

Certification and Accreditation of a PCI's PIV-I Services

Joan Hash

Manager, Computer Security Management
& Assistance

August 29, 2005

NIST Special Publication 800-79

On July 26, 2005, NIST posted SP 800-79

*“Guidelines for the
Certification and Accreditation of PIV
Card Issuing Organizations”*

in WWW.CSRC.NIST.GOV/PIV-Program

What is a PIV Card Issuing Organization?

- An organization authorized to provide FIPS 201 Compliant PIV Services including
 1. PIV Card Applicant Identity Proofing (PIV-I)
 2. PIV Card Applicant Registration (PIV-I)
 3. PIV Card Issuance to Approved Applicants (PIV-II);
 - in accordance with the policy specified in Homeland Security Presidential Directive 12; and
 - in conformance with the procedural and technical specifications of FIPS 201.

Terminology

- NIST SP 800-79 uses the term PIV Card Issuer (PCI) for any PIV Card Issuing Organization performing any PIV service
- Each Agency should have established or selected a PCI before October 27, 2005 that is accredited to perform PIV-I services.
- SP 800-79 states that a provider need to be accredited only those services it offers.

Why PCI Accreditation?

- Homeland Security Presidential Directive 12 requires PIV Cards to be issued only by providers whose reliability has been accredited.
- Accreditation will help to assure competence of, and confidence in, PCI services
- Accreditation should increase the trust of one agency for the PCI services provided by other agencies.

What is PCI Accreditation?

PCI Accreditation is the official management decision of the Designated Accreditation Authority (DAA) to authorize a PCI to offer a PIV service after determining that the PCI's capability and reliability have been satisfactorily established through appropriate assessment and certification processes.

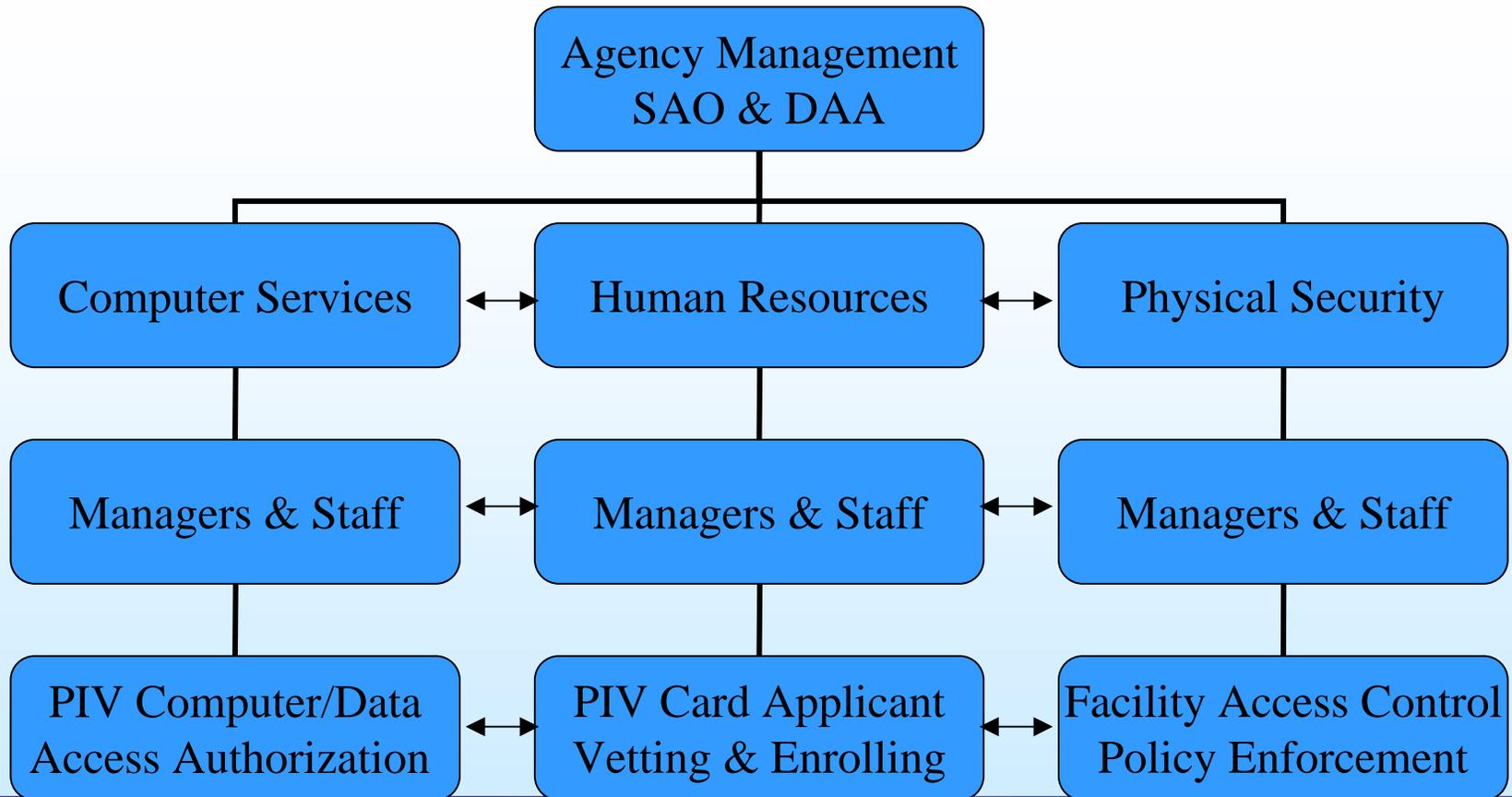
What is PCI Certification?

