FIPS 201-3 Business Requirements Workshop:

Identity Proofing and FIPS 201 Alignment with SP 800-63A

Jim Fenton
David Temoshok
March 19, 2019

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

Session Topics

- FIPS 201 Alignment with SP 800-63A
- FIPS 201 and SP 800-63A Identity Proofing and Enrollment Process Flows
- Identity Evidence Collection and Strength
- Identity Evidence Validation
- FIPS 201 Mitigating Controls
- Virtual In-Person ID Proofing

FIPS 201 Alignment with SP 800-63A

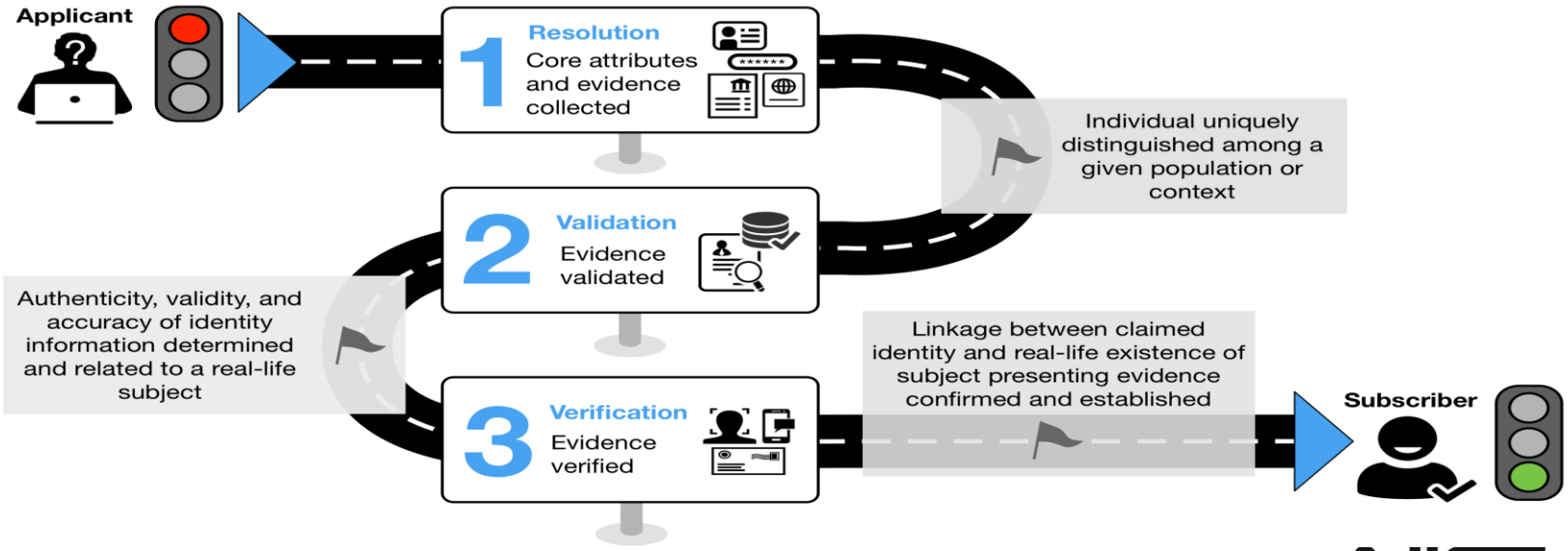
- Objective: Ensure that FIPS 201 and agency PIV identity proofing and enrollment processes meet SP 800-63A IAL3.
- NIST intends to align FIPS 201 with SP 800-63A IAL3
  - Alignment may require changes to both FIPS 201 and 800-63A as joint projects
  - FIPS 201 will be a profile of IAL3, and may have additional requirements and controls.
  - FIPS 201 may incorporate mitigating controls where IAL3 requirements are not fully met.
- Scope:
  - SP 800-63A Scope: Extremely broad and diverse use cases across the USG for public, government and industry identity assurance with little or no prior USG identity proofing.
  - FIPS 201 Scope: Identity assurance for known and vetted USG employees and contractors authorized (sponsored) for PIV enrollment, issuance and use.

