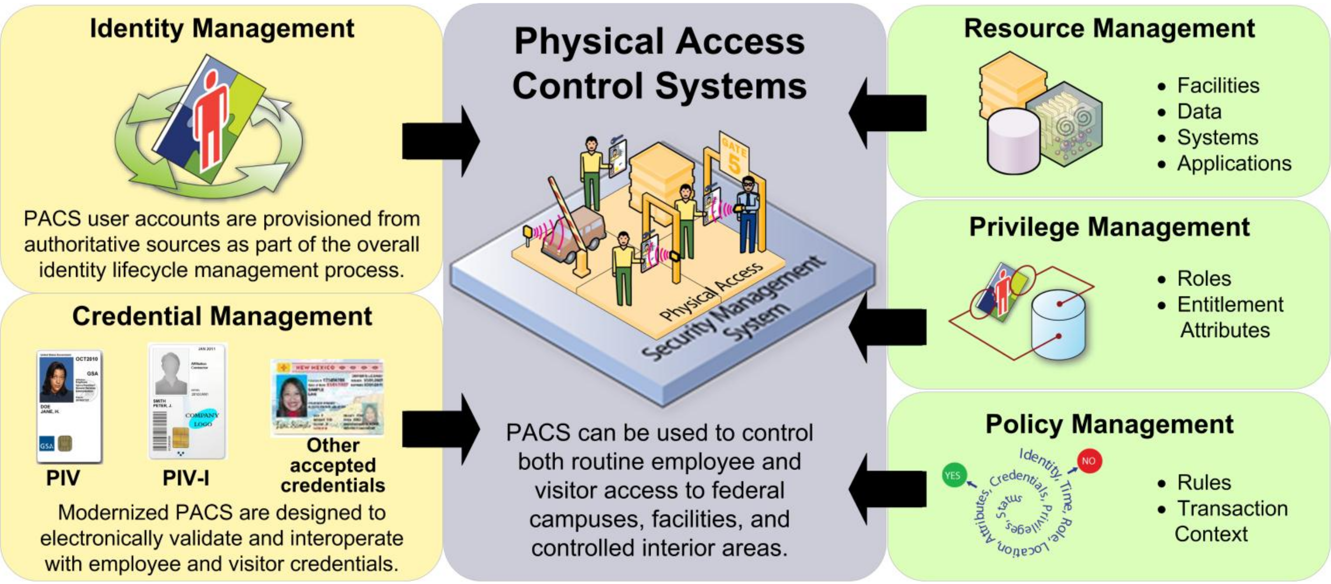
Modernizing Federal Physical Access Control Systems (PACS)

Implementation of Enterprise PACS

PACS modernization involves integrating PACS at the enterprise level, which helps an agency achieve cost savings and efficiencies while preserving local access control decisions. Modernized PACS leverage user identity and credential data from authoritative sources and are supported by enterprise resource, privilege, and policy management processes. PACS modernization also includes use of the PIV card in order to gain physical access to a federally controlled facility, in accordance with HSPD-12.



Physical Access Security Management System
GATE 5
PIV
PIV-I
Other accepted credentials
YES
NO
Identity, Time, Role, Location, Attributes, Credentials, Privileges, Status

Identity Management

PACS user accounts are provisioned from authoritative sources as part of the overall identity lifecycle management process.

Credential Management

Modernized PACS are designed to electronically validate and interoperate with employee and visitor credentials.

Physical Access Control Systems

PACS can be used to control both routine employee and visitor access to federal campuses, facilities, and controlled interior areas.

Resource Management

- Facilities
- Data
- Systems
- Applications

Privilege Management

- Roles
- Entitlement Attributes

Policy Management

- Rules
- Transaction Context

Benefits of PACS Modernization

The design characteristics of a modernized PACS solution offer agencies a wide variety of benefits and increased efficiencies, as described below.

Increases security and privacy at your facility

- Utilizes stronger technology to validate cardholders
- Electronic verification provides reliable information to assist the guard force in making access decisions

Reduces costs and increases efficiency

- Agency-wide approach eliminates redundant processes and investments
- Enterprise integration enables reduced manual efforts

Promotes trust and interoperability

- Supports acceptance of PIV, PIV-I, and other trusted external credentials
- User privileges can be shared across agency locations and with trusted external sites

Improves overall support for ICAM implementation

- Feeds user information from agency-wide identity sources
- Enables sharing of access control log information with security monitoring tools
- Shares data (as needed and permissible) with credentialing system

For more information, visit www.idmanagement.gov

Steps in Implementing a Modernized PACS Solution

PACS modernization involves transitioning from stand alone systems to enterprise level physical access solutions, an effort which should be planned carefully to ensure success and prevent disruptions to operations. The steps for a modernized PACS implementation are highlighted below:

