National Cybersecurity Center of Excellence

Increasing the adoption of standards-based cybersecurity technologies

Derived PIV Credentials COI Call

August 16, 2018

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Agenda

- **Practice Guide, 2nd draft of NIST SP 1800-12 Derived PIV Credentials**
  - Posted on August 2, 2018; Public comments welcomed through October 1, 2018
  - Refresher on contents of the practice guide
  - Review of architectures documented in the practice guide
- **Collaborators**
  - Reflections on collaboration and publication of the practice guide
  - Reflections on derived PIV credential customer requirements and needs
- **Future Directions**

Mission

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

Engagement & Business Model

DEFINE

OUTCOME:
Define a scope of work with industry to solve a pressing cybersecurity challenge

ASSEMBLE

OUTCOME:
Assemble teams of industry orgs, govt agencies, and academic institutions to address all aspects of the cybersecurity challenge

BUILD

OUTCOME:
Build a practical, usable, repeatable implementation to address the cybersecurity challenge

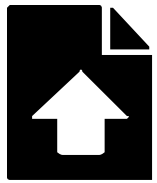
ADVOCATE

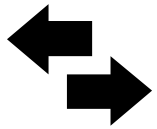
OUTCOME:
Advocate adoption of the example implementation using the practice guide

Engagement & Business Model

ADVOCATE

OUTCOME:
Advocate adoption of the example implementation using the easy-to-understand practice guide





1. Publish SP 1800

- SP 1800 Practice Guides are free publications that encourage and instruct businesses to adapt the example implementation to their own environment
- Available for download at https://nccoe.nist.gov, practice guides include three volumes of varying technical complexity

2. Engage industry and seek feedback

- Each draft practice guide has a public comment period
- Comments are reviewed and incorporated into final SP 1800 Practice Guide publication

3. Encourage adoption of secure technologies

- Through outreach and engagement with industry, demonstrate how the example implementation can help solve the cybersecurity challenge

SP 1800 Series: Cybersecurity Practice Guides

Volume A: Executive Summary

- High-level overview of the project, including summaries of the challenge, solution, and benefits

Volume B: Approach, Architecture, and Security Characteristics

- Deep dive into challenge and solution, including approach, architecture, and security mapping to the Cybersecurity Framework and other relevant standards

