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

Version 1.0

November 10, 2009

Powered by the Federal Chief Information Officers Council and the Federal Enterprise Architecture

This page is intentionally left blank.

Executive Summary

The Federal Government is operating in a constantly shifting threat environment – data breaches are all too common, identity theft is on the rise, and trust relationships are enforced in an inconsistent and hard-to understand manner. Identity management issues have been well-documented by the Government Accountability Office (GAO), National Science and Technology Council (NSTC), Office of Management and Budget (OMB), and as outlined in the new Cybersecurity Initiative, where the Administration has laid out clear goals to make government more accessible to the American public while supporting the privacy and security of information and transactions. In particular, the Open Government Initiative promotes transparent, collaborative and participatory government that fully engages the public – while protecting citizen privacy and ensuring the safekeeping of the data that is exchanged. To meet these goals, cybersecurity must be addressed in a comprehensive manner across the Federal enterprise. The resulting framework can be leveraged in other areas as well – promoting data security, privacy, and the high assurance authentication needed to support improvements in health care and immigration and to promote collaboration through secure information sharing and transparency in government.

The cybersecurity threat is compounded by the increasing need for improved physical security at federally owned and leased facilities and sites. Simultaneously, additional requirements are being identified to support electronic business at all levels of assurance with Federal business partners. Initiatives such as electronic health care records and transparency in government are increasing the need to authenticate the American public in order to enable access to federal websites and applications. Agencies themselves are experiencing a growing need to exchange information securely across network boundaries.

Agencies are working to address these challenges – Personal Identity Verification (PIV) cards are being issued in increasing numbers, the Federal Public Key Infrastructure (PKI) has connected agency and commercial PKIs via a trust framework, and working groups are tackling relevant questions in agency- and mission-specific situations.

It is with a holistic understanding of this environment that 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 name of the subcommittee is representative of a shift in thought as well. The intersection of digital identities (and associated attributes), credentials (including PKI, PIV, and other authentication tokens), and access control into one comprehensive management approach is made official along with the formalization of their interdependence.

This document was developed in support of the ICAM mission to provide a common segment architecture and implementation guidance for use by federal agencies as they continue to invest in ICAM programs. The President's FY2010 budget[1] 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." The budget further recognizes the

[1] http:/www.whitehouse.gov/omb/budget/

importance of the effort in promoting greater trust, 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."

Value Proposition

The purpose of this 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. The benefits associated with implementation of ICAM are summarized below:

- **Increased security,** which correlates directly to reduction in identity theft, data breaches, and trust violations. Specifically, ICAM closes security gaps in the areas of user identification and authentication, encryption of sensitive data, and logging and auditing.
- **Compliance** with laws, regulations, and standards as well as resolution of issues highlighted in GAO reports of agency progress.
- **Improved interoperability**, specifically between agencies using their PIV credentials along with other partners carrying PIV-interoperable[2] or third party credentials that meet the requirements of the federal trust framework. Additional benefits include minimizing the number of credentials requiring lifecycle management.
- **Enhanced customer service,** both within agencies and with their business partners and constituents. Facilitating secure, streamlined, and user-friendly transactions – including information sharing – translates directly into improved customer service scores, lower help desk costs, and increased consumer confidence in agency services.
- **Elimination of redundancy,** both through agency consolidation of processes and workflow and the provision of government-wide services to support ICAM processes. This results in extensibility of the IT enterprise and reduction in the overall cost of security infrastructure.
- **Increase in protection of personally identifiable information (PII)** by consolidating and securing identity data, which is accomplished by locating identity data, improving access controls, proliferating use of encryption, and automating provisioning processes.

These benefits combine to support an improvement in the cybersecurity posture across the Federal Government with 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. Leveraging the digital

[2] As defined in Personal Identity Verification Interoperability for Non-Federal Issuers, Federal CIO Council, May 2009. PIV-interoperable credentials are technically interoperable with PIV credentials and follow the minimum vetting requirements in NIST SP 800-63, "E-authentication Guidance." PIV-interoperable specifications do not apply to individuals for whom HSPD-12 policy is applicable per OMB M-05-24 (i.e. federal employees and contractors with long-term access to federal facilities and information systems).

infrastructure in a secure manner will enable the transformation of business processes, which is vital to the future economic growth of the United States.

This document presents the Federal Government with a common framework and implementation guidance needed to plan and execute ICAM programs. While progress has been made in recent years, this 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 presented in Chapter 5 outlines several new agency initiatives and numerous supporting activities that agencies must complete in order to align with the government-wide ICAM framework, which is critical to addressing the threats and challenges facing the Federal Government.

This page is intentionally left blank

Table of Contents

Executive Summary i
Table of Contents iv
List of Figures ix
1. Introduction 1
1.1. Background 1
1.2. Purpose 2
1.3. Scope 3
1.4. Document Overview 4
2. Overview of Identity, Credential, and Access Management 7
2.1. ICAM in the Federal Government 7
2.1.1. Identity Management 9
2.1.2. Credential Management 10
2.1.3. Access Management 12
2.1.4. ICAM Intersection 13
2.2. ICAM Goals and Objectives 14
2.2.1. Goal 1: Comply with Federal Laws, Regulations, Standards, and Governance Relevant to ICAM 14
2.2.2. Goal 2: Facilitate E-Government by Streamlining Access to Services 15
2.2.3. Goal 3: Improve Security Posture across the Federal Enterprise 16
2.2.4. Goal 4: Enable Trust and Interoperability 17
2.2.5. Goal 5: Reduce Costs and Increase Efficiency Associated with ICAM 18
2.3. ICAM Governance 19
2.3.1. Governing Authorities 19
2.3.2. Federal Policies and Key Initiatives Impacting ICAM Implementation 20
PART A: ICAM Segment Architecture 23
3. ICAM Segment Architecture 25
3.1. Developing the ICAM Segment 25
3.2. ICAM Architectural Layers 26
3.2.1. Performance Architecture 27
3.2.2. Business Architecture 28
3.2.3. Data Architecture 30
3.2.4. Service Architecture 32
3.2.5. Technical Architecture 36
4. ICAM Use Cases 45
4.1. Create and Maintain Digital Identity Record for Internal User 48
4.1.1. As-is Analysis 48
4.1.2. Target Analysis 51
4.1.3. Gaps 55
4.2. Create and Maintain Digital Identity Record for External User 57
4.2.1. As-is Analysis 57
4.2.2. Target Analysis 59
4.2.3. Gaps 62
4.3. Perform Background Investigation for Federal Applicant 63
4.3.1. As-is Analysis 64
4.3.2. Target Analysis 67

4.3.3. Gaps 70
4.4. Create, Issue, and Maintain PIV Card 72
4.4.1. As-is Analysis 72
4.4.2. Target Analysis 78
4.4.3. Gaps 82
4.5. Create, Issue, and Maintain PKI Credential 84
4.5.1. As-is Analysis 84
4.5.2. Target Analysis 89
4.5.3. Gaps 90
4.6. Create, Issue, and Maintain Password Token 91
4.6.1. As-is Analysis 91
4.6.2. Target Analysis 93
4.6.3. Gaps 95
4.7. Provision and Deprovision User Account for an Application 96
4.7.1. As-is Analysis 96
4.7.2. Target Analysis 98
4.7.3. Gaps 101
4.8. Grant Physical Access to Employee or Contractor 103
4.8.1. As-is Analysis 103
4.8.2. Target Analysis 105
4.8.3. Gaps 110
4.9. Grant Visitor or Local Access to Federally-Controlled Facility or Site 111
4.9.1. As-is Analysis 111
4.9.2. Target Analysis 114
4.9.3. Gaps 119
4.10. Grant Logical Access 120
4.10.1. As-is Analysis 120
4.10.2. Target Analysis 122
4.10.3. Gaps 126
4.11. Secure Document or Communication with PKI 128
4.11.1. As-is Analysis 128
4.11.2. Target Analysis 128
4.11.3. Gaps 131
4.12. Application of the ICAM Use Cases 132
4.12.1. IEE: User Management 132
4.12.2. G2G: Emergency Responders 134
4.12.3. G2B: Medical Information Exchange 136
4.12.4. G2C: Citizen Services 138
5. Transition Roadmap and Milestones 139
5.1. Performance Improvement Recommendations 139
5.2. Initiatives and Milestones 141
5.2.1. Government-wide Level Governance Initiatives 142
5.2.2. Agency-level Implementation Initiatives 145
5.2.3. Implementation Sequencing Plan 149
5.3. Performance Metrics 150
PART B: Implementation Guidance 157
6. ICAM Implementation Planning 159
6.1. Program Stakeholders 159
6.1.1. Collaboration and Stakeholder Management 159

6.1.2. ICAM Stakeholders 160
6.2. Risk Management 165
6.3. Capital Planning 165
6.3.1. Acquisition Resources 166
6.3.2. Accreditation 166
6.3.3. Enterprise Architecture 167
6.4. Security Considerations 167
6.5. Privacy Considerations 167
Appendix A Acronym List 169
Appendix B Glossary 171
Appendix C Policy List 177
Appendix D Risk Registry 181
Appendix E ICAM Segment Architecture Development Approach Details 189
Appendix F ICAM Data Standards and Guidance 193
Appendix G ICAM Technical Standards and Guidance 197
Appendix H Acknowledgements 207

This page is intentionally left blank

List of Figures

Figure 1: ICAM Conceptual Diagram 8
Figure 2: FSAM Asset Mapping to Roadmap and Implementation Plan Chapters 26
Figure 3: Segment Architecture Layers 27
Figure 4: ICAM Use Case Overview 30
Figure 5: Cross Government Repositories and Systems 32
Figure 6: Services Framework 33
Figure 7: Agency As-Is Conceptual Diagram 38
Figure 8: Federal PKI Architecture 39
Figure 9: HSPD-12 Conceptual Diagram 40
Figure 10: Agency Target Conceptual Diagram 41
Figure 11: Federal Enterprise Target Conceptual Diagram 42
Figure 12: Federal Enterprise Target Conceptual Diagram: Cross-Agency Access 43
Figure 13: Federal Enterprise Target Conceptual Diagram, Citizen Access 44
Figure 14: Use Case Functional Overview 46
Figure 15: Identity Record Creation by System and User Type 50
Figure 16: Use Case 1 As-is Architecture Details 51
Figure 17: Use Case 1 Target Process Diagram 54
Figure 18: Use Case 1 Target Architecture Details 55
Figure 19: Use Case 2 As-is Architecture Details 59
Figure 20: Use Case 2 Target Process Diagram 61
Figure 21: Use Case 2 Target Architecture Details 62
Figure 22: Use Case 3 As-is Architecture Details 67
Figure 23: Use Case 3 Target Process Diagram 69
Figure 24: Use Case 3 Target Architecture Details 70
Figure 25: Use Case 4 As-is Architecture Details 78
Figure 26: Use Case 4 Target Process Diagram 80
Figure 27: Use Case 4 Target Architecture Details 82
Figure 28: Mapping of PKI Credential and Identity Assurance Levels 84
Figure 29: Use Case 5 As-is Architecture Details 88
Figure 30: Use Case 5 Target Process Diagram 90
Figure 31: Use Case 6 As-is Architecture Details 93
Figure 32: Use Case 7 As-is Architecture Details 98
Figure 33: Use Case 7 Target Process Diagram 100
Figure 34: Use Case 7 Target Architecture Details 101
Figure 35: Use Case 8 As-is Architecture Details 105

Figure 36: PIV Authentication Mechanisms 106
Figure 37: Use Case 8 Target Process Diagram 108
Figure 38: Use Case 8 Target Architectural Analysis Details 109
Figure 39: Use Case 9 As-is Architectural Analysis Details 114
Figure 40: Use Case 9 Target Process Diagram 117
Figure 41: Use Case 9 Target Architectural Analysis Details 119
Figure 42: Use Case 10 As-is Architecture Details 122
Figure 43: Use Case 10 Target Process Diagram 125
Figure 44: Use Case 10 Target Architecture Details 126
Figure 45: Use Case 11 Target Process Diagram (Encryption) 130
Figure 46: Use Case 11 Target Process Diagram (Digital Signature) 130
Figure 47: Use Case 11 As-is Architecture Details 131
Figure 48: ICAM Performance Improvement Recommendation Summary 141
Figure 49: Initiative 1 Transition Activity Summary 143
Figure 50: Initiative 2 Transition Activity Summary 144
Figure 51: Initiative 3 Transition Activity Summary 144
Figure 52: Initiative 4 Transition Activity Summary 145
Figure 53: Initiative 5 Transition Activity Summary 147
Figure 54: Initiative 6 Transition Activity Summary 147
Figure 55: Initiative 7 Transition Activity Summary 148
Figure 56: Initiative 8 Transition Activity Summary 149
Figure 57: Initiative 9 Transition Activity Summary 149
Figure 58: ICAM Performance Metrics (* indicates inclusion in the Data.gov data stream) 155
Figure 59: ICAM Stakeholders 165
Figure 60: Levels of Architecture 189
Figure 61: FSAM Implementation Steps 191
Figure 62: Tailored FSAM Outputs for the Federal ICAM Segment 192

1. Introduction

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 communications infrastructure. The need for effective cybersecurity is at an all-time high, while recent cybersecurity reviews, including the Cyberspace Policy Review released by the White House in May of 2009,[3] have highlighted that the Federal Government must do more to address these threats. The Government Accountability Office (GAO)[4] recently found that most agencies have not implemented the necessary security controls to prevent and detect unauthorized access to federal IT networks, systems and data. Security weaknesses found included the areas of user identification and authentication, encryption of sensitive data, logging and auditing, and physical access.

Identity, Credential, and Access Management (ICAM) efforts within the Federal Government are a key enabler for addressing the nation's cybersecurity need. The Cyberspace Policy Review includes an entire section on the use of identity management in addressing cyber threats. The report includes a near-term action to develop "a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation." These recommendations provide a strong rationale and level of urgency for the implementation of this document.

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[5] has identified the need to develop a common framework that includes key practices for guiding agencies' physical security efforts, such as employing a risk management approach to facility protection, leveraging advanced technology (e.g., smart cards), improving information sharing and coordination, and implementing performance measurement and testing. In a subsequent report[6], GAO outlined the need for standard performance metrics to evaluate the effectiveness of physical security protections. Strong ICAM practices and the common framework outlined in this document will help address the persisting weaknesses within the Federal Government's physical security infrastructure.

In addition to complex cyber and physical security threats, the Federal Government faces significant challenges in being able to carry out its mission activities in a manner that fulfills the needs of its business partners and the American public and appropriately leverages current information technology capabilities to enable electronic service delivery. These challenges lie in being able to verify the identity of an individual or non-person entity (NPE) in the digital realm 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

[3] Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure, Executive Office of the President, May 29, 2009.

[4] GAO-09-701T, Agencies Make Progress in Implementation of Requirements, but Significant Weaknesses Persist, May 19, 2009.

[5] GAO-05-49, Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices, November 2004.

[6] GAO-06-612, Guidance and Standards Are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts, May 2006.

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 approach must also promulgate implementation guidance and best practices, build consensus through government-wide collaboration, and modernize business processes to reduce costs for agency administration.

Despite a complex set of challenges, the Federal Government has made progress regarding ICAM in recent years. The Homeland Security Presidential Directive 12 (HSPD-12) initiative provides a common, standardized identity credential that enables secure, interoperable online transactions. The Federal Public Key Infrastructure (PKI) program[7] has gained traction, furthering the trust framework for interoperable, high-assurance person entity or NPE identity authentication. Standards development has driven advances in physical security architectures and standards, moving forward the convergence of physical and logical security into a holistic security capability. Still, many gaps remain across ICAM programs in the Federal Government, and there is much work that is in progress or yet to be done. Additional focus around the areas of attribute and role management, authorization, and auditing capability will further build trust and security in online transactions while enhancing privacy.

The case for a common ICAM vision and framework is clear. The President's FY2010 budget[8] 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." The 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." This 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. Alignment with the ICAM segment and incorporation of the guidance and best practices laid out in this document are critical to addressing the threats and challenges facing the Federal Government.

1.2. Purpose

The purpose of this 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 a segment architecture for ICAM management programs. The Roadmap provides courses of action, planning considerations, and technical solution information across multiple federal programs spanning the disciplines of identity, credential, and access management.

This document will help the Federal enterprise leverage digital infrastructure to securely conduct business electronically between Federal agencies, their business and coalition partners and with the American public, by promoting the use of authentication, digital signature, and encryption technologies. The architecture, milestones and implementation approaches outlined here will be

[7] http://www.cio.gov/fpkia/

[8] http://www.whitehouse.gov/omb/budget/

leveraged by agencies across the government as they attain greater interoperability and increased security.

In support of the overall purpose, the Roadmap was written to accomplish the following objectives to:

- Provide background information on ICAM and educate the reader about key programs in each area and how they are interrelated;
- Present the business case for identity, credential, and access management programs through the identification of key business drivers and benefits;
- Illustrate the key players and compliance initiatives involved in ICAM programs;
- Give guidance on how to incorporate a segment architecture for ICAM programs;
- Provide a high-level vision for the target state of the federal enterprise's use and management of ICAM systems, technologies, data, and services;
- Establish milestones and timelines within the target state to support agency transition activities;
- Enumerate and provide references to technical standards that are applicable to identity, credential, and access management programs;
- Increase the pursuit of technological interoperability and reuse across the government;
- Identify cost savings to be gained through a carefully planned and well-executed implementation plan; and
- Illustrate tested and proven implementation approaches through the incorporation of case studies and lessons learned.

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. While the document serves to outline a common framework for ICAM in the Federal Government, it is understood that agencies are at different stages in the implementation of their ICAM architectures and programs. As a result, they will need to approach alignment with ICAM from varying perspectives.

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[9] and direction for the implementation of ICAM programs in accordance with the architecture. Given the continual change of the ICAM landscape, the FICAM Roadmap and Implementation Guidance is structured to accommodate future topics that are not included in the current scope. The FICAM Roadmap and Implementation Guidance is intended as a resource for agency implementers of identity, credential, and access management programs. In the event that this document contradicts established Federal Government policies and standards, those documents take precedence.

[9] Scheduled for inclusion in the next iteration and release of this document.

The Roadmap addresses unclassified[10] federal identity, credential, and access management programs and how the Executive Branch of the Federal Government will interact with external organizations and individuals. The scope of the document has been limited to ICAM programs that apply within and across the agencies in a variety of environments and configurations. This includes those associated with emerging IT advancements such as cloud computing, identity-as-a-service, and software-as-a-service. Using PIV certificates provides several benefits (strong authentication, standardized processes, digital signatures) and approved credentials must be supported by all applicable Federally procured services. It is anticipated that tailoring ICAM functionality to meet the unique mission requirements for particular programs that do not include access to federal IT systems or facilities will require additional collaboration and work outside the scope of this document and the common ICAM initiative within the Federal Government.

The document addresses the intersection of the Federal Government with external entities from the perspective of the Federal Government as a relying party of ICAM services and, to some extent, as an issuer of credentials. 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.

In order to achieve broad applicability, the scope of the Roadmap is limited to general guidance and considerations. Specific details related to program implementation are discussed only in the form of lessons learned and case studies highlighting programs at select government agencies. The agencies featured in the case studies provide representative examples of the challenges and successes from which the reader can learn.

1.4. Document Overview

The remaining chapters of this document are organized as follows:

- **Chapter 2: Overview of Identity, Credential, and Access Management.** Provides an overview of Identity, Credential, and Access Management that includes a discussion of the business and regulatory reasons for agencies to implement ICAM initiatives within their organization.
- **PART A: ICAM Segment Architecture**
  - **Chapter 3: ICAM Segment Architecture.** Presents the methodology used to create the government-wide ICAM segment architecture and the key architectural outputs at each layer of the architecture.
  - **Chapter 4: ICAM Use Cases.** Use cases are incorporated into the document to illustrate the as-is and target states of high-level ICAM functions that are performed by agencies. Additionally a gap analysis between the as-is and target states allows for the development of a transition roadmap and milestones.
  - **Chapter 5: Transition Roadmap and Milestones.** The transition roadmap and milestones section defines a series of logical steps or phases that enable the implementation of the target architecture.

[10] National security systems are not covered by this document, but unclassified systems within Defense and Intelligence agencies are.

- **PART B: Implementation Guidance**
  - **Chapter 6: ICAM Implementation Planning.** Augments standard life cycle methodologies as they relate to specific planning considerations common across ICAM programs. Relevant lessons learned and anecdotes are incorporated throughout. The intent behind this section is to discuss how agencies can align their ICAM program strategies to realize synergies and avoid common management pitfalls that tend to disrupt ICAM projects.
  - **Chapters 7-12: Implementation Guidance.** Provides guidance to agencies on how to implement the transition roadmap initiatives identified in the segment architecture. The section includes a wide range of guidance that is either currently lacking or is newly required as a result of changes outlined in the target ICAM architecture. Specific sections and topics in the phase are to include:
    - Identity Proofing and Background Investigations
    - Authoritative Identity Data
    - PKI Credentials
    - Other Credential Types and Interoperability
    - Physical Access
    - Logical Access
    - Privacy and Security
    - Federation and Information Sharing

The FICAM Roadmap and Implementation Guidance document is being developed in two phases. The first phase, completed between February and September 2009 and represented in this version of the document, focused on the development of the common, government-wide ICAM segment architecture. Phase 2, begun in September 2009, builds on Phase 1 and includes the documentation of ICAM best practices and implementation guidance.

This page is intentionally left blank.

2. Overview of Identity, Credential, and Access Management

This section provides an introduction to Identity, Credential, and Access Management (ICAM). The primary compliance drivers relative to ICAM have historically been the Electronic Authentication[11] (E-Authentication) policy framework and two of its enablers, namely the HSPD-12 and Federal PKI initiatives. 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. Understanding ICAM in its entirety and the ways in which it can be leveraged across an enterprise are fundamental to meeting the requirement for the rapid, electronic authentication of individuals, providing the base elements to allow for secure electronic transactions at varying assurance levels; and establishing trust for multiple purposes and multi-layered security.

The E-Authentication policy framework, the Personal Identity Verification (PIV) initiative, and the Federal PKI program are called out by name in this section and throughout the document because they are key ICAM initiatives that cut across all federal agencies. Another challenge common to many agencies is addressing the Federal Government's need to conduct electronic business with the American public using strong authentication mechanisms. As noted in Section 1.3 Scope, the Roadmap discusses ICAM programs common to all agencies within the Federal Government. While other programs specific to a particular agency or mission area are not singled out or discussed at length within the document, it is envisioned that 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 NPEs, bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions, and leverage the credentials to provide authorized access to an agency's resources. ICAM cuts across numerous offices, programs, and systems within an agency's enterprise, which are typically directed and managed separately. As a result, many of the aspects of ICAM within the Federal Government have traditionally been managed within individual stove-pipes. The following figure 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.

[11] References to E-Authentication in this document primarily refer to the federal E-Authentication policy framework, not the E-Authentication E-Government Initiative which began restructuring in 2007. Activities previously addressed as part of the E-authentication Initiative, which was led by the GSA Federal Acquisition Service, are now being addressed by the GSA Office of Government-wide Policy and Federal CIO Council as part of the ISIMC activities.

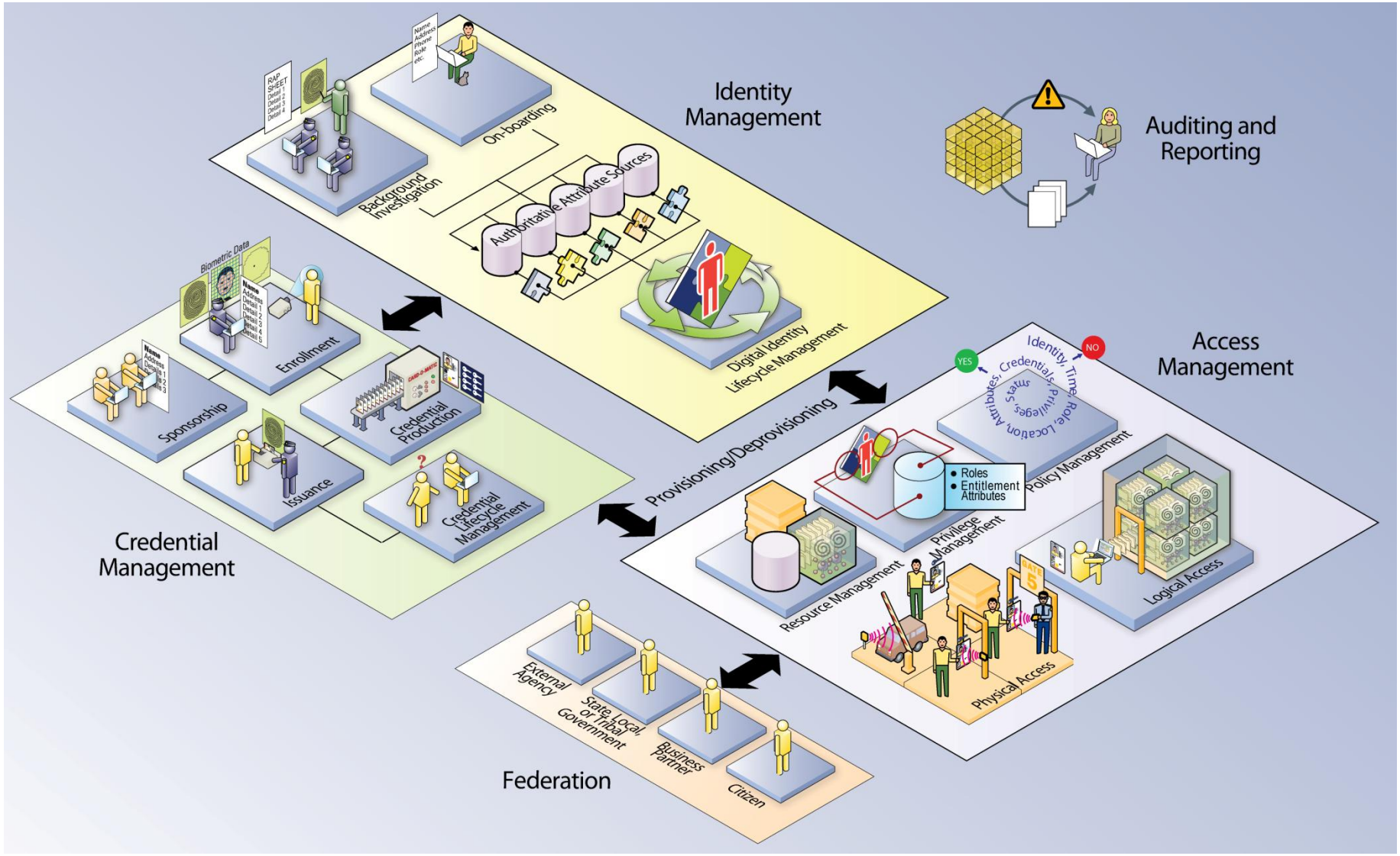

Figure 1: ICAM Conceptual Diagram

This high-level view of ICAM depicts the interdependencies between each area, which are combined to create an enterprise solution. The activities performed in one area are leveraged and built upon in the others. For example, the processes developed and implemented for on-boarding and background investigations can be leveraged to establish authoritative data for the creation of a digital identity. The authoritative data, once collected, may be used to populate an enrollment package to generate a credential. The digital identity can also be associated with a credential for enabling various levels of identity authentication as the basis for authorizing access to applications and facilities. Lifecycle management of the digital identity and its related credentials happens outside of those access processes and solutions but helps facilitate a strong level of trust in the enterprise identity when making access control decisions.

Behind the technology and the solutions that are deployed is 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 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

The NSTC Subcommittee on Biometrics and Identity Management defines identity management 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.[12] Identity management includes the processes for maintaining and protecting the identity data of an individual over its lifecycle. Additionally, many of the processes and technologies used to manage a person's identity may also be applied to NPEs to further security goals within the enterprise.

Today, many application owners and program managers create a digital representation of an identity in order to enable application-specific processes, such as provisioning access privileges. As a result, maintenance and protection of the identity itself is treated as secondary to the mission associated with the application itself. This 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. Unlike accounts to logon to networks, systems or applications, enterprise identity records are not tied to job title, job duties, location, or whether access is needed to a specific system. Those things may become attributes tied to an enterprise identity record, and may also become part of what uniquely identifies an individual in a specific application. Access

[12] Identity Management Task Force Report, National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management, 2008.

control decisions will be based on the context and relevant attributes of a user—not solely their identity. The concept of an enterprise identity is that individuals will have a digital representation of themselves which can be leveraged across departments and agencies for multiple purposes, including access control.

