Microsoft

intercede

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

Derived PIV Credentials Proof of Concept Research

Hildegard Ferraiolo
Senior Computer Scientist
NIST

Jeffrey Cichonski
IT Specialist (Security)
NIST

Paul Fox
Architect
Microsoft

Ryan Holley
Sales Engineer
Intercede

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Agenda

- SP 800-157
- NIST IR 8055 Overview
- Proof of Concept Research

An Overview of
SP 800-157
Derived PIV Credentials

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

The 2015 Cybersecurity Innovation Forum
Walter E. Washington Convention Center, Washington D.C.
September 9th, 2015

Derived PIV Credentials for Mobile Devices

Challenge to Address:

For newer computing devices (mobile devices), the use of the PIV Card for e-authentication is challenging and requires bulky add-on readers

SP 800-157 Goal:

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

What is a Derived PIV Credential?

- An X.509 public key certificate (and associated public/private keys) – similar to the PIV Authentication certificate
- Two options for assurance level of certificate (e-Authentication Assurance Level 3 or 4)

Why Only PKI?

- Interoperability
  - OMB M-11-11: “Agency processes must accept and electronically verify PIV credentials issued by other federal agencies.”
  - Leverages current work to PIV-enable relying party systems.
- Efficiency: PKI is already in place.

Derived? Derived From What?

- General Concept of Derived Credential
  - Specified in SP 800-63-2
  - A credential issued based on proof of possession and control of a token associated with a previously issued credential, so as not to duplicate the identity proofing process.
- Profiled to **PIV** - The Derived **PIV** Credential (SP 800-157)
  - A PIV credential for use with mobile devices that is issued in accordance with SP 800-157 based on proof of possession and control of a PIV Card.

Where does the Derived PIV Credential Reside?

Embedded Security Tokens on Mobile Devices:

- Mobile Device Software tokens (example keystore)
- Embedded Hardware (example TPM)

Removable Security Tokens on Mobile Devices:

- MicroSD tokens (current)
- USB security tokens (near term)
- UICC tokens (near term)

Considerations:

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

Why so Many Options?

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 token type is not sufficient to cover the various mobile devices deployed by USG.

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

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
- 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
- Subscriber does not need a Derived PIV Credential anymore
- If token can be collected, then zeroize the private key or destroying the token. Otherwise, revoke the PIV Derived Authentication certificate.

What About Secure Email?

- Scope of SP 800-157 is limited to issuing an authentication certificate (the Derived PIV Credential). However:
  - Appendix A (informative) notes that mobile device may have its own digital signature key/certificate. Key management key from PIV Card may be stored on mobile device.
  - Appendix B.1 (data model for card application for removable tokens) includes containers for digital signature and key management keys/certificates.

Thank you, Contributors!

Reviewers:

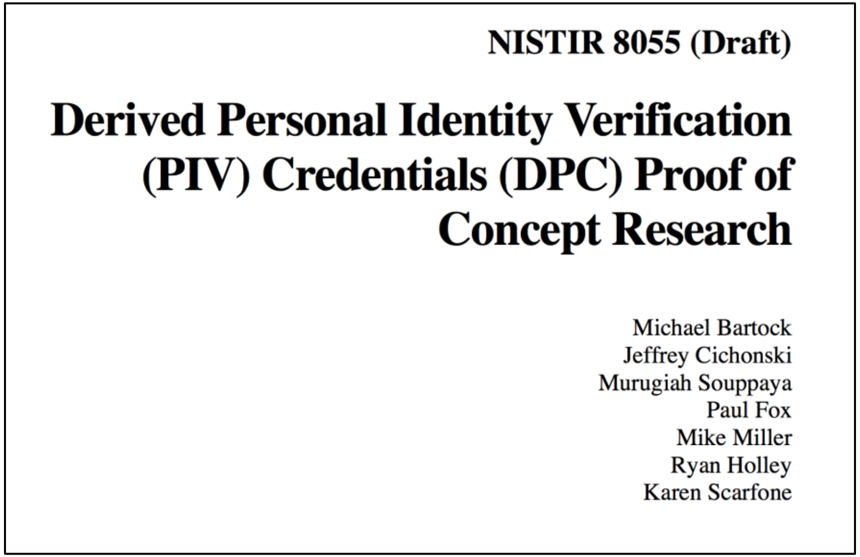
- Mobile Technology Tiger Team (MTTT)
- FICAM Logical Access Working Group (LAWG)
- Federal Chief Information Officer (CIO) Council
- Office of Management and Budget (OMB)

