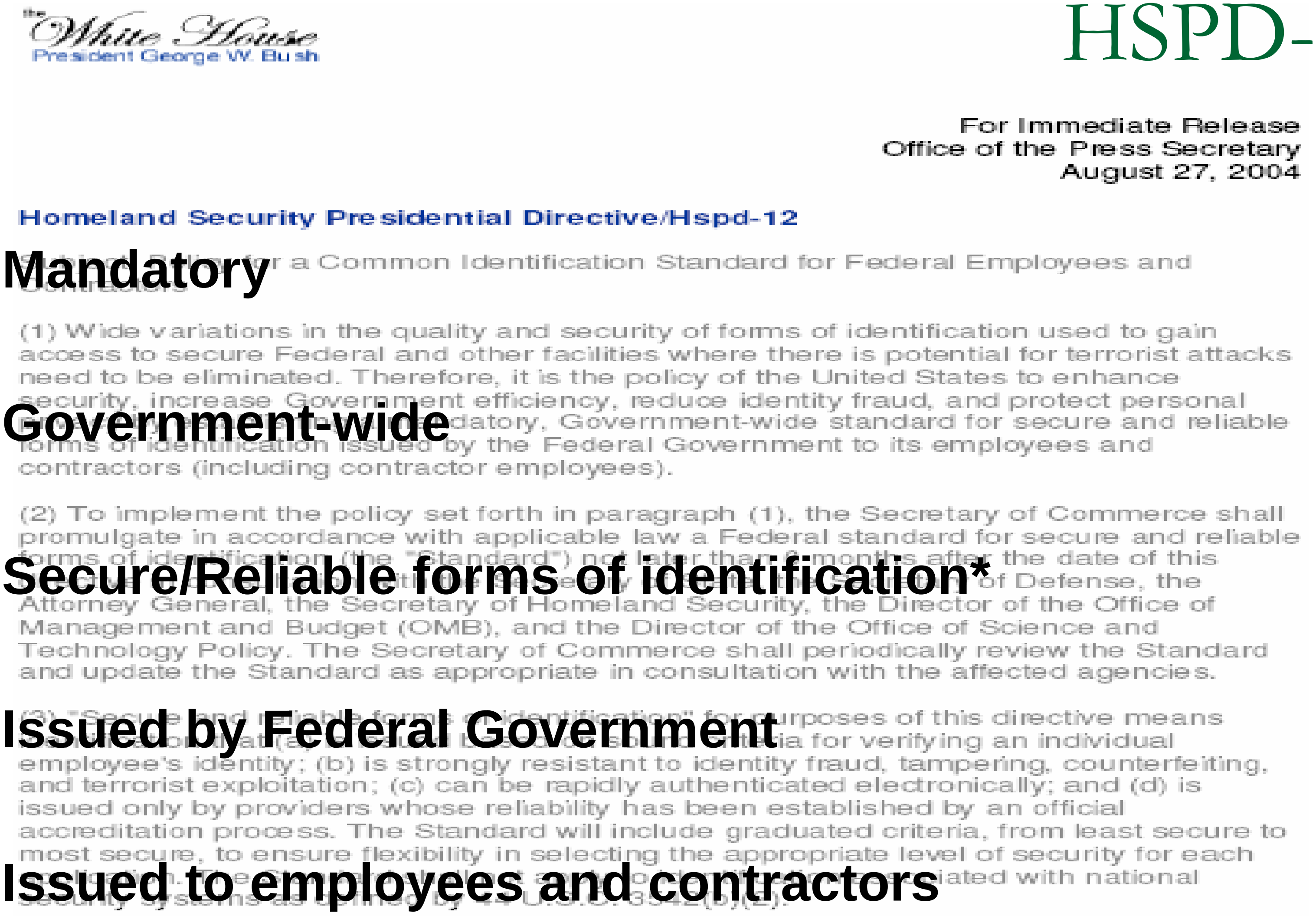
HSPD-12 – What has happened so far. . .

Judith Spencer
Chair, Federal Identity Credentialing
Office of Governmentwide Policy
U.S. General Services Administration

August 27, 2004 – The Mandate HSPD-12



the White House
President George W. Bush

For Immediate Release
Office of the Press Secretary
August 27, 2004

Homeland Security Presidential Directive/Hspd-12

Subject: Policy for a Common Identification Standard for Federal Employees and Contractors

(1) Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

(2) To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.