As shown in Figure 1, establishment of a digital identity typically begins with collecting identity data as part of an on-boarding process. A digital identity is typically comprised of a set of attributes that when aggregated uniquely identify a user within a system or enterprise (this concept is further discussed in Section 4.1.1). In order to establish trust in the individual represented by a digital identity, an agency may also conduct a background investigation. Attributes about an individual may be stored in various authoritative sources within an agency and linked to form an enterprise view of the digital identity. This digital identity may then be provisioned into applications in order to support physical and logical access (part of Access Management, discussed in Section 2.1.3) and deprovisioned when access is no longer required. While the term "on-boarding" and the background investigation process outlined in Section 4.3 are internal to the Federal Government, similar processes may also be applied to external entities for which an agency manages identity data, although they are typically less stringent and vary depending on the usage scenario.

With the establishment of an enterprise identity, it is important that policies and processes are developed to manage the lifecycle of each identity. Management of an identity includes:

- The framework and schema for establishing a unique digital identity,
- The ways in which identity data will be used,
- The protection of Personally Identifiable Information (PII),
- Controlling access to identity data,
- The policies and processes for management of identity data,
- Developing a process for remediation; solving issues or defects,
- The capability to share authoritative identity data with applications that leverage it,
- The revocation of an enterprise identity, and
- The system that provides the services and capabilities to manage identity.

As part of the framework for establishing a digital identity, proper diligence should be employed to limit data stored in each system to the minimum set of attributes required to define the unique digital identity and still meet the requirements of integrated systems. A balance is needed between information stored in systems, information made available to internal and external systems, and the privacy of individuals.

2.1.2. Credential Management

According to National Institute of Standards and Technology Special Publication 800-63 (NIST SP 800-63),[13] a credential is, "an object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person." [14] Credential management supports the lifecycle of the credential itself. In the Federal Government, examples of credentials

[13] NIST SP 800-63, Version 1.0.2, Electronic Authentication Guideline, April 2006.

[14] The credentialing process principals and elements can also be applied for NPE digital identities; however, steps may vary during the credential issuance process (sponsorship, adjudication, etc.) based on an organizations security requirements. For examples of an NPE credential issuance please refer to the X.509 Certificate Policy for the E-Governance Certification Authorities.

are smart cards, private/public cryptographic keys, and digital certificates. 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 [Federal Information Processing Standards 201 (FIPS 201), SP 800-73, etc.] 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. First, an authorized individual sponsors an individual or entity for a credential to establish the need for the credential. Then an individual enrolls for the credential, a process which typically consists of identity proofing and the capture of biographic and biometric data.[15] The types of data required may depend on the credential type and the usage scenario. Additionally, this step may be automatically fed based on authoritative attribute data collected and maintained through identity management processes and systems, since enrollment for a credential requires much of the same data collection that is required as part of Identity Management. Subsequently, a credential must be produced and issued to an individual or NPE. As in the case of enrollment, these processes will vary based upon the credential type in question. Figure 1 depicts graphical elements commonly associated with PIV and PKI credentialing, considered some of the most involved credentialing processes. Identity proofing, production, and issuance requirements for other credential types typically include a subset of the processes or technologies depicted but follow the same general principles. Finally, a credential must be maintained over its lifecycle, which might include revocation, reissuance/replacement, re-enrollment, expiration, 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. Credentials however are usually valid for a pre-defined period of time. An example would be digital certificates which are issued to an individual and expire based on the Issuer's PKI Common Policy. While the identity of an individual does not change, the certificates associated with that individual can be revoked and new ones issued. This does not have a bearing on the identity of an individual as credentials are a tool for authentication that provide varying levels of assurance about the authentication of an individual.

Another key aspect of credential management is the security and protection of credentials, from the issuance to use of credentials. The trust in a credential is dependent on a multi-layered approach to security which protects the credential from attack as well as who can use the credential. ICAM hinges on the level of trust in a credential and the uniformity of security and integrity across the security architecture to retain that trust throughout the use of the credential.

The specific process steps and architectural analysis associated with several common credential types within the Federal Government are depicted in Use Cases 4, 5, and 6 in Chapter 4.

[15] This step typically does not apply to NPEs.

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 the proper identity verification is made when an individual attempts to access security sensitive buildings, computer systems, or data.[16] It has two areas of operations: logical and physical access. Logical access is the access to an IT network, system, service, or application. Physical access is the 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 as to whether he/she is authorized to access the resource can be made. These processes allow agencies to obtain a level of assurance in the identity of the individual attempting access to meet the following:

1. Ensure that all individuals attempting access are properly validated (Authentication)
2. Ensure that all access to information is authorized (Confidentiality)
3. Protect information from unauthorized creation, modification, or deletion (Integrity)
4. Ensure that authorized parties are able to access needed information (Reliability, Maintainability, and Availability)
5. Ensure the accountability of parties when gaining access and performing actions (Non-repudiation)

In addition, access control sets the stage for additional activities outside of the traditional access control paradigm. One corollary to access management is the ability to ensure that all individuals attempting access have a genuine need. This is tied to authentication and authorization, but also to the business rules surrounding the data itself. Privacy is provided by properly ensuring confidentiality and by refraining from collecting more information than that which is necessary.

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 (such as rules for access, credential requirements, etc.) for a resource/asset that may be accessed. This provides rules for the object of an access transaction.
- Privilege Management - Processes for establishing and maintaining the entitlement or privilege attributes that comprise an individual's access profile. This provides rules for the subject of an access transaction. Privileges are considered attributes that can be linked to a digital identity.
- 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 or unallowable in an access transaction.

Typically, a series of workflows[17] also supports making the decision to grant/deny access to individuals. Common factors include:

[16] FIPS-201-1. Introduction, Pg. 1.
[17] "Workflows" as described in this document are not designed to be prescriptive. Agencies should evaluate and select the most efficient means that will meet security and business needs, whether or not it matches what the agency traditionally considers a "workflow."

- Assurance level
- Authorization to access resource
- Security policies
- Trust across physical or logical boundaries
- Validation of credentials
- Properties of the resource being accessed

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 and physical access are often viewed as the most significant parts of ICAM from a return on investment perspective. To maximize that return, a successful access management solution is dependent on identity, credentials, and attributes for making informed access control decisions, preferably through automated mechanisms. Infrastructure level investments must allow for the construction and development of all the foundational elements from which return on investment (ROI) is derived. Lack of this proper foundation will risk the resulting trust models, security services, and envisioned value and need intended from an IAM initiative.

2.1.4. ICAM Intersection

Understanding that ICAM programs have many areas of overlap is crucial to the overall success of these programs. There are many common elements associated with each of the areas addressed in the previous sections, 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. In fact, 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 a credential, user accounts, and access privileges. (While access can be granted based on provisioned identifiers, roles, other attributes or policy based decisions based on several contextual data points, the access decision must correspond to the correct digital identity.) As the necessity to complete transactions across networks with higher levels of assurance increases, so too does the need for the identity to be tied strongly and simultaneously to its high assurance credential, authoritative attributes, and access privileges. These overlaps demonstrate the intersection of identity, credential, and access management.

Due to the size and complexity of the programs and functions related to ICAM, the following challenges have emerged to the adoption of a consistent approach to ICAM implementation, including:

- Lack of standardized terminology. The traditionally stove-piped nature of ICAM initiatives has driven community-specific definitions.
- Pressure to decrease redundant processes, data stores, and IT investments while increasing efficiency.
- Demand associated with quickly increasing the return on investment associated with any ICAM infrastructure investment.
- Dependency on other organizations to adopt enabling technologies and processes that would enable secure cross-use of credentials and identity data.

- Need to establish impromptu areas that securely manage accurate identification and access control in order to accommodate emergency response scenarios.
- Differing levels of maturity for policies, processes, and technologies across departments and agencies who share common business needs.
- Differing levels of operational execution. The goals and priorities of each agency vary and therefore affect the rigor in which ICAM goals are addressed.

The first step to addressing these challenges is to view ICAM holistically instead of viewing it as separate disciplines. The same is true of the existing stove-piped programs across the Federal Government that have been implemented to address separate, but related initiatives. This document promotes a comprehensive, coordinated approach to ICAM initiatives related to help resolve the significant IT, security, and privacy challenges facing the Federal Government. When properly aligned, ICAM creates a basis for trust in securely enabling electronic transactions, which should include secure access to facilities and installations.

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 with many other IT, security, and information sharing endeavors. Some of the most relevant of these including privacy impacts of the ICAM segment architecture, implementation considerations for network and device authentication, and ICAM as a component of information sharing will be discussed more in depth in Part B of this document. However, many of these overlapping and dependent disciplines are too broad and far-reaching to be covered in this document. 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 goals and objectives in this section were created as part of the ICAM segment architecture development effort (described in full in Chapter 4). While they primarily focus on the role of the Federal Government in achieving the ICAM end-state, other key stakeholders have a crucial role in enabling interoperability and trust across the ICAM landscape to accomplish secure information sharing outside of the Federal Government boundaries. These stakeholders, who are mentioned throughout this document, include external business and commercial entities wishing to conduct business with the Federal Government; the health IT community as it increases its reliance on ICAM activities in order to facilitate the use of e-health records; Federal/Emergency Response Official (F/ERO) – emergency preparedness; and state, local, and tribal governments that require information exchanges to meet mission needs.

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

This goal includes aligning and coordinating operations and policies to meet the laws, regulations, standards, and other guidance in forming ICAM systems; aligning federal agencies around common ICAM practices; and where necessary, reviewing and aligning policies to ensure consistency.

2.2.1.1. Objective 1.1: Align and Coordinate Federal Policies and Key Initiatives Impacting ICAM Implementation

For the past several years there have been many inter-related but distinct initiatives in government supporting aspects of ICAM oversight and governance. In addition, programs within other communities of interest have begun identifying their own identity, credential, and access management requirements, needs and procedures.

A key objective of the ICAM segment architecture is to implement a holistic approach for government-wide identity, credential and access management initiatives that support access to federal IT systems and facilities. By the end of FY 2012, it is intended that Federal Executive agencies will implement a coordinated approach to ICAM across E-Government interactions [Government-to-Government, Government-to-Business, Government-to-Citizen, and Internal Effectiveness and Efficiency (IEE)] at all levels of assurance as defined in OMB M-04-04.

The ICAM segment architecture also provides a framework that may be leveraged by other identity management architectural activities within specific communities of interest. The aim is a standards-based approach for all government-wide identity, credential and access management to ensure alignment, clarity, and interoperability.

2.2.1.2. Objective 1.2: Establish and Enforce Accountability for ICAM Implementation to Governance Bodies

Necessary authority must be given to and exercised by the ICAM governance authorities (outlined in Section 2.3.1) to ensure accountability across the Federal Government in meeting its ICAM vision. In addition to developing comprehensive guidance and standards in support of the ICAM segment architecture, the governance bodies must establish and track specific performance metrics. Each agency shares the responsibility for establishing the trust and interoperability processes necessary to achieve the ICAM vision / end state and may be asked to report status against performance metrics publicly.

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

Strong and reliable identity, credential, and access management is a key component of successful E-Government implementation. When enabling electronic government, programs share sensitive information within government, between the government and private industry or individuals, and among governments using network resources and the World Wide Web. Further, this move towards enabling E-Government must be achieved in a flexible, cost-effective manner through collaboration among the public, industry, academia, and the government; and a corresponding policy and management structure must support the implementation of the solution.

2.2.2.1. Objective 2.1: Expand Secure Electronic Access to Government Data and Systems

To align with the ICAM segment architecture, federal agencies should design, build, and deploy ICAM solutions to support a broad range of electronic government use cases which will support their mission areas across Government-to-Government (G2G), Government-to-Business (G2B), and Government-to-Citizen (G2C) interactions. Federal organizations will cooperate across agency boundaries in service delivery to give citizens, businesses, and other governments increased electronic accessibility to Federal Government services through a wide choice of

access mechanisms. The implementation of ICAM initiatives will facilitate the creation of government services that are more accessible, efficient, and easy to use.

2.2.2.2. Objective 2.2: Promote Public Confidence through Transparent ICAM Practices

Public confidence in the security of the government's electronic information and information technology is essential to adoption and use of E-Government services. The Federal Government must build a robust framework of policies and procedures committed to respecting and protecting the privacy of users in order to enable the trust required to move Government transactions online.

2.2.3. Goal 3: Improve Security Posture across the Federal Enterprise

ICAM capabilities play a key role in enhancing the ability to prevent unauthorized access to Federal Government systems, resources, information, and facilities. As a function of logical security, ICAM can help protect information's confidentiality, assure that the information is not altered in an unauthorized way, and ensure information is released only to those entities authorized to receive it. ICAM will support and augment existing security controls as specified by the Federal Information Security Management Act and supporting NIST Special Publications 800-53 and 800-37, by promoting the use of strong identity solutions appropriate to the environment. ICAM further supports the policy and guidance established by the ISC for physical security. A focus on ICAM outcomes—who has access to data and resources, what information is collected—can help improve security posture beyond what controls are in place to meet mandates.

2.2.3.1. Objective 3.1: Enable Cybersecurity Programs

ICAM is a critical piece in protecting information and achieving cybersecurity goals. As a rising priority, cybersecurity will continue to grow and change within the Federal Government. Collaboration and coordination between ICAM and cybersecurity governance is a critical success factor in meeting the objectives of both programs. Moreover, the White House Cyberspace Policy Review states that one of the near term actions would be to "build a cybersecurity-based identity management vision and strategy."

2.2.3.2. Objective 3.2: Integrate Electronic Verification Procedures with Physical Security Systems

The Federal Government has a framework[18] and use cases for the use of strong, electronic authentication mechanisms to support physical access. The next step is for agencies to establish the need for electronic physical security systems and adopt and implement the appropriate policies and technologies to support physical access control leveraging electronic authentication.

[18] NIST SP 800-116

2.2.3.3. Objective 3.3: Drive the Use of a Common Risk Management Framework for Access Control Mechanisms

Existing authentication guidance and best practices for both logical and physical access dictate the use of a common risk management approach in determining the appropriate credential types and access control mechanisms. The Federal Government will work to drive the adoption and use of these approaches to ensure access controls are compliant with security requirements and risk-based analyses.

2.2.3.4. Objective 3.4: Improve Electronic Audit Capabilities

Solutions adopted as part of federal ICAM initiatives will provide robust auditing capabilities to support accountability, provide discrete non-repudiation, and enhance transparency in security effectiveness.

2.2.4. Goal 4: Enable Trust and Interoperability

The Federal Government stands to gain great value and enhanced service delivery by developing a foundation of inter-organizational trust and interoperability across the federal enterprise. Strong, interoperable federal identity credentials are key to streamlining and automating building access, temporary access requests, and other access and authorization within government. The Federal Government must tackle the governance and technical challenges posed by the abundance, variety, and complexity of ICAM-related programs in order to promote trust and interoperability and enable service delivery and information sharing across all partners.

2.2.4.1. Objective 4.1: Support Information Sharing Environment (ISE) Communities of Interest

Federal Government operations rely on collaboration and knowledge sharing with other communities (to include Intelligence, Health IT, state/local/tribal governments, industry, allies and coalition partners, and foreign governments) in order to conduct business. This information sharing demands trust among the various players and an ICAM capability which supports this scope of interoperation. Future federation solutions must acknowledge and account for the need to support interoperable access to systems and data to support information sharing while maintaining control of the allowed access and appropriate information protections. A federal ICAM segment architecture addresses the concept of federated information flow, which requires two or more federated enterprises to support transactions across common interfaces.

2.2.4.2. Objective 4.2: Align Processes with External Partners

The ICAM segment architecture supports a consistent approach for all government-wide identity, credential and access management processes to ensure alignment, transparency, and interoperability. This allows the Federal Government a means to do business with organizations such as banks and health organizations and support G2B transactions by enabling common standards and leveraging an existing federal infrastructure. The Federal Government will respect the different requirements of federal agency partners as to risk, assurance, and mission, and provide solutions that meet those needs and maintain inter-organizational interoperability.

2.2.4.3. Objective 4.3: Establish and Maintain Secure Trust Relationships

Establishing compatible identity, credential and access management policies and approaches and a framework for evaluating partners against these policies is a critical success factor in building trust relationships across the health care, government, commercial, and federal enterprises. The Federal Government will identify and leverage existing trust relationships and continue working to build new trust relationships within the government enterprise and between the Government and its partners (other governments, businesses, the health care community, and the American public) in order to move transactions online.

2.2.4.4. Objective 4.4: Leverage Standards and Commercial Off-the-Shelf Technologies for ICAM Services

The Federal Government will use commercial off the shelf (COTS) products and services, whenever possible, in order to enhance interoperability, spur technological innovation and promote availability of ICAM systems and components. The Federal Government will continue to work with the industry to drive the development and use of standards and product enhancements that meet the requirements of the federal enterprise.

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

One of the major goals of this effort is to allow agencies to create (and maintain) information systems that deliver more convenience, appropriate security, and privacy protection more effectively and at a lower cost. Establishing a clear vision is the first step in supporting these goals. Below are some specific benefits that may be realized from implementing this vision.

2.2.5.1. Objective 5.1: Reduce Administrative Burden Associated with Performing ICAM Tasks

Current ICAM efforts still rely on numerous manual, paper-based processes. Through automation and streamlining processes, the Federal Government stands to significantly reduce the administrative burden and cost associated with the various ICAM tasks. For instance, the legacy practice of manually administering user accounts/privileges on a system-by-system, user-by-user basis creates a great administrative burden.

2.2.5.2. Objective 5.2: Align Existing and Reduce Redundant ICAM Programs

A key objective of the ICAM segment architecture is to reduce or eliminate duplicative efforts and stove-piped programs and systems related to identity vetting, credentialing, and access control. Future ICAM solutions will leverage the existing investments of the Federal Government and provide a more efficient use of tax dollars when designing, deploying and operating ICAM systems.

2.2.5.3. Objective 5.3: Increase Interoperability and Reuse of ICAM Programs and Systems

Implementation of the ICAM segment architecture is intended to unify existing ICAM programs and initiatives, as well as agency-specific ICAM activities, under a common governance framework, recognizing the unique role of each program in the overall structure while eliminating redundancies and increasing interoperability between solutions.

2.3. ICAM Governance

This section identifies the key players and compliance initiatives driving ICAM programs within the Federal Government.

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 OMB. The ICAMSC is a subcommittee of the Information Security and Identity Management Committee (ISIMC), which was chartered in December 2008 as the principal interagency forum for identifying high priority security and identity management initiatives and developing recommendations for policies, procedures, and standards to address those initiatives that enhance the security posture and protection afforded to Federal Government networks, information, and information systems. In addition to the ICAMSC, the ISIMC includes three other subcommittees, which are focused on related security areas. They are:

- Security Program Management Sub Committee (SPMSC), which coordinates with other standing cross agency efforts and advises on FISMA reporting tools and security policy
- Security Acquisitions Sub Committee (SASC), which recommends Security Contract Language changes and reviews Supply Chain Activities
- Network and Infrastructure Security Sub Committee (NISSC), which coordinates with CIO Council Architecture and Infrastructure Committee and advises on Trusted Internet Connection (TIC), Federal Desktop Core Configuration (FDCC), Domain Name Service (DNS) Security, Key Escrow, Directory Services, Multi-factor Authentication, and Network Security.

The ICAMSC works in close coordination with the other subcommittees on issues within their purview that have a direct impact on ICAM work, including larger IT security efforts, application of identity management to NPEs, and privacy and security issues. Relevant portions of the work of these groups will be incorporated into this document; however, it is important to note that the ICAMSC is not the primary authority in these areas and does not seek to duplicate security-related efforts with the subcommittees.

The ICAMSC also works in collaboration with other related governance authorities, including the Executive Office of the President (to include National Security Staff, Office of Management and Budget, and the Office of Science and Technology Policy), the NSTC Subcommittee on Biometrics and Identity Management, and the appropriate Interagency Policy Committees based out of the Executive Office of the President. These groups have a broader focus on the national approach for identity management, whereas the ICAMSC is focused on implementation efforts within the Federal Government. In addition, 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. Due to the large degree of overlap between the work of these groups, the ICAMSC is in close collaboration with the relevant stakeholders to help ensure consistency between the related efforts. A list of primary stakeholders for federal ICAM can be found in Section 6.1.2.

The Interagency Security Committee (ISC), established by Executive Order 12977, is responsible for developing standards, policies and best practices for enhancing the quality and effectiveness of physical security in, and the protection of, nonmilitary federal facilities in the United States. The ISC provides a permanent body to address continuing government-wide security for federal facilities. Due to the strong dependency between the authority of the ISC and the successful implementation of ICAM objectives for physical access, the ICAMSC has been working directly with the ISC to coordinate guidance efforts and develop best practices for inclusion in this document.

The governance authorities identified in this section help shape the strategy and framework for federal ICAM initiatives and are responsible for measuring performance in the achievement of the ICAM goals and objectives. The entities described here are also key stakeholders that were identified as part of the ICAM Segment Architecture Stakeholder List, which can be found in its entirety in Section 6.1.2 of the document.

2.3.2. Federal Policies and Key Initiatives Impacting ICAM Implementation

This section identifies the general laws, regulations, and policies that impact and in many cases have initiated today's ICAM programs. This list represents a subset of the ICAM Segment Architecture Policy List, which can be found in 0 of this document.

- **Privacy Act of 1974.** This act protects certain Federal Government records pertaining to individuals. In particular, the Act covers systems of records that an agency maintains and retrieves by an individual's name or other personal identifier (e.g., social security number).
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA).** HIPAA protects the privacy of individually identifiable health information. The Act also provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information.
- **Government Paperwork Elimination Act of 1998 (GPEA).** GPEA requires Federal agencies, by October 21, 2003, to allow individuals or entities that deal with the agencies the option to submit information or transact with the agency electronically, when practicable, and to maintain records electronically, when practicable. The Act specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form and encourages Federal Government use of a range of electronic signature alternatives.
- **Electronic Signatures In Global and National (ESIGN) Commerce Act of 2000.** This act was intended to facilitate the use of electronic records and signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically.
- **E-Government Act of 2002.** This act is intended to enhance the management and promotion of electronic Government services and processes by establishing a Federal CIO within the Office of Management and Budget, 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.
- **Federal Information Security Management Act (FISMA) of 2002.** This act 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.

- **Federal Government Intelligence Reform and Terrorism Prevention Act of 2004.** This act contains a variety of measures designed to reform the intelligence community and the intelligence and intelligence-related activities of the United States Government.
- **Public Law No: 110-53, The Implementing the 9/11 Commission Recommendations Act of 2007.** This law provides for the implementation of the recommendations of the National Commission on Terrorist Attacks Upon the United States.
- **Homeland Security Presidential Directive 12 (HSPD-12): Policy for a Common Identity Standard for Federal Employees and Contractors.** HSPD-12 calls for a mandatory, government-wide standard for secure and reliable forms of ID issued by the Federal Government to its employees and employees of federal contractors for access to federally controlled facilities and networks.
- **Executive Order 12977.** Established the ISC to develop standards, policies, and best practices for enhancing the quality and effectiveness of physical security in, and the protection of, nonmilitary federal facilities in the United States.
- **Executive Order 13467.** Established to ensure an efficient, practical, reciprocal, and aligned system for investigating and determining suitability for Government employment, contractor employee fitness, and eligibility for access to classified information.
- **OMB Memorandum M-00-10: OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act.** This document provides Executive agencies with the guidance required under Sections 1703 and 1705 of the GPEA, P. L. 105-277, Title XVII. GPEA requires agencies, by October 21, 2003, to provide for the (1) option of electronic maintenance, submission, or disclosure of information, when practicable as a substitute for paper; and (2) use and acceptance of electronic signatures, when practicable. GPEA specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form.
- **OMB Memorandum M 04-04: E-Authentication Guidance for Federal Agencies.** This guidance requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. It establishes and describes four levels of identity assurance for electronic transactions requiring authentication. Assurance levels also provide a basis for assessing Credential Service Providers (CSPs) on behalf of Federal agencies. This document will assist agencies in determining their E-Government authentication needs for users outside the Executive Branch. 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 Memorandum M 05-05: Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services.** This memo requires the use of a shared service provider (SSP) to mitigate the risk of commercial managed services for PKI and electronic signatures.
- **OMB Memorandum M 05-24: Implementation of HSPD-12– Policy for a Common Identification Standard for Federal Employees and Contractors.** This memorandum provides implementation instructions for HSPD-12 and FIPS-201.

- **OMB Memorandum: Streamlining Authentication and Identity Management within the Federal Government (July 3, 2003).** This memorandum details specific actions that agencies should undertake to support electronic authentication by coordinating and consolidating investments related to authentication and identity management.
- **OMB Memorandum M 06-16: Protection of Sensitive Agency Information.** This memorandum directs all Federal Agencies and departments to encrypt all sensitive data on mobile computers and devices.
- **OMB Memorandum M 07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information.** This memorandum guides agencies in how to protect personally identifiable information that is in their possession and how to prevent breaches of that information. The memo provides an outline for agencies to develop a breach notification policy by reviewing existing requirements related to privacy and security.

PART A: ICAM Segment Architecture

This part of the document (Chapters 3, 4, and 5) comprises the government-wide ICAM segment architecture.

This page is intentionally left blank.

3. ICAM Segment Architecture

This chapter provides an overview of segment architecture principles, outlines the approach used to develop the ICAM segment architecture, and presents the core components of the ICAM segment architecture organized into the five layers defined in the Federal Enterprise Architecture (FEA). Chapter 4 categorizes the business layer of the ICAM segment into a set of ICAM use cases, which detail specific processes that support ICAM and present the components of the other architectural layers associated with those processes. Chapter 5 provides the Transition Roadmap and Milestones for achieving the target architecture. Chapters 3, 4, and 5 should be viewed together as the ICAM segment architecture.

It is intended that agencies will align their relevant segment and solution architectures to the common framework defined in the government-wide ICAM segment architecture. Alignment activities include a review of current business practices, identification of gaps in the architecture, and development of a transition plan to fill the identified gaps.

3.1. Developing the ICAM Segment

The ICAM segment architecture was developed under the auspices of the Federal CIO Council by a team of cross-agency representatives supporting the ICAMSC. The development team followed the approach outlined in the Federal Segment Architecture Methodology[19] (FSAM) to create the ICAM segment. The FSAM 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. The FSAM 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 over a specified period of time.

Early in the development of the ICAM segment architecture (and in accordance with the FSAM), a purpose statement was prepared to define its intent:

> *The purpose of the Federal ICAM segment architecture is to provide federal agencies with a standards-based approach for implementing government-wide ICAM initiatives. The use of enterprise architecture techniques will help ensure alignment, clarity, and interoperability across agency ICAM initiatives and enable agencies to eliminate redundancies by identifying shared ICAM services across the Federal Government.*

A key objective of the ICAM segment architecture is to implement a holistic approach for all government-wide identity, credential, and access management initiatives and areas (including civilian, defense, health, financial, intelligence, etc.), which have traditionally been viewed and implemented separately. Additionally, it was recommended that each agency use the information provided by the ICAM segment architecture in order to make the appropriate budget requests for ICAM initiatives beginning with the FY11 budget cycle. Implementation of the ICAM segment architecture will provide the means for agencies to collaborate on the development of government-wide solutions that meet individual needs while remaining consistent with current

[19] Federal Segment Architecture Methodology, Version 1.0, December 12, 2008. http://www.fsam.gov/

policy, guidance, standards, and technical specifications. The ICAM segment architecture is intended to be high-level and flexible enough to accommodate new initiatives, components, and technologies as they arise.

Within each of the five process steps, the FSAM specifies a list of outputs associated with performing the high-level activities and provides sample templates. The FSAM was developed as a prescriptive methodology but was also designed to be flexible and extensible to allow for organization and segment specific adaptations. Since a segment architecture is typically created at the agency level, many of the outputs of the FSAM had to be tailored in order to successfully define a high-level architecture for ICAM at the federal (government-wide) level.

The following table shows how the architecture outputs have been mapped to the chapters within the Roadmap and Implementation Plan. Outputs that have not been included within the body of the text have been provided as Appendices.

