FIPS 201-3 Revision:

Overview of Changes

Andrew Regenscheid

Computer Security Division

NIST

National Institute of Standards and Technology

Technology Administration, U.S. Department of Commerce

HSPD-12

Homeland Security Presidential Directive 12 was issued in 2004 to create a common identification standard for federal employees and contractors for accessing federally-controlled facilities and federal information systems.

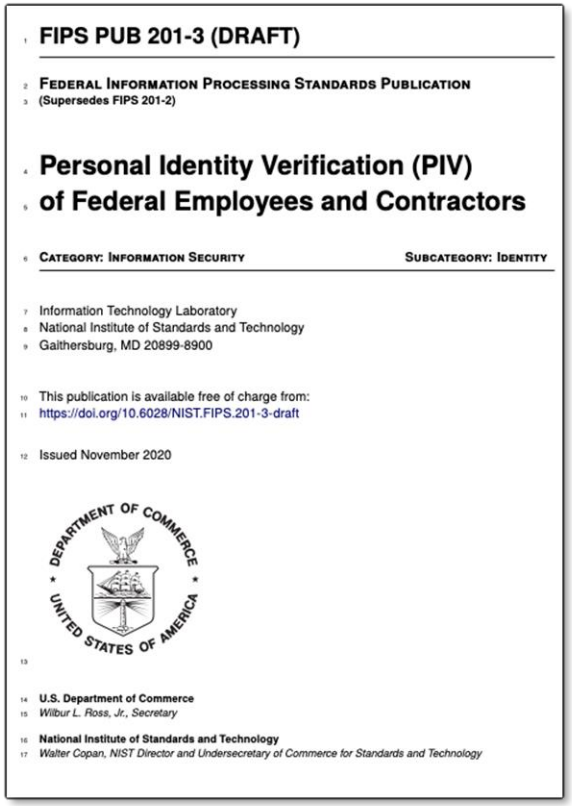
Results:

- A standard, interoperable credential: the PIV credential
- Consistent processes for identity vetting and proofing
- A common, secure approach for accessing facilities and networks
- An increased level of government efficiency

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

FIPS 201-3 Goals

- Align with NIST SP 800-63-3 requirements and terminology
- Support government-wide ICAM policy and guidance
- Adapt to current best practices and provide flexibility to meet future agency needs



FIPS PUB 201-3 (DRAFT)

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Supersedes FIPS 201-2)

Personal Identity Verification (PIV)
of Federal Employees and Contractors

CATEGORY: INFORMATION SECURITY SUBCATEGORY: IDENTITY

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.201-3-draft

Issued November 2020

DEPARTMENT OF COMMERCE * UNITED STATES OF AMERICA *

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

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

Major Updates

Identity Proofing

- Align with SP 800-63-3
- Supervised remote proofing

Authenticators

- Support new authenticators as derived credentials
- Allow derived credentials on additional platforms