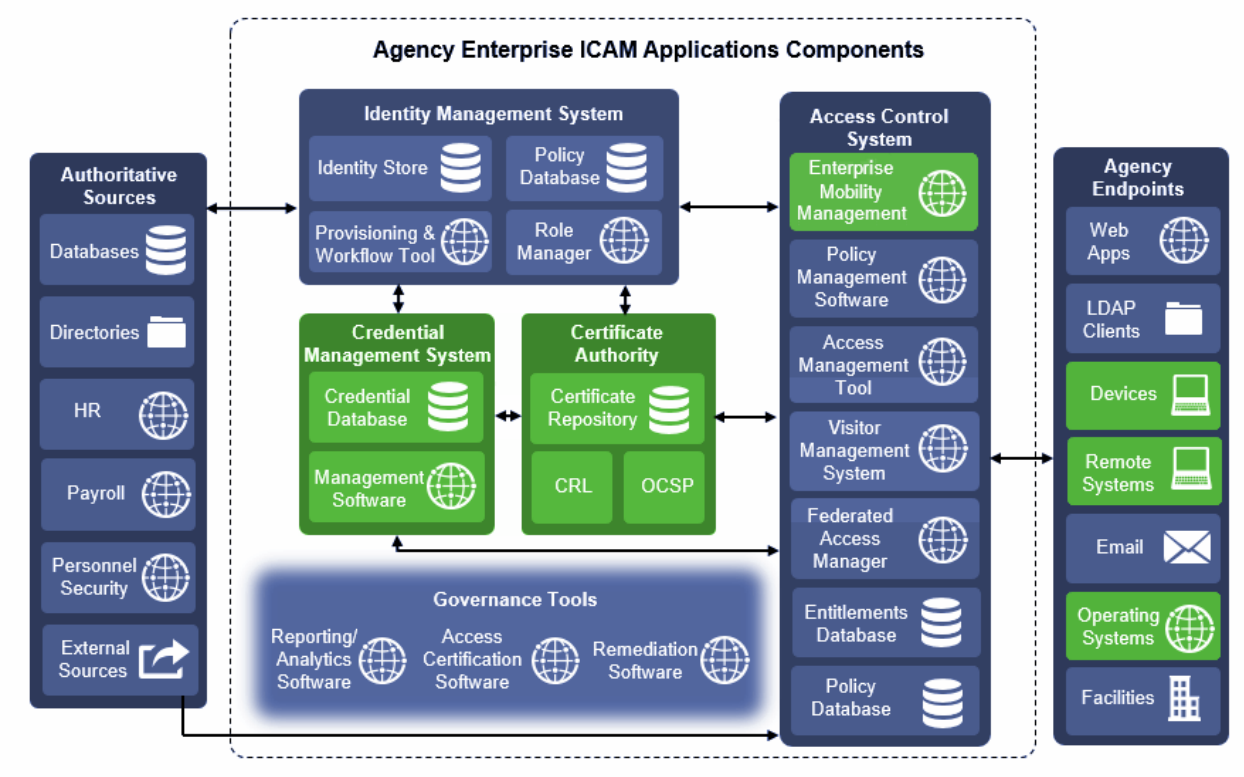
Volume C: How-To Guide

- Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance

Cybersecurity Framework Function	Cybersecurity Framework Category	Cybersecurity Framework Subcategory	NIST SP 800-53 Rev. 4	NIST SP 800-181 Work Roles
PROTECT (PR)	Access Control (PR.AC)	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	IA-2, IA-4, IA-5, AC-2	Software Developer SP-DEV-001), Product Support Manager (OV-PMA-003)
		PR.AC-3: Remote access is managed.	AC-17, AC-19	Information Systems Security Developer (SP-SYS-001), System Administrator (OM-ADM-001)
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	AC-2, AC-19, IA-2, IA-4, IA-5, IA-8	Security Control Assessor (SP-RSK-002), Product Support Manager (OV-PMA-003)