Chapter	Segment Architecture Deliverables Included
Chapter 1: Introduction	• Provides introduction to architecture deliverables contained throughout the document.
Chapter 2: Overview of Identity, Credential, and Access Management	• Policy Map • Business Challenges Analysis • Business Drivers, Goals & Objectives
Chapter 3: ICAM Segment Architecture	• Segment Architecture Purpose Statement • Business Value Chain Analysis • Inventory of Government-wide Data Sources & Data Elements • As-Is System Interface Diagram • Target System Interface Diagram • Services Framework
Chapter 4: ICAM Use Cases	• As-is Use Cases • Target Use Cases • Target Information Flow Diagrams
Chapter 5: Transition Roadmap and Milestones	• Recommendation Implementation Overview • Implementation Sequencing Plan • Transition Plan Milestones • Performance Metrics
Chapter 6: ICAM Implementation Planning	• Stakeholder List • Risk Registry
Chapter 7: Implementation Guidance	• Will provide guidance on how to implement ICAM segment architecture transition plan; planned to be included as an expanded Part B of this document

Figure 2: FSAM Asset Mapping to Roadmap and Implementation Plan Chapters

3.2. ICAM Architectural Layers

The FEA specifies five layers that offer different views of an architecture: Performance, Business, Data, Service, and Technology. These layers are interrelated and mapped to one another to illustrate the ways in which the different aspects of the architecture impact the others. The FEA consists of a set of interrelated "reference models" (one for each architectural layer) that form the framework for describing important elements of the FEA in a common and consistent way across lower level segment and solution architectures. The FEA reference models were leveraged wherever possible in developing the ICAM segment in order to facilitate cross-

agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across agencies. Where necessary, the framework has been extended and specialized to meet the specific needs of the ICAM segment.

The following figure lists the five layers of the architecture and describes the view that each provides of the segment.

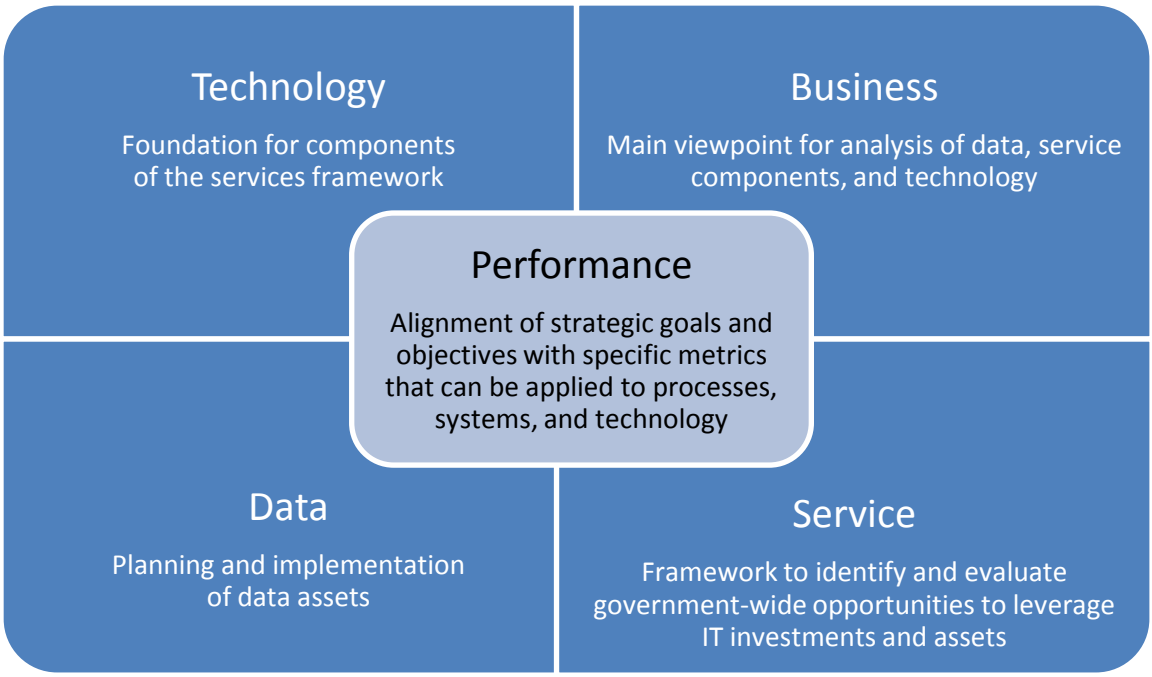

Figure 3: Segment Architecture Layers

The following subsections describe each layer in greater detail and present the core components of the FSAM segment architecture for each layer.

3.2.1. Performance Architecture

The performance architecture aims to align strategic goals and objectives with specific metrics that can be applied to processes, systems, and technology in order to evaluate success against those goals. The goal of performance architecture is to provide the ability to take corrective action on performance results, the capability to measure resource contributions to specific mission value, and the ability to influence strategic objectives. Improved performance is realized through greater focus on mission, agreement on goals and objectives, and timely reporting of results.

The ICAM performance architecture consists of the following components:

- **Business Challenges Analysis.** Provides an overview of the challenges within the current ICAM environment. Business challenges often represent strategic improvement opportunities for the target state architecture. This component has been integrated into the narrative in the document overview and Sections 2.1 and 2.2.
- **Business Drivers, Goals, and Objectives.** Describes the goals, drivers, and objectives for ICAM. The goals and objectives are provided in Section 2.1. The drivers show a direct link to the policies and other guidance documents impacting ICAM implementation and are provided in Section 2.3.2.

- **Performance Metrics.** Create a reporting framework to measure the activities and investments within the ICAM segment. This component is provided in Chapter 6.

Although the performance architecture is typically listed first among the segment layers, it frequently "book ends" the architectural development process, with the definition of strategic goals and objectives occurring in the earliest stages and the refinement and acceptance of performance metrics occurring as one of the last steps in creating the transition plan. The placement of the components of the performance architecture in the Roadmap reflects this split development of the layer.

In order to develop the performance metrics, the development team reviewed many as-is performance metrics that agencies use to track against individual ICAM investments through the OMB Exhibit 300. Analysis of the as-is metrics revealed that agencies are not tracking consistent metrics. Additionally, the majority of the agencies surveyed currently track metrics by one or more of the following individual, rather than integrated initiatives: PKI, PIV, and E-Authentication. These characteristics prevent a line of sight from the agency for a comprehensive view of government-wide ICAM performance. Chapter 5 outlines the ways in which these performance metrics should evolve in order to align ICAM initiatives across these stove-pipes and incorporate additional considerations critical to ICAM functionality.

3.2.2. Business Architecture

The business architecture is a functional perspective of the operations conducted within the ICAM segment. Segment architecture is driven by business management and delivers products that improve the delivery of business services to citizens and agency staff. As such, the business architecture provides the main viewpoint for the analysis of data, service components, and technology at the lower layers of the architecture.

The ICAM business architecture consists of the following components:

- **Business Value Chain Analysis.** Identifies the high-level logical ordering of the chain of processes that deliver value. This output has been modified from the FSAM template in order to gain applicability at the federal level. This component is provided in Section 3.2.2.1 below.
- **As-is and Target Use Cases.** Provide the high-level common business processes that support ICAM functionality. The use cases provide the structure for the detailed architectural information at the Data, Service, and Technology layers of the architecture. An overview of the use cases is provided in Section 3.2.2.2 below. Chapter 4 contains the complete use cases.

3.2.2.1. Business Value Chain Analysis

From an architectural perspective, the business processes for ICAM include multiple actions that are chained together. The achievement of the final outcome of the process relies on the completion of each action within the established chain. In developing a preliminary list of business processes within ICAM, the development team determined that each of the ICAM business process chains deliver value through a link back to one or more of the E-Government service sectors. The sectors are:

- **Government to Citizen (G2C).** Aims to facilitate interaction between government and the American public.

- **Government to Business (G2B).** Drives interaction between agencies and the private sector.
- **Government to Government (G2G).** Fosters the development of inter-agency relationships and information sharing across all levels of government (Federal, state, local and tribal).
- **Internal Efficiency and Effectiveness (IEE).** Drives internal agency processes and activities to become more friendly, convenient, transparent, and cost-effective.

The E-Government sectors are used as a framework in the development of each of the layers of the architecture. In the use cases, certain business functions are categorized separately because the processes varied depending on the sector addressed (e.g., the processes for creating and maintaining identity data for internal employees versus citizens or business partners). Likewise, at the data and technology layers, different data repositories or technologies may fulfill the same business process for different sectors (e.g., business partners and other government entities may use a PIV-interoperable credential to access Federal Government resources, whereas a citizen may use an alternate third-party credential).

3.2.2.2. Use Cases Overview

As the main component of the ICAM business architecture, the Roadmap Development Team identified common use cases that capture the core ICAM business processes. The use cases are not agency specific and instead are intended to capture the common set of activities and challenges facing agencies today in the current state and the ways in which those challenges can be addressed in a desired target state. Agencies are expected to tailor these use cases for their own ICAM segment architectures, which should align with this document. Figure 4: ICAM Use Case Overview provides an overview of the selected use cases and the relevant E-Government sectors to which the use cases align.

Use Case Name	E-Government Alignment				Use Case Description
	IEE	G2G	G2B	G2C	
Create and maintain digital identity record for internal user	✓				Provides the high-level process steps for establishing a digital identity for an internal user and modifying the digital identity record over time as the user's attributes change.
Create and maintain digital identity record for external user	✓	✓	✓	✓	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.
Perform background investigation for federal applicant	✓				Provides the high-level process steps for conducting a background investigation for a federal employee or contractor.
Create, issue, and maintain PIV card	✓				Provides the high-level process steps for creating and issuing a PIV credential to a federal employee or contractor and maintaining it over the credential lifecycle in compliance with FIPS 201.
Create, issue, and maintain PKI credential	✓	✓	✓	✓	Provides the high-level process steps for creating, issuing, and maintaining a PKI certificate over the credential lifecycle in compliance with Federal PKI standards.

Use Case Name	E-Government Alignment				Use Case Description
	IEE	G2G	G2B	G2C	
Create, issue, and maintain password token	✓	✓	✓	✓	Provides the high-level process steps for creating, issuing, and maintaining a password token over the credential lifecycle.
Provision and deprovision user account for an application	✓	✓	✓	✓	Provides the high-level process steps for provisioning and deprovisioning a user account and establishing the access privileges and entitlements for the user in an agency application.
Grant physical access to employee or contractor	✓				Provides the high-level process steps for authenticating and authorizing or denying a federal employee or contractor physical access to a facility or site.
Grant visitor or local access to federally-controlled facility or site	✓	✓	✓	✓	Provides the high-level process steps for authenticating and authorizing or denying a visitor (external to Federal Government or individual from another agency) for physical access to federally-controlled facilities and sites.
Grant logical access	✓	✓	✓	✓	Provides the high-level process steps for authenticating and authorizing or denying a user logical access to systems, applications, and data. The use case provides alternate process flows to address authentication mechanisms at all four levels of assurance.
Secure document or communication with PKI	✓	✓	✓	✓	Provides the high-level process steps for digitally signing and encrypting data and electronic communications using the most common system tools available within the Federal Government.

Figure 4: ICAM Use Case Overview

The architecture analysis sections of each use case additionally provide the following details specific to the use case that support the business architecture layer:

- **E-government Alignment.** Mapping to one of the ICAM E-Government sectors.
- **Trigger.** Event that initiates the process; may be more than one trigger in a use case.
- **Actors.** Individuals, systems or organizations involved in the specific processes described for each use case.
- **Endpoints.** Termination points in the process flow where a specific outcome is achieved or a specific output is produced.

3.2.3. Data Architecture

Data architecture is the planning and implementation of data assets including the set of data, the processes that use that data, and the technologies selected for the creation and operation of information systems. From an EA perspective, data architecture is not the set of detailed models of individual systems; instead, it provides the "big picture," including the information/data stored across the enterprise, the information that needs to be shared, and the ways in which that information should be shared through the use of exchange standards.

The ICAM data architecture consists of the following components:

- **Inventory of Government-wide Data Sources and Data Elements.** Lists and describes the major cross-government ICAM data repositories, the information contained in them,

and the E-Government sectors they service. This component is provided in Section 3.2.3.1 below.

- **Target Information Flow Diagrams.** Depicts the key information flows found in the business processes and assists in discovery of opportunities for re-use of information in the form of information-sharing services. This component is provided in the use cases in Chapter 5.

Additionally, the architecture analysis sections of each of the use cases provided in Chapter 5 include details specific to the ICAM data architecture. An overview of these details is provided in Section 3.2.3.2 below.

3.2.3.1. Inventory of Government-wide Data Sources and Elements

Cross-government repositories are those that are used between one or more agencies and include systems and data stores. Agency-specific systems are unique to a particular agency and do not serve as an authoritative source outside of that agency. Figure 5: Cross Government Repositories and Systems includes an overview of the core cross-government repositories or systems identified across the use cases.

Repository or System	Description	Data Types								E-Gov Alignment			
		Biometrics	Personal Info	Qualifications	Tokens	Roles	Suitability	Privileges	Access Rules	G2B	G2C	G2G	IEE
eVerify	E-Verify is an Internet based system operated by the Department of Homeland Security (DHS) in partnership with the Social Security Administration (SSA) that allows participating employers to electronically verify the employment eligibility of their newly hired employees. E-Verify is the best means available for determining employment eligibility of new hires and the validity of their Social Security Numbers.		✓								✓	✓	✓
Clearance Verification System (CVS)	An Office of Personnel Management system that allows authorized agency officials to access information pertaining to current and former background investigations performed by OPM.		✓				✓	✓					✓
Integrated Automated Fingerprint Identification System (IAFIS)	A national fingerprint and criminal history system maintained by the Federal Bureau of Investigation Criminal Justice Information Services (FBI CJIS) Division. It provides automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.	✓	✓				✓	✓		✓			✓
National Crime Information Center (NCIC)	An FBI nationwide information system dedicated to serving and supporting law enforcement agencies. NCIC assists authorized users in apprehending fugitives, locating missing persons, recovering stolen property, and identifying terrorists.		✓				✓	✓		✓	✓	✓	✓

Repository or System	Description	Data Types							E-Gov Alignment			
		Biometrics	Personal Info	Qualifications	Tokens	Roles	Suitability	Privileges	Access Rules	G2B	G2C	G2G	IEE
Federal / Emergency Response Official Repository	The F/ERO repository is managed by Federal Emergency Management Agency (FEMA) IAW Public Law 100-53 and will link to agency HSPD-12 and local emergency response systems. It is designed to be the authoritative source of responder attributes fed to the FERO repository from Federal, State and Local emergency response coordinators. The F/ERO repository is refreshed every 18 hours.		✓	✓		✓			✓	✓	✓	✓	✓
Joint Personnel Adjudication System (JPAS)	JPAS is the Department of Defense (DoD) personnel security system and provides information regarding clearance, access and investigative status to authorized DoD security personnel and other interfacing organizations.		✓	✓		✓	✓			✓			✓

Figure 5: Cross Government Repositories and Systems

3.2.3.2. Use Case Data Details Overview

Each use case identifies the following data architecture-related details:

- **Data Repositories and Systems**. A central place where data is stored and maintained; a place where multiple databases or files are located for distribution over a network. For each use case, the identified data repositories may be cross-government or agency-specific. Wherever possible, repositories or systems that possess data elements identified as authoritative have themselves been identified as authoritative.
- **Data Elements**. An individual data field stored within a repository or transmitted as part of a transaction. The data elements identified in the use cases are typically identity attributes, such as address, first name, biometric sample, etc. For agency or mission specific elements, different additional elements will be identified.
- **Data Standards**. The required content and format in which particular types of data are to be presented and exchanged such as the National Information Exchange Model (NIEM). Data standards are normally tied to a specific mission or business context and are governed by a group of stewards. Many cross-agency data standards and guidance sources can be found in 0.

3.2.4. Service Architecture

The service architecture provides a functional framework for identifying and evaluating government-wide opportunities to leverage IT investments and assets from a service perspective. This model helps understand the services delivered by the government and assess whether there is an opportunity to group like services and create opportunities for reuse or shared services. The ICAM service architecture consists of the **Services Framework**, a functional framework that classifies ICAM service components with respect to how they support business and/or performance objectives. This component is provided in Sections 3.2.4.1 through 3.2.4.7 below.

Additionally, the architecture analysis sections of each of the use cases provided in Chapter 5 identify the service components used in the use case.

In order to develop the ICAM Services Framework, existing service frameworks from a number of sources were reviewed, including:

- FEA Service Component Reference Model (SRM)
- HSPD-12 Shared Component Architecture v0.1.6
- ISO/IEC JTC 1/SC27 N7237 - IT Security Techniques
- OneVA Identity Services Segment Architecture
- DoD Net-Centric Enterprise Services (NCES)
- DoD Enterprise Services Security Framework (ESSF)

Following the review, several working sessions were conducted to define and gain consensus on the service types and components necessary to support the ICAM segment. Figure 6 shows the resulting ICAM Services Framework.

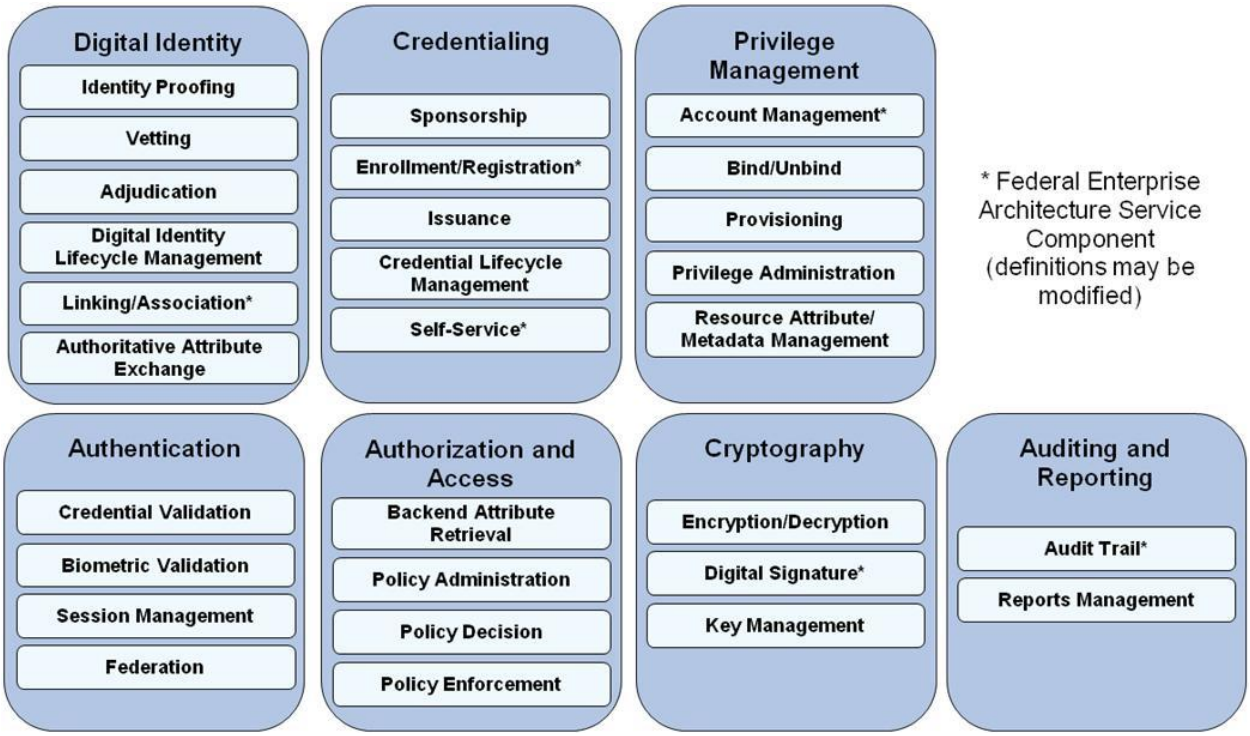

Figure 6: Services Framework

The figure represents two main layers of the Services Framework:

- **Service Type.** Provides a layer of categorization that defines the context of a specific set of service components. The service types in the diagram are represented by the darker blue, outer boxes.
- **Service Component**. A self-contained business process or service with predetermined and well-defined functionality that may be exposed through a well-defined and documented business or technology interface. The service components in the diagram are represented by the lighter blue, inner boxes.

The following subsections provide detailed descriptions of each of the ICAM service components, categorized by service type. It is important to note that while the ICAM Services Framework seeks to provide a common set of services to support common needs across agencies, it is not intended to preclude an agency for augmenting or customizing the framework to provide services to support agency-specific scenarios and to incorporate their mission needs and existing infrastructure.

3.2.4.1. Digital Identity Service Descriptions

Digital identity is the electronic representation of an individual's identity. Digital Identity Services comprise the processes required to capture and validate information to uniquely identify an individual, determine suitability/fitness, and create and manage a digital identity over the lifecycle.

Service Component	Description
Identity Proofing	Process of verifying sufficient information (e.g., identity history, credentials, documents) to establish an individual's right to a claimed identity; initiates chain of trust in establishing a digital identity and binding it to an individual.
Vetting	Process of examination and evaluation, including background check activities; results in establishing verified credentials and attributes.
Adjudication	Process of reviewing identity vetting results and determining eligibility for an identity credential.
Digital Identity Lifecycle Management	Process of establishing and maintaining the attributes that comprise an individual's digital identity; supports general updates to an identity such as a name change or biometric update.
Identity Attribute Discovery	Process of mapping pathways and creating indexes or directories that allows identification of authoritative data sources (ADS) of identity data.
Linking/Association	Process of linking one identity record with another across multiple systems; activation and deactivation of user objects and attributes as they exist in one or more systems, directories, or applications in response to an automated or interactive process; used in conjunction with Authoritative Attribute Exchange.
Authoritative Attribute Exchange	Provides capability to connect various authoritative data sources and share identity and other attributes with the shared infrastructure.

3.2.4.2. Credentialing Service Descriptions

Credentialing is the process of binding an identity to a physical or electronic credential, which can subsequently be used as a proxy for the identity or proof of having particular attributes.

Service Component	Description
Sponsorship	Process for establishing the need for a card/credential by an authorized official; this step is critical for NPE credential request and issuance.
Enrollment/Registration	Process of collecting and storing identity information of an entity in a registry/ repository; associates the entity with minimal information representing the entity within a specific context and allows the entity to be distinguished from any other entity in the context.
Issuance	Process by which possession of a credential is passed to an entity. Service characteristics vary by credential type.
Credential Lifecycle Management	Refers to maintenance of a credential and associated support over the lifecycle; common processes include renewal, reissuance, suspension, blocking and unblocking, revocation, etc. Lifecycle support activities vary depending on the credential type, and may include a Self Service component.
Self-Service	Request access to network and physical resources based on established credentials, reset forgotten passwords, update identity and credential status information, and view corporate and organizational identity information using electronic interfaces and without supervisory intervention.

3.2.4.3. Privilege Management Service Descriptions

Privilege Management is the definition and management of policies and processes that define the ways in which the user is provided access rights to enterprise systems. It governs the management of the data that constitutes the user's privileges and other attributes, including the storage, organization and access to information in directories.

Service Component	Description
Privilege Administration	Process for establishing and maintaining the entitlement or privilege attributes that comprise an individual's access profile; supports updates to privileges over time as an individual's access needs change.
Account Management	Supports user account synchronization with application user repositories and authoritative sources; establishes baseline knowledge of the asset being provisioned such as rules for access, credential requirements, etc.
Bind/Unbind	Building or removing a relationship between an entity's identity and further attribute information on the entity (e.g., properties, status, or credentials).
Provisioning	Creating user access accounts and assigning privileges or entitlements within the scope of a defined process or interaction; provide users with access rights to applications and other resources that may be available in an environment; may include the creation, modification, deletion, suspension, or restoration of a defined set of privileges.
Resource Attribute/ Metadata Management	Process for establishing and maintaining data (such as rules for access, credential requirements, etc.) for a resource/asset being provisioned to define the access, protection, and handling controls. Specific data tags are used that explicitly state how data or a service is accessed, stored, transmitted or even if it can be made discoverable.

3.2.4.4. Authentication Service Descriptions

Authentication is the process of verifying that a claimed identity is genuine and based on valid credentials. Authentication typically leads to a mutually shared level of assurance by the relying parties in the identity. Authentication may occur through a variety of mechanisms including challenge/response, time-based code sequences, biometric comparison, PKI or other techniques.

Service Component	Description
Credential Validation	Establishes the validity of the identity credential presented as part of the authentication transaction; PKI certificates are validated using techniques such as revocation status checking and certificate path validation. Validation of other credentials can include PIN check, security object check, Cardholder Unique Identifier (CHUID) validation, mutual SSL/TLS, the validation of digital signatures, or other non-biometric and non-cryptographic mechanisms.
Biometric Validation	Services to support capturing, extracting, comparing and matching a measurable, physical characteristic or personal behavioral trait used to recognize the identity or verify the claimed identity of an entity. Biometrics modalities include face, fingerprint, and iris recognition and can be matched on card, on reader, or on server.
Session Management	Allows for the sharing of data among multiple relying parties as part of an authenticated user session; includes protocol translation services for access to systems needing different authentication protocols; manages automatic time-outs and requests for re-authentication.
Federation	A trust relationship between discrete digital identity providers (IDPs) that enables a relying party to accept credentials from an external identity provider in order to make access control decisions; provides path discovery and secure access to the credentials needed for authentication; and federated services typically perform security operations at run-time using valid NPE credentials.

3.2.4.5. Authorization and Access Service Descriptions

Authorization and Access are the processes of granting or denying specific requests for obtaining and using information processing services or data and to enter specific physical facilities. It ensures individuals can only use those resources they are entitled to use and then only for approved purposes, enforcing security policies that govern access throughout the enterprise.

Service Component	Description
Backend Attribute Retrieval	Acquires additional information not found in the authenticated credential that is required by a relying party to make an access based decision.
Policy Administration	Provides a standard policy exchange format to compose, modify, manage, and control access control policies.
Policy Enforcement	Restricts access to specific systems or content in accordance with policy decisions that are made.
Policy Decision	Serves as an access control authorization authority for evaluating access control policies based on a variety of inputs.

3.2.4.6. Cryptography Service Descriptions

Cryptography supports the use and management of ciphers including encryption and decryption processes to ensure confidentiality and integrity of data, including necessary functions such as Key History and Key Escrow. Cryptography is often used to secure communications initiated by humans and NPEs.

Service Component	Description
Encryption/Decryption	Encryption is the process of transforming information using a cipher algorithm to make it unreadable to any entity except those possessing special knowledge, usually referred to as a key. Decryption is the process of making encrypted information readable again.
Digital Signature	Information encrypted with an entity's private key, which is appended to a message, document, or transaction to assure the recipient of its authenticity and integrity. The digital signature proves that the message, document, or transaction was signed by the identity associated with the private key. The digital signature becomes invalid if the signed content is changed.
Key Management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction.

3.2.4.7. Auditing & Reporting Service Descriptions

Auditing and Reporting addresses the review and examination of records and activities to assess adequacy of system controls and the presentation of logged data in a meaningful context.

Service Component	Description
Audit Trail	Capture user management audit and logging data; a record showing who has accessed a system and what operations the user has performed
Reports Management	Group of reports that detail information about users and NPEs, user and NPE activity, identity audit information and identity management related system information; includes ad hoc and standardized reporting

3.2.5. Technical Architecture

The technical architecture provides the foundation for the components of the Services Framework, which in turn support the business layer and business-driven approach of the use

cases. Specifically, the technical architecture is used to describe proposed technical solutions using a standard vocabulary and categorization scheme. As agencies propose solutions to fulfill the ICAM segment, the technical architecture allows those solutions to be analyzed for their fit with the desired target state, for duplication with other efforts, and for the architectural gaps they might fill. In addition, it facilitates the re-use of technology across agencies.

The ICAM technical architecture consists of the following components:

- **As-is System Interface Diagrams.** Provide a depiction of the as-is "conceptual solution architecture," which shows the existing systems and services in the as-is state and identifies the relationships between them. This component is provided in Section 3.2.5.1 below.
- **Target System Interface Diagrams.** Provide a depiction of the target "conceptual solution architecture," which shows the proposed systems and services in the target state and identifies the relationships between them. This component is provided in Section 3.2.5.2 below.

Additionally, the architecture analysis sections of each of the use cases provided in Chapter 5 include specific types of hardware and software and the technical standards at the ICAM data architecture layer to support the use case. Technical standards provide the types of product specifications needed, network protocols, or other technical components of the architecture. A list of current ICAM technical guidance and standards applicable across all federal agencies can be found in Appendix G. Standards and technologies listed in the use cases are not normative or exclusive but should be considered prior to implementing local system architectures at an agency to provide enhanced interoperability.

In order to maintain government-wide applicability, the ICAM technical architecture is provided at a higher level than would typically be expected for a segment. As each agency aligns with the ICAM segment, the technical architecture may be translated to a more detailed level as needed by an agency to map the specific products and standards supporting ICAM systems to the overarching framework.