Federation

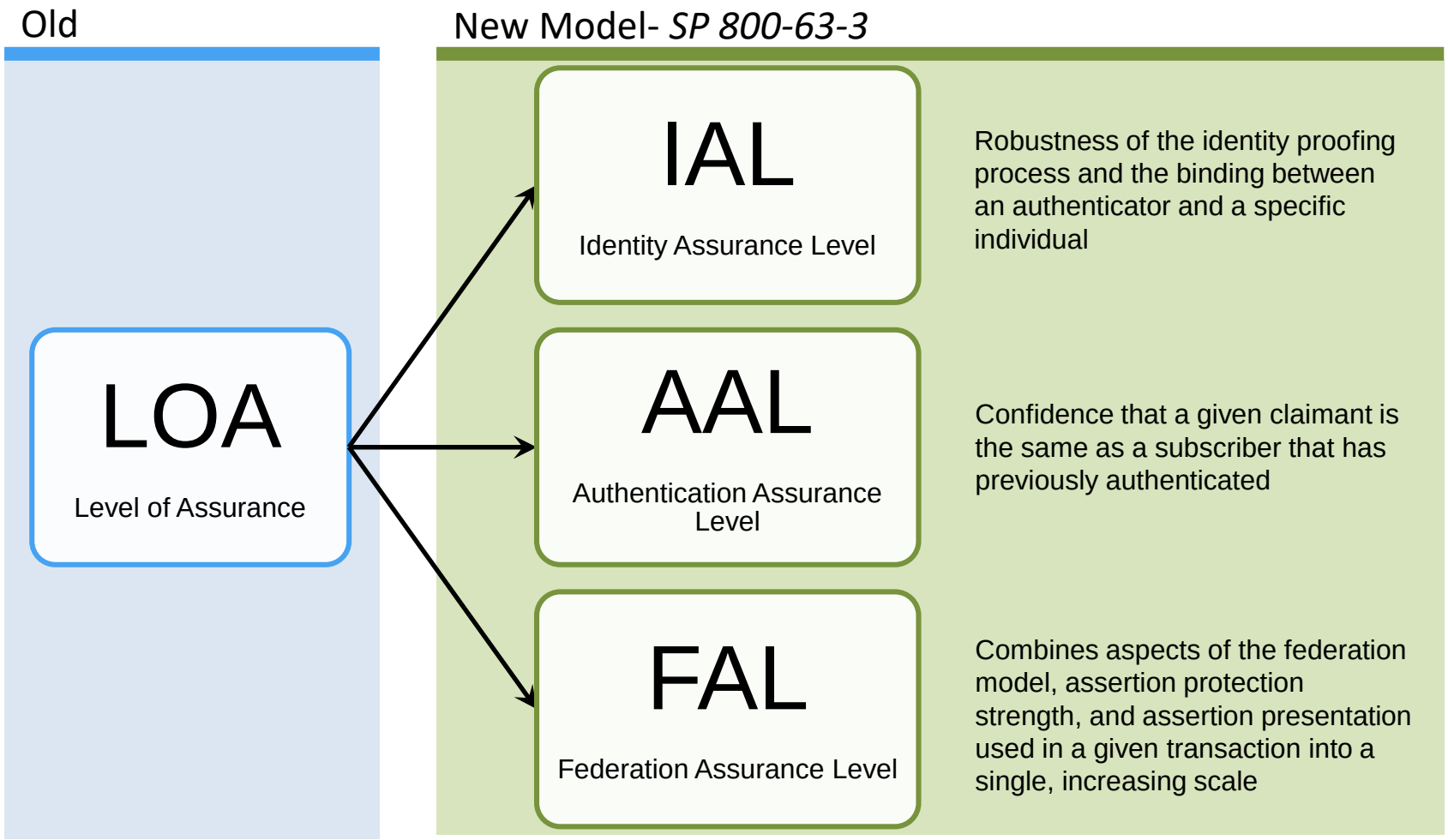
- Facilitate interagency interoperability and trust
- Simplifies support on relying parties

Physical Access Control

- Removal of CHUID authentication mechanism
- Investigate alternative PACS tokens and authentication protocols

