FICAM *in Brief*:

A Smart Card Alliance Summary of the

Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance

A Smart Card Alliance Identity Council and Physical Access Council White Paper

Publication Date: May 2010

Publication Number: IC-10002

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

Purpose of Summary Document

The Smart Card Alliance Identity Council and Physical Access Council developed this condensed summary of Part A of the "Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance" (referred to as the "FICAM document"), published November 10, 2009. The FICAM document was prepared by the Identity, Credential, and Access Management Subcommittee (ICAMSC) under the auspices of the CIO Council and at the request of the Federal Enterprise Architect.

The purpose of the document is to summarize the content of the original document to highlight key concepts and to make it more accessible to its target audiences. In developing and publishing the summary, the Smart Card Alliance hopes to expand the audience reading the document and promote its concepts broadly through the identity, credential and access management industry. Commentary has been kept to a minimum and included in footnotes.

This summary is not intended to be a substitute for the full FICAM document. Readers are encouraged to refer to full document for additional details.

Content has been extracted from the original document and summarized, following the same flow as the original document. Footnotes at the beginning of each section reference the original document pages that were summarized. Please note that footnotes from the original have not been included in this summary.

The Smart Card Alliance encourages readers to review the full original document for further detail and for references. The document is available at: http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf.

TABLE OF CONTENTS

TABLE OF FIGURES

Executive Summary[1]

The Federal Government operates in a constantly shifting threat environment and identity management issues have been well-documented by the Government Accountability Office (GAO), National Science and Technology Council (NSTC) and Office of Management and Budget (OMB). The Administration has laid out clear goals to make government more accessible to the American public and outlined these goals in the new Cybersecurity Initiative.[2] The Open Government Initiative[3] promotes transparent, collaborative and participatory government that fully engages the public, while promoting data security, privacy and high assurance authentication. In addition, there is an increasing need for improved physical security at federally owned and leased facilities and sites. Requirements are being identified to support electronic business at all levels of assurance with Federal business partners and agencies experiencing a growing need to exchange information securely across network boundaries.

Agencies are working to address these challenges by issuing Personal Identity Verification (PIV) cards. The Federal Public Key Infrastructure (PKI) connects agency and commercial PKIs via a trust framework. Working groups are tackling relevant questions in agency- and mission-specific situations. Therefore, the CIO Council established the Identity, Credential, and Access Management Subcommittee (ICAMSC) with the charter to foster effective ICAM policies and enable trust across organizational, operational, physical, and network boundaries. The intersection of digital identities, credentials, and access control and the need for one comprehensive management approach has been officially stated. The FICAM document was developed in support of the ICAM mission to provide a common segment architecture and implementation guidance. The President's FY2010 budget cites the development of the Federal ICAM segment architecture, stating that, "one of the major outcomes of this effort is to allow agencies to create and maintain information systems that deliver more convenience, appropriate security, and privacy protection, with less effort and at a lower cost."

Value Proposition

The purpose of the FICAM document is to provide agencies with architecture and implementation guidance that addresses existing ICAM concerns and issues they face daily. In addition to helping agencies meet current gaps, agencies stand to gain significant benefits around security, cost, and interoperability which will have positive impacts beyond an individual agency in improving the delivery of services by the Federal Government. It also seeks to support the enablement of systems, policies, and processes to facilitate business between the Government and its business partners and constituents. Benefits associated with the proper implementation of ICAM include: increased security, compliance, improved interoperability, enhanced customer service, elimination of redundancy, and increase in protection of personally identifiable information (PII).

These benefits leverage standardized controls around identity and access management. The ICAM target state closes security gaps in the areas of user identification and authentication, encryption of sensitive data, and logging and auditing. It supports the integration of physical access control with enterprise identity and access systems, and enables information sharing across systems and agencies with common access controls and policies. The document is a call to action for ICAM policy makers and program implementers across the Federal Government to take ownership of their role in the overall success of the federal cybersecurity, physical security, and electronic government (E-Government) visions, as supported by ICAM. The Transition Roadmap and Milestones in Chapter 5 of the FICAM document outlines several new agency initiatives and numerous supporting activities that agencies must complete in order to align with the government-wide ICAM framework, and that are also critical to addressing threats and challenges facing the Federal Government.

[1] Summary of Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance, Executive Summary, pages i-iii.

[2] http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

[3] http://www.whitehouse.gov/open/

1 Introduction[4]

1.1 Background

One of the most serious security challenges that the United States faces today is the threat of attacks on its digital information and related communications infrastructure. Security weaknesses found included the areas of user identification and authentication, encryption of sensitive data, logging and auditing, and physical access. The Identity, Credential, and Access Management (ICAM) effort will address the nation's increasing cybersecurity needs.

In recent years, increasing emphasis has also been placed on improving the physical security of the hundreds of thousands of facilities that the Federal Government owns and leases to support the diverse mission work of its agencies. GAO has identified the need to develop a common framework that includes key practices for guiding agencies' physical security efforts. Strong ICAM practices and the common framework outlined in the FICAM document will help address the persisting weaknesses within the Federal Government's physical security infrastructure.

Challenges lie in being able to verify the identity of an individual or non-person entity (NPE) and to establish trust in the use of that identity in conducting business. As a result, strong and reliable ICAM capabilities across the entire Federal Government are a critical factor in the success of all government mission work. A common, standardized, trusted basis for digital identity and access management within the federal sector is needed to provide a consistent approach to deploying and managing appropriate identity assurance, credentialing, and access control services. The Federal budget further recognizes the importance of the effort in promoting federation and interoperability, noting that, "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."

1.2 Purpose

The purpose of the FICAM document is to outline a common framework for ICAM within the Federal Government and to provide supporting implementation guidance for program managers, leadership, and stakeholders as they plan and execute segment architecture for ICAM management programs. The primary audience for the document is Federal Government ICAM implementers at all stages of program planning, design, and implementation; however, the document may also be used as a resource for systems integrators, end users, and other entities, such as state and local governments, and commercial business partners seeking interoperability or compatibility with federal programs.

1.3 Scope

The scope of this document is limited to two main components: 1) a newly offered government-wide ICAM segment architecture, and 2) implementation guidance and direction for the implementation of ICAM programs in accordance with the architecture. The scope is limited to ICAM programs that apply within and across agencies in a variety of environments and configurations. While detailed information is not provided about how an external entity should implement its own ICAM programs, the document provides information that is applicable to conducting business with the government where appropriate.

1.4 Document Overview

Chapter 2 provides an overview of identity, credential, and access management; Chapter 3 presents the methodology used to create the ICAM segment architecture; Chapter 4 describes ICAM use cases; Chapter 5 describes a series of logical steps or phases that enable the implementation of the architecture which defines the roadmap and milestones for full ICAM implementation.

[4] Summary of "Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance," Section 1 - Introduction, pages 1-5.

2 Overview of Identity, Credential and Access Management[5]

Today, there is a strong desire across and within the Federal Government to unify these areas and other identity management initiatives within government to create a comprehensive and integrated approach to ICAM challenges.

This section provides an introduction to identity, credential, and access management (ICAM) referencing the primary compliance drivers: electronic authentication (E-Authentication) policy framework and two of its enablers, namely the HSPD-12 and Federal PKI initiatives. All ICAM programs within the Federal Government will align with the government-wide framework and interoperate with the infrastructure that supports it.

2.1 ICAM in the Federal Government

ICAM comprises the programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and non-person entities (NPEs), and to bind those identities to credentials. ICAM cuts across numerous offices, programs, and systems within an agency's enterprise, which are typically directed and managed separately. Figure 1 provides a high-level overview of the complementary nature of different parts of ICAM and how concepts that were once viewed as stove-pipes can intersect to provide an enterprise capability.

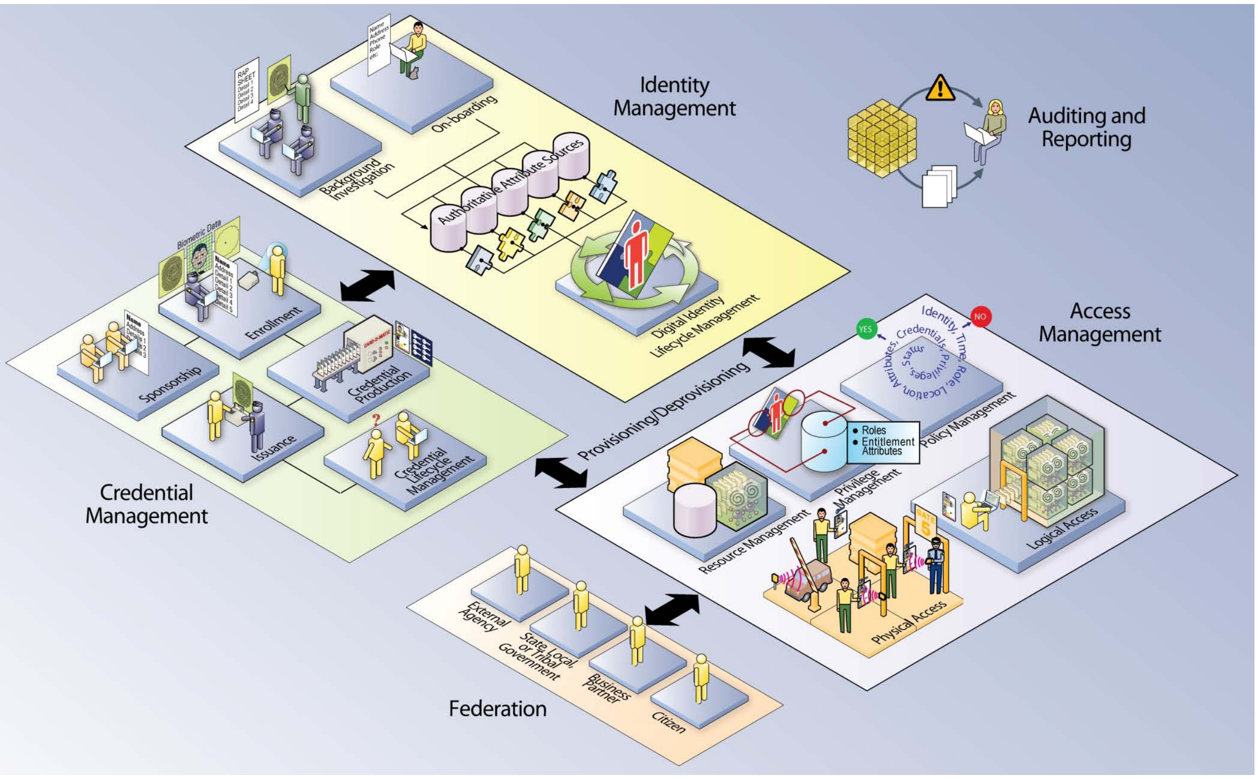


Figure 1. ICAM Conceptual Diagram

Behind the technology and the solutions that are deployed are the governance and policies needed for solutions to be successful from a business and security perspective. For example, each activity depicted must also support policies and accommodate remediation activities for individuals denied access or services. This requires long-term strategic initiatives across departments and agencies which focus on all aspects of ICAM, and not just the technology to be deployed. It also requires the development of trust

[5] Summary of "Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance," Section 2 - Overview of Identity, Credential and Access Management, pages 7-22.

models across departments, agencies, and external entities, ensuring assurance levels are uniform for authentication purposes and defining security policies around authorization and access management.

The following subsections provide additional detail on the constituent parts of ICAM and discuss the elements shown in Figure 1 in greater detail.

2.1.1 Identity Management

Identity management is defined as "the combination of technical systems, rules, and procedures that define the ownership, utilization, and safeguarding of personal identity information." The primary goal of identity management is to establish a trustworthy process for assigning attributes to a digital identity and to connect that identity to an individual. The ICAM document offers an approach to identity management wherein creation and management of digital identity records are shifted from stove-piped applications to an authoritative enterprise view of identity that enables application or mission-specific uses without creating redundant, distributed sources that are harder to protect and keep current. With the establishment of an enterprise identity, it is important that policies and processes are developed to manage the lifecycle of each identity, where management includes a number of factors including schema framework, policies and procedures, and protection of personally identifiable information (PII).

2.1.2 Credential Management

According to NIST SP 800-63, a credential is, "an object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person." Credential management supports the lifecycle of the credential itself. The policies around credential management, from identity proofing to issuance to revocation, are fairly mature compared to the other parts of ICAM. The PIV standards (e.g., Federal Information Processing Standard 201 (FIPS 201), SP 800-73) and Federal PKI Common Policy are examples of documents which have been in place and are foundational to agency-specific credential implementations. As shown in Figure 1, credentialing generally involves five major components: sponsorship, enrollment, credential production, issuance and management (maintenance of a credential over its lifecycle), which might include revocation, reissuance or replacement, re-enrollment, expiration, personal identification number (PIN) reset, suspension, or re-instatement.

A key distinction in the lifecycle management of credentials versus identities is that credentials expire. The attributes which form your digital identity may change or evolve over time, but your identity does not become invalid or terminated from a system perspective. Also, another key aspect of credential management is credential security and protection, from credential issuance to use.

2.1.3 Access Management

Access management is the management and control of the ways in which entities are granted access to resources. The purpose of access management is to ensure that proper identity verification is made when an individual attempts to access security-sensitive buildings, computer systems, or data. It has two areas of operations: logical and physical access. Logical access is access to an IT network, system, service, or application. Physical access is access to a physical location such as a building, parking lot, garage, or office. Access management leverages identities, credentials, and privileges to determine access to resources by authenticating credentials. After authentication, a decision can be made about whether the individual is authorized to access the resource. These processes allow agencies to obtain a level of assurance in the identity of the individual attempting access. Figure 1 shows three core support areas that enable successful access management for both physical and logical access: resource management processes for establishing and maintaining data; privilege management processes for establishing and maintaining the entitlement or privilege attributes that comprise an individual's access profile; and policy management processes for establishing and maintaining policies that incorporate business rules and logic, usually based on attributes or roles. This governs what is allowable in an access transaction.

A key aspect of access management is the ability to leverage an enterprise identity for entitlements, privileges, multi-factor authentication, roles, attributes and different levels of trust. Logical access and physical access are often viewed as the most significant parts of ICAM in order to achieve a return on investment.