3.2.5.1. As-is System Interface Diagrams

Today agencies are employing myriad processes for implementing ICAM capabilities as well as different types of technologies and standards to support these processes. There is such a discrepancy between the ways in which agencies perform ICAM functions that agency systems are not interoperable, stove-pipes abound, processes are duplicated, and authoritative sources are in many cases unknown. These differences pose a significant challenge in trying to define a single, common as-is system interface diagram at the agency level. In order to overcome that challenge, the following figure depicts an example that is common in many agencies.

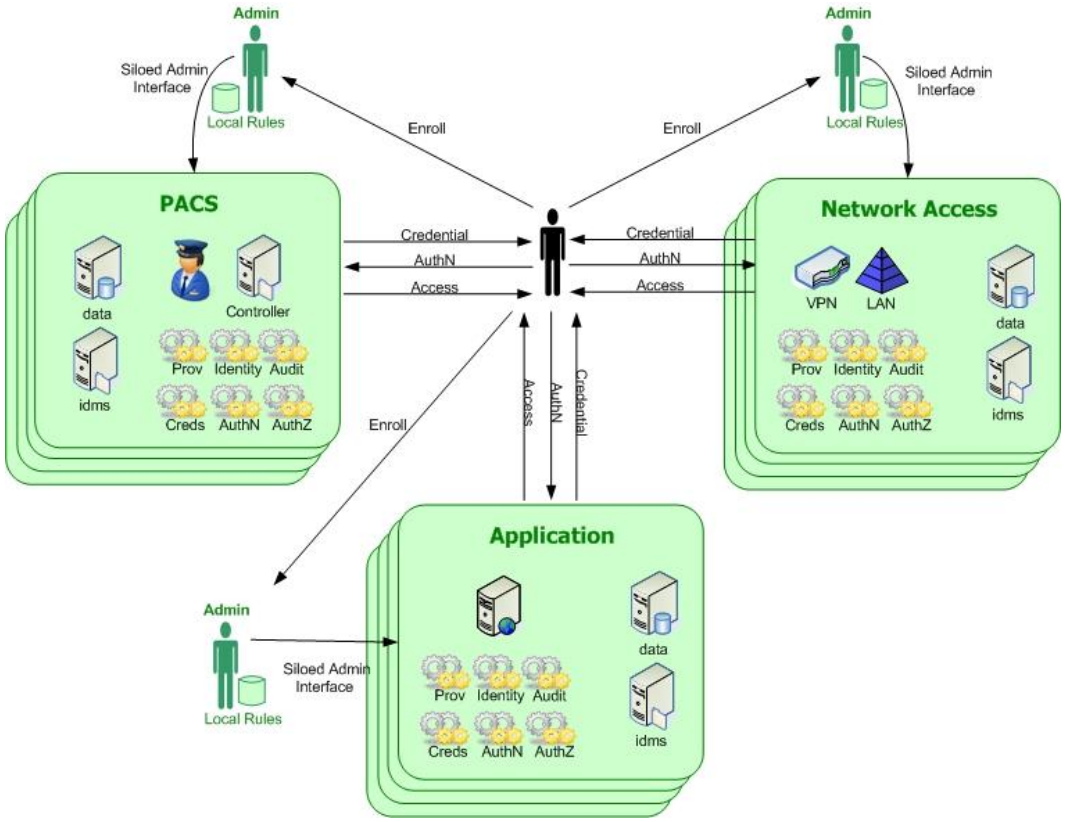

Figure 7: Agency As-Is Conceptual Diagram

The figure above shows ICAM functions performed independently by PACS, networks, and other applications. The systems each have ICAM related functions inside their system boundaries with no shared services. Users are forced to contend with multiple incompatible credentialing, authentication, and access control paradigms. Each system also has a separate administrative interface used for enrollment and privilege management. While the diagram has been streamlined to show three different applications, this structure is generally replicated many times over in each agency, creating considerable redundancies and inefficiencies in agency management of ICAM functions. When establishing functionality for use across federal applications, the net result is the same – the user must be re-credentialed, identity proofed, and provisioned in each system across the federal enterprise.

Figure 8 and Figure 9 depict the as-is system flows of several major ICAM infrastructures at the government-wide level. When attempting to represent the government-wide system interfaces, a pattern arose similar to the findings at the agency level; established ICAM architectures are managed in different silos.

The Federal PKI Architecture shown in Figure 8 depicts the members of the Federal PKI Trust Framework. The Federal PKI operates two primary components: the Federal Bridge Certification Authority (FBCA) and the Federal Common Policy Framework Certification Authority (FCPCA).

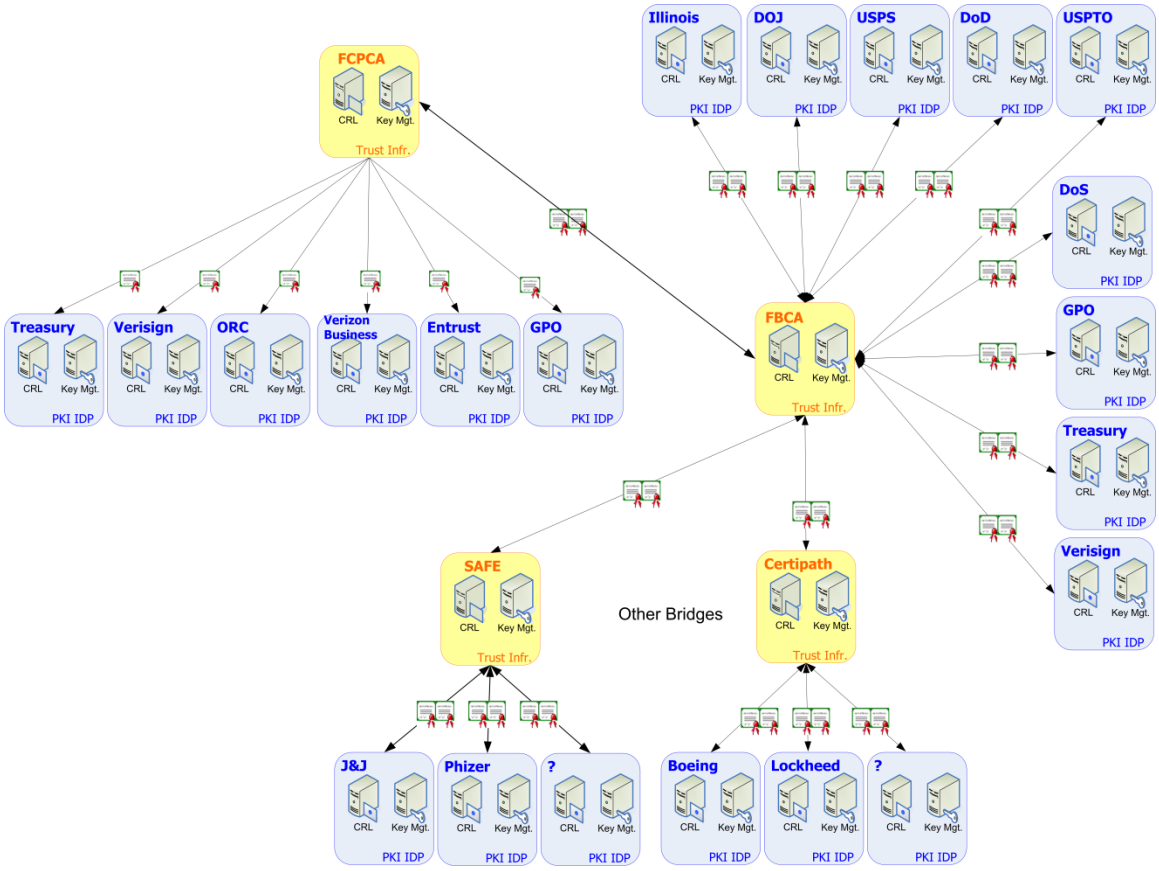

Figure 8: Federal PKI Architecture

The FBCA maintains peer-to-peer cross-certified relationships with Enterprise PKI implementations, including federal agency legacy PKIs. In addition the FBCA maintains a peer-to-peer relationship with two other Bridges: the Safe BioPharma Bridge, operated by the pharmaceutical industry, and the Certipath Bridge, operated by the Aerospace-Defense industry. By contrast, the FCPCA is the Federal PKI Trust Root, acting as the top of a hierarchy which includes a set of SSPs from whom Federal agencies that do not operate a legacy PKI can acquire PKI services that comply with Federal policy requirements. The diagram represents the Common Policy Root Certification Authority (CA) and the three bridges in light orange, with the individual PKIs associated with each in blue. Moving forward in the target state, the Federal Government will take advantage of higher levels of trust in interactions with other governments, businesses and citizens through the use of externally-issued PKI certificates thanks to the efforts of the Four Bridges Forum, which includes the group of trust bridges identified above and the higher education demonstration bridge.

Enabling the appropriate level of identity assurance for non-federal users, as defined in OMB M-04-04, *E-Authentication Guidance for Federal Agencies*, continues to be a challenge for the Federal community. While solutions are available, the ability for the 100 million plus individuals and businesses that need to obtain re-usable credentials that are cost-effective has not been realized. In many cases agency application owners continue to establish userid/password relationships with their constituencies, thereby perpetuating the stove-piped approach to identity management, lacking high assurance of identity when such assurance may be necessary, and incurring high costs in password resets and maintenance. In the target state, it is expected that the

Federal Government will take advantage of a wide variety of identity schemes through the establishment of a government-wide approach to federated identity and the increased availability and acceptance of third party credentials and authentication services for use across federal agencies, state and local partners, and private entities.

Figure 9 shows a generic solution architecture for an agency PIV system.

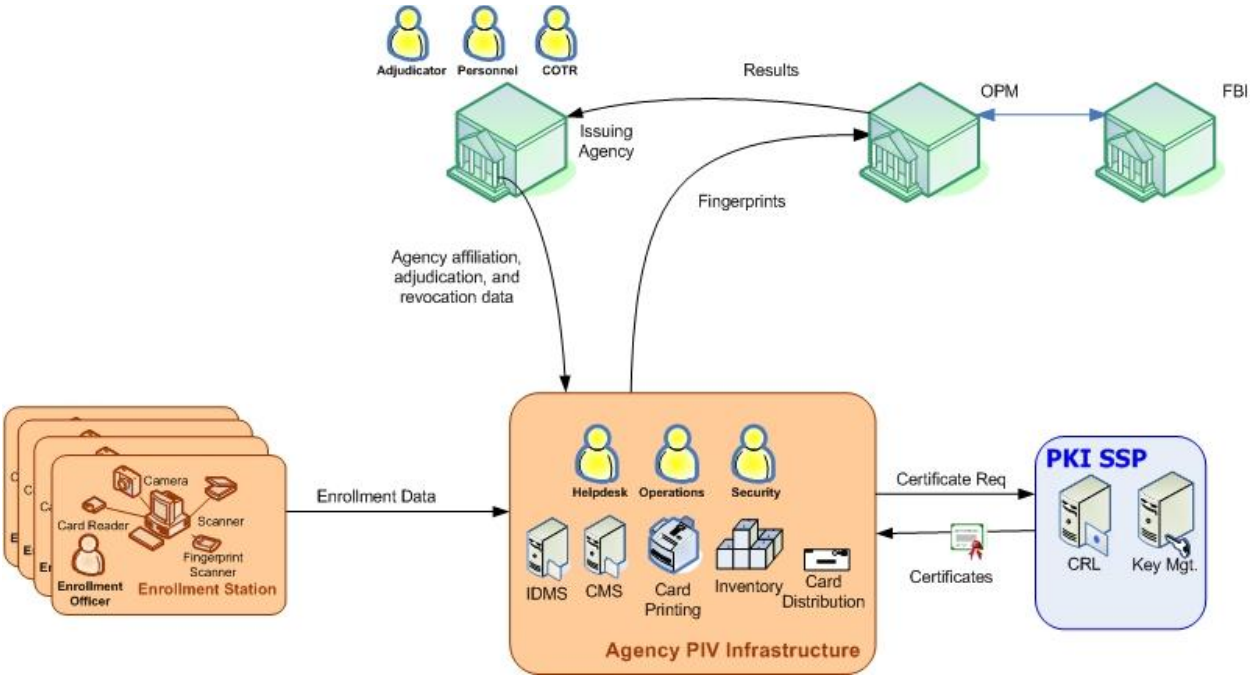

Figure 9: HSPD-12 Conceptual Diagram

In the target state, it is envisioned that agencies will use the PIV credentials for PACS and LACS, and that programs whose constituencies are primarily Federal employees will utilize the capabilities of the PIV card for access control. In addition, the issuance process for the PIV card will leverage common services through automated interfaces in order to improve efficiency in PIV processes.

3.2.5.2. Target Conceptual Diagrams

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 diagrams in this section depict at a simplified, conceptual level the target state vision for ICAM solutions.

Figure 10 shows the target system interfaces at the agency level, as viewed from the user perspective.

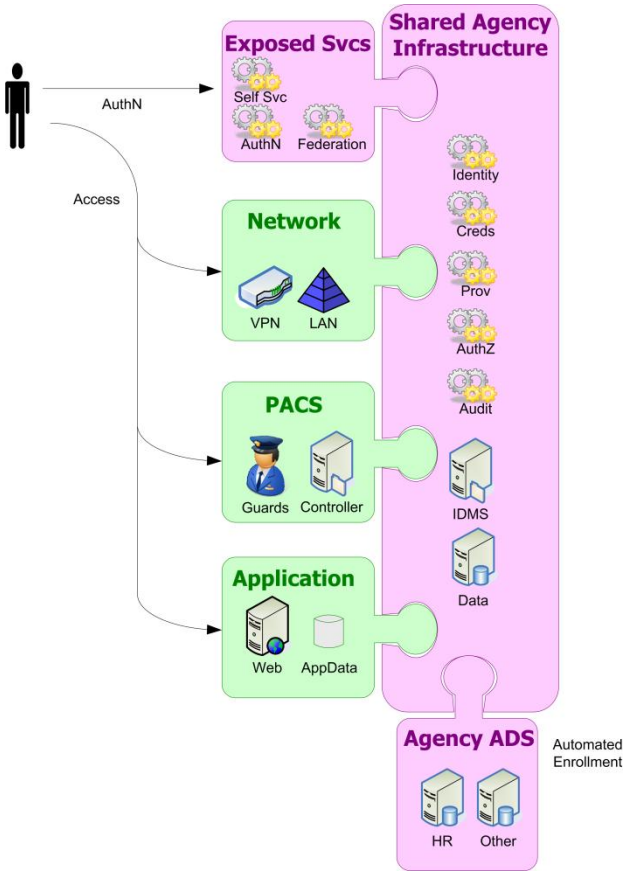

Figure 10: Agency Target Conceptual Diagram

This example depicts agency networks, PACS, and other applications plugged into a shared agency infrastructure. ICAM functions are handled in the shared infrastructure rather than independently in each system. Authoritative Data Sources (ADS) such as Human Resources (HR) systems are also integrated into the shared infrastructure so that enrollment and provisioning can be automated rather than manually entered through various application specific administrative interfaces. The shared infrastructure also exposes user interfaces so that end user can authenticate to the shared infrastructure once, then access various systems without the need to re-authenticate.

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.

The infrastructure should have the following characteristics:

- The shared infrastructure should provide identity management related services to users, such as authentication, federation, and user self-service.
- Applications should access the shared infrastructure to leverage shared identity, credentialing, provisioning, authorization, and auditing services.
- An agency Authoritative Attribute Exchange Service (AAES) should be used to connect various ADS and share data with the shared infrastructure.
- Users authenticated into the shared infrastructure should have seamless access to all integrated applications for which they have permission to access.

- Authenticated user will have access to data within infrastructure based on attributes.

In addition, the shared agency infrastructure shown in Figure 10 will connect to a shared federal infrastructure that provides common, government-wide ICAM services as depicted in Figure 6.

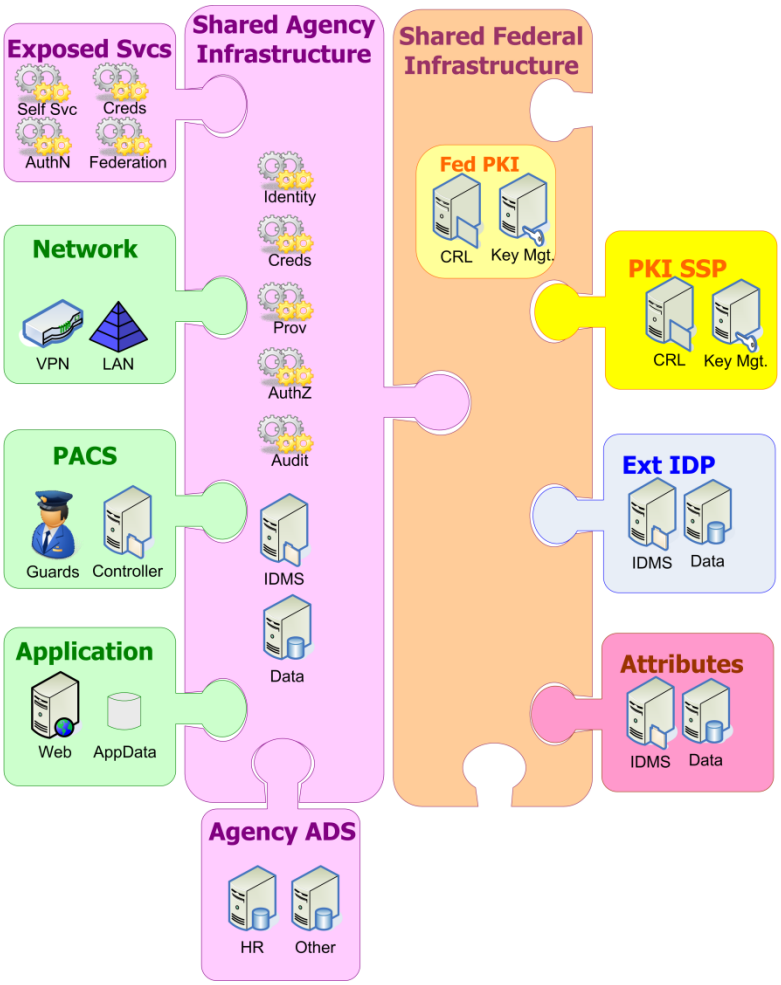

Figure 11: Federal Enterprise Target Conceptual Diagram

The shared federal infrastructure will provide interfaces to PKI SSPs, Identity Providers (IDP), attribute repositories, and other services as needed. The integration between shared agency and federal infrastructures will help achieve the objectives of eliminating redundancies and enhancing interoperability across the government.

A key interoperability issue in the current state is a user from one agency being able to use his PIV credential to gain permitted access to facilities and applications at other agencies. Tying agency infrastructures into a shared federal infrastructure will help resolve this issue. Figure 12 depicts the target concept for cross-agency access. A user issued a PIV credential from any agency can be used for access to various systems at other agencies that have integrated with the Shared Federal Infrastructure.

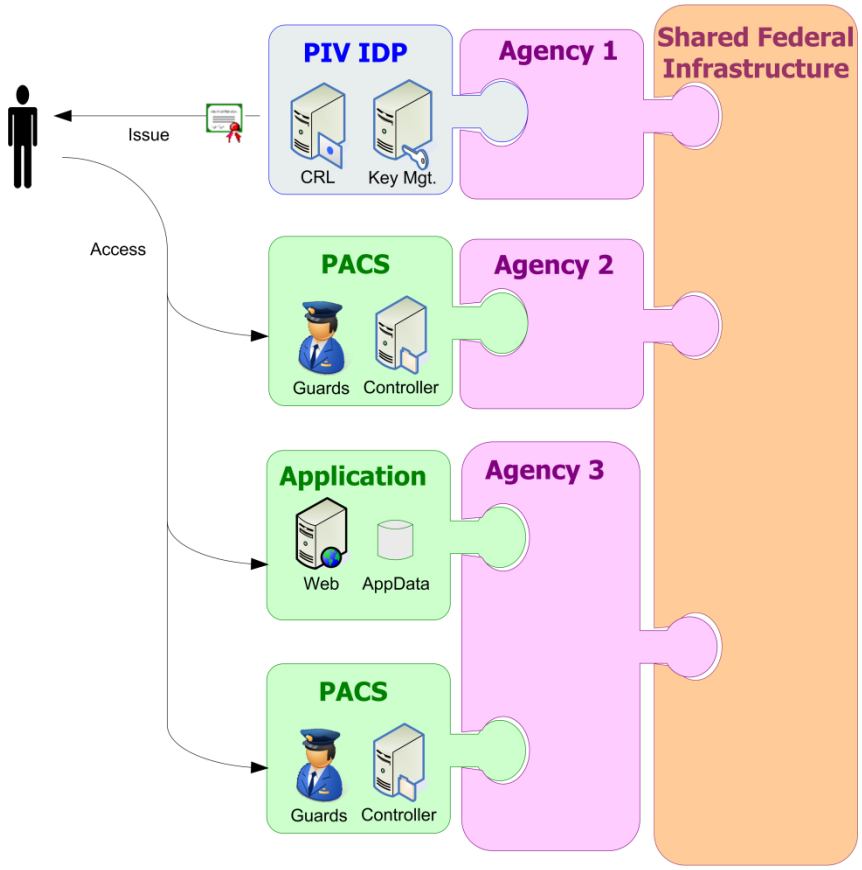

Figure 12: Federal Enterprise Target Conceptual Diagram: Cross-Agency Access

Similar to internal agency users, it is desired that external users in the target state may use a single, third-party credential to achieve a seamless interaction with services across multiple agencies in the Federal Government. Figure 13 shows the scenario where an external user authenticates via an external IDP in order to access services at several different agencies. The external IDP is integrated with the Shared Federal Infrastructure, enabling access to multiple agencies.

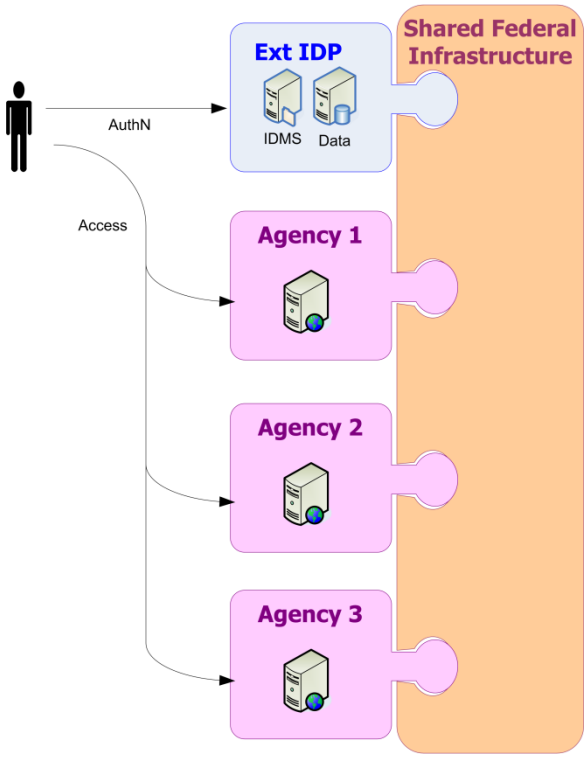

Figure 13: Federal Enterprise Target Conceptual Diagram, Citizen Access

4. ICAM Use Cases

This chapter includes the high-level use cases that outline the components of the ICAM segment architecture within the business functions that they support. Each use case describes a series of actions taking place, the actors involved, the data being exchanged and the systems, applications, technology and standards being leveraged. Each use case includes the following sections:

- **As-is Analysis.** Analysis of the ways in which the business functions are completed today across the Federal Government. It includes any specific challenges in the current state, a process flow narrative and diagram, and a detailed analysis of the architecture components (business, data, service and technology) that support the as-is use case.
- **Target Analysis.** Analysis of the desired way to complete the business functions. It includes a description of the primary differences from the as-is state in terms of process, data, service, or technology. It also includes a process flow narrative and diagram and a detailed analysis of the architecture components that support the target use case.
- **Gap Analysis.** An overview of the primary differences between the as-is and target states. The gaps identified in this section were used to develop the Transition Roadmap and Milestones presented in Chapter 5.

The use cases presented in this chapter have been selected as high-level functions that are performed by federal executive branch agencies. Each was selected to represent part of the core ICAM activities needed in order to service all E-Government sectors and user groups, whether internal or external to an agency, as they conduct business with the Federal Government. In their totality, the use cases encompass the major aspects of ICAM and include identity record creation, vetting, primary credentialing activities, provisioning, and physical and logical access. Some critical areas that support ICAM functionality across the use cases, such as auditing and reporting, are represented within the "Architecture Details" tables in each use case and are discussed further in the implementation guidance in Chapters 7-12.[20] Figure 14 illustrates the high-level functionality encompassed by the use cases in this section.

[20] Implementation Guidance will be developed following the initial release of the FICAM Roadmap and Implementation Guidance.

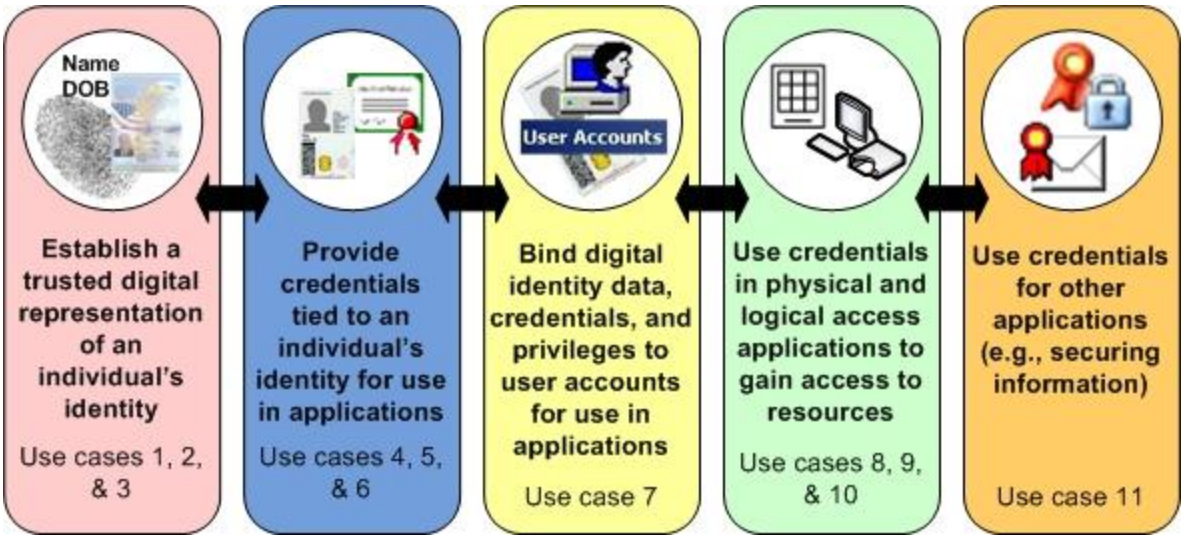

Figure 14: Use Case Functional Overview

While each use case describes a particular ICAM business function, the use cases are highly interrelated. The narrative in each section notes where a use case relies on steps completed as part of another use case or where the functions described currently overlap. The use cases were divided based upon logical stops in process in the as-is state or where a process distinction is intended in the target state analysis. The activities and technologies represented in the use cases have been generalized to maximize applicability across agencies. The use cases note where assumptions were made in order to address the challenge of describing ICAM business functions and the supporting architecture in a way that is general enough to be applicable government-wide but meaningful enough to drive architectural changes for the target state vision. It is expected that target state capabilities, including the use of PIV and PKI credentials, will be integrated into all new ICAM systems/applications.

Many lower level functions and detailed use cases that may be more agency-specific are not addressed in this architecture, as agencies are expected to perform similar analysis on their systems and processes. It is envisioned that the ICAM use cases can be paired together and detailed further to support specific agency use case scenarios, as shown in the following example: a local police officer who possesses a PIV-interoperable First Responder Access Card (FRAC) arrives at a disaster site that has been secured by the Federal Emergency Management Agency (FEMA) to provide assistance. A perimeter security guard authenticates the police officer's FRAC using a handheld device and grants access to the restricted area based on successful authentication and a comparison of the police officer's identity attributes against the access policy.

These use cases are meant to encompass daily functionality as they relate to ICAM systems within federal agencies. However, additional steps are needed to implement systems and procedures such that the target state processes described in this chapter can be realized. Actions and procedures that are required prior to the target steady-state include, but are not limited to, establishing access rules, provisioning workflows, database inventories and linkages, authoritative data sources, centralized role and/or attribute based access control systems, and a federation model. These activities, along with timelines and performance metrics, are described further in Chapter 5. Examples of scenarios that show how many of these use cases may fit together in real world scenarios are found in Section 4.12. An agency may find itself closer to the

target state than the as-is. In these cases, the agency has implemented processes that will make its transition to the target state easier and can expect to surpass the recommended timelines as outlined in Chapter 5.

