HSPD-12 Implementation Architecture Working Group Concept Overview

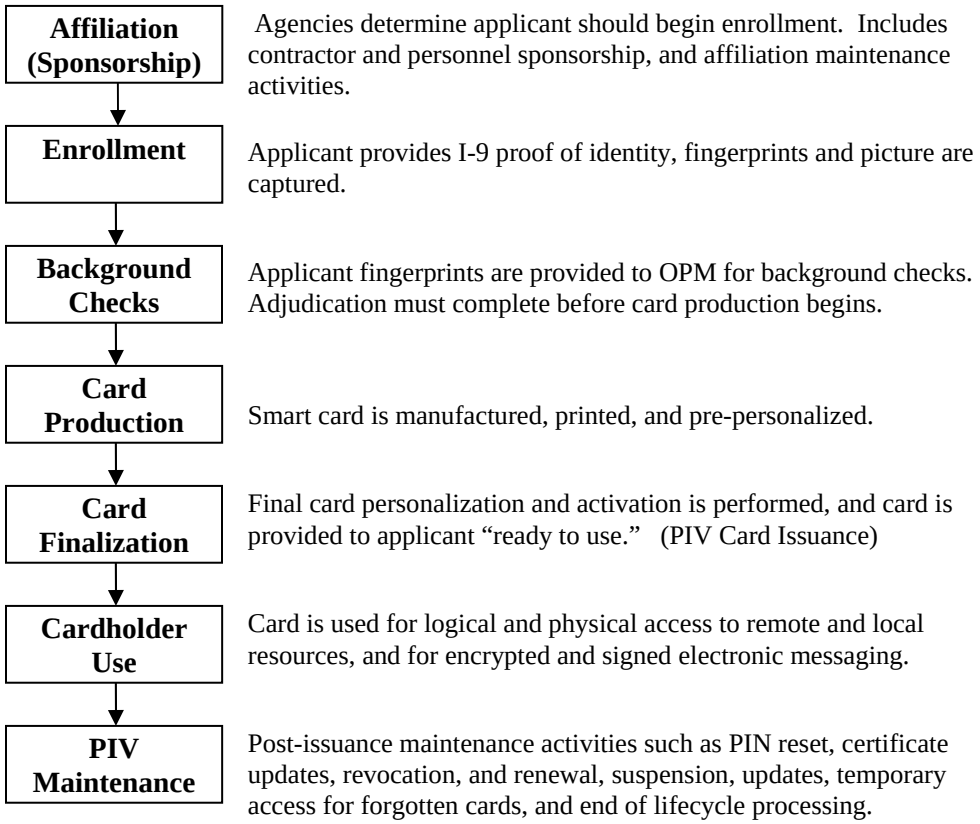
Version 1.0
March 17, 2006

Table of Contents

1 PIV Lifecycle

Figure 1 shows the stages in the PIV lifecycle. It begins with an agency deciding to sponsor an applicant, which establishes an affiliation with the agency and the need for a credential under agency policies. Once applicant affiliation and eligibility is determined, the applicant begins enrollment, providing proof of identity to an enrollment official who takes a picture and fingerprints. After enrollment, the Office of Personnel Management (OPM) checks suitability. At a minimum, OPM checks the fingerprints against the national criminal history database (via the Federal Bureau of Investigation). Once an agency official successfully adjudicates the results, card production begins. This model divides card production into two steps to allow card instantiation and surface printing to be done by a service provider with sophisticated printers. After applicant biometric verification, card personalization is finalized. The agency then provides a "ready to use" card to the applicant. Once the cardholder possesses a usable card, cardholder use and maintenance cases follow. Detailed systems use cases for each stage depend on agency infrastructure choices (i.e., which shared components are used).

