HSPD-12 Implementation

Architectural Concept

Chris Louden
CTO, Enspier Technologies

April 20, 2006

Agenda

Introductions

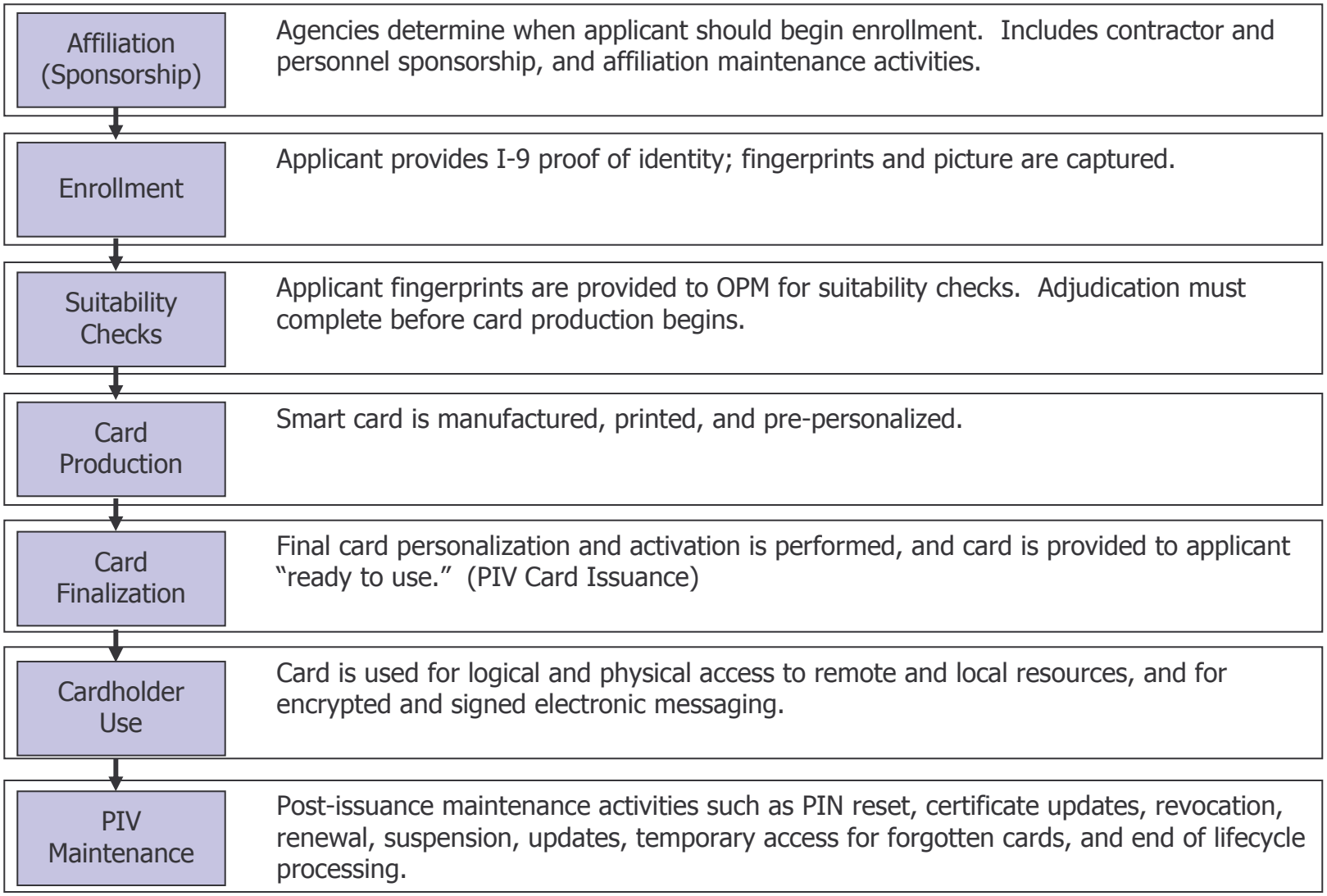
PIV Lifecycle

PIV Infrastructure Components

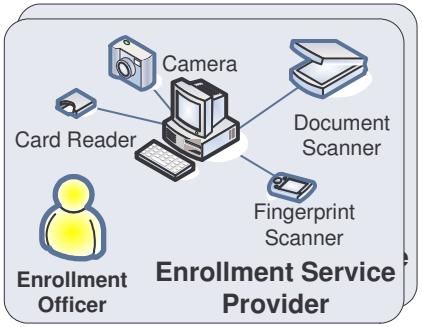
PIV Component Interaction

Next Steps

PIV Lifecycle



PIV Infrastructure Components

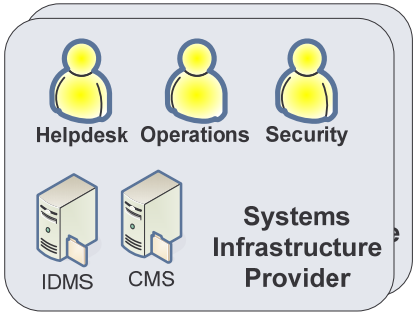


PIV Enrollment Service Providers (ESPs) provide local presence (i.e., at agency sites) for enrollment of applicants. PIV ESPs are used after agency affiliation has been determined. PIV ESPs enroll applicants only when authorized by agencies.