	Data Security (PR.DS)	**PR.DS-2:** Data in transit is protected	SC-8, SC-12	Data Analyst (OM-DTA-002), Cyber Defense Analyst (PR-CDA-001)
		PR.DS-5: Protections against data leaks are implemented	SC-13	Research and Development Specialist (SP-TRD-001), Cyber Defense Analyst (PR-CDA-001)
	Information Protection (PR.IP)	**PR.IP-3:** Configuration change control processes are in place	CM-3	Software Developer (SP-DEV-001), Systems Security Analyst (OM-ANA-001)

Foundational Artifacts

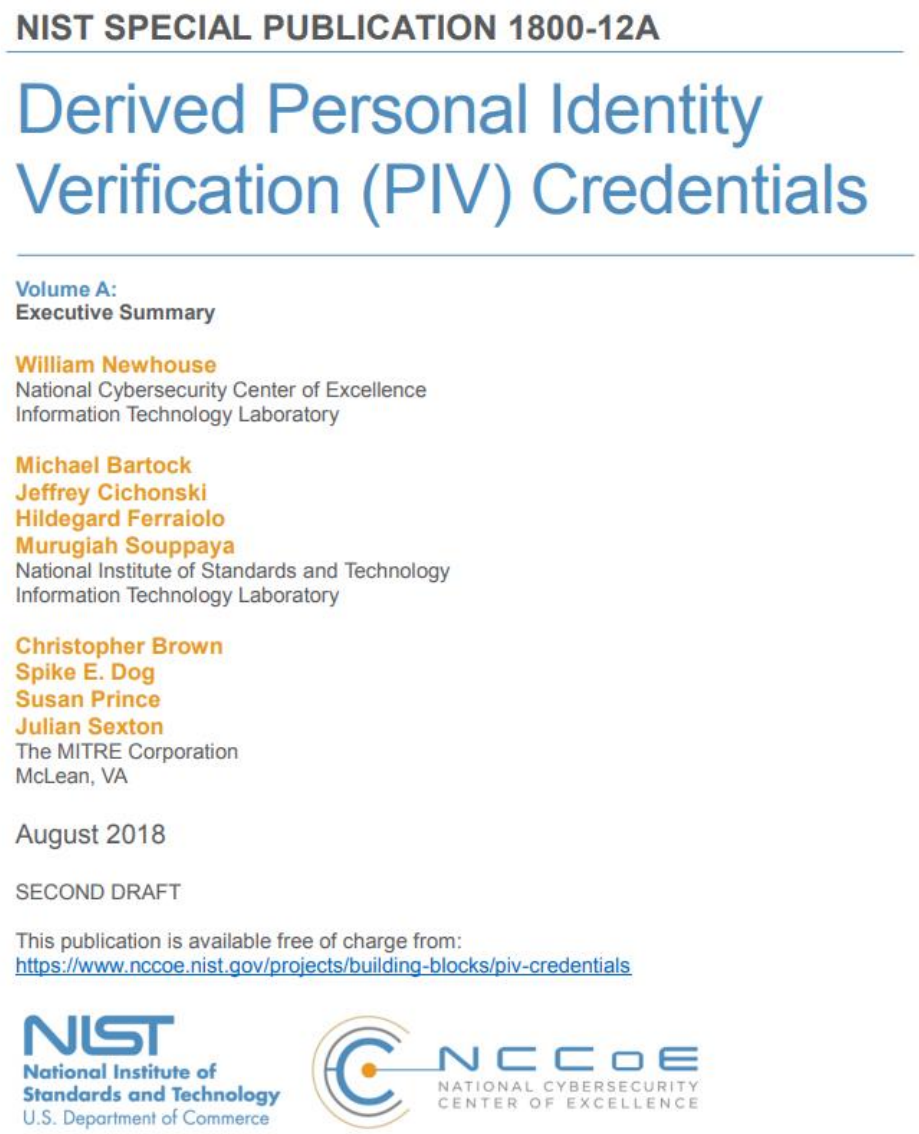
- NIST Special Publication 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials
- Federal ICAM Enterprise Architecture



