NIST Special Publication 800-157
Derived PIV Credentials

Hildegard Ferraiolo
PIV Program Lead
National Institute of Standards and Technology

March 3 - 4, 2014

FIPS 201-2 Supporting Special Publication's Workshop

The Author Team (from A to Z)

- William Burr
- David Cooper
- Hildegard Ferraiolo
- Salvatore Francomacaro
- Sarbari Gupta
- Jason Mohler
- Andrew Regenscheid

Purpose

- Users need to be able to access resources from mobile devices (e.g., smart phones, tablets).
- Not always practical to use PIV Card with a mobile device.
- Need to provide PIV credentials that can be used with mobile devices.

How to PIV-enable a Mobile Device

1. Use PIV Card over contact interface
   - Need smart card reader (SP 800-73-3 or SP 800-73-4)
2. Use PIV Card over contactless interface (NFC)
   - Use PIV Card's virtual contact interface (SP 800-73-4)
3. Use a credential that is not on the PIV Card
   - Derived PIV Credential (SP 800-157)

Scope of SP 800-157

- Derived PIV Credential intended to enable authentication to remote IT systems from mobile devices.
- Other use cases (e.g., physical access) are out of scope.
  - Policy requires that PIV Card be used whenever practical.
- Other guidelines address other aspects of mobile device security (e.g., SP 800-124).

What is a Derived PIV Credential?

- Derived Credential (SP 800-63-2)
  - A credential issued based on proof of possession and control of a token associated with a previously issued credential, so as not to duplicate the identity proofing process.
- Derived PIV Credential (SP 800-157)
  - A PIV credential for use with mobile devices that is issued in accordance with SP 800-157 based on proof of possession and control of a PIV Card.

What is a Derived PIV Credential?

- An X.509 public key certificate – similar to the PIV Authentication certificate
- Several options for cryptographic module:
  - Removable: USB, SD Card, UICC
  - Embedded: hardware or software
- Two options for assurance level of certificate (e-Authentication Assurance Level 3 or 4)

Why Only PKI?

- Interoperability
  - OMB M-11-11: “Agency processes must accept and electronically verify PIV credentials issued by other federal agencies.”
  - Leverages current work to PIV-enable relying party systems.
- Efficiency: PKI is already in place.

What About Secure Email?

- Scope of SP 800-157 is limited to issuing an authentication certificate (the Derived PIV Credential). However:
  - Appendix A (informative) notes that mobile device may have its own digital signature key/certificate. Key management key from PIV Card may be stored on mobile device.
  - Appendix B.1 (data model for card application for removable tokens) includes containers for digital signature and key management keys/certificates.

Summary

- Derived PIV Credentials:
  - Support PIV-enablement of mobile devices, when not practical to use PIV Card.
  - Leverage identity proofing and vetting processes performed during PIV Card issuance.
  - Have minimal impact on PIV-enabled relying party applications.

What did Change from Draft to Final?

- New Appendix C that provides example issuance processes for Derived PIV Credentials to issue both LoA-3 and LoA-4 credentials onto mobile device
- To clarify relationship of PIV Card and Derived PIV Credential, added new Section 2.1, describing the five Derived PIV Credential lifecycle phases and relates these to the PIV Card lifecycle.

What did Change from Draft to Final?

- Removed the details on how the microSD interacts with the mobile device. There are no widely adopted interoperable standard mechanism supported by mobile device vendors.
  - The use of microSD, may limit portability between devices.

What did Change from Draft to Final?

- Require an activation blocking mechanism for software token so that the use of the credential is blocked after too many wrong password tries.
- Also specify a throttling mechanism as an option to block software token activation after the wrong password has been entered too many times.
- Specify an optional unblock mechanism for software derived PIV Credential if password-lockout has occurred. Software implementations may instead choose to issue a new derived PIV Credential following the initial issuance process if the password is forgotten
-

What did Change from Draft to Final?

- Changed PIN to password to allows department and agencies tailoring password policy and make it harder to brut-force (guess) password.
- Wireless 2 factor token have been requested to be added as a solution. Further security study is needed in order to consider these in the next version of SP 800-157
- Not add other use-cases because of current policy direction

Thank you!

Questions?

Hildegard Ferraiolo
PIV Project Lead
NIST ITL Computer Security Division
hildegard.ferraiolo@nist.gov