HSPD-12 Shared Component Architecture

Version 0.1.6
December 4, 2006

DRAFT

Important Note

This document is still in progress and is available solely to solicit early feedback.

Therefore, please do not focus on sections 4.7 – 4.8, as those sections are still in progress and will be addressed in the February 15, 2007 delivery.

This is a draft document subject to further revision. There is no guarantee that the final, approved version will be the same. Please do not use or rely on this document until it is approved.

Executive Summary

The Homeland Security Presidential Directive-12 (HSPD-12) Implementation Executive Steering Committee (ESC) has requested establishment of several shared components with well-defined interfaces to assist agencies in meeting Personal Identity Verification (PIV) requirements. The HSPD-12 Implementation Architecture Working Group (AWG) convened under the auspices of the ESC to develop an architecture that defines shared component interfaces and interactions.

This document describes the Shared Component Architecture (SCA), and captures the following AWG decisions:

- What architectural components are required;
- How and when architectural components interoperate to support all use cases; and
- How architectural components are technically constructed.

AWG decisions derive from the following methodology:

- Identification of Business Processes;
- Identification of known components;
- Creation of Use Cases;
- Analysis of Use Cases; and
- Revision of Use Cases.

The SCA is instantiated as an operational Shared Component Infrastructure (SCI). Three (3) categories of SCI components are discussed:

- **Shared Components (Shared Services)** – various services to be shared government-wide that are the primary focus of this document. Shared components must be implemented in accordance with the SCA and applicable technical interface specifications. The shared components are:
  - ➢ *Enrollment Station Provider (ESP)* – identity proofs applicants in accordance with Federal Information Processing Standard (FIPS) 201-1 standards and I-9 documentation and captures biometrics, including picture and 10-slap fingerprints.
  - ➢ *Systems Infrastructure Provider (SIP)* – manages full life cycle of the PIV card via Identity Management System (IDMS) and Card Management System (CMS) functionality.
  - ➢ *Production Service Provider (PSP)* – produces and personalizes PIV cards.
  - ➢ *Finalization Service Provider (FSP)* – finalizes personalization of PIV cards and completes issuance to the applicant.
- **Agency Components (Agency Systems)** – systems used by a single agency (i.e., not shared). Agency components may or may not already exist and must be implemented in accordance with the SCA and applicable technical interface specifications. Examples of agency components are:
  - ➢ *An agency Human Resource (HR)/Personnel system.*
  - ➢ *An agency's equivalent for a shared component not selected for use.*
- **Services** – resources external to the SCI used to complete tasks that tangentially pertain to or affect SCI processing. An example of a service is:
  - ➢ *Background investigation service.*

The AWG has designed the SCA to be flexible. It supports various service provision models (i.e., configurations) as may be needed over the long term. The spectrum of flexibility ranges from (a) an agency implementing an HSPD-12 solution comprised totally of shared components to (b) an agency implementing an HSPD-12 solution comprised of any mix of shared components and agency components. In all configurations, an agency can use services (e.g., background investigation) as needed. This flexibility ensures each agency can implement the solution best suited or available at the time (see [Business Arch]). The provision models supported by the SCA include[1]:

- Use all shared components but from multiple providers;
- Use all shared components but from a single provider;
- Use some (not all) shared components but from multiple providers; and
- Use some (not all) shared components but from a single provider.

The technical approach is mainly web services based, wherein technical interoperation with shared components (ESP, SIP, PSP, FSP) is via SOAP-wrapped Extensible Markup Language (XML) messages over Hyper Text Transfer Protocol Secure (HTTPS). Each shared component is a web service provider. An agency system, for example, is a web service requester. Other communication with shared components is via secure web interface. Each shared component is a "black box" accessible only via its published message set (i.e., interface specification) or web interface. Technical interoperation with non-shared components (e.g., agency Physical Access System Control System (PACS), agency Logical Access Control System (LACS)) and services (e.g., Office of Personnel Management (OPM), Federal Bureau of Investigation (FBI)) are via interfaces defined and controlled outside of the SCA.

This document is limited to PIV card issuance, credentialing, and maintenance via a SCI. Only those processes and technical interoperations supporting that scope are addressed in detail and presented as normative (i.e., required). However, information beyond scope is included to provide useful context and facilitate understanding of the overall PIV environment. For example, authentication of end users with PIV cards for the purpose of physical access or logical access is outside the scope of this document, but it is discussed to convey a more complete end-to-end business process.

The SCI adheres to a core set of security principles, which the SCI Trust Model (companion document) describes. The SCA does not preclude agencies leveraging the SCI from complying with privacy requirements required by HSPD-12.

The SCA is part of a larger, concerted effort to implement an HSPD-12 shared services solution. Therefore, in and of itself, the SCA does not define a complete, operational system. To achieve an operational system, an SCI governing authority must define and implement additional operational processes, procedures, policies, and rules. At an appropriate time, such a governing authority will facilitate all remaining tasks necessary to achieve an operational system.

The document flow provides the reader with a "building block" approach to understanding the SCA. It begins by defining the various SCI components. It continues by discussing business processes and concludes by presenting the use cases (sequence diagrams and activity diagrams as well) derived from the business processes.

[1] Note that the GSA service offering is different from this broader SCA solution.

Document History

Status	Release	Date	Comment	Audience
Initial	0.0.1	05/31/06	Internal Review	Enspier
Strawman	0.0.2	06/09/06	Internal Review	Enspier
Strawman	0.0.3	06/09/06	Internal Review	Enspier
Strawman	0.0.4	06/12/06	Internal Updates	Enspier
Strawman	0.0.5	06/12/06	Internal Updates	Enspier
Strawman	0.0.6	06/19/06	Updates per AWG	Enspier
Draft	0.0.7	07/12/06	Updates per internal review	Enspier
Draft	0.0.8	07/31/06	Updates per internal review	AWG
Draft	0.0.9	8/15/06	Updates per internal review	Enspier
Draft	0.0.10	08/16/06	Updates per internal review	AWG
Draft	0.0.11	08/18/06	Updates per internal review	AWG
Draft	0.0.12	08/28/06	Updates per internal review	AWG
Draft	0.0.13	08/28/06	Updates per internal review	AWG
Draft	0.0.14	08/29/06	Updates per internal review	AWG
Draft	0.0.15	08/31/06	Updates per internal review	AWG
Draft	0.0.16	08/31/06	Updates per internal review	AWG
Draft	0.1.0	08/31/06	Updates per public and internal review	Public
Draft	0.1.1	09/08/06	Updates per internal review	AWG
Draft	0.1.2	09/14/06	Updates per internal review	AWG
Draft	0.1.3	10/11/06	Updates per internal review	AWG
Draft	0.1.4	11/27/06	Updates per internal review	AWG
Draft	0.1.5	11/28/06	▪ Added section 1.3.3 ▪ Further updates to sections 4.5 and 4.6	AWG
Draft	0.1.6	12/4/06	▪	AWG

Editors

Chris Louden
Glenn Ballard
Jonathan Rich
Poornima Koka

Dave Silver
Treb Farrales
Rick Uhrig
Chris Broberg

Andrew Chiu
Brian Williams
Larry Fobian

Table of Contents

Tables

Figures

1 Introduction

1.1 Background

On August 27, 2004, Homeland Security Presidential Directive-12 (HSPD-12) - "*Policy for a Common Identification Standard for Federal Employees and Contractors*" was issued. HSPD-12 directed the promulgation of a new Federal standard for a secure and reliable form of identification issued by all Federal Agencies to their employees and contractors.

The HSPD-12 Implementation Executive Steering Committee (ESC) has requested establishment of several shared components with well-defined interfaces to assist agencies in meeting Personal Identity Verification (PIV) requirements. The HSPD-12 Implementation Architecture Working Group (AWG) convened under the auspices of the ESC to develop an architecture that defines shared component interfaces and interactions. The AWG based its work on analyses of PIV use cases.

The shared components provide agencies with a variety of options and resources to meet their HSPD-12 implementation requirements. An agency can implement a fully outsourced solution, leveraging shared components for every step in the process. In practice, many agencies will choose only the shared components they need, mixing shared components and agency components to implement their overall HSPD-12 solution.

The HSPD-12 Shared Component Architecture (SCA) supports, as necessary, Federal Information Processing Standard (FIPS) 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* as well as related documents such as National Institute of Standards and Technology (NIST) Special Publication 800-73, *Interfaces for Personal Verification*, NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification*, and NIST Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*. In addition, the architecture preserves compatibility with standards and specifications for existing systems that are related to HSPD-12, such as the Electronic Fingerprint Transmission Specification (EFTS).

In addition, this document does not supersede or contradict any existing NIST publication, and should be used in conjunction with existing policies and procedures.

1.2 Authority

This document has been developed on behalf of The Office of Governmentwide Policy and the HSPD-12 Executive Steering Committee in furtherance of their charter to implement HSPD-12 from a "national" perspective.

1.3 Shared Component Architecture (SCA)

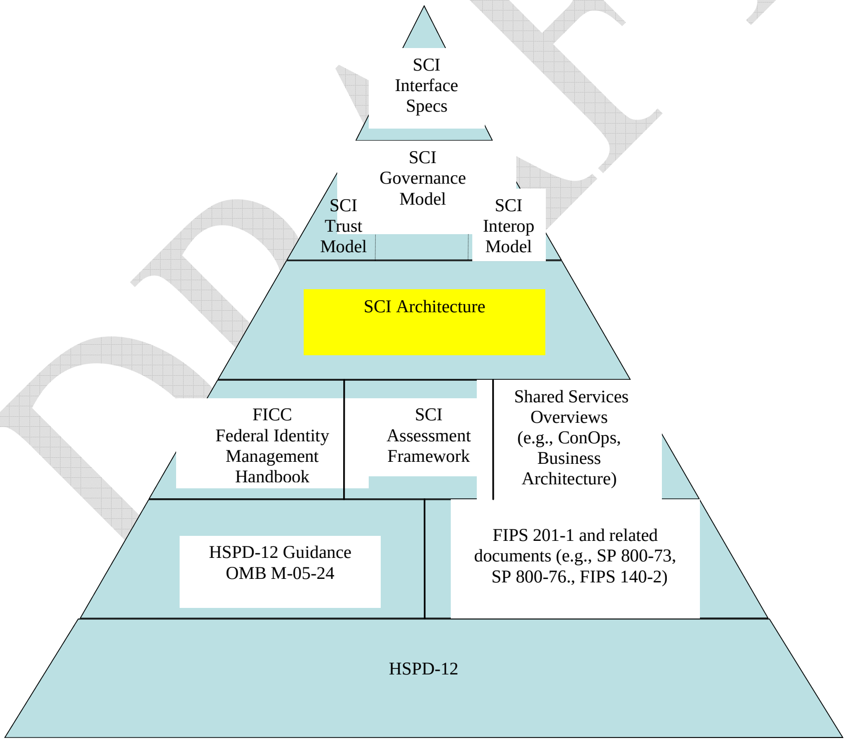
This document describes the SCA and captures Architecture Working Group (AWG) decisions based on relevant business processes and derived use cases. Decisions captured include:

- What architectural components are required;
- How and when architectural components interoperate to support all use cases; and
- How architectural components are technically constructed.

The SCA is instantiated as an operational Shared Component Infrastructure (SCI). A set of use cases, sequence diagrams, and activity diagrams depict all SCI interactions (see Section 4). The diagrams identify architectural requirements, missing specifications, and outsourcing options.

This document is one of many relevant to the SCI, as depicted in Figure 1-1.

Figure 1-1: SCI Documentation Hierarchy



1.3.1 Overview

The government requires an SCA that provides:

- **Componentization** – bundling of functions into commonly used “sub systems” for simplification, standardization, and consistency. Components are well defined, with clearly specified interactions and interrelationships.
- **Interoperability** – Agencies and Departments can use each other’s SCI components in accordance with their proven, standard interfaces. In doing so, there is assurance that SCI transactions are secure, robust, reliable, and consistent. This requires technical and policy interoperability at certain key points within the SCI.

An SCA with these characteristics allows:

- Competitive outsourcing for some components;
- Flexibility in servicing the diverse and unique needs of agencies; and
- Increased service utilization that lowers cost per process.

To support componentization, this document defines three (3) categories of SCI components:

- **Shared Components (Shared Services)** – various services to be shared government-wide that are the primary focus of this document. Shared components must be implemented in accordance with the SCA and applicable technical interface specifications. The shared components are:
  - *Enrollment Station Provider (ESP)* – identity proofs applicants in accordance with FIPS 201-1 standards and I-9 documentation and captures biometrics, including picture and 10-slap fingerprints.
  - *Systems Infrastructure Provider (SIP)* – manages full life cycle of the PIV card via Identity Management System (IDMS) and Card Management System (CMS) functionality.
  - *Production Service Provider (PSP)* – produces and personalizes PIV cards.
  - *Finalization Service Provider (FSP)* – finalizes personalization of PIV cards and completes issuance to the applicant.
- **Agency Components (Agency Systems)** – systems used by a single agency (i.e., not shared). Agency components may or may not already exist and must be implemented in accordance with the SCA and applicable technical interface specifications. Examples of agency components are:
  - An agency Human Resource (HR)/Personnel system.
  - An agency’s equivalent for a shared component not selected for use.
  - **Services** – resources external to the SCI used to complete tasks that tangentially pertain to or affect SCI processing. An example of a service is:
    - Background investigation service.

SCI Providers build and operate SCI components. There are two (2) types of SCI providers:

- **Shared Component Provider** – the provider can be a commercial entity or an agency. A shared component provider that offers a single solution of all shared components is a Bundled Service Provider (BSP).
- **Agency Component Provider** – the provider is an agency or agency contractor. An Agency component is used solely by the agency (i.e., not shared).

The AWG has designed the SCA to be flexible. It supports various service provision models (i.e., configurations) as may be needed over the long term. The spectrum of flexibility ranges from (a) an agency implementing an HSPD-12 solution comprised totally of shared components to (b) an agency implementing an HSPD-12 solution comprised of any mix of shared components and agency components. In all configurations, an agency can use services (e.g., background investigation) as needed. This flexibility ensures each agency can implement the solution best suited or available at the time (see [Business Arch]). The provision models supported by the SCA include[2]:

- **Use all shared components from multiple providers** – an agency uses all the available shared components in their overall HSPD-12 solution, using different providers. This requires the agency to deal with multiple shared component providers.
- **Use all shared components from a BSP** – an agency uses all the available shared components in their overall HSPD-12 solution, using a single provider (the BSP) for all the shared components. This allows an agency to deal with one shared component provider.
- **Use some (not all) shared components from multiple providers** – an agency uses some of the available shared components in their overall HSPD-12 solution, using different providers. This requires the agency to deal with multiple shared component providers. The agency uses its own (non-shared) system(s) in lieu of shared components not selected.
- **Use some (not all) shared components from one provider** – an agency uses some of the available shared components in their overall HSPD-12 solution, using a single provider for the selected set of shared components. This allows an agency to deal with one shared component provider. The agency uses its own (non-shared) system(s) in lieu of shared components not selected.

1.3.2 Scope

This document is limited to PIV card issuance, credentialing, and maintenance via a SCI. Only those processes and technical interoperations supporting that scope are addressed in detail. However, information beyond scope is included to provide useful context and facilitate understanding of the overall PIV environment. For example, authentication of end users with PIV cards for the purpose of physical access or logical access is outside the scope of this document, but is discussed to convey a more complete end-to-end business process.

The following sections are informational:

- Section 2, Component Overview; and
- Section 3, Business Process Overview

The following sections are normative per the authority cited in Section 1.2

- Section 4, Architecture Use Cases is normative

1.3.3 Context

The SCA is part of a larger, concerted effort to implement an HSPD-12 shared services solution. Therefore, in and of itself, the SCA does not define a complete, operational system. The SCA addresses secure, trusted technical interoperability amongst SCI components in accordance with [FIPS 201] and HSPD-12 business use cases. To achieve an operational system, an SCI governing authority must define and implement additional operational processes, procedures, policies, and rules. SCA supporting documents such as [SCI Trust], [SCI Interoperability], and [SCI Metadata] address these at a high-level, but appropriately defer some final operational details to an SCI governing authority. At an appropriate time, such a governing authority will facilitate all remaining tasks necessary to achieve an operational system. This includes, but is not limited to

1. Executing and managing contracts and/or agreements with SCI participants;
2. Publishing time tables and other business requirements and dependencies to SCI participants;
3. Determining and implementing transaction accounting and billing model(s);

[2] Note that the GSA service offering is different from this broader SCA solution.

4. Creating and publishing reference implementations and test harnesses for use in SCI component development;
5. Fully defining the SCI Assessment Framework;
6. Certifying SCI components using the SCI Assessment Framework;
7. Coordinating with the Federal Public Key Infrastructure Operational Authority (FPKIOA) to establish an SCI Trust Certificate Certification Authority;
8. Defining SCI Trust Certificate request procedures;
9. Finalizing SCI metadata content;
10. Assigning SCI participants unique values for certain metadata items;
11. Defining and implementing SCI metadata exchange policies and procedures; and
12. Ongoing oversight and monitoring of SCI participant compliance

1.3.4 SCI Security Principles

The SCI relies on a core set of security principles to protect program and transaction reliability, integrity, and privacy. See [SCI Trust] for details.

1.3.5 Privacy

HSPD-12 explicitly states that "protect[ing] personal privacy" is a requirement of the PIV system. Where applicable, the SCA, and the SCI it describes, adheres to all privacy requirements, in accordance with the spirit and letter of all privacy controls specified in, and referenced by [FIPS 201]. In addition, the SCA does not preclude agencies leveraging the SCI from complying with said privacy requirements.

1.4 Methodology

The SCA presented in this document is the result of the following methodology:

1. **Identification of Business Processes –** the various HSPD-12 business processes that the SCA needs to address were identified and analyzed;
2. **Identification of known components** – the various shared components required to provide a complete HSPD-12 solution were identified and initially defined;
3. **Creation of Use Cases** – one or more use cases for each business process was created;
4. **Analysis of Use Cases** – an iterative process was used to review and discuss use cases. Reviews included internal architect reviews and AWG reviews. Analysis addressed:
   a. Determination of component interaction and dependencies
   b. Refinement of business process definitions and flows
   c. Identification of potential new components
5. **Revision of Use Cases** – use cases were refined per analysis results;

1.5 Essential Terminology

This document uses the following terms to distinguish components:

1. **Shared Component Architecture** – the conceptual technical design of the HSPD-12 shared service solution. Providers must comply with the architecture and its associated technical interface specifications;
2. **Shared Component Infrastructure** –instantiation of the SCA. This is an operational environment where SCI components interoperate;
3. **Shared Component** – a component that is available for use by more than one agency, typically provided by a service provider; and
4. **Agency Component (Agency System) –** a component outsourced or operated by an agency for exclusive use by the agency (i.e., not shared with other agencies).

1.6 Essential Acronyms

This document uses the following acronyms extensively:

1. **SCA** – Shared Component Architecture
2. **SCI** – Shared Component Infrastructure
3. **ESP** – Enrollment Service Provider
4. **SIP** – Systems Infrastructure Provider
5. **PSP** – Production Service Provider
6. **FSP** – Finalization Service Provider
7. **FPKI SSP** – Federal Public Key Infrastructure Shared Service Provider
8. **CMS** – Card Management System
9. **IDMS** – Identity Management System

1.7 References

[Agency-SIP] Agency to System Infrastructure Provider Interface Specification
http://www.smart.gov/awg/documents/AgencytoSIPinterfaceSpec.pdf

[BPEL] *Business Process Engineering Language for Web Services;* Version 1.1; May 5, 2003
http://www-128.ibm.com/developerworks/library/specification/ws-bpel/

[EFTS] Electronic Fingerprint Transmission Specification; DOJ FBI Criminal Justice Information Services (CJIS); May 2, 2005
http://www.fbi.gov/hq/cjisd/iafis/efts71/efts71.pdf

[Business Arch] HSPD-12 Shared Services Business Architecture; GSA HSDP-12 Managed Services Organization; May 2, 2005

[Early Thinking] *HSPD-12 Implementation Architecture Working Group Concept Overview, "Early Thinking"*; Version 1.0; March 17, 2006

[ESP-SIP] Enrollment Service Provider to Systems Infrastructure Provider Interface Specification
http://www.smart.gov/awg/documents/ESPtoSIPinterfaceSpec.pdf

[Fingerprint] HSPD-12 Fingerprint Process Considerations & Research
http://www.smart.gov/awg/documents/HSPD12fingerprintProcess.pdf

[FIPS 201] FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* NIST, March 2006.
http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

[FPKI Arch] Federal Public Key Infrastructure (FPKI) Architecture Technical Overview, FPKI Operational Authority, October 2005
http://www.cio.gov/fbca/documents/FPKIAtechnicalOverview.pdf

http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

[HSPD-12] Homeland Security Presidential Directive/HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors;* August 27, 2004
http://csrc.ncsl.nist.gov/policies/Presidential-Directive-Hspd-12.html

[M-05-24] OMB Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, August 5, 2005
http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf

[NIST 800-73] NIST Special Publication 800-73, *Interfaces for Personal Identity Verification*, NIST, 800-73-1, March 2006. http://csrc.nist.gov/publications/nistpubs/800-73-1/sp800-73-1v7-April20-2006.pdf

[NIST 800-76] NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification*, NIST, February 2006. http://csrc.nist.gov/publications/nistpubs/800-76/sp800-76.pdf

[NIST 800-78] NIST Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, NIST, April 2005, http://csrc.nist.gov/publications/nistpubs/800-78/sp800-78-final.pdf

[NIST 800-87] NIST Special Publication 800-87, *Codes for the Identification of Federal and Federally Assisted Organizations*, NIST, January 2006. http://csrc.nist.gov/publications/nistpubs/800-87/sp800-87-Final.pdf

[OPM-IS] *Requesting OPM Personnel Investigations*; US Office of Personnel Management Investigations Service; May 2001 http://www.opm.gov/extra/investigate/IS-15.pdf

[SCI Interoperability] HSPD-12 Shared Component Infrastructure Technical Interoperability Model http://www.smart.gov/awg/documents/SCItechnicalIOmodel.pdf

[SCI Metadata] HSPD-12 Shared Component Infrastructure Metatdata Management http://www.smart.gov/awg/documents/SCImetadataManagement.pdf

[SCI Trust] HSPD-12 Shared Component Infrastructure Trust Model http://www.smart.gov/awg/documents/SCItrustModel.pdf

[SIP-PSP] PLACEHOLDER – Probably a reference to a Global Platform spec specific to the SCA

[SIP-FPKISSP] PLACEHOLDER – reference to SIP – FPKI SSP

2 Component Overview

This section provides a "module" view of the SCA. It defines (1) the shared components within the SCA, (2) agency components, including those that may be used in lieu of shared components, and (3) services used by agency and/or shared components.

2.1 Shared Components

2.1.1 Enrollment Service Provider (ESP)

ESPs enroll applicants using enrollments stations. An applicant enrolls at an ESP only after the applicant's agency affiliation is determined, and the agency authorizes enrollment.

Enrollment stations facilitate (a) identity proofing of applicants in accordance with [FIPS 201] standards and I-9 documentation, and (b) capture of biometrics, including picture and 10-slap fingerprints. The information captured is used for (1) background investigations, and (2) PIV card personalization. Personally identifiable information (PII) collected at the enrollment station, combined with the processes and procedures for identifying and verifying the applicant's identity, build a strong framework for achieving HSPD-12 control objectives.

Each enrollment station consists of the following components:

- digital camera;
- fingerprint scanner;
- document scanner;
- smart card reader; and
- computer.

Enrollment stations interface with the SIP (see Section 2.1.2) to receive and send information. The ESP retrieves applicant information from the SIP, including authorization to enroll. In addition, the ESP sends all enrollment data back to the SIP for further processing.

A trusted Enrollment Officer facilitates capture of documents and biometrics, as necessary. See [SCI Trust] for additional discussion regarding trusted SCI officers.

An enrollment station may technically interoperate with multiple SIPs – but only one SIP at a time (the SIP associated with the applicant's issuing agency, as indicated in the applicant's Reservation Number).

2.1.2 Systems Infrastructure Provider (SIP)

SIPs provide the software functionality required to manage PIV credentials. SIPs build, host, and operate software that provides critical IDMS and CMS functionality required for the issuance and maintenance of the PIV cards**.** In this context, SIPs act as application service providers. An agency's use of the SIP is optional. Additionally, an agency may choose to leverage its own infrastructure to provide equivalent SIP functionality.

The SIP performs the following functions on behalf of agencies:

1. All CMS functionality;
2. Unlocking of PIV cards at the FSP;
3. Loading of signed objects onto the PIV card at the FSP;
4. Tracking PIV credential state from affiliation, enrollment, suitability, production, finalization, and maintenance;

5. Interfacing with agency systems such as authoritative HR systems, and other shared components through standard interfaces; and
6. Auditing, Logging, and Accounting of transactions

The component interactions are:

1. The SIP accepts affiliation data from agency systems (e.g., personnel systems, contractor registries);
2. The SIP provides applicant information to the enrollment stations and receives corresponding enrollment data from the enrollment stations.
3. The SIP sends fingerprints to the agency system upon agency request;
4. The SIP accepts adjudication results from agency adjudicators, including authorization to begin PIV card production;
5. The SIP sends cardholder information to PSPs;
6. The SIP accepts the chip identifier (ID) used by each cardholder from the PSP;
7. The SIP unlocks PIV cards at the FSP; and
8. The SIP inserts signed objects on to the PIV card in the FSP card reader.

2.1.2.1 SIP Identity Management System (IDMS)

The IDMS is the central component that interacts either directly or indirectly with all other components of the HSPD-12 Architecture. Via the SIP interface, the IDMS receives a transaction from (1) the agency's authoritative data source with all the applicant information (there is no direct contact with the agency's data source), (2) the enrollment stations to receive identity proofing information and biometrics, and (3) the card management system to initiate activities related to card issuance and card lifecycle management.

2.1.2.2 SIP Card Management System (CMS)

The SIP CMS manages a PIV card throughout the card's full lifecycle of activities. The SIP CMS interfaces with the IDMS as well as the FPKI SSP certificate authority (CA), card printing station, and the PIV card itself. The SIP CMS manages the issuance and printing of a PIV card and the public key infrastructure (PKI) certificate (i.e., X.509 certificate) associated with that PIV card. The SIP CMS handles post issuance card updates, as well as card revocation, suspension, and personal identification number (PIN) unblocks.

2.1.3 Production Service Provider (PSP)

PSPs produce and personalize PIV cards. Personalization is limited to surface printing and electrical pre-personalization (i.e., load and instantiate) and does not include card activation. The PSP locks each PIV card with a transport card management key[3] (transport key) unique to each PIV card. The PSP then ships the PIV cards via United State Postal Service to an agency-designated location for finalization. Many discussions refer to finalization as issuance (i.e., confuse finalization with issuance). In fact, finalization is the last step in the issuance process.

An agency may use more than one PSP for PIV card production (via the SIP, which technically interoperates with the PSP on behalf of the agency). However, agency-PSP business arrangements are executed out-of-band, direct between the parties.

Accordingly, a SIP can technically interoperate with more than one PSP – but only one PSP at a time (as configured in the SIP by prior arrangement with the agency, or as optionally directed by the agency on a

[3] Although [FIPS 201] states that a card management key is optional, for SCA purposes, it is required.

per PIV card production request). SIP-PSP technical interoperation requires an established business relationship between the SIP and PSP – for such things as cryptographic key ceremony.

The PSP performs the following functions:

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

The component interactions are:

1. Via the SIP, the agency provides card print specifications, including visual security features;
2. The SIP and PSP share a transport key used during PIV card shipment;
3. The SIP sends cardholder information needed to print individual cards;
4. The SIP designates a location to deliver the cards after production;
5. The PSP sends the chip ID used for each cardholder to the SIP; and
6. The PSP ships PIV cards via United States Postal Service to the agency-designated FSP finalization stations, each PIV card locked with a transport key unique to it.

2.1.3.1 PSP Card Management System (CMS)

The PSP CMS is for PSP-internal use only. It should not be confused with the SIP CMS. The PSP CMS manages PIV cards while they are at the PSP. This includes printing and distribution of the PIV cards. In addition, the PSP CMS tracks card inventory (raw stock and distributed stock) for PSP control, audit, and ordering purposes.

2.1.3.2 PSP Card Printing System (CPS)

The PSP CPS instantiates a PIV card for a specific individual. This includes card surface personalization and electrical pre-personalization.

2.1.3.3 Card Inventory

The PSP maintains a card stock inventory of raw PIV cards.

2.1.4 Federal PKI Shared Service Provider (FPKI SSP)

The FPKI SSP issues digital certificates, manages keys associated with those certificates, and maintains up-to-date certificate status information. The FPKI SSP includes the CA for issuing certificates, key management capabilities, and the capability to provide certificate revocation status information via a Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP). An agency cannot use more than one FPKI SSP (via the SIP, which technically interoperates with the FPKI SPP on behalf of the agency).

2.1.5 Finalization Service Provider (FSP)

FSPs finalize personalization of the cards and complete issuance to the applicant. The same organization that handles ESP operations for an agency may also manage FSP operations. A finalization station may technically interoperate with multiple SIPs – but only one SIP at a time (the SIP associated with the applicant's issuing agency, as indicated in the applicant's Reservation Number).

The FSP performs the following functions:

1. Verifies applicant biometric;
2. Initializes the card into the SIP CMS;
3. Requests loading of signed objects onto the PIV card; and

4. Allows PIN selection by the verified cardholder.

The component interactions are:

1. The FSP receives the physical card from the PSP;
2. The FSP uses the SIP CMS to unlock the card;
3. The 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 applicant establishes their PIN on the PIV card using FSP components (e.g. Card Reader).

2.2 Agency Components

2.2.1 Logical Access Control Systems (LACS)

A LACS interfaces with PIV cards to provide cardholders access to federally controlled networks and information systems. A LACS obtains certificate revocation status information from the FPKI SSP via a CRL or OCSP. A LACS can receive additional provisioning information or attributes by sending the Federal Agency Smart Credential Number (FASC-N) from the certificate to the backend authentication system.

2.2.2 Physical Access Control Systems (PACS)

A PACS interfaces with PIV cards to provide cardholders access to federally controlled facilities. A PACS can also obtain certificate revocation status information from the FPKI SSP via a CRL or OCSP, or credential revocation status by sending the FASC-N from the Cardholder Unique Identifier (CHUID) to the backend authentication system. A PACS can also receive additional provisioning information or attributes by sending the FASC-N from the CHUID or the certificate to the backend authentication system

2.2.3 Agency System

Agency systems (e.g., HR or Personnel system) interface to the SIP to provide information for (1) maintenance and termination of person and sponsorship information, and (2) for requesting credential issuance, update, re-issuance and revocation. That is, the agency system feeds the SIP with the necessary personnel records in order to issue a PIV card and manage the PIV card's card life cycle. In order to interface with the SIP, the agency system requires enhancement to comply with [Agency-SIP]. An agency system may technically interoperate with only one SIP.

2.3 Services

An agency uses external services to accomplish certain tasks. This section discusses those services.

2.3.1 Background Investigation Services

The interests of the national security require that all persons privileged to be employed in the departments and agencies of the government shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States. This means that the appointment of each civilian employee in any department or agency of the government is subject to investigation. The scope of the investigation will vary, depending on the nature of the position and the degree of harm that an individual in that position could cause.

The OPM and the FBI conduct applicant background investigations on behalf of agencies. Agencies use the results of background investigations to determine suitability. The agency must interact directly with the OPM, or the FBI, or both depending upon the type of investigation required or as circumstances warrant[4]. The OPM and/or the FBI forward background investigation results to the requesting agency's adjudication authority for adjudication. The agency forwards its adjudication results to the SIP.

Suitability in this context is not about job skills, but rather is about lack of criminal history, an upstanding character, and an evidenced loyalty to the United States. These determinations come out in the background investigation. Suitability is in addition to proving who an individual is. The National Agency Check with Written Inquiries (NACI), or higher, helps agencies make this suitability determination regardless of their job skills that come out in the interviews and resume.

The final decision as to any employee's suitability for employment, as either a government employee or contractor, is exclusively with the agency's adjudication authority. At a minimum, adjudication requires results from the following:

- NACI; and
- FBI National Criminal History Check.

2.3.1.1 Office of Personnel Management (OPM)

OPM has delegated to agencies the authority to adjudicate the suitability of cases involving applicants and appointees who have undergone the required investigation for appointments subject to investigation by OPM.

OPM Investigations Service (OPM-IS) is responsible for receiving and processing investigative requests (e.g., NACI request). OPM-IS facilitates investigations by completing steps directly (e.g., NACI written inquiries) and/or by initiating requests to other entities (e.g., requesting an FBI name check, requesting an FBI National Criminal History Fingerprint Check). Typically, OPM-IS assembles investigation results and returns the results to the requesting agency adjudication authority.

Agencies with special agreements with OPM-IS can submit fingerprints directly to the FBI, and receive results directly from the FBI, separate from the investigative request submitted to OPM- IS. In this special-agreement scenario, an agency submits requests to both the OPM-IS and the FBI, and receives specific results from each. An agency avoids duplication of effort by indicating on the OPM-IS investigation request form that it submitted a request directly to the FBI.

In regards to a NACI, OPM-IS conducts the following:

- National Agency Check (NAC), which includes:
  - Security/Suitability Investigations Index (SII),
  - Defense Clearance and Investigation Index (DCII),
  - FBI Name Check (request submitted to FBI), and
  - FBI National Criminal History Fingerprint Check (request submitted to FBI).
- Written inquiries and searches of records covering specific areas of an individual's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities). Coverage includes:
  - Employment, 5 years,

[4] The SCA does not include a direct connection between SCI shared components (e.g., SIP) and investigation services because agencies already have this in place.

- Education, 5 years and highest degree verified,
- Residence, 3 years,
- References,
- Law Enforcement, 5 years

2.3.1.2 Federal Bureau of Investigation (FBI)

The FBI Criminal Justice Information Services (CJIS) Division conducts:

- Name Checks; and
- National Criminal History Fingerprint Checks.

The CJIS Division accomplishes this by using its Integrated Automated Fingerprint Identification System (IAFIS). IAFIS maintains the largest biometric database in the world, containing the fingerprints and corresponding criminal history information for more than 47 million subjects in the Criminal Master File.

The FBI returns investigation results to the OPM-IS or directly to the requesting agency adjudication authority if such an arrangement exists.

3 Business Process Overview

This section describes the business processes for implementing HSPD-12 requirements. Each business process gives an overview of the steps to be carried out by an agency and the shared service components to complete a particular HSPD-12 related task. The descriptions in this section are business-oriented rather than component-oriented, and accordingly show the overall flow between multiple components and the relative timing of their interactions from a business user's point of view.

The business processes described in this section are "prototypes" or samples of how an agency might choose to use the HSPD-12 shared components. The business processes were defined in order to verify that the design of the shared components included sufficient functionality to support a prototypical HSPD-12 process end-to-end. However, these business processes are not requirements or even recommendations on how an agency should use the shared service components.

Some processes described, especially the job-related ones for employees and contractors, do not attempt to cover the full process needed for the task, but rather cover solely those activities related to HSPD-12 requirements and the issuance/revocation of PIV cards. For example, the "Initial Card Issuance" process for employees and contractors described below is "complete" in the sense that it covers all of the steps needed under the HSPD-12 requirements including enrollment, investigation, adjudication, and card issuance. However, it does not attempt to include any detail about an agency's process for recruiting new staff nor all the steps needed for adjudicating unfavorable investigation results.