Commenters:

- Directive Health,FICAM, Exponent, Bancgroup, ICAMSC, Norka Tech, Security Architectures, USAF, Certipath, Emergent LLC, Venkat Sundaram, DHS, Apple, G&D, Microsoft, Wave, NASA, Smart Card Alliance, SSA, DoS, Gemalto, Treasury, USDA, Secure Access Technologies 42Tech Inc, DoJ, CPWG Precise Biometric, Intercede, NSA, Oberthur, Tyfone, Inc, CDC, Pomcor, BAH, PrimeKeye, Global Platform,

NIST IR 8055

- Published NIST Interagency report documenting findings implementing a derived PIV credential solution



NISTIR 8055 (Draft)

Derived Personal Identity Verification (PIV) Credentials (DPC) Proof of Concept Research

Michael Bartock
Jeffrey Cichonski
Murugiah Souppaya
Paul Fox
Mike Miller
Ryan Holley
Karen Scarfone

Objective of Research

- Implement derived PIV credential solution that meets SP 800-157 requirements
- Leverage existing PKI infrastructure
- Modern client devices do not support smart card form factor but provide embedded hardware or software token

Scope of Research

- Remote issuance of LOA 3 credentials
- Use derived PIV credentials to:
  - Access to remote resources hosted within an on-premises data center or in a public cloud
  - Sign email on the mobile device

