

FIPS 201-2 Workshop

NIST PIV Team

**National Institute of Standards and Technology
US Department of Commerce**

**Gaithersburg, MD
April 18 – 19, 2011**

IDENTITY PROOFING AND REGISTRATION



1

Acceptable Source Documents

- I-9 is a list of employment eligibility form. Not necessarily designed for identity proofing.
- Confusion about which combination (two document from List A, one document from List B and one document from List C, or is it any two documents from List A, List B, or List C) of source documents must be used to establish identity.
- Discrepancy between COMMON policy, SP 800-63 E-authentication guidelines, and FIPS 201 ID proofing requirements.



Acceptable Source Documents Changes

- FIPS 201-2 provides a complete list of acceptable primary and secondary identity source documents.
- Primary documents shall be neither expired nor cancelled.
- Secondary document requirements are listed explicitly for each document.

Chain-of-trust Record

- A mechanism is needed that will allow Federal PIV Card issuers to maintain PIV cardholder's record integrity internally and to exchange background investigation, demographic, and card validity information with other agencies. For example,
 - Interagency transfer: a Federal employee is transferred from one agency to another.
 - Extended enrollment: a PIV applicant enrolls ten fingerprints for background investigations at one place and time (e.g., at a police station), and two fingerprints for on-card templates at another place and time (e.g., at the PIV enrollment station).
 - Reissuance: a PIV cardholder loses his/her card. Since the card issuer has biometric enrollment data records, the cardholder can perform a 1:1 biometric match to reconnect to the card issuer's chain-of-trust. The card issuer need not repeat the background investigation.



Chain-of-trust Record Changes

- A chain-of-trust is a documentary evidence of the identification data card issuer collects.
- A chain-of-trust is a sequence of related enrollment data records, and shall be created and maintained through the methods of contemporaneous acquisition of data within each enrollment data record, and biometric matching of samples between enrollment data records.
- An enrollment data record shall describe the circumstances of biometric acquisition including the name and role of the acquiring agent, the office and organization, time, place, and acquisition method. An enrollment data record shall retain latest biometric record while it may or may not contain historical biometric data.
- A special publication following release of FIPS 201-2 will address how to import and export a chain-of-trust.