HSPD-12 business processes are divided into three (3) groups:

- **Cardholder Lifecycle Management**: processes related to the lifecycle of an employee or contractor as a cardholder at an agency (e.g., hiring, changing jobs, leaving a job).
- **PIV Card Usage**: processes related to the use of a PIV card and its contents for logical and physical access.
- **Credentials Lifecycle Management**: processes needed to make changes, reissue or renew an existing cardholder's PIV card.

The first two (2) groups, Cardholder Lifecycle Processes, and PIV Card Usage, are the primary focus of the HSPD-12 architecture and requirements. However, to fully implement the needed functionality, it is necessary to describe additional supporting processes for the handling and management of PIV cards and PKI certificates. These processes are included in the third group, "Credentials Lifecycle Management" to ensure the completeness of functional requirements of each shared service component and their assets.

Section 4, Architecture Use Cases, addresses SCI use cases. The use cases describe the collaboration between specific SCI components in greater detail than in the business processes. To provide traceability between the two (2) levels of information, each business process indicates the specific use case it is utilizing.

Table 3-1 provides complete list of business processes and their triggering events. Each business process includes a text description, a collaboration diagram indicating pictorially the flow of the process steps, a list of significant business considerations and assumptions on which the process depends, and a list of use cases implementing the process.

Table 3-1: Summary of Business Processes and the Events that Trigger Them

#	Process	Process Description	Events that Trigger Process
Cardholder Lifecycle Management			
BP-1.1	Initial Card Issuance	Investigate and provide appropriate agency credentials for new employee or contractor.	• Agency hires a new employee. • Agency hires a former agency contractor as an employee. • Agency accepts new contractor to staff a contract. • Agency accepts contractor that had been an employee.
BP-1.2	Job Change	Adjust agency credentials for existing employee or contractor moving to new position within agency.	• Employee changes jobs and/or responsibilities within agency. • Contractor is staffed against new contract involving a change in activities and/or responsibilities within same agency.
BP-1.3	Job Termination	Revoke credentials for employee ending their agency employment for retirement, job termination or any other reason.	• Agency terminates employee. (e.g. resigns, retires, fired) • Company terminates contractor. (e.g. resigns, retires, fired) • Company reassigns contractor outside the agency.
BP-1.4	Suspend Credentials	Suspend agency credentials temporarily, and later reactivate them or revoke them permanently, as needed.	• Cardholder is "missing" their PIV card and/or other credentials, but they do not yet believe that the "missing" credentials are "lost".
PIV Card Usage			
BP-2.1	Use PIV Card for Physical Access	Use PIV card, on-board digital certificate and biometrics for gaining physical access to federal buildings and sites.	• Cardholder enters their agency's building or campus for an appointment. • Cardholder enters another agency's building or campus for an appointment. • Cardholder has a class held in another agency's building. • Cardholder is on a temporary assignment that requires them to work in another agency's building temporarily.
BP-2.2	Use PIV Card for Logical Access	Use PIV card, on-board digital certificate and biometrics to access IT systems, and/or digital sign documents.	• Cardholder logs into their agency's IT network. • Cardholder logs into another agency's IT network to which they have permission to access. • Cardholder digitally signs a document or transaction.
PIV Card Lifecycle Management			
BP-3.1	Card Re-issuance	Issue new card to same cardholder following the loss, damage, theft or compromising of the original card.	• PIV card has been lost. • PIV card has been stolen. • PIV card has been damaged. • PIV card has been compromised • Cardholder name has changed. • Cardholder's organizational affiliation has changed.
BP-3.2	Card Renewal	Issue new PIV card to cardholder with an expired card.	• PIV card has expired or is within six (6) weeks of expiring.
BP-3.3	Card Maintenance	Update digital certificates and/or PIN on PIV card.	• Cardholder changes PIN. • Certificate on PIV card has expired or is close to expiring. • Agency wants to add new certificate for digital signing to cardholder's PIV card.

3.1 Cardholder Lifecycle Management

The purpose of the HSPD-12 initiative is to provide secure and reliable forms of identification for Federal employees and contractors. This first group of business processes covers the job-related processes necessary to issue and revoke PIV cards and related credentials to employees and contractors. There is a different process for each high-level HR event: hiring a new person, an existing person changing jobs, or terminating a person's employment. In addition, at times agencies need the ability to suspend and re-activate HSPD-12 related credentials but without requiring full termination of the federal employee or contractor involved.

3.1.1 Initial Card Issuance Process

The Initial Card Issuance process occurs when a new federal employee or contractor (applicant) is hired at an agency.

Here are the major steps taken in the initial card issuance process for a new hire:

(1) The issuing agency authorizes applicant enrollment and coordinates applicant visit to ESP.

(2) The ESP retrieves applicant data from the SIP, enrolls the applicant, and sends enrollment data back to the SIP.

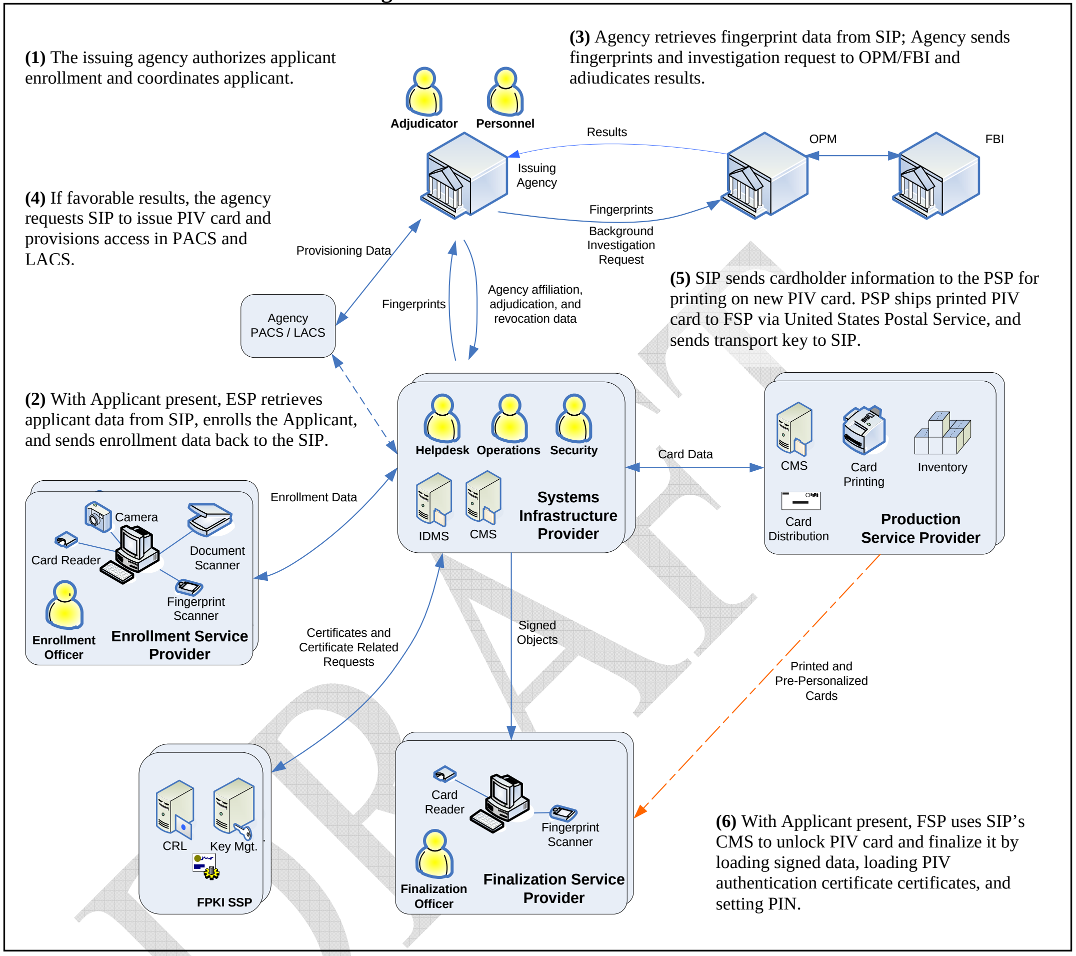
(3) Agency retrieves fingerprint data from the SIP. The agency sends fingerprints and background request to FBI/OPM for investigation, and adjudicates the results.

(4) If the FBI check is favorable and the background investigation is started, then the agency authorizes PIV card issuance by SIP. The agency also authorizes the applicant's physical and logical access to appropriate agency buildings, sites, and IT systems.

(5) The SIP sends cardholder information to the PSP and requests a new PIV card. When PIV card printing is completed, certain data about the PIV card is returned to the SIP, including which chip ID was used for this applicant. The PIV card is then locked with a transport key and shipped to the designated FSP via United States Postal Service.

(6) The FSP validates the applicant's identity, and then uses the SIP CMS to unlock the PIV card, load the objects signed by the SIP, and finalize the PIV card configuration. The PIV authentication certificate must be loaded at this time, and the PIV card's PIN set. The PIV card may be tested to confirm that all features are functioning correctly and it is issued to the applicant, now cardholder.

Figure 3-1: Initial Card Issuance



(1) The issuing agency authorizes applicant enrollment and coordinates applicant.

(2) With Applicant present, ESP retrieves applicant data from SIP, enrolls the Applicant, and sends enrollment data back to the SIP.

(3) Agency retrieves fingerprint data from SIP; Agency sends fingerprints and investigation request to OPM/FBI and adiudicates results.

(4) If favorable results, the agency requests SIP to issue PIV card and provisions access in PACS and LACS.

(5) SIP sends cardholder information to the PSP for printing on new PIV card. PSP ships printed PIV card to FSP via United States Postal Service, and sends transport key to SIP.

(6) With Applicant present, FSP uses SIP’s CMS to unlock PIV card and finalize it by loading signed data, loading PIV authentication certificate certificates, and setting PIN.

Business Assumptions & Considerations

1. Adjudication is the sponsoring agency's responsibility.
2. Typically, agency sponsors and the HR processes they follow will be different for employees vs. contractors (e.g. an HR Officer is the Sponsor for an employee when requesting a background check whereas for a contractor it is usually their Contracting Officer Technical Representative (COTR)).
3. The SIP cannot enroll an applicant or issue a PIV credential without the explicit authorization of an agency.
4. All PIV cards and related credentials must have an expiration date, and that date must not be more than five (5) years from the issuance date. The validity period of the on-board certificates cannot extend beyond the expiration date of the PIV card itself.
5. In addition, the PIV card expiration date for contractors should consider contract duration.
6. During finalization, the mandatory PIV authentication certificate must be added to the PIV card.
7. If the final result of the agency adjudication is unfavorable, the employee's PIV card will be revoked when the SIP receives such a message from the agency.

Use Cases for Process:

1. Agency - SIP:
    a. S-01 Authorize enrollment
    b. X-xx Revoke PIV Card
2. E-01 Sponsored Enrollment
3. Agency, use one of the following:
    a. I-01: OPM Centralized Investigation Services
    b. I-02: OPM & FBI Investigation Services
4. P-01 PIV Card Fulfillment
5. F-01 PIV Card Finalization

3.1.2 Change Job Process

A person can change jobs between agencies or within an agency. Changing jobs between agencies requires revocation of all PIV-related credentials issued by the old agency, and the issuance of new credentials by the new agency. A change in job within the same agency may or may not require a new PIV card to be re-issued. However, it is the responsibility of each agency to determine the need for re-issuance in each case, as they do currently with PACS/LACS credentials. A PIV card only needs to be re-issued if there are changes to information on the outside of the card or to the data or certificates stored on board.

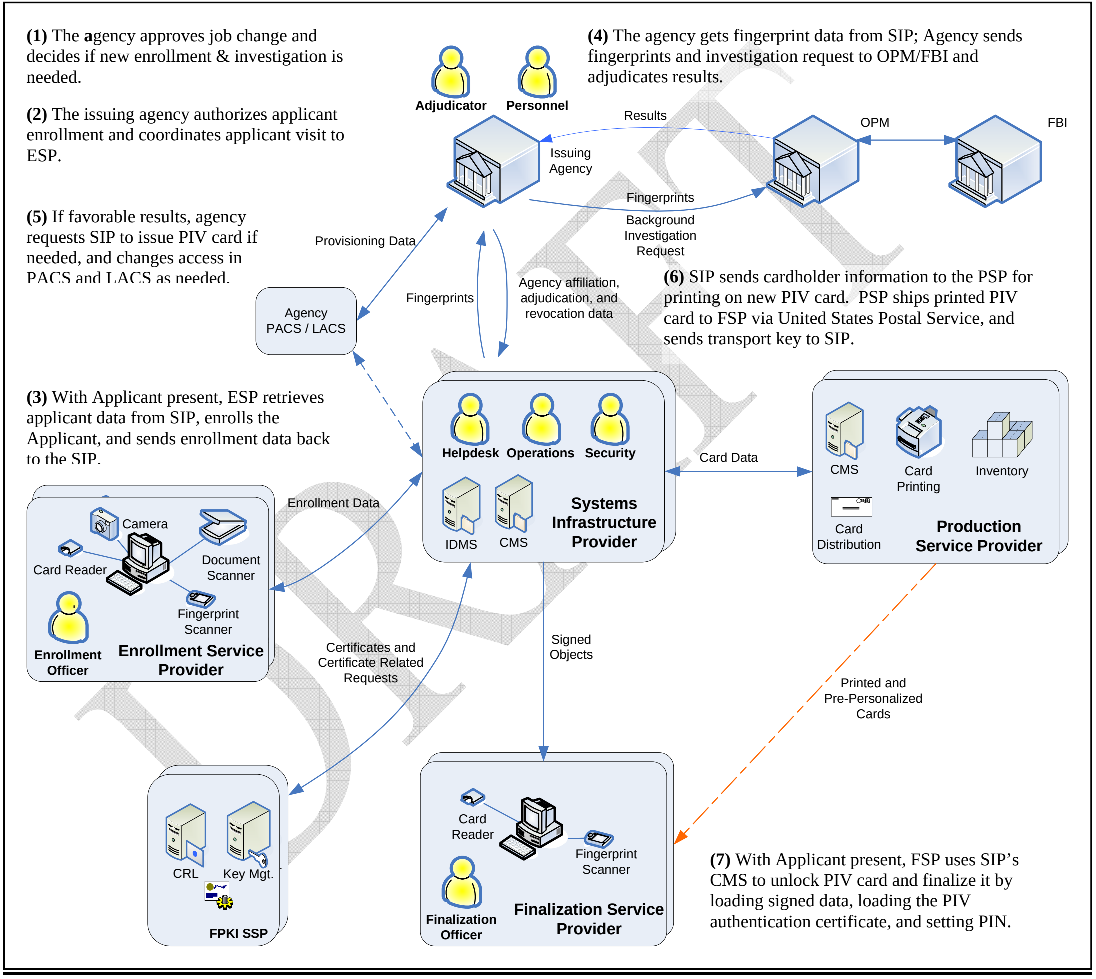
Here are the major steps taken in the re-issuance process for a job change:

(1) The agency approves the change in job assignment and decides whether a new enrollment and investigation is required.
(2) The issuing agency authorizes applicant enrollment and coordinates applicant visit to ESP.
(3) The ESP retrieves applicant data from the SIP, enrolls the applicant verifying them against existing biometrics, and sends enrollment data back to the SIP
(4) The agency gets fingerprint data from the SIP. The agency sends fingerprints and background request to FBI/OPM for investigation.
(5) The agency adjudicates new or existing investigation results. If favorable, the agency decides what credentials, including a PIV card, need to be revoked or issued.
(6) The SIP sends cardholder information to the PSP and requests a new PIV card. When PIV card printing is completed, PIV card data is returned to the SIP, including which chip ID was used

for the applicant. The PIV card is then locked with a transport key and shipped to the designated FSP.

(7) The FSP validates the applicant's identity, and then uses the SIP CMS to unlock the PIV card, load the signed objects, and finalize the PIV card configuration. The mandatory PIV authentication certificate must be loaded at this time, and the PIV card's PIN set. The PIV card may be tested to confirm that all features are functioning correctly and it is issued to the applicant, now cardholder.

Figure 3-2: Change Job Process



(1) The **a**gency approves job change and decides if new enrollment & investigation is needed.

(2) The issuing agency authorizes applicant enrollment and coordinates applicant visit to ESP.

(3) With Applicant present, ESP retrieves applicant data from SIP, enrolls the Applicant, and sends enrollment data back to the SIP.

(4) The agency gets fingerprint data from SIP; Agency sends fingerprints and investigation request to OPM/FBI and adjudicates results.

(5) If favorable results, agency requests SIP to issue PIV card if needed, and changes access in PACS and LACS as needed.

(6) SIP sends cardholder information to the PSP for printing on new PIV card. PSP ships printed PIV card to FSP via United States Postal Service, and sends transport key to SIP.

(7) With Applicant present, FSP uses SIP's CMS to unlock PIV card and finalize it by loading signed data, loading the PIV authentication certificate, and setting PIN.

Business Assumptions & Considerations:

1. When a person changes jobs within an agency, the agency must change PIV credentials only if the information for the credential has changed (e.g., [NIST 800-87] organizational ID being used in the FASC-N or the agency name on the face of the card, expiration date, expiration date).
2. [FIPS 201] does not require re-issuance of a PIV credential as the result of a job change within the same agency.
3. Most agencies do not re-issue identification as the result of a job change.

Use Cases used by Process, all are optional:

1. Agency - SIP:
   a. S-01 Authorize enrollment
   b. X-xx Revoke PIV Card
2. E-01 Sponsored Enrollment
3. Agency, use one of the following:
   a. I-01: OPM Centralized Investigation Services
   b. I-02: OPM & FBI Investigation Services
4. P-01 PIV Card Fulfillment
5. F-01 PIV Card Finalization

3.1.3 Job Termination

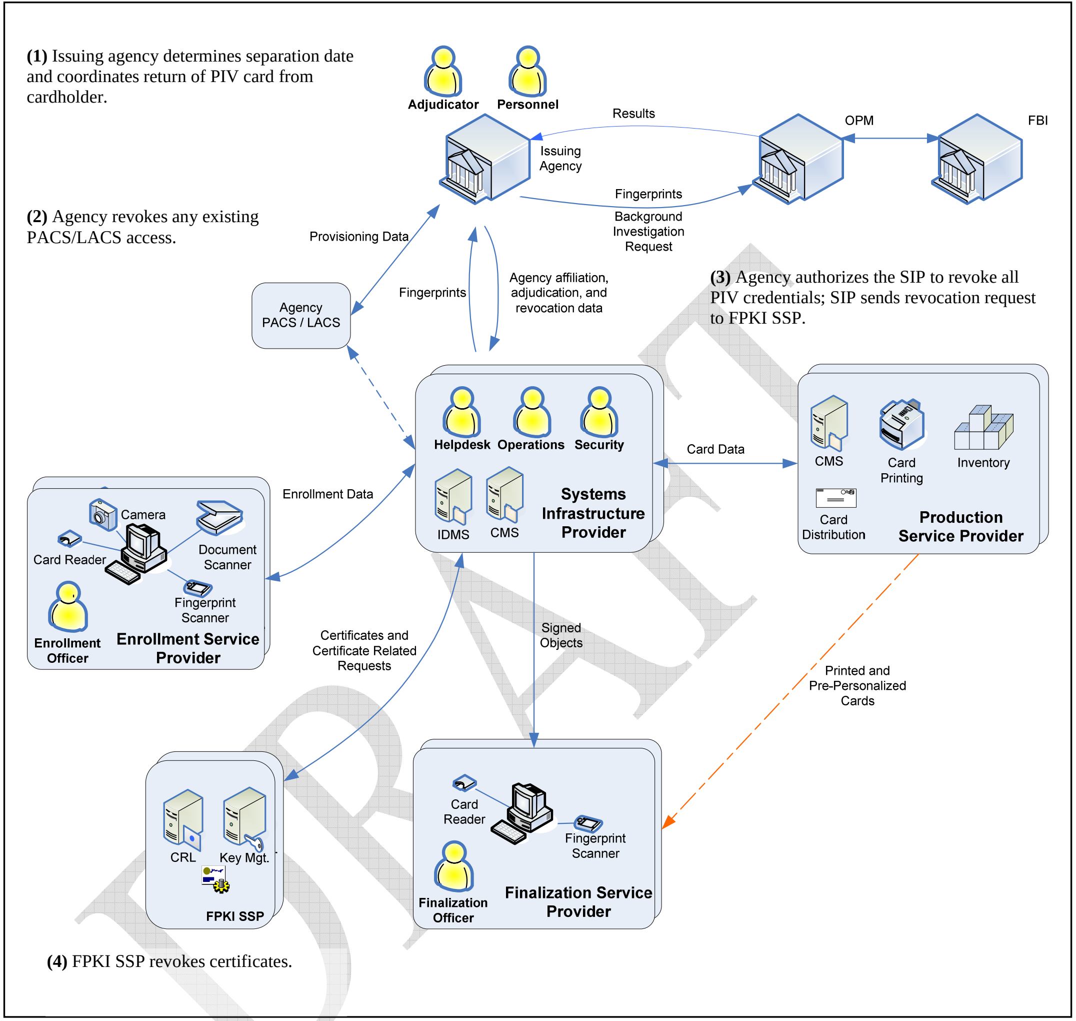
The Job Termination process is simple: all PIV credentials must be revoked. This includes the PIV card and its on-board digital certificates. The PIV card must be returned to the issuing agency and destroyed. In addition, the appropriate Certificate Authority (CA) for any on-board digital certificates must be notified of the revocation request of each certificate.

Unlike in the Suspend/Re-activate Process (described in the next section below), revocation of a PIV card and its certificates is not reversible.

Here are the major steps taken in the revocation process for a job termination:

(1) The issuing agency determines the cardholder’s separation date from the agency’s employment or contract and coordinates the return and disposal of the PIV card with the cardholder.
(2) The agency authorizes the SIP to revoke all PIV credentials as of the separation date; SIP marks the PIV card as revoked in its own system.
(3) The SIP sends revocation request about the cardholder’s certificates to the FPKI SSP.
(4) FPKI SSP revokes certificates.

Figure 3-3: Job Termination Process



(1) Issuing agency determines separation date and coordinates return of PIV card from cardholder.

(2) Agency revokes any existing PACS/LACS access.

(3) Agency authorizes the SIP to revoke all PIV credentials; SIP sends revocation request to FPKI SSP.

(4) FPKI SSP revokes certificates.

Business Assumptions & Considerations

1. All PIV credentials are revoked when a cardholder leaves their employment with the agency for whatever reason.
2. The PIV card shall be terminated if an employee separates (voluntarily or involuntarily) from Federal service. ([FIPS 201], Section 5.3.2.4)
3. The PIV card shall be terminated if an employee separates (voluntarily or involuntarily) from a Federal contractor. (([FIPS 201], Section 5.3.2.4)
4. The PIV card shall be terminated if a contractor changes positions and no longer needs access to Federal buildings or systems. (([FIPS 201], Section 5.3.2.4)
5. The PIV card shall be terminated if a cardholder is determined to hold a fraudulent identity. (([FIPS 201], Section 5.3.2.4)
6. The PIV card shall be terminated if a cardholder passes away. (([FIPS 201], Section 5.3.2.4)
7. Normal PIV card termination procedures shall ensure that the PIV card is collected and destroyed. (([FIPS 201], Section 5.3.2.4)
8. Normal PIV card termination procedures shall ensure that the PIV card itself is revoked. (([FIPS 201], Section 5.3.2.4)
9. Normal PIV card termination procedures shall ensure that any local databases are updated to reflect the change in status. (([FIPS 201], Section 5.3.2.4)
10. Normal PIV card termination procedures shall ensure that the CA is informed. (([FIPS 201], Section 5.3.2.4)
11. Normal PIV card termination procedures shall ensure that the certificate corresponding to PIV authentication key on the PIV card is revoked. (([FIPS 201], Section 5.3.2.4)
12. Normal PIV card termination procedures shall ensure that CRL include the appropriate certificate serial numbers. (([FIPS 201], Section 5.3.2.4)
13. Normal PIV card termination procedures shall ensure that OCSP responders shall be updated so that queries with respect to certificates on the PIV card are answered appropriately. (([FIPS 201], Section 5.3.2.4)

Use Cases used by Process:

1. Agency - SIP:
   a. X-xx Revoke PIV Card
2. SIP-FPKI SSP:
   a. X-xx Revoke certificates

3.1.4 Suspend Credentials Process for Employees

The Suspend Credentials Process is similar to the Job Termination Process except that "suspending" a cardholder's credentials can be reversed by a "reactivation" request without terminating the employee. Suspending a cardholder's credentials requires a SIP to suspend or revoke all PIV credentials in such a way that they can be reactivated if needed. An agency can decide to reactivate the suspended credentials or suspend them permanently by revoking them.

In some cases, it is not possible to "suspend" PIV-related credentials. Most notably, in some cases digital certificates can only be revoked, not suspended. As a result, each SIP must indicate whether they can support the suspension and reactivation of a PIV card.

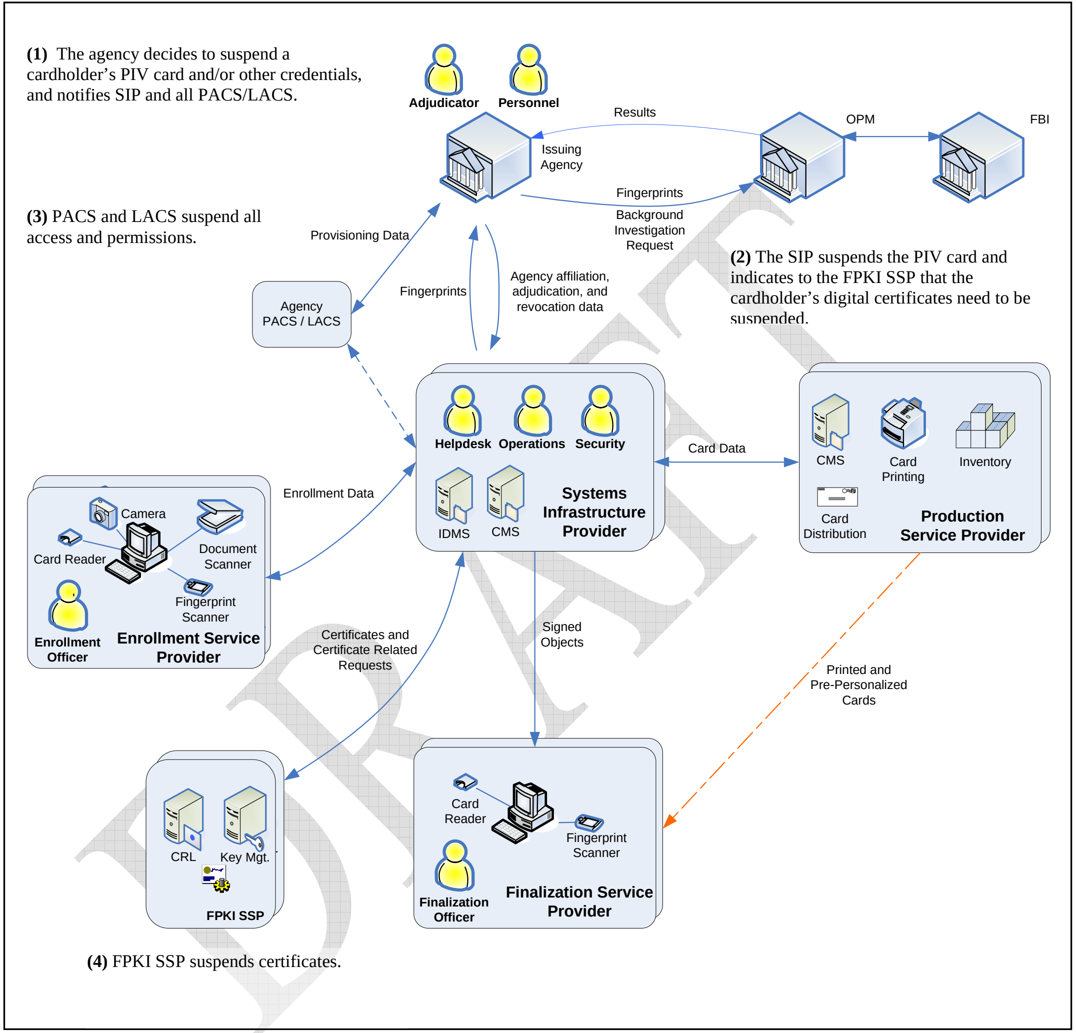
Here are the major steps taken in the suspend process:

(1) The agency decides to suspend a cardholder's PIV card and/or other credentials and notifies SIP and all PACS/LACS.

(2) The SIP suspends the PIV card and indicates to the FPKI SSP that the cardholder's digital certificates need to be suspended.

(3) PACS and LACS suspend all access.
(4) FPKI SSP suspends certificates.

Figure 3-4: Suspend Credentials Process for Employees



(1) The agency decides to suspend a cardholder’s PIV card and/or other credentials, and notifies SIP and all PACS/LACS.

(3) PACS and LACS suspend all access and permissions.

(2) The SIP suspends the PIV card and indicates to the FPKI SSP that the cardholder’s digital certificates need to be suspended.

(4) FPKI SSP suspends certificates.

Business Assumptions & Considerations

1. Supporting suspend and reactivate is an agency decision. Many agencies may choose not to support this process
2. Where supported, the agency must indicate in advance if PIV cards can be suspended and reactivated.

Use Cases used by Process:

1. Agency - SIP:
    a. X-xx Suspend PIV Card
    b. X-xx Reactivate PIV Card
2. SIP-FPKI SSP:
    a. X-xx Suspend certificates
    b. X-xx Reactivate certificates

3.2 PIV Card Usage

3.2.1 Card Issuer Validation and Provisioning Services

This process describes the use of a PIV card for authentication when requesting access to buildings, areas within a building, and other physical sites (PACS) and IT networks and applications (LACS) managed or controlled either by the cardholder's own agency or by another federal agency.

Authentication of the PIV card and the cardholder can be done locally by:

- **Simple flash pass** – where the card looks good to the guard and the picture seems to match (PACS only);and
- **Using PIV card technologies** – requiring PIN entry to prove ownership; comparing fingerprints to those stored on the PIV card; checking issuer signatures; using the certificates (PACS and LACS).

These decisions, along with who can and cannot enter a facility or application, are made by local security officials who weigh risk with efficiency, and the decisions are often modified to meet changing threat conditions. Regarding applications, the official is someone with authority to grant and provision access to the application, and possibly determine which roles get access.

The PIV architecture can add the following capabilities to this post issuance card usage:

- The ability to check the current and continued validity of the PIV card; and
- The ability to obtain additional information that may be pertinent in registry or in making the overall access decision.

The information on, and the validity of, a PIV card is based on the conditions that were in effect when the PIV card was issued. Changes to this information during the life of that PIV card can invalidate some of the information on it or invalidate the PIV card itself. For example, a subsequent termination of employment or a lost or stolen PIV card affects the current validity of the PIV card and its use in authenticating the cardholder.

In addition, attributes needed to determine access, such as current vetting status, might not be available from the PIV card itself. These types of information, when inserted onto card media, cause either costly re-issuance when they change or require PIV card modifications that often require complex infrastructures and work flow solutions. Agencies must weigh these factors when determining additional PIV card content.

The capability to address some of these issues is provided by different aspects of the PIV architecture under the concept of a *Backend or Issuer Authentication Service*. These services allow trusting parties, whether during logical or physical access, to obtain:

- The current status of a PIV card; and
- Additional information to use in making access determinations.

These services are:

- The CA CRL or OCSP responder for PKI certificates validation; and
- A Card Issuer Service to provide the current validation of a PIV card and to provide additional information as required for access of the cardholder.

Either service may be used during the authentication process or on a periodic basis for cardholders who have been provisioned to a local PACS/LACS registry. In addition, the Card Issuer Service can provide information pertinent at the time of initial access or provisioning, as required. This additional information is defined as data on the PIV card that can be used to:

- Enroll/register them in a local system; and
- Apply local rules to determine access or access level.

3.2.1.1 Use PIV Card for authentication during Physical Access

This process describes the use of a PIV card for authentication when requesting physical access to buildings and other sites, whether controlled either by the cardholder's own agency or by another federal agency. The processes are:

- **Process A** – validate PIV card and get information using FASC-N; and
- **Process B** – validate PIV card using certificate.

Each process begins when the Cardholder offers the PIV card for registry or on a onetime basis for validation of a visitor. Process A can be run after Process B to get additional information using the FASC-N in the certificate. Process A-3 to A-6 can be run periodically if the FASC-N is stored in the PACS Registry. Process B-1 can be run periodically if the certificate is stored in the PACS registry.

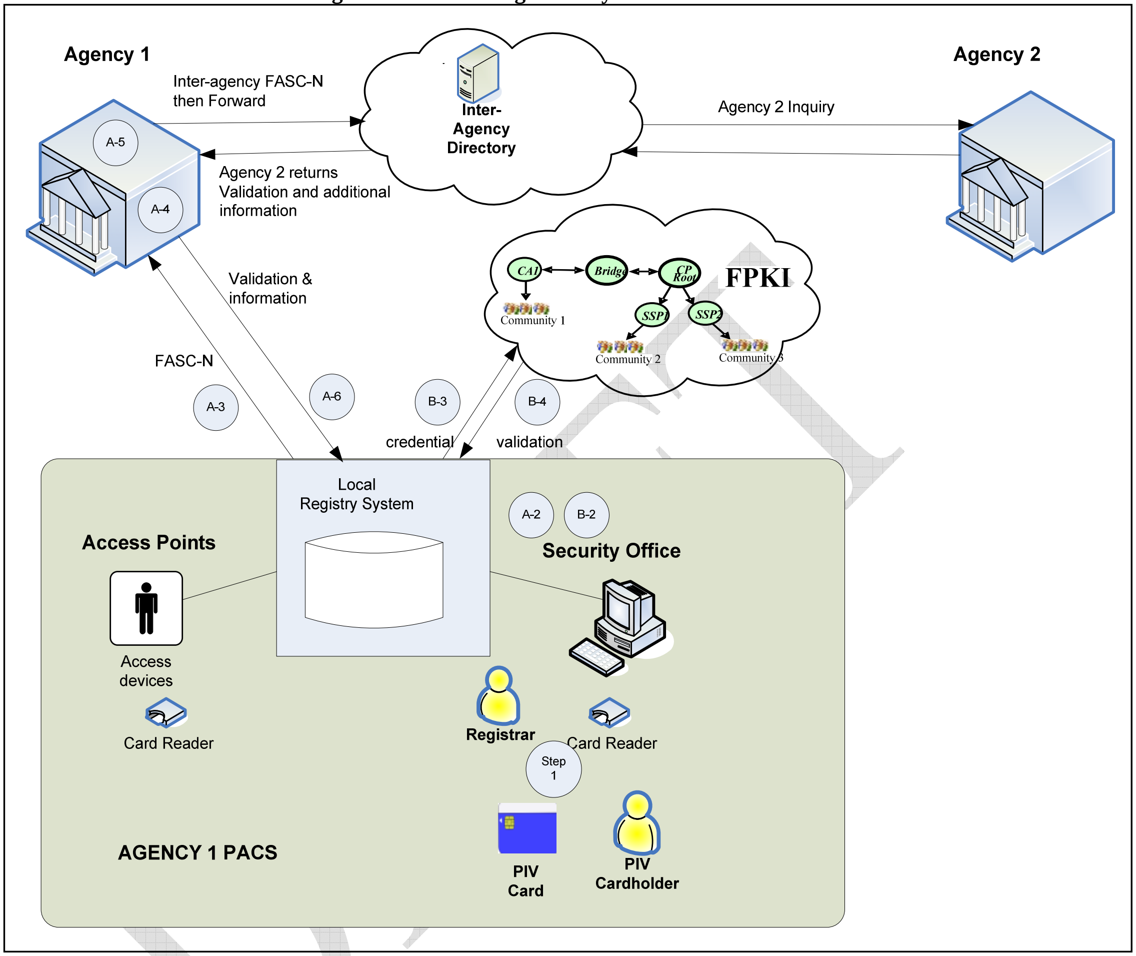
Process A

1. A-2 – the FASC-N is obtained from the contact or contactless chip.
2. A-3 – the FASC-N is passed to the PACS Agency (Agency 1).
3. A-4 – the PACS agency interface evaluates the FASC-N.
4. A-5 – if the agency in the FASC-N is Agency 1 (interagency) then the inquiry is performed on the agency store for current validity of the card and additional information can be obtained for local registry and access evaluation. Otherwise, if the agency is another agency (i.e., inter-agency) the inquiry is sent to the appropriate agency using information in the Inter-agency directory.
5. A-6 – validation and information are returned.

