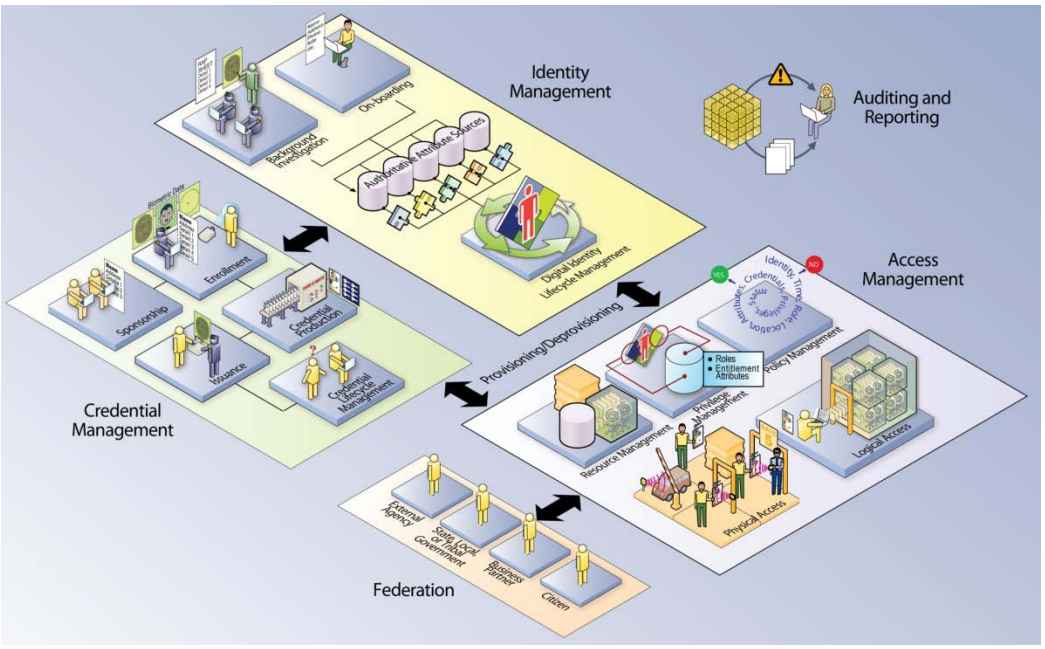
Identity, Credential, and Access Management Segment Architecture

What is Identity, Credential, and Access Management (ICAM)?

ICAM represents the intersection of digital identities (and associated attributes), credentials, and access control into one comprehensive approach. The following figure illustrates the core components of ICAM.



Key ICAM Service Areas:

- Digital Identity
- Credentialing
- Privilege Management
- Authentication
- Authorization & Access
- Cryptography
- Auditing & Reporting

The Roadmap

The Federal ICAM Roadmap addresses unclassified federal identity, credential, and access management programs and how the Executive Branch of the Federal Government will interact with external organizations and individuals. It provides a new government-wide segment architecture for ICAM.

"The ICAM segment architecture will serve as an important tool for providing awareness to external mission partners and drive the development and implementation of interoperable solutions."

– President's 2010 Budget

The purpose of the Roadmap is to outline a common framework for ICAM within the Federal Government and to provide supporting implementation guidance for agencies as they plan and execute their architecture for ICAM programs.

Key Target State Initiatives	Key Performance Metric Targets
1 Augment policy & implementation guidance to agencies	100 % of employees, contractors, and affiliates have been issued PIV cards.
2 Establish federated identity framework for the Federal Government	100% of applications accessed by federal employees and contractors using PIV credentials.
3 Enhance performance measurement & accountability within ICAM initiatives	100% of physical access transactions electronically authenticate the PIV or interoperable credential for internal & external users.
4 Provide government-wide services for common ICAM requirements	100% of electronic transactions with external businesses and citizens use third party credentials.
5 Streamline collection & sharing of digital identity data	
6 Fully leverage Personal Identity Verification (PIV) & interoperable credentials	
7 & 8 Modernize physical & logical access infrastructure	
9 Implement federated identity capability	