2.1.4 ICAM Intersection

ICAM programs have many areas of overlap, including physical and logical access components, digital identities and attributes along with the systems that store them, and the workflow solutions that enable strong and dynamic processes. One of the primary dependencies across both the credentialing and the access control environments is the presence of accurate identity and attribute information necessary to bind the digital representation of an entity to the credential, user accounts, and access privileges. The access decision must correspond to the correct digital identity. This demonstrates the intersection of identity, credential, and access management. Challenges, nevertheless, exist to the adoption of a consistent approach to ICAM implementation. Addressing these challenges begins with viewing ICAM holistically. ICAM promotes a comprehensive, coordinated approach to help resolve the significant IT, security, and privacy challenges facing the Federal Government. Just as identity, credential, and access management activities are not always self-contained and must be treated as a cross-disciplinary effort, ICAM also intersects many other IT, security, and information sharing endeavors. It is expected that ICAM will touch many initiatives not specifically mentioned in this architecture and will be incorporated into holistic agency plans for their enterprise IT, mission and business service architectural segments.

2.2 ICAM Goals and Objectives

The following goals and objectives were created as part of the ICAM segment architecture development effort.

2.2.1 Goal 1: Comply with Federal Laws, Regulations, Standards, and Governance Relevant to ICAM

Objective 1.1: Align and Coordinate Federal Policies & Key Initiatives Impacting ICAM Implementation
Objective 1.2: Establish and Enforce Accountability for ICAM Implementation to Governance Bodies

2.2.2 Goal 2: Facilitate E-Government by Streamlining Access to Services

Objective 2.1: Expand Secure Electronic Access to Government Data and Systems
Objective 2.2: Promote Public Confidence through Transparent ICAM Practices

2.2.3 Goal 3: Improve Security Posture across the Federal Enterprise

Objective 3.1: Enable Cybersecurity Programs
Objective 3.2: Integrate Electronic Verification Procedures with Physical Security Systems
Objective 3.3: Drive the Use of a Common Risk Management Framework for Access
Objective 3.4: Improve Electronic Audit Capabilities

2.2.4 Goal 4: Enable Trust and Interoperability

Objective 4.1: Support Information Sharing Environment (ISE) Communities of Interest
Objective 4.2: Align Processes with External Partners
Objective 4.3: Establish and Maintain Secure Trust Relationships
Objective 4.4: Leverage Standards and Commercial Off-the-Shelf Technologies for ICAM Services

2.2.5 Goal 5: Reduce Costs and Increase Efficiency Associated with ICAM

Objective 5.1: Reduce Administrative Burden Associated with Performing ICAM Tasks
Objective 5.2: Align Existing and Reduce Redundant ICAM Programs
Objective 5.3: Increase Interoperability and Reuse of ICAM Programs and Systems

2.3 ICAM Governance

2.3.1 Governing Authorities

The Federal ICAM initiative is governed under the auspices of the Federal Chief Information Officer (CIO) Council Identity, Credential, and Access Management Subcommittee (ICAMSC) with program support by the GSA Office of Governmentwide Policy (OGP), and direct oversight from the Office of Management and Budget (OMB). Stakeholders such as the Department of Commerce via the National Institute of Science and Technology (NIST) and the Office of Personnel Management (OPM) have oversight and responsibility for policy and standards for ICAM functions across the Executive Branch.

2.3.2 Federal Policies and Key Initiatives Impacting ICAM Implementation

This section identifies the general laws, regulations, and policies that impact and/or initiated today's ICAM programs. The policy list (listed in the FICAM document) includes, but is not limited to: public orders, Executive orders, privacy and other Federal acts, information security acts and related programs, E-Government initiatives, HSPD-12 implementation guidance, and related OMB memoranda.

PART A: ICAM Segment Architecture

3 ICAM Segment Architecture[6]

This chapter presents the core components of the ICAM segment architecture organized into the five layers defined in the Federal Enterprise Architecture (FEA).

3.1 Developing the ICAM Segment

Segment architecture development is a collaborative process forming a bridge between enterprise-level planning and the development and implementation of solution architecture.

The Federal Segment Architecture Methodology (FSAM) is the process by which the ICAM segment architecture was developed. The FSAM:

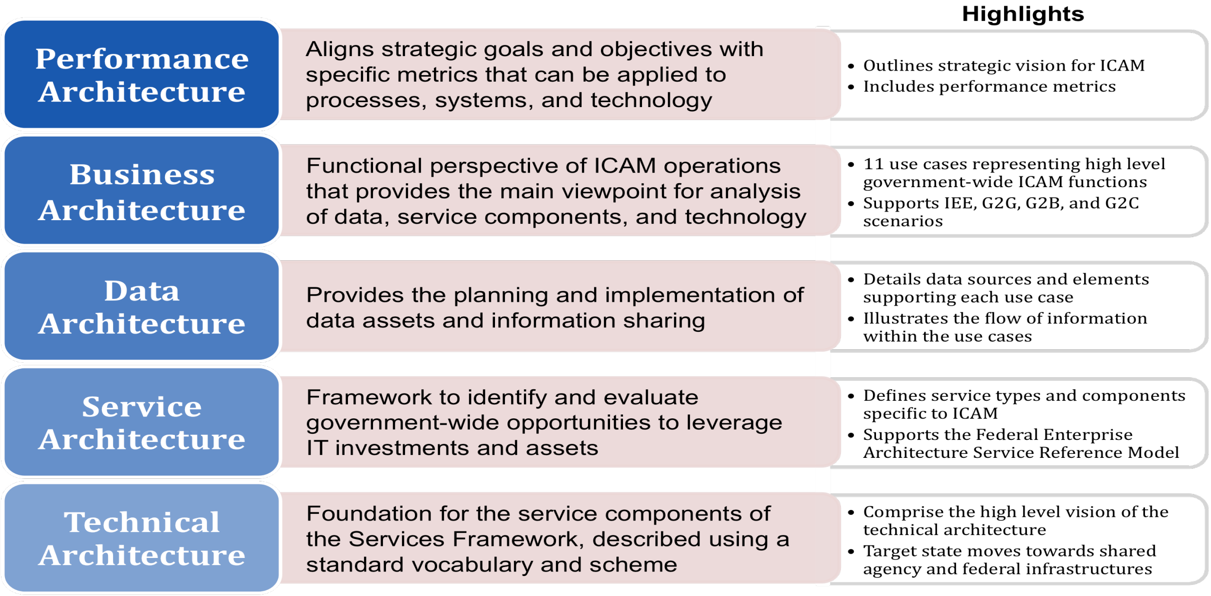
- Defines recommended analytical techniques and sample outputs for defining a business-driven architecture.
- Is a five-step process to help architects identify and validate the business need and scope of the architecture, define the performance improvement opportunities within the segment, and define the target business, data, services, and technology architecture layers required to achieve the performance improvement opportunities.
- Drives the creation of as-is state and future state descriptions, analysis of the gaps, and a transition plan for moving from the as-is to the future state.

Note that the methodology used to create this cross-federal segment was modified in some cases to accommodate direction at a cross-federal level.

3.2 ICAM Architectural Layers

Figure 2 summarizes the definition of the ICAM segment architecture layers.

Figure 2. Segment Architecture Layers and Definitions



		Highlights
Performance Architecture	Aligns strategic goals and objectives with specific metrics that can be applied to processes, systems, and technology	• Outlines strategic vision for ICAM • Includes performance metrics
Business Architecture	Functional perspective of ICAM operations that provides the main viewpoint for analysis of data, service components, and technology	• 11 use cases representing high level government-wide ICAM functions • Supports IEE, G2G, G2B, and G2C scenarios
Data Architecture	Provides the planning and implementation of data assets and information sharing	• Details data sources and elements supporting each use case • Illustrates the flow of information within the use cases
Service Architecture	Framework to identify and evaluate government-wide opportunities to leverage IT investments and assets	• Defines service types and components specific to ICAM • Supports the Federal Enterprise Architecture Service Reference Model
Technical Architecture	Foundation for the service components of the Services Framework, described using a standard vocabulary and scheme	• Comprise the high level vision of the technical architecture • Target state moves towards shared agency and federal infrastructures

[6] Summary of "Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance," Section 3 - ICAM Segment Architecture, pages 25-44.

Individual assets that comprise the architecture are presented throughout the FICAM document chapters. Section 3.2 of the FICAM document describes specific assets developed by architectural layer.

Table 1 below summarizes the assets developed for the FICAM segment architecture and their location within the document.

Table 1. FICAM Segment Architecture Description

Layer	Asset	Description	FICAM References
Performance Layer	Business Challenges Analysis	Provides overview of business challenges within current ICAM environment, representing strategic improvement opportunities for target state.	2.1 2.2
	Business Drivers, Goals and Objectives	Describes the goals, drivers, and objectives for ICAM.	2.1 2.3.2
	Performance Metrics	Creates reporting framework to measure activities and investments within the ICAM segment.	6.
Business Layer	Business Value Chain Analysis	Identifies the high-level logical ordering of the chain of processes that deliver value.	3.2.2
	As-is and Target Use Cases[i]	Provides high-level common business processes that support ICAM functionality. Use cases provide detailed architectural information at the data, service, and technology layers.	4.
Data Layer	Inventory of Government-wide Data Sources and Data Elements [ii]	This is a matrix of known data repositories for ICAM related data across the Federal Government.	3.2.3.1 4.
	Target Information Flow Diagrams [iii]	Depicts key information flows found in business processes and assists in finding opportunities for re-use via information-sharing services.	4.
Service Layer	Service Framework[iv]	Depicts specific service component sets (service types) and self-contained business processes or services exposed through technology interfaces with predetermined and well-defined functionality (service components).	3.2.4, 3.2.4.1 to 3.2.4.6
Technology Layer	As-is System Interface Diagrams [v]	Depicts existing systems and services in the as-is state and identifies relationships between them.	3.2.5.1
	Target System Interface Diagrams [vi]	Shows proposed systems and services in target state and identifies relationships between them.	2.3.5.2

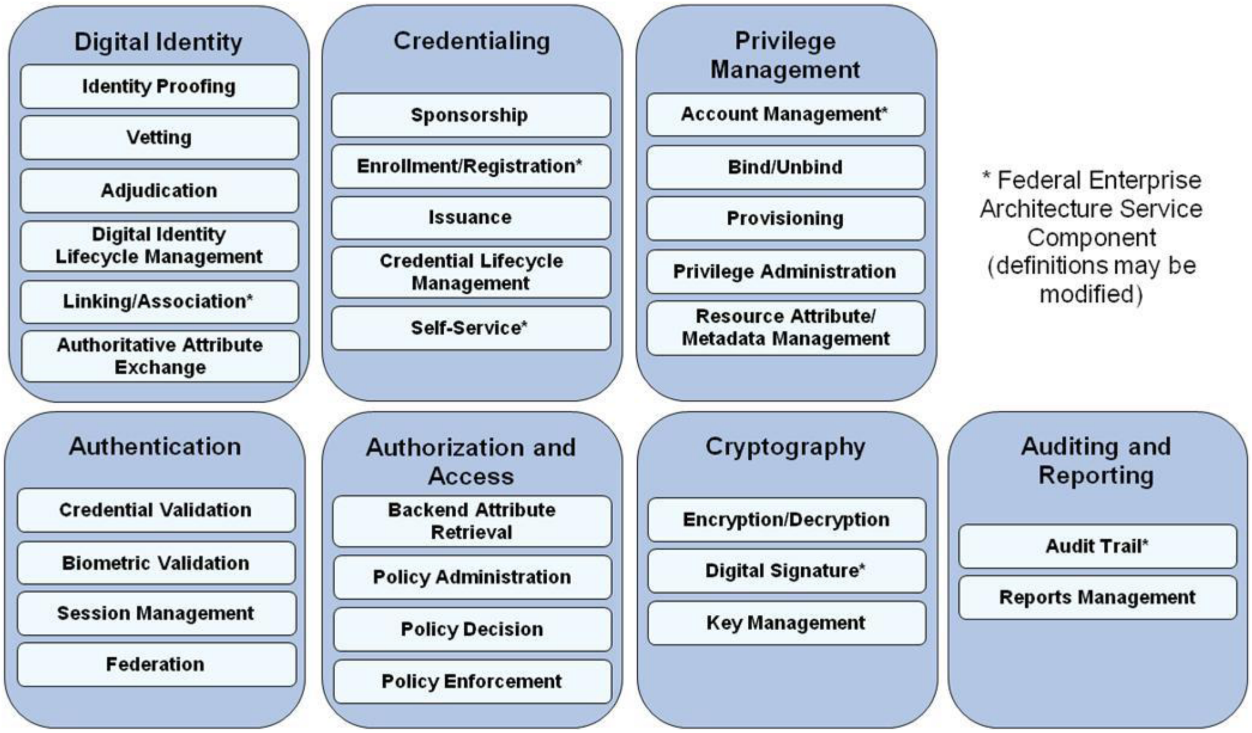
In addition to the descriptions above, several assets warrant more discussion. For example:

- [i] An overview of the 11 use cases is found in Section 3.2.2.2 of the FICAM document. Agencies are expected to tailor these use cases for their own ICAM segment architectures, which should align with this document.
- [ii] Section 3.2.3.1 of the FICAM document describes at a high level the inventory of government-wide data sources and elements used for ICAM.
- [iii] Section 3.2.3.2 of the FICAM document describes the data elements and details that can be found within the use cases of Chapter 4.
- [iv] Section 3.2.4.1 through Section 3.2.4.6 of the FICAM document gives definitions for each of the seven service types and 29 service components.
- [v] Section 3.2.5.1 of the FICAM document shows multiple "as-is" diagrams that provide a baseline of ICAM systems and services.

- [vi] Section 3.2.5.2 of the FICAM document shows multiple “target state” diagrams. It is part of the conceptual solution architecture.

Figure 3 shows the ICAM Services Framework which defines the service types and components necessary to support the ICAM segment architecture.