Process B

1. B-2 – the credential is obtained from the contact chip.
2. B-3 – the credential is determined to be from a trusted source and credential information is sent to an intra or interagency OCSP.
3. B-4 – valid/invalid is returned.

Figure 3-5: Card Usage for Physical Access



Business Assumptions & Considerations

1. PACS cannot provision building access for cardholders beyond the expiration date of the PIV card presented.
2. PACS should at least periodically check for revocation of both agency and non-agency cardholders.

Use Cases used by Process:

1. U-01 Validate credential for Physical Access.
2. U-02 Provide additional information for Physical Access Systems.

3.2.1.2 Use PIV Card for authentication during Logical Access

This process describes the use of a PIV card for authentication when requesting logical access to IT systems, whether controlled either by the cardholder's own agency or by another federal agency.

This process is nearly the same as with the PACS except the certificate is the primary technology to:

- Validate certificate; and
- Additional information for provisioning or authorization.

These cases either can stand alone or can be done sequentially.

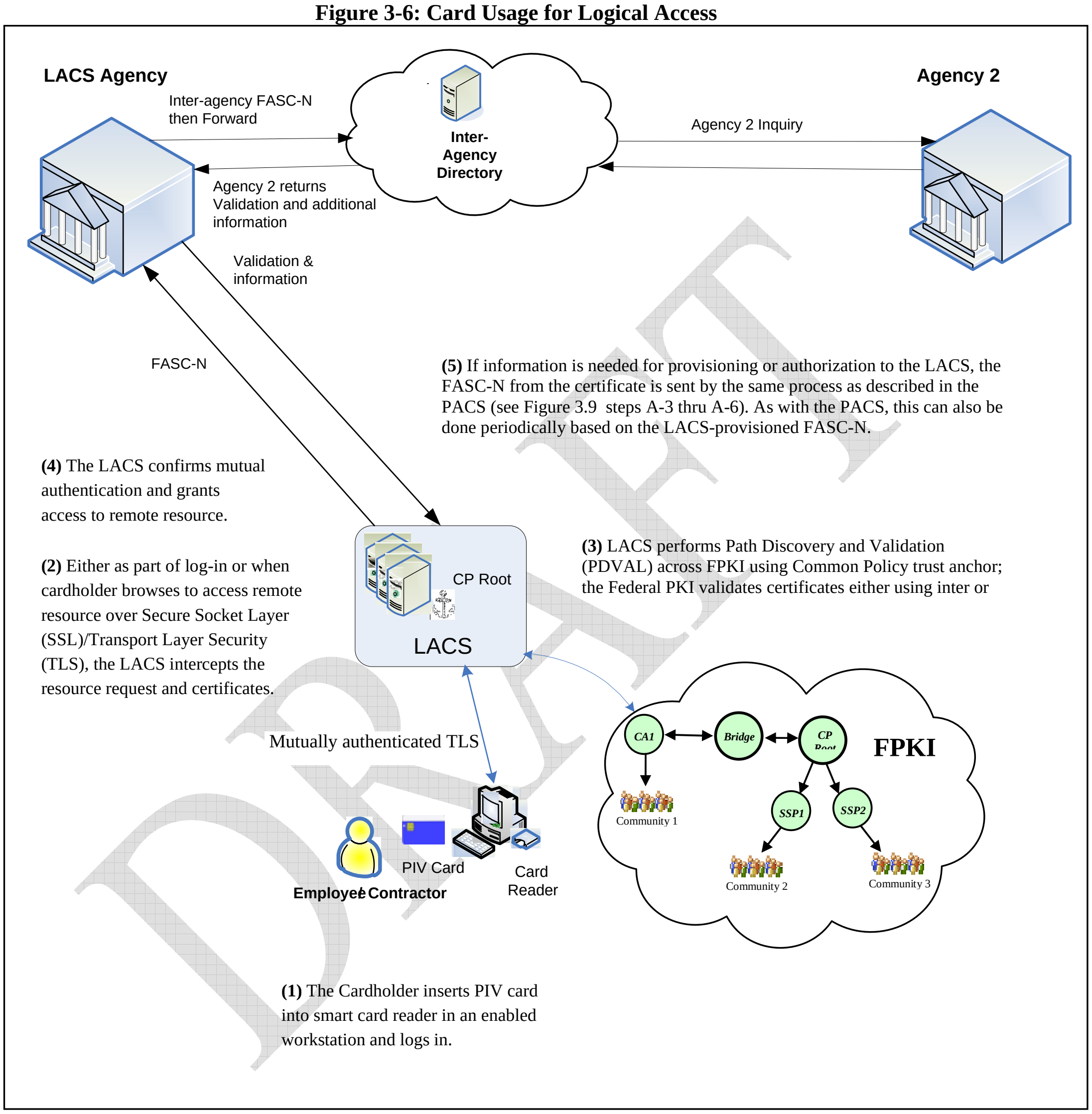
Here are the major steps taken in the authentication process for logical access:

(1) Validate certificate - see Figure 3-6, steps 1 thru 4

(2) Provide additional information - Step 5 describes the same process used for obtaining additional information using the certificate FASC-N as was used in the PACS. This is optional and is probably not done unless the LACS:
  - Needs to provision the certificate holder for continued use of the IT system; and
  - Needs additional information to determine access privileges for the credential holder.

Note that even if some of the registry information can be obtained from the chip, most commercial browser software, while able to use hardware certificates automatically for cryptographic logon, do not offer a similar built-in means to read other information on the chip.

Figure 3-6: Card Usage for Logical Access



(5) If information is needed for provisioning or authorization to the LACS, the FASC-N from the certificate is sent by the same process as described in the PACS (see Figure 3.9 steps A-3 thru A-6). As with the PACS, this can also be done periodically based on the LACS-provisioned FASC-N.

(4) The LACS confirms mutual authentication and grants access to remote resource.

(2) Either as part of log-in or when cardholder browses to access remote resource over Secure Socket Layer (SSL)/Transport Layer Security (TLS), the LACS intercepts the resource request and certificates.

(3) LACS performs Path Discovery and Validation (PDVAL) across FPKI using Common Policy trust anchor; the Federal PKI validates certificates either using inter or

(1) The Cardholder inserts PIV card into smart card reader in an enabled workstation and logs in.

Business Assumptions & Considerations

1. Digital certificates on board a PIV card cannot be used without the cardholder providing a PIN.

Use Cases used by Process:

1. U-03 Validate credential for Logical Access.
2. U-04 Provide additional information for Logical Access.

3.3 Credentials Lifecycle Management

3.3.1 PIV Card Re-issuance

The PIV Card Re-issuance Process occurs when a PIV card has been lost, stolen, compromised or damaged, and a cardholder requests a replacement PIV card. A cardholder must be re-enrolled with new biometric data, and the agency must also verify whether a new background investigation is needed. The on-board PIV authentication certificate must be revoked.

Here are the major steps taken in the re-issuance process:

(1) The cardholder requests the agency to re-issue a PIV card. The agency requests the SIP to revoke the old PIV card, and authorizes re-enrollment of the cardholder. The SIP revokes the old PIV card and the agency coordinates cardholder visit to ESP.

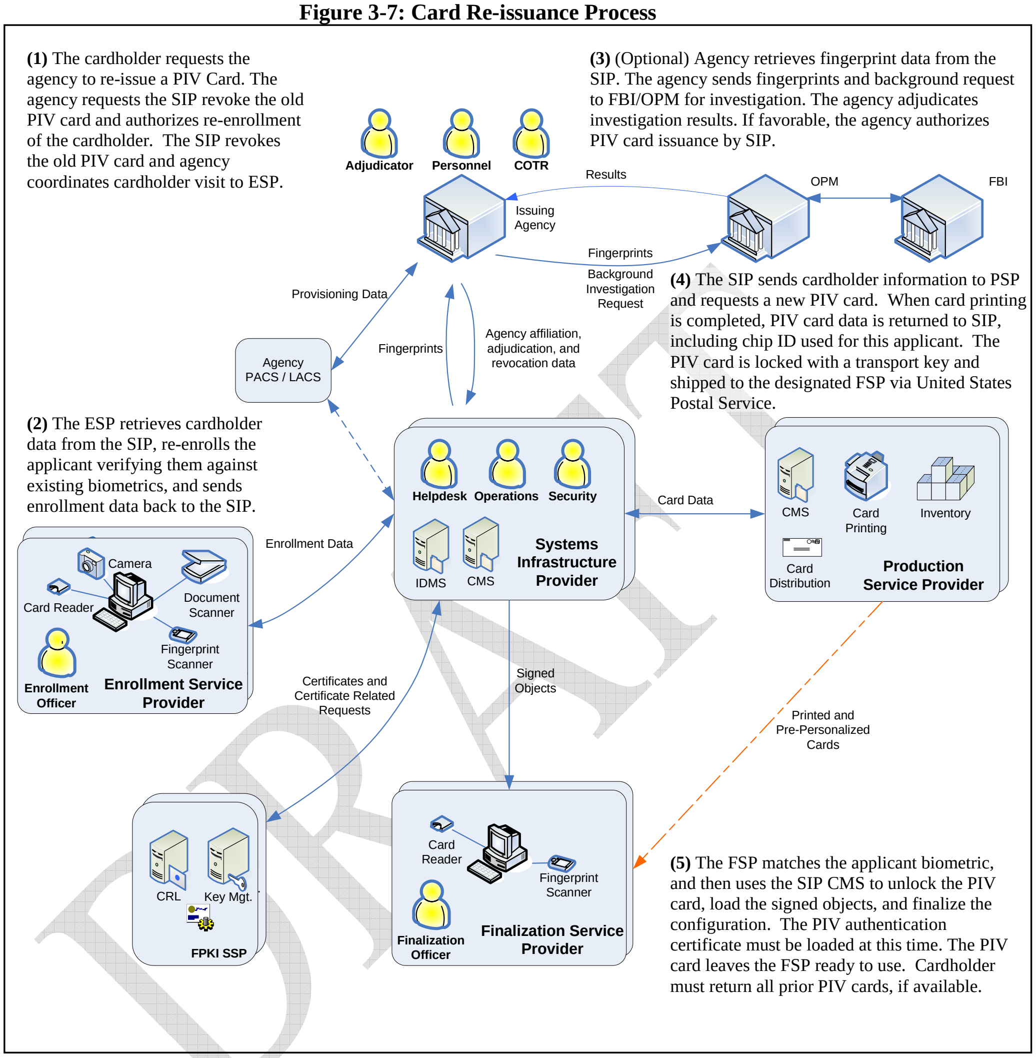
(2) The ESP retrieves cardholder data from the SIP, re-enrolls the applicant verifying them against existing biometrics, and sends enrollment data back to the SIP.

(3) (Optional) Agency retrieves fingerprint data from the SIP. The agency sends fingerprints and background request to FBI/OPM for investigation. The agency adjudicates investigation results. If favorable, the agency authorizes PIV card issuance by SIP.

(4) The SIP sends cardholder information to the PSP and requests a new 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 via United States Postal Service.

(5) The FSP matches the applicant biometric, and then uses the SIP CMS to unlock the PIV card, load the signed objects, and finalize the configuration. The PIV authentication certificate must be loaded at this time. The PIV card leaves the FSP ready for use. The cardholder must return all prior PIV cards, if available.

Figure 3-7: Card Re-issuance Process



(1) The cardholder requests the agency to re-issue a PIV Card. The agency requests the SIP revoke the old PIV card and authorizes re-enrollment of the cardholder. The SIP revokes the old PIV card and agency coordinates cardholder visit to ESP.

(2) The ESP retrieves cardholder data from the SIP, re-enrolls the applicant verifying them against existing biometrics, and sends enrollment data back to the SIP.

(3) (Optional) Agency retrieves fingerprint data from the SIP. The agency sends fingerprints and background request to FBI/OPM for investigation. The agency adjudicates investigation results. If favorable, the agency authorizes PIV card issuance by SIP.

(4) The SIP sends cardholder information to PSP and requests a new PIV card. When card printing is completed, PIV card data is returned to SIP, including chip ID used for this applicant. The PIV card is locked with a transport key and shipped to the designated FSP via United States Postal Service.

(5) The FSP matches the applicant biometric, and then uses the SIP CMS to unlock the PIV card, load the signed objects, and finalize the configuration. The PIV authentication certificate must be loaded at this time. The PIV card leaves the FSP ready to use. Cardholder must return all prior PIV cards, if available.

Business Assumptions & Considerations

1. In order to re-issue a PIV card, the agency must revoke the existing PIV card and its PIV authentication certificate as well as any associated credentials. In addition, a cardholder must be re-enrolled and provide a new set of biometrics for use on the new card.
2. If possible, the old PIV card should be collected from the cardholder during card finalization at the FSP (or before), and returned to the issuing agency for disposal.

Use Cases used by Process:

1. Agency - SIP:
   a. S-01 Authorize enrollment
   b. X-xx Revoke PIV Card
2. E-01 Sponsored Enrollment
3. (Optional) Agency, use one of the following:
   a. I-01: OPM Centralized Investigation Services
   b. I-02: OPM & FBI Investigation Services
4. P-01 PIV Card Fulfillment
5. F-01 PIV Card Finalization

3.3.2 PIV Card Renewal

The PIV Card Renewal Process occurs when a PIV card needs to be renewed because it is about to expire. Generally, the PIV card's expiration should coincide with five (5) years elapsing or the need to re-investigate the cardholder according to OPM guidelines.

PIV card renewals always require the revocation of all prior PIV-related credentials by the issuing agency, and the collection of the old PIV card.

Here are the major steps taken in the renewal process:

(1) (Optional) The issuing agency authorizes applicant enrollment and coordinates applicant visit to ESP.

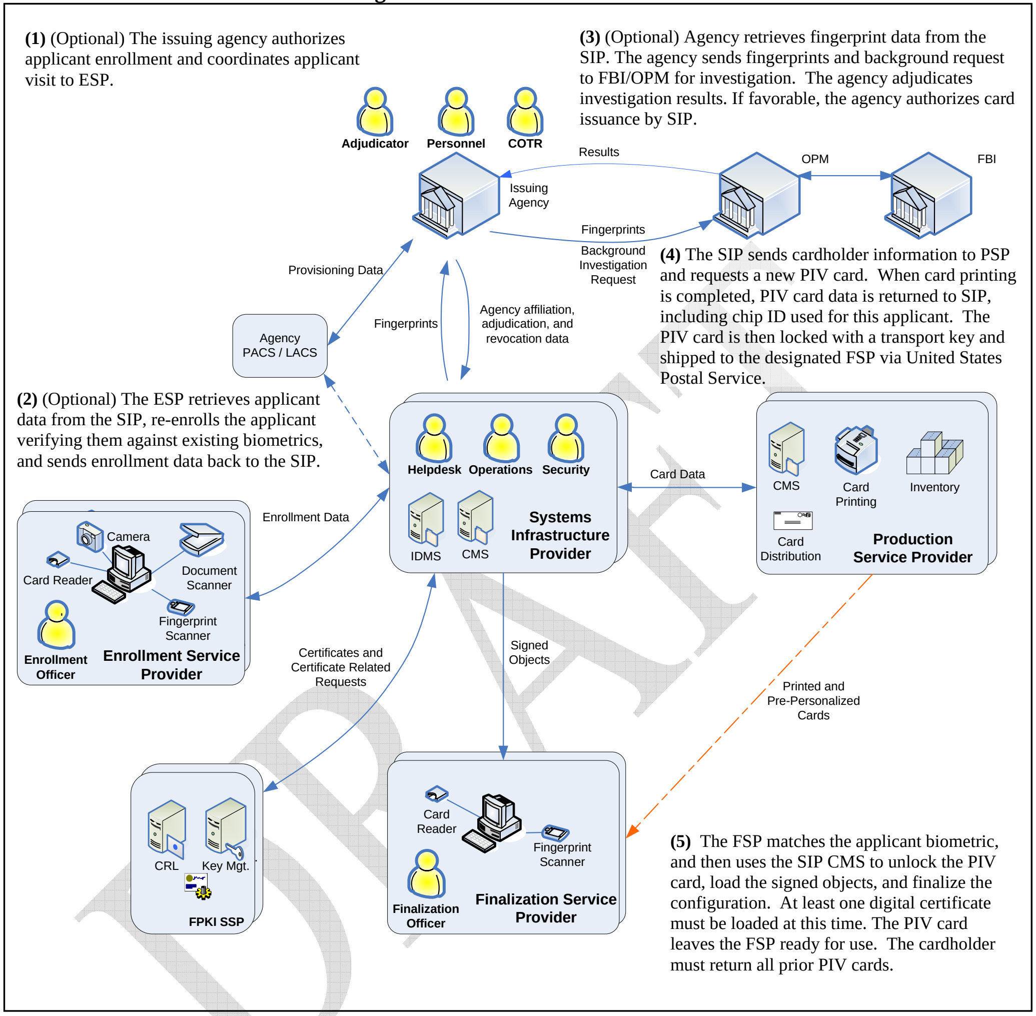
(2) (Optional) The ESP retrieves applicant data from the SIP, re-enrolls the applicant verifying them against existing biometrics, and sends enrollment data back to the SIP.

(3) (Optional) Agency retrieves fingerprint data from the SIP. The agency sends fingerprints and background request to FBI/OPM for investigation. The agency adjudicates investigation results. If favorable, the agency authorizes card issuance by SIP.

(4) The SIP sends cardholder information to the PSP and requests a new 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 via United States Postal Service.

(5) 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 PIV authentication certificate must be loaded at this time. The card leaves the FSP ready to use. The cardholder must return all prior PIV cards.

Figure 3-8: Card Renewal Process



(1) (Optional) The issuing agency authorizes applicant enrollment and coordinates applicant visit to ESP.

(2) (Optional) The ESP retrieves applicant data from the SIP, re-enrolls the applicant verifying them against existing biometrics, and sends enrollment data back to the SIP.

(3) (Optional) Agency retrieves fingerprint data from the SIP. The agency sends fingerprints and background request to FBI/OPM for investigation. The agency adjudicates investigation results. If favorable, the agency authorizes card issuance by SIP.

(4) The SIP sends cardholder information to PSP and requests a new PIV card. When card printing is completed, PIV card data is returned to SIP, including chip ID used for this applicant. The PIV card is then locked with a transport key and shipped to the designated FSP via United States Postal Service.

(5) The FSP matches the applicant biometric, and then uses the SIP CMS to unlock the PIV card, load the signed objects, and finalize the configuration. At least one digital certificate must be loaded at this time. The PIV card leaves the FSP ready for use. The cardholder must return all prior PIV cards.

Business Assumptions & Considerations

1. A cardholder shall be allowed to apply for a renewal starting six weeks prior to the expiration of a valid PIV card and until the actual expiration of the card.

Use Cases used by Process:

1. Agency - SIP:
    a. S-01 Authorize enrollment
    b. X-xx Revoke PIV Card
2. E-01 Sponsored Enrollment
3. Agency, use one of the following:
    a. I-01:OPM Centralized Investigation Services
    b. I-02: OPM & FBI Investigation Services
4. P-01 PIV Card Fulfillment
5. F-01 PIV Card Finalization

3.3.3 PIV Card Maintenance Process

The PIV Card Maintenance process covers changes to be made to a PIV card’s on-board credentials, such as digital certificates and PIN. Besides the required authentication certificate, a PIV card can hold additional certificates including ones for digital signing and encryption. New certificates for digital signing and encryption can be added either at Finalization when the PIV card is first issued (see Initial Card Issuance Process) or afterwards as part of this process, the PIV Card Maintenance Process.

In addition, the PIV card’s PIN for accessing on-board biometric data and certificates can be modified at the discretion of the cardholder, and without prior authorization of their agency. However, reset of a forgotten PIN requires an interface to the SIP.

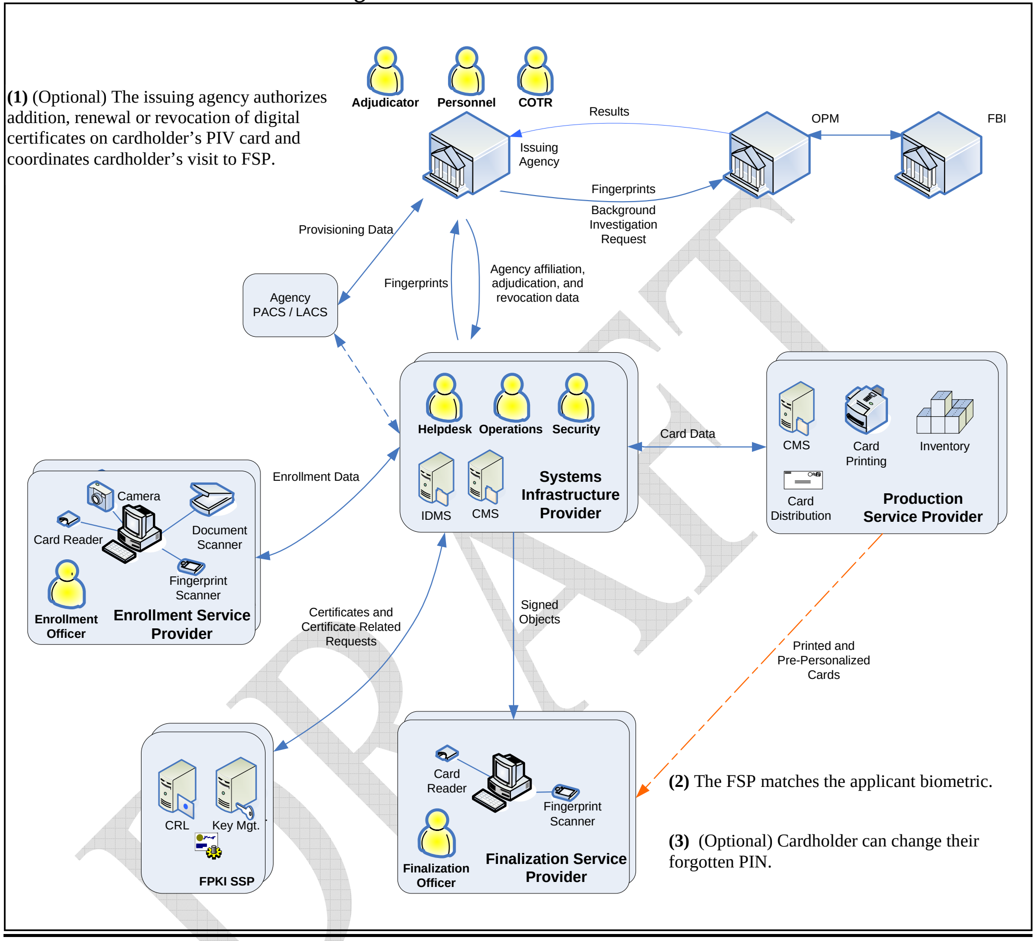
All certificates have specific expiration dates that either coincide with the expiration date of the PIV or are shorter (e.g., three (3) years for certificates vs. five (5) years for employee PIV cards). Therefore, in many cases certificate renewals have to be handled separately from PIV card renewals by issuing new certificates and revoking the old ones.

Changes to a PIV card’s on-board certificates and resetting a forgotten PIN can always be done at the finalization station provided by the FSP. In the future, some SIPs may provide a portal allowing cardholders to add or delete digital certificates and reset their PIN if there is access to a workstation with a compliant PIV card reader.

Here are the major steps for maintaining certificates or resetting PINs:

(1) (Optional) The issuing agency authorizes addition, renewal, or revocation of digital certificates on cardholder’s PIV card and coordinates cardholder’s visit to FSP.
(2) The FSP matches the applicant biometric.
(3) (Optional) Cardholder can change their forgotten PIN.

Figure 3-9: Card Maintenance Process



(1) (Optional) The issuing agency authorizes addition, renewal or revocation of digital certificates on cardholder's PIV card and coordinates cardholder's visit to FSP.

(2) The FSP matches the applicant biometric.

(3) (Optional) Cardholder can change their forgotten PIN.

Business Assumptions & Considerations

1. SIP can add additional digital certificates to an existing PIV card only when authorized by an agency to do so.
2. Cardholders can choose to change their on-board PIN at their discretion.

Use Cases used by Process:

1. Agency - SIP:
   a. X-xx Authorize certificate addition, renewal or revocation
2. SIP-FPKI SSP:
   a. X-xx Issue certificate
   b. X-xx Renew certificate
   c. X-xx Revoke certificate

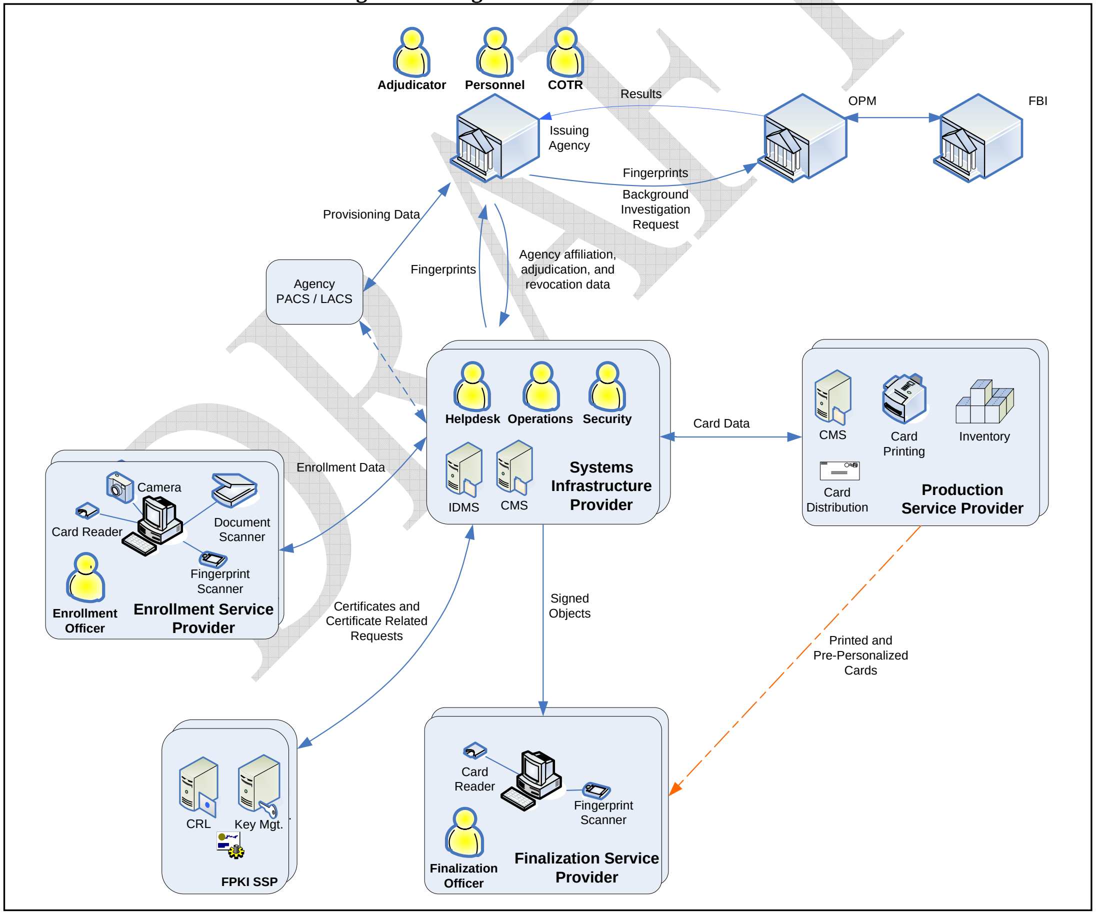
4 Architecture Use Cases

This section provides a “component-and-connector” view of the SCA, which describes (1) what components interoperate under what circumstances, and (2) what information is transferred.

4.1 High Level Overview

Figure 4-1 is a high-level overview of SCI data flow. The technical approach is mainly web services based, wherein technical interoperation with shared components (ESP, SIP, PSP, FSP) is via SOAP-wrapped XML messages over HTTPS. Each shared component is a web service provider. An agency system, for example, is a web service requester. Other communication with shared components is via secure web interface. Each shared component is a “black box” accessible only via its published message set (i.e., interface specification) or web interface. An agency system interoperates with only one SIP (i.e., an agency cannot be associated with more than one SIP). Technical interoperation with non-shared components (e.g., agency PACS/LACS) and services (e.g., OPM, FBI) are via interfaces defined and controlled outside of the SCA.

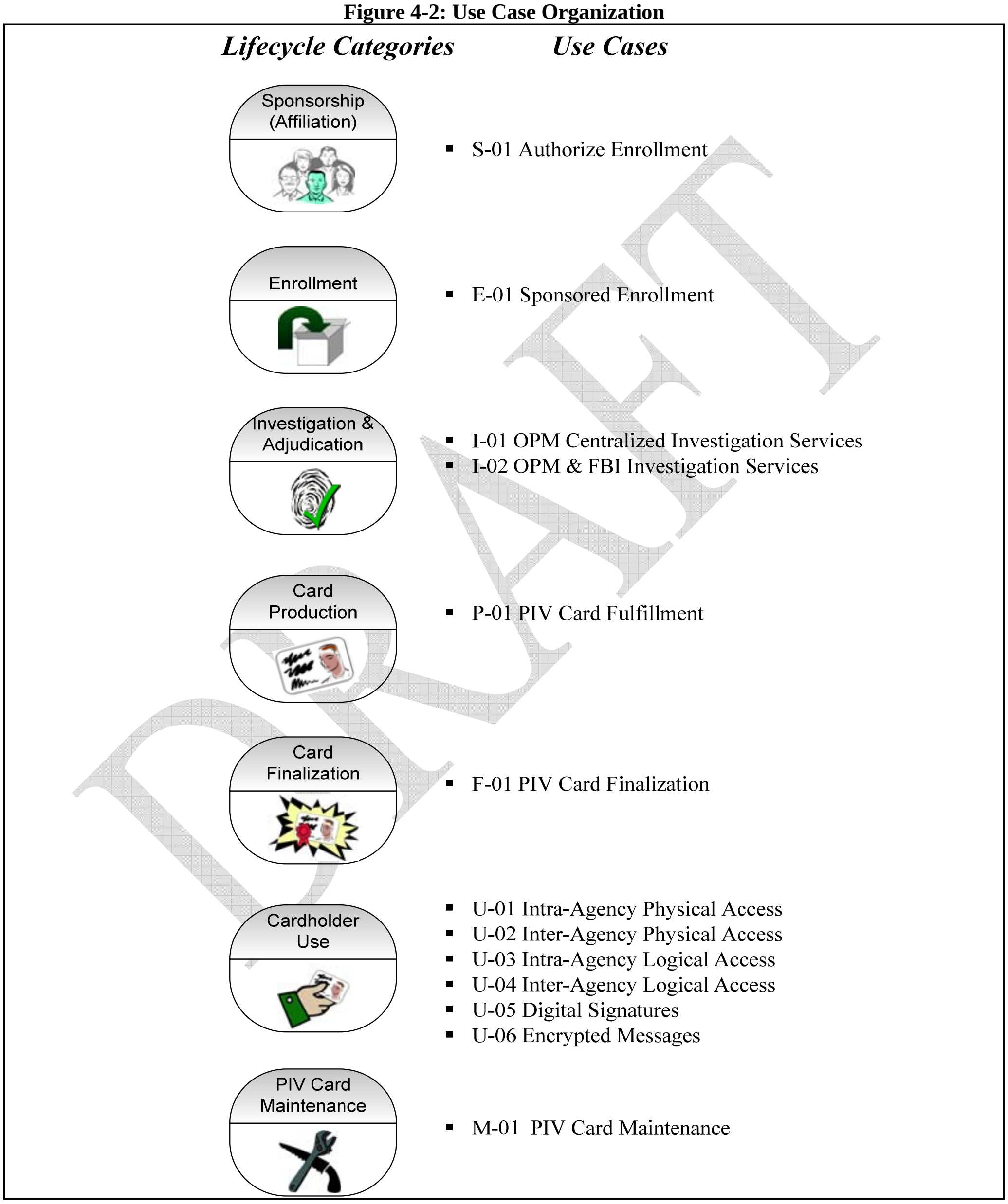
Figure 4-1: High Level SCI Data Flow



4.1.1 Use Case Organization

Figure 4-2 lists the full set of SCA use cases, organized into seven (7) PIV card lifecycle categories. Detailed business process analyses derived the use cases.