Part A

The NCCoE sought existing technologies that provided the following capabilities:

- authenticate users of mobile devices by using secure cryptographic authentication exchanges
- provide a feasible security platform based on Federal Digital Identity Guidelines
- utilize a public key infrastructure (PKI) with credentials derived from a PIV Card
- support operations in PIV, PIV-interoperable (PIV-I), and PIV-compatible (PIV-C) environments
- issue PKI-based DPC at Level of Assurance 3 (AAL-2)
- provide logical access to remote resources hosted in either a data center or the cloud



NIST SPECIAL PUBLICATION 1800-12A

Derived Personal Identity Verification (PIV) Credentials

Volume A:
Executive Summary

William Newhouse
National Cybersecurity Center of Excellence
Information Technology Laboratory

Michael Bartock
Jeffrey Cichonski
Hildegard Ferraiolo
Murugiah Souppaya
National Institute of Standards and Technology
Information Technology Laboratory

Christopher Brown
Spike E. Dog
Susan Prince
Julian Sexton
The MITRE Corporation
McLean, VA

August 2018

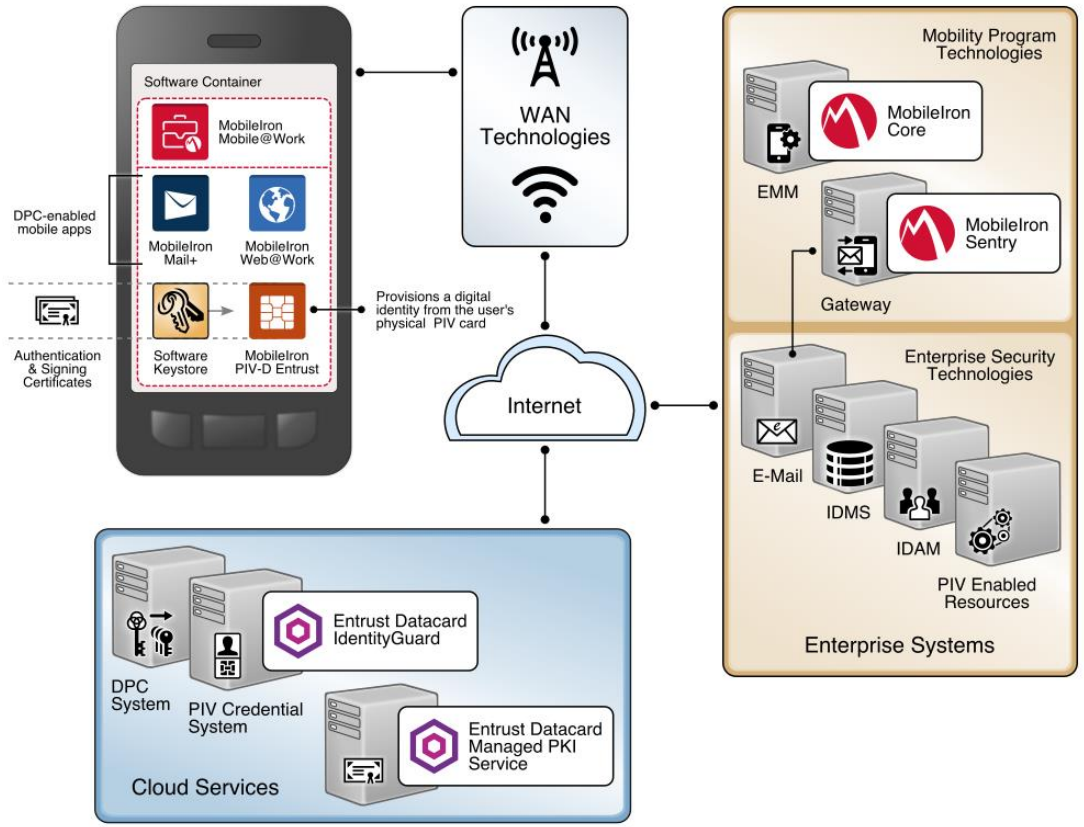
SECOND DRAFT

This publication is available free of charge from:
https://www.nccoe.nist.gov/projects/building-blocks/piv-credentials

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Part B



NIST SPECIAL PUBLICATION 1800-12B

Derived Personal Identity Verification (PIV) Credentials

Volume B:
Approach, Architecture, and Security Characteristics

William Newhouse
National Cybersecurity Center of Excellence
Information Technology Laboratory

Michael Bartock
Jeffrey Cichonski
Hildegard Ferraiolo
Murugiah Souppaya
National Institute of Standards and Technology
Information Technology Laboratory

Christopher Brown
Spike E. Dog
Susan Prince
Julian Sexton
The MITRE Corporation
McLean, VA