Certification of a PIV Service Provider is a formal process of assessing the attributes (e.g. knowledge, capability, availability, personnel, equipment, finances, and adequately supported infrastructures) of the provider of the PIV service using selected methods of assessment (e.g., interviews, document reviews, laboratory test results, procedure evaluations, component validation reports) that support the assertion that the PIV Service Providing organization is reliable and capable of performing the offered service.

When Should Accreditation be Done?

- Accreditation is required before a PIV service may be provided to an agency.
- Accreditation should be repeated within the time period established by the Designated Accreditation Authority of the agency using the services of a PCI.
- Accreditation should be repeated when a major change is made to a PCI or a major problem in the PCI's operation is identified.

Who Should be Involved with PCI?



What is the PIV System?

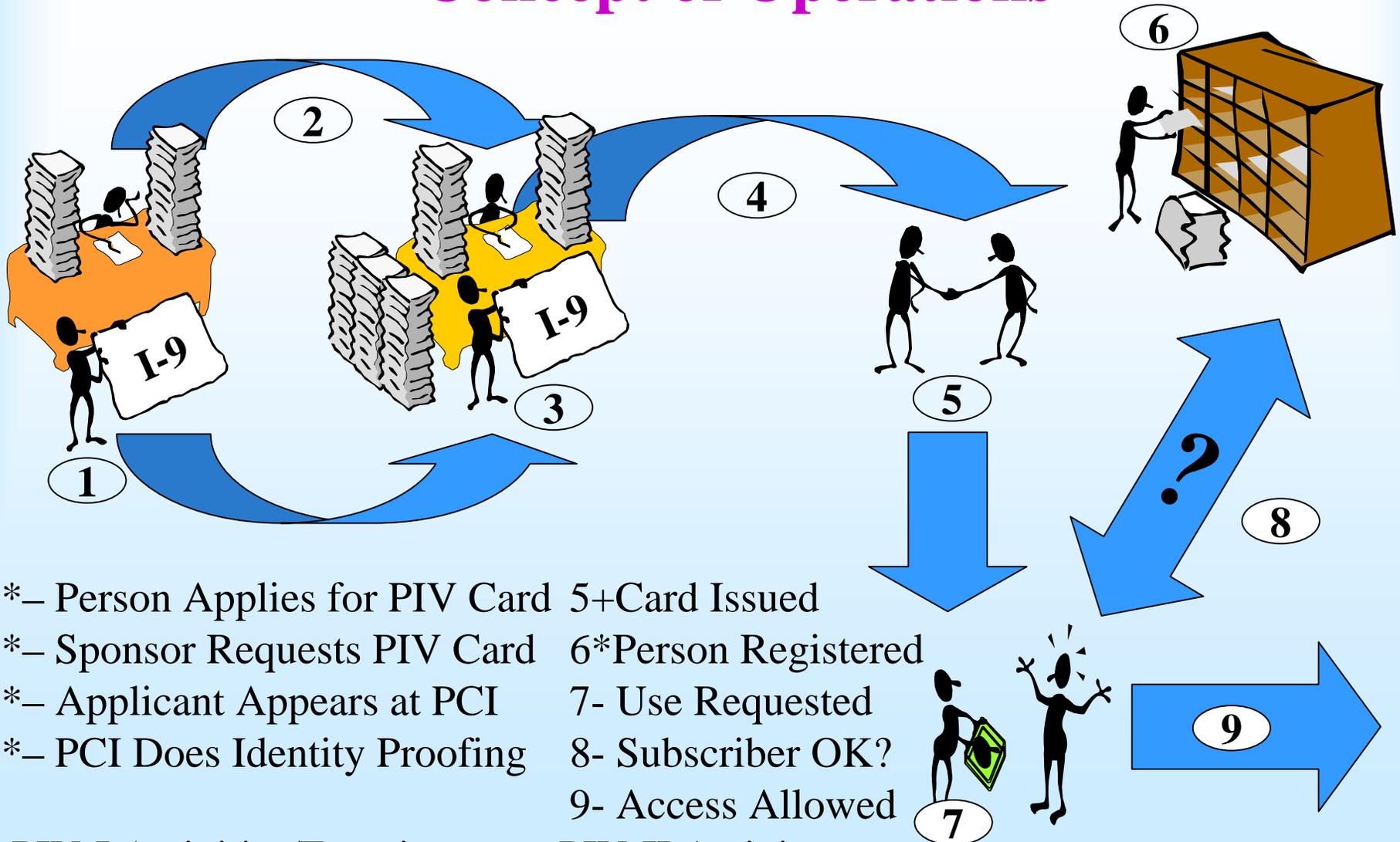
The PIV System may be viewed as a single integrated government-wide system designed according to standards which satisfy common Federal Agencies objectives and policies and use various information systems and applications

Built by and for Independent Federal Agencies

using independently managed computer systems containing independently manufactured components that are expected to change as new technology becomes available and more services are needed.