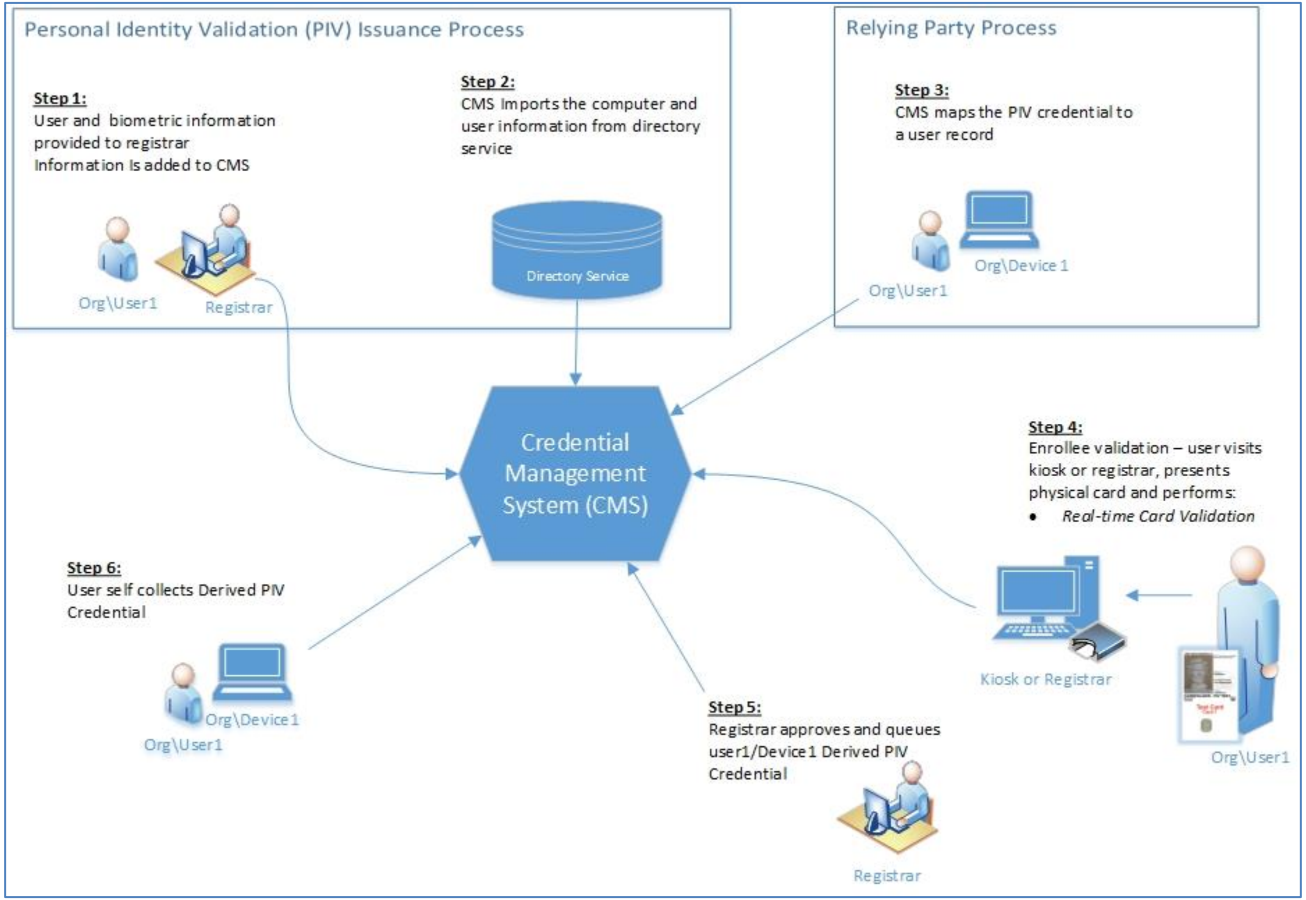
General Requirements

- Private cryptographic key stored in hardware or software cryptographic module
- The ability to issue credentials of SP 800-63 Level of Assurance 3 (LOA-3) with remote enrollment
- Enrollee’s proof of possession of a valid PIV Card to receive a Derived PIV Credential
- The derived credential certificate must be an x509 public key certificate meeting the requirements of the Federal PKI Common Policy Framework

Usage Scenarios

1. Organization provisions PIV cards internally using a card management system (CMS) and internal PKI
   - Capable of supporting the issuance, maintenance, use, and termination of derived PIV X.509-based credentials
2. Shared Provider’s Provisioned PIV cards

Enrollment and Issuance Workflow



Step 1:
User and biometric information provided to registrar
Information Is added to CMS

