PIV Business Requirements Meeting: *Authenticators*

Andrew Regenscheid

Computer Security Division

NIST

National Institute of Standards and Technology

Technology Administration, U.S. Department of Commerce

Status Quo

PIV standards/guidelines and guiding policies recognize two authenticators:

- ***PIV Cards***
  - AAL3 (mostly)
  - *PIV Usage Guides:* https://piv.idmanagement.gov/
- ***Derived PIV Credentials***
  - Usually AAL2
  - By policy, limited to mobile devices where use of PIV cards is impractical
  - *NCCoE Derived PIV Practice Guide*: https://www.nccoe.nist.gov/projects/building-blocks/piv-credentials

Agency and Public Feedback

Calls for greater flexibility in selection and use of authenticators

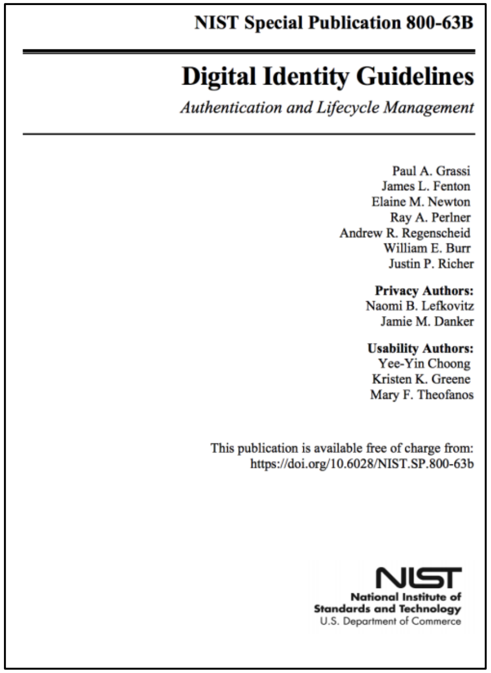
- Not all products and services can use PKI credentials natively
- Not all devices support PIV cards or have strong hardware/software/API support for PKI credentials
- Deployment of Derived PIV limited by the availability of commercial service providers

Draft OMB Identity Memo:
Update NIST SP 800-157, Guidelines for Derived PIV Credentials, to align with NIST SP 800-63 and develop a process to identify innovative technologies and authenticators (where applicable) that can leverage the PIV process for derived credentialing for logical and physical access;

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Proposed Changes in FIPS 201-3

- Broadly allow alternative authenticators to be derived from PIV credentials
  - Specify requirements in new Special Publication
  - **AAL2** and **AAL3**, based on Digital Identity Risk Management
  - Rely on SP 800-63B as the basis for security requirements
  - Facilitate interoperability through federation, not authenticator standards



NIST Special Publication 800-63B

Digital Identity Guidelines

Authentication and Lifecycle Management

Paul A. Grassi
James L. Fenton
Elaine M. Newton
Ray A. Perlner
Andrew R. Regenscheid
William E. Burr
Justin P. Richer

Privacy Authors:
Naomi B. Lefkovitz
Jamie M. Danker

Usability Authors:
Yee-Yin Choong
Kristen K. Greene
Mary F. Theofanos

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63b

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Considerations/Issues

- Authenticator Assurance Levels
- Product Validation
- Interoperability
- Authenticator Binding
- Revocation/Status Information

Authenticator Assurance Levels

	AAL2	AAL3
Types	Combinations providing multifactor authentication: OTP, Out-of-Band, Look-up Secrets, software crypto	Hardware cryptographic authenticators (multifactor authenticators or combinations)
Examples	Passwords with: • Push notifications, • OTP/SecureID • FIDO U2F Software-based Derived PIV	PIV cards* Hardware-based Derived PIV* FIDO with Token Binding + password
MitM Resist.	**Required**	**Required**
Verifier Impersonation Resist.	Not Required	**Required**
Verifier Compromise Resist.	Not Required	**Required**
Auth. Intent	Recommended	**Required**

What authenticators are suitable for government use?

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Product Validation

- We anticipate a need for some form of "Approved Products List" for alternative authenticators
  - Could leverage future SP 800-63 accreditation program(s) under consideration
  - Will consider existing industry-driven testing programs for suitability

- Agency *verification* of authenticator product validation is challenging in Bring-Your-Own-Authenticator scenarios
  - Limited technical solutions, such as attestation, practically available
  - May need to be addressed through policy or physical procedures

What are agency requirements for product validation?

Interoperability

- **Objectives**
  - Support interagency reuse and acceptance
  - Facilitate technical interoperability with applications
- Many non-PKI authenticators are for use with a single CSP/Verifier
  - Limits need for authenticator-based interoperability
- Shift interoperability focus to federation
  - Provides abstraction layer to support multiple authenticators
  - Can simplify authenticator management
- **WebAuthn/FIDO**
  - FIDO/WebAuthn guidance could promote security facilitate compatibility between gov't servers and industry authenticators

WebAuthn

Would this address agency interoperability needs?

Authenticator Binding

- SP 800-63-3 distinguishes different authenticator registration processes:
  - Registration at new CSPs involves a proofing process
  - Registration as existing CSP is post-enrollment binding
- Typical use-case involves binding additional authenticators as derived credentials
  - Under SP 800-63B, this can be done remotely a user-authenticated session without impacting IAL/AAL
  - Under current SP 800-157, LoA-4 requires in-person registration
- Will address derived credentialing and authenticator binding with new technical guidelines based on SP 800-63-3 and SP 800-157
- ***Threat:*** Binding derived credentials with stolen authenticators

Can the risks of remote registration of authenticators be effectively managed at all levels?

Revocation/Status Information

- Non-PKI authenticators lack centralized revocation capabilities (e.g., no CRLs)
  - Challenge handling lost/stolen authenticators
  - No way to communicate employee status information through use of the authenticator
- Federated architectures could provide timely status information

What are agency needs/concerns regarding revocation and employee status information?

Discussion Topics

- What assurance levels and authenticator types are appropriate for government use?
  - e.g., restricted authenticators, like SMS-based OTP
- What are agency requirements for authenticator product validation programs?
- Will the proposed plan address interoperability need?
- Can the risks of remote registration of authenticators be effectively managed at all levels?
- What are agency needs/concerns regarding revocation and employee status information?

Questions?

NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
UNITED STATES DEPARTMENT OF COMMERCE
100 Bureau Drive

Contact Information

PIV PoC:

Hildegard Ferraiolo
PIV Program Manager
hildegard.ferraiolo@nist.gov

Andrew Regenscheid
Andrew.Regenscheid@nist.gov