PIV Identity Proofing, Applicant Registration, Card Issuance, and PIV System Use

Concept of Operations



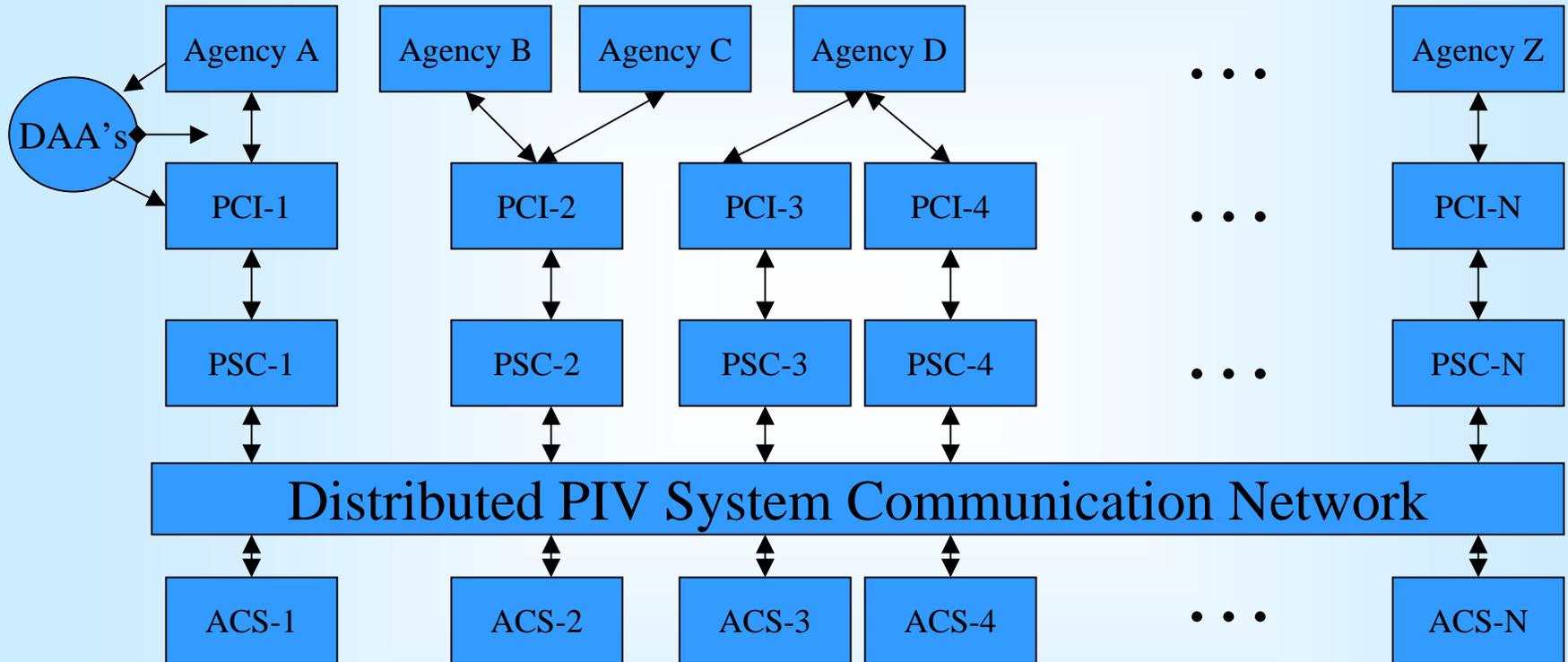
- 1* – Person Applies for PIV Card
- 2* – Sponsor Requests PIV Card
- 3* – Applicant Appears at PCI
- 4* – PCI Does Identity Proofing
- 5+ Card Issued
- 6* Person Registered
- 7- Use Requested
- 8- Subscriber OK?
- 9- Access Allowed

