CHAIN-OF-TRUST:
A Service Provider Perspective

USAccess HSPD-12 Managed Service Office

USAccess Program Overview

- The GSA HSPD-12 Managed Service Office (MSO) is the executive agent responsible for managing government-wide acquisition of information technology to implement HSPD-12 services.
- The USAccess program provides federal agencies with interoperable identity management and credentialing solutions that provide end-to-end services to enroll applicants, issue credentials, and manage the lifecycle of these credentials.
- USAccess is not a contract vehicle.
- Currently USAccess services approximately 100 Customer Agencies and has issued more than 900,000 PIV cards in its 9 years of existence.
- Sponsorship and enrollment data is stored in a set of databases that Customer Agencies access by web and SIP interfaces. Cards are produced and delivered by a secure production facility, or in some cases by a distributed printing network.

Chain-of-Trust as a Philosophy

- Chain-of-trust definitions vary with application. Certificates, Legal evidence, critical manufacturing
- The identity security of PIV relies on a valid Chain-of-Trust.
- There are several items that need to remain in place to keep the Chain-of-Trust intact.
  - Cards are manufactured correctly with no defects.
  - Cardholder uses PIV appropriately.
  - System is operating and being maintained within policy.
  - System role holders are performing work in accordance with Rules of Behavior.
- It is best to use the least amount of data required to maintain Chain-of-Trust.

Importance of Chain-Of-Trust to USAccess

- For our purposes, COT establishes a reliable record of the identity data that is needed to issue a PIV card.
- Acts as a guarantee that the identity data matches and is accurate for and among:
  - The individual
  - The issued card
  - The system record(s)
- Ensures the integrity of identity data as it moves from system to system.
- Provides proof that the PIV issuance process can be outsourced to a shared service without danger of corruption or compromise.
- (Can) facilitate the preservation of or access to longer-term or associated data.. (requires sufficient data)
- Institutes a standard for trusting data exchanges between systems and Agencies.

USAccess Chain-of-Trust Methodology

- Agency sponsors employee or contractor.
  - Name, SSN, associated agency, location information, etc.
  - Record created in system.
- Agency adjudicates applicant as suitable for issuance.
  - Record is updated within system.
- Applicant enrolls at either a Fixed credentialing center, or a Light Credentialing station.
  - Identity (I-9) documents examined and scanned.
  - Fingerprints and photograph captured.
  - Enrollment package is signed and preserved in the system.

USAccess Chain-of-Trust Methodology

- Preissuance validation checks are performed to ensure all required information has been collected and no duplicate records exist in the system.
- Once complete, card is printed & personalized, but not activated.
  - Sent from a secure production facility to ship-to address in the record and checked in at the site upon delivery.
- Applicant makes appointment for card for Activation.
  - Fingerprint match and two forms of identity are required to complete Activation.
  - Record updated in system.
- Card Lost/Stolen/Expired/Employment Lapse > Two Years
  - Re-enrollment required to reestablish Chain-of-Trust.

USAccess Chain-of-Trust Methodology

- Sponsorship record data is available to the Customer Agencies within the shared service.
  - Employees and Contractors that move between Agencies are able to use the same valid sponsorship to enroll and have cards printed at multiple agencies.
    - Activation requirements apply in order to maintain Chain-of-Trust.
  - Agency Specific criteria may or may not accept adjudications from other agencies which means additional Background Investigations may be required.
- Key History is available on-card

Our Findings

- In importing data from other agencies, the exporting agency practice or policy may not be consistently followed.
- Until now, there was no standard government-wide guidance on how to establish and maintain Chain-of-Trust.
- Limited success in enrollment exchange
  - Signed enrollment packages do not maintain a Chain-of-Trust if the identity data is collected at a different time than when the signature is applied.
- Opportunity to influence content of SP 800-156.

Questions

Contact Information

Stephen P. Sill
USAccess Program Manager
Stephen.Sill@gsa.gov
www.fedidcard.gov