Figure 3. ICAM Services Framework

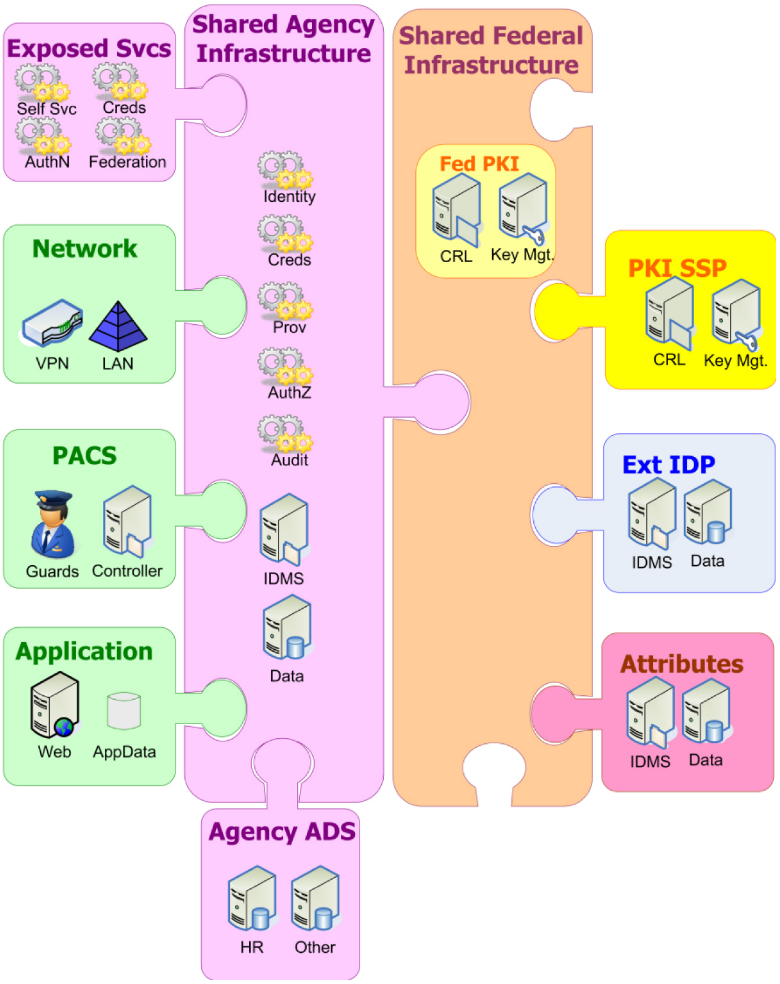


The ICAM Technical Architecture consists of the *as-is system interface diagrams* and *target system interface diagrams*[7]. The as-is architecture is composed of many independent applications and programs that don’t interoperate. Agencies are currently employing myriad processes for implementing ICAM capabilities as well as different types of technologies and standards to support these processes. As a result, agency systems are not interoperable, stove-pipes abound, processes are duplicated, and authoritative sources are, in many cases, unknown. In order to achieve the ICAM goals and objectives identified for the Federal Government, system changes must be made at both the agency and government-wide levels to create increased automation and interoperability within and across ICAM systems.

The target system will make better use of cross-government resources through designed cooperation and institution of centralized services. The key transition between the current agency architecture and the target state is the introduction of a shared agency infrastructure providing ICAM functions in place of independent functionality in every system. In addition, the shared agency infrastructure will connect to a shared Federal infrastructure that provides common, government-wide ICAM services. Figure 4 shows a conceptual diagram of the shared infrastructure. Similar to internal agency users, it is desired that external users in the target state may use a single, third-party credential to achieve seamless interaction with services across multiple agencies in the Federal Government.

[7] The reader is encouraged to review section 3 of the full FICAM document which includes a typical as-is diagram and a series of target system interface diagrams. These diagrams take the reader through the details of interoperability and shared services within an agency architecture, to growth of the solution to include services shared across the Federal Government, to interoperability with external identity providers.

Figure 4. Federal Enterprise Target Conceptual Diagram



4 ICAM Use Cases[8]

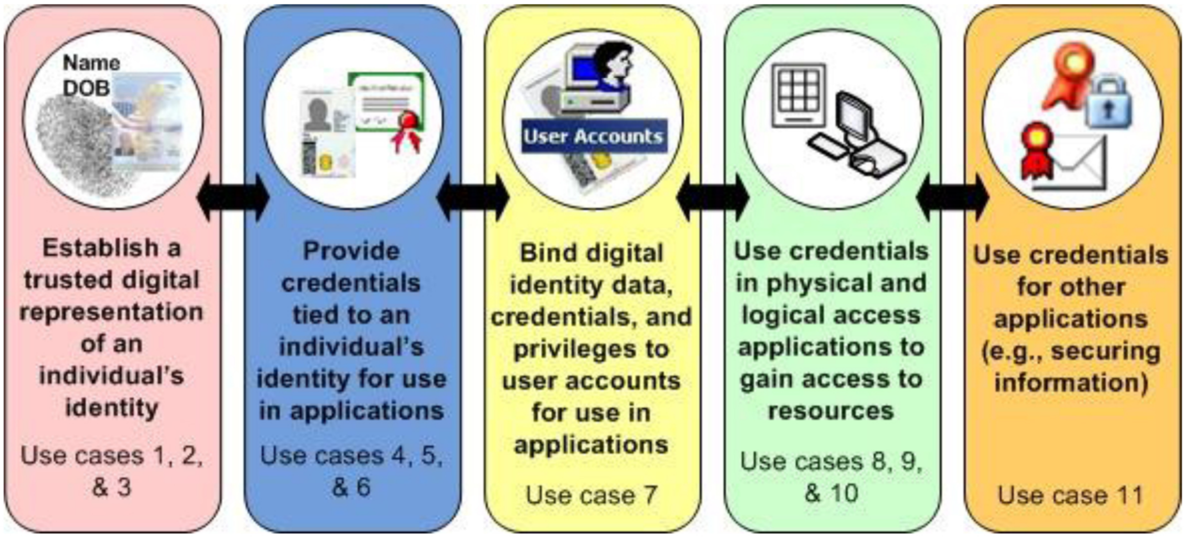
This chapter includes a synopsis of the high-level use cases that outline a related business function, including sections for:

- As-is analysis – the way the business function is completed today in the Federal Government
- Target analysis – the desired way to complete the business function
- Gap analysis – overview of the primary differences, for the transition roadmap and milestones

Each use case was selected to represent part of the core ICAM activities needed to service E-Government sectors and user groups, whether internal or external to an agency, as they conduct business with the Federal Government. These use cases encompass the major aspects of ICAM and include identity record creation, vetting, primary credentialing activities, provisioning, and physical and logical access.

Figure 5 provides an overview of the categories of use cases, grouped into lifecycle events.

Figure 5. Use Case Functional Overview


Name
DOB
User Accounts
Establish a trusted digital representation of an individual's identity
Use cases 1, 2, & 3
Provide credentials tied to an individual's identity for use in applications
Use cases 4, 5, & 6
Bind digital identity data, credentials, and privileges to user accounts for use in applications
Use case 7
Use credentials in physical and logical access applications to gain access to resources
Use cases 8, 9, & 10
Use credentials for other applications (e.g., securing information)
Use case 11

These use cases are meant to encompass daily functionality as they relate to ICAM systems within Federal agencies. It is expected that target state capabilities, including the use of the PIV card and PKI credentials, will be integrated into all new ICAM systems and applications. However, additional steps are needed to implement systems and procedures such that the target state processes described can be realized. Common actions and procedures that are required prior to the target steady-state include, but are not limited to:

- Identify and establish access rules
- Develop provisioning workflows
- Develop database inventories and linkages
- Identify authoritative data sources
- Centralize role and/or attribute based access control systems
- Complete a federation model

These activities, along with timelines and performance metrics, are described further in Chapter 5 of the FICAM document.

The following sub-sections provide a synopsis of the ICAM use cases using the following format:

[8] "Summary of Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance," Section 4 - ICAM Use Cases, pages 45-138.

- Challenges in the as-is analysis of the use case(s)
- Synopsis of characteristics and advantages of the target state
- Gaps and actions needed to migrate from the as-is state to the target state
- Alignment of use cases to E-Government and supporting examples

For the detailed sample process flows for each use case, please refer to the FICAM document and related sub-section.

4.1 Create and Maintain Digital Identity Record for Internal User

Use case 1 provides the high-level process for establishing a digital identity for an internal user and modifying the digital identity record over time as the user's attributes change. A digital identity record should be distinguishable from other stored electronic identities.

This use case is distinct from credentialing (covered in use cases 4, 5, and 6) in that identity records can be created without the issuance of a credential. Likewise, identity data can be shared with other systems for assignment of privileges. In the as-is state, identity record creation, credentialing, and provisioning are often tightly bound processes.

As-Is Analysis. This use case describes the processes of capturing data to identify an individual within a system of digital identity records. Once a record is established, policies may be applied or conclusions drawn. Some common attributes associated with a digital identity include:

- **Identity attributes**. Data such as name, eye and hair color, or place of birth.
- **Biographic attributes**. Contact information such as address, phone number, or e-mail address.
- **Context-specific attributes**. Data such as health, salary data, rank, title, or clearance level.
- **Affiliations**. Associations with specific agency locations, roles, internal or external groups, or professional/academic organizations.
- **Biometrics**. Attributes, such as facial image, fingerprints or voice.
- **Credentials**. Passwords, digital certificates, or ID cards for humans and digital certificates or other technologies for non-person entities.
- **Role information**. Categories often used to trigger rules (i.e., for access, provisioning).

In the as-is state, digital identity record creation is generally accomplished through independent means in numerous diverse ”stove-piped” systems with no reliable synchronization of identity data. Typically, there is no means to provide for uniqueness of users across the enterprise. Key issues with maintaining a digital identity in the as-is use case include:

- Administrative burden associated with digital identity creation and maintenance. Current processes require manual attribute updates within multiple systems, creating administrative burden.
- Identity data accuracy. Identity information is often duplicated across multiple systems. Records can easily get out of synchronization, resulting in conflicting records across the enterprise.
- Data security. Maintaining the same identity information in multiple systems increases the possibility of exposure of the information.
- Lack of integration. Lack of coordination across systems increases the risk associated with failing to terminate all associated accounts upon user separation from the organization.

Key assumptions for the as-is analysis include:

- Identity proofing, adjudication and background checks, and security clearance process completion are completed outside of this use case.
- Identity record deletion processes are not uniform.
- The identity record creation process steps generally align across agencies.

Process Flow. The as-is steps are broken into two different paths:

- Part 1: Create a new identity record
- Part 2: Change an existing identity record

Target Analysis. The target state vision is for a digital identity to be created or modified once in the authoritative system(s) and for authoritative identity attributes to be linked and shared with other systems across the enterprise. This distinction allows for streamlined management of digital identity information.

For the target vision, the following architectural changes are assumed:

- A common, government-wide specification for core attributes of a digital identity record.
- A mechanism for sharing authoritative identity data from core repositories across the enterprise.
- Interoperability between systems by establishing or leveraging existing data standards.
- Minimization of paper-based processes for collecting and sharing data to create an identity record.

The following assumptions are added in the target state for this use case:

- Data is exchanged electronically, with the authoritative data source identified for each core identity attribute.
- Data formerly managed in paper-based systems will have appropriate auditing and archiving.
- Workflows for appropriate sharing of identity data are established prior to start of process flows.

Process Flow. The target steps are the same two paths as the as-is steps:

- Part 1: Create a new identity record
- Part 2: Change an existing identity record

Gaps. The high-level gaps include: (1) lack of common definition or data specification for the minimum data elements for creating and sharing digital identity data; (2) lack of common definitions of additional identity attributes for mission-specific functions; (3) inability to correlate and synchronize digital identity records and automatically push and pull identity data between systems; (4) lack of authoritative sources for contractor/affiliate identity data; and (5) prevalence of redundant collection and management of digital identity data for a single user. To address these agencies should:

- Standardize core data elements and other common identity attributes.
- Adopt methods to translate local data to the standardized set to enable data sharing across agencies.
- Develop a service such as the Authoritative Attribute Exchange Service (AAES) and/or a set of common interconnections to index and link authoritative sources so that core identity data and peripheral data may be collected once and shared many times across applications.
- Minimize collection of digital identity data, instead linking to the authoritative source to manage updates and reduce the need to request the information.

4.2 Create and Maintain Digital Identity Record for External User

Use case 2 provides the high-level process steps for establishing a digital identity for an external user and modifying the digital identity record over time as the user's attributes change. External users provide information during the course of doing business with the government (e.g., student loan applications, Internal Revenue Service (IRS) tax records). The information collected forms the basis for user account access in individual applications (addressed in use cases 8, 9 and 10).

This use case represents a complex and varied set of mission-specific scenarios through which Federal agencies collect and maintain personal information for users external to their agencies. An external user may be an employee, contractor, or affiliate of another Federal Executive Branch agency; an individual from another branch of the Federal Government or from a state, local, or tribal government; or an individual external to the Federal Government. Despite its complexity, this use case has been included to address increasing interest in managing digital identities for individuals outside an agency in order to build a foundation for secure, efficient, and transparent electronic interactions with these external sectors.

As-Is Analysis. The process for creating a digital identity record in the as-is state is tied closely to credentialing (use case 6) and provisioning (use case 7).

Current challenges associated with the as-is model include:

- There is no agreed upon identity data model within most mission segments, or the way in which identity data should be formatted and transmitted.
- Identity records are not linked to authoritative sources, so that multiple records for an individual exist within an agency or across the federal enterprise. Mission-related data (e.g., tax ID number for the IRS) are commonly used to verify individuals for access to each individual application.

Process Flow. The as-is steps for this use case are broken into two different paths:

- Part 1: Create a new identity record
- Part 2: Change an existing identity record

Target Analysis. In the target state, many mission-specific, external-facing applications will likely continue to need to establish a basic record for users in order to grant access; however, it is intended that mission segments will have agreed-upon standards for the information that is to be collected to minimize the gathering of unnecessary data and to enable greater information sharing where possible. As with use case 1, it is envisioned that the creation of application-specific credentials will be decoupled from the creation of the identity record such that identity credentials issued by third parties can be linked to user accounts across applications (discussed further in use cases 6 and 10).

Specific communities of interest may establish common formats for common fields to enable interoperability. Needed adjustments include translating common data formats and exploring opportunities for automation. Links to external systems may also be required to use existing credentials, affiliations, and background investigations that were provided by a trusted partner organization. Examples of this include state and local law enforcement identities and visitors from different agencies.

Process Flow. The target steps for this use case are broken into the same two paths:

- Part 1: Create a new identity record
- Part 2: Change an existing identity record

Gaps. The high-level gaps include: (1) need for common definitions of identity attributes required for mission-specific functions; (2) prevalence of redundant collection and management of digital identity data for the same user; (3) need for a capability to bind third party credentials to an external user’s identity record. To address these, agencies should:

- Standardize other common identity attributes and adopt methods to translate local data to the standardized set in order to enable data sharing across agencies.
- Minimize duplicative data collection across agency applications that service external communities by leveraging existing agency data sources for external users.
- Link external users' digital identity records to externally issued credentials.

4.3 Perform Background Investigation for Federal Applicant

Use case 3 provides the high-level process steps for conducting a background investigation for a federal employee, contractor, or affiliate, focusing on the common aspects that are processed by OPM on behalf of an agency. Although the process for creating and issuing a PIV card is addressed in a separate use case (use case 4), the processes are intertwined, and it is intended in the target state that the architectural components supporting the PIV use case be fully leveraged to streamline the conduct of a background investigation.