PIV Cards will remain primary authenticator

NIST SP 800-63-3 Model



PIV Architecture

PKI

CAs, RAs, CRL/OCSP

Card Management

PIV Card

Relying Parties

Logical Access

Physical Access

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

PIV Architecture

PKI

CAs, RAs, CRL/OCSP

Identity Management

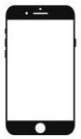
Card Management

PACS Controller

Enterprise IDMS

Authenticators

PIV Card



Derived PIV Credentials

Relying Parties

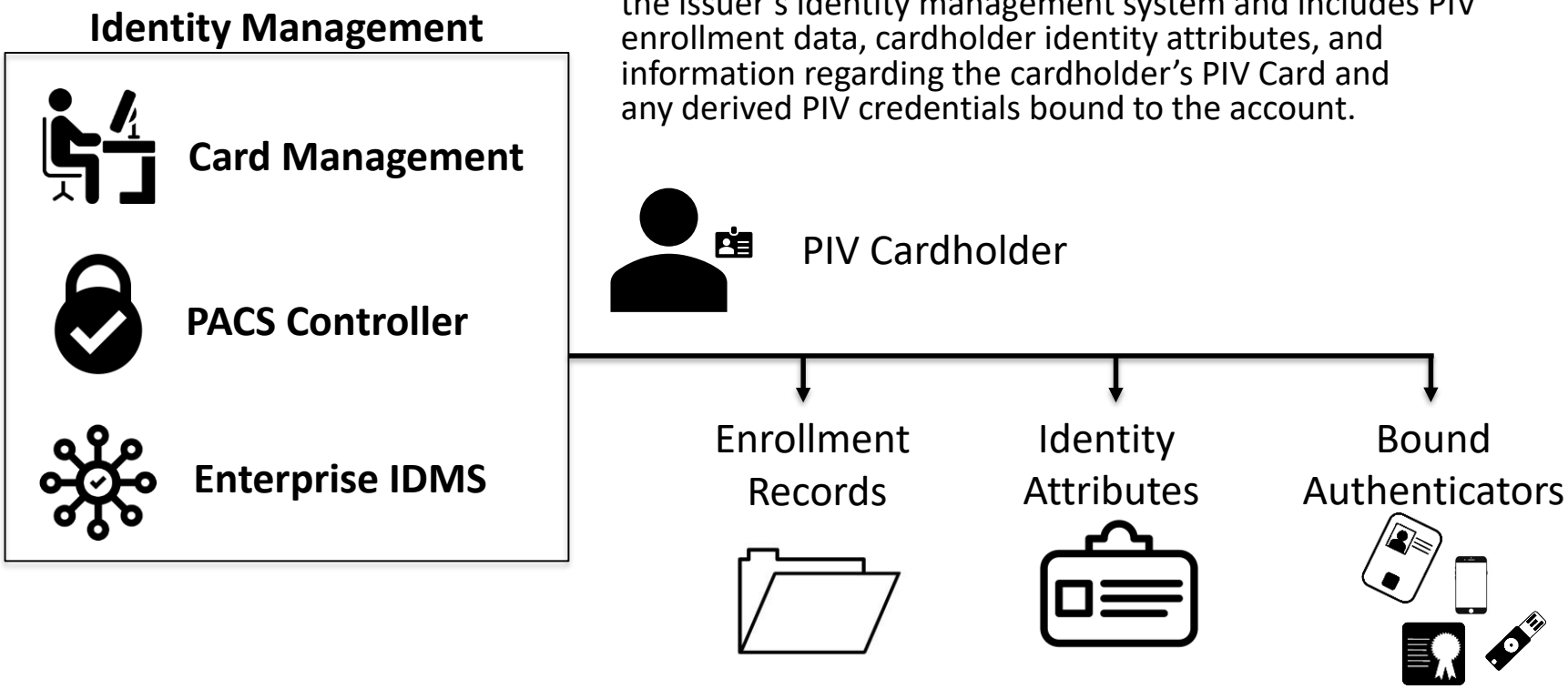
Logical Access

Physical Access

PIV Account

PIV Account:

The logical record containing credentialing information for a given PIV cardholder. This is stored within the issuer's identity management system and includes PIV enrollment data, cardholder identity attributes, and information regarding the cardholder's PIV Card and any derived PIV credentials bound to the account.



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

PIV 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
- **Termination of Credentials**
  - Revoking PKI certificates, as appropriate
  - Unbind/Invalidate [Derived] PIV credentials in PIV account

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

Federation

Definition:

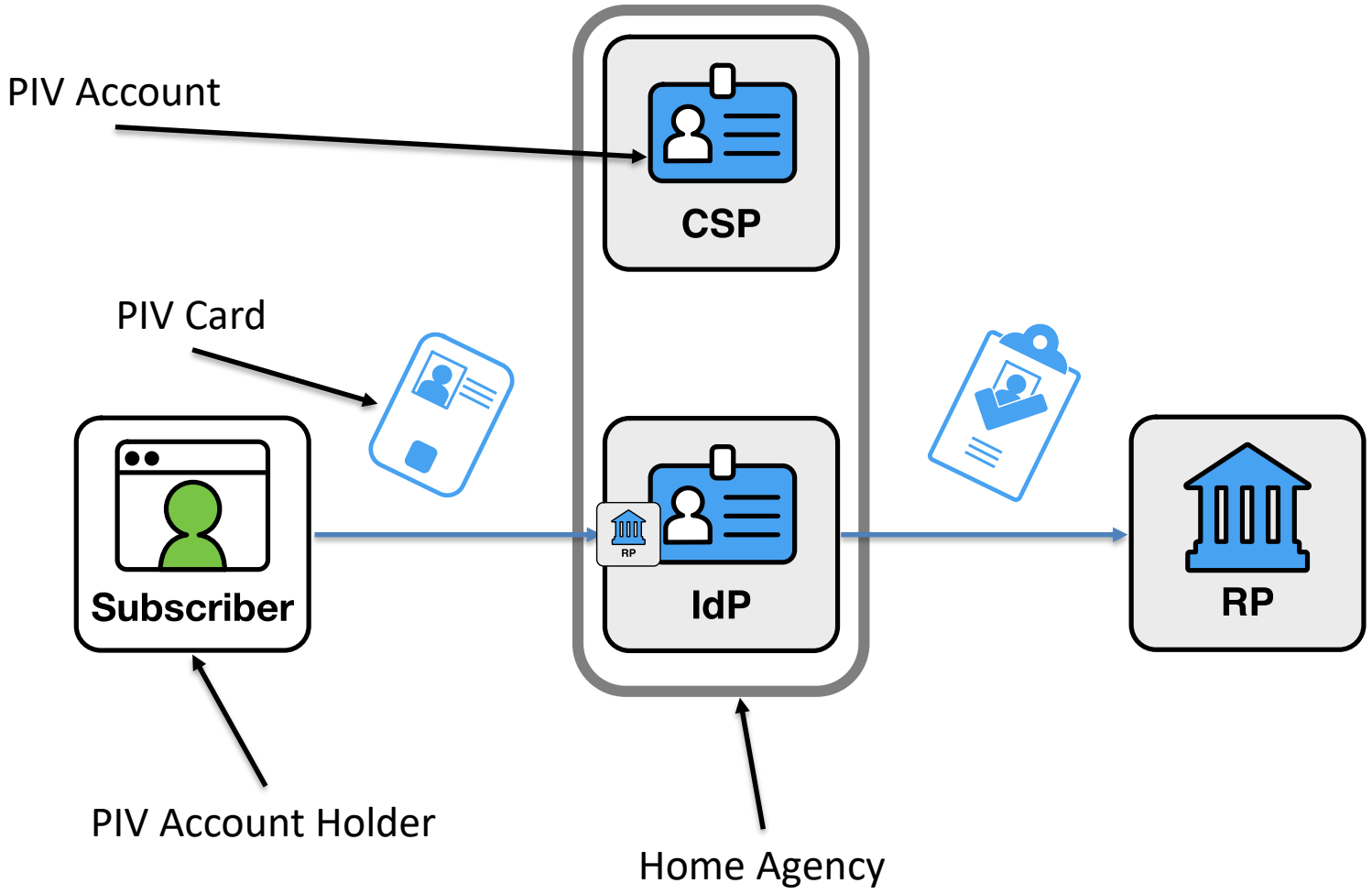
A process that allows the conveyance of identity and authentication information across a set of networked systems.