Figure 4-2: Use Case Organization

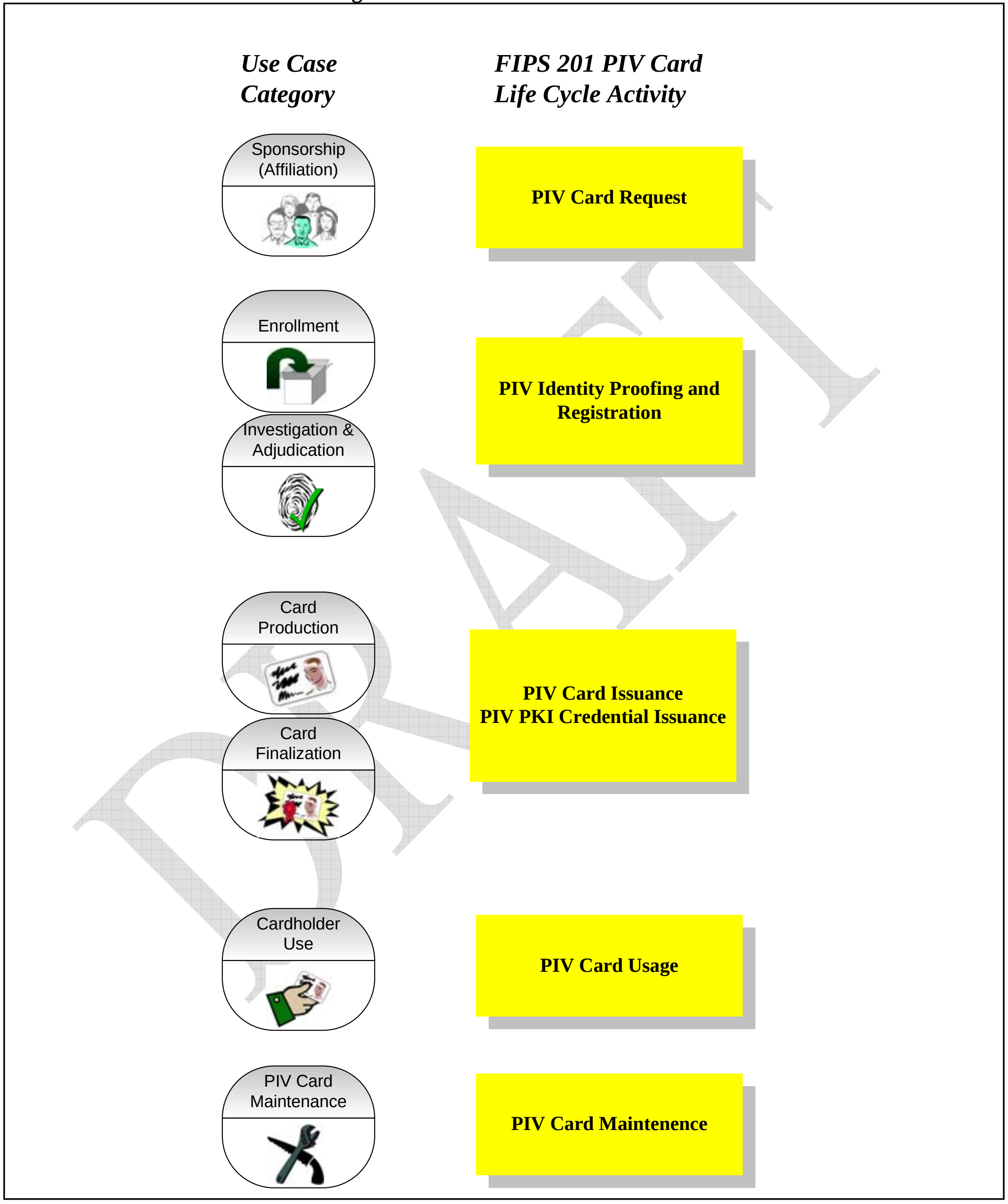


Lifecycle Categories	*Use Cases*
Sponsorship (Affiliation)	▪ S-01 Authorize Enrollment
Enrollment	▪ E-01 Sponsored Enrollment
Investigation & Adjudication	▪ I-01 OPM Centralized Investigation Services ▪ I-02 OPM & FBI Investigation Services
Card Production	▪ P-01 PIV Card Fulfillment
Card Finalization	▪ F-01 PIV Card Finalization
Cardholder Use	▪ U-01 Intra-Agency Physical Access ▪ U-02 Inter-Agency Physical Access ▪ U-03 Intra-Agency Logical Access ▪ U-04 Inter-Agency Logical Access ▪ U-05 Digital Signatures ▪ U-06 Encrypted Messages
PIV Card Maintenance	▪ M-01 PIV Card Maintenance

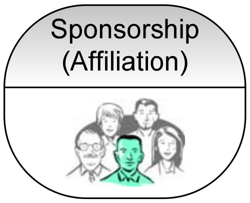
4.1.2 Crosswalk with FIPS 201

Figure 4-3 maps SCA lifecycle categories to corresponding [FIPS 201] PIV card life cycle activities.

Figure 4-3: Crosswalk with FIPS 201



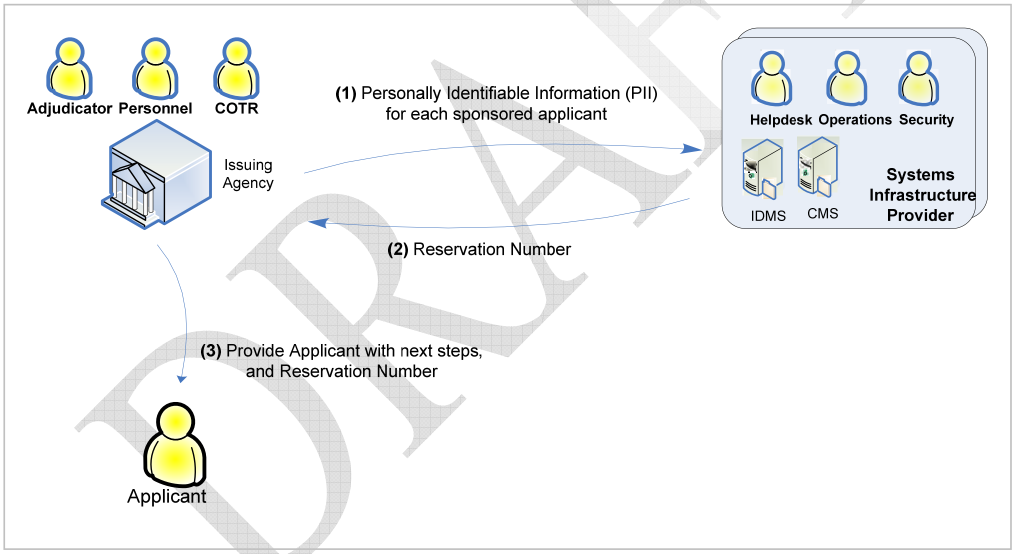
4.2 Sponsorship



This section details the sponsorship business process. One (1) use case addresses Sponsorship: (1) authorize enrollment. Sequence and activity diagrams provide additional details.

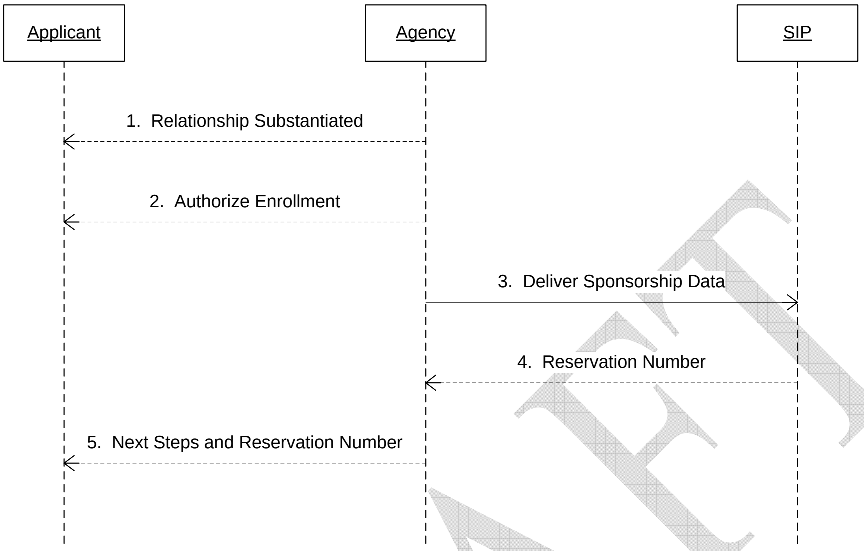
4.2.1 Use Case S-01 Authorize Enrollment

This use case illustrates agency authorization of enrollment of an applicant. An applicant is either a potential employee or potential contractor. The agency must substantiate that it is acceptable for the applicant to receive a PIV card and begin the enrollment process. Once an agency authorizes an applicant for enrollment, the agency sends applicant information to the SIP.


Adjudicator
Personnel
COTR
Issuing Agency
(1) Personally Identifiable Information (PII) for each sponsored applicant
(2) Reservation Number
Helpdesk
Operations
Security
IDMS
CMS
Systems Infrastructure Provider
(3) Provide Applicant with next steps, and Reservation Number
Applicant

4.2.1.1 S-01 Sequence Diagram – Authorize Enrollment

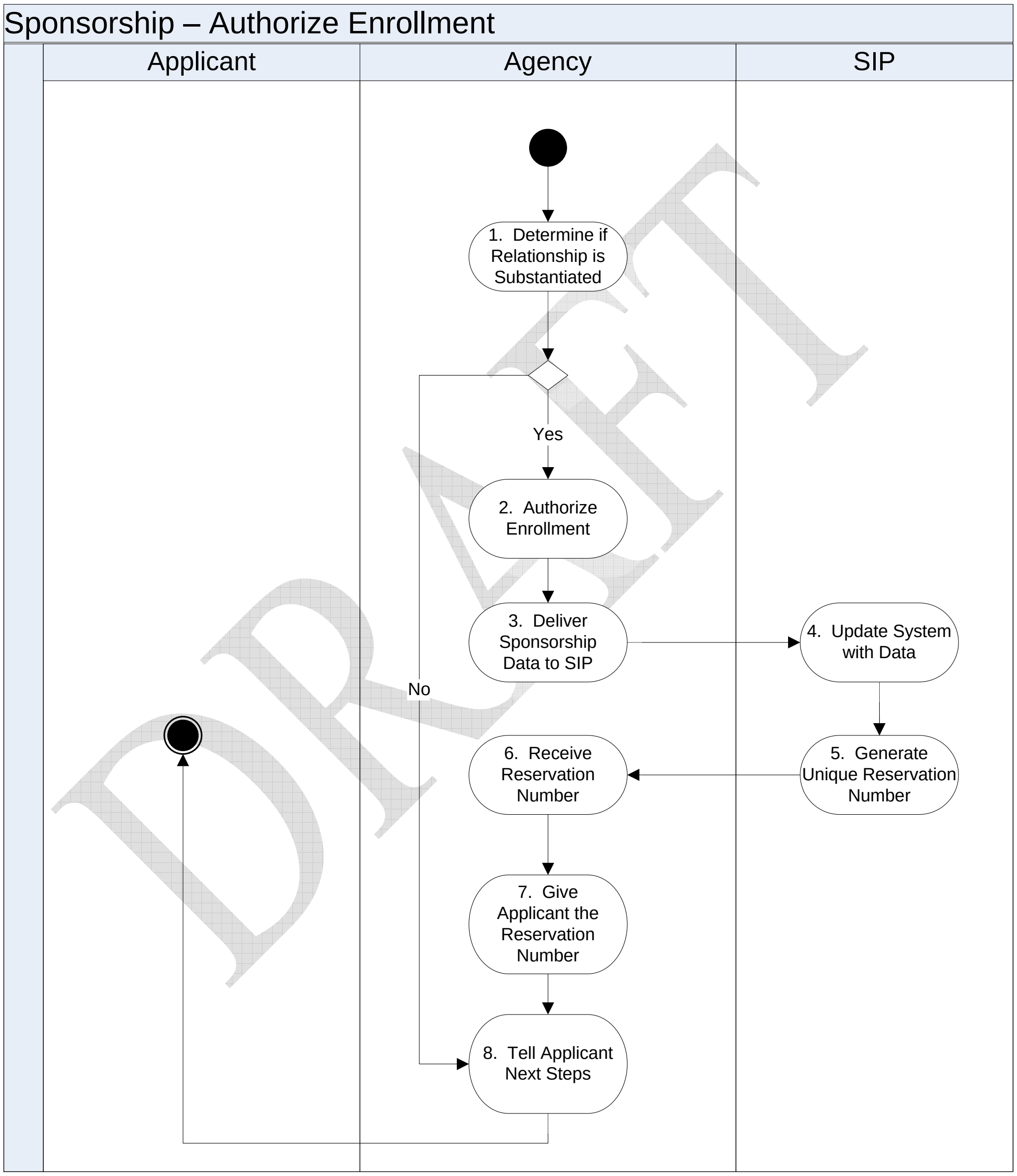
This sequence diagram illustrates the sequences during the authorization of enrollment.


Applicant
Agency
SIP
1. Relationship Substantiated
2. Authorize Enrollment
3. Deliver Sponsorship Data
4. Reservation Number
5. Next Steps and Reservation Number

Sequence #	List of SCA Interface Specifications / Transactions
1	Not applicable
2	Not applicable
3	[Agency-SIP], CreateNewEmployeeContractor transaction
4	[Agency-SIP], CreateNewEmployeeContractorResponse transaction
5	Not applicable

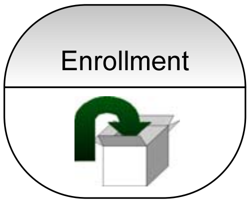
4.2.1.2 S-01 Activity Diagram – Authorize Enrollment

This activity diagram illustrates the activities during authorization of enrollment. The sponsoring agency performs the majority of this effort.


Sponsorship – Authorize Enrollment
Applicant
Agency
SIP
1. Determine if Relationship is Substantiated
Yes
No
2. Authorize Enrollment
3. Deliver Sponsorship Data to SIP
4. Update System with Data
5. Generate Unique Reservation Number
6. Receive Reservation Number
7. Give Applicant the Reservation Number
8. Tell Applicant Next Steps

Activity Step #	Description
1	The agency substantiates their relationship with the applicant
2	If the relationship is substantiated, the agency authorizes applicant enrollment. If the relationship is not substantiated, the agency does not authorize enrollment, notifies the applicant accordingly, and the sponsorship process ends.
3	The agency updates the SIP with the applicant's sponsorship information. This includes PII and enrollment eligibility.
4	The SIP updates its applicant record with the information provided by the enrollment station.
5	The SIP generates a unique Reservation Number that is associated with this authorized enrollment and associated finalization.
6	The SIP returns the Reservation Number to the enrollment station.
7	The agency gives the Reservation Number to the applicant. The applicant must present this Reservation Number at the enrollment station and at the finalization station in order for processing to begin at each station.
8	The agency tells the applicant what the next steps are. For an authorized enrollment, the next steps include: (a) go to a specific enrollment station, (b) bring appropriate I-9 documentation.

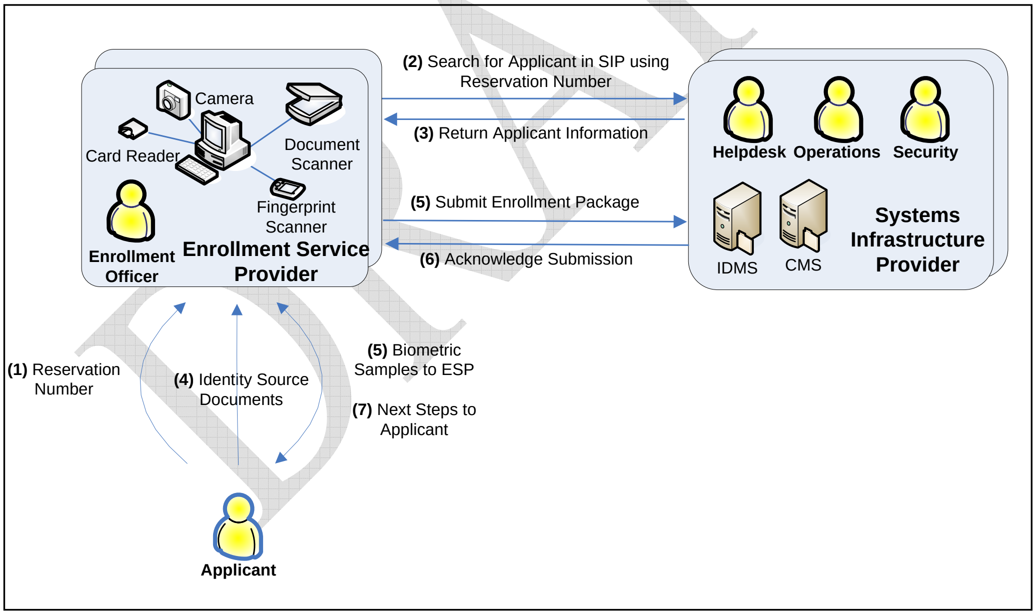
4.3 Enrollment



This section details the enrollment business process. A single use case addresses Enrollment: (1) sponsored enrollment. However, enrollment encompasses two scenarios: (a) initial enrollment (i.e., initial PIV card issuance), and (b) re-enrollment (i.e., PIV card renewal or reissue). Processing of the scenarios are the same except that re-enrollment has the additional step of cross checking (when possible) the previously submitted enrollment documents with those currently presented to the Enrollment Officer (EO). Both scenarios require a valid Reservation Number to search the appropriate SIP. The following sections describe the initial enrollment scenario. Sequence and activity diagrams provide additional details.

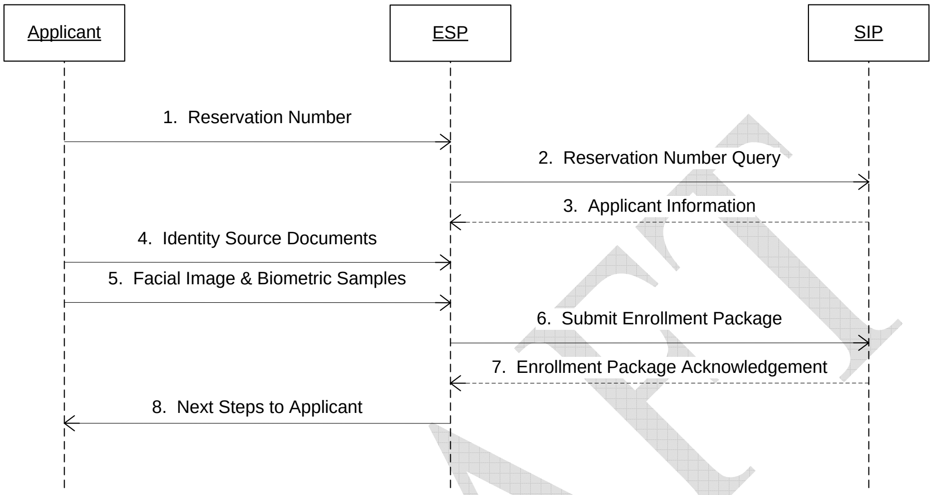
4.3.1 Use Case E-01 Sponsored Enrollment

This use case illustrates enrollment of a sponsored applicant. It supports the capturing of documents and biometric samples for identity proofing. The design provides common baseline functionality for support of agency PIV implementations.


Camera
Card Reader
Document Scanner
Fingerprint Scanner
Enrollment Officer
Enrollment Service Provider
(2) Search for Applicant in SIP using Reservation Number
(3) Return Applicant Information
(5) Submit Enrollment Package
(6) Acknowledge Submission
Helpdesk
Operations
Security
IDMS
CMS
Systems Infrastructure Provider
(1) Reservation Number
(4) Identity Source Documents
(5) Biometric Samples to ESP
(7) Next Steps to Applicant
Applicant

4.3.1.1 E-01 Sequence Diagram – Sponsored Enrollment

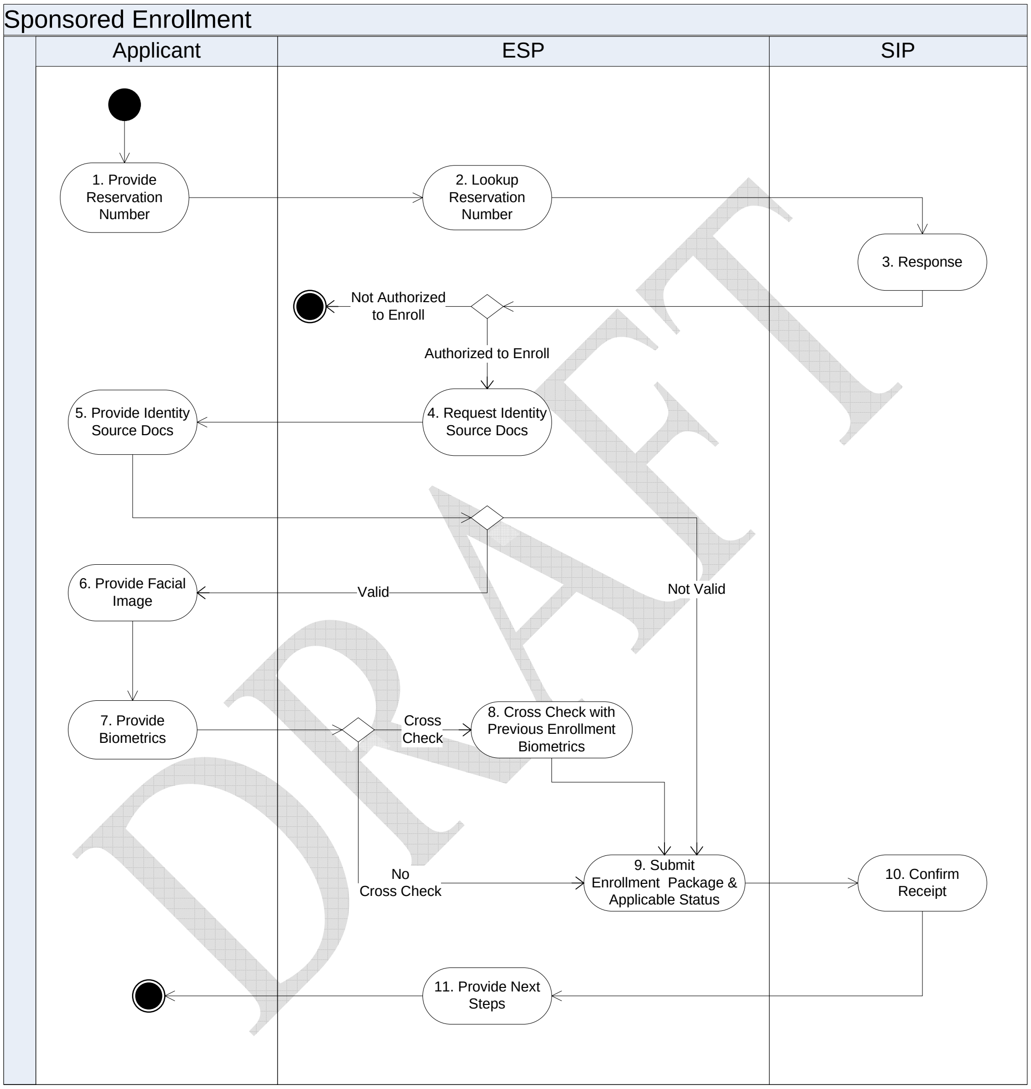
This sequence diagram illustrates the sequence of communications between the various actors in the Sponsored Enrollment use case.


Applicant
ESP
SIP
1. Reservation Number
2. Reservation Number Query
3. Applicant Information
4. Identity Source Documents
5. Facial Image & Biometric Samples
6. Submit Enrollment Package
7. Enrollment Package Acknowledgement
8. Next Steps to Applicant

Sequence #	List of SCA Interface Specifications / Transactions
1	Not applicable
2	[ESP-SIP], EnrollmentAuthLookup transaction
3	[ESP-SIP], EnrollmentAuthLookupResult transaction
4	Not applicable
5	Not applicable
6	[ESP-SIP], EnrollmentPackage transaction
7	[ESP-SIP], EnrollmentPackageResponse transaction
8	Not applicable

4.3.1.2 E-01 Activity Diagram – Sponsored Enrollment

This activity diagram illustrates the entire process for enrollment of a sponsored applicant.


Sponsored Enrollment
Applicant
ESP
SIP
1. Provide Reservation Number
2. Lookup Reservation Number
3. Response
Not Authorized to Enroll
Authorized to Enroll
4. Request Identity Source Docs
5. Provide Identity Source Docs
Valid
Not Valid
6. Provide Facial Image
7. Provide Biometrics
Cross Check
8. Cross Check with Previous Enrollment Biometrics
No Cross Check
9. Submit Enrollment Package & Applicable Status
10. Confirm Receipt
11. Provide Next Steps

Activity Step #	Description
1	The applicant gives the EO his/her Reservation Number.
2	The EO looks up the applicant in the SIP, using the Reservation Number. The enrollment station uses the first portion of the Reservation Number to determine the SIP to connect to (see [Agency-SIP] and [SCI Metadata]).
3	The SIP response to the ESP indicates whether the applicant is authorized to enroll. If the applicant is not authorized, enrollment ends without further processing. If the applicant is authorized, the SIP also returns applicant personal information and applicant sponsorship information. If available, the SIP additionally returns any I-9 document information, photograph information, and/or fingerprint information it has stored from the last successful enrollment.
4	The EO requests identity source documents from applicant.
5	The applicant provides identity source documents to EO. The EO validates source documents provided by applicant. If source documents are not valid, processing skips[5] to step #9 to provide forensics for any subsequent investigation of this incident.
6	The applicant provides facial image for capture by the EO.
7	The applicant provides fingerprints for capture by the EO. The applicant tests biometric sample (minutiae) to ensure proper capture.
8	If the SIP returned biometrics from an earlier enrollment, the EO compares (crosschecks) just captured biometrics with SIP-returned biometrics.
9	The EO digitally signs enrollment package content. The enrollment station then digitally signs[6] and encrypts the SOAP-wrapped enrollment package, and submits the enrollment package to the SIP with the appropriate status (and status message if necessary). Depending upon the enrollment status and message, the SIP may notify the agency via email[7].
10	The SIP acknowledges receipt of the enrollment package to the enrollment station. The EO can use the returned receipt to verify processing of the correct enrollment package by the SIP.
11	The EO communicates to the applicant: (a) any noteworthy points about the enrollment, and (b) next steps.

[5] Additional capture of biometrics is strongly recommended to enhance subsequent investigation of this incident.

[6] Note that the EO digital signature is separate and distinct from the enrollment station digital signature.

[7] Email notifications will not contain PII, and will likely require the agency to use the SIP web Interface to obtain additional information

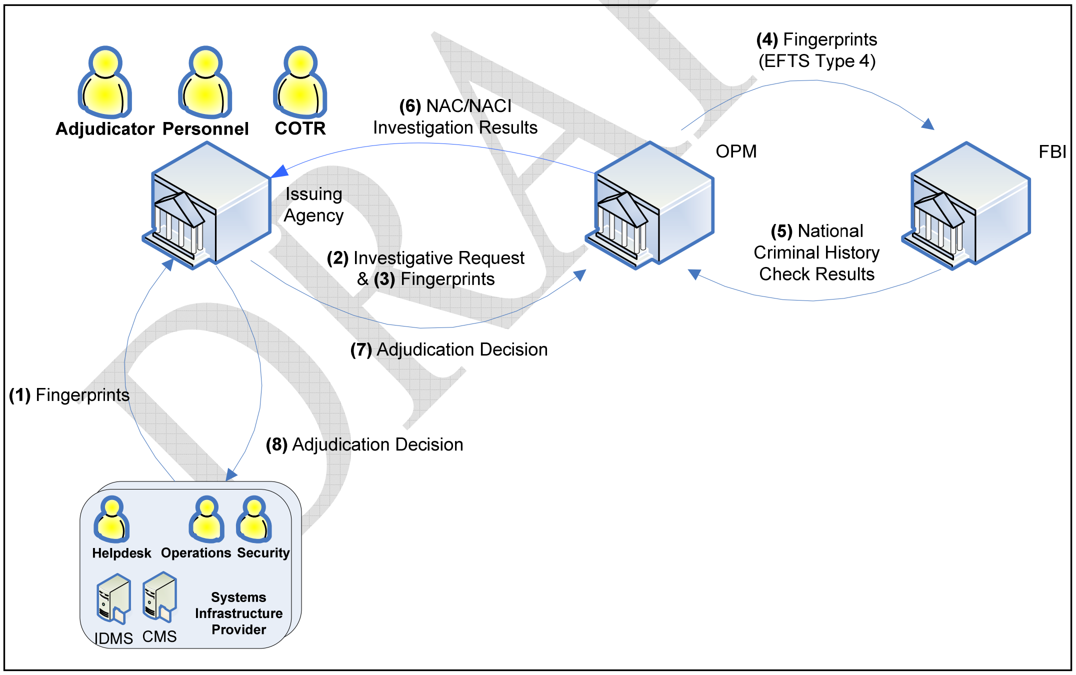
4.4 *Investigation and Adjudication*

This section details the investigation and adjudication business process. Two (2) use cases address Investigation and Adjudication: (1) OPM centralized investigation services, and (2) OPM & FBI investigation services. In either case, the agency is responsible for obtaining applicant fingerprints from the SIP and forwarding them to OPM and/or FBI. Sequence and activity diagrams provide additional details.

4.4.1 Use Case I-01 OPM Centralized Investigation Services

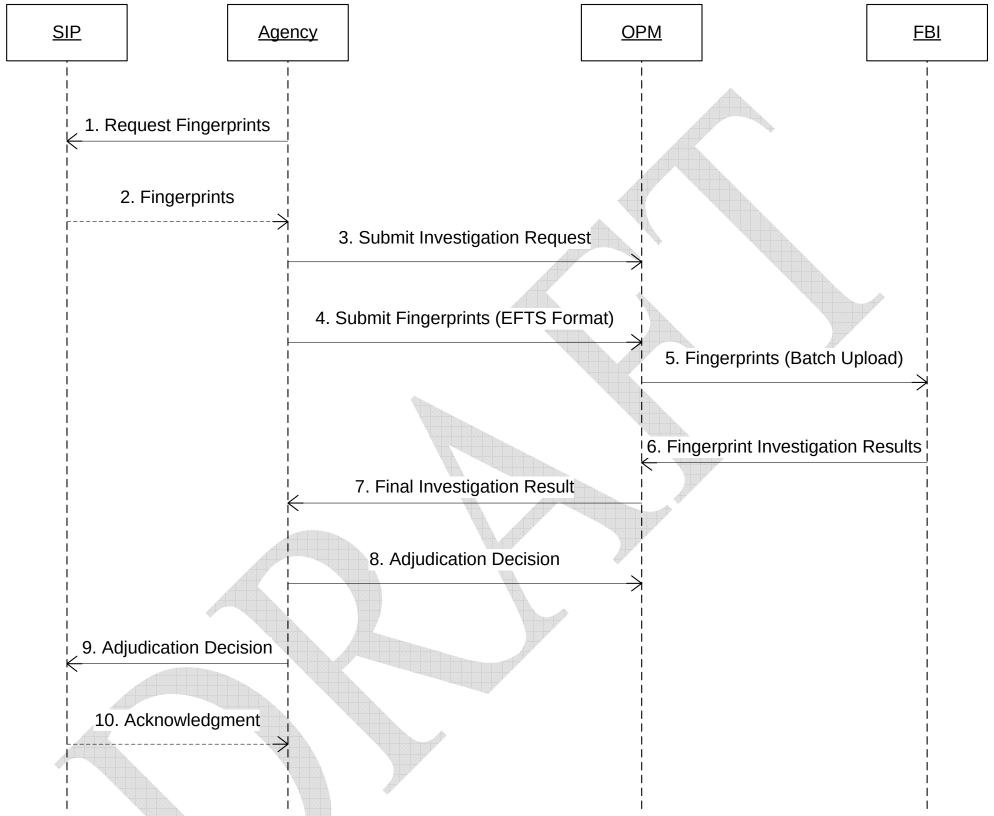
Comment [CB1]: We'd like to explore packages going from the SIP to OPM.

This use case illustrates the OPM as a central clearinghouse for all background investigation services, including fingerprint checks processed by the FBI CJIS Division's IAFIS system.


Adjudicator
Personnel
COTR
Issuing Agency
OPM
FBI
(4) Fingerprints (EFTS Type 4)
(6) NAC/NACI Investigation Results
(2) Investigative Request & (3) Fingerprints
(5) National Criminal History Check Results
(7) Adjudication Decision
(1) Fingerprints
(8) Adjudication Decision
Helpdesk
Operations
Security
IDMS
CMS
Systems Infrastructure Provider

4.4.1.1 I-01 Sequence Diagram – OPM Centralized Investigation Services

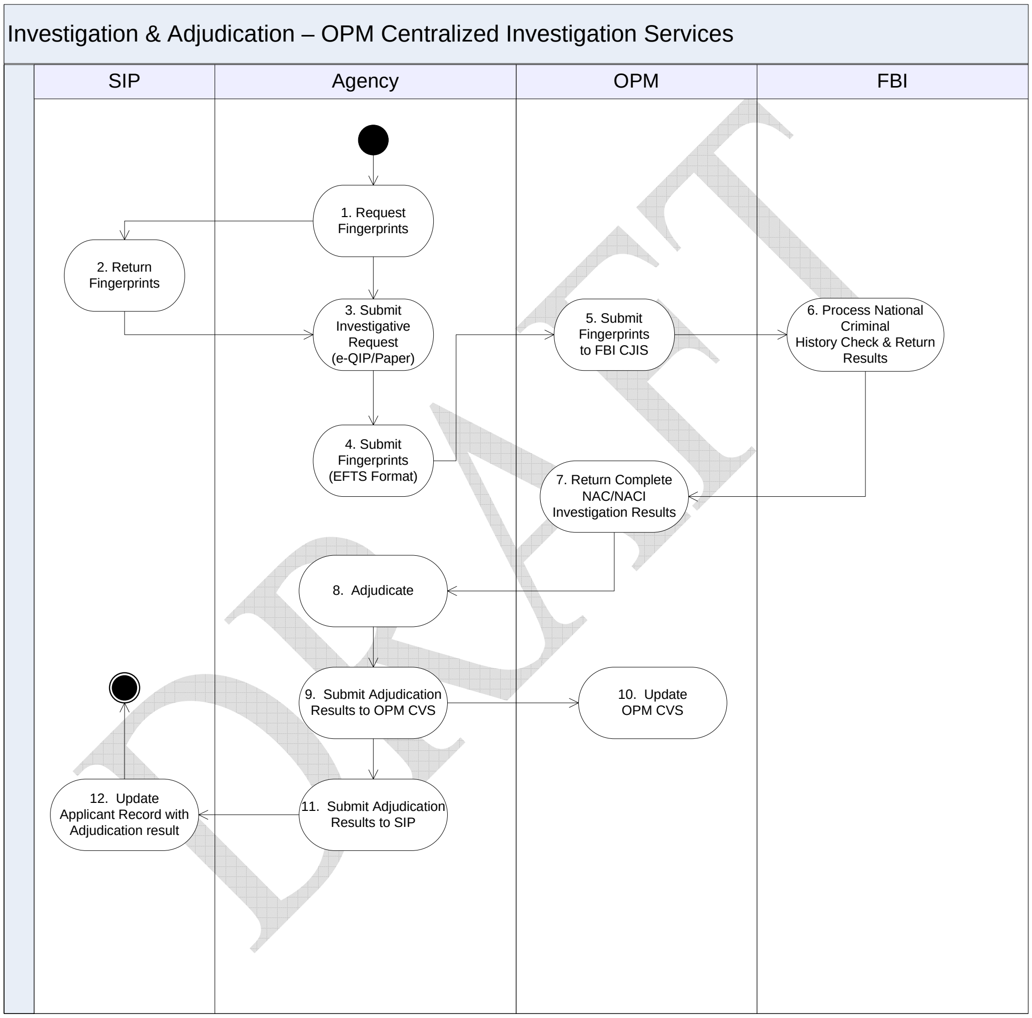
This sequence diagram illustrates an agency using OPM as the primary clearinghouse for background investigative services. Most agencies transmit fingerprint data to the FBI via OPM. We do not expect current agency practices for interacting with OPM/FBI to change. Some agencies do their own investigation. Here too, we do not expect those agencies to change that practice.