(3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).

- ➔ **Mandatory**
- ➔ **Government-wide**
- ➔ **Secure/Reliable forms of identification***
- ➔ **Issued by Federal Government**
- ➔ **Issued to employees and contractors**

Calls for. . .

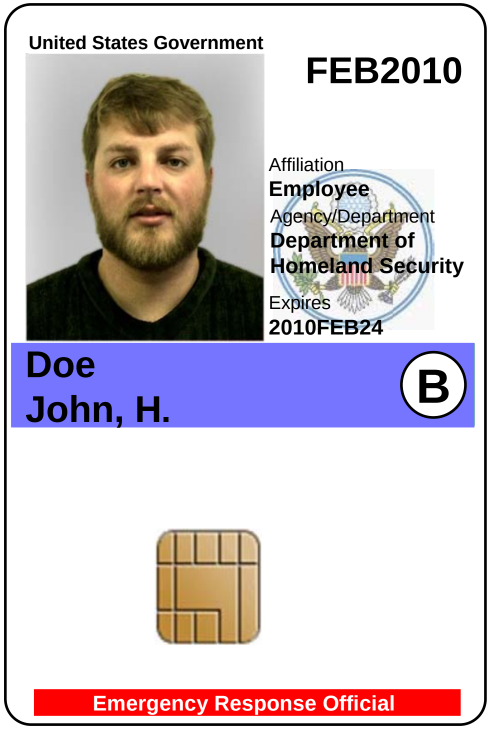
- A new Federal Standard for secure and reliable forms of identification
- Use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems.

February 25, 2005 – The Standard FIPS 201

Personal Identity Verification for Federal Employees and Contractors

- Part 1: Personal Identity Verification System
  - Defines minimum requirements for identity proofing, registration and issuance
- Part 2: Technical interoperability among PIV systems
  - Card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card.
  - Physical card characteristics, storage media, and data elements that make up identity credentials

The Card – Physical Attributes



United States Government

FEB2010

Affiliation
Employee
Agency/Department
Department of Homeland Security
Expires
2010FEB24

Doe
John, H.

B

Emergency Response Official

- Governed by SP 800-104
- Card face indicates
  - Name
  - Affiliation (Employee/Contractor)
  - Expiration Date
  - First Responders
  - Citizenship
- Color codes indicate Affiliation:
  - White (no color) - Employee
  - Blue – Foreign National
  - Green – Contractor

The Card – Electronic Attributes

- Contactless Interface
  - CHUID
- Contact Interface
  - Card Capability
  - CHUID
  - Printed Information (optional)
  - Biometrics
    - Fingerprint Minutiae
    - Facial Image (optional)
  - Digital Certificates
    - PIV Authentication
    - Signature (optional)
    - Key Management (optional)
    - Card Authentication (optional)
  - Security Object