* PIV-I Activities/Functions + PIV-II Activity

PIV System Activities/Functions

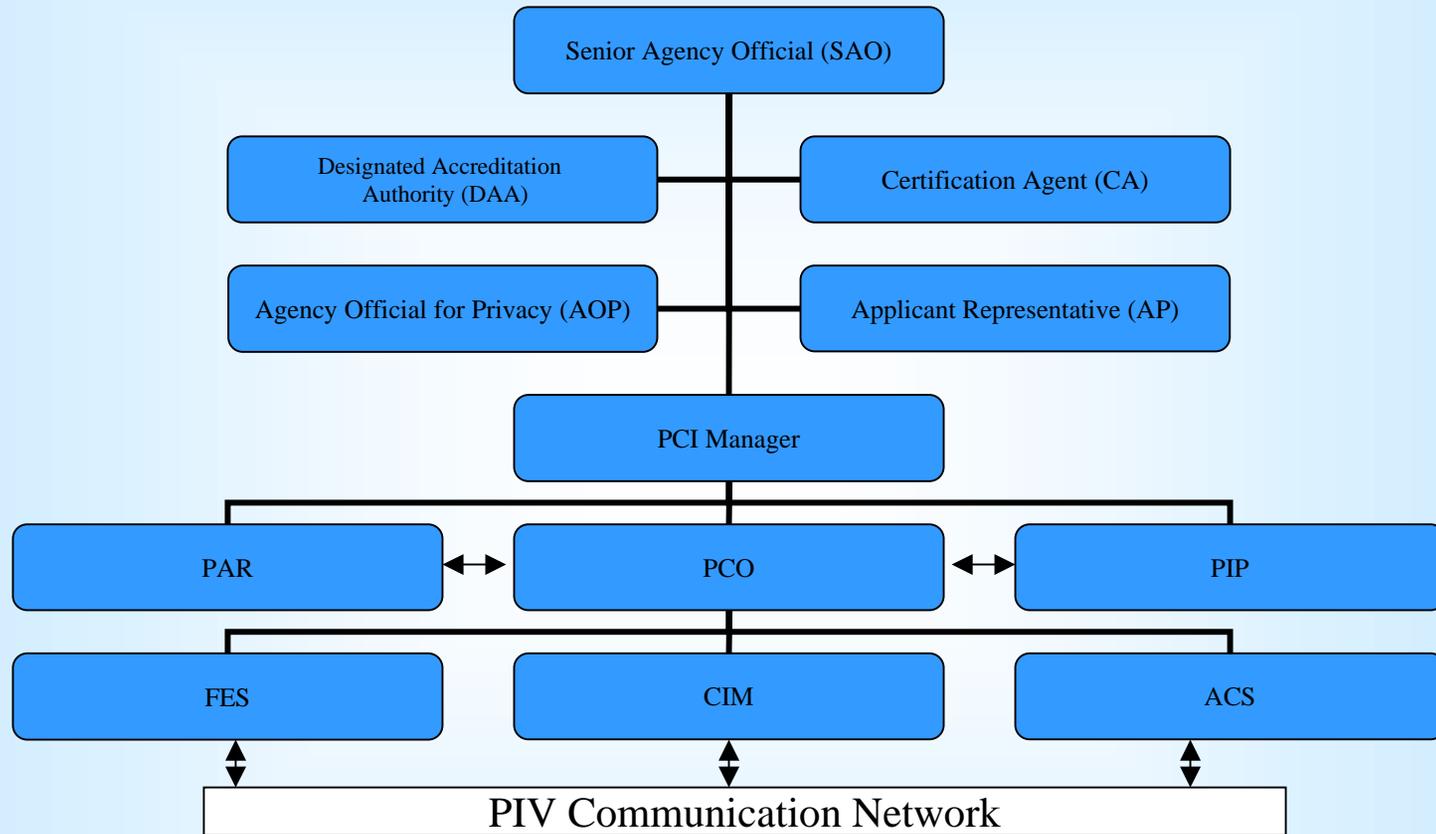
- Enrolls PIV Subscribers using PCI Systems
- Obtains Subscriber Access Authorizations
- Processes Subscriber's Access Requests
- Verifies Subscriber's Credentials from Card
- Grants/Denies Requests using Authorizations
- Maintains very large Subscriber Databases
- Maintains standard, temporary, and emergency (First Responder) Subscriber Authorizations
- Prepares and Issues PIV Usage and Audit Reports

A Logical View of the PIV System



DAA: Designated Accred. Auth.; PCI: PIV Card Issuer; PSC: PCI Support Computer; ACS: Access Control System

Sample PCI Organization Structure/Roles



PAR: PIV Applicant Registrar; PCO: PIV Card Operations; PIP: PIV Identity Proofing; FES: PIV Front End System; CIM: Card Issuance & Management; ACS: Access Control System

Required Attributes of a PCI

- Reliability of a PCI/PSP is exhibited by its being
 - Knowledgeable
 - Capable
 - Accountable
 - Available
 - Legal
 - Compliant
 - Well Managed
 - Trustworthy and Secure
 - Adequately Supported

Desirable Attributes of a PCI

- Prepared/responsive/efficient – ability to perform a service in a timely manner
- Cost effective – ability to perform a service at a reasonable cost proportional to its value to a client
- Adaptable – ability to change to new environments, technologies, and requirements.
- Cooperative – ability to work within agency and with other agencies using the PIV System.

Methods of Assessing Attributes

- Review and Analysis
- Interview
- Demonstration/Observation
- Sampling/Statistics
- Evaluation/Measurement
- Compliance/Conformance with standards
- Precedence/Accepted Practice
- Comparison with Peers
- Experience
- Testing/Validation

Phase 1 of Certification and Accreditation

- Initiation Phase

- Identify Resources (Create C & A Team)
 - Designated Accreditation Authority (DAA)
 - Certification Agent (CA)
 - PIV Card Issuer (PCI) Manager
 - PIV Card Applicant's Representative (AP)
- Collect Relevant Standards, Guidelines, etc.
- Obtain PCI's Operational Plan
- Create DAA's Certification Plan

Phase 2 of Certification and Accreditation

- Certification Phase
 - Specify Attributes of the PCI to be Assessed
 - Select the Assessment Methods to be Used
 - Apply selected assessment methods to:
 - PCI's Personnel, Documentation,
 - Planned Services, Operational Plan
 - Prepare Assessment Reports
 - Provide Reports to PCI Manager and CA

Phase 3 of Certification and Accreditation

- Accreditation Phase

- Review the results of the certification phase
- Review the residual risks expected after reducing discovered vulnerabilities
- Review the accreditation documentation
- DAA makes the accreditation decision
 - *Authorize to Operate if risks are acceptable
 - *Interim Authorization to Operate if correctable
 - *Deny Authorization to Operate if unacceptable

Phase 4 of Certification and Accreditation

- Monitoring Phase

- PCI provides accredited services (e.g., PIV-I) in compliance with FIPS 201
- PCI Security Officer monitors security and operating procedures
- PCI Quality Control samples and evaluates PIV Card creation, issuance, and management
- PCI staff reports results to PCI Manager
- PCI Manager should report significant problems to Designated Accreditation Authority (DAA)

Authorization to Operate Alternatives

- The agency's Designated Accreditation Authority issues to a PCI:
 - An Authorization to Operate if fully accredited after its reliability has been accredited;
 - An Interim Authorization to Operate under specific terms (i.e., 3 months) and conditions (e.g., pursuing Corrective Action Plan);
 - A Denial of Authorization to Operate if the assessments are unsatisfactory.

