Best Practices for Privileged User PIV Authentication

Hildegard Ferraiolo

PIV Project Manager

NIST ITL - Computer Security Division

hildegard.ferraiolo@nist.gov

Federal Computer Security Managers' Meeting

April 21, 2016

Drivers

Spring Effort of Summer 2015

- focused on enhancing cybersecurity of Federal information and assets
- Multi-faceted: comprehensive review of the Federal Government’s cybersecurity policies, procedures, and practices
- included effort to accelerate 2 factor authentication with the PIV Credentials for privileged user access

M-16-04 - *The Cybersecurity Strategy and Implementation Plan*, October 30, 2015

- incorporates findings/reviews by Sprint team
- identifies critical cybersecurity gaps and emerging priorities,
- make specific recommendations to address those gaps and priorities.

- directs NIST to publish best practices for privileged user access with PIV Credentials

Overview of:

NIST's Best Practices for Privileged User PIV Authentication

NIST's Best Practices for Privileged User PIV Authentication

Preface: Limitations of Password-Based Single-Factor Authentication

- Password are vulnerable to capture, guessing, offline cracking attacks

The Need to Strengthen Authentication for Privileged Users

- Benefit of Multi-Factor Authentication Using PIV Credentials
  - Something you have (PIV Credential) + something you KNOW and/or ARE
  - mitigates weaknesses of password attacks, especially replay attacks
  - High identity assurance

NIST's Best Practices for Privileged User PIV Authentication (continued)

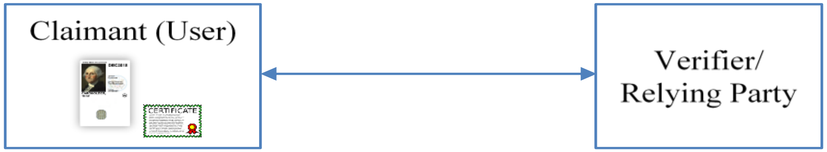
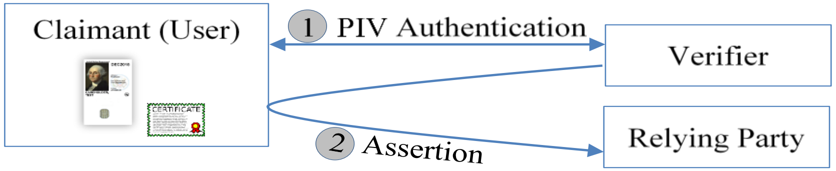
General Best Practices

- Minimize Privileged Access
- Issue Dedicated Endpoint Devices for Privileged Use
- Integrate LOA-3 and 4 Privileged Authentication Requirements into an Overall Risk-Based Approach

*LoA-4 and 3 are the goal for Privileged Access.

NIST’s Best Practices for Privileged User PIV Authentication (continued)

Selecting the appropriate PIV Authentication Architecture:

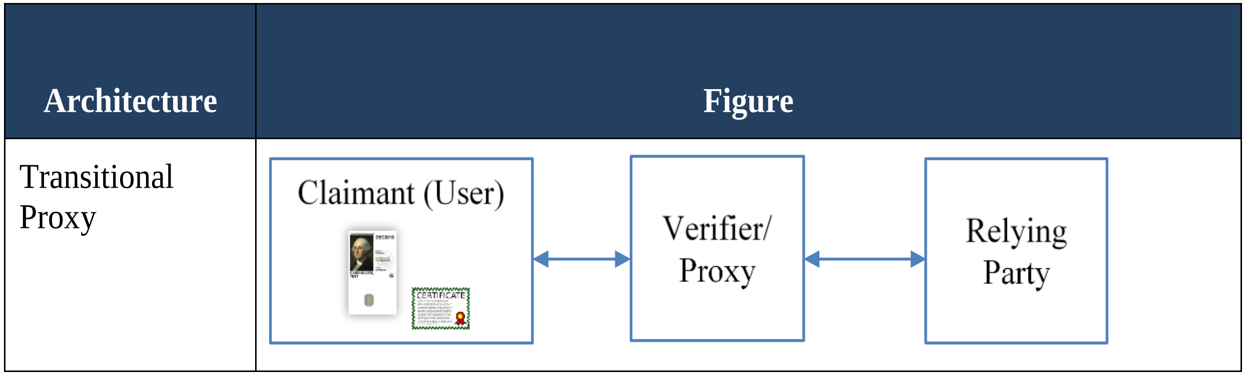
Architecture	Figure
Direct Verification	 Claimant (User) Verifier/ Relying Party
Indirect Verification	 Claimant (User) 1 PIV Authentication Verifier 2 Assertion Relying Party

Examples:

- Direct model: TLS client/ AuthN with PIV PKI Credential (achieves LoA-4)
- Indirect model: PIV PKI credential AuthN -> Kerberos (achieves LoA-4)
PIV PKI credential AuthN -> Assertion (achieves LoA-3 or 4)

NIST's Best Practices for Privileged User PIV Authentication (continued)

Selecting the appropriate PIV Authentication Architecture



Architecture	Figure
Transitional Proxy	Claimant (User) ↔ Verifier/ Proxy ↔ Relying Party

Figure 1: High-Level Transitional Proxy Architecture

Examples:

PIV PKI credential AuthN -> protected (Username/password)

- achieves LoA-2

The PROXY Model is a TRANSITIONAL ARCHITECURE used while transitioning to LoA-4 or LoA-3 direct or indirect models via POA&M..

Addressed: Major Comments on the Draft version

175 comments from 21 email submissions:

- Dedicated devices is not enough -- need dedicated credentials as well.
- Cost is too much to have dedicated devices.
- Need more product-specific guidelines.
- Proxy architecture should be permanent and not transitional.
- Derived PIV Credential should not be allowed to access privileged accounts.
- POA&M end date should be specified.

Next Steps…

- Work with FICAM to aid with the Playbooks

Resources

- **Best Practices for Privileged User PIV Authentication, April 21, 2016** http://csrc.nist.gov/publications/papers/2016/best-practices-privileged-user-piv-authentication.pdf

- **M-16-04 - *The Cybersecurity Strategy and Implementation Plan*, October 30, 2015** **https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf**

Questions?

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