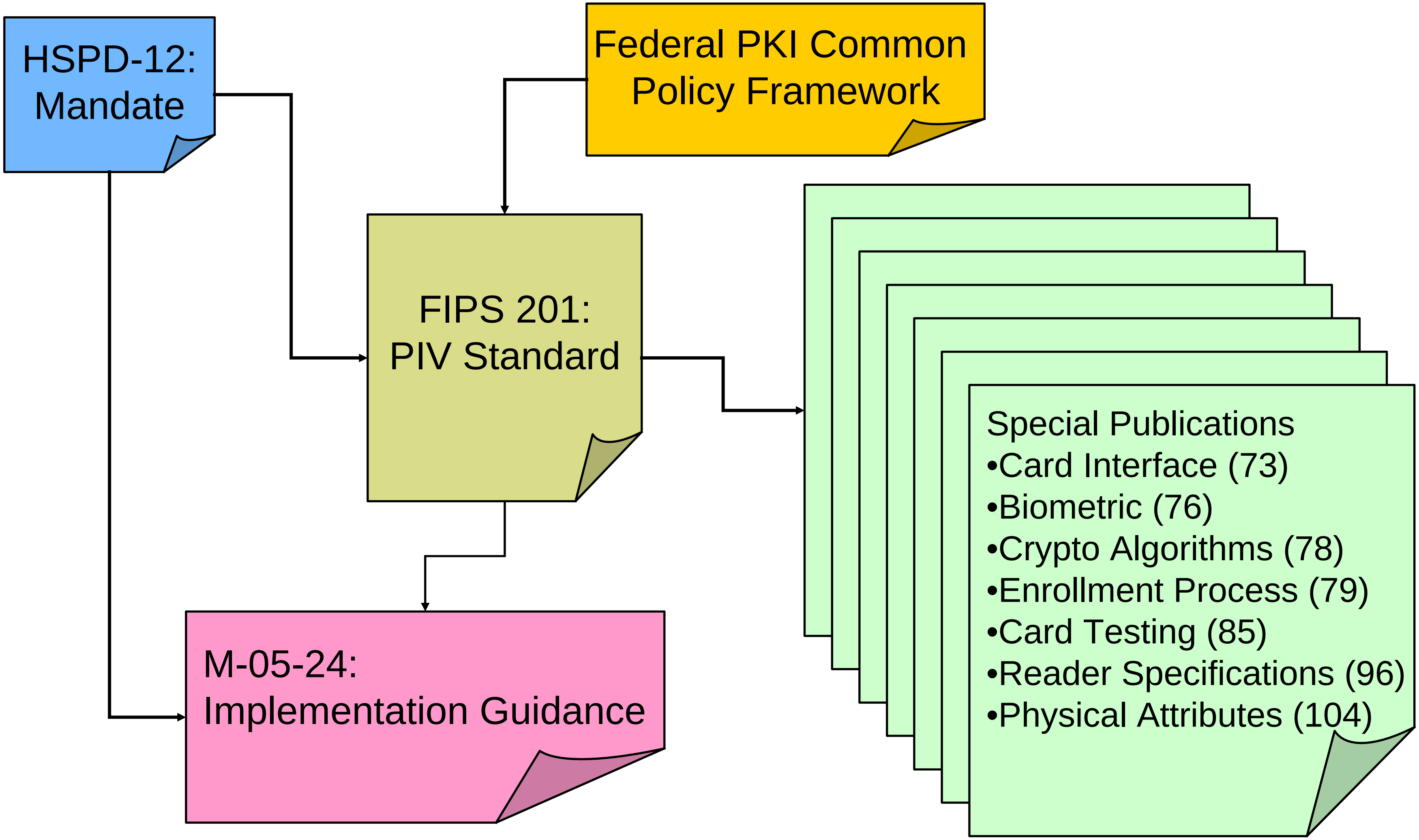
Digital Credentialing

- Credentials must be either:
  - Issued from an Agency Enterprise PKI participating in the Federal Bridge federation (only to that agency's employees and contractors).
  - Issued by a Federal PKI Certified Shared Service Provider
- Credentials must conform to Special Publication 800-78
- Shared Service Providers are governed by the X.509 U.S. Federal PKI Common Policy Framework, commonly referred to as COMMON.

August 5, 2005 – Policy Guidance OMB M-05-24

- Defines “Employees,” “Contractors,” “Federally-controlled Facilities,” and “Federally-controlled Information Systems.”
- Provides a schedule for implementing FIPS 201 – Part 1
- Provides guidance on implementing FIPS 201 – Part 2
  - Deployment
  - Acquisition
  - Privacy
  - Other Considerations