SIP
Agency
OPM
FBI
1. Request Fingerprints
2. Fingerprints
3. Submit Investigation Request
4. Submit Fingerprints (EFTS Format)
5. Fingerprints (Batch Upload)
6. Fingerprint Investigation Results
7. Final Investigation Result
8. Adjudication Decision
9. Adjudication Decision
10. Acknowledgment

Sequence #	List of SCA Interface Specifications / Transactions
1	[Agency-SIP], QuerySIP transaction
2	[Agency-SIP], QuerySIPResponse transaction
3	Not applicable However, for your information (FYI): e-QIP or hard copy. For details regarding e-QIP, please go to http://www.opm.gov/e-qip/
4	Not applicable However, FYI: valid EFTS format to OPM Store and Forward Fingerprint Transaction System. For details regarding the methods to submit fingerprints to OPM Store and Forward Fingerprint Transaction System, please go to the following web site: http://www.opm.gov/extra/investigate/Fin-2000/FIN0004-Attachmnt.asp. See [EFTS] for details regarding the EFTS.
5	Not applicable
6	Not applicable
7	Not applicable However, FYI: Electronic means or via mail.
8	Not applicable However, FYI: Electronic means or via mail.
9	[Agency-SIP], UpdateEmployeeContractor transaction
10	[Agency-SIP], UpdateEmployeeContractorResponse transaction

4.4.1.2 I-01 Activity Diagram – OPM Centralized Investigation Services

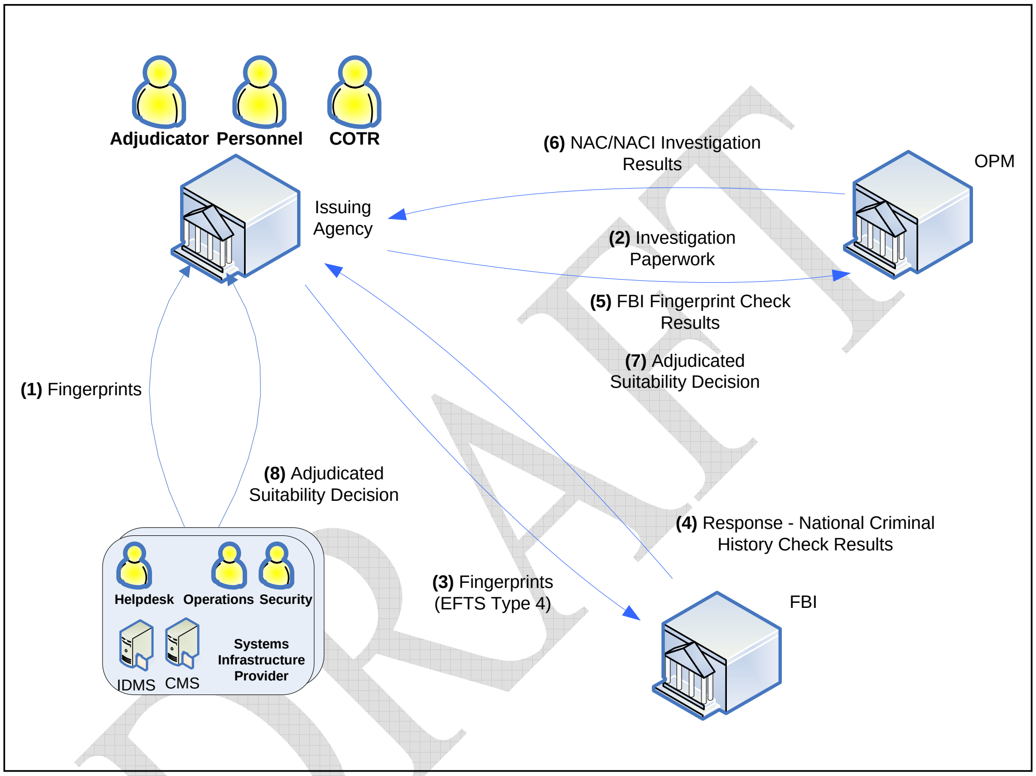
This activity diagram illustrates all steps in the process to have OPM conduct and coordinate background investigations, including management of the fingerprint interface with FBI.


Investigation & Adjudication – OPM Centralized Investigation Services
SIP
Agency
OPM
FBI
1. Request Fingerprints
2. Return Fingerprints
3. Submit Investigative Request (e-QIP/Paper)
4. Submit Fingerprints (EFTS Format)
5. Submit Fingerprints to FBI CJIS
6. Process National Criminal History Check & Return Results
7. Return Complete NAC/NACI Investigation Results
8. Adjudicate
9. Submit Adjudication Results to OPM CVS
10. Update OPM CVS
11. Submit Adjudication Results to SIP
12. Update Applicant Record with Adjudication result

Activity Step #	Description
1	The agency requests the applicant's fingerprints stored at the SIP.
2	The SIP responds to request by returning the applicant's fingerprints.
3	The agency sends investigative request to OPM via e-QIP or hard copy.
4	The agency submits fingerprints to the OPM Store and Forward Fingerprint Transaction System using a valid EFTS format.
5	OPM forwards fingerprints to the FBI.
6	The FBI processes a National Criminal History Check and returns the results to OPM.
7	The OPM provides completed NAC/NACI investigative results to agency.
8	The agency adjudicates, per the results returned to it.
9	The agency provides adjudication results to OPM CVS.
10	OPM updates CVS with the adjudication decision.
11	The agency provides adjudication results to the SIP.
12	The SIP updates the applicant's record with the adjudication decision.

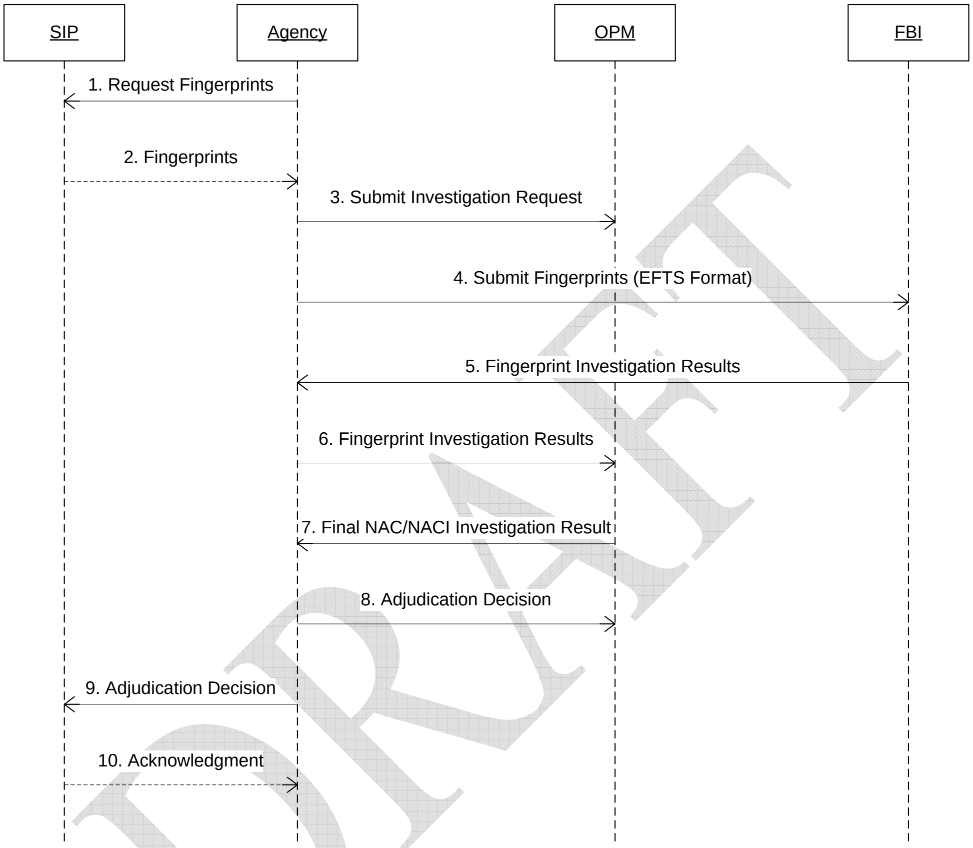
4.4.2 Use Case I-02 OPM & FBI Investigation Services

This use case illustrates an agency's use of OPM-IS, which has a direct channel to the FBI for fingerprint checks. Not that in step 1, the agency indicates to OPM that the agency itself will send the fingerprints to the FBI, and will forward fingerprint check results to OPM.


Adjudicator
Personnel
COTR
Issuing Agency
(6) NAC/NACI Investigation Results
OPM
(2) Investigation Paperwork
(5) FBI Fingerprint Check Results
(7) Adjudicated Suitability Decision
(1) Fingerprints
(8) Adjudicated Suitability Decision
(4) Response - National Criminal History Check Results
Helpdesk
Operations
Security
(3) Fingerprints (EFTS Type 4)
FBI
Systems Infrastructure Provider
IDMS
CMS

4.4.2.1 I-02 Sequence Diagram – OPM & FBI Investigation Services

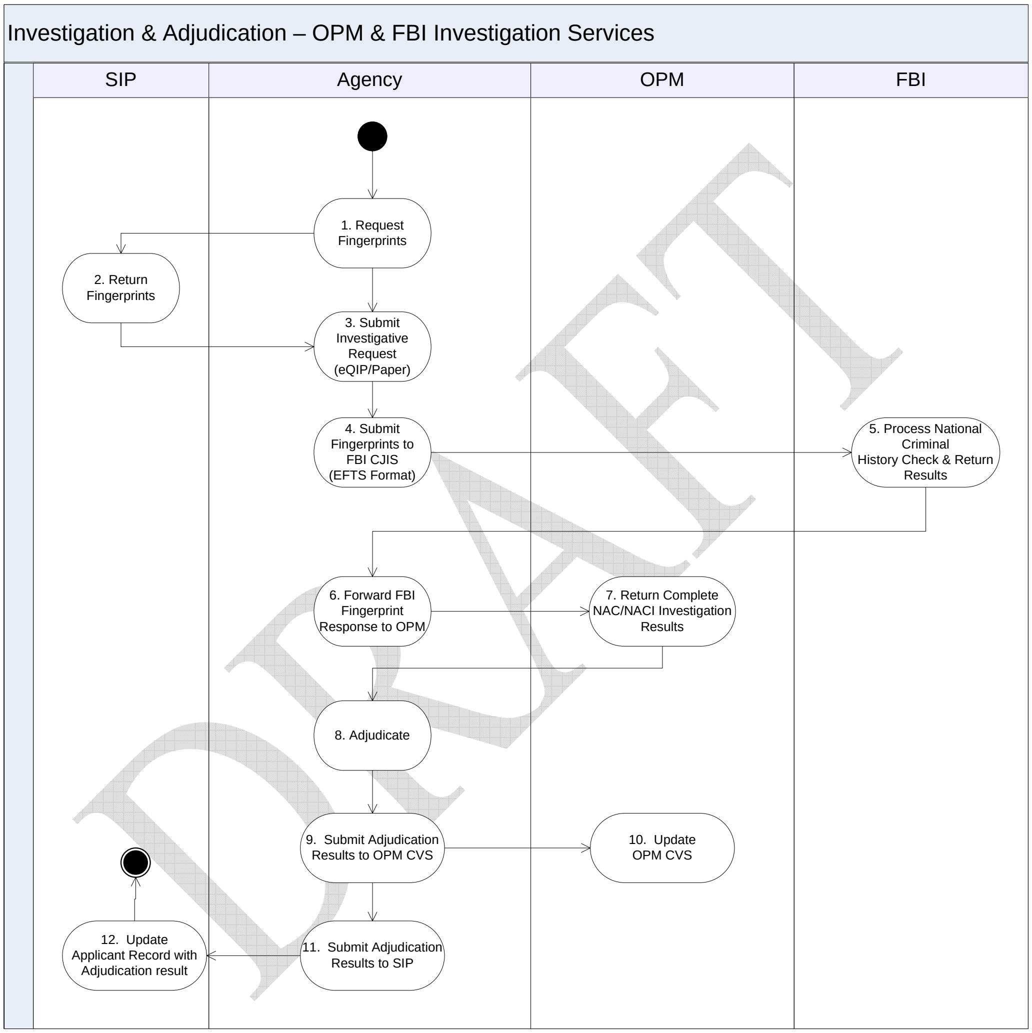
This sequence diagram illustrates using OPM and FBI separately. Note the direct agency-to-FBI interface for fingerprints.


SIP
Agency
OPM
FBI
1. Request Fingerprints
2. Fingerprints
3. Submit Investigation Request
4. Submit Fingerprints (EFTS Format)
5. Fingerprint Investigation Results
6. Fingerprint Investigation Results
7. Final NAC/NACI Investigation Result
8. Adjudication Decision
9. Adjudication Decision
10. Acknowledgment

Sequence #	List of SCA Interface Specifications / Transactions
1	[Agency-SIP], QuerySIP transaction
2	[Agency-SIP], QuerySIPResponse transaction
3	Not applicable However, FYI: via e-QIP or hard copy. For details regarding e-QIP, please go to: http://www.opm.gov/e-qip/.
4	Not applicable However, FYI: valid EFTS format to FBI CJIS. See [EFTS].
5	Not applicable However, FYI: Electronic or paper (mail)
6	Not applicable However, FYI: Fax
7	Not applicable However, FYI: Electronic means or via mail.
8	Not applicable However, FYI: Electronic means or via mail.
9	[Agency-SIP], UpdateEmployeeContractor transaction
10	[Agency-SIP], UpdateEmployeeContractorResponse transaction

4.4.2.2 I-02 Activity Diagram – OPM & FBI Investigation Services

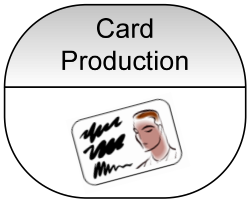
This activity diagram illustrates background investigation using OPM and FBI separately.


Investigation & Adjudication – OPM & FBI Investigation Services
SIP
Agency
OPM
FBI
1. Request Fingerprints
2. Return Fingerprints
3. Submit Investigative Request (eQIP/Paper)
4. Submit Fingerprints to FBI CJIS (EFTS Format)
5. Process National Criminal History Check & Return Results
6. Forward FBI Fingerprint Response to OPM
7. Return Complete NAC/NACI Investigation Results
8. Adjudicate
9. Submit Adjudication Results to OPM CVS
10. Update OPM CVS
11. Submit Adjudication Results to SIP
12. Update Applicant Record with Adjudication result

Activity Step #	Description
1	The agency requests the applicant’s fingerprints stored at the SIP.
2	The SIP responds to request by returning the applicant’s fingerprints.
3	The agency sends investigation request to OPM via eQIP or hard copy.
4	The agency submits fingerprints to FBI CJIS using a valid EFTS format.
5	The FBI provides National Criminal History Check response to agency.
6	The agency supplies OPM with copy of FBI fingerprint investigation results.
7	OPM provides NAC/NACI investigative results to agency.
8	The agency adjudicates, per the results returned to it.
9	The agency provides adjudication results to OPM CVS.
10	OPM updates CVS with the adjudication decision.
11	The agency provides adjudication results to the SIP.
12	The SIP updates the applicant’s record with the adjudication decision.

4.5 Card Production

Comment [Rnote2]: Add flow for updating SIP if problem encountered

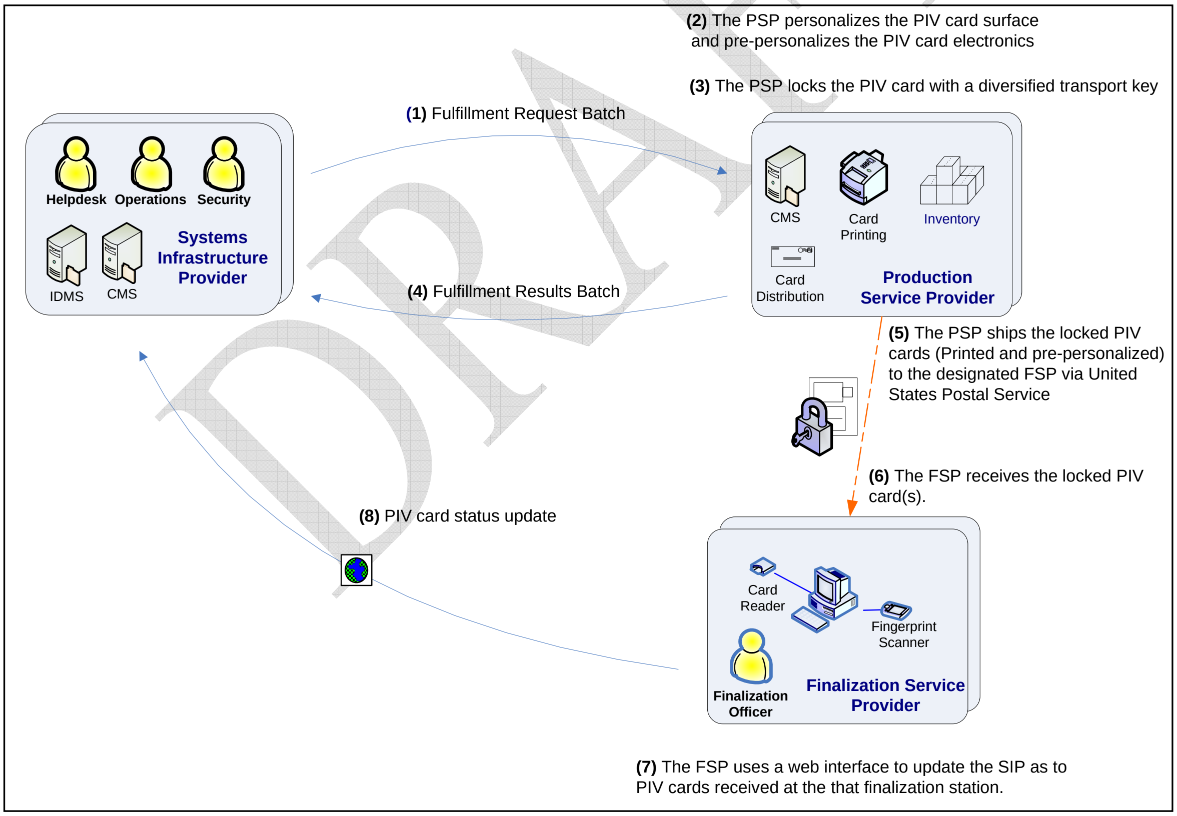


This section details the PIV card production business process. One use case addresses Card Production: (1) PIV Card Fulfillment. Fulfillment encompasses (a) personalizing the PIV card surface, and (b) pre-personalizing the PIV card electronics in advance of loading objects. Tasks such as key ceremonies, implementing card production profiles, card stock management are done out-of-band and are therefore out-of-scope for the SCA.

4.5.1 Use Case P-01 PIV Card Fulfillment

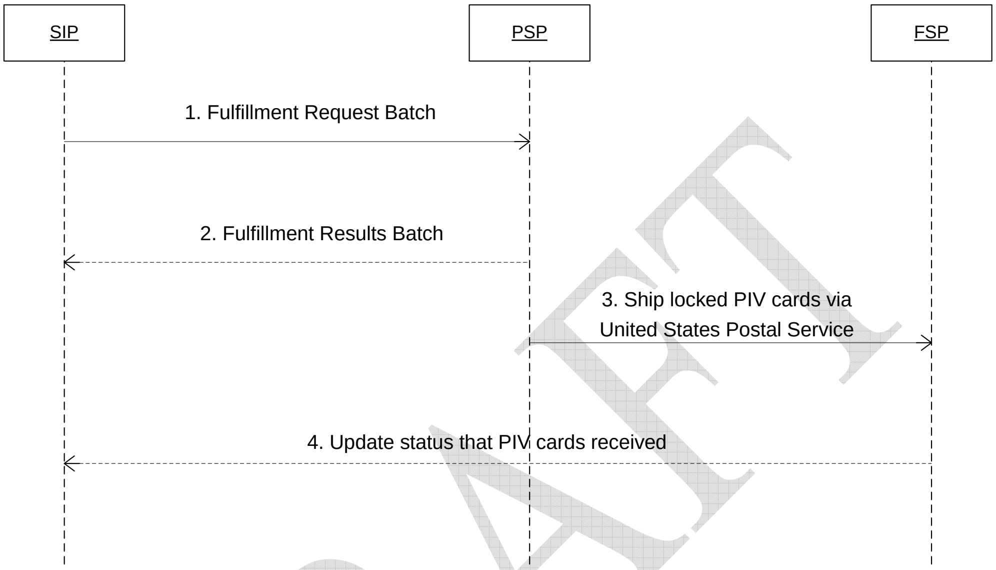
Comment [Rnote3]: This changes per final Global Platform decisions

Upon agency authorization, the SIP submits a fulfillment request batch to the PSP. A batch contains one or more fulfillment requests, including what profile(s) to use for each fulfillment request. Upon batch processing completion, the PSP returns a results batch to the SIP. The results batch indicates fulfillment success or failure per fulfillment request in the batch. The PSP locks the successfully fulfilled PIV cards with transport keys, and ships them to the appropriate FSP via United States Postal Service. The FSP updates the SIP regarding PIV cards received.


(2) The PSP personalizes the PIV card surface and pre-personalizes the PIV card electronics
(3) The PSP locks the PIV card with a diversified transport key
(1) Fulfillment Request Batch
Helpdesk
Operations
Security
IDMS
CMS
Systems Infrastructure Provider
CMS
Card Printing
Inventory
Card Distribution
Production Service Provider
(4) Fulfillment Results Batch
(5) The PSP ships the locked PIV cards (Printed and pre-personalized) to the designated FSP via United States Postal Service
(6) The FSP receives the locked PIV card(s).
(8) PIV card status update
Card Reader
Fingerprint Scanner
Finalization Officer
Finalization Service Provider
(7) The FSP uses a web interface to update the SIP as to PIV cards received at the that finalization station.

4.5.1.1 P-01 Sequence Diagram – PIV Card Fulfillment

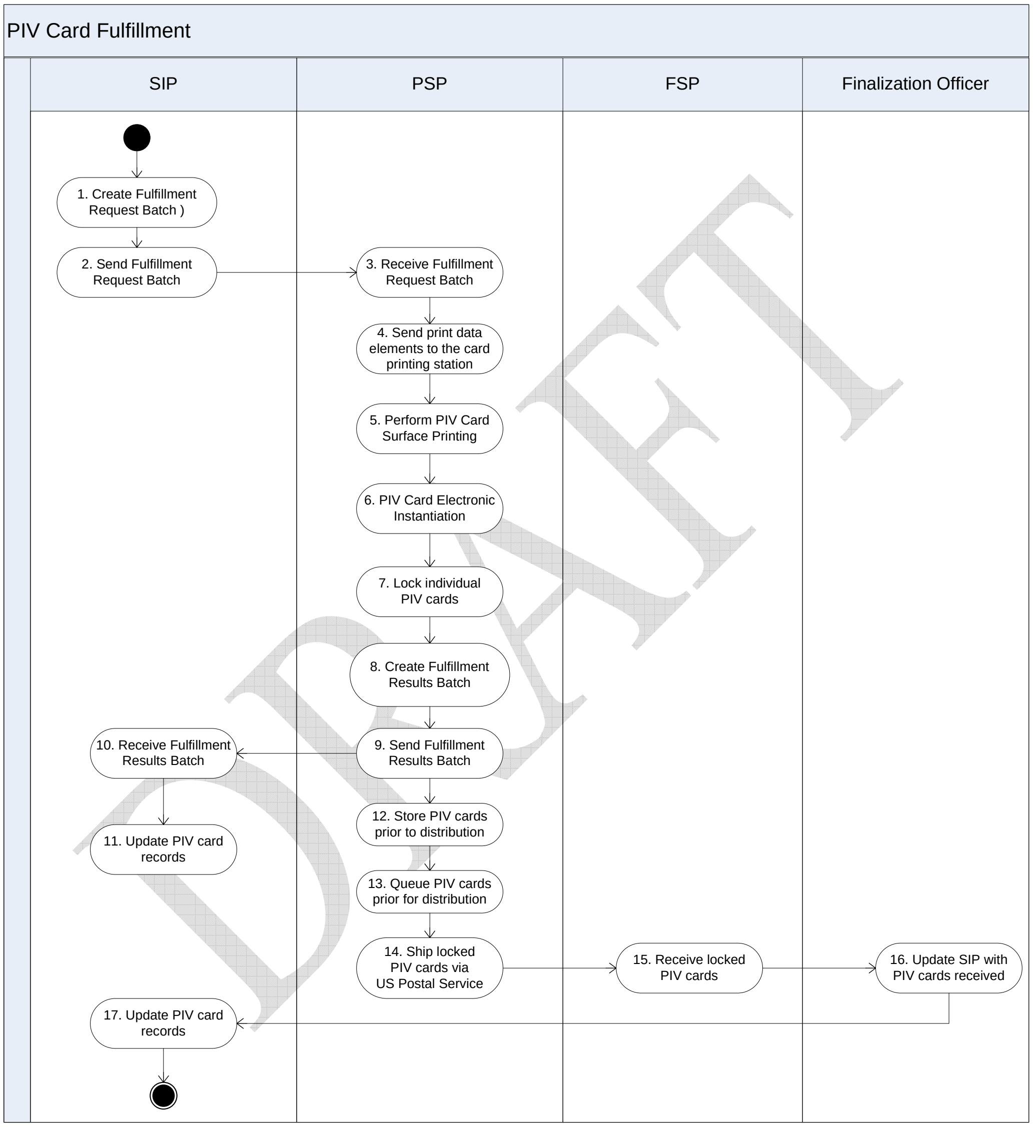
This sequence diagram illustrates the sequence of events and data communications required to fulfill a PIV card production order. [SIP-PSP] discusses the data elements described in this diagram in more detail.


SIP
PSP
FSP
1. Fulfillment Request Batch
2. Fulfillment Results Batch
3. Ship locked PIV cards via
United States Postal Service
4. Update status that PIV cards received

Sequence #	List of SCA Interface Specifications / Transactions
1	[SIP-PSP]
2	[SIP-PSP]
3	Not applicable
4	SIP Web Interface

4.5.1.2 P-01 Activity Diagram – PIV Card Fulfillment

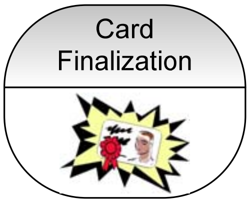
This activity diagram illustrates the trigger and activities of card production.


PIV Card Fulfillment
SIP
PSP
FSP
Finalization Officer
1. Create Fulfillment Request Batch)
2. Send Fulfillment Request Batch
3. Receive Fulfillment Request Batch
4. Send print data elements to the card printing station
5. Perform PIV Card Surface Printing
6. PIV Card Electronic Instantiation
7. Lock individual PIV cards
8. Create Fulfillment Results Batch
9. Send Fulfillment Results Batch
10. Receive Fulfillment Results Batch
11. Update PIV card records
12. Store PIV cards prior to distribution
13. Queue PIV cards prior for distribution
14. Ship locked PIV cards via US Postal Service
15. Receive locked PIV cards
16. Update SIP with PIV cards received
17. Update PIV card records

Activity Step #	Description
1	The SIP creates a fulfillment request batch containing one or more fulfillment requests, as authorized by agencies. The fulfillment request batch can contain requests from different agencies, but is limited to requests for the same PSP and destined for the same finalization station. Each fulfillment request in the batch includes all information and instructions (e.g., what card production profiles to use) required by the PSP.
2	The SIP communicates the fulfillment request batch to the PSP.
3	The PSP receives the fulfillment request batch, and for each fulfillment request in the batch, begins PIV card production processing
4	The PSP sends the PIV card data elements to the card printing station (cardholder data and agency template).
5	The PSP card printing station prints the PIV card surface.
6	The PSP card printing station pre-personalizes (initializes) the PIV card electronics. This includes allocating space, creating directories, loading and instantiating applets and containers.
7	The PSP locks the PIV card with a diversified transport key that is unique to the PIV card.
8	The PSP creates a fulfillment results batch, indictaing which fulfillment requests were successfully processed, and which were not. Additional information (e.g., chip ID) is also returned, as necessary.
9	The PSP sends the fulfillment results batch to the SIP.
10	The SIP receives the fulfillment results batch from the PSP.
11	The SIP updates its records in accordance with the fulfillment results batch.
12	The PSP card printing station sends newly locked PIV cards to the inventory facility for storage while waiting to be scheduled for shipment.
13	The locked PIV cards are sent to the PSP card distribution center and scheduled for shipment to the designated finalization station.
14	The PSP card distribution center ships the PIV cards via United States Postal Service (for law enforcement reasons) to the designated finalization station.
15	The FSP receives the locked PIV cards via United States Postal Service.
16	The Finalization Officer connects to the SIP via web interface to update the SIP as to which PIV cards have been received at that finalization station.
17	The SIP updates PIV cards records indicating they have been received at the finalization station. The SIP may notify the agency of this event via email.

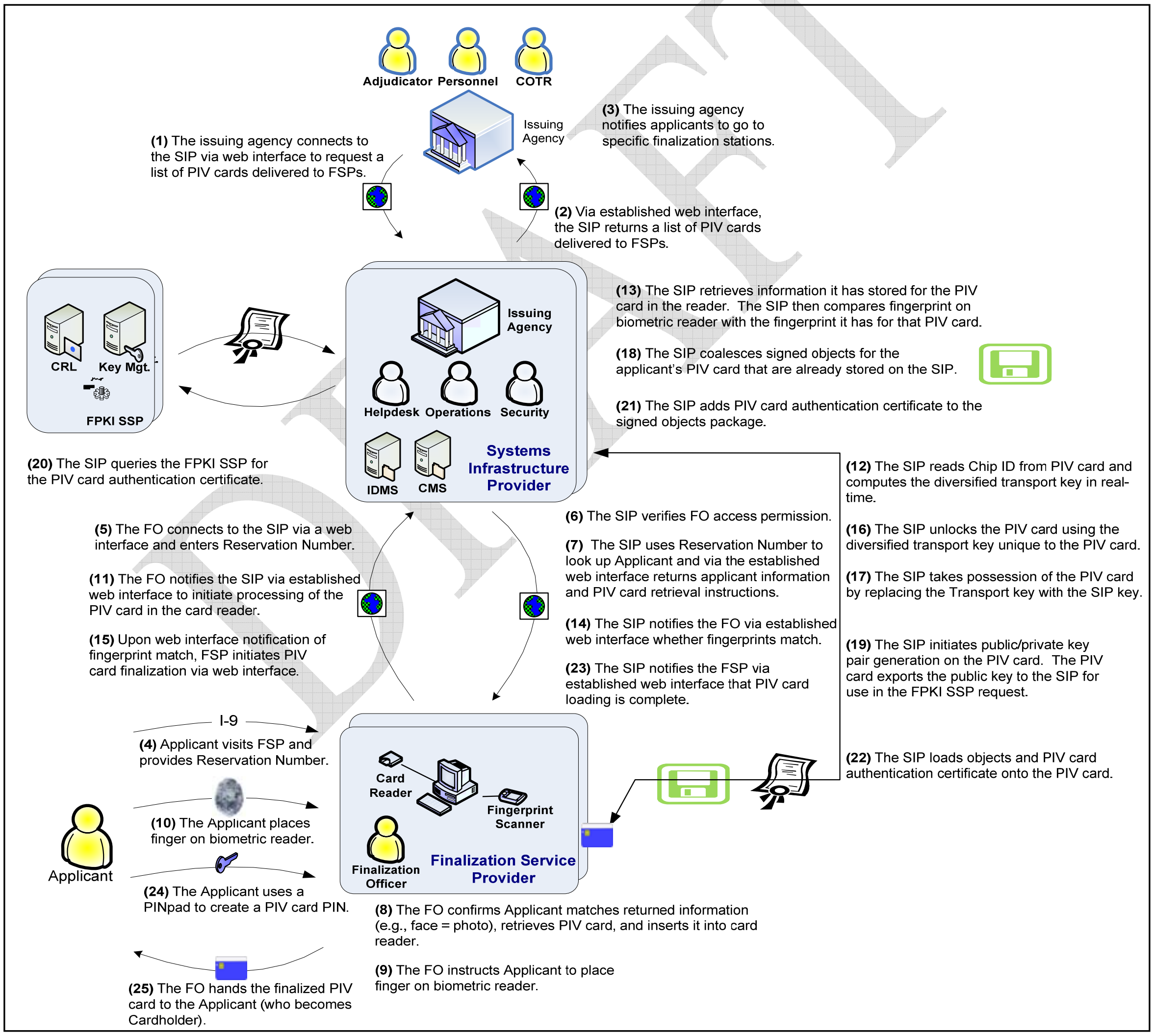
Comment [Rnote4]: What interim statuses should be noted (card personalized, card shipped). And who stores the interim statuses: the PSP and/or the SIP? Either way, additional interface transactions are required to retrieve such statuses

4.6 Card Finalization



Card Finalization is the final step in the card issuance process that binds applicants to their PIV card, and activates the OIV card for use. A Finalization Officer (FO) facilitates the card finalization process, including identity proofing, using FSP components (e.g., card reader, fingerprint scanner), and initiating SIP finalization of the PIV card.

4.6.1 Use Case F-01 PIV Card Finalization



(1) The issuing agency connects to the SIP via web interface to request a list of PIV cards delivered to FSPs.

(2) Via established web interface, the SIP returns a list of PIV cards delivered to FSPs.

(3) The issuing agency notifies applicants to go to specific finalization stations.

(4) Applicant visits FSP and provides Reservation Number.

(5) The FO connects to the SIP via a web interface and enters Reservation Number.

(6) The SIP verifies FO access permission.

(7) The SIP uses Reservation Number to look up Applicant and via the established web interface returns applicant information and PIV card retrieval instructions.

(8) The FO confirms Applicant matches returned information (e.g., face = photo), retrieves PIV card, and inserts it into card reader.

(9) The FO instructs Applicant to place finger on biometric reader.

(10) The Applicant places finger on biometric reader.

(11) The FO notifies the SIP via established web interface to initiate processing of the PIV card in the card reader.

(12) The SIP reads Chip ID from PIV card and computes the diversified transport key in real-time.

(13) The SIP retrieves information it has stored for the PIV card in the reader. The SIP then compares fingerprint on biometric reader with the fingerprint it has for that PIV card.

(14) The SIP notifies the FO via established web interface whether fingerprints match.

(15) Upon web interface notification of fingerprint match, FSP initiates PIV card finalization via web interface.

(16) The SIP unlocks the PIV card using the diversified transport key unique to the PIV card.

(17) The SIP takes possession of the PIV card by replacing the Transport key with the SIP key.

(18) The SIP coalesces signed objects for the applicant's PIV card that are already stored on the SIP.

(19) The SIP initiates public/private key pair generation on the PIV card. The PIV card exports the public key to the SIP for use in the FPKI SSP request.

(20) The SIP queries the FPKI SSP for the PIV card authentication certificate.

(21) The SIP adds PIV card authentication certificate to the signed objects package.

(22) The SIP loads objects and PIV card authentication certificate onto the PIV card.

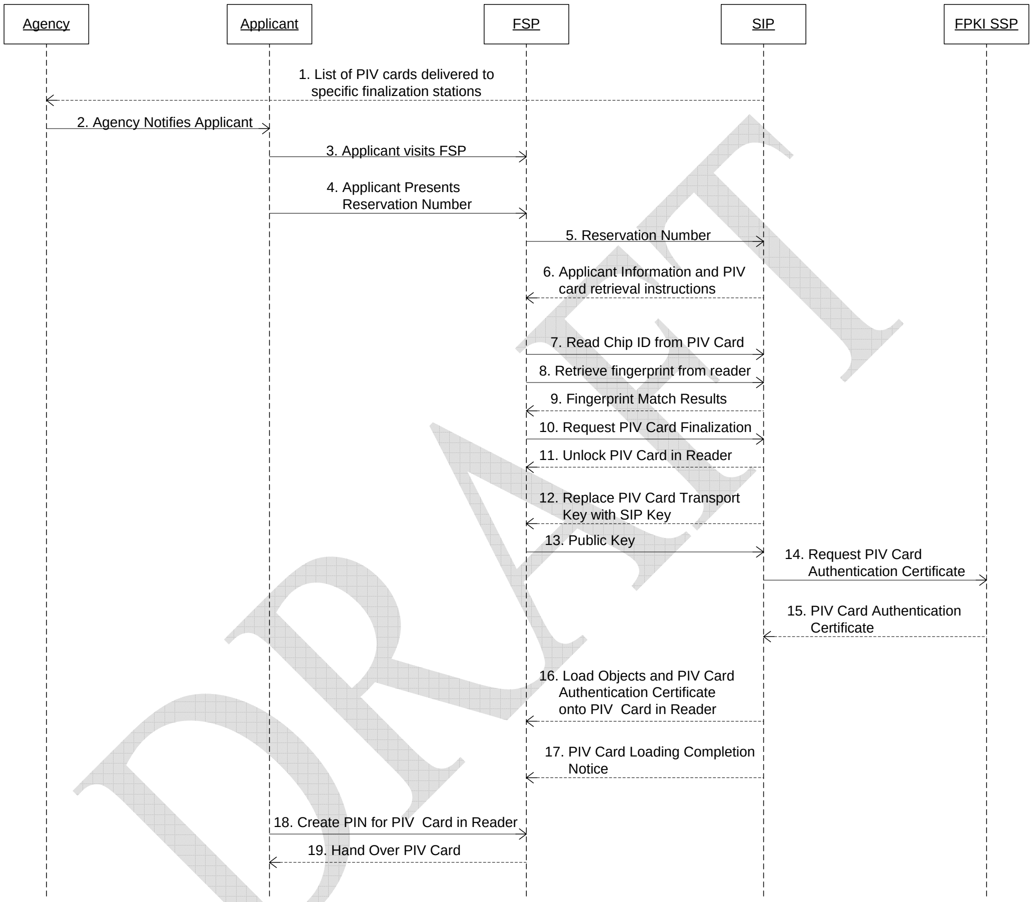
(23) The SIP notifies the FSP via established web interface that PIV card loading is complete.