August 2018

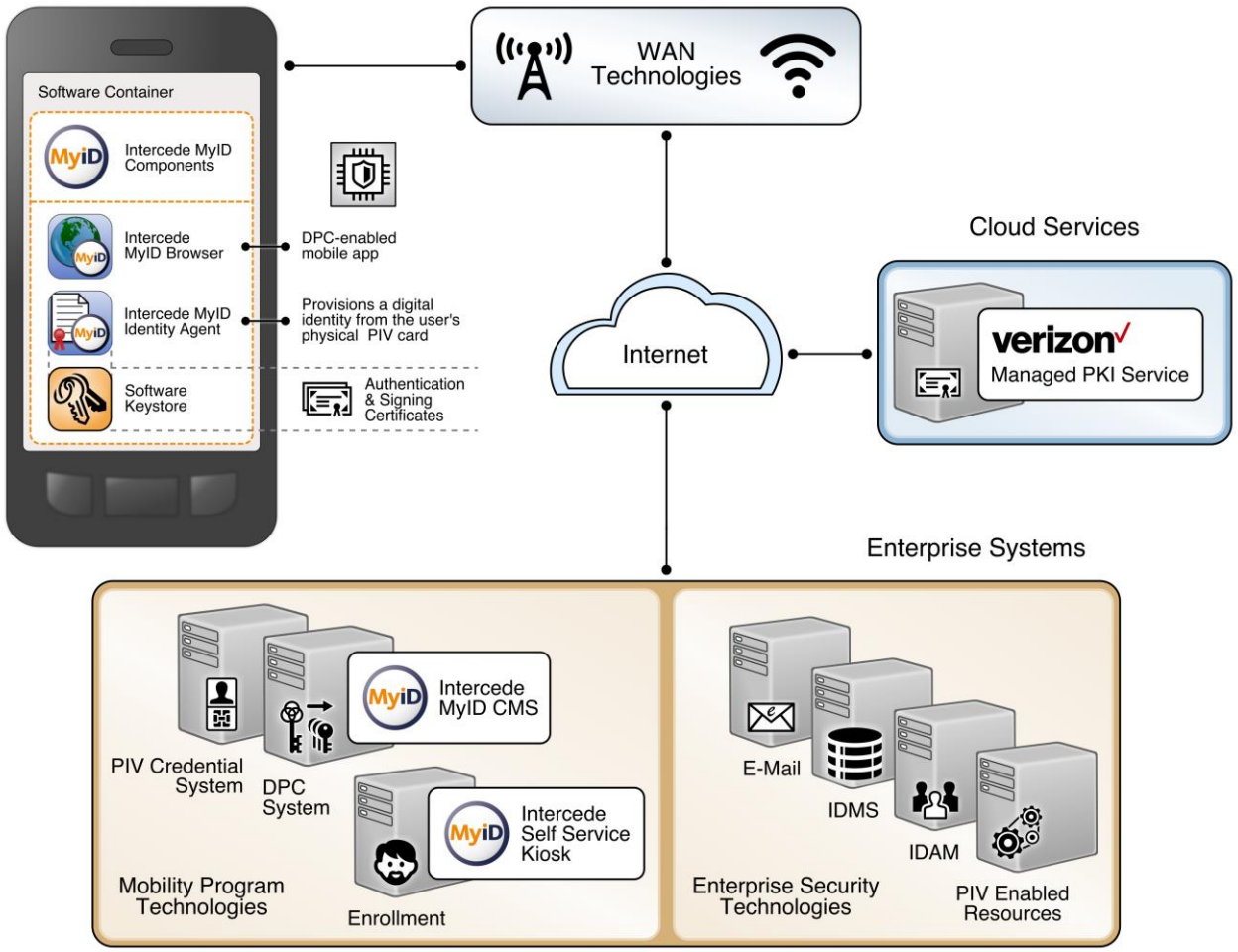
SECOND DRAFT

This publication is available free of charge from:
https://www.nccoe.nist.gov/projects/building-blocks/piv-credentials

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Part B



NIST SPECIAL PUBLICATION 1800-12B

Derived Personal Identity Verification (PIV) Credentials

Volume B:
Approach, Architecture, and Security Characteristics

William Newhouse
National Cybersecurity Center of Excellence
Information Technology Laboratory

Michael Bartock
Jeffrey Cichonski
Hildegard Ferraiolo
Murugiah Souppaya
National Institute of Standards and Technology
Information Technology Laboratory

Christopher Brown
Spike E. Dog
Susan Prince
Julian Sexton
The MITRE Corporation
McLean, VA

