

NIST Special Publication 800-157

Derived PIV Credentials

David Cooper

National Institute of Standards and Technology

October 30, 2014

13th Annual Smart Card Alliance Government Conference

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).
- Often impractical 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.