(24) The Applicant uses a PINpad to create a PIV card PIN.

(25) The FO hands the finalized PIV card to the Applicant (who becomes Cardholder).

4.6.1.1 F-01 Sequence Diagram – PIV Card Finalization

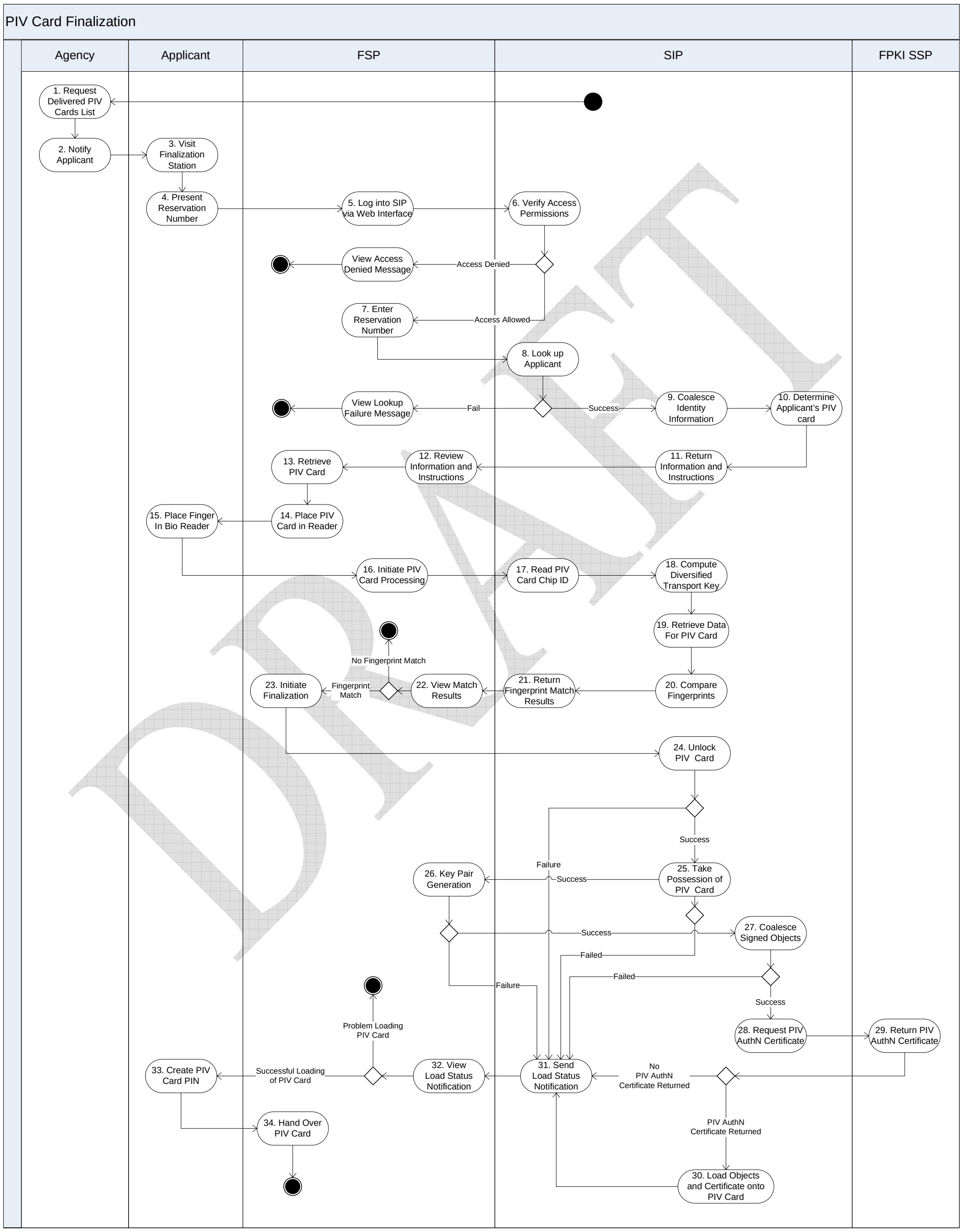
This sequence diagram illustrates when the applicant interacts with the FO and the steps performed by the FO to initiate communication between components.


Agency
Applicant
FSP
SIP
FPKI SSP
1. List of PIV cards delivered to specific finalization stations
2. Agency Notifies Applicant
3. Applicant visits FSP
4. Applicant Presents Reservation Number
5. Reservation Number
6. Applicant Information and PIV card retrieval instructions
7. Read Chip ID from PIV Card
8. Retrieve fingerprint from reader
9. Fingerprint Match Results
10. Request PIV Card Finalization
11. Unlock PIV Card in Reader
12. Replace PIV Card Transport Key with SIP Key
13. Public Key
14. Request PIV Card Authentication Certificate
15. PIV Card Authentication Certificate
16. Load Objects and PIV Card Authentication Certificate onto PIV Card in Reader
17. PIV Card Loading Completion Notice
18. Create PIN for PIV Card in Reader
19. Hand Over PIV Card

Sequence #	List of SCA Interface Specifications / Transactions
1	Email notification, SIP web interface
2	Not applicable (internal agency business process)
3	Not applicable
4	Not applicable
5	SIP web interface
6	SIP web interface
7	Card Management Interface (specific to card type, responsibility of SIP CMS)
8	Biometric Reader Interface
9	SIP web interface
10	SIP web interface
11	Card Management Interface (specific to card type, responsibility of SIP CMS)
12	Card Management Interface (specific to card type, responsibility of SIP CMS)
13	Card Management Interface (specific to card type, responsibility of SIP CMS)
14	[SIP-FPKISSP], SIP Authentication Certificate Request
15	[SIP-FPKISSP], FPKI SSP Certificate Response
16	Card Management Interface (specific to card type, responsibility of SIP CMS)
17	SIP web interface
18	PIN pad connected to card reader
19	Not applicable

4.6.1.2 F-01 Activity Diagram – PIV Card Finalization

This activity diagram illustrates how the FO facilitates card finalization and issuance.


PIV Card Finalization
Agency
Applicant
FSP
SIP
FPKI SSP
1. Request Delivered PIV Cards List
2. Notify Applicant
3. Visit Finalization Station
4. Present Reservation Number
5. Log into SIP via Web Interface
6. Verify Access Permissions
View Access Denied Message
Access Denied
7. Enter Reservation Number
Access Allowed
8. Look up Applicant
View Lookup Failure Message
Fail
Success
9. Coalesce Identity Information
10. Determine Applicant's PIV card
11. Return Information and Instructions
12. Review Information and Instructions
13. Retrieve PIV Card
14. Place PIV Card in Reader
15. Place Finger In Bio Reader
16. Initiate PIV Card Processing
17. Read PIV Card Chip ID
18. Compute Diversified Transport Key
19. Retrieve Data For PIV Card
20. Compare Fingerprints
21. Return Fingerprint Match Results
22. View Match Results
No Fingerprint Match
Fingerprint Match
23. Initiate Finalization
24. Unlock PIV Card
Success
Failure
25. Take Possession of PIV Card
Success
26. Key Pair Generation
Success
27. Coalesce Signed Objects
Failed
Failed
Failure
Success
28. Request PIV AuthN Certificate
29. Return PIV AuthN Certificate
No PIV AuthN Certificate Returned
PIV AuthN Certificate Returned
30. Load Objects and Certificate onto PIV Card
31. Send Load Status Notification
32. View Load Status Notification
Problem Loading PIV Card
Successful Loading of PIV Card
33. Create PIV Card PIN
34. Hand Over PIV Card

Activity Step #	Description
1	The agency uses a SIP web interface, on an ongoing basis, to ascertain which PIV cards have been delivered to which FSP finalization stations.
2	Upon determining newly delivered PIV cards, the agency notifies appropriate applicants to go to specific finalization stations to receive their PIV cards. The notification process is agency-specific.
3	The applicant visits the specified finalization station, per agency instructions.
4	The applicant gives the FO his/her Reservation Number.
5	Via the SIP web interface, the FO connects to the SIP using his/her PIV card. The Reservation Number prefix (i.e., left of the hyphen) indicates which SIP to connect to for this applicant (see [Agency-SIP] and [SCI Metadata]).
6	Using information in the FO's certificate, the SIP verifies that the FO has access rights. If the FO does not have access permission, the SIP returns an appropriate to the FO via the web interface, and processing ends.
7	The FO submits the Reservation Number to the SIP via the established web interface.
8	The SIP looks up the applicant associated with the Reservation Number. If the SIP fails to find a corresponding applicant, the SIP returns an appropriate message to the FO via the web interface, and processing ends. The FO provides the applicant with instructions as necessary.
9	This SIP retrieves identity for the applicant associated with the Reservation Number. This includes, but is not limited to photograph from the most recent enrollment, first name, last name. If the SIP encounters a problem retrieving applicant information, the SIP returns an appropriate message to the FO via the web interface, and processing ends. The FO provides the applicant with instructions as necessary. The FO uses the SIP web interface to update status for this applicant to indicate what problem occurred. Upon receiving the status, the SIP may notify the agency of the problem via email.
10	The SIP obtains information identifying information for the PIV card associated with this applicant (i.e., unique PIV card identifier printed on the PIV card). If the SIP encounters a problem retrieving PIV card identifying information, the SIP returns an appropriate message to the FO via the web interface, and processing ends. The FO provides the applicant with instructions as necessary. The FO uses the SIP web interface to update status for this applicant to indicate what problem occurred. Upon receiving the status, the SIP may notify the agency of the problem via email.
11	The SIP returns applicant information and PIV card identifying information to the FO via the established web interface.
12	The FO reviews the applicant information and PIV card identifying information returned via the web interface.
13	Using information returned by the SIP, the FO retrieves the PIV card for that applicant.
14	The FO puts the PIV card into the PIV card reader.
15	The FO instructs the applicant to place their finger into the biometric reader.
16	Via the SIP web interface, the FO connects to the SIP to initiate PIV card finalization. The reservation number prefix (i.e., left of the hyphen) indicates which SIP to connect to for this applicant (see [Agency-SIP] and [SCI Metadata]).

Activity Step #	Description
17	The SIP reads the chip ID from the PIV card in the reader. This is a direct read by the SIP to the card reader via a secure channel. If this step fails, processing skips to step #23.
18	In real-time, the SIP computes diversified transport key for the PIV card in the reader. If this step fails, processing skips to step #23.
19	The SIP uses the unique chip ID to retrieve information it has stored (e.g., fingerprints from enrollment) for the PIV card in the reader. If this step fails, processing skips to step #23.
20	The SIP obtains the applicant's fingerprint from the FSP biometric reader. This is a direct read by the SIP to the biometric reader over a secure channel. If the read fails, processing skips to step #23. The SIP then compares the applicant's fingerprint on the biometric reader with the fingerprint it has stored for that PIV card. This 1:1 biometric match ensures that the FSP issues the PIV card to the intended applicant.
21	Via the earlier established SIP web interface connection, the SIP notifies the FO of as to whether the fingerprint comparison resulted in a match or not..
22	The FO reviews the fingerprint comparison results returned by the SIP. If the fingerprints did not match, processing skips to step #23.
23	Upon notification from the SIP of a successful fingerprint match, the FO uses the earlier established SIP web interface connection to initiate loading of the PIV card with applicable objects and the PIV authentication certificate.
24	The SIP uses the diversified transport key it created earlier in this finalization process to unlock the PIV card (i.e., gain full access to the PIV card). If this step fails, processing skips to step #23.
25	The SIP takes possession of the PIV card by replacing the diversified transport key already on the PIV card with a diversified SIP key. The diversified SIP key ensures only that SIP can conduct card management activities on this PIV card – now and in the future. If this step fails, processing skips to step #23.
26	The SIP initiates public/private key pair generation on the PIV card. Once successfully generated, the public key is exported to the SIP for use in the subsequent request to the FPKI SSP. If this step fails, processing skips to step #23.
27	The SIP coalesces all objects to be loaded onto the PIV card. If this step fails, processing skips to step #23.
28	The SIP submits a request to the FPKI SSP for a PIV card authentication certificate – for the PIV card in the reader.
29	The FPKI SSP returns a PIV card authentication certificate for the PIV card. If this step fails (e.g., no PIV card authentication certificate returned), processing skips to step #23.
30	The SIP loads all applicable objects and the PIV card authentication certificate directly onto the PIV card in the reader. If this step fails at any point, processing skips to step #23.
31	Via the earlier established SIP web interface connection, the SIP provides the FO with a load status notification, which indicates whether the PIV card loading was successful or not. If loading was not successful, the notification includes an indication of what step failed, to allow the FO to make any adjustments, if possible, and to try again.

Comment [Rnote5]: there are more details to follow regarding how the applets and signed objects are actually created

Activity Step #	Description
32	The FO views the load completion message returned by the SIP. If there is an indication of a problem, the finalization process ends – unless the FO can make adjustments and try again. The FO uses the SIP web interface to update status for this applicant to indicate what problem occurred. Upon receiving the status, the SIP may notify the agency of the problem via email.
33	Upon successful PIV card loading, the FO instructs the applicant to create a PIN. The applicant creates the PIN using the finalization station PIN pad. If there is a problem setting the PIN, the finalization process ends. The FO uses the SIP web interface to update status for this applicant to indicate this failure. Upon receiving the status, the SIP may notify the agency of this problem via email.
34	The FO hands the PIV card to the cardholder, provides usage instructions, and uses the SIP web interface to update status for this applicant to indicate that finalization has completed successfully.

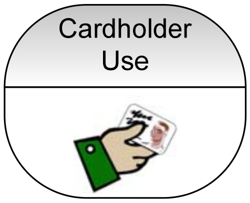
If during the finalization process the FO determines that a PIV card is defective, the FO uses the SIP web interface to update status of the applicant to indicate that the PIV card is defective. Upon receiving the status, the SIP may notify the agency of this problem via email.

The SIP monitors for abandoned PIV cards, and updates PIV card status accordingly. The determination is in accordance with pre-defined business rules. A FO finds out about abandoned PIV cards at their finalization station via the SIP web interface. The FO then processes abandoned PIV cards in accordance with pre-defined business processes.

4.7 Cardholder Use --- In development, disregard until next release

Comment [Rnote6]: Remember to include:

Defective card

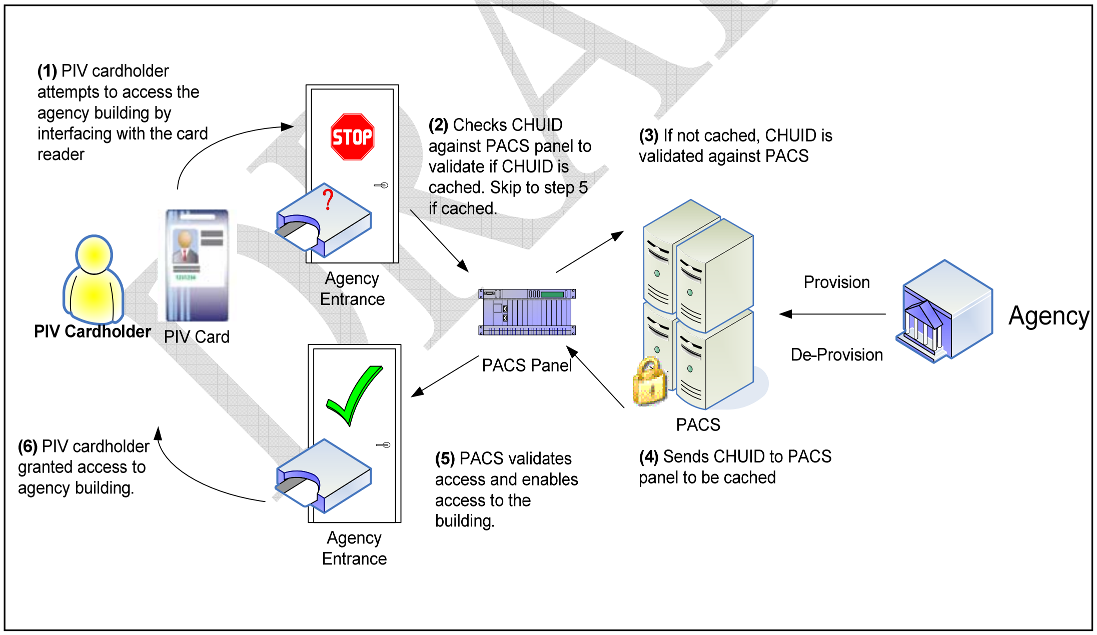


This section details the cardholder use business process. Six use cases address Cardholder Use: (1) intra-agency physical access, (2) inter-agency physical access, (3) intra-agency logical access, (4) inter-agency logical access, (5) digital signatures, and (6) encrypted messages. Sequence and activity diagrams provide additional details.

4.7.1 Use Case U-01 Intra-Agency Physical Access

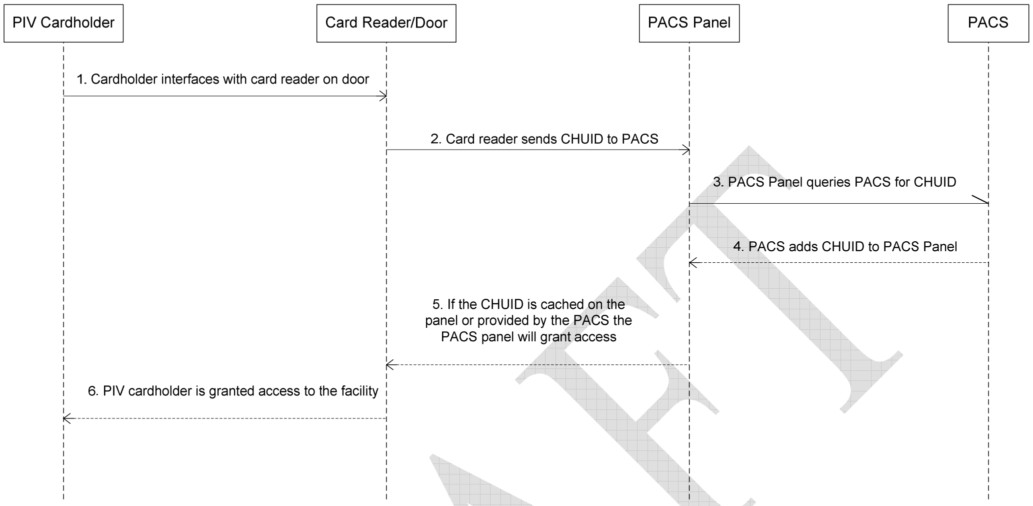
This use case illustrates how an employee or contractor is granted access to an intra-agency facility. By design, the PACS panels deployed on-site validate user access by referencing the CHUID found on the cardholder's PIV card. In an event when a CHUID is not cached on the panel, the panel will reference the PACS central system and validate whether the CHUID was provisioned into the PACS by the agency.

This use case shows provisioning is a one-way communication initiated by the agency. The agency has the option to provision or de-provision a user into their PACS.


(1) PIV cardholder attempts to access the agency building by interfacing with the card reader
STOP
?
Agency Entrance
(2) Checks CHUID against PACS panel to validate if CHUID is cached. Skip to step 5 if cached.
(3) If not cached, CHUID is validated against PACS
PIV Cardholder
PIV Card
PACS Panel
Provision
De-Provision
Agency
PACS
(6) PIV cardholder granted access to agency building.
(5) PACS validates access and enables access to the building.
(4) Sends CHUID to PACS panel to be cached
Agency Entrance

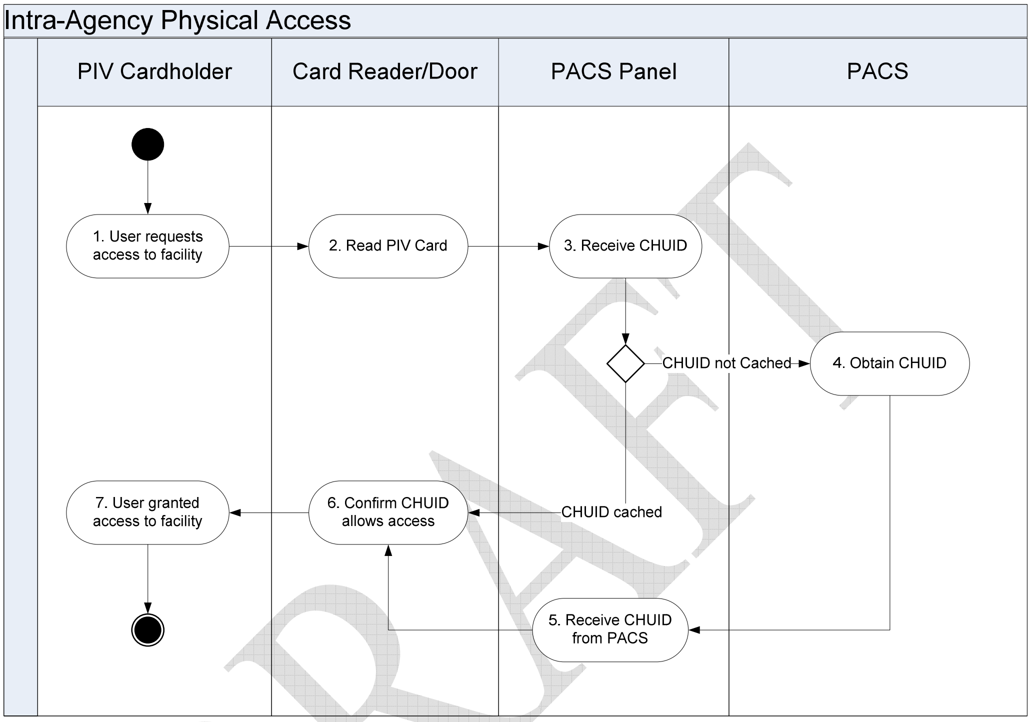
4.7.1.1 U-01 Sequence Diagram – Intra-Agency Physical Access

This sequence diagram illustrates the sequence of events and communications required to validate whether an employee or contractor can be granted physical access to a facility.


PIV Cardholder
Card Reader/Door
PACS Panel
PACS
1. Cardholder interfaces with card reader on door
2. Card reader sends CHUID to PACS
3. PACS Panel queries PACS for CHUID
4. PACS adds CHUID to PACS Panel
5. If the CHUID is cached on the panel or provided by the PACS the PACS panel will grant access
6. PIV cardholder is granted access to the facility

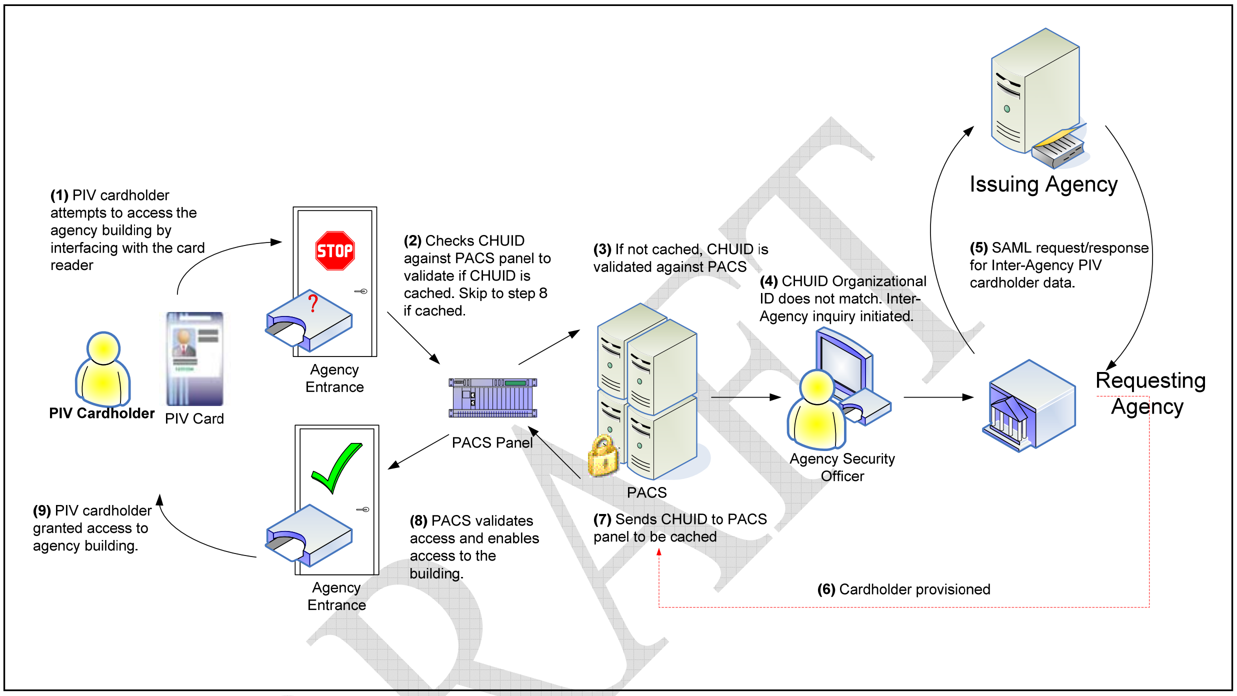
4.7.1.2 U-01 Activity Diagram **-** *Intra-Agency Physical Access*

This activity diagram illustrates the decision points and steps required to grant an employee or contractor access to a facility.


Intra-Agency Physical Access
PIV Cardholder
Card Reader/Door
PACS Panel
PACS
1. User requests access to facility
2. Read PIV Card
3. Receive CHUID
CHUID not Cached
4. Obtain CHUID
7. User granted access to facility
6. Confirm CHUID allows access
CHUID cached
5. Receive CHUID from PACS

4.7.2 Use Case U-02 Inter-Agency Physical Access

This use case illustrates an employee or contractor requesting inter-agency physical access to a facility. In comparison to use case U-01, this use case includes inter-agency backend authentication as a part of the validation process. Step 5 depicts PIV data transmitted over SOAP using SAML.



(1) PIV cardholder attempts to access the agency building by interfacing with the card reader

(2) Checks CHUID against PACS panel to validate if CHUID is cached. Skip to step 8 if cached.

(3) If not cached, CHUID is validated against PACS

(4) CHUID Organizational ID does not match. Inter-Agency inquiry initiated.

(5) SAML request/response for Inter-Agency PIV cardholder data.

(6) Cardholder provisioned

(7) Sends CHUID to PACS panel to be cached

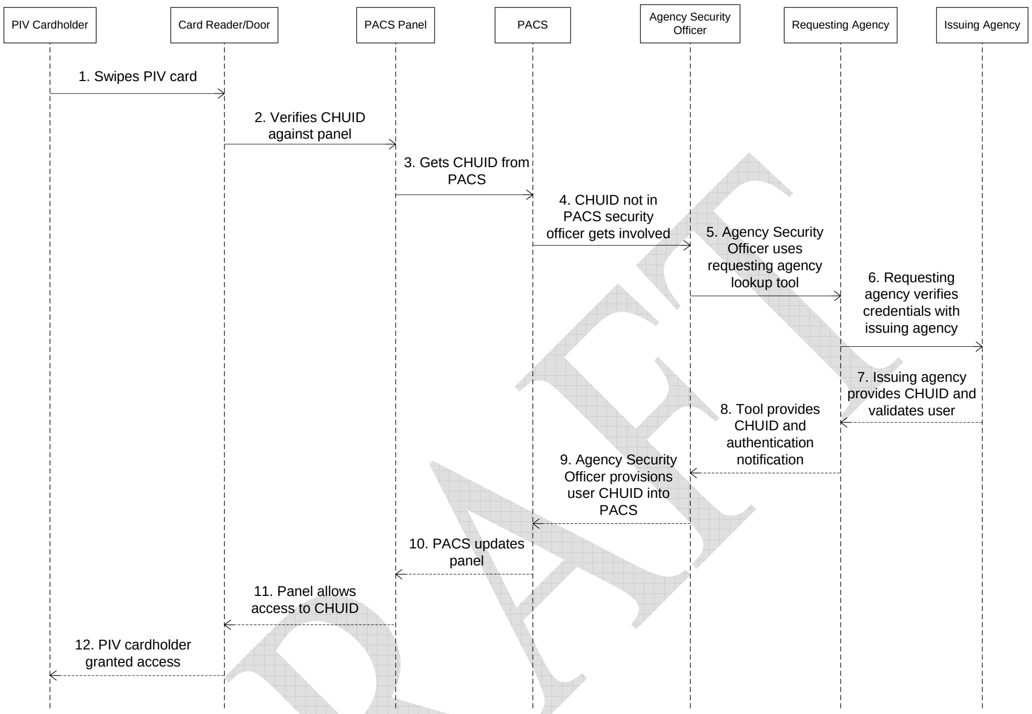
(8) PACS validates access and enables access to the building.

(9) PIV cardholder granted access to agency building.

4.7.2.1 U-02 Sequence Diagram - Inter-Agency Physical Access

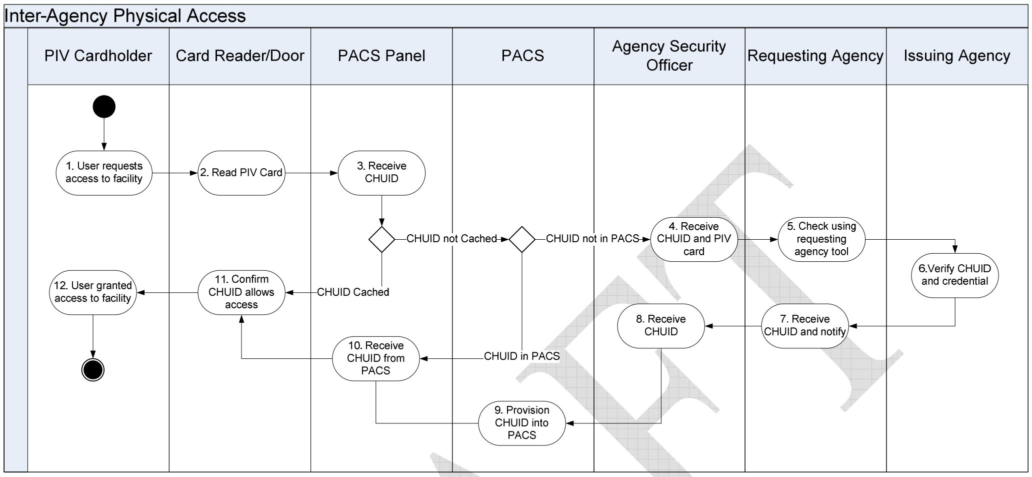
This sequence diagram illustrates the interaction between the employee or contractor and the security officer at the point of entry.

.


PIV Cardholder
Card Reader/Door
PACS Panel
PACS
Agency Security Officer
Requesting Agency
Issuing Agency
1. Swipes PIV card
2. Verifies CHUID against panel
3. Gets CHUID from PACS
4. CHUID not in PACS security officer gets involved
5. Agency Security Officer uses requesting agency lookup tool
6. Requesting agency verifies credentials with issuing agency
7. Issuing agency provides CHUID and validates user
8. Tool provides CHUID and authentication notification
9. Agency Security Officer provisions user CHUID into PACS
10. PACS updates panel
11. Panel allows access to CHUID
12. PIV cardholder granted access

4.7.2.2 U-02 Activity Diagram - Inter-Agency Physical Access

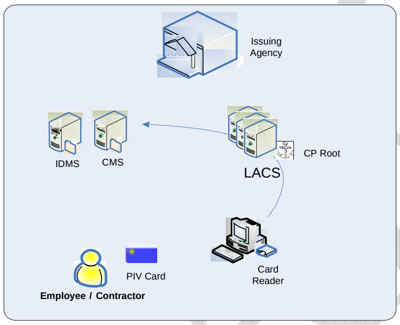
This activity diagram includes the actors and the decision point required to determine inter-agency access for PIV cardholders.


Inter-Agency Physical Access
PIV Cardholder
Card Reader/Door
PACS Panel
PACS
Agency Security Officer
Requesting Agency
Issuing Agency
1. User requests access to facility
2. Read PIV Card
3. Receive CHUID
CHUID not Cached
CHUID not in PACS
4. Receive CHUID and PIV card
5. Check using requesting agency tool
6.Verify CHUID and credential
7. Receive CHUID and notify
8. Receive CHUID
9. Provision CHUID into PACS
10. Receive CHUID from PACS
CHUID in PACS
CHUID Cached
11. Confirm CHUID allows access
12. User granted access to facility

4.7.3 Use Case U-03 Intra-Agency Logical Access

This use case illustrates how employees or contractors access intra-agency logical resources. The illustration shows the employee or contractor validating credentials against a logical access system that determines if the PIV card user is authorized to access the logical resource.

(3) PIV cardholder is granted access to pre-provisioned logical resources.

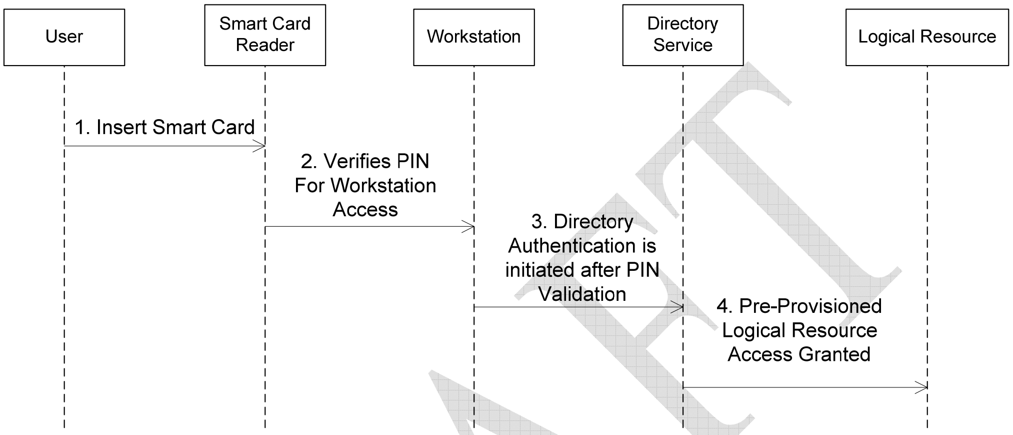


(2) PIV cardholder types his/her PIN to authenticate to the PIV card and the network.

(1) PIV cardholder inserts PIV card into smart card reader in the smart card enabled workstation.