August 2018

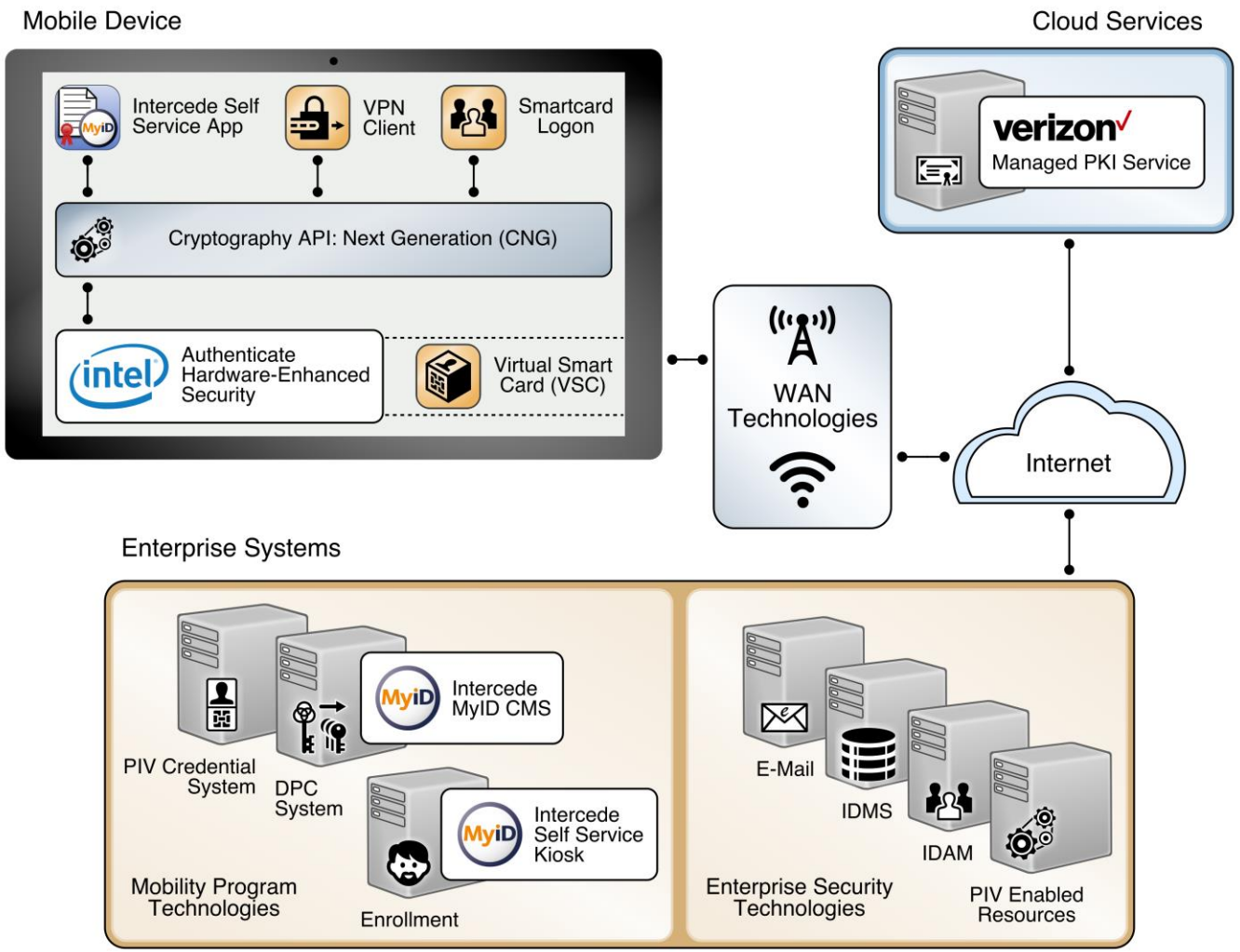
SECOND DRAFT

This publication is available free of charge from:
https://www.nccoe.nist.gov/projects/building-blocks/piv-credentials

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Part B



NIST SPECIAL PUBLICATION 1800-12B

Derived Personal Identity Verification (PIV) Credentials

Volume B:
Approach, Architecture, and Security Characteristics

William Newhouse
National Cybersecurity Center of Excellence
Information Technology Laboratory

Michael Bartock
Jeffrey Cichonski
Hildegard Ferraiolo
Murugiah Souppaya
National Institute of Standards and Technology
Information Technology Laboratory

Christopher Brown
Spike E. Dog
Susan Prince
Julian Sexton
The MITRE Corporation
McLean, VA

August 2018

SECOND DRAFT

This publication is available free of charge from:
https://www.nccoe.nist.gov/projects/building-blocks/piv-credentials

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Part C

Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance

NIST SPECIAL PUBLICATION 1800-12C

Derived Personal Identity Verification (PIV) Credentials

Volume C:
How-To Guides

William Newhouse
National Cybersecurity Center of Excellence
Information Technology Laboratory

Michael Bartock
Jeffrey Cichonski
Hildegard Ferraiolo
Murugiah Souppaya
National Institute of Standards and Technology
Information Technology Laboratory

