An Overview of Draft SP 800-157 *Derived PIV Credentials* and Draft NISTIR 7981 *Mobile, PIV, and Authentication*

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

IAB Meeting
March 26, 2014

Draft SP 800-157 – Derived PIV Credential for Mobile Devices

Scope:

- The Derived PIV Credential is an additional PIV Credential to satisfy HSPD-12’s ‘Common Identification‘ mandate
- Provide PIV-enabled authentication services on the mobile device to authenticate the mobile device owner to remote systems

FIPS 201-2 Authentication Mechanisms for PIV Card Credentials and Derived PIV Credentials

PIV Assurance Level Required by Application/ Resource	PACS	LACS Local Workstation Environment	LACS Remote/Network System Environment
LITTLE or NO confidence	VIS, CHUID	CHUID*	
SOME confidence	PKI-CAK, SYM-CAK	PKI-CAK	PKI-CAK,
HIGH confidence	BIO	BIO	**PKI-Derived**
VERY HIGH confidence	BIO-A, OCC-AUTH, PKI-AUTH	BIO-A, OCC-AUTH, PKI-AUTH	PKI-AUTH, **PKI-Derived**

Yellow font indicates the environments for the PIV Card Credentials and their authentication mechanisms. **Red** indicates the environments where the new "PKI-Derived" authentication mechanism for Mobile Devices applies.

Draft SP 800-157 – Derived PIV Credential for Mobile Devices

Motivation:

- PIV Cards have been geared towards traditional computing platforms (laptop, desktop)
- For newer computing devices (mobile devices), the use of the PIV Card for e-authentication is challenging and requires bulky add-on readers

Goal: To provide alternative approaches to PIV-enabled e-authentication with mobile device - without PIV Card and add-on readers.

Draft SP 800-157 – Derived PIV Credential for Mobile Devices

Goal (continued):

- While leveraging the PIV Infrastructure for:
  - Interoperability: Take advantage of the same PKI infrastructure
  - Cost-savings: Leverage the trust and identity-proofing performed for 5 million issued PIV cards via SP 800-63 concept of credential derivation

Draft SP 800-157 – Derived PIV Credential for Mobile Devices

Mobile devices and their capabilities vary by:

- Mobile device manufacturers, platforms, ports, Mobile Network Operators and have capabilities that are often different in focus (e.g., tablet vs smart phone).

- One technical approach is not sufficient to cover the various mobile devices deployed by USG.

- Draft SP 800-157 is flexible and offers a spectrum of approaches to electronic authentication on mobile devices.

Draft SP 800-157 – Derived PIV Credential for Mobile Devices

Integrated Security Tokens for Mobile Devices:

- Mobile Device Software tokens (current)
- MicroSD tokens (current)
- USB security tokens (near term)
- UICC tokens (near term)
- Embedded Hardware (near term)

Benefits:

- Derived PIV Credential - leverages identity proofing and vetting processes of PIV cardholder
- It's integrated -> better user experience

Considerations:

- Provisioning and management of mobile device specific credential
- Limited mobile OS and application support (MicroSD, USB, UICC)

Draft SP 800-157 – Derived PIV Credential for Mobile Devices

SP 800-157 defines a Derived PIV Credentials for the Security Tokens:

- Define the Derived PIV Credential (a PKI-based credential)
- Both LoA-3 (software) and LoA-4 (hardware) Derived PIV Credential are possible
- Key size and algorithm options are the same as for the PIV Authentication private key

- Removable security tokens (UICC, USB micro SD) have two defined interfaces for:
  - The application layer: the Derived PIV Application (an ISO/IEC 7816 APDU-based interface) and
  - The transportation layer, an interface to transfer APDU from token to mobile device (and vice versa)
- No interface requirements apply for embedded Security Tokens (software or hardware). These are are part of Mobile Device's hardware/OS/ software.

Draft SP 800-157 – Derived PIV Credential for Mobile Devices – Lifecycle Processes

Derivation & Initial issuance:

- Derivation of Derived PIV Credential is based on proof of possession of the PIV card
- Issuance of a LoA-4 credential is in person, while issuance of an LoA-3 allows for remote issuance

Maintenance (rekey and re-issuance):

- Remote rekey to a LoA-3 Derived PIV Credential token
- Remote rekey to a LoA-4 Derived PIV Credential token when rekeying to the same token
- Issuance of a Derived PIV Credential to a new (replacement) token can be done remotely for LoA-3 credential and in-person for an LoA-4 credential
- Derived PIV Credential is unaffected by loss, theft or damage to the Subscriber's PIV Card.