Certification & Accreditation Tasks

- Preparation
- Resource Identification
- PCI Operations Plan Review
- PCI Attribute Specification and Assessment
- PCI Certification Documentation
- DAA Accreditation Decision
- Certification and Accreditation Documentation
- PCI Operations Management and Quality Control
- PCI Attribute (Quality, Reliability) Monitoring
- PCI Operations Quality and Reliability Reporting

PCI Reliability C & A

- Quality control and reliability monitoring should be a part of normal organizational management.
- C & A should be conducted as a normal part of organization oversight/performance evaluation.
- Should be performed initially to verify that FIPS 201 is being implemented and used properly.
- Should be performed periodically to verify that all PCI's are complying with FIPS 201 equivalently.
- Should help assure an agency that PIV Cards issued by other agencies may be Trusted.

PCI Activities for PIV-I

- Assignment of Responsibilities (Roles, etc.)
- Data Gathering (Card sources, SF 85 Forms, etc.)
- Applicant Vetting (ID Source Document Proofing & Applicant Background Check)
- Approval of Applicants- Credential and Card Issuance Authorization
- Issuance of PIV Credentials/Card
- PIV Subscriber Record & Credential Maintenance

Example of Initiating PCI

- Following five slides selected from an agency's briefing on PCI Planning, Initiation, C & A
- Example of appropriate application of NIST SP 800-79 to assist agency in PCI Initiation development and C & A

PIV Related Roles/Responsibilities

- **Senior Authorizing Official**

- The Senior Agency Official (SAO) is responsible for the establishment, budget, and oversight of the PIV functions and services of an agency.

- **Designated Accreditation Authority**

- The Designated Accreditation Authority (DAA) is a senior agency official with the authority to formally accredit the reliability of PCIs as required by HSPD-12.

- **Agency Identity Management Official**

- Agency Identity Management Official (AIMO) is responsible for ensuring that all the services specified in FIPS 201 are provided reliably and that PIV Cards are produced and issued in accordance with its requirements.

PIV/PCI Roles/Responsibilities

- **Certification Agent (CA)**
 - The Certification Agent (CA) has the appropriate skills, resources, and competencies to perform certifications (i.e., comprehensive assessments) of a PCI. The CA should identify discrepancies between the current status of the PCI Facility and the requirements of FIPS 201, and present them to the PCI Facility Manager who will prepare recommended corrective actions to reduce or eliminate the discrepancies.
 - The CA will review the corrective actions, report if they are adequate or not, and then ensure that the final set of acceptable corrective actions are properly applied.
 - Prior to initiating the activities of the certification process, the CA provides a plan to ensure that a realistic assessment of the current reliability of the PCI will be obtained.
 - **To preserve the impartial and unbiased nature of certifications, the CA should be independent of, and organizationally separate from, the persons and the office (s) directly responsible for the day-to-day card issuance.**