For more information, visit www.idmanagement.gov

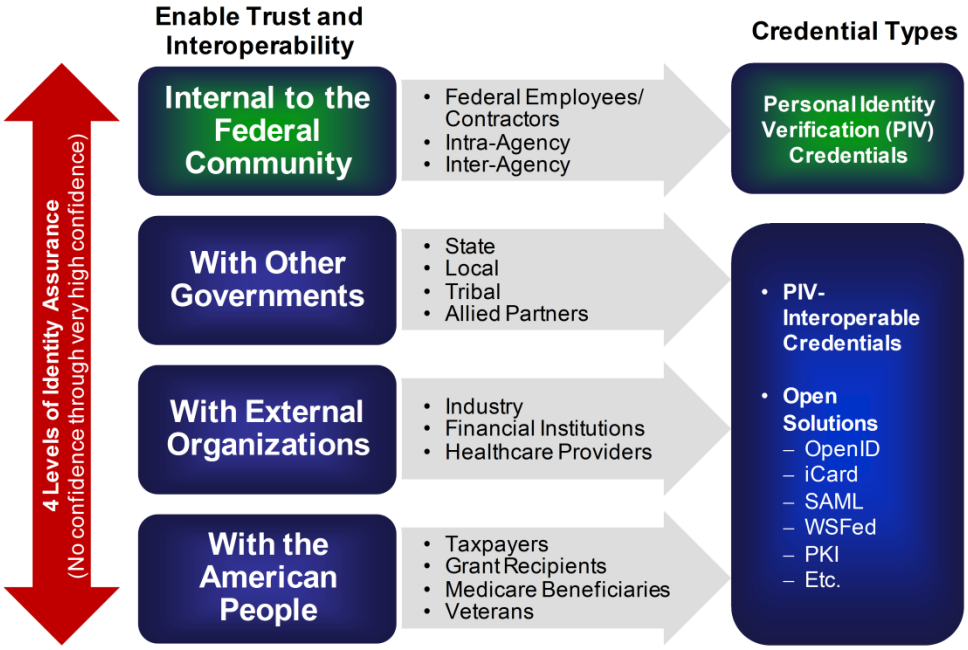
Strategic Vision

The Federal ICAM Roadmap outlines a strategic vision for identity, credential, and access management efforts with the Executive Branch of the Federal Government and demonstrates the importance of implementing the ICAM segment architecture in support of five overarching strategic goals and their related objectives. These are listed in the figure below.

Goal 1: Comply with Federal Laws Relevant to ICAM	Goal 2: Facilitate E-Government by Streamlining Access to Services	Goal 3: Improve Security Posture across the Federal Enterprise	Goal 4: Enable Trust and Interoperability	Goal 5: Reduce Costs and Increase Efficiency
• Align and Coordinate Federal Policies and Key ICAM Initiatives • Establish/Enforce Accountability to Governance Bodies	• Expand Secure Electronic Access to Government Data and Systems • Promote Public Confidence through Transparent Practices	• Support Cybersecurity Programs • Integrate Electronic Verification Procedures with Physical Security • Drive the Use of a Risk-based Framework for Access Control • Improve Electronic Audit Capabilities	• Support Information Sharing Communities of Interest • Align Processes with External Partners • Establish and Maintain Trust Relationships • Leverage Standards and Commercially Available Products	• Reduce Administrative Burden Associated with ICAM • Align Existing and Reduce Redundant Programs • Increase Interoperability and Reuse of Programs and Systems

Value Proposition

The ICAM segment architecture establishes the foundation for trust and interoperability in conducting electronic transactions both within the Federal Government and with external organizations. It encompasses the core capabilities to be able to identify, authenticate, and authorize individuals to provide appropriate access to resources, which is the lynchpin to the success of the national Cybersecurity initiative and the successful and secure adoption of electronic health records for the healthcare industry.



- **Increased security, decreased identity theft, data breaches, and trust violations**
- **Compliance with laws, regulations, and standards**
- **Improved interoperability**
- **Enhanced customer service**
- **Elimination of redundancy**
- **Increase in protection of personally identifiable information (PII)**