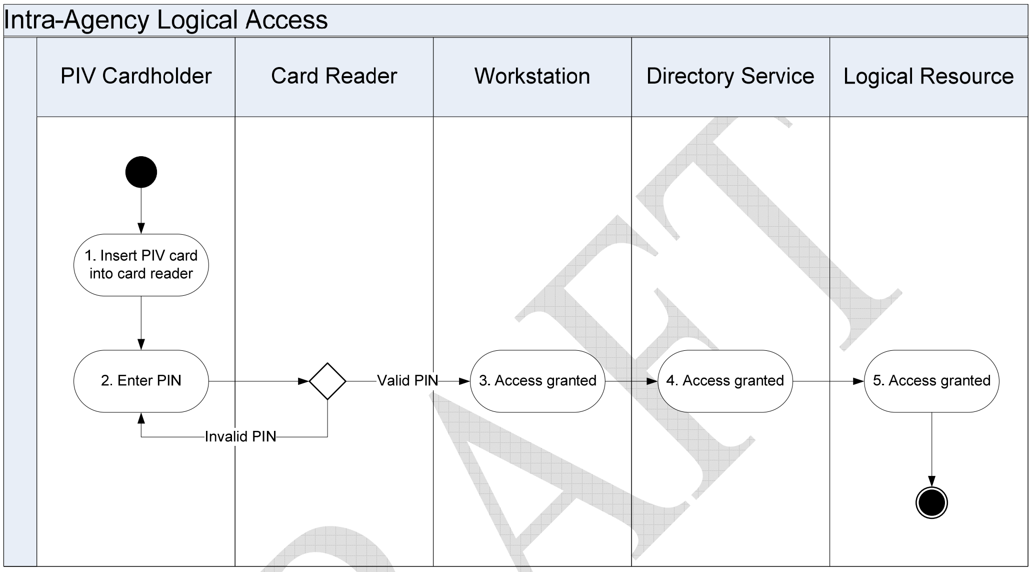
4.7.3.1 U-03 Sequence Diagram – Intra-Agency Logical Access

This sequence diagram illustrates the sequence of steps and events required to access a logical resource in a local network. The PIN is only between the PIV card and the workstation (it is not even that if there is a smart reader). That makes the certificate keys usable.


User
Smart Card Reader
Workstation
Directory Service
Logical Resource
1. Insert Smart Card
2. Verifies PIN For Workstation Access
3. Directory Authentication is initiated after PIN Validation
4. Pre-Provisioned Logical Resource Access Granted

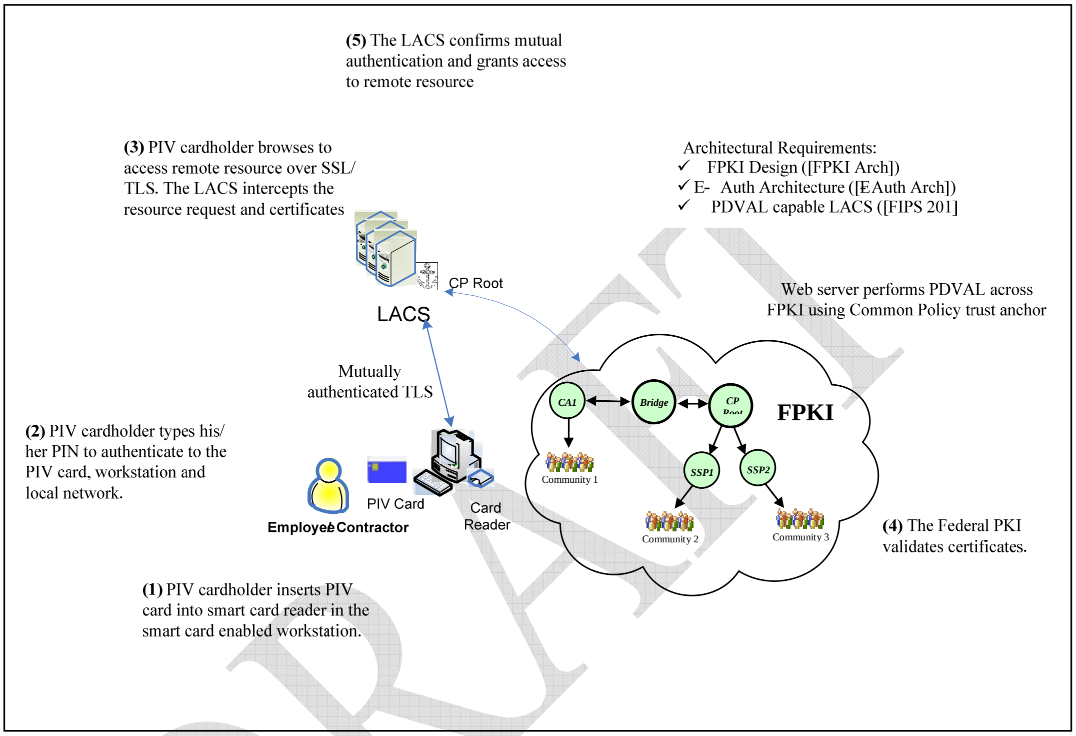
4.7.3.2 U-03 Activity Diagram – Intra-Agency Logical Access

This activity diagram illustrates a user attempting to access a local logical resource in a local network. Prior to access, the user must enter a PIN to authenticate him or herself to the PIV card, and then the network decides whether to allow access to a logical resource.



4.7.4 Use Case U-04 Inter-Agency Logical Access

This use case illustrates how users utilize their PIV cards access remote logical resources.



(5) The LACS confirms mutual authentication and grants access to remote resource

(3) PIV cardholder browses to access remote resource over SSL/TLS. The LACS intercepts the resource request and certificates

Architectural Requirements:
✓ FPKI Design ([FPKI Arch])
✓ E- Auth Architecture ([E-Auth Arch])
✓ PDVAL capable LACS ([FIPS 201]

Web server performs PDVAL across FPKI using Common Policy trust anchor

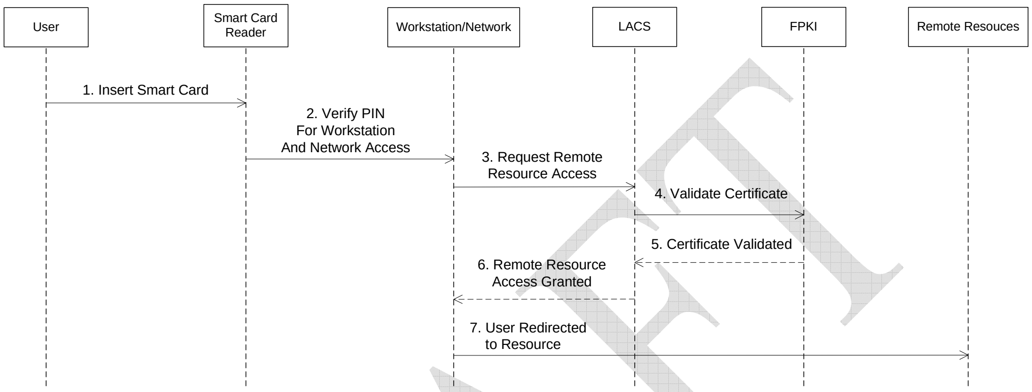
(2) PIV cardholder types his/her PIN to authenticate to the PIV card, workstation and local network.

(4) The Federal PKI validates certificates.

(1) PIV cardholder inserts PIV card into smart card reader in the smart card enabled workstation.

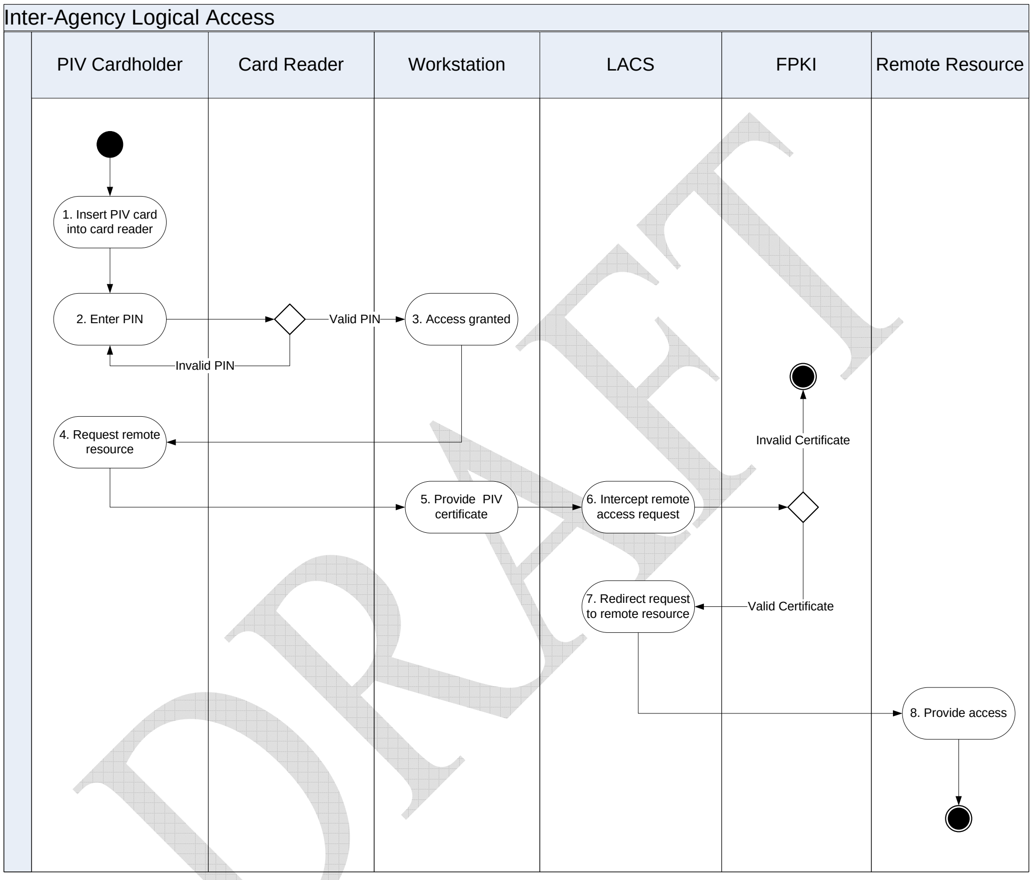
4.7.4.1 U-04 Sequence Diagram – Inter-Agency Logical Access

This sequence diagram illustrates the sequence of events and communications between internal networking components and external components (FPKI) to authorize a PIV card accessing remote logical resources. A significant difference between the sequence diagram in U-03 and U-04 is that the FPKI is introduced to validate whether the PIV card credential.


User
Smart Card Reader
Workstation/Network
LACS
FPKI
Remote Resouces
1. Insert Smart Card
2. Verify PIN For Workstation And Network Access
3. Request Remote Resource Access
4. Validate Certificate
5. Certificate Validated
6. Remote Resource Access Granted
7. User Redirected to Resource

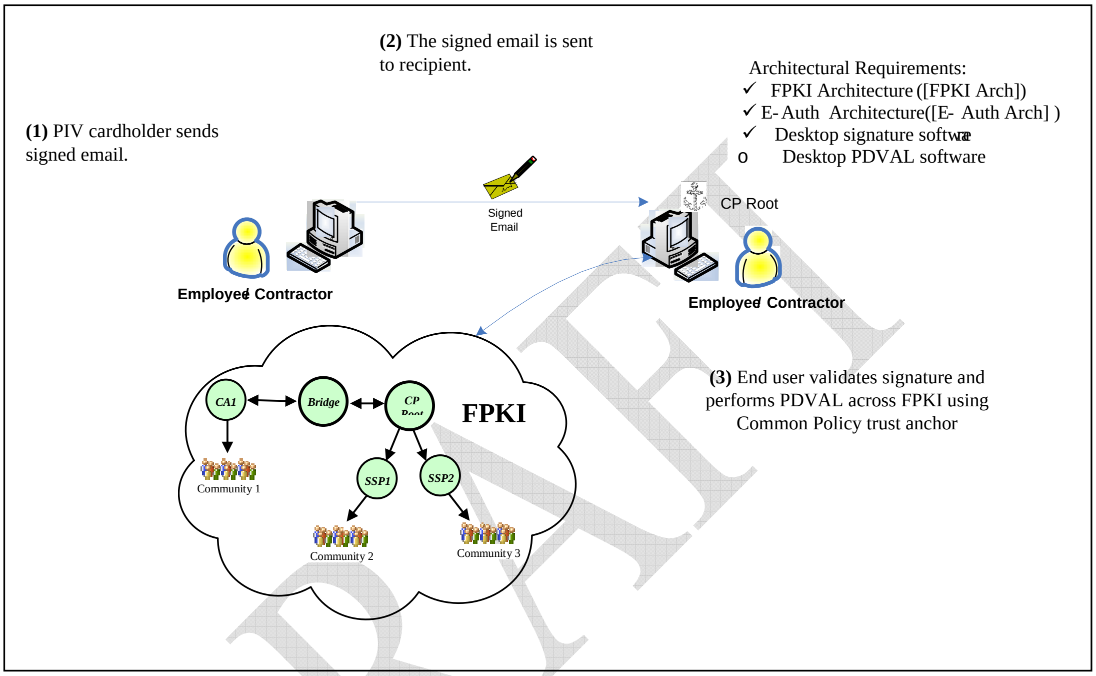
4.7.4.2 U-04 Activity Diagram – Inter-Agency Logical Access

The activity diagram illustrates the actions, steps and decisions required to complete remote physical access.


Inter-Agency Logical Access
PIV Cardholder
Card Reader
Workstation
LACS
FPKI
Remote Resource
1. Insert PIV card into card reader
2. Enter PIN
Valid PIN
Invalid PIN
3. Access granted
4. Request remote resource
5. Provide PIV certificate
6. Intercept remote access request
Invalid Certificate
Valid Certificate
7. Redirect request to remote resource
8. Provide access

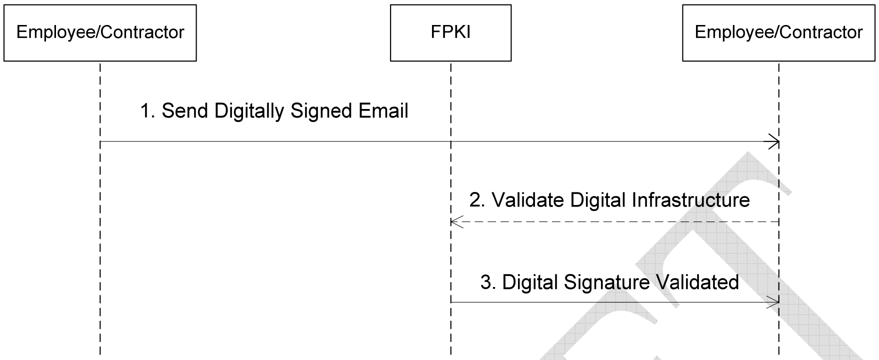
4.7.5 Use Case U-05 Digital Signatures

This use case illustrates an employee or contractor using their PIV card to sign their email. In addition, it illustrates how email recipients validate the digital signature by communicating with the FPKI.


(2) The signed email is sent to recipient.
Architectural Requirements:
✓ FPKI Architecture ([FPKI Arch])
✓ E-Auth Architecture([E- Auth Arch])
✓ Desktop signature software
o Desktop PDVAL software
(1) PIV cardholder sends signed email.
Signed Email
CP Root
Employee/ Contractor
Employee/ Contractor
(3) End user validates signature and performs PDVAL across FPKI using Common Policy trust anchor
CA1
Bridge
CP Root
FPKI
SSP1
SSP2
Community 1
Community 2
Community 3

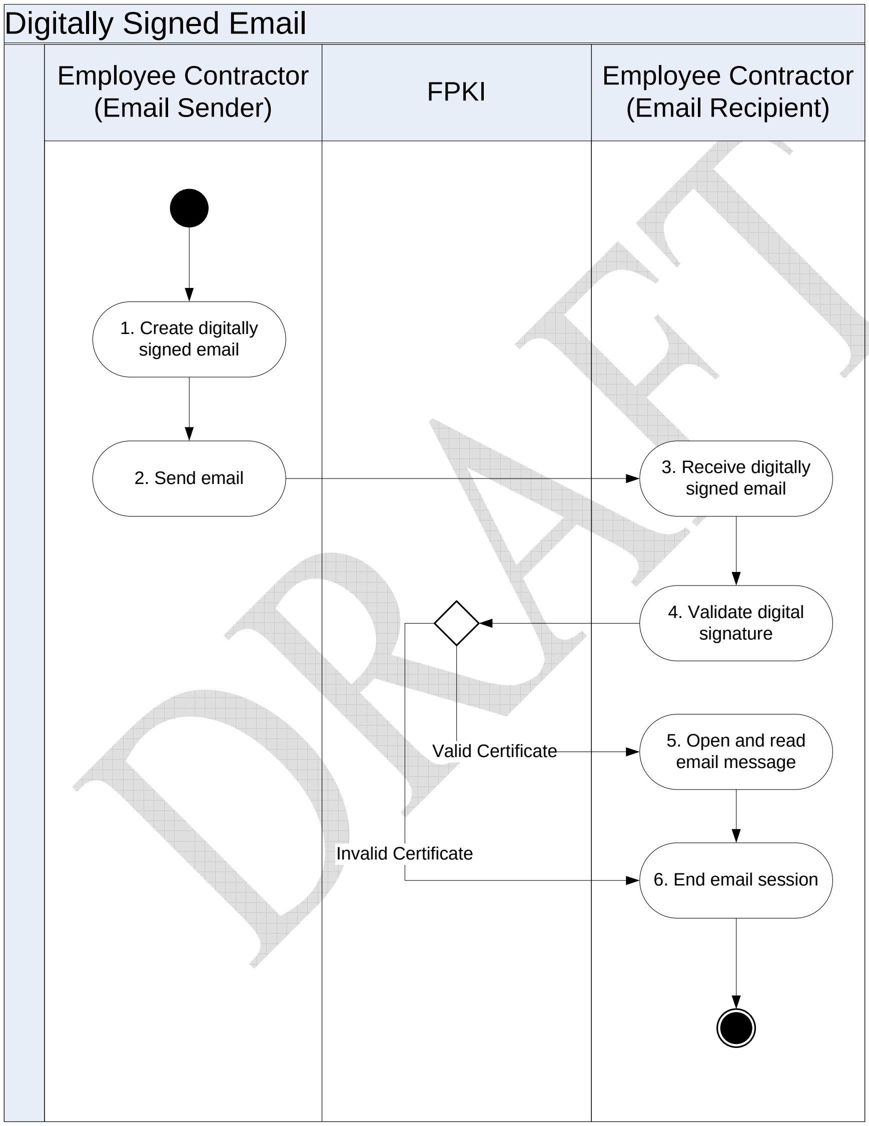
4.7.5.1 U-05 Sequence Diagram – Digital Signatures

This sequence diagram illustrates the events and communication required to digitally sign an email with a PIV card, and how the employee or contractor receiving the email validates the digital signature.


Employee/Contractor
FPKI
Employee/Contractor
1. Send Digitally Signed Email
2. Validate Digital Infrastructure
3. Digital Signature Validated

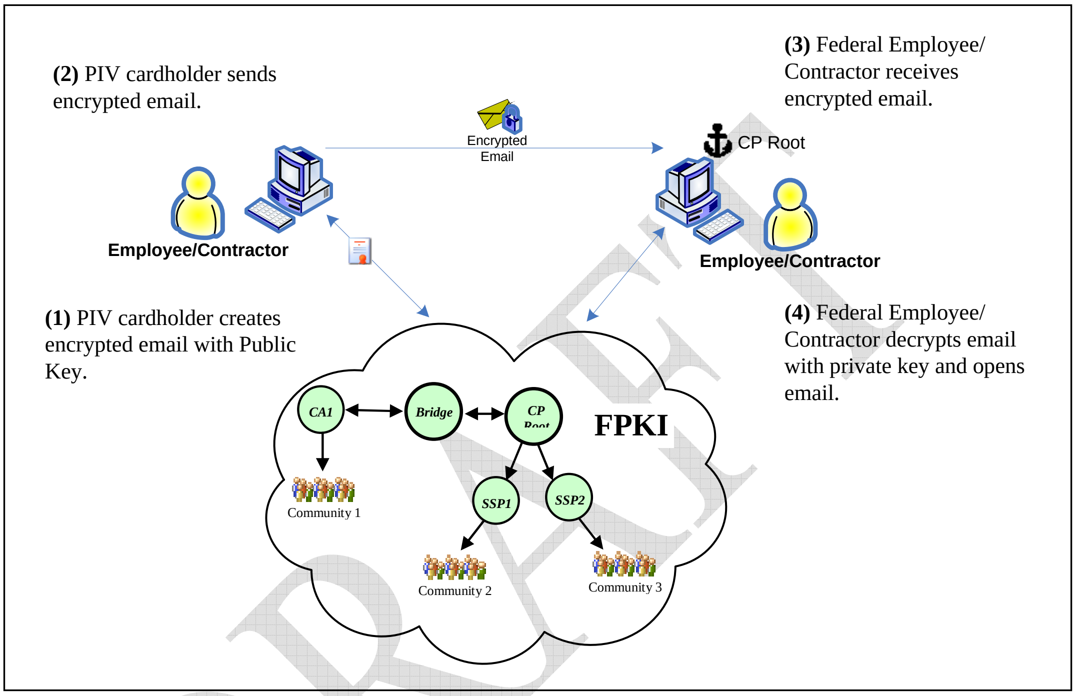
4.7.5.2 U-05 Activity Diagram – Digital Signatures

The activity diagram illustrates the FPKI's role as a validation component in the digital signature use case.


Digitally Signed Email
Employee Contractor (Email Sender)
FPKI
Employee Contractor (Email Recipient)
1. Create digitally signed email
2. Send email
3. Receive digitally signed email
4. Validate digital signature
Valid Certificate
5. Open and read email message
Invalid Certificate
6. End email session

4.7.6 Use Case U-06 Encrypted Messages

This use case illustrates an employee or contractor encrypting an email and sending it to another employee or contractor. The use case shows the importance of the FPKI and its role as a validating entity.



(1) PIV cardholder creates encrypted email with Public Key.

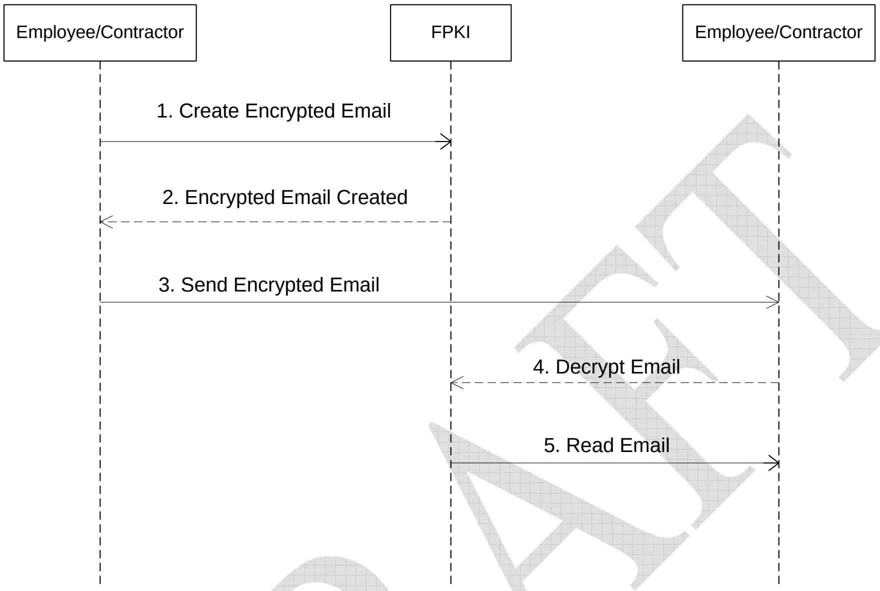
(2) PIV cardholder sends encrypted email.

(3) Federal Employee/ Contractor receives encrypted email.

(4) Federal Employee/ Contractor decrypts email with private key and opens email.

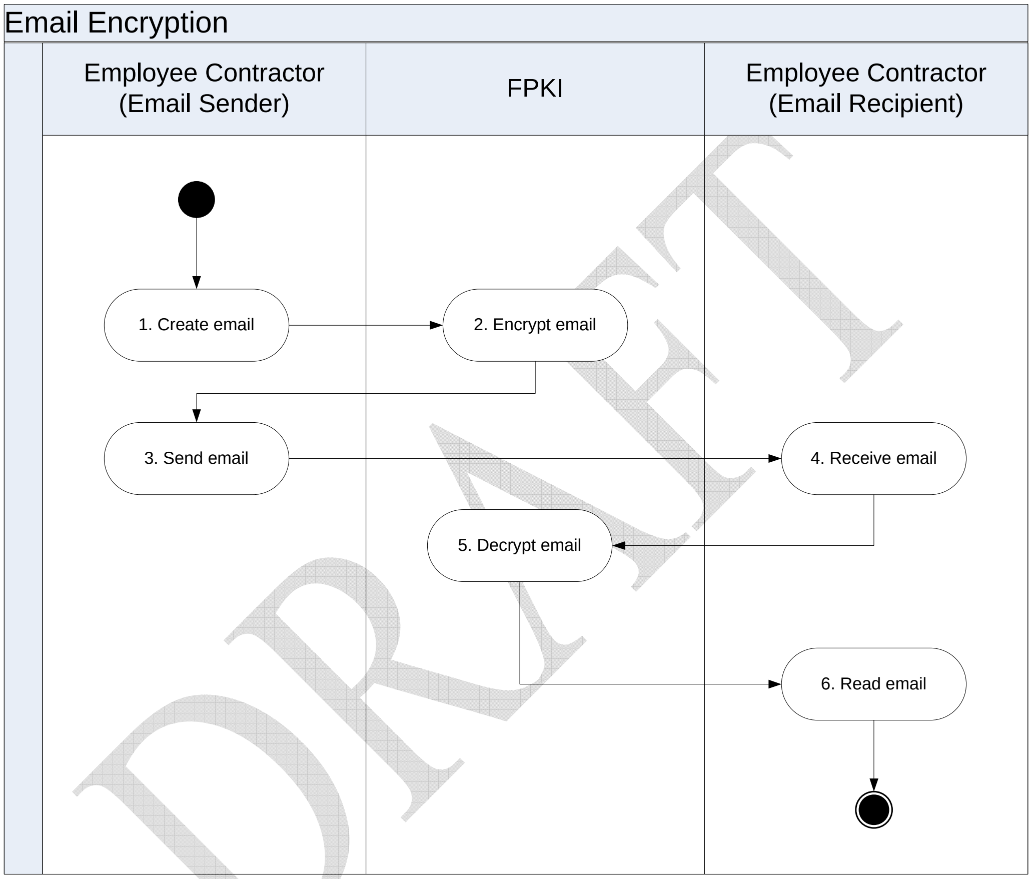
4.7.6.1 U-06 Sequence Diagram – Encrypted Messages

This sequence diagram illustrates the FPKI role when an employee or contractor uses the PIV card to encrypt or decrypt an email.

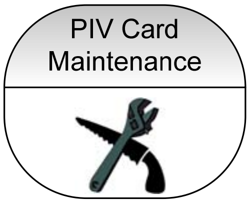


4.7.6.2 U-06 Activity Diagram – Encrypted Messages

This activity diagram illustrates the steps required to send and receive and encrypted email, and how the FPKI interacts with the sender and the recipient.



4.8 PIV Card Maintenance --- In development, disregard until next release

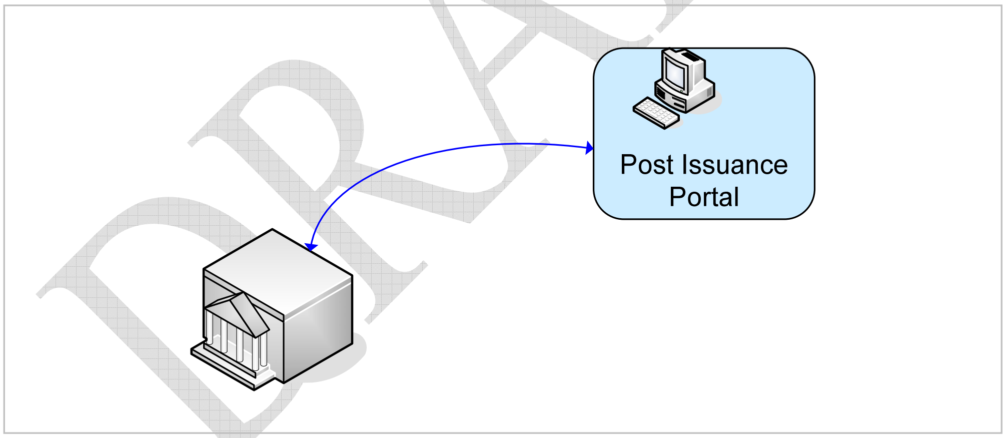


This section details the maintenance business process. A single use case addresses PIV Card Maintenance: (1) PIV card maintenance. All maintenance activities are initiated through the Post Issuance Portal. Possible maintenance actions include PIV card updates, modification, renewal, revocation, transfer to another agency, transport of cards, suspension, PIN reset, printed data change, certificate update, and sponsor change. Initiation of maintenance activities occur in the following ways: (1) by an agency informing the SIP (e.g., employee terminated), and (2) by a cardholder in the field (e.g., PIN reset).

Comment [CB7]: The Post Issuance Portal is still in discussions and its functionality and scope is not finalized.

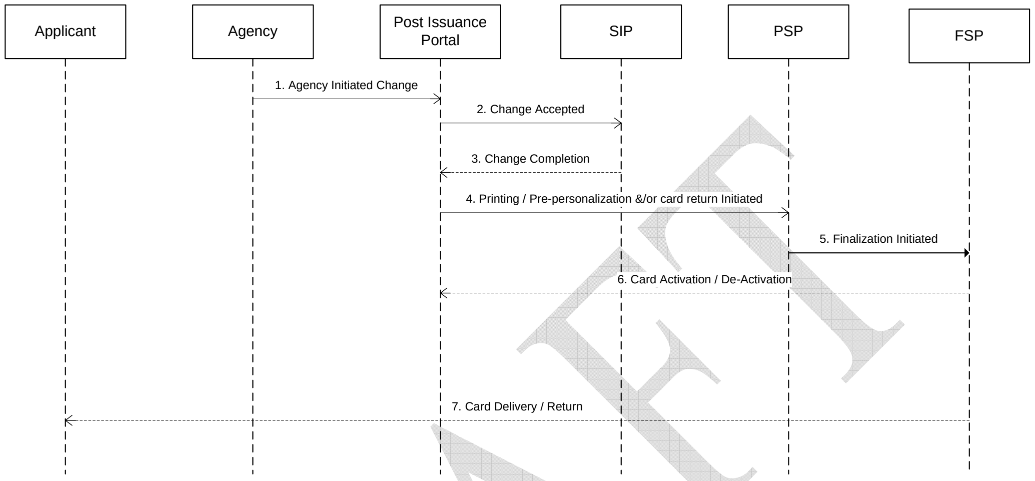
4.8.1 Use Case M-01 PIV Card Maintenance

This use case illustrates an agency initiating a PIV card maintenance activity by accessing the Post Issuance Portal.



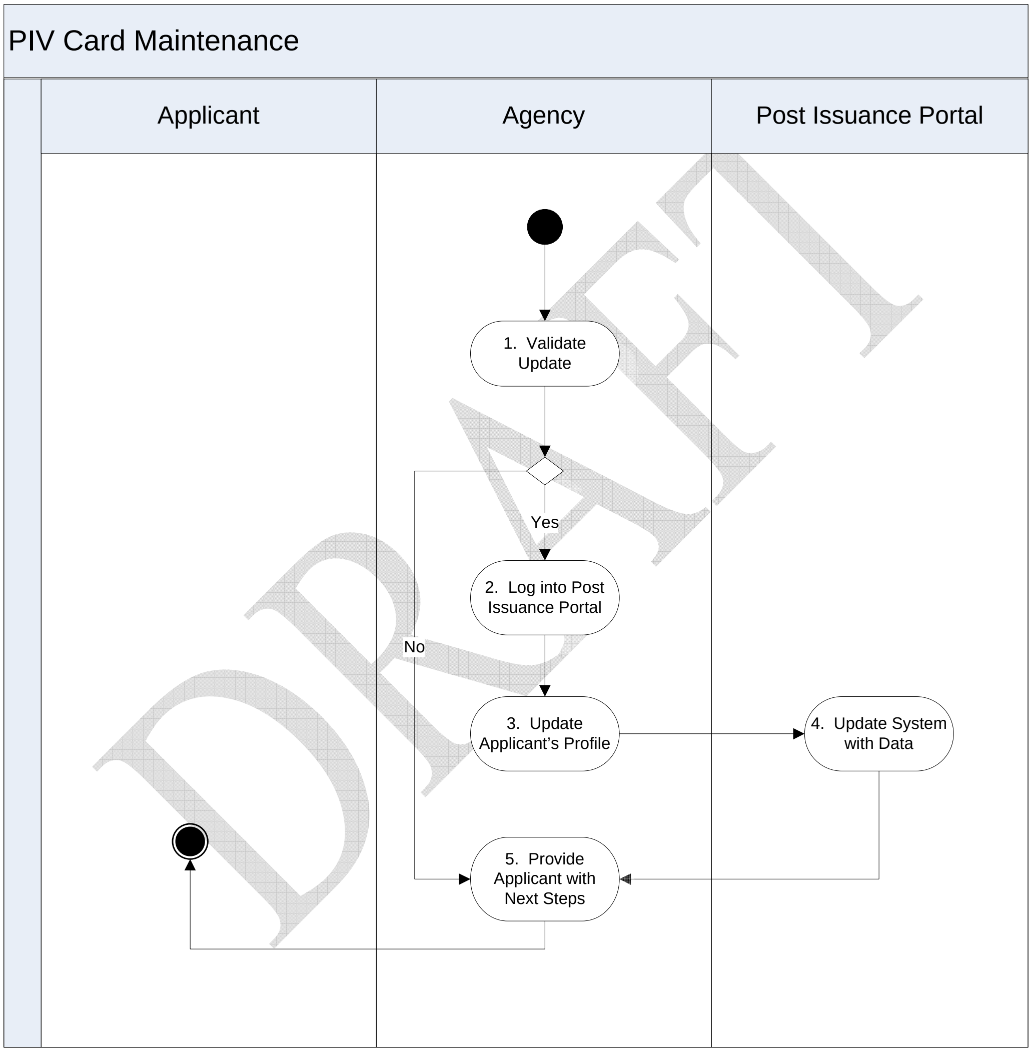
4.8.1.1 M-01 Sequence Diagram – PIV Card Maintenance

This sequence diagram illustrates the sequence for all PIV card maintenance activities.


Applicant
Agency
Post Issuance Portal
SIP
PSP
FSP
1. Agency Initiated Change
2. Change Accepted
3. Change Completion
4. Printing / Pre-personalization &/or card return Initiated
5. Finalization Initiated
6. Card Activation / De-Activation
7. Card Delivery / Return

4.8.1.2 M-01 Activity Diagram – PIV Card Maintenance

This activity diagram illustrates the entire process for PIV card maintenance. The agency and Post Issuance Portal perform the main activities.