Standards and Guidance for HSPD-12



HSPD-12: Mandate

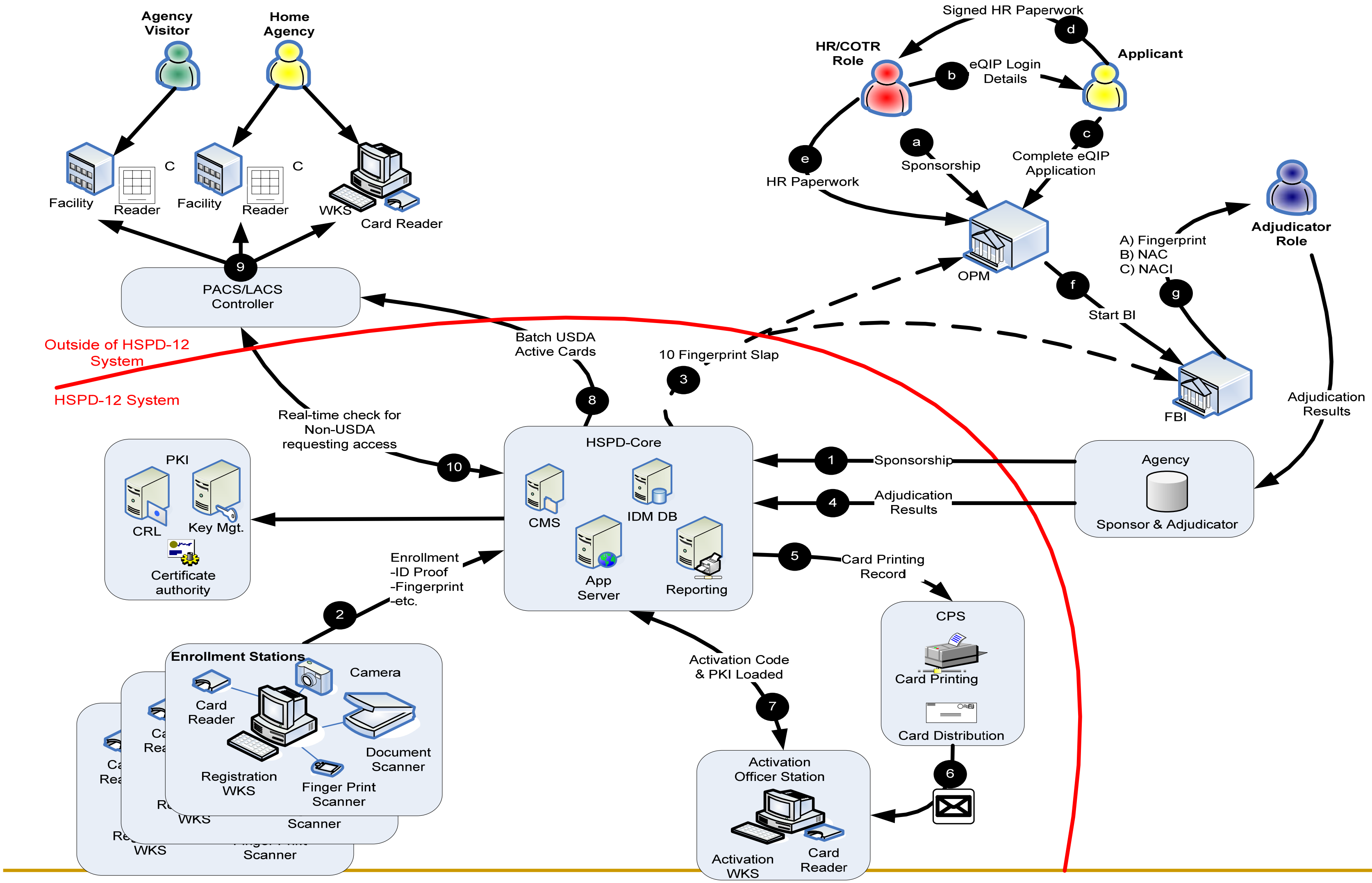
Federal PKI Common Policy Framework

FIPS 201: PIV Standard

M-05-24: Implementation Guidance

Special Publications
- Card Interface (73)
- Biometric (76)
- Crypto Algorithms (78)
- Enrollment Process (79)
- Card Testing (85)
- Reader Specifications (96)
- Physical Attributes (104)

Architecture



Agency Visitor

Home Agency

Facility

Reader

C

Facility

Reader

C

WKS

Card Reader

9

PACS/LACS Controller

Outside of HSPD-12 System

HSPD-12 System

Real-time check for Non-USDA requesting access

10

PKI

CRL

Key Mgt.

Certificate authority

Batch USDA Active Cards

8

10 Fingerprint Slap

3

HSPD-Core

CMS

IDM DB

App Server

Reporting

Enrollment -ID Proof -Fingerprint -etc.

