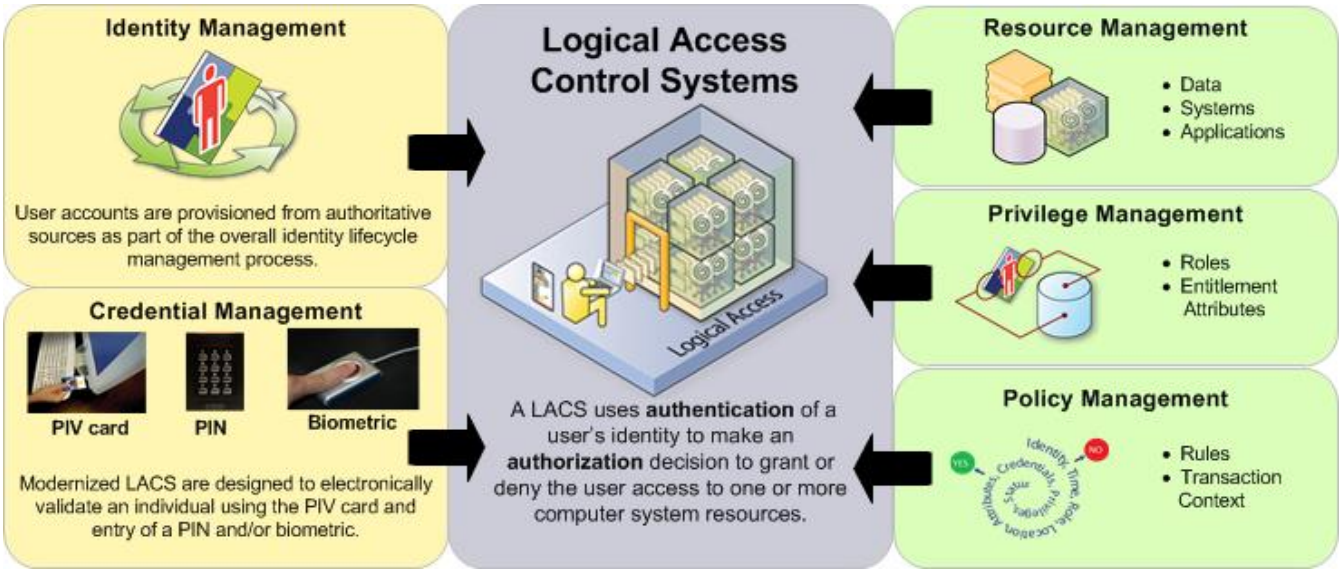
Modernizing Federal Logical Access Control Systems (LACS)

Implementation of Enterprise LACS

LACS modernization involves integrating an agency's IT resources at the enterprise level, to control access in a streamlined and consistent manner. A modernized LACS standardizes on use of the PIV credential as the common means of validating the identity of a user and granting access to networks and information systems, in accordance with federal policies.



Benefits of LACS Modernization

A modernized LACS solution offers agencies a wide variety of benefits and increased efficiencies, as described below.

Improved Security. Provides high assurance of user identity and strong authentication for users accessing agency resources. Securely authenticates remote users while leveraging existing infrastructure.

Reduced Administrative Burden and Cost. Requires less effort on the part of resource owners and administrators to manage user accounts and access privileges, resulting in lower life-cycle costs.

Increased Compliance. Enables detection and remediation of conflicting access privileges within and across resources (e.g., segregation of duties).

Increased Customer Satisfaction and Convenience. Provides consumers ease of use with the ability to access multiple applications using a single credential.

Support for Encryption/Digital Signature Services. Supports additional security functionality to encrypt and digitally sign data using the PIV card.

Key Target State Metrics

1 digital identity per user

100% of employees and contractors have PIV credentials

100% of applications are accessible to employees and contractors using PIV cards

100% of externally-facing applications are enabled to accept third-party credentials

100% of applications are integrated with an automated provisioning workflow

For more information, visit www.idmanagement.gov

LACS Design Approaches

A modernized LACS solution includes the use of shared agency-level resources to manage access across the enterprise, such as provisioning and policy rules. One key decision point when designing a modernized LACS is whether the LACS handles authentication and authorization services in a centralized or decentralized way. The figure below discusses characteristics of each of these options.

Recommended Design Approach: Enterprise Authentication & Authorization

- Individual applications use the agency-level services to authenticate and grant access to users
- Enables single sign-on (SSO) capabilities across multiple applications
- This approach is recommended for most agencies, particularly those with a large inventory of user applications

Alternative Design Approaches

Enterprise Authentication & Decentralized Authorization

- Individual applications use the agency-level services to perform user authentication but access decisions are executed locally by the resource
- Generally applied to agencies using legacy applications or when local resource control is favorable

Decentralized Authentication & Enterprise Authorization

- Individual applications authenticate users locally but execute access decisions using agency-level services
- Generally applied to agencies with diverse and complex applications or high-risk applications

Decentralized Authentication & Authorization

- Users are authenticated and granted access by mechanisms within each individual application
- Generally applied to agencies with a small number of applications, a large proportion of legacy or proprietary applications, or where enterprise connectivity may be limited

LACS Application Integration

Once the LACS solution components have been deployed, the next step is integrating the agency's applications and resources with the solution. Below are some steps that an agency can leverage to assist in this process.

1 Launch

- Gain leadership buy-in and support for LACS program integration
- Demonstrate organizational value through successes of early adopters
- Obtain executive sponsorship reaching the Deputy Secretary level

2 Application Discovery

- Obtain a list of target applications for LACS integration, where available
- Develop a complete list of target applications for LACS integration
- Begin categorizing information based on: risk profile, technical readiness, and operational readiness

3 Analysis

- Perform application risk and compliance assessment
- Determine application interoperability requirements
- Analyze application integration to determine integration complexity
- Categorize and prioritize applications for integration

4 Integration Plan

- Evaluate level of effort based on integration complexity and prioritization
- Develop and communicate integration timeline
- Construct comprehensive integration plan and obtain support from leadership and application owners
- Develop detailed integration schedule

Summary of Policy Requirements

- ☑ Incorporate and fund security as part of your agency's IT systems and architectures
- ☑ Enable all new systems to accept PIV cards for user authentication
- ☑ Plan to enable existing systems to accept PIV cards as they are modernized
- ☑ Accept and electronically verify PIV credentials issued by other agencies
- ☑ Use the PIV card to provide two factor authentication for remote system users

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

ICAM
Identity, Credential, & Access Management