4.1. Create and Maintain Digital Identity Record for Internal User

This use case provides the high-level process steps for establishing a digital identity for an internal user and modifying the digital identity record over time as the user's attributes change. Internal users are those who are primarily affiliated with the agency performing the process defined in the use case. They are typically employees, contractors, or affiliates for whom the agency is responsible for vetting and/or maintaining authoritative identity data. The creation of a digital identity for internal users is typically tied to an employee or contractor on-boarding process, initiated when an individual becomes affiliated with an agency. A digital identity is an electronic representation of an individual that is composed of identity attributes, commonly biographic and biometric data elements. 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 linked and shared with other systems separate from the creation of a particular user account or the assignment of privileges typically performed as part of provisioning processes (Use Case 7). In the as-is state, however, creation of an identity record, credentialing, and provisioning are often tightly bound processes.[21]

4.1.1. As-is Analysis

This use case describes the processes of capturing data to identify an individual within a system of digital identity records. Personal data is used to create a digital identity record, which can be used as a proxy for a person's true identity within IT systems. Once a record is established within a system, one benefit inherent to the management of identities is its segregation of people and things into classes or groups, to which policies may be applied or conclusions drawn. There are many ways to classify attributes, and some common elements associated with a digital identity include:

- **Identity attributes.** Data that help uniquely describe an identity such as name, eye and hair color, place of birth, etc.
- **Biographic attributes**. Contact information such as address, phone number, or e-mail address that is affiliated with an individual.
- **Context-specific attributes.** Data that are only used in a specific context 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.** Biological and behavioral attributes, such as facial image, fingerprints, voice recognition, or other forms of biometrics.
- **Credentials.** An object that may be presented by an individual, system, or object to prove the authenticity of an identity claim. This includes a password, digital certificate, or ID card 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).

[21] It is important also to note that creating and using a core record for individuals across an enterprise will require the application of all appropriate privacy and security controls, especially when transmitting personally identifiable information across system boundaries. These controls are discussed in greater detail in Part B of this document.

In the as-is state, digital identity record creation is generally accomplished through independent means in numerous diverse systems with no reliable synchronization of identity data, which can lead to inefficiencies and even security problems. There is typically no minimum set of data required within an organization to provide for uniqueness or enable disambiguating 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.** The current processes and systems often require manual attribute updates within multiple systems, creating a large administrative burden for identity record maintenance.
- **Identity data accuracy.** Identity information is often duplicated across multiple systems. Records can easily get out of sync when updates are performed in one system but not the others, resulting in conflicting records for an individual across the enterprise.
- **Data security.** Maintaining the same identity information in multiple systems increases the possibility of exposure of the information.
- **Lack of integration.** A given user's attributes, credentials, and privileges are often distributed across multiple identity systems that are not linked, preventing a complete view of an individual's authoritative identity attributes and the ability to share identity data within or outside the enterprise. The lack of coordination across systems also increases the risk associated with failing to terminate all associated accounts upon user separation from the organization, a common IG finding.

Key assumptions for this use case include:

- Identity Proofing, Adjudication and Background Checks, which include vetting of individuals against claimed identity, validation of an Applicant's eligibility for access to government resources, and completion of the security clearance process (as applicable), is completed outside of this use case. Identity Proofing enables a level of trust that identity records are properly assigned to the right individuals, and is closely tied to identity record creation. Background Checks, on the other hand, provide information such that an eligibility determination may be made.
- Identity records deletion processes are governed by mission and other agency policies, and cannot be uniformly described in this use case. Record retention policies and practices must comply with all federal laws and regulations, including privacy laws and statutes.
- The identity record creation process steps generally align across agencies based on personnel type (employee, contractor, or affiliate). Differences based on personnel type have been noted within the process flow.

4.1.1.1. Process Flow

The as-is steps for this use case are broken into two different paths: 1) create a new identity record and 2) change an existing identity record.

Part 1: Create a new identity record

1. An individual becomes affiliated with an agency via the on-boarding process. An on-boarding package is created from various requests for information (either paper-based or electronic) from the individual.
2. The on-boarding package is provided to a Data Administrator or Authorized User for each of the applicable systems that store digital identity records within the agency. The

Data Administrator or Authorized User creates a record for the individual that includes the data elements applicable to the respective system. Digital identity records are typically created separately by different Data Administrators across the systems shown in the following table:[22]

System Type	Identity Data Stored	Internal User Type
HR System	Biographical, affiliation, citizenship, benefits	Employee
Personnel Security System[23]	Biographical, suitability, security/clearance (if applicable), biometric, role	Employee, Contractor, Affiliate
Payroll System	Biographical, role, salary	Employee
Contract/Contractor Management System	Biographical, affiliation, citizenship, contract data	Employee, Contractor
Physical Access Control System	Biographical, affiliation, security/clearance, biometric, role, credential	Employee, Contractor, Affiliate
Logical Access Control System	Biographical, security, biometric, PIN	Employee, Contractor, Affiliate

Figure 15: Identity Record Creation by System and User Type

Part 2: Change an existing identity record

1. Data Administrator(s)/Authorized User(s) receive a notification or request to update an individual's identity record. Attribute changes that might trigger a record update include changes in biographical information (such as name), affiliation, citizenship, clearance level, and work location. If an attribute change is initiated in one system, it does not necessarily mean that the change will be initiated in other systems affected by the change.
2. The appropriate Data Administrator/Authorized User verifies the attribute change per agency policy and updates the affected identity attributes in the appropriate system. More than one Data Administrator is typically responsible for manually updating identity data where it is stored in multiple, unlinked systems.
3. The identity record is maintained for the required time period and deactivated or flagged as needed.

4.1.1.2. Architecture Analysis

The following table provides details for the Business, Data, Service, and Technology Layers of the ICAM segment architecture in support of this use case in the as-is state. An overview of the segment architecture layers can be found in Chapter 4.

[22] Please note that an agency may categorize users into many different types, some systems may manage multiple user types, and an individual may be classified into more than one category.

[23] HR systems may also commonly include security clearance information; agencies may have one database to support Personnel Security and HR data.

Architecture Layer	Architecture Details

Business	• **E-Government Alignment:** IEE
	• **Trigger:**
	  ○ Part 1: An individual becomes affiliated with an agency
	  ○ Part 2: An individual's identity data changes, requiring an update to his digital identity record
	• **Actors:** Individual/Internal User, Data Administrator, Authorized User
	• **Endpoints:**
	  ○ Part 1: Identity record created
	  ○ Part 2: Change made to identity record

Data	**Data Elements** • Identifier • Core attributes • Context specific attributes • Affiliations • Biometrics • Role info • Benefit data • Salary data • Clearance/Suitability/Fitness/Credential Eligibility data • Contract data **Data Repositories/Systems** • HR System • Personnel Security System • Payroll System • Contract/Contractor Management System • eVerify • PACS • LACS • Other agency systems
Service	• Digital Identity Lifecycle Management • Linking/Association
Technology	**Hardware/Software** • Database Management System (DBMS), servers to support systems • Directory Services • USAJobs (portal software) • Electronic Questionnaires for Investigations Processing (e-QIP) (portal software) **Standards** • eXtensible Markup Language (XML)

Figure 16: Use Case 1 As-is Architecture Details

4.1.2. Target Analysis

The underlying business need and function for creating and maintaining digital identity records for internal users remain the same in the target state; however, 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 in an automated fashion with other systems across the enterprise. In this vision, a core identity record is established in a single authoritative repository. Application-specific credentials and role information or privileges are decoupled from the core identity record and are applied as needed via provisioning workflows for individual applications (as described in Use Case 7). This distinction allows for streamlined management of digital identity information.

In order to support the target vision, the process flows in this section reflect the following architectural changes:

- Developing a common, government-wide specification for the minimum set of core attributes that comprise a digital identity record for an internal user.
  - These attributes may tend to be static in nature and not subject to frequent changes.
  - Establishing unique user profiles will require agencies to employ a methodology to deterministically establish unique records, including establishing data quality and transformation services to clean up low quality data.
  - Agencies must establish a way for the core identity store to be configured so that representatives from each of these systems can create, update, or delete the appropriate attributes as needed.
- Establishing a mechanism by which the authoritative identity data to be shared from core data repositories is utilized across the enterprise.
  - In the case of core digital identity attributes, all systems should be automatically provisioned from the core identity repository. A fully compliant system will provide an authoritative view of an individual's identity for all core attributes.
  - In the case of peripheral attributes, such as training certifications, an automated service such as a direct connection between systems or an AAES should allow for the linking of these attributes to any systems or services that may require them.
- Enabling interoperability between systems by establishing or leveraging existing data standards.
- Minimizing paper-based processes for collecting and sharing data that is used to create a digital identity record.

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

- Data is exchanged electronically, and authoritative data sources have been identified for each of the core identity attributes identified in the planned digital identity specification.
- Data that was formerly managed in paper-based systems will have appropriate auditing and archiving standards now that the data is stored electronically.
- Workflows for the appropriate sharing of identity data within the digital identity record creation and maintenance processes have been established in advance of the start of the process flows described.

4.1.2.1. Process Flow

The target steps for this use case are broken into two different paths: 1) create a new identity record and 2) change an existing identity record.

Part 1: Create a new identity record

1. An individual becomes affiliated with an agency via the on-boarding process. An on-boarding package is created based upon information provided by the individual on standardized, electronic forms.
2. The on-boarding package is provided electronically to a Data Administrator or Authorized User for an authoritative identity data repository. The Data Administrator or Authorized User authenticates to the system, and then creates a record for the individual

that includes the data elements applicable to the respective system. In cases where a digital identity record exists for a user in another system, the digital identity record may be automatically populated with data shared using the AAES.

3. Upon completion of the identity record creation process, core identity attributes in the record may be made available via the AAES to one or more additional systems based on the agency's architecture. This step is often tied closely to provisioning (see Use Case 7).

An alternative mechanism to create a digital identity record for an individual is to leverage information already established about an individual from outside sources. The process flow in this case would mirror the processes outlined in the target state of *Use Case 2: Create and Maintain Identity Record for External User*.

Part 2: Change an existing identity record

1. A request is initiated to change an individual's digital identity record or the changes are made directly using one of the following methods:
   a. The Data Administrator/Authorized User receives an electronic notification or request to update an individual's identity record. The Data Administrator/Authorized User logs into the system and verifies the attribute change per agency policy and updates the affected identity attributes in the appropriate system.
   b. The individual logs into the system and updates his own identity data in the affected system where this is allowed and available via a self-service interface.
   c. The record change is triggered and completed automatically based upon workflows established within the agency.
2. The updated identity attribute(s) are made available to affected systems via direct connection or an AAES.
3. The identity record is maintained for the required time period and deactivated or otherwise flagged.

The figure below shows the data interchanges and information flow as described in the processes outlined above. The hexagonal figures represent the various services that are employed throughout the process. Repositories and actors are also depicted. This graphical depiction of the process should illustrate the architecture needed to support this target state use case.

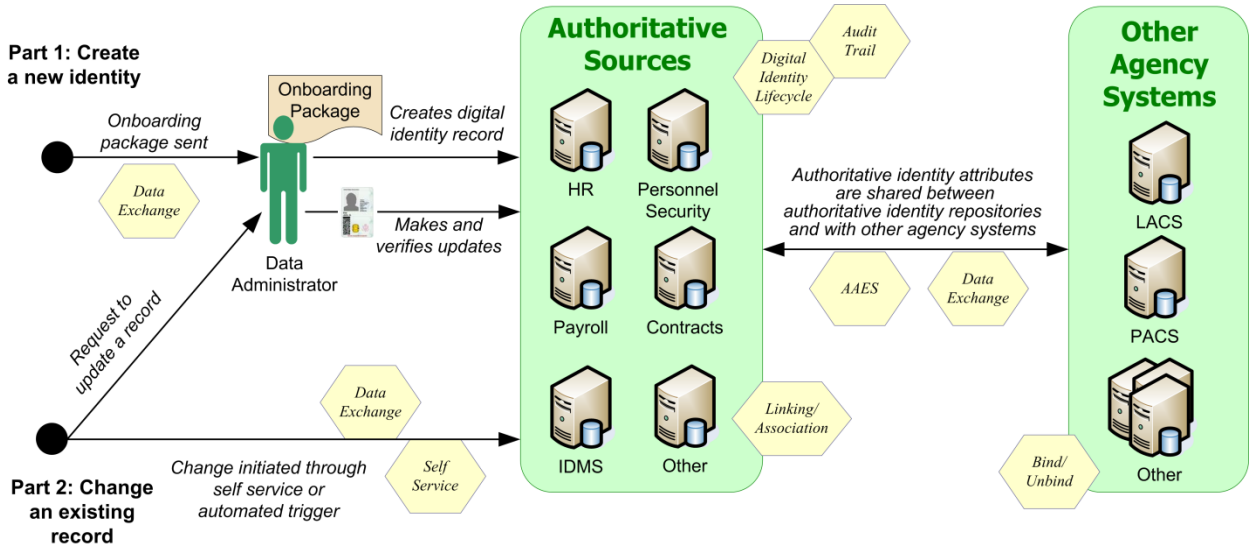

Figure 17: Use Case 1 Target Process Diagram

4.1.2.2. Architecture Analysis

The following table provides details for the Business, Data, Service, and Technology Layers of the ICAM segment architecture in support of this use case in the target state. An overview of the segment architecture layers can be found in Chapter 4.

Architecture Layer	Architecture Details

Business	• **E-Government Alignment:** IEE
	• **Trigger:**
	  ○ Part 1: An individual becomes affiliated with an agency
	  ○ Part 2: An individual's identity data changes, requiring an update to his digital identity record
	• **Actors:** Individual/Internal User, Data Administrator, Authorized User
	• **Endpoints:**
	  ○ Part 1: Identity record created
	  ○ Part 2: Change made to identity record

Data	**Data Elements** • Identifier • Core attributes • Context specific attributes • Affiliations • Biometrics • Role info • Benefit data • Salary data • Clearance/Suitability/Fitness/Credential Eligibility data • Contract data **Data Repositories/Systems** • HR System • Personnel Security System • Payroll System • Contract/Contractor Management System • PACS • LACS • Other agency systems

Architecture Layer	Architecture Details
Service	• Authoritative Attribute Exchange • Digital Identity Lifecycle Management • Linking/Association • Data Exchange • Bind/Unbind • Self-Service • Audit Trail
Technology	**Hardware/Software** • DBMS, servers to support systems • Directory Services • USAJobs (portal software) • e-QIP (portal software) **Standards** • XML • Simple Object Access Protocol (SOAP) • REST • SSL • SAML 2.0

Figure 18: Use Case 1 Target Architecture Details

4.1.3. Gaps

This section provides a summary of the high-level gaps between the as-is and target states for this use case. Gaps may focus on Data, Technology, Business and/or Service Layer activities. Explanations about the drivers and impact of each gap are also provided.

- **No common definition or data specification identifying the minimum data elements for creating and sharing digital identity data.** A digital identity data specification will help minimize duplicate entries based on mismatched information for a single individual. The standard will also help streamline the manner in which users can be provisioned into systems.
- **Need for common definitions of additional identity attributes required for mission-specific functions.** In addition to core data elements, other common identity attributes should be standardized, and methods should be adopted to translate local data to the standardized set in order to enable data sharing across agencies. This set of data may be considered mission-specific and may be identified by the communities of interest that will share it. In particular, standardizing attributes used to make authorization decisions has the potential to greatly reduce costs.
- **Inability to correlate and synchronize digital identity records and automatically push and pull identity data between systems.** A service such as the AAES and/or a set of common interconnections must be developed to index and link authoritative sources of core identity data and peripheral data such that it may be collected once and shared many times across applications.
- **Lack of authoritative sources for contractor/affiliate identity data.** Identity information is not collected centrally for agency contractors and other tightly affiliated personnel that are not employees. The lack of authoritative sources for this data can cause security risks such as improper overlapping responsibilities, lack of deprovisioning, and also cause inefficiencies when contractors work on multiple contracts within an agency or across multiple agencies.

- **Prevalence of redundant collection and management of digital identity data for a single user.** Attributes are currently collected and stored in multiple locations, sometimes within a single application. Data should be collected as infrequently as possible, and the information should be linked 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

This use case 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 of a state, local, or tribal government; or an individual external to the Federal Government. This use case does not attempt to standardize or centralize the processes within individual missions, which would violate security and privacy tenets. Despite its complexity, this use case has been included to address increasing interest in managing digital identity for individuals outside an agency in order to build a foundation for secure, efficient, and transparent electronic interactions with these external sectors.

4.2.1. As-is Analysis

The process for creating a digital identity record in the as-is state is tied closely to the process for credentialing (described in Use Case 6) and the process for provisioning (described in Use Case 7), largely because digital identity records typically are created for external users for the purpose of obtaining a user account and associated credential to access that user account within a mission-specific application. Information is collected from users during various mission focused activities, irrespective of where that information may have been collected and stored for the same individual previously. These distributed interactions require that the user enter or update identity data manually across numerous diverse systems.

Current challenges associated with the as-is model include:

- There is no agreed upon data model within most mission segments that constitutes an identity or the way in which that information should be formatted and transmitted.
- Mission-related data (e.g., tax ID number for the IRS) are commonly used to verify individuals for their access credentials through each individual application. As a result, records are not linked to authoritative sources and multiple records for an individual exist within each agency and across the federal enterprise. In addition, these records are not always up-to-date or accurate as they are not maintained equally across the enterprise.

A key assumption for this use case is that the preservation, privacy, and protection of personal information is paramount in order to maintain public confidence in the security of the government's electronic information and information technology. This confidence is essential to adoption and use of E-Government services.

4.2.1.1. Process Flow

The as-is steps for this use case are broken into two different paths: 1) create a new identity record and 2) change an existing identity record.

Part 1: Create a new identity record

1. An Applicant for a government service requests an account and provides identity information to an application, usually accessible via the Internet.
2. The mission application/service collects and stores the identity information in a record for the individual. In some cases, this process may require that the record be created by an Application Administrator or that the request for an account follow an approval workflow before it is created.
3. The identity information may be checked against other data repositories.
4. Identity information is used to establish a user account and associated login credentials to the mission application.

Part 2: Change an existing identity record

1. The user requests an update to personal information via website or helpdesk, presenting existing credentials as needed.
2. The Application Administrator verifies the requested update, where applicable (e.g., name change with the Social Security Administration, change in school affiliation and student status with the Department of Education).
3. The Application Administrator updates the user's identity attributes in the appropriate application/service. Alternatively, the user may update his own digital identity record within the application, where permissible.
4. The identity record is maintained for the required time period and then and deactivated or otherwise flagged.

4.2.1.2. Architecture Analysis

The following table provides details for the Business, Data, Service, and Technology Layers of the ICAM segment architecture in support of this use case in the as-is state. An overview of the segment architecture layers can be found in Chapter 4.

Architecture Layer	Architecture Details

Business	• **E-Government Alignment:** IEE, G2G, G2C, G2B
	• **Trigger:**
	  ○ Part 1: Applicant requests account for government application
	  ○ Part 2: User requests update to digital identity record attribute(s)
	• **Actors:** Applicant/User, Application Administrator
	• **Endpoint:**
	  ○ Part 1: Identity record created
	  ○ Part 2: Change made to identity record

Data	**Data Elements** • Identity data • Mission-specific data **Data Repository/System** • Agency applications
Service	• Digital Identity Lifecycle Management • Linking/Association • Self-Service • Identity Proofing

Architecture Layer	Architecture Details
Technology	**Hardware/Software** • DBMS • Mission applications • Directory Services **Standards** • XML

Figure 19: Use Case 2 As-is Architecture Details

4.2.2. Target Analysis

In the target state, many mission-specific external facing applications likely will 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 what information is collected to minimize the gathering of unnecessary data and 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).

In addition, specific Communities of Interest may establish common formats for common fields to enable interoperability for users when using a single credential to access several of their accounts. Adjustments needed in the target state include translating to common data formats and exploring opportunities for automation. Links to external systems may also be required in order to utilize 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.

Based upon the work by ongoing federal initiatives, this use case assumes that the acceptance of third-party identity credentials for external users will create opportunities to minimize the number of external user identity data records and the types of data kept for external users. It also assumes that the process for linking records is accomplished according to best practices, with the individual in question positively identified to the same degree in both repositories to maintain data integrity.

4.2.2.1. Process Flow

The target steps for this use case are broken into two different paths: 1) create a new identity record and 2) change an existing identity record.

Part 1: Create a new identity record

1. An Applicant for a government service requests an account for an application, usually accessible via the Internet.
2. The mission application/service collects and stores the identity information in a record for the individual. In some cases, this process may require that the record be created by an Application Administrator or that the request for an account follow an approval workflow before it is created. In cases where a digital identity record exists for a user in another system, the digital identity record may be automatically populated with data shared using the AAES.
3. The identity information may be checked against other data repositories.

4. Users may choose to associate credentials issued from a trusted partner with their new agency identity during the record creation so they can be used in future transactions.

Part 2: Change an existing identity record

1. A request is initiated to change an individual's digital identity record or the changes are made directly using one of the following methods:
    a. The Application Administrator receives an electronic notification or request to update an individual's identity record. The Application Administrator verifies the requested update per agency policy, and may require authentication using a credential associated with the user account, and processes and updates the affected identity attributes in the appropriate system. (This process could be wholly automated as well.)
    b. The individual updates his own identity data in the affected system where this is allowed and available via a self-service interface, which may also require associated credentials to be verified.
    c. The record change is triggered and completed automatically based upon workflows established within the agency.
2. The identity record is maintained for the required time period and then is deactivated or otherwise flagged.

The figure below shows the data interchanges and information flow as described in the processes outlined above. The hexagonal figures represent the various services that are employed throughout the process. Repositories and actors are also depicted. This graphical depiction of the process illustrates the architecture needed to support this target state use case. In this use case, the Application Administrator role may be wholly automated based on business rules, depending on the nature of the attribute and the type of repository in which it is stored.

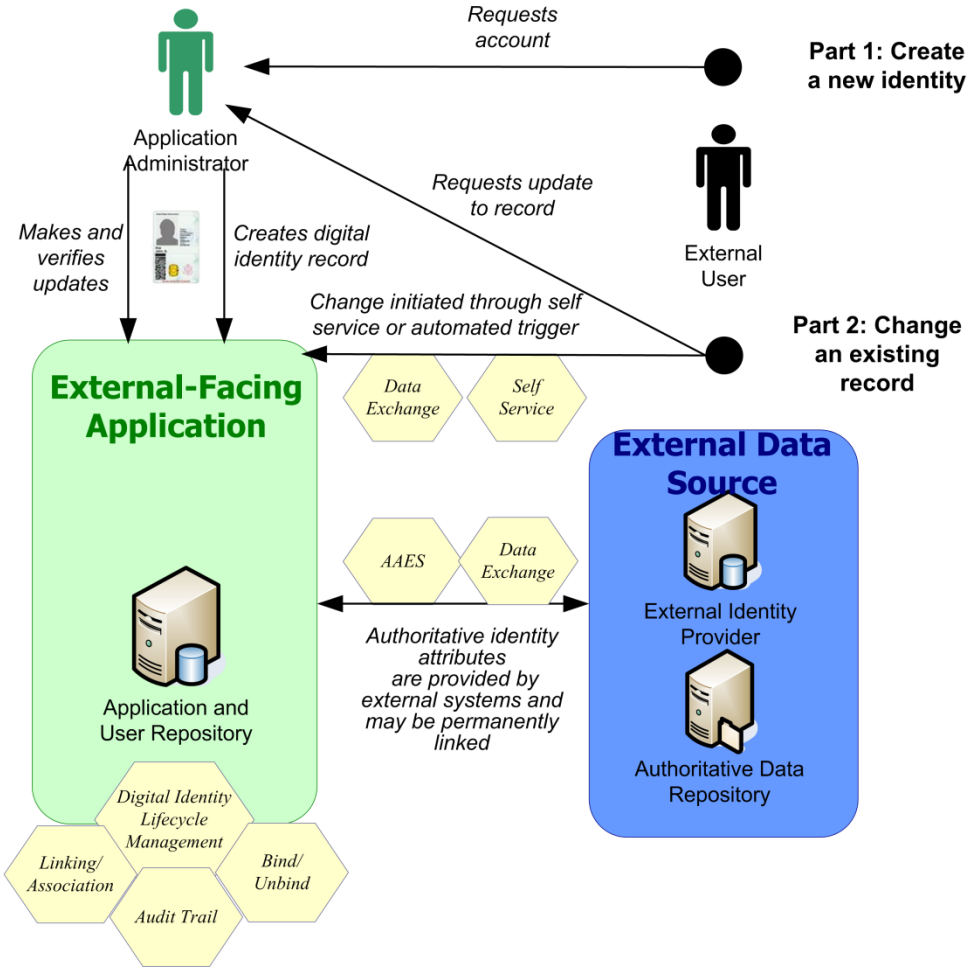

Figure 20: Use Case 2 Target Process Diagram

4.2.2.2. Architecture Analysis

The following table provides details for the Business, Data, Service, and Technology Layers of the ICAM segment architecture in support of this use case in the target state. An overview of the segment architecture layers can be found in Chapter 4.

Architecture Layer	Architecture Details
Business	• **E-Government Alignment:** IEE (in the case of conditional hires or job applicants), G2G, G2C, G2B • **Trigger:** ○ Part 1: Applicant requests account for government application ○ Part 2: User requests update to digital identity record attribute(s) • **Actors:** Applicant/User, Application Administrator • **Endpoint:** ○ Part 1: Identity record created ○ Part 2: Change made to identity record

Architecture Layer	Architecture Details
Data	**Data Elements** • Identifier • Core attributes • Context specific attributes • Affiliations **Data Repositories/Systems** • Mission delivery applications (e.g., grant/loan applications) • Other agency systems
Service	• Digital Identity Lifecycle Management • Linking/Association • Bind/Unbind • Self-Service • Data Exchange • Authoritative Attribute Exchange • Audit Trail
Technology	**Hardware/Software** • DBMS • Directory Services • OCSP/CRL/SCVP **Standards** • XML • SSL • X.509

Figure 21: Use Case 2 Target Architecture Details

4.2.3. Gaps

This section provides a summary of the high-level gaps between the as-is and target states for this use case. Gaps may focus on Data, Technology, Business and/or Service Layer activities. Explanations about the drivers and impact of each gap are also provided.

- **Need for common definitions of additional identity attributes required for mission-specific functions.** In addition to core data elements, other common identity attributes should be standardized and methods should be adopted to translate local data to the standardized set in order to enable data sharing across agencies. This set of data may be considered mission-specific and may be identified by the communities of interest that will share them.
- **Prevalence of redundant collection and management of digital identity data for the same user.** Agencies should identify opportunities to leverage existing agency data sources for external users and minimize duplicative data collection across agency applications that service external communities.
- **Need for a capability to bind third party credentials to an external user's identity record.** The creation and vetting of digital identities must be distinct from the creation of external user credentials. Linking digital identity records of external users to externally issued credentials can enable access applications using third party credentials. However, currently, there is no mechanism for a user to select which credential provider he or she would like to use, nor is there a mechanism to link that credential record with the newly created identity record within an agency.

4.3. Perform Background Investigation for Federal Applicant

This use case provides the high-level process steps for conducting a background investigation for a federal employee, contractor, or affiliate. The background investigation often results in a determination of suitability/fitness for federal employment or fitness to perform work as a contractor. In order to maintain applicability across all agencies, this use case focuses on the common aspects of background investigations processed by OPM on behalf of an agency. Agencies should refer to the OPM guidance for information related to a specific investigation type or process. 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.

Certain terms are used in this use case and throughout this document to describe personnel investigation activities that are conducted for a variety of purposes. As such it is important to have an understanding of the terminology and its proper usage. The table below provides official definitions for common terms related to personnel and security investigations.