As-Is Analysis. A background investigation consists of searches of records covering specific areas of an individual‘s background, typically during the past five years. The background investigation is typically conducted by OPM on behalf of an agency; however, some agencies have the authority to conduct their own investigations. Challenges associated with the as-is model include:

- A heavy reliance on manual and paper records systems
- Redundant and stove-piped information collection
- No direct link between FBI National Criminal History Fingerprint Check and PIV credentialing
- No direct link to other ICAM systems or use cases
- Specialized or non-standard investigations that engender little trust or reciprocity across agencies
- A long delay between the initiation of a background investigation and its adjudication

Key assumptions for this use case include:

- Agency-specific processes or requirements are considered outside the scope of this use case.
- Completion of the security clearance process is outside the scope of this use case.
- Background investigations for Federal employees and contractors is considered within scope.
- Background investigations for individuals outside of the Federal government are out of scope.

Process Flow. The as-is steps for this use case include:

- Process A: A background investigation has already been completed and is current.
- Process B: A new background investigation must be conducted.

Target Analysis. The main objectives in the target state are to automate processes that are currently manual and to better integrate with and leverage other ICAM processes to streamline the background investigation process. Achieving the target state objectives requires the following architectural changes:

- Fully leveraging the PIV enrollment process to capture and share biometric and biographic data to support background investigations.
- Reducing or eliminating paper forms and manual processes in favor of automated systems.
- Sharing information between related databases to reduce administrative burden on applicants.
- Making background investigation result information available to agencies to honor reciprocity of a background investigation completed by another agency.
- Using the Clearance Verification System (CVS) to streamline the process for honoring reciprocity of an existing investigation.

Gaps. The high-level gaps include: (1) lack of reciprocity in the acceptance of background investigations completed by or on behalf of another agency; (2) need for common interface standards to conduct automated record checks; (3) lack of mapping between credential issuance and ongoing investigative results; (4) lack of integration between PIV enrollment and background investigation processes; and (5) redundant data collection between background investigations and other ICAM processes.

To address these, agencies should:

- Work to honor reciprocity of background investigations wherever possible.
- Ensure that common data standards are employed at agency-level authoritative sources and other cross-agency repositories that must interface with them.
- Monitor and manage a person's eligibility over time. Changes in status or eligibility should be reported through reciprocity.
- Better integrate enrollment and investigative processes to eliminate redundancy and ensure a strong tie between data used to determine suitability/fitness and data used in credentialing.
- Minimize duplicative data entry for end users by collecting data once and reusing it for background investigations or other processes wherever possible.

4.4 Create, Issue, and Maintain PIV Card

Use case 4 describes high-level process for (1) creating and issuing, and (2) maintaining a PIV credential for a Federal employee or contractor, as defined by FIPS 201, for the lifecycle of the card. Similar issuance processes may occur for PIV-interoperable credentials outside of the Federal Government.

As-Is Analysis. Responsibilities for creating and issuing a PIV card are split among roles, separating duties so that no insider operating alone can cause a PIV card to be fraudulently issued.

Current challenges with the as-is model include:

- Little coordination between background check and PIV enrollment processes.
- Integration of changes to related standards and directives into the PIV process, including Federal/Emergency Response Official (F/ERO) repository linkage and alternative biometric verification processes.

Assumptions include:

- Temporarily lost or forgotten PIV card replacement processes are out of scope of this use case.

- Recovery of a revoked PIV card is governed by agency-specific policies and is out of scope.
- All events are logged in an audit log system.

Process Flow. The as-is steps for this use case are:

- Part 1: Create a new PIV record, including four mandatory steps proceeding in the following order: (1) sponsorship; (2) enrollment; (3) adjudication; and (4) issuance.
- Part 2: Maintain an existing PIV record, encompassing seven distinct events that may occur over the PIV lifecycle, in any order: (1) PIV card certificate update; (2) reissuance of PIV card that is lost, stolen, or compromised; (3) renewal of PIV card; (4) PIN change; (5) PIN reset; (6) key recovery of the key management key; and (7) PIV card termination/revocation.

Target Analysis. The as-is and target use cases are very similar in terms of technology and data. The target state includes more direct integration to outside lines of business. Current limitations include the lack of:

- Common interface to existing investigative databases, causing duplicate paperwork.
- Interface between human resource (HR) systems and the identity management system (IDMS).
- Links to authoritative source data such as identity attributes, training, and employment status.

Architectural changes needed to get to the target state are:

- Creating a direct link to FEMA's F/ERO repository.
- Creating a link from the PIV IDMS to the agency provisioning engines to support automated provisioning into logical access control system (LACS) and physical access control system (PACS) applications.
- Clarifying guidance for use of alternate biometric modalities in PIV processes for users without usable fingerprint biometrics.
- Enabling automated key recovery.

Gaps. Identified gaps center around redundant activities that result from the lack of integration with adjacent systems and processes. To address these, agencies should:

- Incorporate first responder requirements into PIV systems, standardize responder designations, and interface to the FEMA F/ERO database.
- Link identity data required for PIV identity proofing and enrollment processes to authoritative repositories or directories to enable synchronized updates.
- Integrate enrollment and investigative processes so that fingerprints captured during PIV enrollment are forwarded to OPM/FBI, and results are made available to adjudicators. Fingerprints taken during PIV enrollment must be linked to the investigative record on file.
- Reduce the number of PIV cards (credentials) issued to each individual, and instead enable the use of the PIV card already issued to that individual.

4.5 Create, Issue, and Maintain PKI Credential

PKI credentials on PIV cards are covered by use case 4, being a significant example of PKI credential usage. Use case 5 more generally addresses the minimum processes outlined in the Federal PKI Common Policy Framework (COMMON) and the Federal Bridge Certification Authority (FBCA) Certificate Policy, which govern PKI credentials in both PIV and non-PIV environments.

PKI certificates can be issued as “soft” certificates, with the private key installed as part of a software application (usually directly to a computer or other device) or as hardware certificates, where the private key is installed on a protected, FIPS 140-validated hardware token.

As-Is Analysis. Per NIST SP 800-63 and OMB M-04-04, PKI certificates issued under COMMON or by certification authorities (CAs) cross-certified with the FBCA are acceptable for authenticating entities at Assurance Levels 3 and 4, and may be used for authentication, digital signature and encryption. Assurance Level 4 certificates must be installed on a hardware token, while Assurance Level 3 certificates may be hard or soft. Identity proofing requirements vary based on the assurance level.

Specific challenges associated with the current state include:

- Some agency CAs are not cross certified with the FBCA, operating in violation of policy.
- Federal rules and guidance for managing key history are not well-defined.
- Federal rules and guidance for managing key escrow are not well-defined.

Process Flow. The as-is process flow includes:

- Part 1: Create and issue a new PKI certificate, including two mandatory steps which occur in the following order: (1) identity proofing, and (2) issuance.
- Part 2: Maintain an existing PKI certificate, encompassing four distinct events that may occur over the certificate lifecycle, in any order: (1) certificate renewal; (2) certificate re-key; (3) certificate modification; and (4) certificate revocation.

Target Analysis. No process changes are needed for creation and issuance of PKI certificates, as these are well developed under the Federal Bridge Policy Authority. However, there are some key changes regarding usage and lifecycle support capabilities.

Agencies should eliminate the issuance of separate, non-PIV PKI credentials to internal users, using instead the PIV card's PKI credentials: (1) PIV Authentication Key (for facility access and smart card logon); (2) Card Authentication Key (for facility access applications); (3) Digital Signature Key (for digitally signing documents and email); and Key Management Key (for managing keys to encrypt email and documents).

Agencies should accept third-party credentials at Assurance Levels 3 or 4 for external users (e.g., state or local government users or business partners), eliminating cost and administrative burden. (Additional information is included in use case 10.)

The target state incorporates:

- Issuance of certificates from CAs cross-certified with the Federal Bridge.
- Implementation of key history practices at the CA.
- Increased directory mappings to allow certificates issued from external CAs to be used.

Gaps. Identified gaps center around underutilization of PIV PKI certificates, lack of government-wide guidance for key history, redundant credentialing, lack of adoption of path discovery and validation, and needed infrastructure upgrades. To address these, agencies should:

- Minimize or eliminate issuance of separate soft certificates to PIV cardholders.
- Protect on-card key history with password, PIN or cardholder biometric.
- Leverage government adoption schemas for additional technologies at Assurance Levels 3 and 4, using common services and technologies where possible.
- Implement path discovery and validation that can trust external PKI and cross-certified Federal Bridge issuers.
- Upgrade the public key infrastructure to support the anticipated increase in usage.

4.6 Create, Issue, and Maintain Password Token

Password tokens must be created and issued to users, and changed periodically when forgotten or compromised. Password tokens are typically application-specific, and often closely tied to creation of a digital identity record and user account within that application. Use case 6 has been split from use case 1 to clearly articulate that managing identities can and should be handled separately from managing the credentialing and access that relies on them.

As-Is Analysis. Application owners primarily control creation and issuance of password tokens to users, leading to stove-piped credentialing processes. The norm is for each application to manage its own access and password management processes, though exceptions exist. Some application passwords (e.g., Windows logon) are managed across the enterprise, and, in some limited scenarios, external users (e.g., businesses, citizens) are provided password tokens centrally for use in multiple applications.

Today, most Federal applications are accessed using passwords, so that password management is a primary activity for application administrators. In addition, many issuance processes do not incorporate identity proofing, are not mapped to Federal authentication assurance levels and can be easily compromised. Specific challenges faced in the current state include:

- A significant cost of helpdesk operations directly related to resetting passwords.
- Internal control of password creation per application, requiring multiple passwords for users and resulting in redundant costs and a less favorable user experience.

Assumptions for the as-is state include:

- Password management does not occur via domain controllers or other central management tools.
- Management of roles, identity data or privileges associated with the password is out of scope.

Process Flow. The as-is steps include:

- Part 1: Create a new password token
- Part 2: Change an existing password token

Target Analysis. Use of passwords for internal users is minimized in favor of the PIV card and other identity credentialing solutions. Application owners and administrators migrate away from passwords to use of the PIV card.

For the external user communities (i.e., government to consumer (G2C), government to business (G2B), government to government (G2G)), trusted external identity providers (IDPs) are leveraged to issue identity tokens to user communities and to provide identity assertions to local applications. Applications trust the IDP‘s assertion of the user‘s identity, freeing administrators from managing user password tokens.

The Federal Government must accommodate citizens that do not have credentials from a third party and legacy applications that cannot use externally supplied assertions. These exceptions should be minimized to the extent possible, and local administrators must follow rules set in NIST SP 800-63 governing password strength.

The target state incorporates the following changes to the architecture:

- Elimination of password tokens where possible, replaced by the PIV card and identity assertions
- Elimination of duplicative infrastructure, to reduce costs of expired or forgotten passwords
- Reduction in requirement for agencies to update passwords
- Use of high assurance credentials wherever possible

Process Flow. The target state eliminates this use case 6 in favor of creating a digital identity for a user (use cases 1 and 2), provisioning a user account and binding an external credential to the account (use case 7), and granting logical access using either the PIV card or external identity assertions (use case 10).

Gaps. Identified gaps center around the burden associated with managing and remembering standalone passwords, and lack of full adoption of the PIV card. To address these, agencies should:

- Stop issuing password tokens wherever possible, instead leveraging PIV credentials and accepting assertions from approved IDPs.
- Complete their PIV implementation plans and begin using PIV cards and credentials in lieu of password logon.

4.7 Provision and Deprovision User Account for an Application

Provisioning is the mechanism by which identity accounts are linked to access privileges within applications; access to applications or facilities cannot be accomplished if the user account has not yet been provisioned.

As-Is Analysis. In the current state, the provisioning and deprovisioning of accounts are typically managed through manual, application-specific work streams. This creates a great administrative burden on application administrators and some provisioning processes employ paper-based approval workflows that are labor- and time-intensive. These conditions present a number of challenges for agencies:

- Efficiency. Manual approval and provisioning processes increase the time and effort required, resulting in higher cost and delays in the delivery of services.
- Scalability. As size and complexity grow, manual provisioning becomes harder to sustain.
- Security. It is not uncommon for user accounts and access privileges to remain available after the termination of the access need, posing a security risk to Federal Government resources.
- Segregation of duties. Manual processes lack visibility across applications and resources to determine if access permissions violate segregation of duties policies.
- Auditability. The ability to easily audit a specific person's accounts, privileges and activity in different systems across the enterprise is generally lacking.

Process Flow. The as-is process flow for this use case is broken into three parts.

- Part 1: Provision a user account and apply user permissions
- Part 2: Modify user permissions
- Part 3: Deprovision a user account

Target Analysis. In the target state, the underlying business need and function for provisioning and deprovisioning remain the same. The target flows reflect the following changes to the architecture:

- Automated and centralized workflows, automating repetitive, time-consuming tasks, allowing for quick, complex changes while reducing administrative costs, errors and deprovisioning processing time, and improving visibility across applications.
- Linking to external credentials/identity tokens trusted by the Federal Government

Assumptions for the target state include:

- Automated workflows to support individual provisioning are established, including routing of requests to appropriate individuals and the approval rules for establishing/altering accounts and privileges.
- Regular updates to provisioned attribute information is maintained and kept current.

Process Flow. The target process flow for this use case is broken into the same three parts.

- Part 1: Provision a user account and apply user permissions
- Part 2: Modify user permissions
- Part 3: Deprovision a user account

Gaps. Identified gaps center around the lack of automation, integration and interoperability of the provisioning and access control systems. To address these gaps, agencies should:

- Replace manual provisioning processes with centralized workflow engines which can provision/change/deprovision users for multiple access control points; tie all relevant applications/systems into the automated provisioning workflow where feasible, and upgrade legacy systems as needed.
- Integrate centralized provisioning functionality with the other ICAM processes, including credentialing, and leverage authoritative identity data for users to improve the accuracy and reliability of user data tied to accounts within individual applications.

4.8 Grant Physical Access to Employee or Contractor

Use case 8 provides the high-level process steps for granting physical access to a facility or site to internal agency employees, contractors, and affiliates who require PIV cards. This use case is separated from granting physical access to visitors and individuals with limited local facility access (use case 9) because it assumes that employees and contractors will be granted access using a common process and credential (i.e., legacy agency ID card in as-is state, PIV card in target state), whereas other individuals may be granted access through different processes with multiple ID types. This use case also relies upon completion of digital identity creation (use case 1), credentialing (use case 4), and provisioning (use case 7) in advance of the physical access attempt.

As-Is Analysis. Agencies control access to facilities through PACS. Current processes for granting physical access rely heavily on visual inspection and electronic access using diverse legacy technologies.