2

Enrollment Stations

Card Reader

Camera

Registration WKS

Document Scanner

Finger Print Scanner

Activation Code & PKI Loaded

7

Activation Officer Station

Activation WKS

Card Reader

HR/COTR Role

Signed HR Paperwork

d

Applicant

b

eQIP Login Details

a

Sponsorship

c

Complete eQIP Application

e

HR Paperwork

OPM

f

Start BI

A) Fingerprint
B) NAC
C) NACI

g

Adjudicator Role

FBI

Adjudication Results

1

Sponsorship

4

Adjudication Results

Agency

Sponsor & Adjudicator

5

Card Printing Record

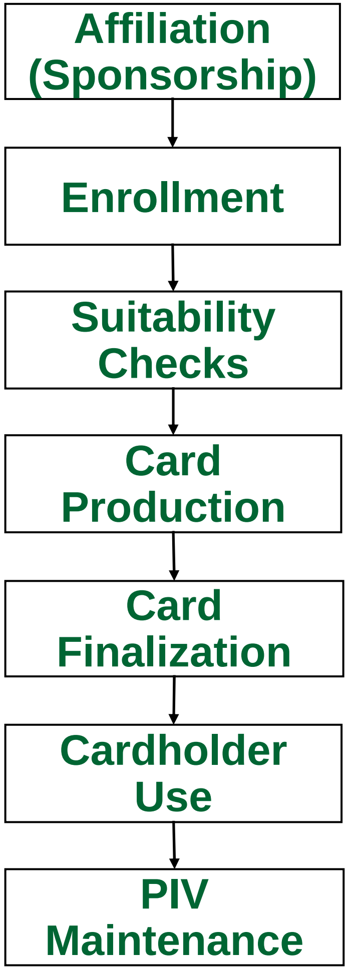
CPS

Card Printing

Card Distribution

6

Life Cycle



Affiliation (Sponsorship)	Agencies determine applicant should begin enrollment. Includes contractor and personnel sponsorship, and affiliation maintenance activities.
Enrollment	Applicant provides I-9 proof of identity, fingerprints and picture are captured.
Suitability Checks	Applicant fingerprints are provided to OPM for suitability checks. Adjudication must complete before card production begins.
Card Production	Smart card is manufactured, printed, and pre-personalized.
Card Finalization	Final card personalization and activation is performed, and card is provided to applicant "ready to use." (PIV Card Issuance)
Cardholder Use	Card is used for logical and physical access to remote and local resources, and for encrypted and signed electronic messaging.
PIV Maintenance	Post-issuance maintenance activities such as PIN reset, certificate updates, revocation, and renewal, suspension, updates, temporary access for forgotten cards, and end of lifecycle processing.