Term	Definition
Adjudication[24]	Evaluation of pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether a covered individual is: • suitable for Government employment; • eligible for logical and physical access; • eligible for access to classified information; • eligible to hold a sensitive position; or • fit to perform work for or on behalf of the Government as a contractor employee.
Credentialing Determination	Determination of whether or an individual is eligible[25] to receive a PIV credential as either a federal employee or contractor. A PIV credential must be issued following the control objectives and PIV Identity Proofing and Registration Requirements in NIST FIPS 201 Section 2, and additional OPM requirements as applicable: The process shall begin with the initiation of the OPM required background investigation. To issue a PIV credential, the background investigation paperwork must be submitted to OPM and be in-process, the FBI National Criminal History Check (fingerprint check) must be completed, and the applicant must provide two forms of identity source documents included in the Form I-9, at least one of which is a valid Federal or State government-issued picture identification. 2. A final credentialing decision is made following completion and adjudication of the required investigation, or verification that a background investigation (meeting the minimum standard or higher) has already been completed.
Suitability Determination[26]	A decision by OPM or an agency with delegated authority that a person is suitable or is not suitable for employment in the competitive service, in the excepted service where the incumbent can be noncompetitively converted to competitive service, or career appointment in the Senior Executive Service
Fitness Determination	A decision by an agency that an individual has or does not have the required level of character and conduct necessary to perform work for or on behalf of a Federal agency as an employee in the excepted service (other than in an excepted service position where the incumbent can be noncompetitively converted to competitive service) or as a contractor employee.
Security Clearance	Determination of whether or not an individual is eligible for access to sensitive or classified

[24] As defined in Executive Order 13467, The White House, June 30, 2008.

[25] This document uses the term eligibility to describe an individual's eligibility to receive a PIV credential

[26] As defined in the Code of Federal Regulations, Title 5 Volume 2, Government Printing Office, January 1, 2005.

Term	Definition
Determination	information.[27]

4.3.1. 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 due to a lack of electronic interfaces and agency-specific processes,
- Redundant and stove-piped information collection,
- No direct link between FBI National Criminal History Fingerprint Check and PIV credentialing process,
- No direct link to other ICAM systems or use cases,
- Specialized or non-standard investigations[28] engender little trust or reciprocity across agencies, and
- A long delay between the initiation of a background investigation[29] and its adjudication due in part to agency-specific processes and a lack of technical interfaces between agency applications.

Key assumptions for this use case include:

- Agency-specific processes or requirements that are not common across government are considered outside the scope of this use case.
- Completion of the security clearance process (as applicable) is considered outside the scope of this use case.
- The completion of background investigations is considered within the scope of the ICAM segment architecture as it provides the basis for trust in a digital identity of an individual and helps define eligibility for specific privileges that may be assigned for access to resources.
- Background investigations for individuals outside of the Federal Government are considered outside of the scope of this use case.

4.3.1.1. As-is Process Flow

This use case includes the following steps:

1. An Applicant is selected for employment with or to perform contract work for an agency, triggering the need to perform a background investigation.
    a. For Employees, an Agency Representative (usually from HR or Personnel Security) initiates the background investigation process during on-boarding.

[27] "Classified information" means information that has been determined pursuant to Executive Order 12958 of April 17, 1995, as amended, or a successor or predecessor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.) to require protection against unauthorized disclosure.

[28] OPM determines the minimum investigation required to support reciprocity, and currently conducts the NACI as the minimum standardized investigation for PIV credential applicants.

[29] Based upon GAO-07-842T, Delays and Inadequate Documentation Found for Industry Personnel, GAO, May 2007.

b. For Contractors, a Contracting Officer (CO), Contract Officer's Technical Representative (COTR), or Program Officer (PO) triggers the background investigation, often in conjunction with the Facility Security Officer (FSO) of the applicable contracting firm via a paper-based process once an Applicant has been selected to support a particular contract.

2. The Agency Representative determines whether a current background investigation is available for the Applicant in the Clearance Verification System (CVS) or other background investigation systems. If a background investigation has already been conducted, the use case follows Process A; if not, the use case follows Process B.

Process A: A background investigation has already been completed and is current:

1. The Agency Representative contacts the Agency Representative at the agency that conducted the investigation via phone or email to confirm the adjudication results of the background investigation.
2. If the investigation is current, complete, meets appropriate criteria, adjudication results were favorable, and a PIV was issued, the Agency Representative honors reciprocity of the background investigation and the investigative requirement is met. If the adjudication results were unfavorable and the applicant was previously denied a PIV, the Agency Representative may exercise discretion to deny a PIV. If the applicant is subsequently granted a security clearance, found suitable for the competitive service, or found fit for excepted service or contract employment, the agency should re-adjudicate PIV eligibility based on government-wide standards. Reciprocity of background investigations across agencies is not always enabled, resulting in new investigations for individuals who already have a current investigation on file.

Process B: a new background investigation must be conducted:

1. If a new investigation is conducted, data is collected from the Applicant using paper and electronic tools.
   a. The Applicant completes the appropriate OMB-approved form to provide the required background information. This paper form is submitted to the security officer responsible for the investigation.
   (or)
   b. The Applicant enters data into the Electronic Questionnaires for Investigations Processing (e-QIP). Data is sent to the appropriate authorities for both manual and electronic verification. These authorities include FBI, OPM, or other investigative bodies.
2. The Applicant's fingerprint samples are taken. In many as-is systems, this process is done via ink cards that are scanned into an electronic format. Alternatively, some agencies use electronic fingerprint capture devices.
3. The fingerprint samples are sent to FBI or OPM to check for criminal history in the IAFIS. FBI accepts flat or rolled fingerprint sample submissions, while OPM accepts only rolled fingerprint samples.
4. Results from the fingerprint check are returned electronically to the system that initiated the request.

5. The Investigative Service Provider performs other checks as needed and sends the results of the investigation to the agency.
6. An agency Adjudicator adjudicates the results of the investigation to determine the eligibility of the Applicant against standard criteria. All results generated are documented.
7. The Agency Representative submits the adjudication results of the completed background investigation to the PIV Registrar to support PIV credentialing.

4.3.1.2. Architecture Analysis

The following table provides details for the Business, Data, Service, and Technology Layers of the ICAM segment architecture in support of this use case in the as-is state. An overview of the segment architecture layers can be found in Chapter 4.

Architecture Layer	Architecture Details
Business	• **E-Government Alignment:** IEE • **Trigger:** An Applicant needs a background investigation due to the Applicant's status as a federal employee or contractor. • **Actors:** Applicant, Agency Representative, Investigative Service Provider (ISP), Adjudicator • **Endpoint:** A background investigation has been completed and adjudicated.
Data	**Data Elements**[30] • Applicant biographic data • Applicant employment history for previous 5 years • Applicant education attained during previous 5 years including highest degree verified • Applicant place of residence for previous 5 years • Applicant Citizenship status • Applicant references • Applicant law enforcement check for previous 5 years • Applicant NACs • Applicant fingerprint samples • Agency data **Data Repositories/Systems** • CVS • Personnel Investigations Processing System (PIPS) • JPAS • FBI IAFIS • Fingerprint Transaction System (FTS) • Agency HR database • Agency Personnel Security database • Other agency-specific databases
Service	• Adjudication • Digital Identity Lifecycle Management

[30] Data elements referenced here are provided as examples only. Specific data required will vary based on the type of investigation and the applicant.

Architecture Layer	Architecture Details
Technology	**Hardware/Software** • e-QIP • DBMS, servers for core systems **Standards** • FIPS 201 • ANSI/NIST-ITL 1-2000

Figure 22: Use Case 3 As-is Architecture Details

4.3.2. 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. The Applicant's biometric sample must positively match with the biometric reference sample that was previously submitted and stored on the credential used to determine eligibility. The Applicant's trial biometric sample(s) can be compared to the entire biometric reference database to ensure that the applicant is not already in the database and associated with a different identity.
- Reducing or eliminating paper application forms and manual processes in favor of automated systems.
- Sharing information between related databases to reduce administrative burden on Applicants, especially when updating background information or transferring between departments or agencies.
- Making background investigation result information available to agencies (based upon an authorized need to access it) with sufficient detail in order to honor reciprocity of a background investigation completed by another agency.
- Utilizing the planned capability within CVS to view background investigation adjudication result in order to streamline the process for honoring reciprocity of an existing investigation.

4.3.2.1. Process Flow

1. An Applicant is selected for employment with or to perform contract work for an agency, triggering the need to perform a background investigation.
   a. For Employees, an Agency Representative (usually from HR or Personnel Security) initiates the background investigation process during on-boarding.
   b. For Contractors, a Contracting Officer (CO), Contract Officer's Technical Representative (COTR), or Program Officer (PO) triggers the background investigation, often in conjunction with the Facility Security Officer (FSO) of the applicable contracting firm, via a standardized electronic process once an Applicant has been selected to support a particular contract.
2. The Agency Representative determines if a current background investigation is available for the Applicant in the CVS and other background investigation systems. If a

background investigation has already been conducted, the use case follows Process A; if not, the use case follows Process B.

Process A: A background investigation has already been completed and is current:

1. The Agency Representative confirms the adjudication results of the background investigation in CVS. (Contractors will be required to have their background investigation status available for searching to authorized personnel.)
2. If the investigation is current, complete, meets appropriate criteria, adjudication results were favorable, and a PIV was issued, the Agency Representative honors reciprocity of the background investigation and the investigative requirement is met. If the adjudication results were unfavorable, the Agency Representative may exercise discretion to deny a PIV. If the applicant is subsequently granted a security clearance, found suitable for the competitive service, or found fit for excepted service or contract employment, the agency should re-adjudicate PIV eligibility based on government-wide standards.

Process B: A new background investigation must be conducted:

1. The Agency Representative assigns employees and contractors a level of risk associated with their service function as it relates to their job duties as defined by OPM, and initiates the background investigation that is required at that risk level.[31]
2. The Applicant enters data into e-QIP. Data is sent to the Investigative Service Provider for both manual and electronic verification. ISPs can include FBI, OPM, other investigative bodies or designees.
3. The Applicant's fingerprints are captured electronically using a PIV enrollment station.
4. The fingerprints are sent automatically along with any necessary biographic data to FBI or OPM to check for criminal history in the IAFIS and are linked up with the background investigation request and e-QIP data.
5. The Investigative Service Provider performs other checks as needed and sends the results of the investigation to the agency electronically.
6. An agency Adjudicator adjudicates the results of the investigation to determine the eligibility of the Applicant against standard criteria. All results generated are documented.
7. The Agency Representative submits the adjudication results of the completed background investigation to CVS and to the PIV Registrar to support PIV credentialing.

The figure below shows the data interchanges and information flow as described in the processes outlined above. The hexagonal figures represent the various services that are employed throughout the process. Repositories and actors are also depicted. This graphical depiction of the process illustrates the architecture needed to support this target state use case.

[31] Federal risk levels and associated background investigations are currently being revised by OPM.

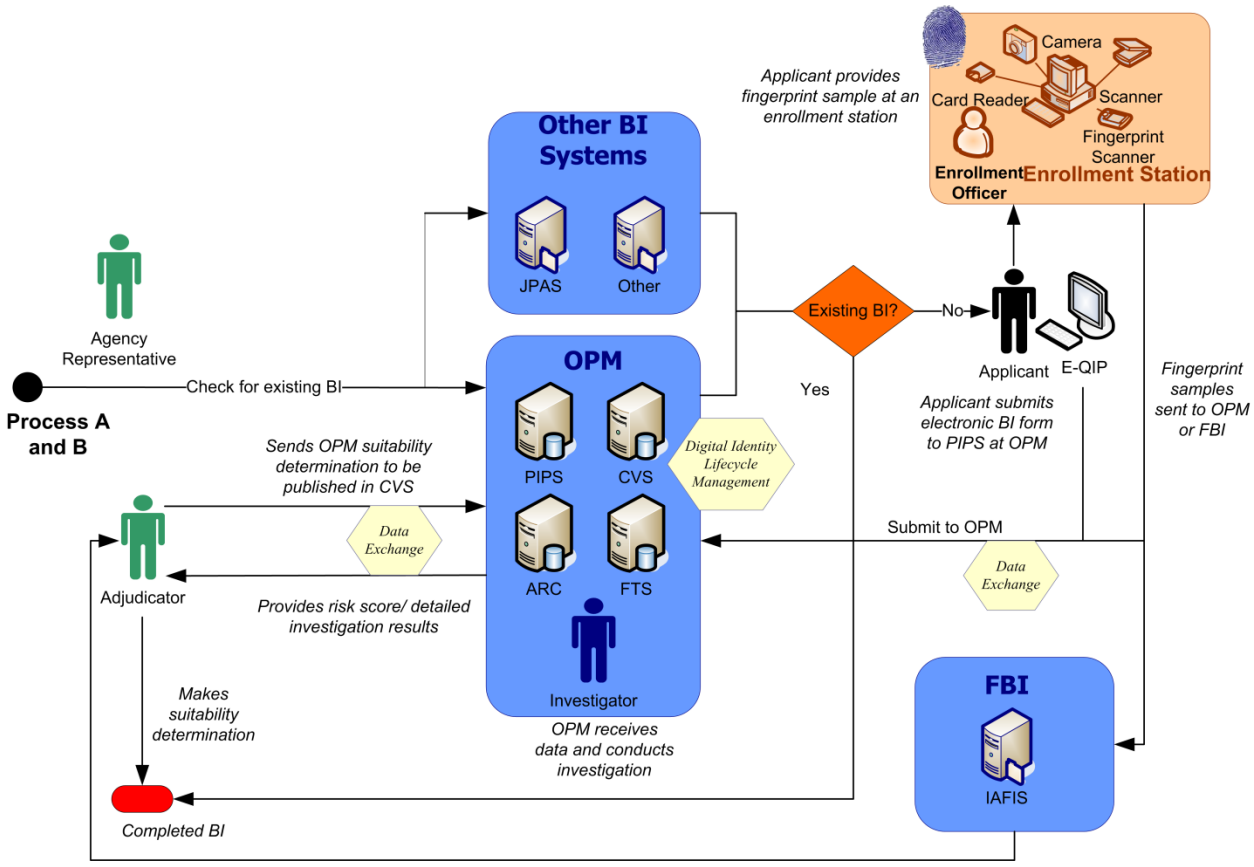

Figure 23: Use Case 3 Target Process Diagram

4.3.2.2. Architecture Analysis

The following table provides details for the Business, Data, Service, and Technology Layers of the ICAM segment architecture in support of this use case in the target state. An overview of the segment architecture layers can be found in Chapter 4.

Architecture Layer	Architecture Details
Business	• **E-Government Alignment:** IEE • **Trigger:** An Applicant needs a background investigation due to the Applicant's status as a federal employee or contractor. • **Actors:** Applicant, Agency Representative, Investigative Service Provider, Adjudicator • **Endpoint:** A background investigation has been completed and adjudicated.

Architecture Layer	Architecture Details
Data	**Data Elements** (can vary by the type of investigation required**)** • Applicant biographic data • Applicant employment history for previous 5 years • Applicant education attained during previous 5 years including highest degree verified • Applicant place of residence for previous 5 years • Applicant Citizenship status • Applicant references • Applicant law enforcement check for previous 5 years • Applicant NACs • Applicant fingerprint samples • Agency data **Data Repositories/Systems** • CVS • Central Contractor Registration (CCR) database • PIPS • JPAS • FBI IAFIS • Fingerprint Transaction System (FTS) • Agency HR database • Agency Personnel Security database • Other agency-specific databases
Service	• Data Exchange • Adjudication • Digital Identity Lifecycle Management
Technology	**Hardware/Software** • e-QIP • DBMS, servers for core systems **Standards** • FIPS 201 • SSL • ANSI/NIST-ITL 1-2000

Figure 24: Use Case 3 Target Architecture Details

4.3.3. Gaps

This section provides a summary of the high-level gaps between the as-is and target states for this use case. Gaps may focus on Data, Technology, Business and/or Service Layer activities. Explanations about the drivers and impact of each gap are also provided.

- **Lack of reciprocity in the acceptance of background investigations completed by or on behalf of another agency.** While the OPM Final Credentialing Standards[32] prescribe government-wide reciprocity requirements, agencies must work to honor reciprocity of background investigations to reduce costs and administrative burden, wherever possible.[33]
- **Need for common interface standards to conduct automated record checks.** Agencies should identify authoritative sources at the agency level and other cross-agency

[32] Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12, Office of Personnel Management, July 31, 2008.

[33] OMB memo (06-21) dictates certain goals for reciprocity.

repositories that must interface with internal authoritative repositories and ensure that common data standards are employed.

- **Lack of mapping between credential issuance and ongoing investigative results**. The ongoing validity of an initial background investigation and the impact to the assurance level granted to an individual are not always correlated. There should be a means for monitoring and managing the lifecycle of a person's eligibility over time. Changes in status or eligibility factors should be reported to agencies leveraging a person's results through reciprocity and informing credential issuers.
- **Lack of integration between PIV enrollment and background investigation processes.** Agencies should better integrate enrollment and investigative processes to eliminate redundant processes and ensure a strong tie between the data used to determine suitability/fitness and the data used in credentialing processes.
- **Redundant data collection between background investigations and other ICAM processes.** Agencies should attempt to 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

This use case provides the high-level process steps for creating and issuing a PIV credential to a federal employee or contractor,[34] as defined by FIPS 201. This use case also provides the high-level process steps for maintaining a PIV card over the life cycle of the card. Similar issuance processes may occur for PIV-interoperable credentials outside of the Federal Government, but this use case is focused specifically on federal requirements and processes.

4.4.1. As-is Analysis

The responsibilities for creating and issuing a PIV credential are split amongst various actors, each outlined in FIPS 201. PIV systems are required to separate duties so that no bad actor within the system can issue a card fraudulently. The mechanisms that support this collaboration can be implemented in a variety of ways, so system interfaces and supporting technologies can be diverse. This use case attempts to capture the common systems and technologies government-wide.

Current challenges with the as-is model include:

- There is little coordination currently enabled between background check processes and the PIV enrollment processes.
- Changes to related standards and directives must be integrated into the PIV process, including F/ERO repository linkage and alternative biometric verification processes.

Assumptions include:

- Temporarily lost or forgotten PIV card replacement processes are not covered in this Use Case.
- Agency specific policies govern the mechanism by which the physical credential is recovered upon revocation (a requirement of FIPS 201 and Federal PKI rules) and are not covered in this Use Case.
- All events are logged in an audit log system.

4.4.1.1. Process Flow

The scenarios supporting this use case include the following major steps.

Part 1: Create a new PIV record:

Sponsorship

1. The Applicant requests a PIV card.
2. The Sponsor substantiates the Applicant's need for a PIV credential within the agency and authorizes the request for a PIV Card.
3. The Sponsor enters basic information about the Applicant into the PIV IDMS, either on an individual basis, or as part of a group in a batched process (batch processing may be handled in various ways at individual agencies).

[34] HSPD-12 applies to federal employees, contractors, and affiliates requiring long-term access to federal facilities and information systems in accordance with OMB M-05-24. Applicability to affiliates, which may include foreign nationals and other parties, is an agency-level risk-based decision.

4. The Sponsor approves and digitally signs the Applicant(s) PIV IDMS record(s).

Enrollment

1. The Applicant appears for enrollment with supporting documentation (two forms of ID are required that meet Form I-9 requirements, at least one of which must be a government-issued photo ID).
2. The Registrar/Enrollment Official inspects and confirms all supporting documents using automated means if available. Registrar/Enrollment Official may also scan and retain a copy of all supporting documents.
3. The Registrar/Enrollment Official establishes that the individual present matches the supporting documents.
4. The Registrar/Enrollment Official confirms Sponsor approval for PIV.
5. The Registrar/Enrollment Official captures the Applicant's digital facial image.
6. The Registrar/Enrollment Official captures fingerprint biometrics from the Applicant, typically both rolled and flat prints of all ten fingers. (These fingerprints are intended to be forwarded for the background investigation, although it is not currently done on a consistent basis.)
7. The Registrar/Enrollment Official captures any additional required biographic data from the Applicant that was not captured during Sponsorship.
8. The Registrar/Enrollment Official digitally signs and submits the completed electronic enrollment package to the IDMS for storage and processing.
9. The IDMS verifies the integrity of that package by confirming completeness, accuracy, and digital signatures.

Adjudication

1. The IDMS may perform a 1: many search to assure that the individual identified in the package has not applied previously under a different name.
2. The Adjudicator may receive notification that the enrollment package has been completed for the Applicant and requires a determination of eligibility to receive a PIV card.
3. The Adjudicator provides an initial interim card issuance determination based on fingerprint result findings and National Agency Check (NAC) results or a single final eligibility determination through a background investigation. At a minimum, the FBI National Criminal History Check (fingerprint check) must be completed before credential issuance as per FIPS 201/OMB Memorandum M-05-24.
4. Full background check information is typically collected via related background investigation processes associated with on-boarding (see Use Case 3). The Adjudicator provides a final card issuance determination based upon the results of the completed background investigation. If a card has been issued based upon the fingerprint check, and the investigation produces an unfavorable determination, the card should be revoked.

5. After a favorable fingerprint check result, the Adjudicator approves card production for the credential on an interim (6 month) basis. This process may be automated based on integration with FBI results.
6. After a favorable adjudication result, the interim approval status is updated in the IDMS and on the PIV credential through an update to the NACI Indicator to show full approval (the NACI Indicator is located on the PIV Authentication Certificate). This process is handled different by many agencies.

Issuance

1. Depending on the issuance model, card stock or cards that have been pre-personalized with personal information are shipped and tracked to an issuance site.
2. The IDMS or the Issuer notifies the Applicant to schedule an issuance session.
3. Upon arrival, the Issuer verifies the Applicant biometrically by performing a one-to-one match between the applicant and the fingerprint sample collected during enrollment.
4. The Applicant's card is finalized, with any remaining personal information loaded on the chip. In the case of local printing, blank card stock is personalized, printed and finalized.
5. The Applicant creates a PIN that will be used to gain access to the card certificates.
6. The certificates[35] and PIN are loaded onto the credential (if they have not been so already) and the card is released to the Cardholder.
7. The Cardholder signs an agreement indicating acceptance of the terms and conditions of holding digital certificates. This is either a paper or electronic process.

Part 2: Maintain an existing PIV record

Maintenance activities are performed during various stages of the PIV lifecycle. Not all activities are performed for each PIV card, and the activities listed below may not be performed in this order.

PIV Card Certificate Update

1. Cardholder is notified via automated system that PKI certificates held in the PIV card are due to expire.
2. Cardholder follows directions in notification to request new certificates.
3. Automated system uses old certificate challenge/response to determine validity of renewal request and updates the certificates on the card.

Reissuance of PIV Card (lost, stolen, compromised)

1. Cardholder notifies an appropriate authority (agency specific, but could be security personnel, issuer, sponsor or other entity) that the PIV Card has been lost, stolen, or suffered compromise and is directed to an enrollment station for reissuance. (Wait times or additional security procedures may be required by agency policy for lost or stolen PIV cards.)

[35] The digital certificates issued as part of the PIV card must be compliant with the Federal PKI Common Policy.

2. The PIV Card itself is revoked. Any local databases that indicate current valid (or invalid) Federal Agency Smart Credential Number (FASC-N) values must be updated to reflect the change in status.
3. The CA is informed and the certificate corresponding to PIV authentication key on the PIV Card must be revoked. Departments and agencies will revoke certificates corresponding to the optional digital signature and key management keys if they have also been issued. Certificate revocation lists (CRL) issued shall include the appropriate certificate serial numbers within 18 hours of revocation.
4. Online Certificate Status Protocol (OCSP) responders are updated so that queries with respect to certificates on the PIV Card are answered appropriately. This may be performed indirectly (by publishing the CRL above) or directly (by updating the OCSP server's internal revocation records).
5. The entire registration and issuance process (described in Part 1 above), including fingerprint and facial image capture, must be conducted.
6. The Issuer verifies that the employee remains in good standing and personnel records are current before reissuing the card and associated credentials.
7. The Issuer issues a new credential (following the procedures for initial issuance) and updates the IDMS record.
8. Issuer digitally signs the recaptured biometric sample and new credential record.
9. If issued, a new key management key is be escrowed. Existing key management keys previously escrowed may be recovered in accordance with agency policy.

Renewal of PIV Card

1. The Cardholder receives notice (automated or manual) within 6 weeks of PIV card expiration.
2. The Cardholder presents his current PIV card to the Registrar/Enrollment Official prior to the date of expiration.
3. The Registrar/Enrollment Official ensures that the IDMS record for this individual states the credential is not expired. If the PIV Card presented is past the expiration date, the Issuer must follow re-issuance procedures.
4. The Registrar/Enrollment Official verifies the Cardholder against the IDMS record digital photograph.
5. If the digital photograph and biometric reference data are stored locally within the IDMS, the same biometric data may be re-used for the new PIV card. The same data may only be used if it accurately depicts the physical appearance of the applicant. If the photo and biometric data are not stored locally, the Registrar/Enrollment Official recaptures biometrics and digital facial image.
6. The Registrar/Enrollment Official submits all paperwork to the Adjudicator or the IDMS for storage and processing.
7. The Adjudicator verifies that the background investigation on record for the Cardholder is still current and valid and approves issuance.

8. The Issuer issues a new credential (following procedures for initial issuance) and updates the IDMS record.
9. The Issuer digitally signs the recaptured biometrics and new credential record.
10. The new key management key is escrowed.

PIN Change (Cardholder requires or requests new PIN)

1. The Cardholder arrives at a designated support kiosk, approved computer terminal, issuance or enrollment station and puts the PIV card into the reader.
2. The PIV System prompts the Cardholder for his previous PIN (in cases where the PIN has not been forgotten).
3. If authentication is successful, the Cardholder selects PIN Change.
4. For PIN Change, the IDMS prompts the Cardholder to enter the current PIN, enter a new PIN value and confirm the new PIN. The system verifies that the entered PIN conforms to established policy for PIN values.
5. The system confirms PIN change was successful.

PIN Reset (PIN is blocked or forgotten)

1. The Cardholder arrives at a designated issuance or enrollment station and puts the PIV card into the reader.
2. A biometric match between the Cardholder and IDMS is required in order to request a new PIN.
3. The PIV System prompts the Cardholder to enter a new PIN.
4. The system verifies that the entered PIN conforms to established policy for PIN values.
5. The system confirms PIN change was successful.

Key Recovery (key management key only, if required)

1. Cardholder, investigative authority or other authorized person (subscriber) requests a key recovery.
2. Paper forms are submitted to the agency key recovery officer or appropriate local registration agent (LRA).
3. Key recovery officer or LRA submits request to key recovery agent (KRA) at the issuing authority.
4. The KRA recovers the key following security policies and sends it as a soft certificate to the subscriber via encrypted media (CD, etc.).
5. Two halves of the associated password are provided separately by two KRAs (no single KRA is allowed to know the entire password for security reasons).
6. Events are manually logged and recorded.

Card Termination/Revocation

1. Official notification is sent to Card Management System.

2. The Card Management System Administrator performs the PIV card termination process within the Card Management System.
3. The events are logged in an audit log system.
4. The card is terminated in IDMS.
5. The digital credentials on the card are revoked.
6. Revocation status is propagated to applicable provisioning software or individual applications, notifying them of card termination.

4.4.1.2. Architecture Analysis

The following table provides details for the Business, Data, Service, and Technology Layers of the ICAM segment architecture in support of this use case in the as-is state. An overview of the segment architecture layers can be found in Chapter 4.

Architecture Layer	Architecture Details

Business	• **E-Government Alignment:** IEE
	• **Trigger:**
	  ○ Part 1: A sponsor requests a PIV card for an employee or contractor.
	  ○ Part 2: A Cardholders PIV card requires a maintenance activity.
	• **Actors:** Applicant /Cardholder, Sponsor, Registrar/Enrollment Official, Adjudicator, Issuer, Card Management System Administrator, Subscriber, Key Recovery Officer, Local Registration Agent, Key Recovery Agent
	• **Endpoint:**
	  ○ Part 1: A PIV card is issued.
	  ○ Part 2: A PIV card is maintained and ultimately expires/is revoked.