Step 2:
CMS Imports the computer and user information from directory service

Step 3:
CMS maps the PIV credential to a user record

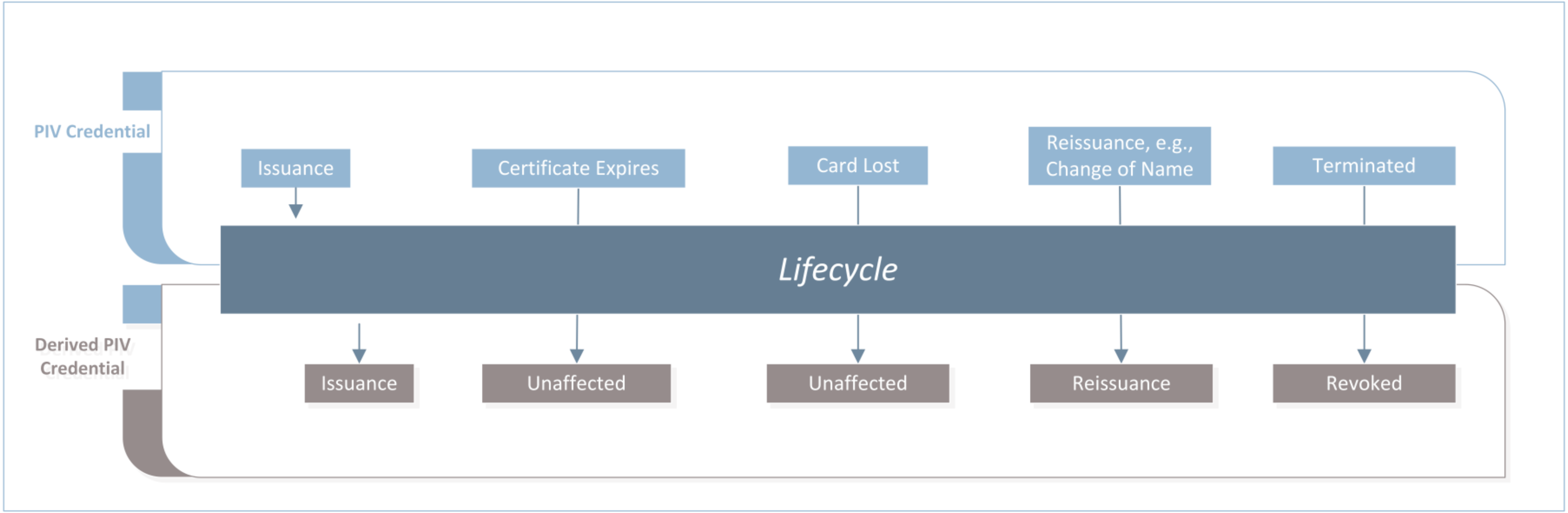
Step 4:
Enrollee validation – user visits kiosk or registrar, presents physical card and performs:

- *Real-time Card Validation*

Step 5:
Registrar approves and queues user1/Device1 Derived PIV Credential

Step 6:
User self collects Derived PIV Credential

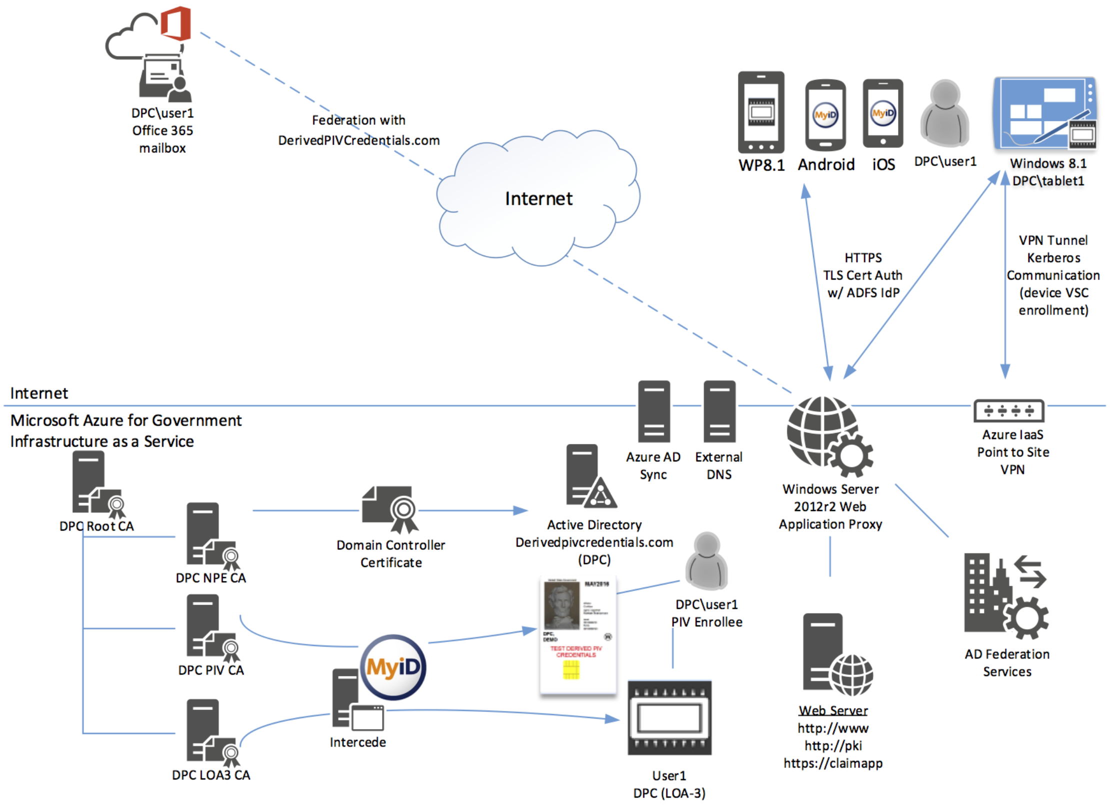
PIV and DPC Lifecycle Relationship



Proof of Concept Research

- Goal is to demonstrate the issuance and usage of Derived PIV Credential (DPC) in accordance to SP 800-157
- Intercede MyID for the lifecycle management of DPC
- Microsoft technologies for the protection and usage of the DPC credential

DerivedPIVCredentials.com



Intercede MyID FIPS 201 CMS

- MyID performs the entire lifecycle of the PIV credential, including PIV identity verification, credential issuance, lifecycle management and termination workflows
- MyID self-service kiosk guides Applicants through the DPC issuance processes

intercede

Mobile Devices

- iOS and Android require the MyID Identity Agent for both issuance and usage
- MyID Identity Agent is the key container for the DPC
- MyID Browser and MyID Mail leverage the DPC within the MyID key container

Mobile Devices

- Windows OS (8+) and Windows Phone (8.1+) use the Virtual Smart Card technology
- Requires the MyID Identity Agent for issuance
- The Microsoft Cryptographic Service Provider presents the DPC just like a smart card

Implementation Capabilities

- SP 800-63-2 Level of Assurance 3 (LOA-3)
- Test OIDs to identify DPC LOA-3 credential
- MyID issues PIV card and DPCs
- Method of issuance + Windows 8 OS = LOA-3 DPC

Microsoft Virtual Smart Card

- Trusted Platform Module (TPM) is a microcontroller that stores keys, passwords and digital certificates.
- TPM is the secure element used by the Windows 8 Virtual Smart Card (VSC)
- VSC utilizing a TPM provide the three main security principles of traditional smart cards (non-exportability, isolated cryptography and anti-hammering)
- Active Directory logon (Kerberos) and federation authentication (TLS certificate based auth)

MyID Self-Service Kiosk Issuance

- LOA-3 issuance and LOA-4 issuance (biometric required)
- Securely communicates to the MyID CMS
- Proof of identity (PIN, FASC-N, CHUID)
- Validation of PIV credential (PKI-Auth)
- 7 day revocation check (RC2.4)

intercede

MyID DPC Maintenance

- DPC PIN change/unblock for platforms utilizing the MyID Mobile SDK
- DPC PIN unblock for Active Directory domain joined system

intercede

MyID DPC Termination

- Within 7 days of issuance of DPC the originating PIV credential validity is checked
- Remove Person revokes all credentials issued to Subscriber
- PIV and DPC can be managed independently
- Key word is “eligible”

intercede

DPC Usage

- The scope of the Derived PIV Credential is to provide PIV-enabled authentication services on the mobile device to authenticate the credential holder to remote system
- X.509 based authentication to Microsoft Cloud Services

Office 365 Outlook Web Access (OWA)

- Uses the WS-Federation passive profile
- User authenticates with DPC at their federation identity provider
- IE supports S/MIME

Office 365 Outlook Modern Authentication

- Microsoft’s SAML 2.0 and OAuth 2.0 protocols for rich applications
- X.509 authentication for Outlook
- Outlook 2013 March 2015 Update

Outlook S/MIME

- Digital signature and encryption are supported

Federation

- Microsoft Cloud Services support claims based authentication
- On premises application are being developed to support claims - Exchange 2013 SP OWA, SharePoint 2013, and more coming

Next Steps

- Expand upon research with NCCoE Building Block

nccoe.nist.gov/projects/building_blocks/piv_credentials

Questions?