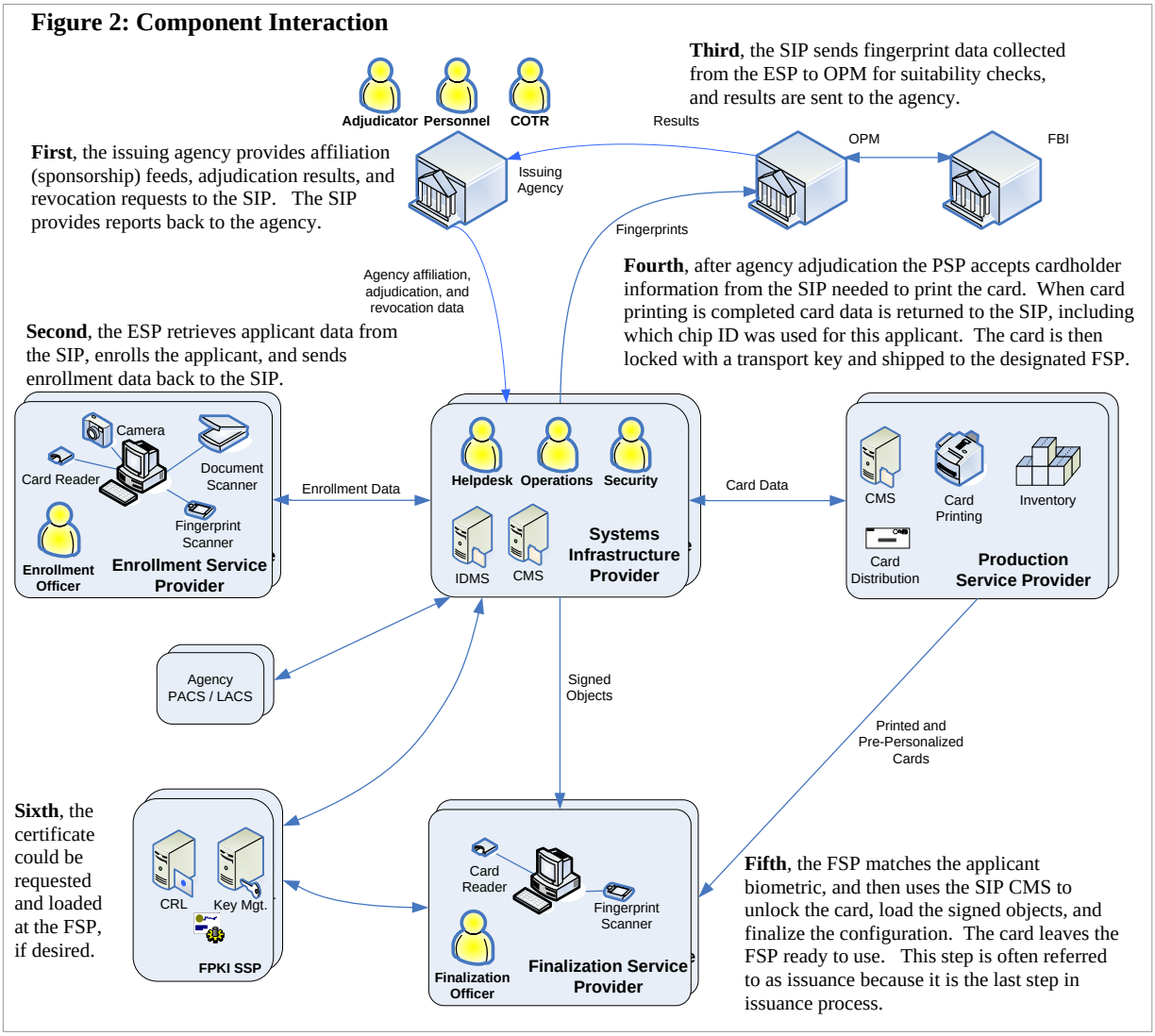
Figure 1: Organization of Use Cases



2 High Level Component Interaction Diagram

Figure 2 shows how the shared components interact for the affiliation, enrollment, suitability, card production, and card finalization use cases[1]. The diagram depicts an agency that has outsourced all functions to shared components. However, agencies may elect to perform some functions on their own. For example, and agency with a deployed Card Management System (CMS) may elect not to use a PIV Systems Infrastructure Provider (SIP), but could still leverage the other shared components by using their standardized interfaces. In addition, existing agency enrollment stations could act as the PIV Enrollment Service Provider (ESP) for some locations, using the standardized interfaces to interact with the other shared components.

Figure 2: Component Interaction



[1] Not all interactions described in section 3 are displayed for readability.

3 PIV Infrastructure Components

The following sections provide more description for the shared components shown in Section Three. The Component descriptions below assume an agency elected to outsource all functions. Agencies may elect to perform some or all of the functions within this model on their own; however, the same functions are applicable regardless of the strategy chosen.

Future stages of this effort will define interface specifications among the components, including encryption and strong authentication.

3.1 PIV Enrollment Service Providers

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.

The component interactions are:

1. The PIV ESPs retrieve applicant information from the SIP, including authorization to enroll; and
2. The PIV ESPs send all enrollment data back to the SIP for further processing.

3.2 PIV Systems Infrastructure Providers

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.

The component interactions are:

1. The PIV SIP accepts affiliation data from agency systems (e.g., personnel systems, contractor registries);
2. The PIV SIP accepts enrollment data from agency enrollment stations and/or PIV ESPs, and transmits applicant information to the stations;

3. The PIV SIP sends fingerprints to OPM services for criminal history checks;
4. The PIV SIP accepts adjudication results from agency adjudicators, including authorization to begin production;
5. The PIV SIP sends cardholder information to agency card printing stations or PIV PSPs;
6. The PIV SIP accepts the chip ID used for each used for each cardholder from the PSP; and
7. The PIV SIP sends signed objects to the FSP for card insertion.

3.3 PIV Production Service Providers

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).

The component interactions are:

1. The agency provides card print specifications, including visual security features;
2. The agency and PIV PSP share a transport key used during card shipment;
3. The FSP sends cardholder information needed to print individual cards;
4. The SIP designates a location to deliver the cards after production;
5. The PIV PSP sends the chip identifier (id) used for each cardholder to the SIP; and
6. The PIV PSP ships the card to the agency-designated location (FSP) locked with the transport key.

3.4 PIV Finalization Service Providers

PIV Finalization Service Providers (PIV 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 FSP will perform 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.

The component interactions are:

1. The PIV FSP is be shipped the physical card;

2. The PIV FSP uses the SIP CMS to unlock the card;
3. The PIV FSP uses the SIP CMS to load signed objects onto the card based on the association of the cardholder to the chip confirmed by the biometric match; and
4. The PIV FSP uses the SIP CMS to allow setting of the PIN.

3.5 FPKI SSP

The Federal PKI has already established the Shared Service Provider (SSP) program for PKI related services. More information is available at http://www.cio.gov/fpkipa/.