Proximity cards using 125 kHz frequency and tokens are the predominant legacy technologies, but magnetic stripe, bar code, barium ferrite, and some contactless smart card technologies are also used within the Federal Government. With the exception of contactless smart cards, each transmits a static number to the PACS, which matches the number against an access control list in order to grant access.

Challenges in the as-is state include:

- Interoperability. PACS are generally facility-centric rather than enterprise-centric with proprietary PACS architectures. Many ID cards operate only with the PACS for which they were issued.
- Scalability. Some deployed systems are limited in their capability to process the longer credential numbers (i.e., Card Holder Unique Identifier (CHUID)) associated with PIV cards necessary for government-wide interoperability.
- Security. Deployed PACS readers in most cases do not perform a challenge/response exchange. Bar code, magnetic stripe, and contact cards can be copied easily, offering little or no assurance.
- Validity. Many existing PACS verify expiration of credentials through a stored local date, with no synchronization to expiration or revocation information across multiple sites.

Key assumptions for the target state include:

- The processes to determine risk for particular areas and establish different authentication mechanisms and security features are considered outside the scope of this use case.
- Use of the PIV card for physical access is considered future state and is outside of the scope.
- Provisioning users and establishing access control policies and lists are performed in advance.

The as-is process flow offers two options for authenticating an individual and granting access:

- *Option 1: Physical/visual inspection*
- Option 2: *Electronic card verification*

Target Analysis. The target state assumes full implementation of the PIV card for electronic physical access for employees and contractors based on the guidance provided in SP 800-116. This enables use of a PIV card and multiple authentication factors described in FIPS 201 and SP 800-116. A conformant PACS may be configured to offer the relying party a high level of confidence in the true identity of the visiting individual as well as in the authenticity of the presented card.

Assumptions include:

- The card is PIV-conformant based on SP 800-73.
- Provisioning users and establishing access control policies are performed in advance.
- PIV authentication mechanisms are determined at agency discretion and are outside the scope.
- All challenge/response scenarios use asymmetric keys.
- All biometric authentication is performed with the standard fingerprint biometrics specified in FIPS 201 and SP 800-76. Alternate biometrics specific to an agency implementation are out of scope.
- Process flows authenticate successfully; failure to authenticate results in a failed access.

*Process Flow***.** A cardholder desiring access to a facility/area presents a PIV card to a card reader at the access point. The panel controlling access to the door performs one of the following:

A. CHUID + VIS: The PACS receives and validates the CHUID read from the PIV card.
B. Card Authentication Key (CAK): The PACS obtains the CAK certificate from the PIV card, validates the certificate, and verifies that the card holds the correct private key.
C. BIO: The cardholder provides the PIN and the live fingerprint sample that is validated against the biometric information embedded within the PIV card.
D. BIO-A: Uses the same process as with BIO above but the process is performed in the presence of a security officer.
E. PKI: The PIV card validates the cardholder-provided PIN and releases the PIV Authentication Certificate. The PACS validates the digital signature of the certificate via challenge/response.
F. CAK + BIO-A: This process includes an integration of the steps from options B and D.

In all cases, the PACS performs authorization based on local policies to grant or deny access. When access is granted, the entry point opens. The PACS creates a record of the access event.

Gaps. High-level gaps include: (1) inability of many installed PACS technologies to meet new requirements for electronic authentication outlined in NIST SP 800-116; (2) lack of integration between PACS and other ICAM provisioning and credentialing systems; and (3) the need to determine which PIV features are required. To address these, agencies should:

- Upgrade current technologies to support authentication of PIV cards, as defined in SP 800-116.
- Adopt an approach to managing and update PACS processes across the enterprise.
- Link with centralized or federated systems that can provide user attributes and credential information from authoritative data sources.
- Conduct facility risk assessments to determine which authentication mechanisms offer an acceptable level of physical security risk.

4.9 Grant Visitor or Local Access to Federally-Controlled Facility or Site

A visitor is an individual external to the agency who requires access (often short-term or intermittent) to a facility or site controlled by the agency. Local access or facility access applies to an individual who requires more long-term access, typically to a single facility, but who does not qualify to receive a PIV card (e.g., child care center workers, non-federal building tenants, Legislative and Judicial Branch employees). Both groups are addressed and it is expected that they may be granted access through different processes with multiple ID types.

As-Is Analysis. In the as-is state, there are disjointed processes and mechanisms for performing identity proofing and temporary credential issuance for visitors, regardless of whether they hold a valid Federal agency identity card or not. Challenges include:

- Inability of current infrastructure to validate external agency identity credentials.
- Lack of automated mechanisms to collect visitor data prior to arrival at the Federal facility.
- Lack of standardization around the types of credentials issued for visitor or facility access.

Key assumptions include:

- No data is being provisioned in the PACS in the as-is state.
- Processes for access to restricted or higher clearance areas/facilities are out of scope.
- All visitor access is substantiated by a sponsor, who validates the visitor's need for access.
- A visitor management system, either electronic or manual, is used to track visitor access.

Process Flow**.** This use case is divided into two parts:

- Part 1: Grant access to an agency visitor
- Part 2: Grant local facility access to an individual

Target Analysis. In the target state, processes should be automated to eliminate cumbersome paper-based processes, improve traceability for visitor sponsorship and access logging, and reduce the amount of time necessary to process visitors upon arrival at a facility. For visitors from another Federal agency with PIV cards, agencies should: standardize on the use of PIV credentials for access; incorporate the ability to provision external PIV credentials into the PACS; and perform electronic authentication of those credentials.

For individuals who required long-term facility access but do not meet the requirements to receive a PIV card, it is expected that agencies will adopt a common approach for issuing and accepting a Facility Access Card (FAC) and allow access to local facilities through electronic authentication mechanisms leveraging the FAC.

Key assumptions for this use case include:

- An electronic visitor management system is in place.
- An infrastructure is in place to support cross-agency use and acceptance of PIV cards.

Process Flow**.** This use case is divided into the same two parts:

- Part 1: Grant access to an agency visitor
- Part 2: Grant local facility access to an individual

Gaps. Identified gaps between the as-is state and the target state for agencies center around the lack of automation and consistency in processes, and the current inability of most agencies to electronically authenticate and accept PIV credentials. To address these gaps, agencies should:

- Upgrade current technologies, including web-enabled functionality, to support more automated processes for submitting an access request form prior to arriving at a site.
- Upgrade PACS to use PIV and PIV-interoperable credentials for across-agency visitors.

4.10 Grant Logical Access

This use case provides the high-level process steps for authenticating and authorizing a user to grant logical access to systems, applications, and data. The use case applies to both internal and external users using government and commercially-issued credentials to gain logical access across all assurance levels.

As-is Analysis. The as-is state includes a variety of mechanisms for granting logical access, many of which are tied to a specific application. Typically, an application is set up to use only one type of credential; a user ID/password combination is most prevalent in the as-is state. Other examples of tokens for granting logical access that are currently in use at agencies may include a one-time password (OTP) generator, internally or externally issued PKI certificates, USB tokens and other hardware tokens such as smart cards holding PKI certificates, and biometric matching.

Current challenges with logical access control include:

- Lack of integration with other ICAM processes and systems. Logical access control is typically run independently by each application. Many legacy applications aren't able to interface easily with enterprise single sign-on or provisioning tools.
- Lack of trust. The framework for trusting external identity and credential providers for access to local applications is not yet established, even within an agency.
- Redundant and incompatible authentication mechanisms. Selection of credentials have historically been application-specific, resulting in a wide array of credentials and protocols.

Key assumptions for this use case include:

- Provisioning users and establishing access control policies are performed in advance.
- The high-level steps for performing authentication and authorization are similar, regardless of the credential type used. Methods specific to a particular credential type are out of scope.
- Determining risk level for a particular application and establishing authentication mechanisms and security features are considered out of scope.
- Use of the PIV card for logical access is considered a future state process and is out of scope.
- Access to unrestricted applications is out of scope.

Process Flow. This use case has a single part for granting logical access.

Target Analysis. In the target state, granting logical access includes two main models. For internal users, it is intended that agencies will leverage the various capabilities of the PIV card, particularly the PIV authentication digital credential, to grant access to applications at all levels of assurance. A key goal is enabling single sign-on for Federal users of applications.

For external users, it is intended that agencies will adopt a model for federated identity, accepting third party credentials from external parties. A key goal for external users is to be able to access a variety of government services using a reduced set of login credentials and reusing existing credentials issued by a third party provider. Over time, it is anticipated that certain external users within the G2G and G2B sectors will possess PIV-interoperable credentials. Wherever possible, these credentials should be leveraged to maximize interoperability. Work is ongoing to develop acceptance criteria for third party credential types that are suitable for use by other external users at each of the four identity assurance levels outlined for federal systems within OMB M-04-04 and NIST SP 800-63.

Achieving the target state goals requires the following architectural changes:

- Implementing LACS. A flexible centrally-managed agency LACS is required to layer attributes and permissions, and map those to the authentication mechanism to make access decisions for all agency applications, including legacy.
- Enabling federation. The target state will require agreement on versions, technologies, formats, and oversight mechanisms to transfer and trust identities and credentials across agency boundaries and with external entities. Establishing trusted identity providers and similar mechanisms will enable service providers to make access decisions based on defined levels of trust.
- Fully enabling use of PIV and PIV-interoperable credentials. Agency LACS and applications must be upgraded where necessary to fully leverage the PIV credential for all network and application access for internal users. Where possible, this infrastructure can be leveraged to support users with PIV-interoperable credentials in other sectors.

Assumptions for this use case include:

- The processes to provision users into an application and establish access control policies and lists are performed in advance of the start of the process flow based upon applicable policy and guidance.
- Processes for granting access to internal users are based upon use of the PIV card. Use of other authentication types is considered outside the scope of the target process flow.
- Processes for granting access to external users are based upon consumption of credentials from external identity and credential providers. Scenarios utilizing individual application credentials are considered as-is state only.
- A mechanism for interim access in the event of lost or stolen cards is able to support smart card login without major impact to security or productivity.
- Target process flows reflect the use of a centralized LACS within an agency. However, control over access policies should still remain with application owners.

Process Flow. This use case is divided into two parts:

- Part 1: Grant access to a Federal agency employee or contractor
- Part 2: Grant logical access to external users

Gaps. The high-level gaps include (1) lack of ability to accept externally issued credentials; (2) lack of adoption of PIV technologies and processes; (3) need for enterprise-wide access management capability at the agency level; and (4) need for enhanced role and attribute data to perform situational access control.

To address these, agencies should:

- Enable relevant applications to accept external third party credentials.
- Adopt the authentication mechanisms of the PIV credential for logical access authentication at all assurance levels for internal users, and upgrade systems to enable PIV use.
- Complete an upgrade of current application infrastructures to allow for centralized workflow management for logical access, and determine architecture at the agency level to provide centralized workflows (e.g., implementation of enterprise-wide LACS application).
- Determine how to enable contextual (risk adaptive) role- or attribute-based access control based on established policy and rule sets and for real-time situational access control.

4.11 Secure Document or Communication with PKI

This use case provides the high-level process steps for digitally signing or encrypting data and electronic communications using the most common system tools available within the Federal Government.

- **Encryption** is the process of transforming data from a readable form into a form that requires an individual to possess a cryptographic key in order to read it. It is used to provide confidentiality for data.
- **Digital signature** is the result of a cryptographic transformation of data in order to provide origin authentication, data integrity, and signatory non-repudiation.

These capabilities are traditionally considered information security processes, but as important security applications of PKI credentials, they are included within the ICAM segment architecture.

As-is Analysis. Currently the use of PKI for encryption and digital signature is oftentimes inconsistently applied. This use case is considered a future state process and no process flow is provided.

Target Analysis. In the target state for internal users, the PIV card will be used as the PKI source for digital signatures and encryption. The target state provides guidance and best practices to uniformly apply encryption and digital signatures to secure documents and communications. Issues preventing widespread application of encryption and digital signatures in the current state will be addressed as follows.

- Solutions will be available to validate legitimate older digital signatures, even after the certificates themselves have expired.
- PKI will be used to support the Paperwork Reduction Act and provide higher efficiency through the use of digital signatures.
- Guidance will be made available to agencies for managing key history.
- Applications must be able to validate and decrypt secure documents and communications.
- Mechanisms will be in place to allow path discovery and validation trust across enterprises to enable agencies to accept PKI credentials from external users.

Assumptions in this use case include:

- PKI certificates for signing and encryption will only be accepted if they meet Federal Bridge standards and are issued from a CA that is a member of the Federal PKI trust framework.
- Certificate registration processes needed to recognize a PKI certificate are complete.
- Infrastructure and applications to process encryption and digital signatures are implemented.
- While best practices dictate the use of symmetric keys to perform encryption for large files, symmetric keys are considered outside the scope of ICAM as they are not tied to an individual.
- Cryptographic processes are largely transparent to the end user.

Process Flow. This use case is divided into parts for encrypting and digitally signing data:

- Part 1: Encryption and decryption of a file
- Part 2: Digitally signing a file or communication

Gaps. The high-level gaps include lack of government-wide (1) guidance regarding use of encryption and digital signatures; (2) adoption of PKI technologies and processes; and (3) guidance for key history management. To address these the Federal Government should:

- Develop guidance and standards for using PKI to secure email, encrypt controlled unidentified information (CUT) materials, and sign legal documents.
- Enable applications used for documentation and email exchange to use the PIV PKI credential.
- Develop guidance for key history management.

Gaps and Actions

The following table was included in the FICAM document, Section 5.1, with the addition of the use case(s) that the gap applies to.