Identity Proofing and Enrollment Process Flows

FIPS 201 PIV Enrollment

Suitability/ Fitness Adjudication → Sponsorship → In-person ID Proofing Evidence Validation Biometric Collection → In-person Biometric matching, PIV Issuance and Binding

SP 800-63A Identity Proofing and Enrollment



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

Identity Proofing/Enrollment Requirements Snapshot

	SP 800-63A IAL3	FIPS 201-2
Scope of User Population	Identity Assurance for very broad, diverse populations to access USG online services and applications	Identity Assurance for USG employees and contractors authorized (sponsored) for PIV enrollment
Presence	In-person	In-person
Identity evidence collection	Open-ended (no static list) -- collection based on evidence strength evaluation – weak, fair, strong, superior.	Static list of basically I-9 documents – primary and secondary classification
Strength of evidence	2 pieces Superior or 1 Superior + 1 Strong or 2 Strong + 1 Fair	1 piece of primary evidence + 1 primary or secondary evidence
Evidence validation (inspection)	Required (authenticity, security features, alteration)	Required (authenticity, security features, alteration)
Evidence data validation	Data validation required (issuing or authoritative source) for each piece of evidence at the same strength as the evidence presented.	Not required.
Identity verification	Ownership of claimed identity verified by physical or biometric match against strongest piece of evidence.	• Suitability and fitness adjudication • NACI and Criminal history checks • Background investigation • Biometric binding at PIV issuance

FIPS 201 Notional Evidence Strength

FIPS 201 Primary Evidence	63A Strength
• PIV Card • U.S. Passport or Passport Card* • Most Foreign Passports* • Permanent Resident Card (Form I-551)*	Superior
• Employment Authorization Doc. Form I-766 • State Drivers License or ID Card • U.S. Military ID (and dependents) Card	Strong

FIPS 201 Secondary Evidence	63A Strength
• Native American tribal document (Bio)*	Superior/ Strong
• U.S. Citizenship Certificate • U.S. Naturalization Certificate • U.S. Coast Guard Merchant Mariner Card • Reentry Permit (Form I-327) • Refugee Travel Document (Form I-571)	Strong
• Birth Certificate • U.S. Social Security Card • Voter Registration Card	Fair/Weak

Photographs as biometrics

- 63A does not clearly recognize pictures as biometrics on evidence
  - "photograph or biometric template" (weak -> strong)
  - "photograph and biometric template" (superior)
- Result: little acceptable Superior evidence
- Potential area of -63A revision
- Is the 800-63A requirement for 2 strong + 1 fair evidence workable?

FIPS 201 Mitigating Controls

- FIPS 201 does not require the validation of information from identity evidence through issuing or authoritative sources as required by 800-63A.
- SP 800-63-3 provides that Agencies may determine alternatives to normative requirements based on *mission, existing business processes, special considerations for certain populations, or due to other capabilities*.
- SP 800-63-3 states: "*the agency MAY adjust their implementation of solutions based on the agency's ability to mitigate risk via means not explicitly addressed by SP 800-63 requirements*."
- PIV identity proofing and enrollment present the following considerations for mitigating and compensating controls:
  - Target population is subject to employment vetting;
  - Employment controls for national agency checks, criminal history checks, background investigation, and suitability and fitness adjudication may be determined to be additional mitigating controls for PIV identity proofing.
- NIST specifically seeks input from Agencies on the adequacy of PIV enrollment mitigating controls to compensate for identity evidence validation controls.

Virtual in-person proofing

- A kiosk or similar device controlled by the CSP that provides comparable proofing security to an in-person process
- Likely includes:
  - Multiple cameras: high-resolution image of applicant, document cameras/scanners, wide-angle camera to supervise use of device
  - Biometric (e.g., fingerprint) sensor
  - Document validation aids: UV light, RFID reader
- Located at a site supervised by a trusted (but not trained) person
- Secure Internet connection to centrally-located trained enrollment staff
- May be componentized/transportable

Discussion topics

- Adequacy of PIV enrollment mitigating controls to compensate for identity evidence validation controls.
- Are any of the cited forms of evidence not used or not accepted by your agency?
- Is the 800-63A requirement for 2 strong + 1 fair evidence workable?
- Should REAL ID compliant driver's licenses be treated differently from non-compliant for evidence strength?
- Are existing requirements for Superior evidence too hard to achieve?

Questions?

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