PIV Card Maintenance
Applicant
Agency
Post Issuance Portal
1. Validate Update
Yes
No
2. Log into Post Issuance Portal
3. Update Applicant's Profile
4. Update System with Data
5. Provide Applicant with Next Steps

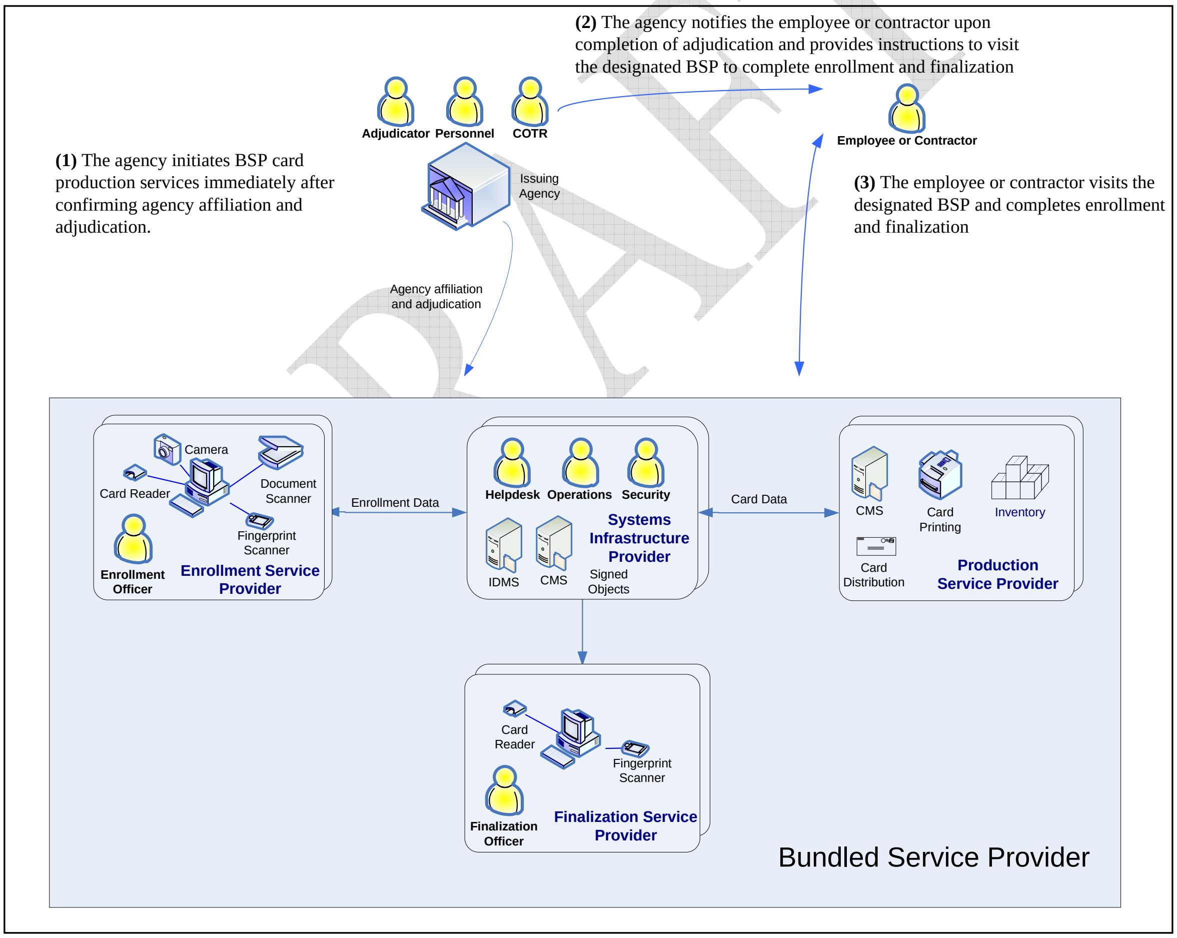
Comment [Rnote8]: Need a table

Appendix A: Bundled Service Provider

This Appendix provides an overview of the Bundled Service Provider (BSP) scenario. A BSP provides all SCI components as a single, fully integrated solution. No additional procurement or integration is required.

A1: Use Case B-01 Bundled Approach

The BSP use case illustrates the interactions between the agency, the BSP and the applicant with a primary focus on card production activities. An agency confirming applicant adjudication status to the BSP initiates card production. Adjudication triggers an applicant notification followed by direct interaction between the applicant and the BSP. The applicant may visit BSP stations individually, or the BSP may provide integrated services that include enrollment, finalization and the PIV card issuance via one station. Note that enrollment and finalization steps in this use case are oversimplified to highlight BSP card production tasks.



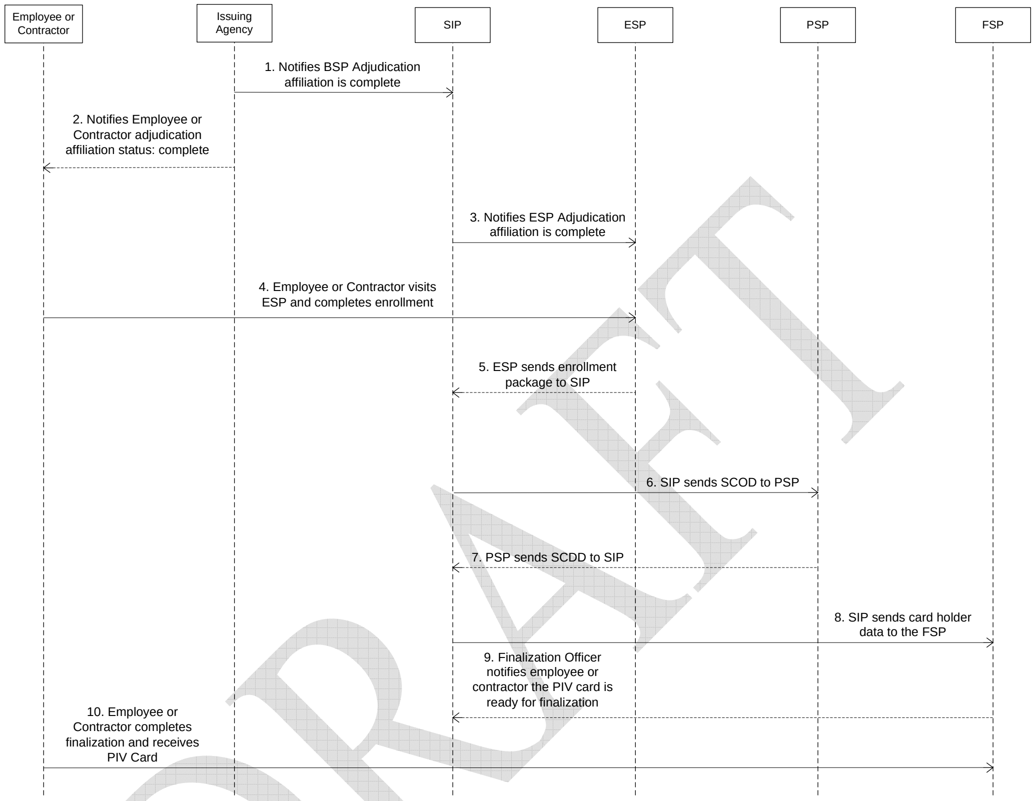
(1) The agency initiates BSP card production services immediately after confirming agency affiliation and adjudication.

(2) The agency notifies the employee or contractor upon completion of adjudication and provides instructions to visit the designated BSP to complete enrollment and finalization

(3) The employee or contractor visits the designated BSP and completes enrollment and finalization

A2: B-01 Sequence Diagram – Bundled Approach

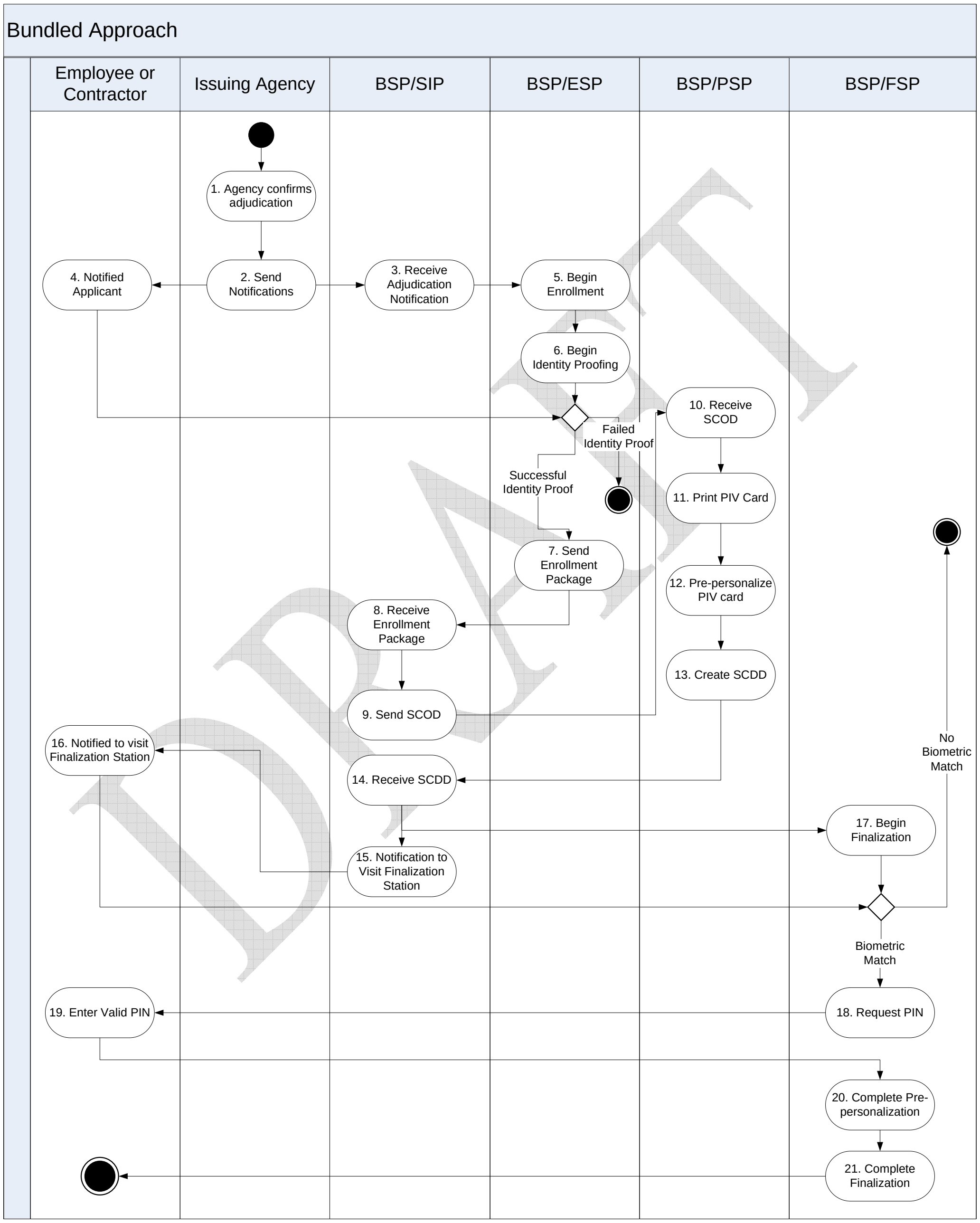
This sequence diagram illustrates the data elements exchanged between the four BSP components (SIP ESP, PSP and FSP) and the order in which data is communicated during card production.


Employee or Contractor
Issuing Agency
SIP
ESP
PSP
FSP
1. Notifies BSP Adjudication affiliation is complete
2. Notifies Employee or Contractor adjudication affiliation status: complete
3. Notifies ESP Adjudication affiliation is complete
4. Employee or Contractor visits ESP and completes enrollment
5. ESP sends enrollment package to SIP
6. SIP sends SCOD to PSP
7. PSP sends SCDD to SIP
8. SIP sends card holder data to the FSP
9. Finalization Officer notifies employee or contractor the PIV card is ready for finalization
10. Employee or Contractor completes finalization and receives PIV Card

Sequence #	List of Interface Specifications / Transactions
1	Currently, no interface specification and transaction exists
2	Currently, no interface specification and transaction exists
3	Currently, no interface specification and transaction exists
4	Currently, no interface specification and transaction exists
5	Currently, no interface specification and transaction exists
6	Currently, no interface specification and transaction exists
7	Currently, no interface specification and transaction exists
8	Currently, no interface specification and transaction exists
9	Currently, no interface specification and transaction exists
10	Currently, no interface specification and transaction exists

A3: B-01 Activity Diagram – Bundled Approach

The activity diagram illustrates the trigger and activities involved with BSP card production and pre-personalization.


Bundled Approach
Employee or Contractor
Issuing Agency
BSP/SIP
BSP/ESP
BSP/PSP
BSP/FSP
1. Agency confirms adjudication
2. Send Notifications
3. Receive Adjudication Notification
4. Notified Applicant
5. Begin Enrollment
6. Begin Identity Proofing
Failed Identity Proof
Successful Identity Proof
7. Send Enrollment Package
8. Receive Enrollment Package
9. Send SCOD
10. Receive SCOD
11. Print PIV Card
12. Pre-personalize PIV card
13. Create SCDD
14. Receive SCDD
15. Notification to Visit Finalization Station
16. Notified to visit Finalization Station
17. Begin Finalization
No Biometric Match
Biometric Match
18. Request PIN
19. Enter Valid PIN
20. Complete Pre-personalization
21. Complete Finalization

Activity Step #	Description
1	Issuing agency confirms adjudication.
2	Issuing agency informs the BSP/SIP and applicant that a PIV card can be issued
3	The BSP/SIP receives the adjudication status.
4	The applicant receives notification to visit the BSP/ESP for enrollment services.
5	The applicant arrives at the BSP/ESP whereupon enrollment begins.
6	The applicant is identity proofed using I-9 documentation. If the applicant fails identity proofing, the enrollment process ends.
7	After completing the enrollment process the enrollment data is sent to the BSP/SIP.
8	The BSP/SIP receives the enrollment data package.
9	The BSP/SIP sends a SCOD to the BSP/PSP.
10	The BSP/PSP receives the SCOD.
11	The BSP/PSP prints the PIV card based on the information provided in the SCOD.
12	The BSP/PSP pre-personalizes the PIV card based on the information provided in the SCOD.
13	The BSP/PSP creates the SCDD and sends it to the BSP/SIP.
14	The BSP/SIP receives the SCDD and stores the chip ID provided in the SCDD along with the associated identity.
15	The BSP/SIP sends a notification to the BSP/FSP that the specified applicant(s) are ready for finalization.
16	The BSP/FSP receives the notification from the BSP/SIP regarding the applicants who are ready for finalization and issuance.
17	The BSP/SIP notifies the application regarding the status of the card production.
18	The applicant receives the card production notification and is instructed to visit the FO or finalization station.
20 (a)	Prior to finalization the applicant is instructed to verify their identify using finger print scanner – Success.
20 (b)	Prior to finalization the applicant is instructed to verify their identify using finger print scanner – Failure.
21 (a)	The FO initiates finalization by asking the applicant to create a their PIN.
21 (b)	The FO will terminate the finalization process.
22	The applicant creates a secret PIN and confirms the PIN on the finalization end-user terminal.
23	The FO completes personalization PIV card activities.
24	The FO completes finalization.
25	The applicant is issued the PIV card.

Comment [Rnote9]: Needs to be fixed – per PSP/FSP decisions

Appendix B: Glossary and Acronyms

Term	Description
10-slap	Obtains only the prominent face of the finger as pressed, resulting in a normal sized "thin" fingerprint.
Adjudication	The final decision as to any employee's suitability for employment, either as a government employee or contractor, exclusively determined by the agency's adjudication authority, using at a minimum the results of the: (a) NACI, and (b) FBI National Criminal History Check.
Agency component	A component used by a single agency, it may be outsourced or operated by agency employees.
Applicant	Individual seeking a PIV card.
Backend Authentication	Uniform way for PIV issuance backends to communicate with other PIV issuance backends to determine if a credential is valid and authentic. This includes addressing at a minimum: (1) ability to authenticate and validate PIV credentials of visitors, and (2) ability for backend PIV infrastructure to make available information on changes in card validity (e.g. terminations, lost/stolen) of PIV cardholders.
Background investigation	The interests of the national security require that all persons privileged to be employed in the departments and agencies of the government shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States. This means that the appointment of each civilian employee in any department or agency of the government is subject to investigation. The scope of the investigation will vary, depending on the nature of the position and the degree of harm that an individual in that position could cause. The basic and minimum investigation required on all new Federal employees consisting of a NAC with written inquiries and searches of records covering specific areas of an individual's background during the past five years.
Bundled Services Provider (BSP)	A BSP is a single provider for all shared components required by an agency. This allows an agency to deal with one provider for all its shared component needs.
Business Use Case	A business use case is a simple generalization that captures user intentions in a technology and implementation independent manner. It captures all behavioral aspects that have cross-enterprise business significance. This allows each participant to understand and plan for conformance to the business protocol, and to establish the necessary cross-enterprise automated business processes.

Term	Description
Card Management System (CMS)	The CMS manages card lifecycle activities. The CMS interfaces with the IDMS as well as the certificate authority, card printing station, and the PIV card itself. The CMS manages the issuance and printing of a PIV card and the PKI certificate associated with that card. In addition, the CMS handles post issuance card updates, as well as card revocation, suspension, and PIN unblocks.
Card Printing System (CPS)	The CPS manages the printing and distribution of the actual PIV cards. Card printing and distribution interface directly with the CMS and the applicant and indirectly with PKI, and IDMS.
Certificate Revocation List (CRL)	A list of revoked public key certificates created and digitally signed by a Certification Authority. Any certificate listed on the CRL must not be trusted.
Certification Authority (CA)	A trusted entity that issues and revokes public key certificates. More specifically, a CA is an authority in a network that issues and manages security credentials and public keys for message encryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate. Depending on the public key infrastructure implementation, the certificate includes the owner's public key, the expiration date of the certificate, the owner's name, and other information about the public key owner.
Common Policy (FPKI Common Policy)	The FPKI Common Policy governs issuance of certificates to Federal employees, contractors and other affiliated personnel requiring PKI credentials for access to Federal systems not designated by law as national security systems.
Component	A software object, meant to interact with other components, encapsulating certain functionality or a set of functionalities. A component has a clearly defined interface and conforms to a prescribed behavior common to all components within an architecture. *(Definition derived from: Web Services Glossary - W3C Working Group Note 11 February 2004 http://www.w3.org/TR/2004/NOTE-ws-gloss-20040211)*
Componentization	Major components that support the PIV environment are identified and well defined, with clearly specified interactions and interrelationships.

Term	Description
Criminal Justice Information Services (CJIS) Division	The CJIS Division was established in February 1992 to serve as the focal point and central repository for criminal justice information services in the FBI. It is the largest Division within the FBI. Programs that were initially consolidated under the CJIS Division include the National Crime Information Center (NCIC), Uniform Crime Reporting (UCR), and Fingerprint Identification. In addition, responsibility for several ongoing technological initiatives were also transferred to the CJIS Division, including the Integrated Automated Fingerprint Identification System (IAFIS), NCIC 2000, and the National Incident-Based Reporting System (NIBRS). The CJIS Division mission is to Reduce terrorist and criminal activities by maximizing the ability to provide timely and relevant criminal justice information to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies concerning individuals, stolen property, criminal organizations and activities, and other law enforcement related data.
Diversified Key	A key derived from a master key and unique information from a PIV card (e.g. chip ID). A diversified key is unique per PIV card and cannot be reverse engineered.
Electronic Fingerprint Transmission Specification (EFTS)	Specifies certain requirements to which agencies must adhere to communicate electronically with the FBI's Integrated Automated Fingerprint Identification System (IAFIS).
Electronic Questionnaires for Investigations Processing (e-QIP)	e-QIP is part of an e-government initiative sponsored by the Office of Personnel Management. e-QIP allows applicants to electronically enter, update, and transmit their personal investigative data over a secure Internet connection to their employing agency for review and approval.
Enrollment	An applicant to whom an identity credential is to be issued provides supporting enrollment documentation for claimed identity (i.e., enrollment establishes that the individual present matches the supporting documents). Enrollment delivers a secured enrollment package to the IDMS for adjudication. There are two enrollment scenarios: • Initial Enrollment – an applicant's first ever enrollment, evidenced by no enrollment package for the applicant yet residing at the SIP; • Re-enrollment – all enrollments where an enrollment package for the applicant already resides at the SIP. Re-enrollment may occur for many reasons including, but not limited to PIV card renewal, PIV card reissuance.
Enrollment Package	Source documents (e.g., I-9 documents) and/or biometrics (e.g. photograph, fingerprints) collected from an applicant at an enrollment station as part of identity proofing.

Term	Description
Enrollment Service Provider (ESP)	ESPs provide local presence for enrollment of applicants using enrollment stations. Enrollment stations identity proof applicants in accordance with [FIPS 201] standards and I-9 documentation, and capture biometrics including picture and 10-slap fingerprints. The information captured is used for (1) background investigations, and (2) printing information on the PIV card.
Extensible Markup Language (XML)	Specification developed by the W3C. XML is a pared-down version of SGML, designed especially for Web documents. It allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations.
Federal Public Key Infrastructure (FPKI)	The FPKI is a PKI to support secure electronic commerce and electronic messaging as well as other Federal agency programs requiring the use of public key cryptography. The main issue for the FPKI is how to create certification paths between Federal agencies that will provide for reliable and broad propagation of trust. A Bridge Certification Authority (BCA) provides systematic certification paths between CAs in agencies, and outside the government. Federal CAs that meet certain standards and requirements will be eligible to cross-certify with the FBCA, thereby gaining the certification paths needed to establish interoperation between the Federal and commercial PKIs.
Finalization Service Provider (FSP)	FSPs provide local presence to finalize personalization of the cards and complete issuance to the applicant. The same organization that handles ESP operations for an agency may also manage FSP operations.
Governance (SCI Governance)	Governance comprises the organizations, policies, processes and systems that control, direct, and oversee the SCI in a comprehensive and authoritative manner. Governance ensures ongoing SCI consistency, reliability, and trustworthiness, which are the basis of agency reliance on SCI components. Examples of governance include (1) determining which SCI components can participate, and under what conditions, (2) approving issuance of credentials, (3) metadata management, and (4) SCI provider/component certification. Comprehensive SCI governance protects the best interests of the Federal government and HSPD-12.
Governing Authority (SCI Governing Authority)	The organization responsible for comprehensive SCI governance. The Governing Authority facilitates development of SCI governance policies, processes, and systems.
Homeland Security Presidential Directive-12 (HSPD-12)	"*Policy for a Common Identification Standard for Federal Employees and Contractors*" directs the promulgation of a new Federal standard for a secure and reliable form of identification issued by all Federal Agencies to their employees and contractors.

Term	Description
HSPD-12 Implementation Architecture Working Group (AWG)	The HSPD-12 Implementation Architecture Working Group convened under the auspices of the HSPD-12 Implementation Executive Steering Committee to develop an architecture that defines shared component interfaces and interactions. The AWG addressed: • What architectural components are required; • How and when architectural components interoperate to support all use cases; and • How architectural components are technically constructed.
Hypertext Transfer Protocol, Secure (HTTPS)	The protocol for accessing a secure Web server. Using HTTPS in the URL instead of HTTP directs the message to a secure port number rather than the default Web port number of 80. The session is then managed by a security protocol such as Secure Socket Layer (SSL).
I-9	Federal government Employment Eligibility Verification form. All U.S. employers are responsible for completion and retention of Form I-9 for each individual they hire for employment in the United States. This includes citizens and non-citizens. On the form, the employer must verify the employment eligibility and identity documents presented by the employee and record the document information on the Form I-9.
Identity Management System (IDMS)	The IDMS is the central component that interacts either directly or indirectly with all other components of the PIV II Architecture. The IDMS interfaces with the authoritative data source to receive applicant information, the enrollment stations to receive identity proofing information and biometrics, the card management system to initiate activities related to card issuance and card lifecycle management, and to the client logical access and physical access control systems (LACS and PACS) to provision cardholder information and updates.
Integrated Automated Fingerprint Identification System (IAFIS)	The Integrated Automated Fingerprint Identification System, more commonly known as IAFIS, is a national fingerprint and criminal history system maintained by the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division. The IAFIS provides automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses, 24 hours a day, 365 days a year. As a result of submitting fingerprints electronically, agencies receive electronic responses to criminal ten-print fingerprint submissions within two hours and within 24 hours for civil fingerprint submissions. The IAFIS maintains the largest biometric database in the world, containing the fingerprints and corresponding criminal history information for more than 47 million subjects in the Criminal Master File. The fingerprints and corresponding criminal history information are submitted voluntarily by state, local, and federal law enforcement agencies.

Term	Description
Interoperability	Agencies and Departments can rely on each other's HSPD-12 implementations. Interoperability requires technical and policy interoperability at certain key points within the SCA.
Issuing Agency	The organization that is sponsoring and providing the PIV card to an Applicant. Typically this is an organization for which the Applicant is working.
Logical Access Control System (LACS)	Grants or denies access to a particular logical resource (e.g., computer system) and includes an identification and authentication (I&A) component as well as an authorization component. The I&A component interacts with the PIV Card and uses mechanisms to identify and authenticate cardholders
Master Key	A single key that is used with PIV-unique information (e.g., chip ID) to generate "diversified" keys.
Metadata	Information necessary for SCI components (e.g., ESP, SIP, PSP, FSP, agency system) to technically interoperate. An SCI component must be configured with metadata. Failure to completely and correctly configure metadata can preclude technical interoperation, or result in unexpected consequences or negative impacts to any number of SCI components. The SCI Governing Authority maintains an authoritative copy of metadata, and distributes it to SCI providers who must use the metadata to configure their SCI components before operating. Metatadata is not sensitive information and is not expected to change very often.
Minutia	In fingerprinting terms, are the points of interest in a fingerprint, such as bifurcations (a ridge splitting into two) and ridge endings.
National Agency Check (NAC)	An integral part of all background investigations, consisting of searches of the OPM *Security/Suitability Investigations Index (SII)*, the *Defense Clearance and Investigations Index (DCII)*, the Federal Bureau of Investigation (FBI) Identification Division's name and fingerprint files, and other files or indices.
National Agency Check with Written Inquiries (NACI)	The basic and minimum investigation required on all new Federal employees consisting of a NAC with written inquiries and searches of records covering specific areas of an individual's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities). Coverage includes: – Employment, 5 years – Education, 5 years and highest degree verified – Residence, 3 years – References – Law Enforcement, 5 years – NACs
Online Certificate Status Protocol (OCSP)	On-line, real-time protocol used to determine the status of a public key certificate. OCSP overcomes the chief limitation of CRL: that updates must be frequently dowloaded to keep the client-side list current. When a user attempts to access a server, OCSP sends a request for certificate status information. The server sends back a response of "current", "expired," or

Term	Description
	"unknown."
Outsourced component	Something operated by a contractor on behalf of the government. An outsourced component may be shared, centralized, or operated for a single agency.
Path Validation and Discovery (PDVal)	Path discovery (also called path building) is the process of locating all of the intermediate certificates and certificate revocation lists (CRLs) needed to validate an end entity certificate (e.g., the end user's public key certificate) or determining that no valid certification path exists. Path validation is the process of verifying the discovered chain of certificates. Verification checks each certificate in the path for a variety of factors relevant to trust, including, but not limited to: • Verifying the digital signature on each certificate in the discovered path • Verifying that each certificate in the discovered path has not been revoked • Verifying that each certificate in the discovered path has not expired • Verifying that each certificate in the discovered path has a compatible assurance level PDVal is used to validate a public key certificate. It is a method for finding a trusted chain of certificates from an AA's trust anchor, through the FPKI, to the end user's issuing CA. It is the E-Authentication Initiative recommended approach because it simplifies management of the AA and improves security by allowing the AA to leverage the FPKI, rather than using a manual configuration process to replicate the security and policy information embedded in cross-certificates. Path building is complex and can lead to many interesting problems in complex PKIs. Two primary alternatives are the Trusted List model found in browsers, and online certificate validation services. The former relies on distribution of all trust anchors to all systems. The latter provides an external service. Certificate path validation procedures are based on the algorithm supplied in ITU-T Recommendation X.509 and further defined in Internet Engineering Task Force (IETF) Request for Comments (RFC) 3280. Certificate path processing verifies the binding between the subject distinguished name and/or subject alternative name and the subject public key defined in the target certificate. The binding is limited by constraints, which are specified in the certificates that comprise the path, and inputs that are specified by the relying party. To ensure secure interoperation of PKI-enabled applications, the path validation must be done in accordance with the X.509 and RFC 3280 specifications.

Term	Description
Personalization	PIV card surface printing (i.e., cardholder data and agency template). Personalization does not include card activation.
Physical Access Control System (PACS)	Grants or denies access to a particular physical resource (e.g., building) and includes an identification and authentication (I&A) component as well as an authorization component. The I&A component interacts with the PIV Card and uses mechanisms to identify and authenticate cardholders
Personal Identity Verification Card (PIV Card)	A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).
Pre-personalization	Initialization of PIV card electronics. This includes allocating space, creating directories, loading and instantiating applets and containers on the PIV card.
Production Service Provider (PSP)	PSPs produce and personalize PIV cards.
Provider (Component Provider)	Component providers (providers) build, deliver, and operate components. For shared components, the provider can be a commercial entity or an agency – in either case, the provider makes their component(s) available for use government wide. For agency components, the provider is the agency itself, and the components (e.g., HR system) likely already exist and simply need enhancement to interoperate with the appropriate shared component.
Public key Infrastructure Shared Service Provider (PKI SSP)	The Shared Service Providers (SSP) program is an effort by the Federal Identity Credentialing Committee (FICC) to provide federal agencies with approved entities that can supply PKI services consistent with Federal Common Policy terms. SSP is a managed service solution that enables customers to use a single badge at multiple facilities for both physical and logical access. In March 2004, GSA's Office of Government-wide Policy announced its intent to establish a certified Shared Service Providers program list for PKI services.
Reissue (Reissuance)	Replacement of something (e.g., PIV card, PIV certificate) not yet expired.
Renew (Renewal)	Replacement of something (e.g., PIV card, PIV certificate) expired.
Shared component	A component that is used by more than one agency, typically provided by a service provider.
Shared Component Architecture (SCA)	The conceptual technical design of the HSPD-12 shared service solution. Providers must comply with the architecture and its associated technical interface specifications;
Shared Component Infrastructure (SCI)	Instantiation of the shared component architecture. This is the operational environment with components interoperating;

Term	Description
Signed Objects	Cryptographically protected data objects on the PIV card (e.g., CHUID, fingerprints, PIV card authentication certificate). See [FIPS 201] for details.
SIP Card Management Key (SIP Key)	Card management key (loaded on the PIV card) used by a SIP to bind the PIV card to that SIP (i.e., only that SIP has access to the PIV card for card management purposes). SIP keys are derived or "diversified" using a generic secret (i.e. master SIP key) and information unique to the specific PIV card (e.g. the chip ID).
Smart Card Delivery Descriptor	XML based descriptor that describes the attributes (including the chip ID) created by the PSP during card production and pre-personalization. For a comprehensive list of attributes included in the Smart Card Delivery Descriptor reference [SIP-PSP].
Smart Card Order Descriptor	XML based descriptor that describes the required attributes used by the PSP to complete card production and pre-personalization. For a comprehensive list of attributes included in the Smart Card Order Descriptor reference *The* [SIP-PSP].
SOAP	Lightweight XML-based messaging protocol used to encode the information in Web service request and response messages before sending them over a network. It consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined data types, and a convention for representing remote procedure calls and responses. SOAP messages are independent of any operating system or protocol and may be transported using a variety of Internet protocols, including MIME and HTTP.
Sponsorship	An agency-authorized individual substantiates the need for a PIV credential to be issued to an individual (i.e, employee, contractor), and provides sponsorship to the individual. The PIV Sponsor requests the issuance of a PIV credential to the individual, who is then considered and applicant.
Suitability	Suitability is not about job skills, but rather is about lack of criminal history, an upstanding character, and an evidenced loyalty to the United States. These determinations come out in the background investigation. Suitability is in addition to proving who an individual is. The NACI or higher, helps agencies make this suitability determination regardless of their job skills that come out in the interviews and resume. The final decision as to any employee's suitability for employment, as either a government employee or contractor, is exclusively with the agency's adjudication authority. At a minimum, the following results are needed to adjudicate: ▪ NACI; and ▪ FBI National Criminal History Check
Systems Infrastructure Provider (SIP)	SIPs provide the software functionality required to manage PIV credentials. SIPs build, host, and operate software that provides agencies with critical IDMS and Card Management System (CMS) functionality.
System Use Case	A system use case illustrates design. It is more detailed than a

Term	Description
(Technical Use Case)	business use case and is technology-oriented. Technical use cases describe the high-level implementation of the system, which may include internal details of process flows such as messages transmitted and web service operations.
Transport Card Management Key (Transport Key)	Card management key (loaded on the PIV card) used to lock a PIV card (e.g., during shipment from PSP to FSP). This prevents unauthorized access to and use of the PIV card. Transport keys are derived or "diversified" using a generic secret (i.e. master transport key) and information unique to the specific PIV card (e.g. the chip ID).
Transport Layer Security (TLS)	TLS is a protocol created to provide authentication, confidentiality and data integrity between two communicating applications. TLS is based on a precursor protocol called “The Secure Sockets Layer Version 3.0” (SSL 3.0) and is considered to be an improvement to SSL 3.0. TLS is defined by [RFC 2246] and [RFC 3546]. TLS is effectively SSL version 3.1.
Trust Anchor	A trust anchor is a trusted public key certificate or trusted root certificate used to assert the trust of another public key certificate. That is, a trust anchor is signed by the private key of a CA you and others trust. A system that has installed a particular CA’s trust anchor will trust any public key certificate issued by that CA. Trust anchors are important in certificate path discovery and validation.
Trusted (Trusted Actor)	A participant or system in a business process whose identity and/or action(s) can be relied upon because of their conformance to [SCI Trust] or use of a PIV card.
Use Case	A methodology used in system analysis to identify, clarify, and organize system requirements.

Acronym	Abbreviation For
AuthN	Authentication
AuthZ	Authorization
BPEL	Business Process Engineering Language
BSP	Bundled Services Provider
CA	Certification Authority
CHUID	Cardholder Unique Identifier
CJIS	Criminal Justice Information Services
CMS	Card Management System
CPS	Card Printing System
CRL	Certificate Revocation List
CVS	Clearance Verification System
DCII	Defense Clearance and Investigations Index
EFTS	Electronic Fingerprint Transmission Specification
EO	Enrollment Officer
e-QIP	Electronic Questionnaires for Investigations Processing
ESP	Enrollment Service Provider
FASC-N	Federal Agency Smart Credential Number
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FO	Finalization Officer
FPKI	Federal Public Key Infrastructure
FYI	For Your Information
HR	Human Resources
HSPD-12	Homeland Security Presidential Directive #12
HTTPS	Hypertext Transfer Protocol, Secure
IAFIS	Integrated Automated Fingerprint Identification System
ID	Identifier
IDMS	Identity Management System
IT	Information technology
LACS	Logical Access Control System
NAC	National Agency Check
NACI	National Agency Check with Written Inquiries
NIST	National Institutes of Science and Technology
OCSP	Online Certificate Status Protocol
OPM	Office of Personnel Management
PACS	Physical Access Control System
PDVal	Path Discovery and Validation
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key infrastructure
PSP	Production Service Provider
RA	Registration Authority
SCA	HSPD-12 Shared Component Architecture
SCDD	Smart Card Delivery Descriptor
SCOD	Smart Card Order Descriptor
SII	Security/Suitability Investigations Index

Acronym	Abbreviation For
SIP	Systems Infrastructure Provider
SSL	Secure Socket Layer
SSP	Shared Service Provider
TLS	Transport Layer Security
XML	Extensible Markup Language