Item	Gaps	Actions	Use Case

Item	Gaps	Actions	Use Case
1	No common definition or data specification identifying the minimum data elements for creating and sharing digital identity data.	Develop and implement a government-wide digital identity data specification to standardize and streamline collection, management, and sharing of identity data for an individual.	4.1
2	Need for common definitions of additional identity attributes required for mission-specific functions.	Implement Backend Attribute Exchange (BAE) common data elements or other shared attribute exchange models to support data sharing of common, mission-specific identity attributes outside of the core digital identity data elements within specific communities of interest.	4.1. 4.2
3	Inability to correlate and synchronize digital identity records and automatically push and pull identity data between systems.	Develop an authoritative AAES at the agency level to index and link authoritative sources of identity data and synchronize digital identity records for an individual.	4.1
4	Lack of authoritative sources for contractor/affiliate identity data.	Establish a government-wide approach for creating and maintaining contractor and affiliate identity data that can be used across agencies.	4.1
5	Prevalence of redundant collection and management of digital identity data for the same user.	Modify processes and systems such that identity data may be collected once and linked to authoritative sources throughout the enterprise for management and use of the data.	4.1, 4.2
6	Need capability to bind externally-issued credentials to an agency's identity record for an external user.	Develop and implement approaches and technologies enabling the linking of third party credentials to the digital identity records of external users for use in application access.	4.2
7	Lack of reciprocity in the acceptance of background investigations completed by or on behalf of another agency.	Resolve process and technology shortfalls preventing agencies from referencing and honoring reciprocity of background investigations for individuals adjudicated by another agency.	4.3
8	Lack of integration between PIV enrollment and background investigation processes.	Close process gap to ensure that the fingerprints used in processing background investigations are collected as part of the PIV enrollment and submitted electronically.	4.3, 4.4
9	No capability to reference prior background investigation for an individual based upon fingerprint biometric.	Establish capability to tie an individual to a prior background investigation based upon referencing fingerprints.	4.3
10	Lack of integration between PIV systems and FEMA F/ERO repository.	Integrate PIV systems with F/ERO database to provide required data.	4.4
11	Redundant credentialing processes.	Reduce the number of credentials issued for the same individual within and across agencies and enable the use of PIV and other credentials that have already been issued.	4.4, 4.5
12	Underutilization of PIV certificates as primary PKI credentials for internal users.	Enable the use of PIV certificates across the enterprise and eliminate redundant credentials.	4.5, 4.7
13	Lack of government-wide approach and guidance for managing key.	Provide guidance on the management of key history.	4.5, 4.11
14	Lack of product adoption for path discovery and validation.	Implement path discovery and validation products.	4.5
15	Administrative and user burden associated with managing and remembering numerous Federally-issued standalone password tokens.	Minimize the reliance on password tokens by enabling PIV usage for internal users and the acceptance of externally-issued credentials for external users.	4.6

Item	Gaps	Actions	Use Case
16	Lack of automation in provisioning workflows.	Implement automated processes and technologies to provision or deprovision users based on established business rules. Eliminate manual provisioning processes by tying applications/systems into the automated workflow.	4.7
17	Inability to perform cross-agency provisioning.	Work collaboratively to establish business rules for sharing identity/access record data as needed between agencies in order to provision access.	4.7
18	Lack of government-wide approach for provisioning logical access for external users.	Work collaboratively to determine approach for provisioning logical access for external users at all assurance levels.	4.7
19	Inability of many installed PACS technologies to meet new requirements for electronic authentication outlined in NIST SP 800-116.	Upgrade current processes and technologies to meet requirements.	4.8
20	Lack of integration between PACS and other ICAM systems (provisioning and credentialing systems).	Federate PACS with other ICAM systems to allow sharing of user attributes and credential information from authoritative data sources.	4.8
21	Lack of automation and consistency in agency processes/systems used for visitor access control.	Upgrade technologies to support secure, automated processes for requesting and provisioning visitor access.	4.9
22	Inability to electronically authenticate and accept PIV and PIV-interoperable credentials from visitors.	Enable the use of PIV and PIV-interoperable cards for visitor access.	4.8, 4.10
23	Need for enterprise-wide access management capability at the agency level.	Implement processes and technologies to support an agency-wide approach for managing logical access that links individual applications to a common access management infrastructure wherever possible.	4.10
24	Insufficient maturity in Backend Attribute Exchange implementation to support cross-agency data exchange in access scenarios.	Provide implementation guidance based on pilot deployment of the BAE to further enable ability to share data across agencies.	4.10
25	Lack of government-wide guidance regarding use of encryption and digital signatures.	Develop government-wide implementation guidance for the use of encryption and digital signatures.	4.11
26	Lack of adoption of PKI technologies and processes.	Fully enable the use of the PIV to further encryption and digital signature usage.	4.11

4.12 Application of the ICAM Use Cases

The eleven use cases outlined in this chapter are deliberately high-level so they can be applied across the federal enterprise. Agencies are expected to perform similar analyses on their systems and processes so that their ICAM architectures are specific to their own business processes. The general ICAM use cases outlined in this document can be combined and supplemented with agency-specific details that explain their own use case scenarios and process flows.

The overall purpose of the identification of the use cases is to combine the individual use cases and target architecture and technology and apply them to the relevant E-Government sectors to which the use cases align. Figure 5 (from Section 3.2.2.2 of the FICAM document) provides a mapping of the use cases to the E-Government sectors to which they may be applied. Four samples of applications in each of the E-Government sectors are identified and summarized; for details of the sample applications refer to the original FICAM document.

Figure 5. ICAM Use Case Alignment with E-Government Sectors

No.	Use Case Name	IEE	G2G	G2B	G2C
1	Create and maintain digital identity record for internal user	✓			

2	Create and maintain digital identity record for external user	✓	✓	✓	✓
3	Perform background investigation for federal applicant	✓			
4	Create, issue, and maintain PIV card	✓			
5	Create, issue, and maintain PKI credential	✓	✓	✓	✓
6	Create, issue, and maintain password token	✓	✓	✓	✓
7	Provision and deprovision user account for an application	✓	✓	✓	✓
8	Grant physical access to employee or contractor	✓			
9	Grant visitor or local access to federally-controlled facility or site	✓	✓	✓	✓
10	Grant logical access	✓	✓	✓	✓
11	Secure document or communication with PKI	✓	✓	✓	✓

Internal Effectiveness and Efficiency (IEE): User Management Scenario. A contractor working for an agency is hired to the Federal staff.

In this scenario, a Federal contractor has already been issued a secret clearance and a PIV credential for the agency where the contractor works, and will already have core identity and attribute data stored in authoritative repositories within the agency. The contractor is offered a position as a Federal employee within the same agency, but must switch to a new physical location. The contractor must re-enroll or be reissued a Federal PIV credential to indicate change in status. Likewise, many legacy application logins and Active Directories were based on the contractor's old username and role as a government contractor (e.g., Jane.Smith@contractor.gov). The agency's contractor authoritative source, hosted by the procurement office, is not the same repository as the employee authoritative source held within human resources. This scenario requires revoking old credentials and terminating access privileges to many of the applications to which the contractor had access, and then reinstating access rights to these or other applications using new credentials.

Government to Government (G2G): Emergency Responders. An incident occurs at a sensitive location and the incident site commander requests emergency responders with specific attributes from surrounding counties.

In this scenario, a hurricane has damaged a large classified facility, knocking down walls and scattering office documents. Hazardous Waste Operations (HAZWOPER) teams are required due to damage caused to the facility's power station. Due to the sensitive nature of scattered documentation that a responder may encounter, only those with suitable clearances are allowed to enter the perimeter. Personnel with proper attributes must be identified, requested, and allowed access into the perimeter using PIV and PIV-interoperable credentials. Some responders will use a PIV credential (e.g., the Department of Defense Common Access Card or CAC) while others will use a PIV-interoperable card (e.g., the First Responder Authentication Credential or FRAC).

Government to Business (G2B): Medical Information Exchange Scenario. A medical professional wishes to access restricted information about a clinical trial performed by a Federal agency (target state scenario).

In this scenario, a person who represents a hospital (a partner organization to a Federal agency) is requesting access to clinical trial information conducted by others, and is also attempting to report results for a clinical trial conducted using Federal funds. The user requires access to two applications from clinicaltrials.gov. The first application requires a level 3 token to access and report official trial data; the second application requires level 1 authentication as it is only used to create a personalized search page of public data not otherwise requiring authentication for access. In addition, the first application requires appropriate proof that the user is an authorized representative of a trusted partner organization.

Government to Consumer (G2C): Citizen Services. A citizen uses an existing identity credential to access a Federal research website.

In this scenario, a citizen is required to enter information into an online grant application form, and will need to use an Assurance Level one or higher credential to access the application. The user has not had previous dealings with the agency, so must provide basic information to the agency to create a user profile. The user is then able to use a password issued by a trusted member of a federated identity community (for example, OpenID) in which they are already a user.

5 Transition Roadmap and Milestones[9]

This section defines ways in which ICAM initiatives work together to improve performance by meeting major milestones, and to track overall progress against expected performance outcomes.

The Transition Roadmap is divided into three main parts:

- **Performance Improvement Recommendations.** Outlines implementation recommendations to address gaps defined in section four.
- **Initiatives and Milestones.** Prioritizes the implementation recommendations into a sequencing plan. Agencies are encouraged to include the activities in Section 5.2 of the FICAM document in their FY11 budget submissions.
- **Performance Metrics.** Defines government-wide performance metrics to create a reporting framework to measure success and investments.

5.1 Performance Improvement Recommendations

Based upon use case gap analyses, a set of high-level recommendations has been created to drive business performance improvements. Below are selected examples of the original 26 recommendations. For a complete list of recommendations see Section 5.1 of the original FICAM document.

- Develop and implement a government-wide identity data specification, collection and sharing approach that includes contractor and affiliate data, linkage to authoritative sources for data usage, as well as guidance for background check reciprocity.
- Close process gaps: collect fingerprints once for background investigations (BI) and PIV enrollment; link previous BIs to PIV issuance; reduce number of credentials and certificates issued per person; minimize use of passwords; automate provisioning and de-provisioning; and provide guidance on the management of key history.
- Work collaboratively to share identity/access record data and to provision logical access for external users.

5.2 Initiatives and Milestones

This section outlines the activities required to complete the overall transition of business processes, systems, and services to achieve the target state. The transition activities have been organized within nine core initiatives that support the goals and objectives of the ICAM segment for completion at the government-wide level and by the agencies themselves.

5.2.1 Government-wide Level Governance Initiatives

The ICAM governing authorities outlined in Section 2.3.1 of the FICAM document are primarily responsible for the following ICAM transition initiatives:

- Initiative1: Augment policy and implementation guidance to agencies
- Initiative 2: Establish federated identity framework for the Federal Government
- Initiative3: Enhance performance measurement and accountability within ICAM initiatives
- Initiative 4: Provide government-wide services for common ICAM requirements

[9] Summary of "Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance, Section 4 5 - Transition Roadmap and Milestones, pages 139-155.

5.2.1.1 Initiative 1: Augment policy and implementation guidance to agencies

Initiative 1 covers transition activities. Milestone dates associated with the augmentation of policy and implementation guidance to agencies begin in late 2009 and will proceed through October 2010 with benchmark dates throughout the time period. Transition activities have been grouped by activity owner.

- Architecture Working Group (AWG). Conduct survey for a common baseline of digital identity data elements and formats; review data elements and existing Federal data standards; provide further detail supporting the technical and data layers of the ICAM segment; develop a government-wide technical architecture; develop and publish an interface specification to facilitate the use of AAES for exchange of digital identity data across agencies and, with the Roadmap Development Team (RDT), determine if consolidation of ICAM services is feasible for the entire government.
- NIST. Create draft government-wide digital identity data specification that supplies the minimum data elements and data formats that provide a common definition of a digital identity record and issue guidance to agencies; issue agency guidance on final digital identity data specification; develop technical key management guidance; and, along with ICAMSC; develop guidance on alternative biometric modalities.
- ICAMSC. Promote understanding of OMB requirements; develop implementation guidance for the use of encryption and digital signatures; and address perceived liability with IDP services.
- RDT. Provide implementation guidance on BAE specification; expand the ICAM glossary; develop guidance on encryption and digital signatures and guidance on applicability of ICAM to NPEs.
- Federal agencies. Issue agency/department level policy on the use of PIV credentials for PACS/LACS access.

5.2.1.2 Initiative 2: Establish federated identity framework for the Federal Government

The activity owners will support transition activities, grouped below by owner, with milestones associated with establishing a federated identity framework for the Federal Government. These activities begin in late 2009 and will proceed through October 2010, with benchmark dates throughout the time period

- Citizen Outreach Focus Group (COFG). Provide recommendations for mechanisms to accept externally-issued credentials for application authentication of external users and support approach for provisioning logical access for external users; establish processes related to accepting and trusting externally issued credentials; provide guidance on authentication of external entities and decentralized identity provider models.
- ICAMSC. Establish and document certification process for federated credential and identity providers.

Some activities will be in coordination with ICAMSC, AWG, FPKIPA and FIWG. In addition, the AWG will complete scheme adoption processes for authentication technologies at all assurance levels.

5.2.1.3 Initiative 3: Enhance performance measurement and accountability within ICAM initiatives

The activity owners will support the transition activities, grouped below by owner, with milestone dates associated with the enhancement of performance measurement and accountability across ICAM initiatives. These activities begin in late 2009 and will proceed through October 2010, with benchmark dates throughout the time period.

- OMB. Incorporate SP 800-116 maturity model into the transition plan template and, along with RDT, create updated transition plan template for agencies to use.
- ICAMSC and RDT. Develop access control, credentialing, and identity data management recommendations for ICAM maturity models.

- Agencies. Develop transition plan to align agency architecture with the Federal ICAM segment architecture.
- RDT. Develop a performance reference model mapping for ICAM performance architecture.
- RDT and Interagency Security Committee (ISC) Convergence Committee. Develop measurable performance metrics to evaluate support for and usage of third party (PIV-interoperable) credentials.

5.2.1.4 Initiative 4: Provide government-wide services for common ICAM requirements

The activity owners will support the transition activities, and milestone dates beginning June 2010 through March 2011, associated with the provision of government-wide services for common ICAM requirements as listed below:

- OPM. Upgrade CVS to support reciprocity and communicate guidance and procedures to facilitate trust amongst agencies.
- FBI. Establish a mechanism to reference completed BIs based upon fingerprints to tie an individual claiming an identity to a previously vetted identity.
- GSA. Determine the feasibility of contractor PIV issuance that transcends agency boundaries; establish government-wide procurement vehicles for provisioning/workflow technologies and complete upgrades to Federal PKI. These activities are targeted for completion by September 2010.

5.2.2 Agency-level Implementation Initiatives

Each Federal Executive Branch agency is responsible for the following ICAM transition initiatives:

- Initiative 5: Streamline collection and sharing of digital identity data
- Initiative 6: Fully leverage PIV and PIV-interoperable credentials
- Initiative 7: Modernize PACS infrastructure
- Initiative 8: Modernize LACS infrastructure
- Initiative 9: Implement federated identity capability

Implementation milestone dates have been provided for each agency-level initiative as a guideline only. Agencies will establish completion milestones in collaboration with OMB based on their as-is state. These milestones will be reported and tracked using the ICAM Transition Plan template. Each agency is also expected to comply with the previously established dates.

5.2.2.1 Initiative 5: Streamline collection and sharing of digital identity data

The activity owners will support the transition activities, grouped below by owner, with milestone dates through October 2010, associated with streamlining the collection and sharing of digital identity data subject to all applicable privacy laws and regulations.