PCI Manager

The PCI Manager

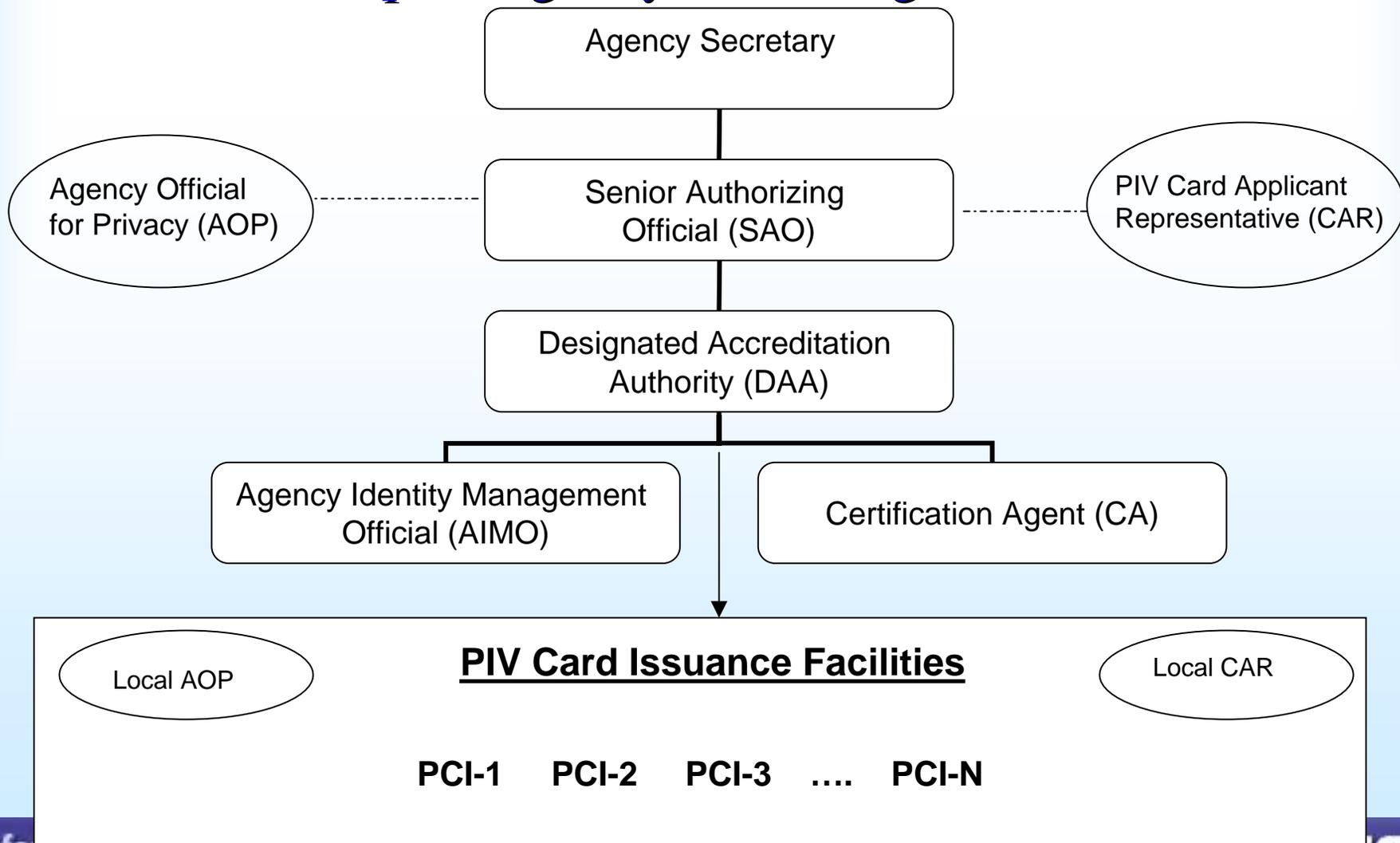
Responsible for ensuring that all the services specified in FIPS 201 are provided reliably and that PIV Cards are produced and issued in accordance with its requirements.

Other PIV Related Roles

(Agency and Local levels)

- **PIV Card Applicant Representative**
 - represents the interests of current or prospective Federal employees and contractors who are the Applicants for PIV Cards.
 - represent the privacy concerns of applicants
 - assist an applicant who is denied a PIV Card because of missing or incorrect information in an Identity Source document, or act as a surrogate for an applicant that is not available for performing required actions.
- **Agency Official for Privacy**
 - The role of the Agency Official for Privacy (AOP) is defined in FIPS 201 and may not assume any other operational role in the PIV system.
 - The AOP oversees privacy-related matters in the PIV system and should work with the PIV Card Applicant Representative to ensure that the rights of Applicants and PIV Subscribers are protected.

Sample: Agency C&A Organization



Summary of PCI C & A

- The Reliability of a PCI should be accredited in accordance with HSPD-12 and NIST SP 800-79 before it can provide PCI Services.
- The Security of a PCI's Computer Support Systems should be accredited in accordance with NIST SP 800-37 before PCI services are provided.
- A PCI should be accredited only for those activities it performs for the services provided.