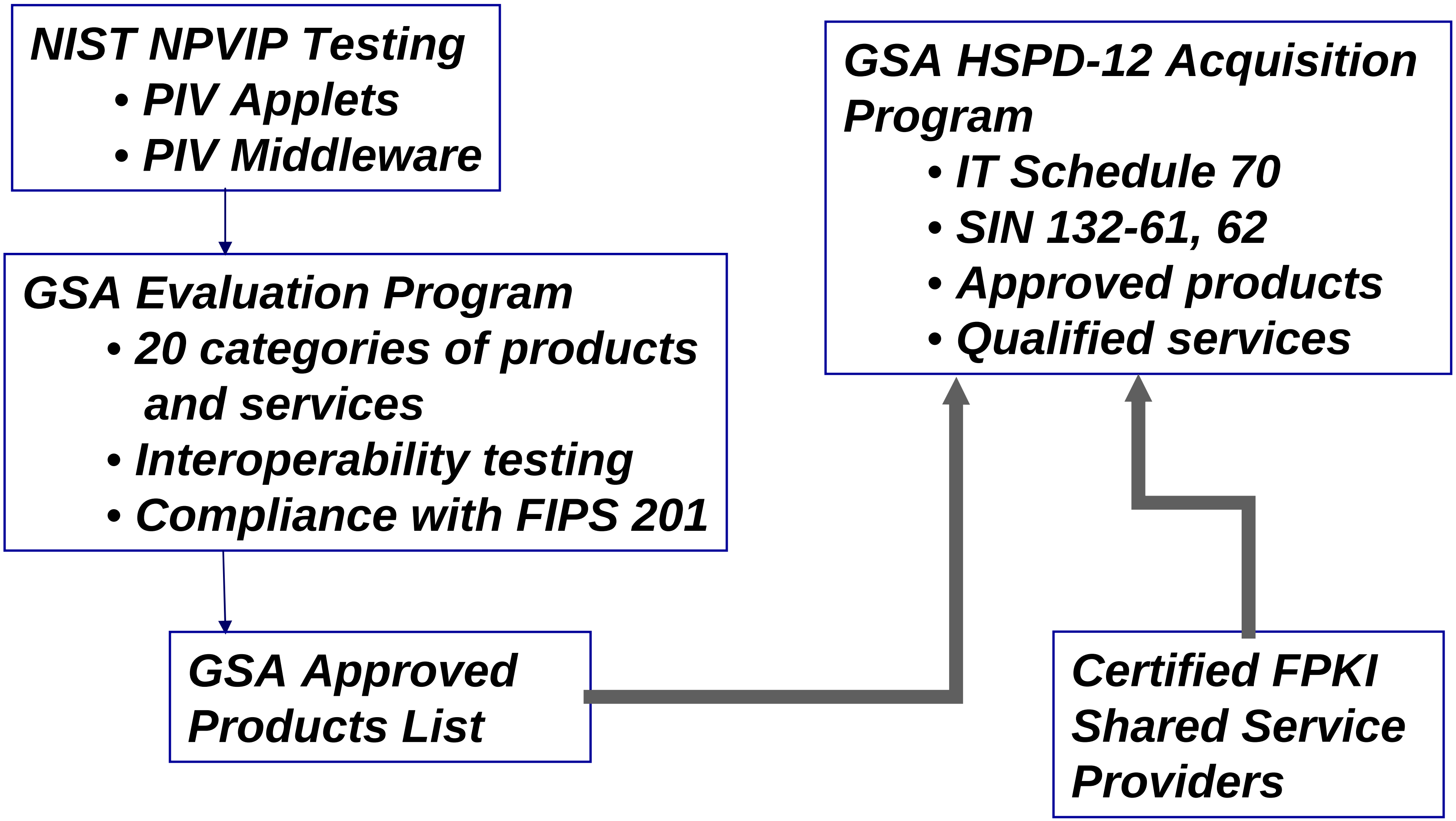
Infrastructure Components

- **Enrollment Service Providers** – provide local presence for enrollment of applicants
- **Systems Infrastructure Providers** – provide the software functionality required to manage PIV credentials
- **Production Service Providers** – produce and personalize (print & load applets) smart cards.
- **Finalization Service Providers** – provide local presence to finalize personalization and issue to applicant
- **PKI Shared Service Providers** – provides digital certificates for cards.

Architectural Interfaces

- Agency to System Infrastructure Provider
  - Agency sends applicant information and sponsorship to SIP
  - SIP provides enrollment information to Agency
- Enrollment Service Provider to System Infrastructure Provider
  - ESP retrieves applicant information from the SIP (verifies applicant)
  - Provides enrollment information to the SIP for card production
- Finalization Service Provider to System Infrastructure Provider
  - FSP initiates finalization (provides local point of presence)
  - SIP controls and manages the finalization process
- System Infrastructure Provider to Production Service Provider
  - SIP sends Card Customization Request to PSP
  - PSP completes card production and informs SIP
- System Infrastructure Provider to PKI Shared Service Provider
  - SIP requests PIV Authentication Certificate as part of finalization
  - SSP provides the certificate

FIPS-201 Compliant Products & Services



NIST NPVIP Testing

- ***PIV Applets***
- ***PIV Middleware***

GSA Evaluation Program

- ***20 categories of products and services***
- ***Interoperability testing***
- ***Compliance with FIPS 201***

GSA Approved Products List

GSA HSPD-12 Acquisition Program

- ***IT Schedule 70***
- ***SIN 132-61, 62***
- ***Approved products***
- ***Qualified services***

Certified FPKI Shared Service Providers

Deploying the New ID Card

- Enrollment and Card Issuance requires:
    - Adjudicated Fingerprints (NACI)
    - In person registration
    - Subscriber acknowledgment
    - Identity verification at issuance and activation
- Agencies Can:
    - Do it themselves – Go It Alone
    - Acquire Services through the GSA Managed Service Offering