Termination:

- The subscriber is no longer eligible for a PIV Card or is no longer in need of a Derived PIV Credentials
- If token can be collected, then zeroize the private key or destroying the token. Otherwise, revoke the PIV Derived Authentication certificate.

Draft SP 800-157 – Derived PIV Credential for Mobile Devices

Draft SP 800-157 also includes:

- Technical requirements for:
  - Certificate Policy under which the Derived PIV Credential is issued (a ref)
  - How to include an optional Digital Signature Key and the Encryption Key in the Derived PIV Credential security token (Appendix A)

Draft SP 800-157 – Derived PIV Credential for Mobile Devices

Appendix C -- Derived PIV Credentials in Relation to OMB Memoranda

Credential Type	Token Type	PIV Assurance Level	Comparable OMB E-Auth Level	Target Guidance:	
				M-06-16/ M-07-16 for Separate Tokens	Future Alternate OMB Guidance for Integrated Tokens
PIV Derived Authentication certificate	MicroSD Token	Very High	4		✓
	USB Security Token	Very High	4	✓	
	Software Token	High	3		✓
	Embedded Hardware Token	Very High	4		✓
	UICC Token	Very High	4		✓
PIV Card's PIV Authentication certificate credential	**PIV Card** (via attached reader or NFC)	Very High	4	✓	

With integrated tokens, authentication factors are not provided by a separate token

"Future guidance will be made available by OMB to provide an alternative to the remote authentication policy in M-06-16 and M-07-16."

Draft NIST IR 7981
Mobile, PIV, and Authentication

A Companion Document to Draft SP 800-157

- Analyzes different approaches to PIV-enable mobile devices
  - Includes the use of PIV Cards with mobile devices in addition to Derived PIV Credentials
- Points out benefits and considerations (pros/cons) for each approach
  - Example: UICC approach requires cooperation with MNO
- Approximates when these approach might become available
  - Categorized approaches in ‘current’ and ‘near term’ solutions
- Includes Recommendations
  - Hardware rooted solutions provide better security
  - Software solution are available now – NIST IR 7981 recommends complementing these by hardware-backed mechanism to protect the private key of the Derived PIV Credential when not in use (the hybrid solution)
  - In the longer-term, NIST IR recommends adoption of hardware-supported security mechanisms in mobile devices, such as the Roots of Trust (SP 800-164) to support stronger assurance of identity

Mobile, PIV and Authentication

- **Both Draft SP 800-157 and NIST IR 7981 are available for public commenting**
- **Instructions to comment are provided at: http://csrc.nist.gov/groups/SNS/piv/announcements.html**

- **Public comment period closes April 21st**

What's Next?

- Resolve public comments and produce final SP 800-157 and final NIST IR 7981

- Draft SP 800-166 Derived PIV Credential Test Requirements for
  - Derived PIV Credential Data Model and Interface and
  - Portability: Removable security tokens ((USB, microSD, UICC) should be portable from one device to another.
  -

- Test Tool based on SP 800-166

- Setup Laboratory Accreditation program for vendor product testing

- SP 800-79-2 Guidelines for the Accreditation of PIV Card Issuers and Derived PIV Credential Issuers (under development)

The Author Team (from A to Z)

Draft SP 800-157:

- Bill Burr (william.burr@nist.gov)
- David Cooper (david.cooper@nist.gov)
- Hildegard Ferraiolo (hildegard.ferraiolo@nist.gov)
- Salvatore Francomacaro (salfra@nist.gov)
- Sarbari Gupta (sarbari@electrosoft-inc.com)
- Jason Mohler (jmohler@electrosoft-inc.com)
- Andrew Regenscheid (andrew.regenscheid@nist.gov)

Draft NIST IR 7981

- Bill Burr (william.burr@nist.gov)
- David Cooper (david.cooper@nist.gov)
- Hildegard Ferraiolo (hildegard.ferraiolo@nist.gov)
- Salvatore Francomacaro (salfra@nist.gov)
- Andrew Regenscheid (andrew.regenscheid@nist.gov)

"Thank you," Reviewers:

- Mobile Technology Tiger Team (MTTT)
- FICAM Logical Access Working Group (LAWG)
- Federal Chief Information Officer (CIO) Council
- Office of Management and Budget (OMB)

Thank you

Questions?

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