PIV System Concept and Model

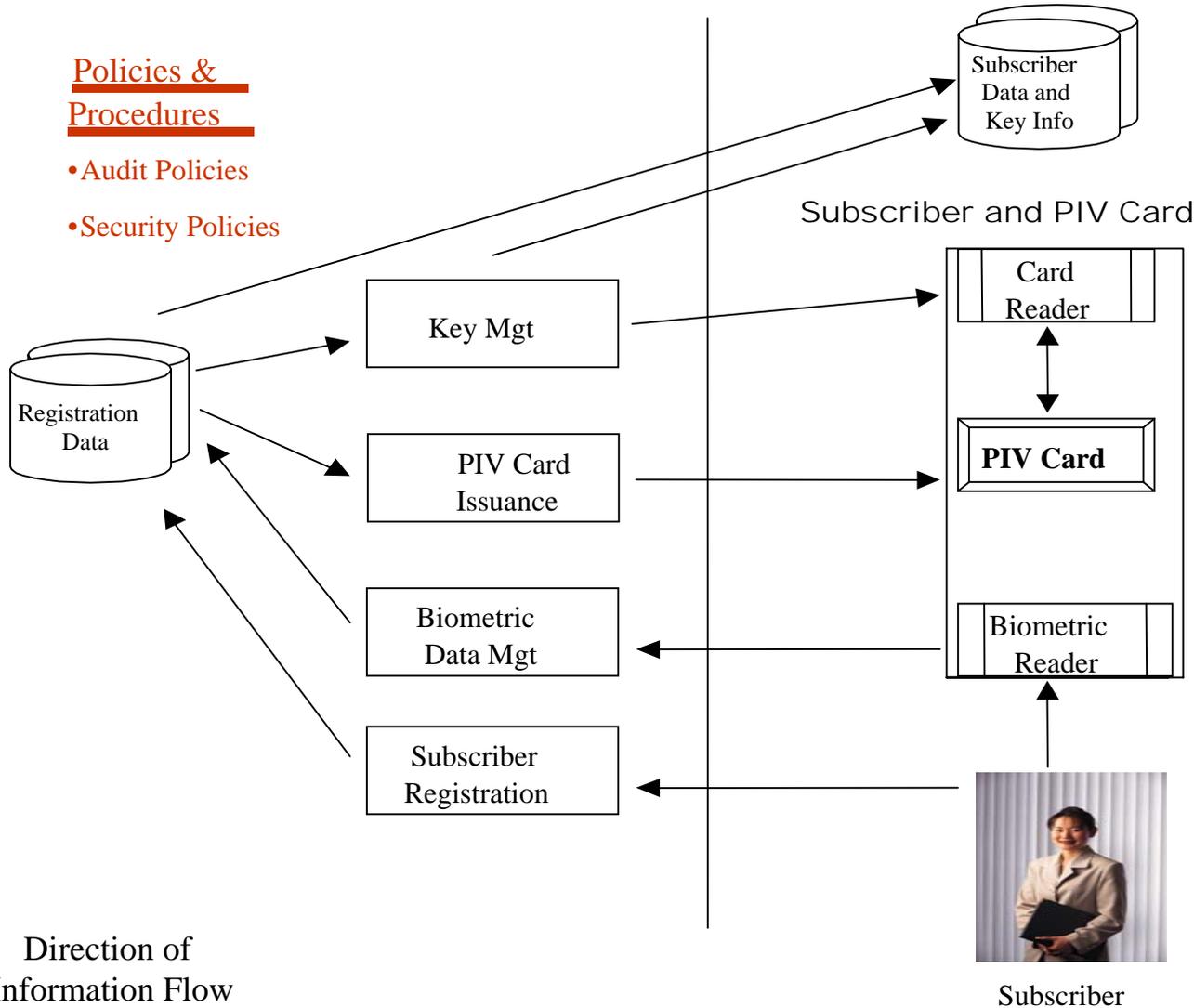
PIV-II Card Issuance and Management

PIV Card Issuance and Management Infrastructure

Subscriber Data

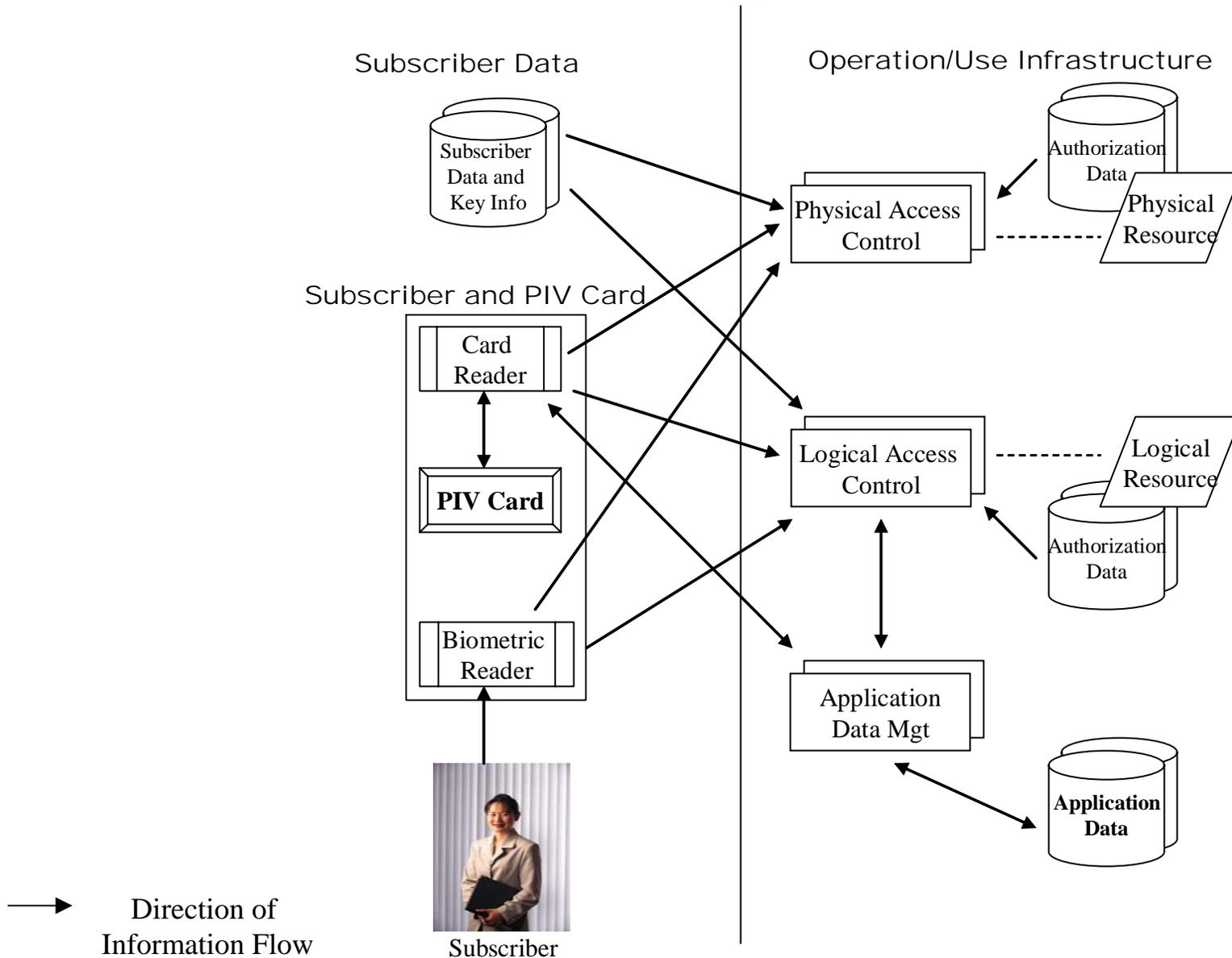
Policies & Procedures

- Audit Policies
- Security Policies

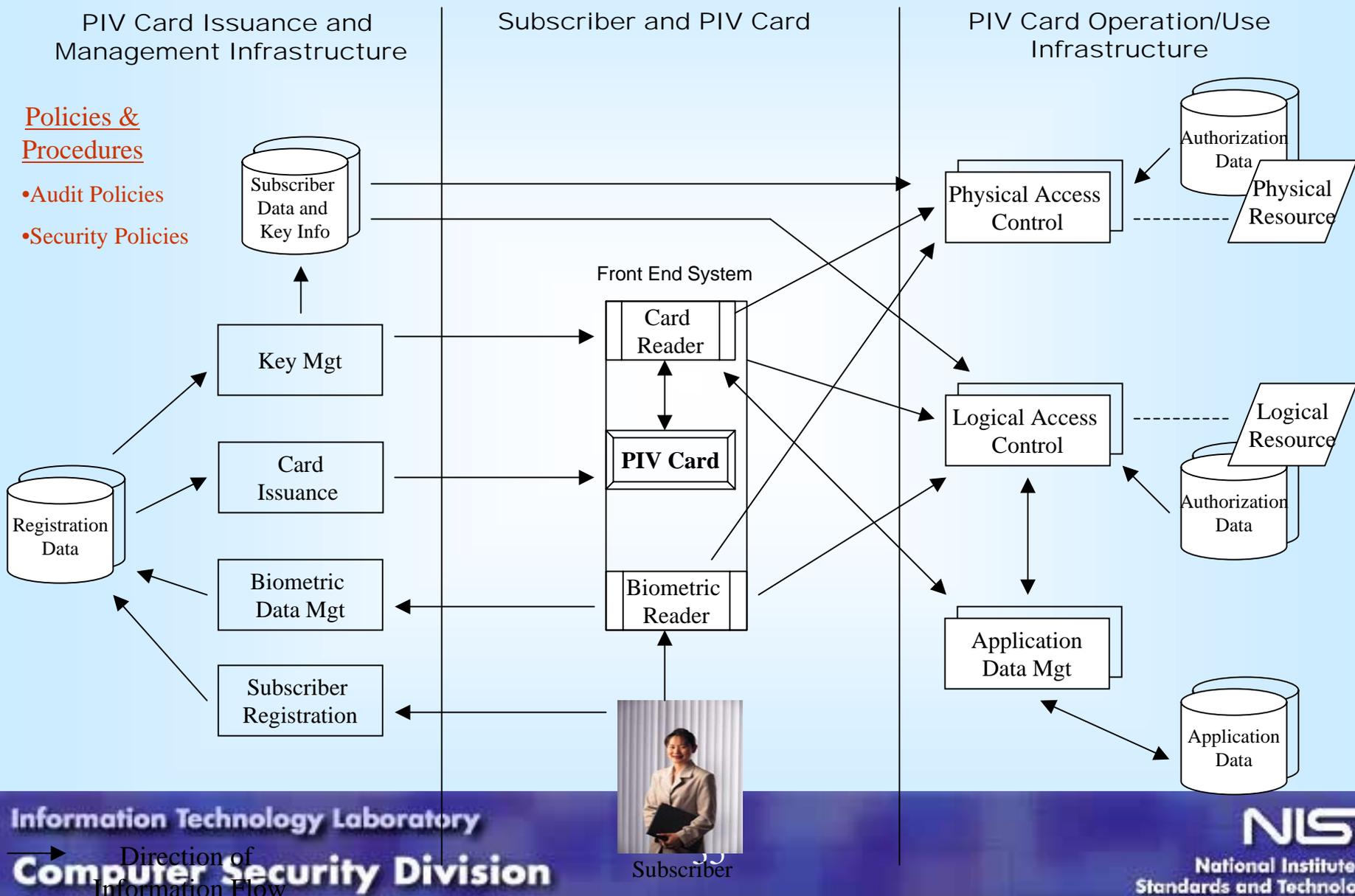


PIV System Concept and Model

PIV-II Card Operation/Use



PIV System Concept and Model Operation



Vocabulary

- Assessment
 - determination of an organization's capability, competence, reliability, compliance with standard procedures, and use of products conforming with specifications of a standard.
- Validation
 - determination of a product's or a service's conformance to standards

Vocabulary

- Compliance
 - Status of an organization when it has implemented and is using a standard in a manner that satisfies the requirements.
- Conformance
 - Status of a product or a service when it has been designed, implemented, and is being used in a manner that satisfies the specifications of a standard.