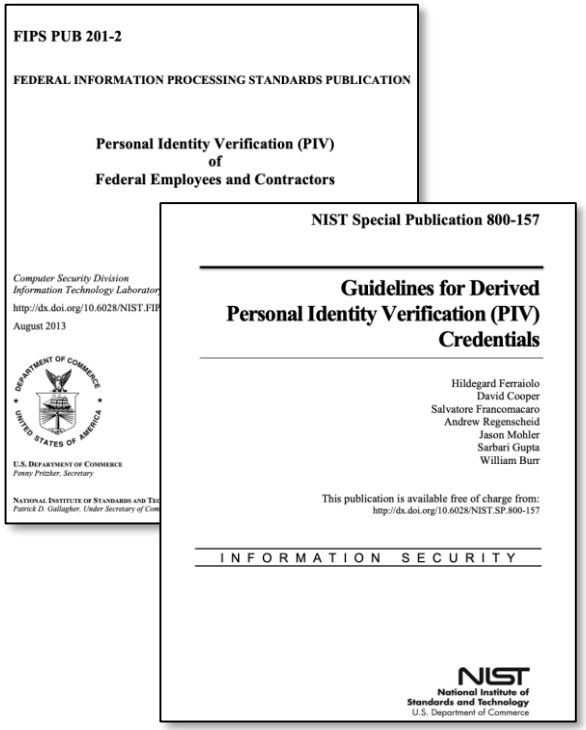
FIPS 201-3:
Derived PIV Credentials

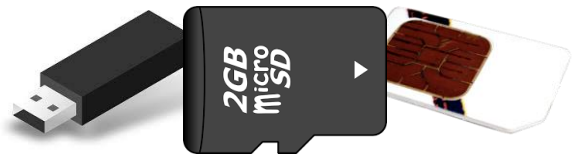
Andrew Regenscheid
Computer Security Division
Information Technology Laboratory (ITL)

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

FIPS 201-2 and Derived PIV Credentials

- **FIPS 201-2** (Aug. 2013) included Derived PIV Credentials
  - ***Derived Credential (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.
  - ***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.
- Policy restricted its use to mobile devices
- Intended to maximize interoperability with PIV card issuance and relying party systems





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

Authenticators

FIPS 201-3 Goals

- Accommodate innovative authenticators for emerging use cases while maintaining HSPD-12 security and interoperability goals

Agency 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

Develop guidance to facilitate deployment and use of derived credentials for logical and physical access using authenticators that satisfy the security and privacy requirements of NIST SP 800-63 while leveraging the PIV identity proofing process.

--OMB M-19-17

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

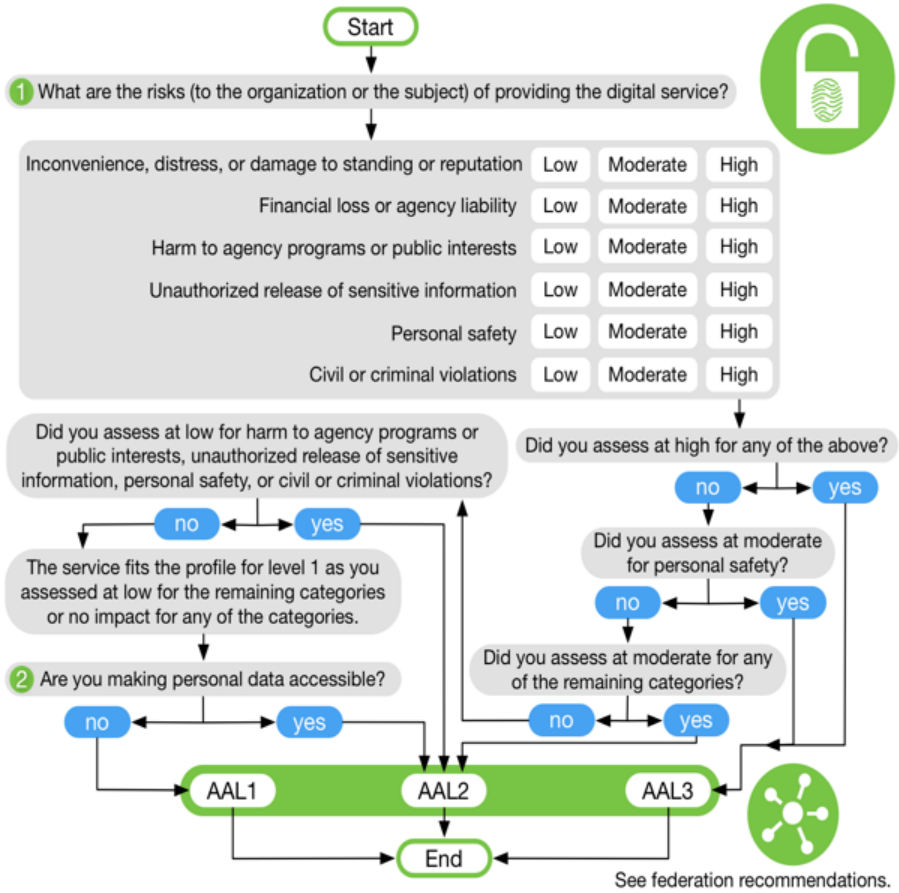
DPCs in FIPS 201-3

- Expanded Derived PIV Credentials (DPC)
  - An authenticator bound to subject's PIV account after successful authentication with PIV credential
  - Remote registration/binding allowed, with notification to the cardholder
  - Allowable authenticators based on AAL2/AAL3 in SP 800-63B
- **DPCs must be managed by PIV issuer**
  - Cardholder's home agency has strongest relationship to employee
  - Non-PKI credentials can only be verified by PIV Issuer's IdP
  - Interagency use cases supported through federation
- Technical guidelines will be developed in SP 800-157