Data	**Data Elements**
	• PIV Sponsor
	  ○ Name
	  ○ Organization
	  ○ Contact Information
	• Applicant
	  ○ Name
	  ○ Date of Birth
	  ○ Position
	  ○ Contact Information
	  ○ Digitally Captured Facial Image
	  ○ Fingerprints
	  ○ Background Investigation Results
	  ○ I-9 Source Identity Documentation Data
	  ○ Document title
	  ○ Document issuing authority
	  ○ Document number
	  ○ Document expiration date (if any)
	  ○ CHUID (FASC-N)
	  ○ PIN
	  ○ Cryptographic Key Pairs
	  ○ Cryptographic Key Pairs Certificates
	  ○ PIV Credential Holder signature
	• PIV Registrar
	  ○ Name
	  ○ Contact Information
	  ○ Completed & signed PIV Request
	  ○ Completed & signed SF 85 (or equivalent)
	• PIV Issuer

Architecture Layer	Architecture Details
	○ Name ○ Contact Information ○ Completed & formally authorized PIV request ○ Approval notice from PIV Registrar ○ Agency Card Serial Number ○ Signed acceptance form from PIV credential holder **Data Repositories/Systems** • Identity Management System • Card Management System • Certificate Revocation List • Audit Log System
Service	• Sponsorship • Enrollment • Adjudication • Issuance/Activation • Credential Lifecycle Management • Digital Signature • Audit Trail
Technology	**Hardware/Software** • See the GSA Approved Products List supported by the HSPD-12 Evaluation Program: • Card Printer Station • CHUID Reader (Contact) • CHUID Reader (Contactless) • Cryptographic Module • Electromagnetically Opaque Sleeve • Electronic Personalization (Product) • Electronic Personalization (Service) • Facial Image Capturing (Middleware) • Facial Image Capturing Camera • Fingerprint Capture Station • Graphical Personalization • OCSP Responder • PIV Card • PIV Middleware • Single Fingerprint Capture Device • Template Generator • Template Matcher • Transparent Reader **Standards** • FIPS 140 • FIPS 201 • SP800-76 • SP800-73 • SP800-78 • SP800-96 • SP800-79 • SP800-104

Figure 25: Use Case 4 As-is Architecture Details

4.4.2. Target Analysis

Since most agencies are issuing PIV cards to new employees, the as-is and target use cases will look very similar in terms of technology and data. However, a major shift in the target state will include more direct integration to outside lines of business and related ICAM functionalities. For

example, a major limitation with current PIV systems is the lack of a common interface to existing investigative databases that causes duplicate paperwork. Another example is the lack of an interface between HR systems and the IDMS, which is imperative for binding of the identity, background investigation, and auditability to the hiring agent and enrollment/registration personnel. Another issue is the absence of a link to authoritative source data such as identity attributes, training, employment status, etc. Automating these interfaces can support other use cases during various lifecycle events, such as deprovisioning once a PIV card is revoked.

Special consideration on the data and services layer must be outlined in the solution architecture within each agency to identify areas where PIV systems may integrate with HR, Identity and Access Management, FEMA Federal Emergency Response Official (FERO) databases, or other systems, as these interfaces are controlled at the agency level.

4.4.2.1. Process Flow

Due to the strong similarities between the as-is and target states, a separate target process flow is not provided for this use case. Instead, this section provides a list of the architecture changes in the target state along with the process steps affected by changes. These are:

- Create a direct link to FEMA's F/ERO repository. The development of agency linkages is being overseen by FEMA, who will host the repository.[36]
  - Process step: if a PIV Applicant is approved to be assigned a FERO status, the PIVAUTH Cert and the attribute assigned that individual as required by the NRF, NIPP, or NCPIP must be sent to FEMA upon card issuance and updated on a period basis. This becomes a new step 7 for Part 1, Issuance.
- Create a link from the PIV IDMS to the agency provisioning engines to support automated provisioning into LACS and PACS applications.
  - Process step: Relevant updates to a Cardholder's record or credential information in the IDMS should be made available to provisioning engine to support automation with LACS and PACS. (Defined in Use Cases 7, 8 and 10, respectively). This workflow should provide tie-ins to HR and other authoritative source databases. The steps affected include:
    - Part 2, PIV Card Certificate Update, Step 3
    - Part 2, Renewal of PIV Card, Step 6
    - Part 2, Card Termination/Revocation, Step 4
- Clarify guidance for use of alternate biometric modalities in PIV processes (e.g., alternate PIN reset and issuance procedures) for users without usable fingerprint biometrics. The steps affected include:
  - Part 1, Enrollment, Step 6
  - Part 1, Adjudication, Steps 4 and 5
  - Part 1, Issuance, Step 5

[36] This is a mandate arising from House Resolution 12.

- Part 2, Reissuance, Steps 3, 5, and 7
- Part 2, Renewal of PIV Card, Steps 4 and 5
- Part 2, PIN Change, Step 4

- Enable automated key recovery. This will alter the as-is process of key recovery for PIV card holders. However, the process for investigative authorities or other authorized subscribers will remain the same as the As-Is process.

  1. Cardholder may perform key recovery automatically via request sent to Card Management System.
  2. Card Management System verifies cardholder (via PIV authentication challenge/ response) and automatically recovers keys and delivers them to the PIV card via secure session.
  3. Events are automatically logged in an audit log system.

The figure below shows the data interchanges and information flow as described in the processes outlined above. The hexagonal figures represent the various services that are employed throughout the process. Repositories and actors are also depicted. This graphical depiction of the process should illustrate the architecture needed to support this target state use case.

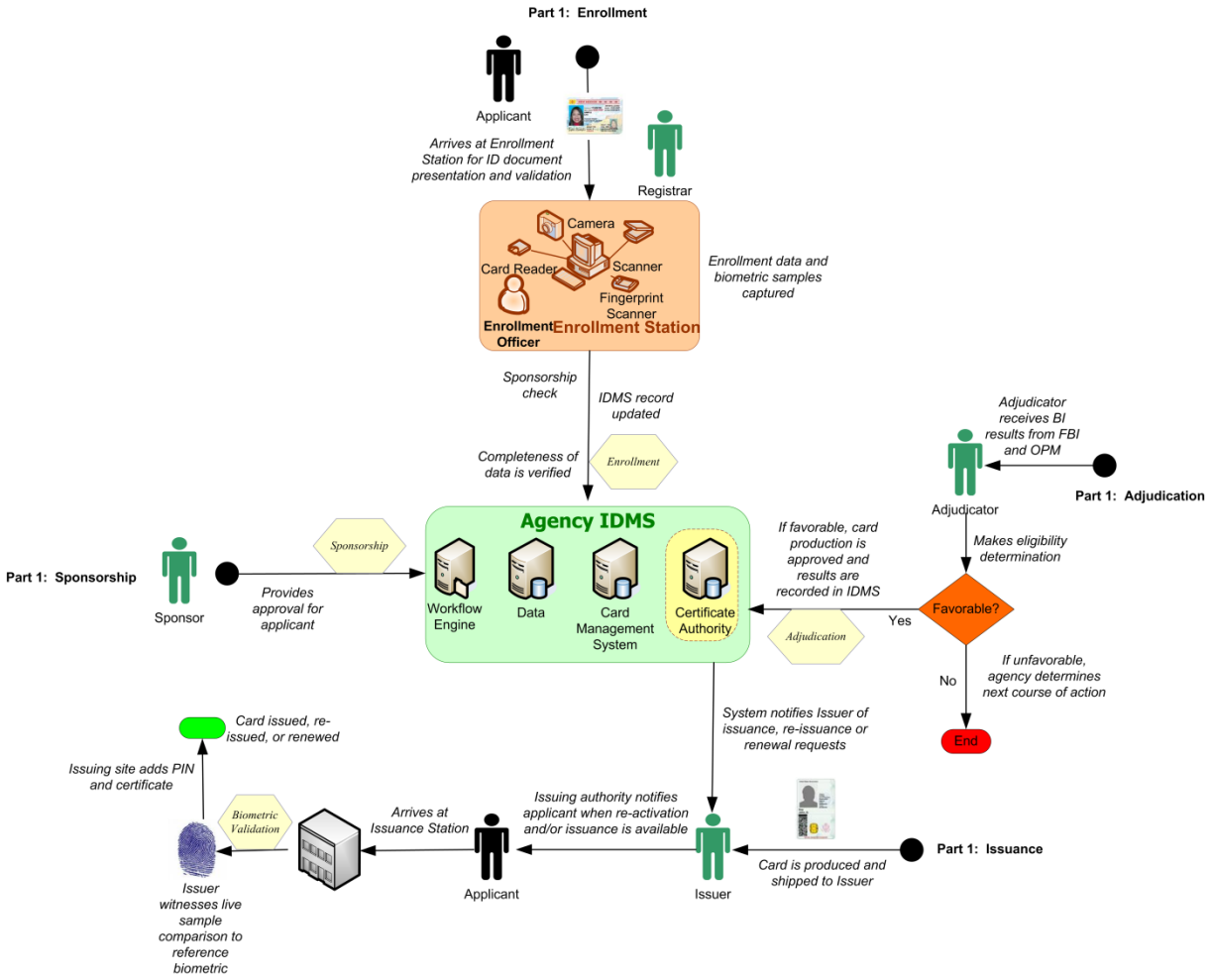

Figure 26: Use Case 4 Target Process Diagram

4.4.2.2. Architecture Analysis

The following table provides details for the Business, Data, Service, and Technology Layers of the ICAM segment architecture in support of this use case in the target state. An overview of the segment architecture layers can be found in Chapter 4.

Architecture Layer	Architecture Details

Business	• **E-Government Alignment:** IEE
	• **Trigger:**
	  ○ Part 1: An employee or contractor requests a PIV card.
	  ○ Part 2: A Cardholders PIV card requires a maintenance activity.
	• **Actors:** Applicant /Cardholder, Sponsor, Registrar/Enrollment Official, Adjudicator, Issuer, Card Management System Administrator, Subscriber, Key Recovery Officer, Local Registration Agent, Key Recovery Agent
	• **Endpoint:**
	  ○ Part 1: A PIV card is issued.
	  ○ Part 2: A PIV card is maintained and ultimately expires/is revoked.

Data	**Data Elements**
	• PIV Sponsor
	  ○ Name
	  ○ Organization
	  ○ Contact Information
	• Applicant
	  ○ Name
	  ○ Date of Birth
	  ○ Position
	  ○ Contact Information
	  ○ Digitally Captured Facial Image
	  ○ Fingerprints
	  ○ Background Investigation Results
	  ○ I-9 Source Identity Documentation Data
	  ○ Document title
	  ○ Document issuing authority
	  ○ Document number
	  ○ Document expiration date (if any)
	  ○ CHUID (FASC-N)
	  ○ PIN
	  ○ Cryptographic Key Pairs
	  ○ Cryptographic Key Pairs Certificates
	  ○ PIV Credential Holder signature
	• PIV Registrar
	  ○ Name
	  ○ Contact Information
	  ○ Completed & signed PIV Request
	  ○ Completed & signed SF 85 (or equivalent)
	• PIV Issuer
	  ○ Name
	  ○ Contact Information
	  ○ Completed & formally authorized PIV request
	  ○ Approval notice from PIV Registrar
	  ○ Agency Card Serial Number
	  ○ Signed acceptance form from PIV credential holder
	Data Repositories/Systems
	• Identity Management System
	• Card Management System
	• Certificate Revocation List

Architecture Layer	Architecture Details
Service	• Sponsorship • Enrollment • Adjudication • Issuance • Credential Lifecycle Management • Digital Signature • Key Management • Audit Trail
Technology	**Hardware/Software** • See the GSA Approved Products List supported by the HSPD-12 Evaluation Program: • Card Printer Station • CHUID Reader (Contact) • CHUID Reader (Contactless) • Cryptographic Module • Electromagnetically Opaque Sleeve • Electronic Personalization (Product) • Electronic Personalization (Service) • Facial Image Capturing (Middleware) • Facial Image Capturing Camera • Fingerprint Capture Station • Graphical Personalization • OCSP Responder • PIV Card • PIV Middleware • Single Fingerprint Capture Device • Template Generator • Template Matcher • Transparent Reader **Standards** • FIPS 140 • FIPS 201 • SP800-76 • SP800-73 • SP800-78 • SP800-96 • SP800-79 • SP800-104

Figure 27: Use Case 4 Target Architecture Details

4.4.3. Gaps

This section provides a summary of the high-level gaps between the as-is and target states for this use case. Gaps may focus on Data, Technology, Business and/or Service Layer activities. Explanations about the drivers and impact of each gap are also provided.

- **Lack of integration between PIV systems and FEMA Emergency Response Official database.** Incorporate First Responder requirements into PIV systems, including standardization of Responder designations and building any required interface to the FEMA Emergency Response Official database.
- **Redundant collection of identity data between credentialing and other ICAM processes.** Agencies should link identity data required as part of the PIV identity proofing and enrollment processes to authoritative repositories or directories to enable synchronized updates to identity records.

- **Lack of integration between PIV enrollment and background investigation processes.** Agencies should integrate enrollment and investigative processes such that fingerprint samples captured as part of PIV enrollment are forwarded to OPM/FBI, and the results of which are made available to adjudicators for required background checks. It is critical that the fingerprint samples taken during a PIV enrollment are linked to an investigative record on file.
- **Redundant credentialing processes.** Agencies should standardize and reduce the number of credentials issued for the same individual within and across agencies, and enable the use of PIV credentials already issued.

4.5. Create, Issue, and Maintain PKI Credential

This use case provides the high-level process steps associated with creating, issuing, and maintaining a PKI certificate over the credential lifecycle in compliance with Federal PKI standards. PKI certificates can be issued as software, or "soft," certificates, where the private key of the PKI key pair is installed as part of a software application, usually directly to a computer or other devices, or as hardware certificates, where the private key is installed on a protected hardware token that has been tested and certified to be FIPS 140 compliant.

It is important to note that the creation, issuance, and maintenance of PKI credentials as part of PIV cards is included in Use Case 4; however, PIV cards are only one example of PKI credential usage in the Federal Government. This use case addresses the minimum processes outlined in the Federal PKI Common Policy Framework[37] (COMMON), the policy governing the PKI component of the Federal Enterprise Architecture, and the FBCA Certificate Policy, which may be used to implement PKI credentials in non-PIV environments. Together, COMMON and the FBCA Certificate Policy form the basis for creating and issuing PKI certificates to users such that they may be trusted within the Federal Government.

4.5.1. As-is Analysis

According to NIST SP 800-63, the PKI certificates issued under COMMON or issued by Certification Authorities cross-certified with the FBCA are acceptable credentials for use in authenticating entities at Assurance Levels 3 and 4[38] and may be used to provide authentication, digital signature and encryption functionality. PKI certificates that are to be used at Assurance Level 4 must be installed on a hardware token, while soft certificates are acceptable at Assurance Level 3. As defined in the as-is process flow, the high-level processes for issuing a PKI certificate are similar for soft or hardware certificates; however, the identity proofing requirements vary based on the assurance level. Where the processes differ between Assurance Levels 3 and 4, it has been noted in the process flow.

The following table provides a mapping between the assurance levels defined for COMMON and FBCA credentials and Assurances Levels 3 and 4 as defined in OMB M-04-04. (Note: PKI certificates are also acceptable at Levels 1 and 2 in lieu of passwords or other lower level tokens to provide a higher level of assurance.)

PKI Credential	M-04-04 Level 3	M-04-04 Level 4
FBCA Basic Assurance	X	
FBCA Medium Assurance	X	
FBCA Medium Hardware	X	X
FBCA High Assurance	X	X
COMMON (Software)	X	
COMMON_Hardware	X	X
COMMON_High	X	X

Figure 28: Mapping of PKI Credential and Identity Assurance Levels

[37] X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 3647 - 1.6, February 11, 2009

[38] As defined in OMB Memorandum M-04-04.

Specific challenges associated with the current state include:

- Some certificate authorities within agencies are not cross certified with the Federal Bridge, and are therefore operating in violation of policy guidance.
- Rules and guidance for managing Key History are not well-defined across government.
- Rules and guidance for Key Escrow are not well-defined across government

Key assumptions for this use case include:

- PKI issuance for non-person subscribers (i.e., machine certificates) is similar in most ways to PKI issuance to humans. However, the specific variations associated with creating, issuing, and maintaining certificates for non-person subscribers are considered out of scope for this use case.
- Certificate creation, issuance, and maintenance processes that do not comply with the COMMON Policy or FBCA are considered out of scope for this use case.
- The process steps defined here are intended to be high-level. The detailed processes employed will vary by PKI provider and are defined in a particular provider's certification practice statement (CPS).

4.5.1.1. Process Flow

The high-level scenario supporting this use case includes the following steps.

Part 1: Create and issue a new PKI certificate

Identity Proofing

1. An Authorized Sponsoring Agency Employee submits an application for a user certificate for an Applicant.
2. The (RA) verifies that a request for certificate issuance to the Applicant was submitted by an authorized sponsoring agency employee.
3. The RA establishes the Applicant's identity either by remote or in-person proofing before the RA based on one of the following processes:
    a. Remote identity proofing (Level 3)
        i. The applicant accesses a secure web-form and provides identity information including name, Date of Birth, and mailing address, along with details from a valid government ID (e.g., driver license or passport) and a second verifiable identifier such as a financial account number.
        ii. The RA verifies the information provided by the applicant through record checks in such a manner as to determine the data provided is sufficient to identify a unique individual. Record checks through the system involve linking with trusted databases containing personnel information.
        iii. The RA then responds to the applicant in a manner that confirms address of record (e.g., out-of-band response to address of record).
    b. In-Person identity proofing (Level 4)

i. The Applicant appears before the Registrar, Trusted Agent, or an individual certified by a State or Federal entity as being authorized to confirm identities and presents a government-issued form of identification as proof of identity.

ii. The RA or Trusted Agent examines the presented credential for biometric data that can be linked to the Applicant.

iii. Based on the level of assurance required in the Applicant's identity, the Applicant may be required to present current corroborating information to the RA.

iv. Information provided by the Applicant is verified through record checks in such a manner as to determine legitimacy of the information.

4. In cases where an audit trail is required for dispute resolution, the RA or CA may record and maintain one or more biometric samples from the Applicant.
5. The RA verifies any role or authorization information requested for inclusion in the certificate.

Issuance

1. Once the identity proofing requirements have been met satisfactorily, a public/private key pair is generated (this may be done by the applicant, or may be performed by the CA and delivered to the applicant with the certificate).
2. The CA/RA builds a certificate, binds it to the public key of the Applicant, and signs it once all certificate requirements have been met (in the case of an RA completing this step, the CA must sign the certificate). The Applicant, once he has received the certificate, is subsequently referred to as a Subscriber.
3. The CA/RA makes the certificate available to the subscriber after confirming that the subscriber has formally acknowledged his obligations. For Medium and High Assurance levels, the subscriber is required to sign a document containing the requirements the subscriber will meet, respecting protection of the private key and use of the certificate. For Basic Assurance level, the subscriber is required to acknowledge his obligations respecting protection of the private key and use of the certificate.
4. The CA publishes the certificate in a repository that is publicly accessible per the requirements laid out in the Federal PKI Common or FBCA Policy.

Part 2: Maintain an existing PKI certificate

Maintenance activities are performed during various stages of the PKI lifecycle. Not all activities are performed for each certificate, and the activities listed below may not be performed in this order. Once a certificate has been issued, the Applicant in the prior steps is referred to as a Subscriber.

Certificate Renewal

1. An Authorized Sponsoring Agency Employee submits a certificate renewal request for a Subscriber.
2. The CA creates a new certificate with the same name, key, and other information as the old key, but with a new, extended validity period and a new serial number.
3. The CA may optionally revoke the old certificate as part of renewal.

4. The CA informs the Subscriber of his certificate and the contents of the certificate.
5. The CA publishes the certificate in a repository that is publicly accessible per the requirements laid out in the Federal PKI Common or FBCA Policy.

Certificate Re-key

1. An Authorized Sponsoring Agency Employee submits a certificate re-keying request for a Subscriber.
2. The CA creates a new certificate with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key.
3. The CA may optionally revoke the old certificate as part of renewal.
4. The CA publishes the certificate in a repository that is publicly accessible per the requirements laid out in the Federal PKI Common or FBCA Policy.

Certificate Modification

1. A Subscriber with a currently valid certificate requests a certificate modification. Alternatively, a CA or RA may request certificate modification on behalf of a Subscriber.
2. The RA or other designated agent verifies proof of all subject information changes (e.g., change in name or privileges) triggering the certificate modification.
3. The CA creates a new certificate with the same key or a different key and a different serial number, and that differs in one or more other fields from the old certificate.
4. The CA may optionally revoke the old certificate as part of certificate modification. If the Subscriber authorizations have been reduced, the old certificate must be revoked.
5. The CA publishes the certificate in a repository that is publicly accessible per the requirements laid out in the Federal PKI Common or FBCA Policy.

Certificate Revocation

1. The Subscriber, RA, or authorized agency official requests the revocation of a Subscriber's certificate. A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed).
2. The CA authenticates the revocation requests.
3. The CA revokes the certificate within the CA server and its subordinate directories.
4. The CA publishes the revocation information to all affected CRLs. Where on-line status checking is supported, the CA updates the status information and makes it available to relying parties.
5. If the CA triggers certificate revocation, a written notice and brief explanation for the revocation shall subsequently be provided to the Subscriber.

4.5.1.2. Architecture Analysis

The following table provides details for the Business, Data, Service, and Technology Layers of the ICAM segment architecture in support of this use case in the as-is state. An overview of the segment architecture layers can be found in Chapter 4.

Architecture Layer	Architecture Details

Business	• **E-Government Alignment:** IEE, G2G, G2B, G2C
	• **Trigger:** User requests a PKI certificate
	• **Actors:** CA, Certificate Status Servers, RA, Applicant/Subscriber, Authorized Sponsoring Agency Employee
	• **Endpoints:**
	  ○ Part 1: A PKI certificate is issued.
	  ○ Part 2: PKI Maintenance activity is successfully completed.

Data	**Data Elements** RA • The identity of the person performing the identification • A signed declaration by that person that he verified the identity of the Applicant • Unique identifying number(s) from the ID(s) of the Applicant, or a facsimile of the ID(s) • Applicant's biometric data • The date and time of the verification • A declaration of identity signed by the Applicant using a handwritten signature and performed in the presence of the person performing the identity authentication Sponsor • Contact information to enable the CA or RA to communicate with the Sponsor when required **Data Repositories/Systems** • Certification Authority • Certificate Directories
Service	• Identity Proofing • Credential Lifecycle Management • Sponsorship • Enrollment/Registration • Adjudication • Issuance • Self Service • Digital Signature • Key Management • Audit Trail
Technology	**Hardware/Software** • Smart card (hard tokens) • PKI issuance software **Standards** • Federal PKI Common Policy • FBCA Certificate Policy • FIPS 186 • FIPS 180 • XML • NIST Special Publication 800-67 • NIST Special Publication 800-78 • ISO/IEC 18033-3:2005 • X.509 CRLs • Online Certificate Status Protocol (OCSP)

Figure 29: Use Case 5 As-is Architecture Details

4.5.2. Target Analysis

PKI creation and issuance processes are well developed under the Federal Bridge Policy Authority. As such, no process changes are proposed in the target state; however, there are some key changes in the target state regarding the usage of and lifecycle support capabilities for PKI certificates. These recommendations vary slightly depending on the E-Government sector considered.

In the target state, it is intended that agencies will eliminate the issuance of separate PKI credentials to internal users and that scenarios that require the use of PKI credentials will be addressed using the PKI certificates commonly found on the PIV card:

- PIV Authentication Key (mandatory) – Used for PACS and smart card logon in LACS.
- Card Authentication Key (optional) – Used for PACS applications.
- Digital Signature Key (optional) – Used for digital signatures.
- Key Management Key (optional) - Used for managing the keys on the card. This key is often also used for encryption in email and documents.

For external business partners, state and local government users, or other users of federal networks requiring authentication at Assurance Levels 3 or 4, agencies should continue to create, issue, and maintain PKI credentials in accordance with the process outlined in the as-is process flow when necessary. Alternatively, agencies may eliminate cost and administrative burden by accepting third-party credentials for external users where they are available at the higher assurance levels (discussed further in Use Case 10).

The target state will incorporate the following elements:

- Issuance of certificates only from Certificate Authorities cross-certified with the Federal Bridge.
- Implementation of key history practices at the Certification Authority.
- Increased directory mappings to allow certificates issued from external certificate authorities to be utilized.

The figure below shows the data interchanges and information flow as described in the processes outlined above. The hexagonal figures represent the various services that are employed throughout the process. Repositories and actors are also depicted. This graphical depiction of the process should illustrate the architecture needed to support this target state use case.

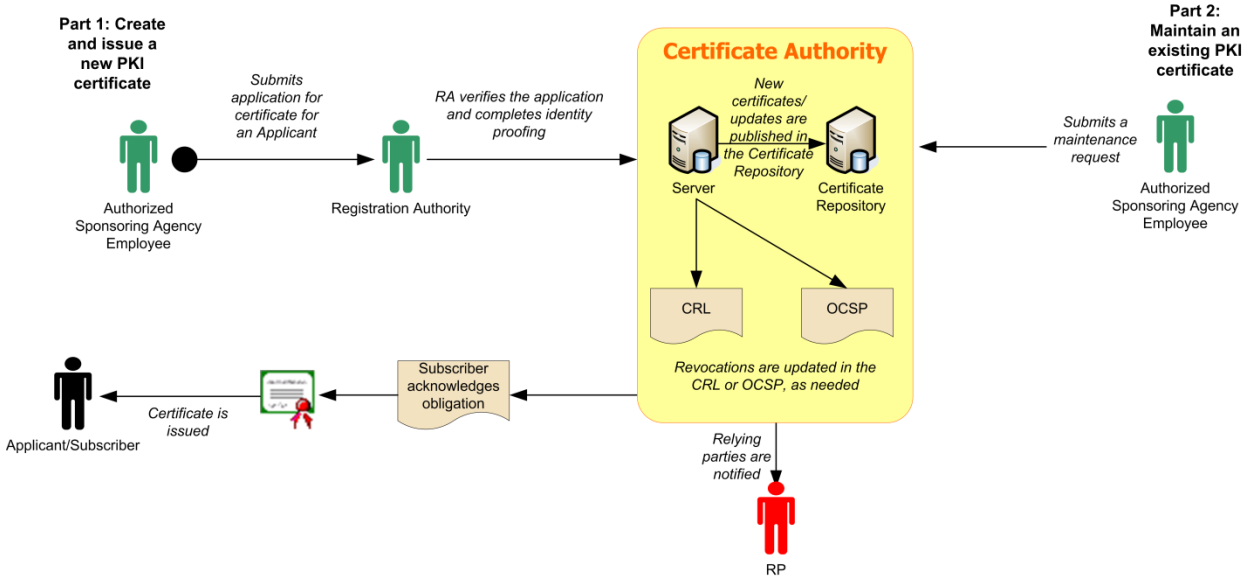

Figure 30: Use Case 5 Target Process Diagram

4.5.3. Gaps

This section provides a summary of the high-level gaps between the as-is and target states for this use case. Gaps may focus on Data, Technology, Business and/or Service Layer activities. Explanations about the drivers and impact of each gap are also provided.

- **Underutilization of PIV certificates as primary PKI credentials for internal users.** Agencies should minimize or eliminate the creation and issuance of separate soft certificates to internal users and PIV holders.
- **Lack of government-wide approach and guidance for managing key history.** Key history is needed to recover documents that have been encrypted using keys now expired or revoked. This capability must ensure that self-access to or requests for private keys can be validated and provided for in a secure manner. Where key history is stored 'on card,' it must be protected by biometric, password, or PIN by the Subscriber.
- **Redundant credentialing processes.** Agencies should leverage efforts to develop government adoption schemas for additional technologies at assurance levels 3 & 4, and use common services and technologies where possible.
- **Lack of product adoption for path discovery and validation.** Industry should increase the number and availability of path discovery and validation products acceptable for use by the Federal Government. Federal agencies should implement path discovery and validation products such that they can trust external PKI and cross certified Federal Bridge issuers.
- **Federal PKI Infrastructure upgrades needed.** The current infrastructure that was put in place for the Federal PKI program is not sufficient to support the significant increase in users that is expected as the PIV program reaches full implementation. Upgrades are needed to support the anticipated increase in capacity.

4.6. Create, Issue, and Maintain Password Token

This use case provides the high-level process steps associated with creating and issuing a password token[39] to a user and the maintenance steps required to change the password at periodic intervals or when it has been forgotten or compromised. Password tokens are typically created specifically by and for the application being accessed and the process is often closely tied to creation of a digital identity record and user account within the application. As discussed in Use Case 1, these two business processes have been split in order to clearly articulate the process steps for credentialing and to demonstrate that managing identities can and should be handled separately from managing the credentialing and access processes that rely on those identities.

4.6.1. As-is Analysis

In the as-is state, application owners primarily control the creation and issuance of password tokens to users, which leads to stove-piped credentialing processes. Some application passwords are managed via major applications across an enterprise for internal users (e.g., Windows logon), and in some limited as-is scenarios there are external (business, citizen) initiatives that provide password tokens centrally and allow their use by multiple applications; however, the norm is for each application to manage its own access and password management processes. Today, most federal applications for both internal and external user groups are accessed using passwords, and as a result, password management is a primary activity for application owners/administrators. In addition, many username and password issuance processes do not incorporate required 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 is directly related to resetting passwords.
- Each application controls password creation internally, requiring multiple passwords for application users and additional administrative burden for application owners/administrators. This results in redundant costs and a less favorable user experience.

Assumptions in this use case include:

- The as-is process will not describe password management via domain controllers or other central management tools.
- Management of roles, identity data or privileges associated with the password is out of scope of this use case; those activities are described in other use cases.