Step 1: Review & Update Policies/Procedures

- ✓ Review existing policies for alignment with ICAM segment architecture
- ✓ Ensure policy is in place for PIV-enabling PACS in accordance with M-11-11
- ✓ Confirm alignment with additional standards (e.g., NFPA codes, FISMA)

Step 2: Conduct a Risk Assessment

- ✓ Take inventory of sites, facilities, and existing PACS
- ✓ Follow Interagency Security Committee Compendium of Standards
- ✓ Identify risks and determine appropriate countermeasures (e.g., electronic, guard force)

Step 3: Select Authentication Mechanisms

- ✓ Follow SP 800-116 for acceptable authentication mechanisms by access area
- ✓ Evaluate ability of existing PACS to meet authentication needs
- ✓ Determine required system upgrades/ replacement

Step 4: Procure Products & Services

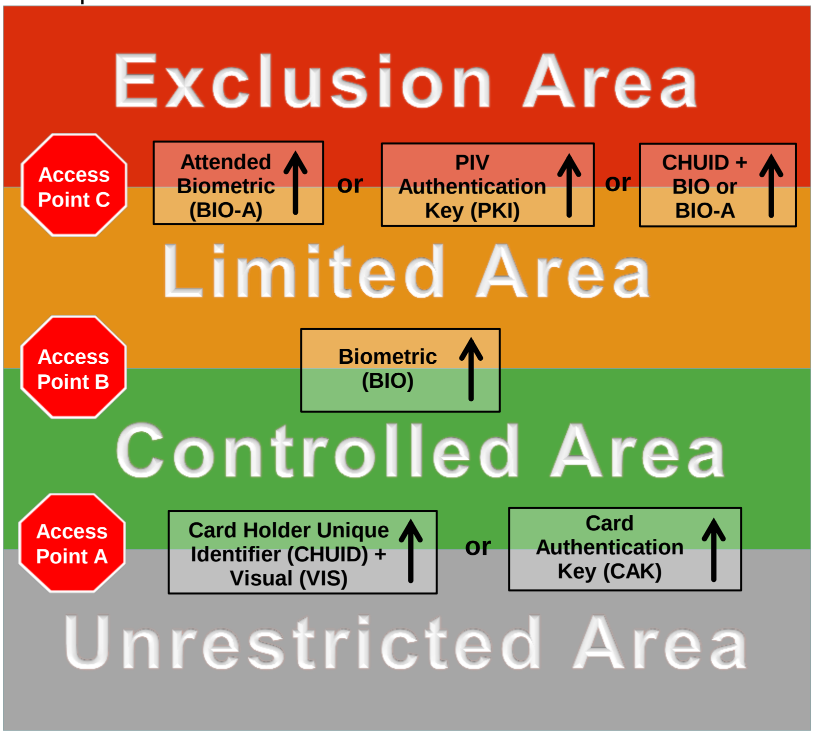
- ✓ Perform PACS modernization budget planning
- ✓ Identify and secure funding sources
- ✓ Procure products and services in accordance with the Federal Acquisition Regulations (FAR)

Step 5: Implement a PACS Solution

- ✓ Develop an implementation plan and schedule
- ✓ Perform and complete upgrades
- ✓ Maintain security and quality throughout implementation

Enabling PACS Using the PIV Card

An important step in PACS modernization is determining the appropriate PIV authentication mechanism(s) that should be deployed at each access point. The figures below illustrate the type of authentication mechanism(s) that may be used at access points to each security area and provides a description of each authentication mechanism available on the PIV card.



Exclusion Area

Access Point C: Attended Biometric (BIO-A) or PIV Authentication Key (PKI) or CHUID + BIO or BIO-A

Limited Area

Access Point B: Biometric (BIO)

Controlled Area

Access Point A: Card Holder Unique Identifier (CHUID) + Visual (VIS) or Card Authentication Key (CAK)

Unrestricted Area

PIV Authentication Mechanisms

- **Multi Factor.** Validates something you have (a PIV), something you know (a PIN), & something you are (biometric).
- **PIV Authentication Key (PKI).** Verifies a claimed identity through validation of a digital certificate (contact interface after PIN entry).
- **Biometric (BIO).** Matches reference biometric on the PIV card with the sample biometric provided.
- **Card Authentication Key (CAK).** Verifies PIV card through validation of a digital certificate (contactless interface; no PIN).
- **Cardholder Unique Identifier (CHUID).** Matches identifier read from the card against identifier in system (no identity authentication).

Federal Chief Information Officer (CIO) Council
Information Security and Identity Management Committee
Identity, Credential, and Access Management Subcommittee

ICAM
Identity, Credential, & Access Management