to MobileIron key store?**

   See above

7. **Are the certs deployed in a virtual card? Containing additional related certs like digital signature & encryption or just the Derived PIV Auth cert?**

The Derived PIV Authentication certificate is provisioned into the MobileIron secure software container in this architecture. The optional digital signature and recovered encryption keys are also installed during the enrollment process, but the practice guide focuses on the lifecycle of the Derived PIV Authentication certificate.

Levels of Assurance

8. **Is this an LOA-3 solution? If so, has an LOA-4 solution been created?**

   NIST SP 1800-12 shows only L0A-3 architectures. This project has no plans to tackle LOA-4.

   For the purposes of this project we documented the MobileIron Secure Container at AAL-2 (new 800-63-3 language).

9. **What's the integration between Sentry & enterprise services... KCD? KCD = Kerberos Constrained Delegation, but thanks, you answered it**

   In our reference solution Sentry was used for VPN services into the lab enterprise network. KCD was not explored in this architecture.

10. **Are the crypto modules FIPS 140-2 validated in the demonstration at NCCoE? More importantly resistant to the recent ROCA (return of the Coopersmith's attack)?**

    Yes, MobileIron's product is validated. See Table 3-3 in Section 3.4.3 in NIST SP 1800-12 Practice Guide Vol B. As we integrate hardware into future architectures, we will evaluate to identify if the ROCA Infineon attack is relevant.

11. **Is Entrust Managed PKI approved to issue the LOA3, id-fpki-common-pivAuth-derived Object Identifier (OID)?**

    Please contact Entrust Managed PKI and FPKI GSA APL for the latest service offerings:

    https://www.idmanagement.gov/trust-services/

12. **Does NIST believe most federal use cases are at the AAL 2 level? Including Network logon via VPN**

    A lot of applications are at the AAL 2 level and are capable of meeting most Federal use cases security needs.

13. **As the vendors outline their implementation, will they show the "NIST" publication they are implementing.**

    Referencing a NIST SP is allowed but not required.

14. **And is that OID on the derived credential certificates issued in your pilot?**

    We used a test Object Identifier (OID). See Part C of the practice guide for more details.

15. **The diagram on slide 8 shows both authentication and signing certificates but no mention of encryption keys. To work effectively the mobile device needs to have the same encryption key as the PIV card itself so that messages can be decrypted using the same key and messages can be encrypted at the device. The encryption key must be the same as the one used at the desktop (PIV) and the mobile device.**

    We did not explore key escrow practices in this architecture. This encryption certificate key escrow challenges are on our future challenges roadmap. We agree with your assertion.

16. **Will the NCCOE Document be Normative or informative for Federal Agencies?**

    NCCoE NIST 1800 series special publications are informative.

17. **Is MobileIron software available in the cloud as AWS AMIs?**

    Please contact MobileIron for the latest service offerings. Sean Frazier at sfrazier@mobileiron.com

18. **Is there a path through the NCCoE efforts to expand the scope of SP 800-157? In particular form factors, such as FIDO U2F/YubiKey Nano 4, Alt-Token (DoD and others) smartcards as Derived PIV; and scope beyond only logical access, for example appropriate use of Mobile Devices for Derived PIV physical access applications.**

    The Federal Government has been leveraging PKI and any changes FIPS 201 would certainly be a good project for the NCCoE to tackle by building a reference architecture that demonstrates the integration of new authenticators and government-wide interoperability of digital identity standards.

19. **Would a next iteration consider the use of a PIV backed FIDO credential?**

    See 18

20. **Does the RSA issue only affect Infineon chips or others also like NXP?**

    At this point the only NVD alert is here https://nvd.nist.gov/vuln/detail/CVE-2017-15361

21. **New to MobileIron products---do they have a tool for encryption for cellular phone devices?**

    Please contact MobileIron for the latest service offerings. Sean Frazier at sfrazier@mobileiron.com

22. **It is true that SP 800-157 only applies to authentication, right? Most who implement also want, or possibly only need, Email protection (Signing/Encryption) including integrity and confidentiality. Can you elaborate on these points regarding the pilots?**

    NIST SP 800-157 only applies for authentication. However, 800-157 does cover signing and encryption as a capability. The NCCoE project may address both signing (NISTIR 8055 includes signing) and encryption in the future.

23. **Intercede MyID also can provision into native keystore for native apps to access as well, such as Safari and email apps.**

    Correct, however this capability was not within the scope of the current phase of this project. Contact Intercede for more information. Won Jun at Won.Jun@Intercede.com

24. **Has any thought been put into automated revocation of credentials when the device is wiped?**

    In our architecture, there is no connection between wiping the MobileIron software storage container and revoking the credential from Entrust. Thoughts around automated revocation require careful examination of policy and support to continued access for credential holders.

25. **How is the PIV credential validation to the initial issuer accomplished?**

    The solution validates the PIV credential through PIV-AUTH mechanism per SP 800-157.