The **PIV ESP** performs the following functions:

1. Identity proofing according to FIPS 201 standards, I-9 documentation; and
2. Capture of biometric sample, including picture and 10-slap fingerprints.

PIV Infrastructure Components (cont'd.)

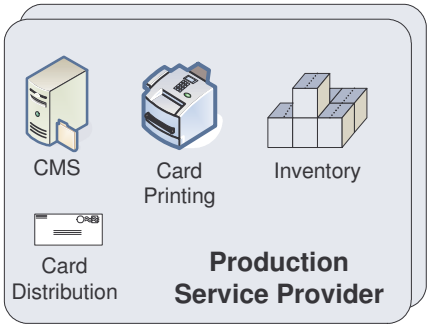


PIV Systems Infrastructure Providers (SIPs) provide the software functionality required to manage PIV credentials. Specifically, PIV SIPs build, host, and operate software that provides agencies with critical Identity Management System (IDMS) and Card Management System (CMS) functionality. In this context, PIV SIPs act as Application Service Providers (ASPs).

The **PIV SIP** performs the following functions on behalf of agencies:

1. All CMS functionality;
2. Tracking PIV credential state from affiliation, enrollment, suitability, production, finalization, and maintenance;
3. Interfacing with agency systems (e.g., HR, PACS, and LACS) and other shared components through standard interfaces; and
4. Auditing, Logging, and Accounting of transactions.

PIV Infrastructure Components (cont'd.)

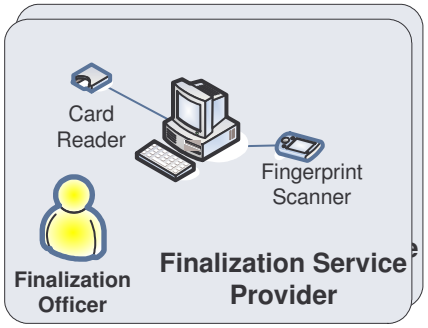


PIV Production Service Providers (PSPs) produce and personalize PIV smart cards. Personalization is limited to surface printing and electrical pre-personalization (i.e., load and instantiate). The PIV PSP locks the cards with a transport key and ships them to an agency-designated location for finalization. This finalization is often referred to as issuance, but it is really just the last step in the issuance process.

The **PIV PSP** performs the following functions:

1. Card production;
2. Card surface personalization (i.e., cardholder data and agency template); and
3. Electrical pre-personalization (i.e., load and instantiate applets and containers).

PIV Infrastructure Components (cont'd.)

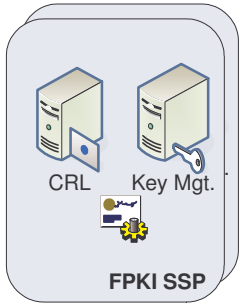


PIV Finalization Service Providers (FSPs) provide local presence to finalize personalization of the cards and complete issuance to the applicant. In practice, FSP operations may be managed by the same organization which handles ESP operations for an agency.

The **PIV FSP** performs the following functions:

1. Verify applicant biometric;
2. Unlock the card (the card is locked during shipment with a transport key);
3. Initialize the card into the Agency CMS;
4. Load signed objects onto the card; and
5. Allow for PIN selection by the verified cardholder.

PIV Infrastructure Components (cont'd.)



Federal Public Key Infrastructure Shared Service Provider (FPKI SSP) has been established to provide PKI related services.

More information about the **FPKI SSP** can be found at:

1. http://www.cio.gov/fpkipa/

PIV Component Interaction

Interaction Diagram

First, the issuing agency provides affiliation (sponsorship) feeds, adjudication results, and revocation requests to the SIP. The SIP provides reports back to the agency.