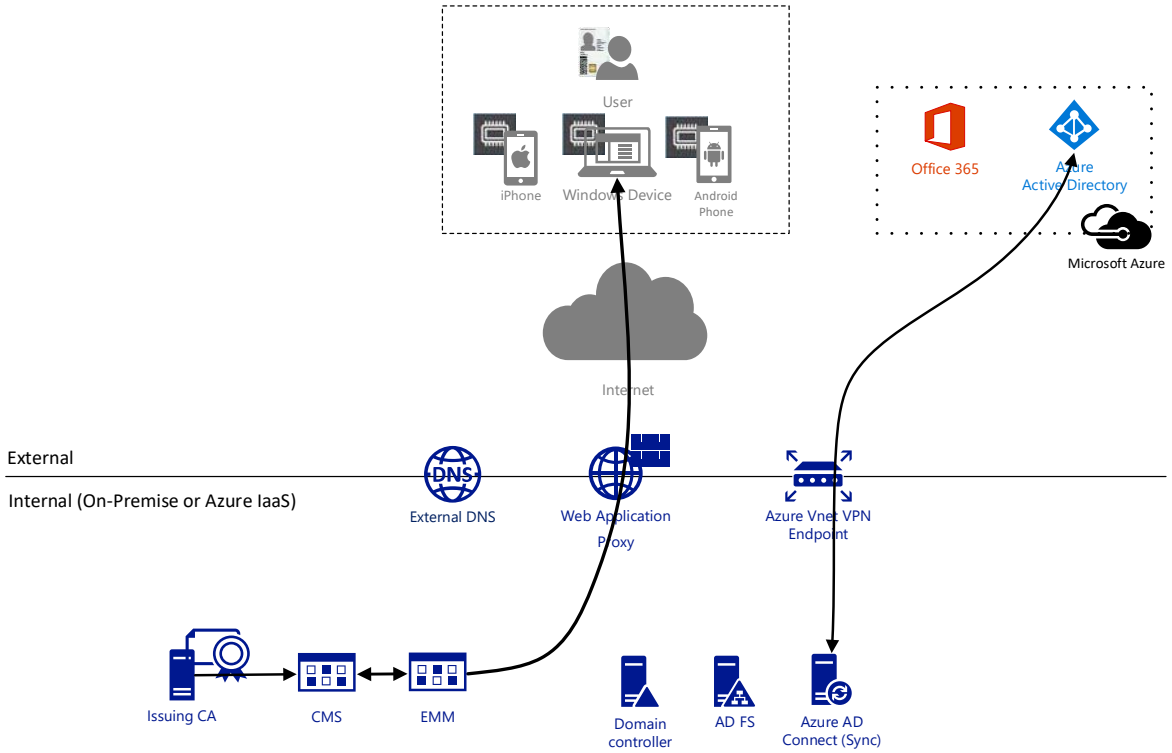
Christopher Brown
Spike E. Dog
Susan Prince
Julian Sexton
The MITRE Corporation
McLean, VA

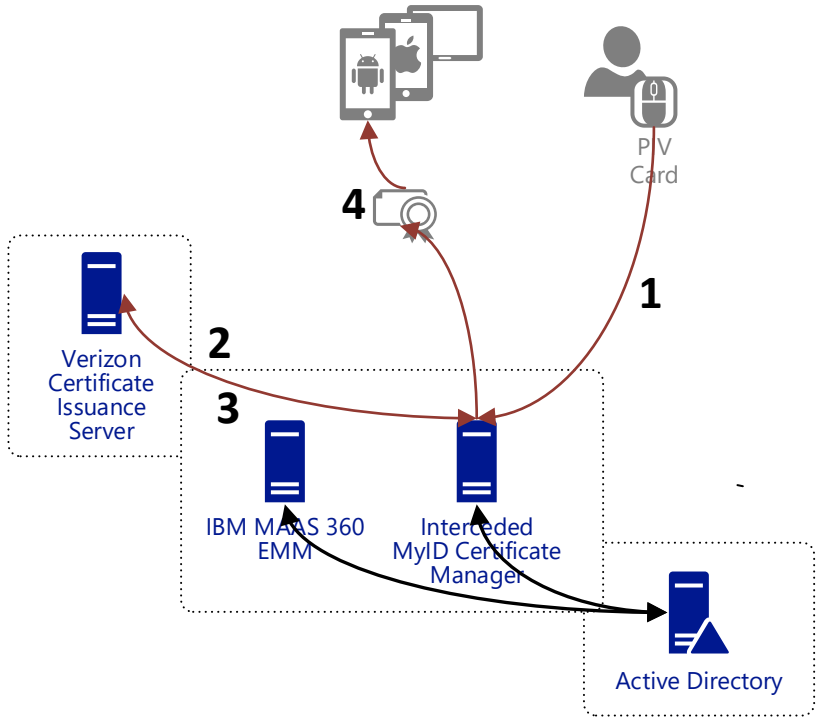
August 2018

SECOND DRAFT

This publication is available free of charge from:
https://www.nccoe.nist.gov/projects/building-blocks/piv-credentials

NIST DPC Activity





Q & A

- **Second Draft**
- **Future Directions**
  - Architecture expansion
    - Mobile Device Management
  - Application Enablement
  - Strengthening the Cybersecurity of Federal Agencies through Improved Identity, Credential, and Access Management (OMB Draft April 6, 2018 https://policy.cio.gov/identity-draft/)
  - Digital Signature and Key Management Keys
  - Identification of Practical Authenticator Assurance Level 3 (AAL3) Use Cases for Mobile Devices

Questions?

Bill Newhouse, Principle Investigator

bill.newhouse@nist.gov

301.975.0232

https://www.nccoe.nist.gov/projects/building-blocks/piv-credentials

http://nccoe.nist.gov

301-975-0200

nccoe@nist.gov