- Agencies. Implement government-wide digital identity data standard; inventory authoritative data sources; establish AAES of digital identity data; enable synchronization processes and technologies; transition transmission of biographic data and biometrics to electronic processes; minimize collection of biographic data and utilize AAES; eliminate paper processes; populate required identity data using authoritative repositories; incorporate first responder requirements with PIV systems and develop interface to the FEMA databases; and make fingerprint capture for BIs as part of PIV enrollment.
- Federation Interoperability Working Group (FIWG). Use BAE common data elements for sharing across departments to allow for real-time access decisions; determine mechanisms to share with appropriate agency partners; and establish business rules for sharing identity/access record data.

- ICAMSC. Evaluate a government-wide approach for creating and maintaining contractor and affiliate identity data.

5.2.2.2 Initiative 6: Fully leverage PIV and PIV-interoperable credentials

The activity owners will support the transition activities, grouped below by owner, with milestone dates beginning in January 2010 through June 2011, associated with fully leveraging existing PIV and PIV-interoperable credentials across agencies.

- Agencies. Begin enabling relevant applications to accept PIV cards from other Executive Branch agencies and PIV-interoperable cards; reduce or eliminate the creation and issuance of separate soft certificates; implement use of PIV credentials and eliminate separate usernames/passwords; employ standard lease agreements requiring the use of FIPS 201 or FIPS 201 interoperable credentials for unescorted physical access; standardize procurement language that requires LACS/PACS to support PIV cards; leverage the results from FIPS 199 assessments for PIV enablement; support the use of encryption, digital signature, and PKI authentication; expand the use of digital signatures; develop capability to recover data encrypted with expired/lost credentials; implement path discovery and validation products.
- RDT. Develop guidance for use of PIV credentials for authentication at all levels by internal users and requiring agencies to issue internal policy on the use of PIV.
- AWG. Establish the minimum certification process by which external organizations become trusted PIV-interoperable issuers.

5.2.2.3 Initiative 7: Modernize PACS infrastructure

Agencies will support the transition activities and milestone dates through March 2012 associated with the modernization of the PACS infrastructure based on SP 800-116, including Section 508 accessibility requirements. Specific activities include:

- Develop business case and funding request based on planned process and technology upgrades for electronic authentication of PIV cards and multi-factor authentication.
- Link individual PACS via a federated network for an agency-wide approach to managing physical access.
- Populate PACS user attributes and credential information from authoritative data sources.
- Determine which authentication mechanisms are required at each facility access point and develop interfaces to support PIV PKI certificate checks based on risk assessment.
- Leverage common Federal data standards such as UCore or National Information Exchange Model (NIEM) to increase interoperability.
- Upgrade technologies to support secure, automated processes for requesting and provisioning visitor access.
- Define and implement a process for supporting externally issued credentials, including PIV and PIV-II.

5.2.2.4 Initiative 8: Modernize LACS infrastructure

Agencies will support the transition activities and milestone dates through March 2012 associated with the modernization of agency LACS infrastructures.

- Link individual applications to a common agency-wide access management infrastructure.
- Upgrade the logical access infrastructure to allow for centralized provisioning and workflow management.
- Establish internal and external user provisioning workflow business rules.

- Develop business case and funding request based on upgrade needed for current provisioning/workflow management technologies.
- Tie all relevant applications/systems into the automated workflow; upgrade legacy systems.

5.2.2.5 Initiative 9: Implement federated identity capability

Agencies will support the transition activities and milestone dates through March 2012 associated with the implementation of federated identity capabilities.

- Issue agency-specific policy for externally-issued credentials that follow the trust framework processes established by the Federal CIO Council.
- Implement guidance on consuming external credentials and identity records.
- Reduce the creation/maintenance of passwords for external users by accepting externally issued credentials.
- Enable public-facing applications to accept third party credentials, as appropriate.
- Incorporate CVS functionality for checking adjudication of prior background investigations for an individual.

5.2.3 Implementation Sequencing Plan

The sequencing plan is part of the ICAM Transition Plan template and provides a cross-agency view of the activities needed to achieve the target architecture. A Microsoft Project template plan will be provided to each agency. Agencies will then create a detailed work breakdown structure (WBS) based on their existing ICAM implementation baselines and unique environment. Each plan will provide implementation deliverables; specific IT investment(s), system(s) and program(s) to support the activity; dependencies/constraints and completion dates to support performance measurement and accountability. Agencies should use this to forecast and request funding beginning with the FY2011 budget cycle.

5.3 Performance Metrics

The performance metrics provided in this section create a line of sight from IT investment performance to the ICAM strategic goals and objectives. The performance metrics, some newly created and others compiled from existing sources, will streamline agency tracking and reporting of their ICAM progress. Additional agency metrics may be included, but common metrics will allow ICAM governance entities to compare programs consistently across the Federal Government.

The performance metrics include an end state target that aligns with the ICAM segment architecture. Agencies will set their own targets for each fiscal year in collaboration with OMB and report their performance metrics in one of three reporting locations:

1. Exhibit 300: If an agency has existing or planned investments specific to ICAM. The inclusion should also be referenced in the ICAM Transition Plan.
2. Agency ICAM Transition Plan: The template will include annual metrics reporting along with agency-specific yearly targets. Absent ICAM capital investments, the Transition Plan should be used to report progress.
3. Data.gov: Four metrics have been identified for public reporting on Data.gov via agency websites.

The performance metrics includes 32 line items. Each line item details a strategic goal, objectives, measurement area, measurement category, measurement grouping, measurement indicator and target end state.

The “strategic goals” listed with each metric are related to individual specific goals set throughout the document such as reducing cost, increasing efficiency and improve security. The “objective” aligns each goal with the section of the document where it is discussed. Examples of the “measurement area” include customer results, mission or business results, and processes and activities. Examples of the "measurement category" include productivity, security and privacy, and administrative management. Examples of the "measurement grouping" include access, security management, delivery time and efficiency. The "measurement indicator" defines exactly what is being measured such as number of transactions, average time to complete a specific task or certain percentages. The "target end state" outlines the expected target to be met based on the measurement indicator.

PART B: Implementation Guidance

Part B of the FICAM document provides guidance to agencies for planning and implementing ICAM programs and initiatives outlined as part of the ICAM segment architecture. Part B will be completed as part of Phase 2 of the development effort beginning in September 2009.

6 ICAM Implementation Planning

This document summary does not summarize content from November 2009 FICAM document, Section 6, ICAM Implementation Planning, since guidance is still being developed.

7 ICAM Document Appendices[10]

This section lists the FICAM document appendices with selected content from the original document. The Smart Card Alliance encourages readers to review the original document for the full set of information.

7.1 Appendix A: Acronym List

Appendix A of the FICAM document includes 99 acronyms representing relevant terminology as they apply to identity, credential and access management. Below are selected acronyms from Appendix A:

AAES	Authoritative Attribute Exchange Service
ADS	Authoritative Data Source
ANSI	American National Standards Institute
AWG	Architecture Working Group
BAE	Backend Attribute Exchange
CA	Certificate Authority
CIO	Chief Information Officer
COFG	Citizen Outreach Focus Group
COMMON	Federal PKI Common Policy Framework
CSP	Credential Service Provider
CUI	Controlled Unclassified Information
CVS	Clearance Verification System
DBMS	Database Management System
EA	Enterprise Architecture
FASC-N	Federal Agency Smart Credential Number
FBCA	Federal Bridge Certification Authority
FEA	Federal Enterprise Architecture
FICAM	Federal Identity Credential and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FSAM	Federal Segment Architecture Methodology
G2B	Government-to-Business
G2C	Government-to-Citizen
G2G	Government-to-Government
IAM	Identity Access Management
ICAM	Identity, Credential & Access Management
ICAMSC	Identity, Credential & Access Management Subcommittee
IDMS	Identity Management System
IDP	Identity Provider
IEE	Internal Effectiveness & Efficiency
ISC	Interagency Security Committee
LACS	Logical Access Control System
NIEM	National Information Exchange Model
NPE	Non-Person Entity
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
PACS	Physical Access Control System
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RDT	Roadmap Development Team
SCA	Smart Card Alliance
SIA	Security Industry Association

[10] Summary of Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance, Appendix A-H, pages 169-207.

7.2 Appendix B: Glossary

Appendix B of the ICAM document includes sixty-three (63) Terms and Definitions. Below are selected glossary references from Appendix B.

Applicant. Individuals that request issuance of a credential or access to an application. An applicant becomes a credential holder after issuance and a user after being granted access to an application.

Authentication Credential, A type of authenticator possessed by a user that provides a strong mechanism used to prove the credential holder’s identity. Examples include a PKI certificate or a PIV card.

Authoritative Data Source. The repository or system that contains the data and attributes about an individual and that is considered to be the primary source for this information. If two systems with an individual's data have mismatched information, the authoritative data source is used as the most correct.

Biometrics. A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.

Card Management System, An application that manages the issuance and administration of multi-function enterprise access smart cards. The CMS manages cards, as well as data, applets and digital credentials, including PKI certificates related to the cards throughout their lifecycle.

Certificate Revocation List. A composite list of all expired and revoked certificates issued from a CA that can be used to verify the current status of a PKI certificate.

Core Identity Attributes. Attributes that are specific to an individual and, when aggregated, uniquely identify a user within and across agency systems. Core identity attributes are also the list of attributes that agencies must make available to one another to enable federation of identity records.

Digital Identity. The representation of identity in a digital environment.

E-Authentication Assurance Level (EAAL). Evaluation categories by which authentication mechanisms are measured based on SP 800-63. The lowest level assurance is 1; the highest assurance level is 4.

Non-Person Entity (NPE). Any type of non-human device (e.g., routers, servers, switches, firewalls, sensors) or software object

Privilege Manager. Individual or system that validates the individual's need for account access and provides the access request to the application administrator. The privilege manager can also provide a request to the application administrator to deactivate a user's need for account access.

Registration Authorities. An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of an authorized CA).

Relying Party. An entity that requests and/or receives information about the identity of an individual or authentication assertions from another party such as an IDP, CSP, or trusted broker. The requestor is referred to as a relying party, since the requestor relies upon information provided from an external source to authenticate an identity. When a relying party requests information about the validity of a user's identity, they receive an assertion based on the source, the time of creation, and attributes associated with the source. The relying party trusts the information provided to them about the user and makes access decisions based upon the IDP's or trusted broker's assertions.

Trusted Broker (TB). Entity that enables trust between IDPs and relying parties by passing authentication assertions from one to the other. Trusted brokers include parties also known as verifiers.

Verifying Party. The entity that supplies trusted assertions to a relying party confirming that a user was authenticated. The verifying party is also sometimes referred to as the responder or claimant.

7.3 Appendix C: Policy List

Appendix C of the FICAM document includes a policy list with links to documents from Joint Security & Suitability Reform Teams, OMB (memoranda), The Office of the President (Homeland Security Presidential Directives (HSPD)), DOJ, DHS, OPM, and ISA. Below are selected policies from Appendix C.

GROUP	DOCUMENT NAME	DESCRIPTION
Joint Security and Suitability Reform Team	Federal Investigative Standards	Provides standards to align suitability and national security investigations under consistent criteria. Applies to investigations performed in support of determinations of eligibility for access to classified information, eligibility to hold a sensitive position, suitability for government employment, and eligibility for physical and logical access.
OMB	M-04-04	Requires agencies to review new and existing electronic transactions to ensure authentication processes provide the appropriate level of assurance. Establishes four levels of identity assurance for electronic transactions requiring authentication. Agency business-process owners bear the primary responsibility to identify assurance levels and strategies for providing them. This responsibility extends to electronic authentication systems.
OMB	M-05-05	Requires the use of an SSP (Shared Service Provider) to mitigate the risk of commercial managed services for public key infrastructure (PKI) and electronic signatures.
OMB	M-05-24	Provides implementing instructions for HSPD-12 and FIPS 201.
OMB	M-06-18	Updates direction for acquiring products and services for the implementation of HSPD-12.
OMB	M-07-06	Discusses validation and monitoring agency issuance of PIV compliant identity credentials.
Presidential Directive	HSPD-12	Calls for a mandatory, government-wide standard for secure and reliable forms of ID issued by the Federal Government to federal employees and contractors for access to federally-controlled facilities and networks.
OPM	Final Credentialing Standards	*Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12,* provides final government-wide credentialing standards for use by all Federal departments and agencies in determining whether to issue or revoke PIV cards to their employees and contractor personnel, including non-United States citizens.
N/A	E-Government Act of 2002	Enhances the management and promotion of electronic government services and processes by establishing a Federal CIO within OMB, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to government information and services, and for other purposes.
N/A	Federal Information Security Management Act of 2002 (FISMA)	Requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
N/A	Executive Order 12977	Establishes the ISC to develop standards, policies and best practices for enhancing the quality and effectiveness of physical security in, and the protection of, non-military federal facilities in the United States.

7.4 Appendix D: Risk Registry

Appendix D identifies 22 risks categorized by cost, governance, performance, policy/guidance, privacy, security and technology.