- NIST SP 800-63-3 Appendix A

Federation

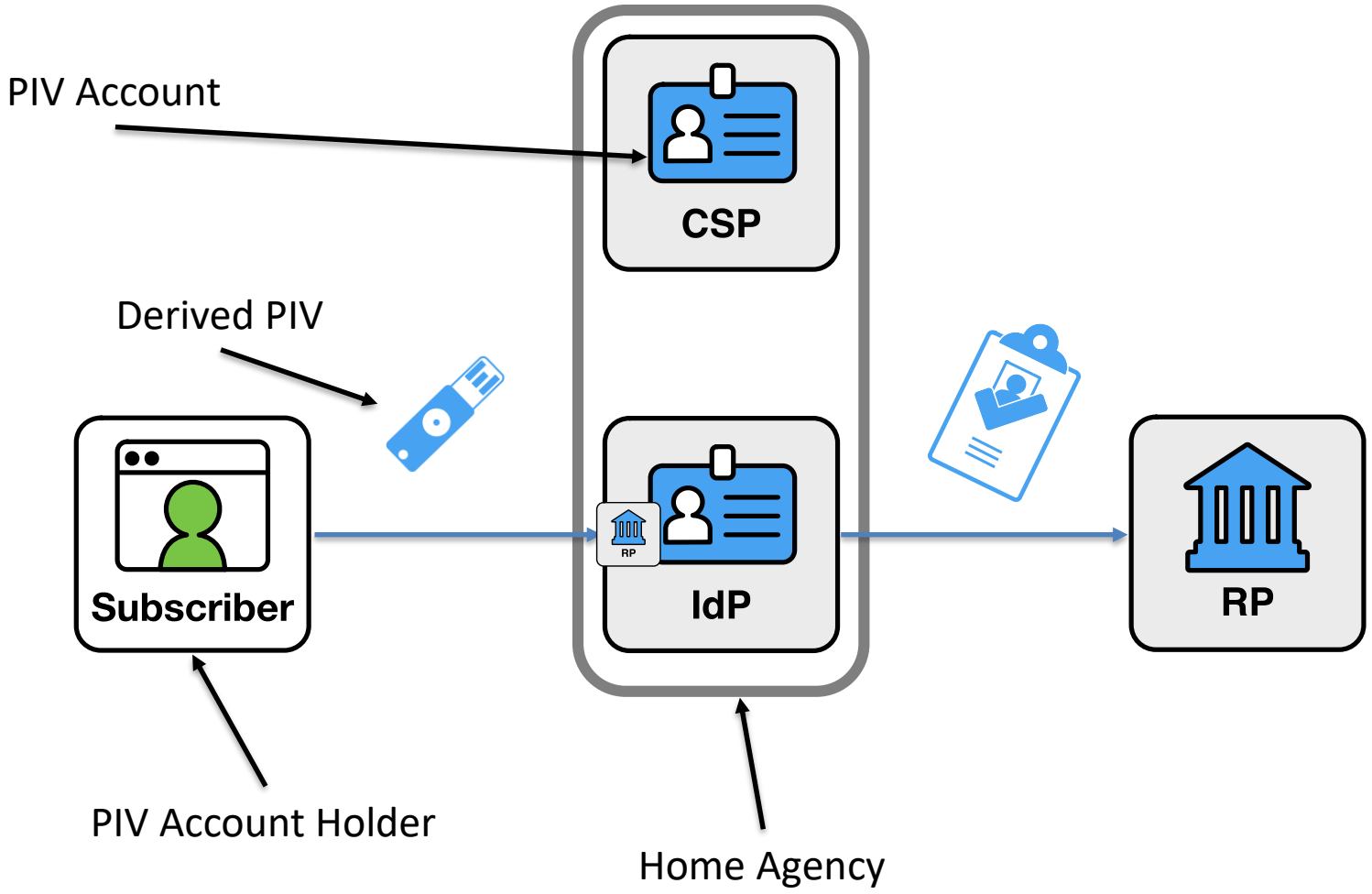
- Recommended way to accept and process PIV credentials from other agencies
- Provides real-time sharing and identity assertions and attributes from the PIV account at cardholder's home agency
- Facilitates interoperability between relying parties and a variety of authenticators

Federation with PIV



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

Derived Credentials



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

Wrap Up

- FIPS 201-3: Increased focus on PIV as federal enterprise identity management
- Major goals/updates:
  - Facilitate stronger, centralized identity management
  - Maintain high-assurance identity proofing
  - Increased flexibility to accommodate emerging use cases and architectures
  - Focus on federation for interoperability and interagency trust