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

Selecting Assurance Levels

- Agencies may use a combination of AAL2/AAL3 authenticators
- Base selections off the *Digital Identity Risk Management* process
- See NIST SP 800-63-3 for more details



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

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**
Authentication Intent	Recommended	**Required**

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

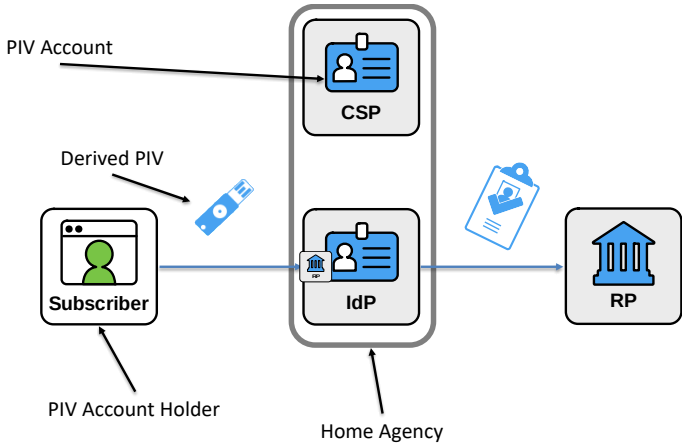
What makes a *Derived Credential* a *Derived *PIV* Credential*?

- **Under FIPS 201-2:**
  - DPCs are PKI credentials issued from a FPKI CA under new DPIV Certificate Policies
  - Certificate profiles mimicked PIV Authentication certificate
  - Interagency acceptance inherited from trust in FPKI
  - Generally stored in mobile device keystore

- **Under FIPS 201-3:**
  - DPCs are ***any*** allowed authenticator issued based on proof of possession of a PIV card and managed with existing PIV credentials
  - Specific technical requirements will be specified in revision to SP 800-157
  - Interagency acceptance through federation
  - Authenticator types may include hw/sw crypto tokens, FIDO authenticators, push notification authenticators, etc.

PIV/DPC Lifecycle

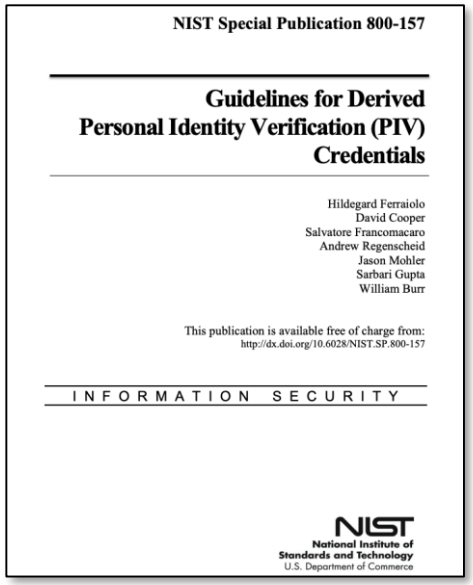
- **PIV Registration/Issuance**
  - Create the PIV Account in IDMS
  - Create a PIV Card
  - Bind the PIV Card to the Account
- **Registration of Derived PIV Credentials**
  - Bind to PIV Account after successful authentication with PIV credential
  - Managed by cardholder's home agency
- **PIV Credential Usage**
  - Direct or federation between systems/agencies
  - Federation required to use non-PKI authenticators as DPCs
- **Termination of Credentials**
  - Revoking PKI certificates, as appropriate
  - Unbind/Invalidate [Derived] PIV credentials in PIV account



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

Guidelines on DPC

- Upcoming revisions to SP 800-157:
  - *Revise issuance process:* As binding an additional authenticator to PIV Account
  - *Maintenance/revocation of DPCs:* As invalidating DPCs in DIV Account
  - *Authenticators:* Guidelines on selecting authenticator types from SP 800-63B
- Maintain existing PKI-based DPC guidelines
  - Accommodate existing architectures
  - Allow direct/offline authentication
  - Support stronger authentication programs and client-authenticated TLS


NIST Special Publication 800-157

Guidelines for Derived Personal Identity Verification (PIV) Credentials

Hildegard Ferraiolo
David Cooper
Salvatore Francomacaro
Andrew Regenscheid
Jason Mohler
Sarbari Gupta
William Burr

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-157

INFORMATION SECURITY

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

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