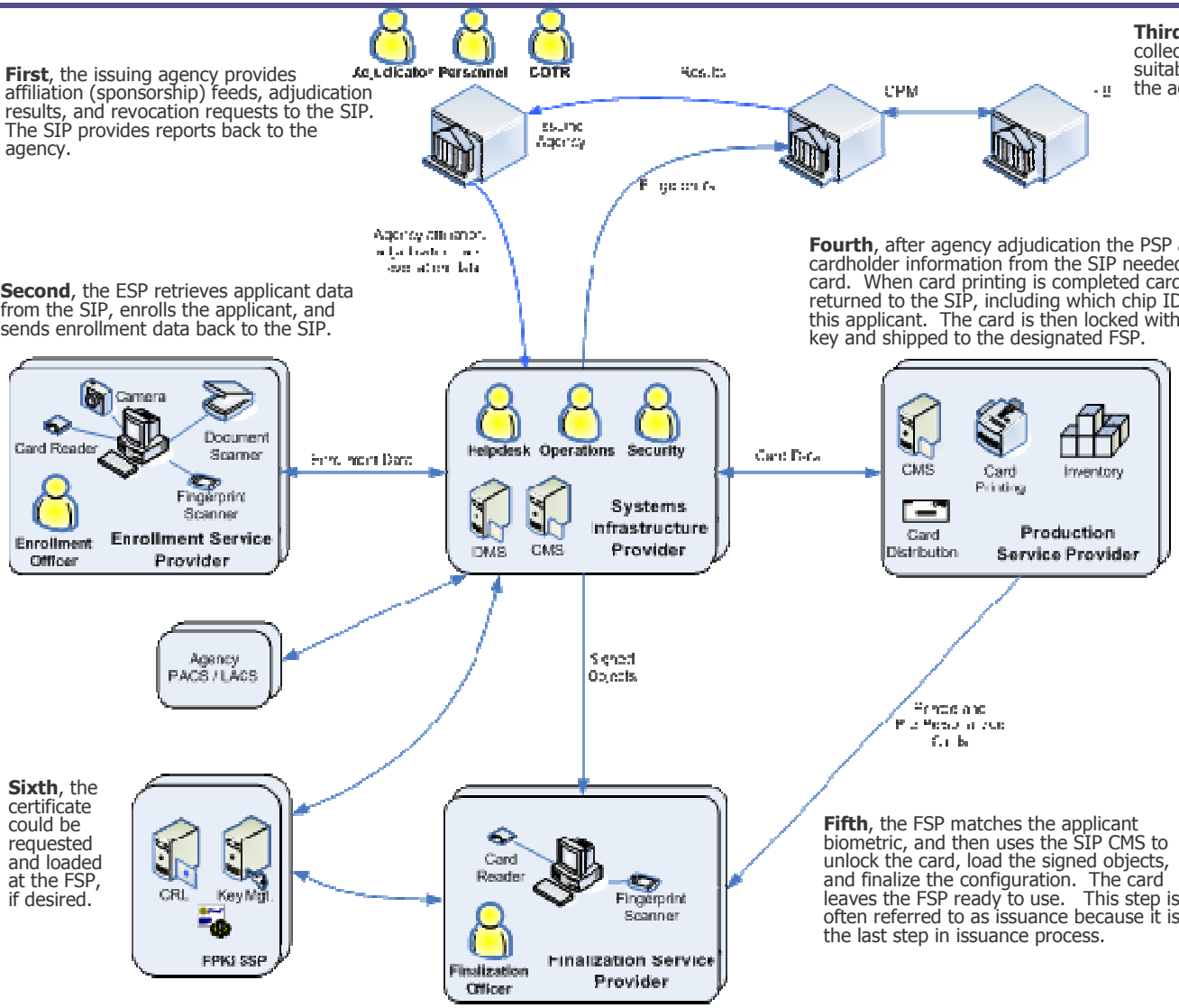
Second, the ESP retrieves applicant data from the SIP, enrolls the applicant, and sends enrollment data back to the SIP.

Third, the SIP sends fingerprint data collected from the ESP to OPM for suitability checks, and results are sent to the agency.

Fourth, after agency adjudication the PSP accepts cardholder information from the SIP needed to print the card. When card printing is completed card data is returned to the SIP, including which chip ID was used for this applicant. The card is then locked with a transport key and shipped to the designated FSP.

Fifth, the FSP matches the applicant biometric, and then uses the SIP CMS to unlock the card, load the signed objects, and finalize the configuration. The card leaves the FSP ready to use. This step is often referred to as issuance because it is the last step in issuance process.

Sixth, the certificate could be requested and loaded at the FSP, if desired.



Next Steps

- Begin defining interface requirements
  - Business Process Definitions – Use Cases
  - Components
  - Component Interactions
- Establish vetting/review process/participants
  - Government review
  - Industry participation/validation
- Establish "Cardholder Use" use cases as part of architecture
  - Logical vs. physical access
  - Local vs. remote access
  - Maintenance (lost card, name change, etc)