H = High
M = Medium
L = Low

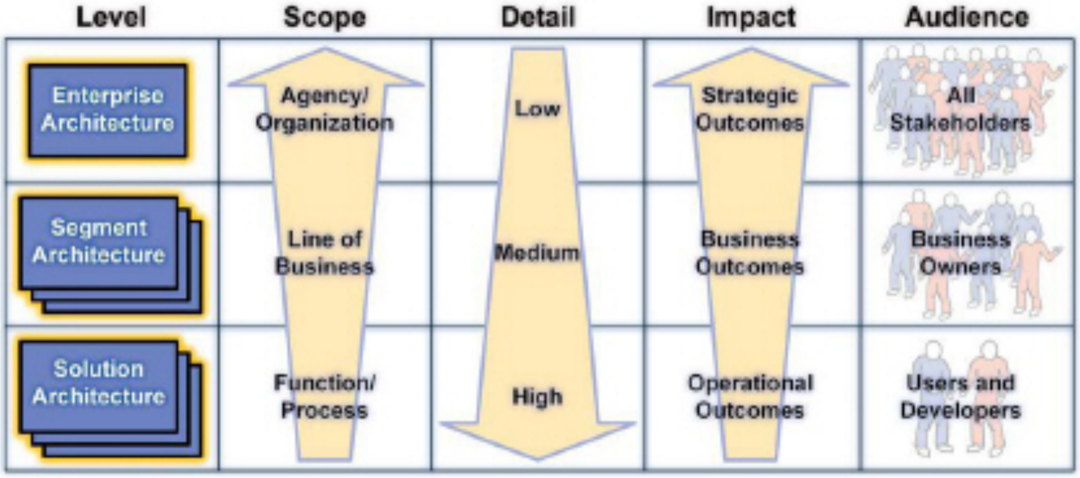
			Severity	Probability	Risk Score	
#	Risk Label	Risk Description	S	P	R	Mitigation Plan
Cost Risk						
1	Segment Cost Impacts	Agency plans and budgets may not include ICAM activities; as a result, adequate funding may not be available.	H	H	H	Transition plan with milestones and priorities to guide agency budget requests. Agencies must ensure (via adequate budget requests) sufficient resources are available for ICAM activities.
Governance Risk						
2	ICAM compliance and alignment	Agencies may resist compliance with ICAM segment architecture, perpetuating inefficiencies and threatening success of government-wide ICAM vision.	H	H	H	Incorporate security, efficiency and other objectives described in the ICAM segment architecture into planning and budgeting activities. To facilitate this OMB and GSA will continue outreach to agencies.
3	M 04-04/SP 800-63 Compliance	Trust for services across agencies may be undermined by lack of compliance and adoption of existing policies/standards.	H	M	H	Identify reasons for non-compliance. Seek executive buy-in. Incorporate requirements into FISMA/ATO processes and sign-off, and IG/GAO audit plans.
4	Role Authentication	Inability to authenticate user role could threaten success of G2B, where user identity is less important than role within a company (i.e., to commit firm).	L	H	M	Address government-wide approach through work of the ICAMSC. Additional guidance following development of government-wide approach.
5	PIV Traction	Agency adoption of PIV technology and PIV-enablement of applications has lagged and may continue to lag.	L	L	L	"PIV capable" requirement incorporated into investment approval and FISMA/ATO requirements. Conduct outreach to IG/GAO to help ensure audit plans incorporate requirements.
6	Organizational Trust	Consistent approach for negotiating organizational trust lags behind standards for trusted credentials and transaction-based identity authentication.	M	M	M	Additional guidance/use cases for establishing organizational trust relationships between service providers and consumers.
Performance Risk						
7	Citizen Outreach Traction	The Federal Government will not achieve effective service delivery and ROI on citizen outreach efforts unless offerings attract a sufficient number of users.	M	M	M	ICAM initiatives must include deliberate action to drive applications or credentials to critical mass. Select high value target applications within specific communities of interest to drive rapid adoption.
8	Performance Tracking	Without appropriate tracking and consequences, agencies may not meet performance metrics.	M	M	M	Implement controls to track performance.
Policy/Guidance Risk						
9	IDP Liability	Commercial entities may be unwilling to serve as an IDP to the government over liability concerns, threatening successful federation models.	M	M	M	Engage privacy community, DOJ, and industry groups to provide solutions that mitigate this risk.
10	Digital Sign-ature Traction	Agencies may resist adoption of digital signature applications based upon historical behavior.	L	L	L	Enhanced digital signature guidance.

#	Risk Label	Risk Description	S	P	R	Mitigation Plan
Privacy Risk						
11	Exposure of PII	Driving an increase in e-Government creates additional points of electronic exposure for personally identifiable information (PII), increasing risk of data compromise.	H	L	M	Augment SP 800-53 controls to adequately address ICAM data security. Incorporate FISMA controls into ICAM solution design in order to increase security and mitigate privacy risk.
12	Cross Agency Event Correlation	Perceived privacy concerns may delay solutions that allow correlation of citizen activities across agencies.	L	M	L	Avoid single centralized architectural components where possible, and easily traceable "trails" left behind by authentication solutions (e.g., SSNs). Incorporate privacy into solution level architecture.
Security Risk						
13	Claims Assurance	Poor authorization decisions may result if FICAM focus is limited to identity authentication without incorporation of claims like attributes, privileges, and roles.	M	H	H	New guidance around attribute authorities. Potential guidance on binding claims to identities. Incorporate claims delivery and trust into FICAM conceptual solution architecture.
14	Visual Authentication	Agencies continue to rely on visual PIV authentication for physical access, undermining enhanced security available and enabled by electronic authentication.	M	H	H	Implementation of the maturity model identified in SP 800-116 with oversight and tracking by agency IG.
Technology Risk						
15	Discovery of federal trust graph	As new mechanisms (e.g.,bridges, interfederation) are employed, it may become difficult to deterministically discover every IDP trusted (directly and indirectly).	M	H	H	Architectural solutions should address.
16	Non-PIV solution alignment	Related credentialing efforts (e.g., FRAC, TWIC, eHealth) may not align with PIV or Federal PKI, affecting credential interoperability and service delivery.	M	H	H	Engage stakeholders in collaboration and consolidation of ICAM initiatives to promote alignment of standards and technology.
17	Interoperable authentication components	Systems built independently by separate agencies may not be interoperable with all IDPs, which could delay or prevent large-scale adoption of government services.	M	M	M	Requires multi-tiered interoperability approach, including industry testing, deployment testing, scheme adoption lifecycle, and implementation guidance.
18	Digital identity schema incompatibility	Lack of digital identity standards and incompatibilities between existing schemas and products could prevent use of desired standards/products (e.g., SAML).	M	M	M	Define government-wide standards for identity data schemas. Coordinate with vendors through interoperability lab to find solutions.
19	Lack of approved technologies	Interoperability could be compromised if an approved set of technologies and vendors is not specified for technologies in new and rapidly evolving areas.	M	M	M	Coordinate existing approved products mechanisms (including SIN 132-6X) and procurement vehicles (schedules) across ICAM initiatives.
20	COTS PD-VAL	Support for Path Discovery and Validation (PD-Val) is not widespread, resulting in third party applications that don't work properly with government ID credentials.	L	H	M	Update Public Key Interoperability Test Suite (PKITS). Refresh PD-VAL testing. Education on PIV/PD-VAL connection. Publish vendor capabilities.
21	Product availability	Lack of alignment between government and other communities of interest could threaten necessary scale to drive industry solutions to meet service needs.	L	M	L	ICAM segment architecture transition plan should include approach to provide coordination with solution providers and other solution consumers.
22	Availability of alternate biometrics	Lack of common, standardized alternative biometrics could prevent interoperability for exceptional use cases across Agencies (primarily for PIV and PIV-I).	L	M	L	Additional guidance/standards regarding alternate biometrics pending. Identify authoritative source for government .

7.5 Appendix E: ICAM Segment Architecture Development Approach Details

Architectures within the FEA may be developed at the enterprise, segment, or solution level. Figure 6, provided in the FEA Practice Guidance document, depicts the hierarchical relationships between enterprise, segment, and solution architectures.

Figure 6. Architecture Relationships



Segment architecture defines a simple roadmap for a core mission area, business service, or enterprise service. ICAM is considered an enterprise service segment, but it supports and functions across mission areas. **Working groups** were developed to facilitate the effort over time: **Roadmap Development Team Lead, Roadmap Development Team, Lead Architect and Core Team.**

The Roadmap Development Team wanted to help clarify the following business questions:

- How should ICAM work with other initiatives to improve integrated identity management services to the Federal Government?
- How do we define the future state for ICAM? What should it include or exclude especially in the area of identity management?
- What is the best transition strategy to implement the desired ICAM future state and why? How can OMB and the agencies minimize cost and the time needed to complete the implementation?
- How can the agencies improve their ICAM-related planning to improve their compliance with OMB requirements?

The approach outlined in the FSAM was followed to create the ICAM segment. The FSAM is a five-step process that helps architects identify and validate the business need and scope of the architecture, define the performance improvement opportunities within the segment, and define the target business, data, services, and technology architecture layers required to achieve the performance improvement opportunities. The steps outlined in the FSAM are:

- **Step 1: Determine Participants and Launch the Project.**
- **Step 2: Define the Segment Scope and Strategic Intent.**
- **Step 3: Define Business and Information Requirements.**
- **Step 4: Define the Conceptual Solution Architecture.**
- **Step 5: Author the Modernization Blueprint.**

The ICAM document includes a figure (Figure 62: Tailored FSAM Outputs for the FICAM Segment) that details the activities that were performed and the outputs that were created for each process step during the development of the ICAM segment architecture.

7.6 Appendix F: ICAM Data Standards and Guidance

Group	Document Name
AWG	HSPD-12 Shared Component Infrastructure Interface Specification Common Elements
AWG	HSPD-12 Shared Component Infrastructure Metadata Management
AWG	Finalization Service Provider to System Infrastructure Provider Interface
AWG	System Infrastructure Provider and Production Service Provider Interface Specification
AWG	System infrastructure Provider to Federal PKI Shared Service Provider Interface Specification
NIST	SP 800-73
NIST	SP 800-73, Parts 1, 2, 3, and 4
NIST	SP 800-76
NIST	SP 800-87
NIST	SP 800-103
NIST	SP 800-104
NIST	SP 800-122
NIST	FIPS 199
NIST	FIPS 201-1
GSA	E-Authentication Federation Adopted
IAB	Technical Implementation Guidance Smart Card Enabled Physical Access Control Systems
UCore	UCore
NIEM	NIEM
NIST	ANSI/NIST-ITL 1-2000 and 2006
ISO/IEC	ISO/IEC 24727

7.7 Appendix G: ICAM Technical Standards and Guidance

Appendix G of the FICAM document provides references and links to technical standards and guidance documents from various groups and organizations including: ANSI, SIA (OSIPS family of documents), AWG, NIST, Federal CIO Council, GSA, FPKIA, FIPS 201 Evaluation Program, NIST/NSA and ISO.

7.8 Appendix H: Acknowledgements

The ICAM document was prepared by the Identity, Credential, and Access Management Subcommittee (ICAMSC) under the auspices of the CIO Council and at the request of the Federal Enterprise Architect. The ICAMSC **Core Architecture Team** members included: Tim Baldridge, National Aeronautics and Space Administration (NASA); Carol Bales, Executive Office of the President (EOP); Deb Gallagher, Lead Architect, Department of Homeland Security (DHS); Paul Grant, Department of Defense (DoD); William MacGregor, National Institute of Standards and Technology; James Smith, Government Printing Office (GPO); Judith Spencer, General Services Administration (GSA); Owen Unangst, Department of Agriculture; Jeremy Warren, Department of Justice, (DOJ). The **Roadmap Development Team** included Duane Blackburn, EOP; Ken Clark, Office of the Director of National Intelligence; Michael Cockrell, Treasury Department; Bill Erwin, GSA; Arthur Friedman, NSA; Steve Gregory, State Department; John Hannan, Government Printing Office; Johnna Hoban, DOJ; Bernard Holt, DHS; Corinne Irwin, NASA; Richard Lewis, Department of Labor; Ron Martin, Department of Health and Human Services; Brandi Meighan, DOJ. **Additional agency personnel and support staff and the members of the Interagency Security Committee (ISC)** reviewed and provided comments and include: Keith Minard, DoD; Rachel Murdock, GSA; Robert Myers, State Department; Kshemendra Paul, EOP; Tammy Paul, Office of Personnel, Management; Brant Petrick, GSA; Sheron Randolph, DoD; Gina Reyes, Treasury Department; Jonathan Rich, GSA; Judith Snoich, Department of the Interior; David Temoshok, GSA; George White, DOJ; David Wilson, Securities and Exchange Commission.

8 Publication Acknowledgements

This document summary was developed by the Smart Card Alliance Identity Council and Physical Access Council to highlight key concepts and to make it more accessible to its target audiences. In developing and publishing the summary, the Smart Card Alliance hopes to expand the audience reading the document and promote its concepts broadly through the identity, credential and access management industry. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Identity Council and Physical Access Council members for their contributions. Participants involved in the development of this summary included: AMAG Technology; Booz Allen Hamilton; Cogent Systems; Datawatch; Deloitte; Diebold; Gemalto; GSA; Hewlett Packard Enterprise Services; Hirsch Electronics; IBM; Identification Technology Partners; IDmachines; IQ Devices; Probaris; Roehr Consulting; SCM Microsystems; Shane-Gelling Company; TrustBearer; Tyco International; U.S. Department of Defense/Defense Manpower Data Center; U.S. Department of State; XTec, Inc.

Special thanks go to **Tony Damalas**, Diebold, who led the project, and to the following Identity Council and Physical Access Council members who led the development and review of the document summary:

- **Ben Black**, Deloitte
- **Tony Damalas**, Diebold
- **Lolie Kull**, HP Enterprise Services
- **LaChelle LeVan**, Probaris
- **Stafford Mahfouz**, Tyco International
- **Steve Rogers**, IQ Devices
- **Adam Shane**, AMAG Technology
- **Lars Suneborn**, Hirsch Electronics
- **Rick Uhrig**, XTec, Inc.
- **Rob Zivney**, Hirsch Electronics

Special thanks go to the following Council members who participated in reviewing and commenting on the document:

- **Reed Anderson**, DoD/ DMDC
- **Todd Arnold**, XTec, Inc.
- **Bill Boggess**, DoD/DMDC
- **Sal D'Agostino**, IDmachines
- **Mark Dale**, HP Enterprise Services
- **Marty Frary**, Consultant
- **Marlon Guarino**, DoD/DMDC
- **Walter Hamilton**, ID Technology Partners
- **Shelly Hartsook,** Deloitte
- **Daryl Hendricks**, GSA
- **Andy Jones**, XTec, Inc.
- **Brian Kelly**, TrustBearer
- **Russ Kent**, HP Enterprise Services
- **Gilles Lisimaque**, ID Technology Partners
- **John McKeon**, IBM
- **Cathy Medich**, Smart Card Alliance
- **Bob Merkert**, SCM Microsystems
- **Carey Miller**, Deloitte
- **Neville Pattinson**, Gemalto
- **Rod Pieper**, HP Enterprise Services
- **Kenny Reed**, Datawatch
- **Roger Roehr**, Roehr Consulting
- **Dale Shane**, Shane-Gelling Company
- **Mike Sulak**, Dept. of State
- **Andy Tarbox**, Booz Allen Hamilton
- **David Walker**, Cogent Systems

About the Smart Card Alliance Identity Council

The Smart Card Alliance Identity Council is focused on promoting the need for technologies and usage solutions regarding human identity information to address the challenges of securing identity information and reducing identity fraud and to help organizations realize the benefits that secure identity information delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.

About the Smart Card Alliance Physical Access Council

The Smart Card Alliance Physical Access Council is focused on accelerating widespread acceptance, use, and application of smart card technology for physical access control. The Council brings together leading users and technologists from both the public and private sectors in an open forum and works on activities that are important to the physical access industry and address key issues that end user organizations have in deploying new physical access system technology. The Physical Access Council includes participants from across the smart card and physical access control system industry, including end users; smart card chip, card, software, and reader vendors; physical access control system vendors; and integration service providers.

Trademark Notice

All registered trademarks, trademarks, or service marks are the property of their respective owners.
marks are the property of their respective owners.