

# The December CDM Webinar

## We will begin at 12:00PM EST

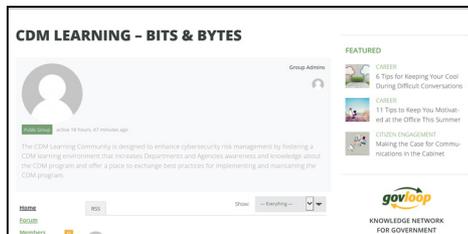
# Welcome to the CDM Webinar: Best Practices for Privileged User PIV Authentication: Getting Ready for PRIVMGMT

While you wait, check out:



## Our CDM Homepage

<https://www.us-cert.gov/cdm/training>



## Our CDM Bits and Bytes Blog

<https://www.govloop.com/groups/cdm-learning-bits-bytes/>

*Have a topic suggestion for a future event or blog post? Want to join our membership list? Please reach out to [cdmlearning@hq.dhs.gov](mailto:cdmlearning@hq.dhs.gov)*



Homeland  
Security

Federal Network Resilience

# Best Practices for Privileged User PIV Authentication: Getting Ready for PRIVMGMT

December 8, 2016

12:00 – 1:00 PM EST

A CDM Learning Webinar



Homeland  
Security

Federal Network Resilience

# Hildegard (Hildy) Ferraiolo

## Computer Scientist, NIST



- Lead for PIV Program activities
- Coordinator for PIV-related activities with the HSPD-12 Support Team, the FICAM Test Program, and the Government Smart Cards-Interagency Advisory Board
- Co-authored and developed several NIST publications in the FIPS 201 standard suite
- Launched the NIST Personal Identity Verification test program (NPIVP)



# Best Practices for Privileged User PIV Authentication

---

## Today's Topics

- History/Drivers for PIV authentication
- Best Practices Overview
- All about LOAs
- Examples and Concerns



# Best Practices for Privileged User PIV Authentication

**Hildegard Ferraiolo**

**PIV Project Manager**

**NIST ITL - Computer Security Division**

**[hildegard.ferraiolo@nist.gov](mailto:hildegard.ferraiolo@nist.gov)**

CDM December Webinar

December 8, 2016

# Drivers

## Sprint Effort of Summer 2015

- 30 day++ initiative by the FCIO and led by OMB
- Focused on enhancing cybersecurity of Federal information and assets in 5 key areas
- Multi-faceted: comprehensive review of the Federal Government's cybersecurity policies, procedures, and practices
- Included effort to accelerate 2 factor authentication with PIV Credentials for privileged user access

## **M-16-04 - *The Cybersecurity Strategy and Implementation Plan (CSIP)*, October 30, 2015**

- Incorporates findings/reviews by the Sprint Effort
- Identified 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**
- Directed DHS to accelerate the deployment of Continuous Diagnostics and Mitigation (CDM) and EINSTEIN capabilities to all participating Federal agencies to enhance detection of cyber vulnerabilities and protection from cyber threats

**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)

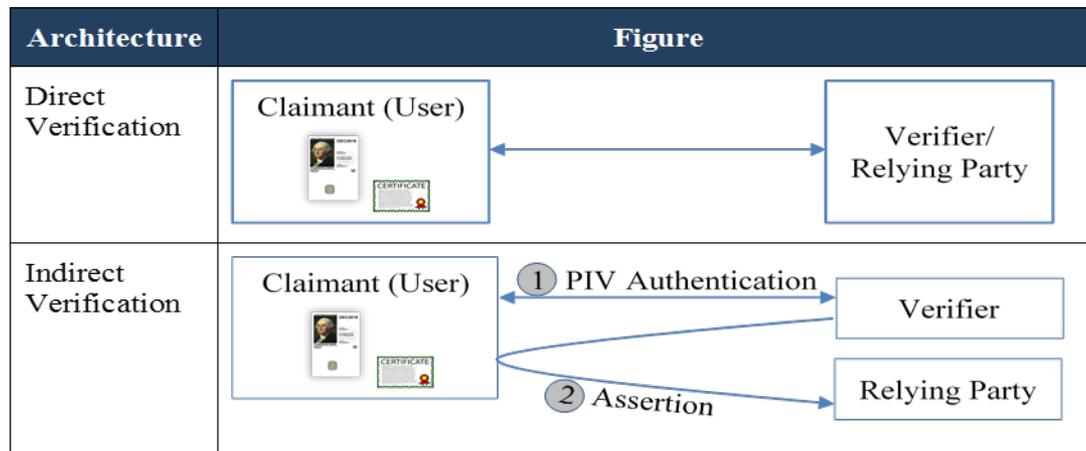
## General Best Practices

- 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:



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

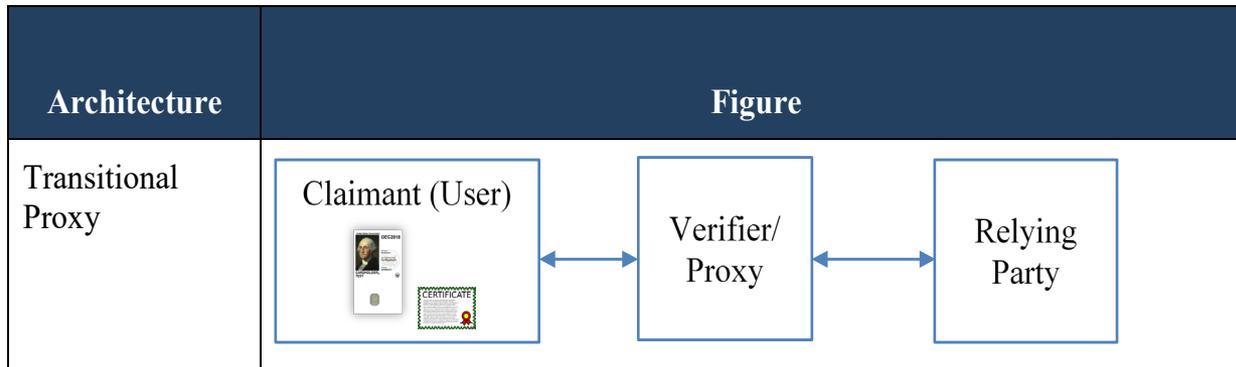


Figure 1: High-Level Transitional Proxy Architecture

### Examples:

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

- achieves LoA-2

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

# Resources:

- Best Practices for Privileged User PIV Authentication
  - <http://csrc.nist.gov/publications/papers/2016/best-practices-privileged-user-piv-authentication.pdf>
- M-16-04 - Cybersecurity Strategy and Implementation Plan (CSIP) for Federal Civilian Government
  - <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf>

# Questions and Answers

***What is the impact of ...??***

***What about ....??***

***How did the stakeholders adjust to ....??***

***What would you do differently about ....??***

***What should I do about ....??***

***What would you recommend for ....??***

***How much time did it take to ....??***

***How are you maintaining 95% compliance with CSM CAP....??***

***How did you handle ... (latency, centralization, control issues, etc.) ??***



# The CDM Learning Program

## CDM Learning Program

- Monthly Learning Community Event (CDM-LCE)
- Monthly Webinars
- Weekly CDM Bits & Bytes
- Online Vignettes

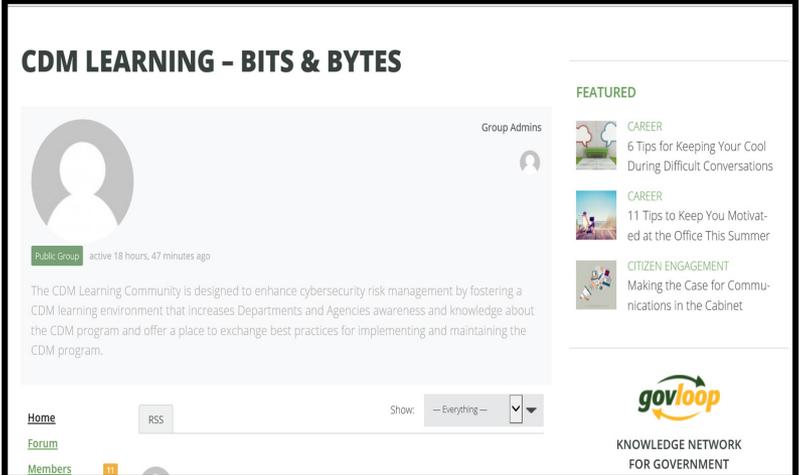
Resources Available:

<https://www.us-cert.gov/cdm>

Sign up to receive event  
information:

[cdmlearning@hq.dhs.gov](mailto:cdmlearning@hq.dhs.gov)

Sign up for the CDM learning blog:  
<https://www.govloop.com/groups/cdm-learning-bits-bytes>



The screenshot shows the 'CDM LEARNING - BITS & BYTES' group page on Govloop. The page features a profile picture placeholder, a 'Public Group' label, and a description: 'The CDM Learning Community is designed to enhance cybersecurity risk management by fostering a CDM learning environment that increases Departments and Agencies awareness and knowledge about the CDM program and offer a place to exchange best practices for implementing and maintaining the CDM program.' The page also includes a 'FEATURED' section with three articles: '6 Tips for Keeping Your Cool During Difficult Conversations', '11 Tips to Keep You Motivated at the Office This Summer', and 'Making the Case for Communications in the Cabinet'. The Govloop logo and 'KNOWLEDGE NETWORK FOR GOVERNMENT' tagline are visible in the bottom right corner.

# Event Conclusion

---

Thank you for attending today's  
CDM Webinar!

- A certificate of attendance will be available to download on the CDM Learning Program website at [www.us-cert.gov/cdm/training](http://www.us-cert.gov/cdm/training), within one week of today's event
- Visit our website to learn more about the CDM Learning Program and upcoming events at [www.us-cert.gov/cdm](http://www.us-cert.gov/cdm)
- For any questions, comments, or suggestions for future topics, please email us at [cdmlearning@hq.dhs.gov](mailto:cdmlearning@hq.dhs.gov)