4.6.1.1. Process Flow

The scenarios supporting this use case include the following major steps.

Part 1: Create a new password token

[39] For the purposes of this use case, the term "password token" is derived from SP 800-63. A password token is a secret that a claimant memorizes and uses to authenticate his or her identity, and thus falls into the credential category of "something you know," whereas the PIV and PKI credentials discussed in Use Cases 4 and 5 respectively are considered credentials in the category of "something you have." Common password tokens are username/password combinations.

1. A User requests an account for an application. Alternatively, an Authorized Agency Employee may automatically enroll the User in the application through a batch process.
2. The RA establishes the Applicant's identity either by remote or in-person proofing based on one of the following processes:
    a. Assurance Level 1: No specific identity proofing requirements. Proceed to Step 3.
    b. Remote identity proofing (Level 2):
        i. The RA inspects both the valid government ID and the financial account number supplied by Applicant and verifies the information through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address, and other personal information in records are in balance and consistent with the application and sufficient to identify a unique individual.
        ii. The RA then responds to the applicant in a manner that confirms address of record (e.g., out-of-band response to address of record).
    c. In-person identity proofing (Level 2):
        i. The RA inspects the Applicant's photo ID, compares picture to Applicant, and records the ID number, address and Date of Birth.
        ii. If the ID confirms the address of record, the RA authorizes the credentials and sends a notice to address of record. If the ID does not confirm address of record, the RA responds to the applicant in a manner that confirms address of record (e.g., out-of-band response to address of record).
3. The application administrator creates a user name/password or other shared secret or prompts the user to create these fields.
4. If the credential is automatically generated, the application administrator provides the credential (user name/password or shared secret) to the user via mail, email, text or phone message, or other format. In these cases, the user may be asked to immediately change or update the password upon initial log-in to the application.

Part 2: Change an existing password token

Password maintenance processes are usually different for each application in the enterprise, resulting in redundant infrastructures and high maintenance costs. Since as-is functions are managed in a variety of ways, the process flow described here is necessarily very generic. For example, many applications have self service functions, but not all applications allow self service if the password has expired, and some commonly used applications typically have help desk support. The process includes the following steps:

1. The User is notified that his password is due to expire and requires changing. Alternatively, the User may request a new password if he has forgotten the existing password.
2. The User logs onto the application and updates the password using a self service capability, or

The User notifies the Help Desk to request a password reset/change. Following identity authentication, the Help Desk resets the User's password to a new permanent or temporary password.

3. The User may be asked to immediately change or update the password upon next log-in to the application.

4.6.1.2. Architecture Analysis

The following table provides details for the Business, Data, Service, and Technology Layers of the ICAM segment architecture in support of this use case in the as-is state. An overview of the segment architecture layers can be found in Chapter 4.

Architecture Layer	Details

Business	• **E-Government Alignment:** IEE, G2G, G2C, G2B
	• **Trigger:**
	  ○ Part 1: User requests access to a logical resource
	  ○ Part 2: User is required or desires to change password
	• **Actors:** User, Application Administrator, Help Desk
	• **Endpoint:** Issuance of password token

Data	**Data Elements**
	• Personal Data
	  ○ Name
	  ○ Date of Birth
	  ○ Address
	  ○ Other personal information
	  ○ Unique Identifiers (to the system/application consuming the password)
	  ○ Usernames
	  ○ Passwords
	Data Repositories/Systems
	• LACS
	• Local Application

Service	• Identity Proofing • Account Management • Enrollment/Registration • Issuance • Credential Lifecycle Management • Self Service
Technology	**Hardware/Software** • Domain Controller • Computer terminal • LACS Server • Network and other Applications • Directory Services **Standards** • Interface specifications between the service and IDPs • Lightweight Directory Access Protocol (LDAP) v.2 and v.3 • SAML 1.0 and 2.0 for transmission between IDPs • SSL

Figure 31: Use Case 6 As-is Architecture Details

4.6.2. Target Analysis

In the target state, the use of passwords for internal users is minimized in favor of other identity credentialing solutions. For internal efficiencies and effectiveness (the Federal employee

community as constituent/user), application owners and administrators will migrate away from password based access control systems to an identity and access management solution that utilizes the capabilities of the Federal PIV card. For the remaining user communities (G2C, G2B, G2G), one way to enable this scenario is to leverage trusted external parties (IDPs) that issue identity tokens to user communities and then provide identity assertions to local applications. The local applications trust the IDP's assertion of the user's identity, thus freeing local administrators from managing user password tokens locally. There are a variety of solutions already operating in the public domain working with the Federal Government to design methodologies by which this process will be governed, and additional guidance will be forthcoming from the Federal CIO Council's Identity, Credential and Access Management Subcommittee.

The Federal Government must supply a mechanism for citizens to access data and services, including citizens that do not have credentials from a third party. Likewise, there will be a number of legacy applications that cannot use externally supplied assertions. In these cases, the government, an agency, or a department may choose to stand up an identity provider service, or continue allowing application administrators to create and manage passwords locally. However, these exceptions should be minimized to the extent possible, and local administrators must follow rules set in NIST SP800-63 governing password strength.

The target process flows reflect the following changes to the architecture:

- Application-specific password tokens are eliminated wherever possible, and applications are enabled to accept the PIV card for federal employees and contractors and identity assertions from third parties for external users.
- Once the creation and maintenance of password tokens is minimized, agencies should eliminate duplicative infrastructure to reduce or eliminate the costs associated with expired/forgotten passwords.
- The requirement for agencies to update passwords will be reduced or eliminated as fewer credentials are issued within federal systems, and the maintenance of externally issued credentials falls to the credential provider.
- Where identity assurance is required, agencies will use high assurance credentials wherever possible.

4.6.2.1. Process Flow

The use case to create, issue, and maintain password tokens is eliminated in the target state. This business function is instead supported by the processes for creating a digital identity for a user (see Use Cases 1 and 2), provisioning a user account and binding an external credential to the account (see Use Case 7), and granting logical access using either the PIV or external identity assertions (see Use Case 10).

4.6.2.2. Architecture Analysis

See the Architecture Analysis tables in Sections 4.1.2.2, 4.2.2.2, 4.7.2.2, and 4.10.2.2 for architectural details relevant to the target state for this use case.

4.6.3. Gaps

This section provides a summary of the high-level gaps between the as-is and target states for this use case. Gaps may focus on Data, Technology, Business and/or Service Layer activities. Explanations about the drivers and impact of each gap are also provided.

- **Administrative and user burden associated with managing and remembering numerous Federally-issued stand-alone password tokens.** Application owners should no longer issue password tokens to their user populations, wherever possible. Rather, applications must be able to leverage PIV credentials for Federal users and accept assertions from approved IDPs whether they are from within the agency, from other federal, state and local partners, or from the private sector.
- **Lack of full adoption and usage of PIV credential for internal users.** The PIV card represents a consistent solution to enable efficiencies and benefits of scale while removing the administrative burden from application owners for managing redundant credentials for PIV cardholders. Agencies must complete their PIV implementation plans and begin utilizing them in lieu of password logon.

4.7. Provision and Deprovision User Account for an Application

This use case provides the high-level process steps for provisioning and deprovisioning a user account in an agency application. It includes the creation and subsequent removal of a user account and the assignment and management of the appropriate entitlement attributes for access to applications and other resources. The process is driven by an underlying need for access to an agency resource, either physical or logical, and applies equally to internal and external users.

This use case is directly linked to identity account creation, logical access and physical access use cases. 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. In the as-is state, provisioning is performed at the same time as identity account creation and credential issuance in many applications, and may not be recognized as a separate step.

4.7.1. As-is Analysis

This use case encompasses a variety of agency and application-specific processes for managing user accounts and permissions. Due to the level of variation, the process flow steps and the supporting architecture are represented at a high-level, capturing commonalities across provisioning as a business function for the Federal Government. The process steps are divided into the following three main flows, which are interrelated but typically occur as separate transactions at different points in time:

- Provision a user account and apply user permissions
- Modify user permissions
- Deprovision user account and end user permissions

The provisioning of a user account is performed when a need for access is identified. For internal users, the scenario that typically causes this event is an employee becoming affiliated with the agency or being assigned to a particular position or role within the agency that carries specific job duties and required access permissions. For external users, the scenario that typically causes this event is a user desires to use an external-facing agency application.

Over time, a user's permissions may change, prompting modifications to the entitlement attributes associated with the user account. This is particularly common in the internal user population, where an employee may change positions or the responsibilities associated with a position drive a change in the access needs.

Deprovisioning is performed when there is a need to permanently eliminate an existing access permission or remove a user account altogether. For internal users, the scenarios that typically cause this event include an employee changing positions or roles or his position is eliminated, the requirements for access under an existing position have been eliminated, or the employee severs the relationship with the organization.

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 across the large number of applications and associated users within the enterprise. Additionally, some provisioning processes employ paper-based approval workflows that are labor and time intensive. These conditions present the following challenges:

- **Efficiency.** Manual approval and provisioning processes increase the amount of time and effort associated with creating user accounts and granting permissions. This results in higher cost and delays in the delivery of services.
- **Scalability.** As the size and complexity of an agency's IT infrastructure continues to grow, manual provisioning processes become harder to sustain and scale.
- **Security.** It is difficult to track all of the permissions that have been granted to a user over time across applications. When a user no longer requires access, 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 for granting permission lack visibility across applications and resources to determine if access permissions violate segregation of duties policies.
- **Auditability.** Processes for maintaining audit trails for creating or modifying an account/access privilege are inconsistent and lack visibility. It is not always clear who verifies the continued need for access and how it is tracked over time. The ability to easily audit a specific person's accounts, privileges and activity in different systems across the enterprise is generally lacking.

4.7.1.1. 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

1. An individual completes a request for access to an application and provides it to the individual responsible for access approvals (hereafter referred to as the Privilege Manager[40]).
2. The Privilege Manager validates the individual's need for access and provides the access request to the Application Administrator.
3. The Application Administrator creates a user account for the individual in the application with the appropriate user permissions.
4. The Application Administrator notifies the user of the account creation.

Part 2: Modify user permissions

1. The user completes a request for a change in privileges.
2. The Privilege Manager validates the user's need for access and provides the access request to the Application Administrator.
3. The Application Administrator updates the user's access permissions in the application.
4. The Application Administrator notifies the user of the permission change, often via phone, email or another manual process.

Part 3: Deprovision a user account

[40] This generic title represents a number of individuals within an agency who may have authority to approve account creation of privilege assignment to a user. This may at times be the same individual as the Application Administrator but is generally considered to be a manager or other entity with direct knowledge of an individual's need to have access to or specific user privileges within an application.

1. The Privilege Manager notifies the Application Administrator that the user no longer requires access to the application.
2. The Application Administrator removes the access permissions and the user account from the application.

Some processes within provisioning are commonly managed via a help desk service that can replace or augment some of the activities performed by the Application Administrator or the Privilege Manager.

4.7.1.2. Architecture Analysis

The following table provides details for the Business, Data, Service, and Technology Layers of the ICAM segment architecture in support of this use case in the as-is state. An overview of the segment architecture layers can be found in Chapter 4.

Architecture Layer	Architecture Details
Business	• **E-Government Alignment:** IEE, G2G, G2B, G2C • **Triggers:** ○ Part 1: A User requires access to an application ○ Part 2: A User's access need has changed ○ Part 3: A User no longer requires access to the application • **Actors:** Individual/User, Privilege Manager, Application Administrator • **Endpoints:** ○ Part 1: A user account is created for the user with the appropriate access privileges ○ Part 2: The user's access privileges are updated to reflect a change in access need ○ Part 3: The user account is deactivated or removed from the application
Data	**Data Elements** • Username • Position • Membership • Authentication Credential • Access Permission **Data Repository/System** • Application-specific user database
Service	• Account Management • Bind/Unbind • Provisioning • Privilege Administration • Policy Administration • Audit Trail
Technology	**Hardware/Software** • Application administrator Global Unique Identifier (GUI)

Figure 32: Use Case 7 As-is Architecture Details

4.7.2. Target Analysis

The underlying business need and function for provisioning and deprovisioning remain the same in the target state; however, several changes are required to address the challenges of the as-is state. The target process flows reflect the following changes to the architecture for provisioning and deprovisioning:

- **Automated and centralized workflows.** Automating the repetitive and time-consuming tasks associated with account management allows for quick, complex changes while

reducing administrative costs. Automation also reduces errors, improves visibility across applications, and improves deprovisioning processing time once access is no longer required. Centralized provisioning workflows can reduce the number of actors providing provisioning services and link business rules across the agency.

- **Linking to external credentials.** In order to meet the target state goals for authentication and reduced government issuance of credentials, the target provisioning use case includes activating user accounts with external credentials. For internal users, this relates to the use of the PIV card and PKI certificates. For external users, this relates to a variety of external identity tokens that may be trusted by the Federal Government.

Assumptions for this use case are:

- A precondition of the following use case is the establishment of automated workflows to support the desired outcome in individual provisioning scenarios. This includes the routing of requests to the appropriate individual and the approval rules for establishing or altering accounts and privileges.
- Attributes can be identified, collected, and provisioned in anticipation of access control decisions that rely on this information. Regular updates to provisioned attribute information must be maintained and kept current.

4.7.2.1. Process Flow

The target process flow for this use case is broken into three parts.

Part 1: Provision a user account and apply user permissions

1. A request for an application user account and access permissions is completed in one of the following ways:
    a. An individual completes an electronic request for access to an application.
    b. A predefined trigger (e.g., assignment to a particular role or the change of a relevant identity attribute) initiates the provisioning process by a central authority without necessary intervention from the user. In this case, skip to Step 4.
2. The Provisioning Workflow routes the access request to the individual responsible for access approvals (Privilege Manager) if applicable.
3. The Privilege Manager validates the individual's need for access and submits an electronic approval of the request (if applicable based on application-specific processes).
4. The Provisioning Workflow automatically populates relevant identity attributes from agency authoritative sources, creates a user account for the individual in the application with the appropriate user permissions, and notifies the user of the account creation.

Part 2: Modify user permissions

1. A request for a change in privileges is completed in one of the following ways:
    a. An individual completes an electronic request for a change in access privileges.
    b. A predefined trigger (e.g., assignment to a particular role or the change of a relevant identity attribute) initiates the change by a central authority without necessary intervention from the user. In this case, skip to Step 4.

2. The Provisioning Workflow routes the change request to the Privilege Manager.
3. The Privilege Manager validates the user's need for access and submits an electronic approval of the request (if applicable based on application-specific processes).
4. The Provisioning Workflow updates the user's access permissions in the application and notifies the user of the permission change.

Part 3: Deprovision a user account

1. A request to deprovision a user account is completed in one of the following ways:
   a. The Privilege Manager completes an electronic notification that the user no longer requires access to the application.
   b. A predefined trigger (e.g., change in user attributes, affiliation, or need for access) initiates the deprovisioning process automatically by a central authority without the need for user interaction.
2. The Provisioning Workflow removes the access permissions and the user account from the application.
3. Sufficient records are maintained about the user account and activities such that complete auditing functions can be performed for a specified period of time.

The figure below shows the data interchanges and information flow as described in the processes outlined above. The hexagonal figures represent the various services that are employed throughout the process. Repositories and actors are also depicted. This graphical depiction of the process should illustrate the architecture needed to support this target state use case.

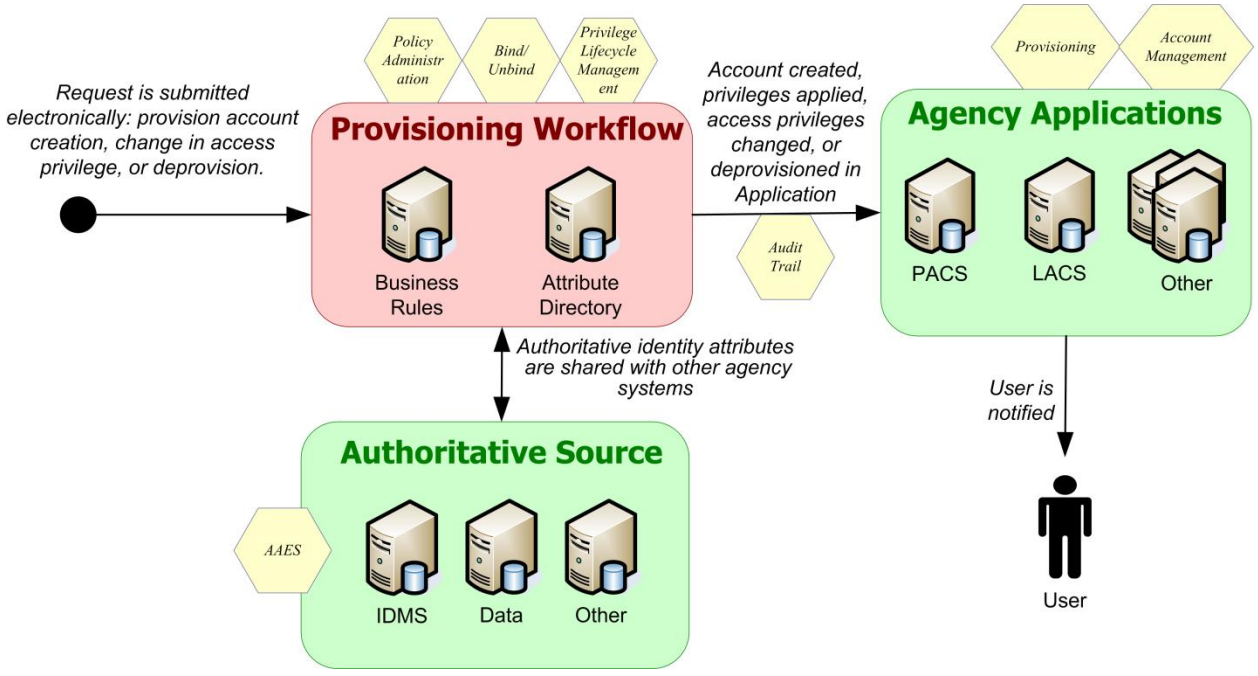

Figure 33: Use Case 7 Target Process Diagram

4.7.2.2. Architecture Analysis

The following table provides details for the Business, Data, Service, and Technology Layers of the ICAM segment architecture in support of this use case in the target state. An overview of the segment architecture layers can be found in Chapter 4.

Architecture Layer	Architecture Details

Business	• **E-Government Alignment:** IEE, G2G, G2B, G2C
	• **Trigger:**
	  ○ Part 1: A user requires access to an application
	  ○ Part 2: A user's access need has changed
	  ○ Part 3: A user no longer requires access to the application
	• **Actors:** Individual/User, Privilege Manager, Provisioning Workflow
	• **Endpoint:**
	  ○ Part 1: A user account is created for the user with the appropriate access privileges
	  ○ Part 2: The user's access privileges are updated to reflect a change in access need
	  ○ Part 3: The user account is deactivated or removed from the application

Data	**Data Elements** • Username • Position • Membership • Access Permission • Roles and Attributes **Data Repositories//Systems** • Authoritative agency identity repositories • Application-specific user database
Service	• AAES • Resource Attribute/Metadata Management • Account Management • Bind/Unbind • Provisioning • Privilege Administration • Backend Attribute Retrieval • Policy Administration • Audit Trail
Technology	**Hardware/Software** • Standards based provisioning engines **Standards** • Backend Attribute Exchange (BAE) Specifications • LDAP v.2 and v.3; • XML • SAML 2.0 • SPML • WSDL • WS-Federation/ID-WSF • WS-I BSP

Figure 34: Use Case 7 Target Architecture Details

4.7.3. Gaps

This section provides a summary of the high-level gaps between the as-is and target states for this use case. Gaps may focus on Data, Technology, Business and/or Service Layer activities. Explanations about the drivers and impact of each gap are also provided.

- **Lack of automation in provisioning workflows.** Manual provisioning should be replaced by centralized workflow engines. These engines should be able to provision or deprovision users based on established business rules such that a single push can provision/change/deprovision multiple access control points or a user access request can trigger pull-based queries to provision/change/deprovision a single access point. Agencies must tie all relevant applications/systems into the automated workflow where feasible and upgrade legacy systems as needed.
- **Lack of integration between provisioning and other ICAM processes (e.g., credentialing and access control).** Centralizing provisioning functionality and leveraging authoritative identity data for users will increase accuracy and reliability of user data tied to accounts within individual applications.
- **Lack of integration interoperability from a technology perspective.** Many of the products that would be targets for integration do not have open/exposed interfaces for this capability.

4.8. Grant Physical Access to Employee or Contractor

This use case 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 has been separated from granting physical access to visitors and individuals with limited local facility access (covered in 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 the as-is state and a PIV card in the 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) processes in advance of the physical access attempt.

4.8.1. As-is Analysis

Agencies control access to their facilities through the use of PACS. In the as-is state, the 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 cards technologies are also used across the Federal Government. With the exception of contactless smart cards, each of these technologies transmits a static number, which is matched against an access control list, to the PACS in order to grant access.

Legacy PACS implementations provide little assurance in the identity of the individual requesting access. Transmission rates for the technologies are relatively low, which limits the size of the number that can be transmitted. The small number size combined with the prevalence of proprietary formats increases the chances that a card number will not be unique, which could allow an unintended individual access. Additional authentication factors that could increase assurance, such as PINs and biometrics, are not widely used outside of highly secured facilities.

PACS systems are commonly comprised of readers located at a doorway or portal, and locking devices installed at access points throughout a facility. One or more servers store identity, card, access point, and transaction information. To improve the speed of the access control transaction and reduce single points of failure, information is distributed to an array of panels that receive information from the readers, make access control decisions and release locking devices based on predefined rules. The PACS panels are normally located in the secured zones of the building.

Challenges in the as-is state include:

- **Interoperability.** PACS deployed in many Federal buildings are generally facility-centric rather than enterprise-centric and utilize proprietary PACS architectures. Therefore, many issued 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. CHUID) associated with PIV cards necessary for government-wide interoperability.
- **Security.** Deployed PACS readers can read an identifying number from a card, but in most cases they do not perform a cryptographic challenge/response exchange. Most bar code, magnetic stripe, and contact cards can be copied easily. The technologies used in these systems may offer little or no identity assurance (they validate the card not the cardholder).

- **Validity.** Many existing PACS verify expiration of credentials through a date stored in a site database. There is no simple way to synchronize the expiration or revocation of credentials for a Federal employee or contractor across multiple sites.

Key assumptions for this use case include:

- Access points referred to in the process flow should be considered general representations of any access point for a facility. 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 a future state process and is outside of the scope of the as-is process flow.
- Processes to provision users into the PACS and establish access control policies and lists are performed in advance of the start of the process flow.

4.8.1.1. Process Flow

This as-is process flow for this use case offers two options for authenticating an individual and granting access: 1) physical/visual inspection, 2) electronic verification of the card. One or both options may be in place within an agency, depending on the facility/access point. The steps for each option are:

Option 1: Physical/Visual Inspection

1. A Cardholder desires access to a facility/area and presents his ID card to the security officer at the entry point.
2. The security officer visually authenticates the card by inspecting the topographical features on the front and back of the card. The officer checks to see that the card looks genuine, compares the cardholder's facial features to the facial image on the card, checks the expiration date printed on the card, checks for the issuing authority's logo/emblem and visually verifies available security features on the card.
3. Following successful visual authentication, the security officer grants or denies access to the Cardholder based on the access policy at that access point.

Option 2: Electronic card verification

1. A Cardholder desires access to a facility/area and presents his card to the card reader on the attack side of the access point.
2. The reader reads the static number from the card and transmits it to the PACS panel. The reader may additionally prompt the Cardholder to perform a PIN or biometric match in some instances.
3. The panel matches the card number against an access control list and access policies to make an access determination.
4. Upon successful verification, the panel notifies the locking mechanism, the entry point opens, and the Cardholder is granted access to the facility/area. If verification is unsuccessful, the access attempt is denied, and the locking mechanism remains locked.
5. The PACS creates a record of the access event.

4.8.1.2. Architecture Analysis

The following table provides details for the Business, Data, Service, and Technology Layers of the ICAM segment architecture in support of this use case in the as-is state. An overview of the segment architecture layers can be found in Chapter 4.

Architecture Layer	Architecture Details
Business	• **E-Government Alignment:** IEE • **Trigger:** Cardholder requests access to a facility • **Actors:** Cardholder, Security Officer • **Endpoint:** Cardholder granted or denied access

Data	**Data Elements**
	• Agency ID Card Physical Data
	  ○ First, Middle, and Last Name
	  ○ Facial Image/Photo
	  ○ Employee Affiliation
	  ○ Organizational Affiliation
	  ○ Expiration Date
	  ○ Agency Card Serial Number
	  ○ Issuer Identification
	• Contact or PIV Card Logical Data
	  ○ Unique Identifier
	  ○ Electronic Proprietary Unique Identifier
	Data Repositories/Systems
	• PACS

Service	• Access Authorization • Data Exchange • Policy Enforcement • Policy Decision • Audit Trail
Technology	**Hardware/Software** • Card – contact or contactless • Panel • Reader – 125 kHz or 13.56 MHz • PACS Server **Standards** • ISO/IEC 7810 (card physical structure) • ISO/IEC 10373 (card physical structure) • ANSI 322 (card physical structure) • ISO/IEC 7816 (contact card specification) • ISO/IEC 14443 (contactless card specification) • ISO/IEC 7811 (magnetic stripe specification)

Figure 35: Use Case 8 As-is Architecture Details

4.8.2. Target Analysis

The target state for this use case reflects full implementation of the PIV card for electronic physical access for employees and contractors based on the guidance provided in SP 800-116. By establishing an access control enterprise, agencies will promote government-wide interoperability and resolve the security challenges in the current state. Multi-factor authentication involves three distinct types of authentication factors: a) something you have, in this case, a PIV card, b) something you know, knowledge of the PIN to access protected areas of the PIV card, and c) something you are, cardholder fingerprint match with biometric data stored on the card. The confidence of the authentication increases with the number of factors used.

SP 800-116 specifies several authentication mechanisms using the PIV card to establish confidence in the identity of the cardholder. Figure 36 provides a list of PIV authentication mechanisms and their authentication factors.

PIV Authentication Mechanism	Have	Know	Are	Authentication Factors	Interface
Card Authentication Key (CAK) + BIO-A	X	X	X	3	Contact
Attended Biometric Match (BIO-A)	X		X	2	Contact
PKI	X	X		2	Contact
Biometric Match (BIO)			X	1	Contact
CAK	X			1	Contact/ Contactless
CHUID verification + Visual Inspection (VIS)	X			1	Contact/ Contactless

Figure 36: PIV Authentication Mechanisms

Assumptions for this use case include:

- The card leveraged in this use case is a PIV conformant card based on SP 800-73.
- Processes to provision users into the PACS and establish access control policies and lists are performed in advance of the start of the process flow.
- Specific combinations of PIV authentication mechanisms are determined at agency discretion and are outside the scope of this use case.[41]
- 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 forms of biometrics specific to an agency implementation are not included in this use case.
- Process flows assume successful authentication; failure to authenticate will result in a failed access attempt.

4.8.2.1. Process Flow

The target state for this use case includes the following steps:

1. A Cardholder desires access to a facility/area and presents his card to the card reader on the attack side of the access point.

[41] A list of authentication mechanism combinations can be found in Appendix C of SP 800-116.

2. The Cardholder presents his PIV card (contact or contactless interface) to the card reader. The Cardholder performs authentication using one or some combination of the following processes:
    a. **CHUID + VIS:** The panel controlling access to this door receives frequent updates from the PACS server and validates the CHUID on the PIV card. In order to achieve single factor authentication, the asymmetric signature of the CHUID must also be validated at the reader. In order to check the signature, the panel would have to have all the public keys.
    b. **CAK:** Authentication of card is completed using the Card Authentication Key (CAK), a unique PIV key that may be used on a contactless or contact card in a challenge/response protocol. The card reader obtains the CAK certificate from the PIV card, validates the certificate (checking the certificate's expiration date) and sends a challenge to the card to verify that the card holds the private key corresponding to the certificate. The certificate and rights to access the facility are already pre-provisioned to the server.
    c. **BIO:** A PIN match must be performed before the biometric match can be attempted. The cardholder provides a live fingerprint sample, which is validated against the biometric information embedded within the PIV card. The PACS verifies the signature on the biometric data object. *This authentication mechanism does not include authentication of the PIV card.*
    d. **BIO-A:** A PIN match must be performed before the biometric match can be attempted. In addition to the steps in process C, a Security Officer supervises the use of the PIV card and the submission of the PIN and the biometric sample by the cardholder.
    e. **PKI:** The Cardholder provides PIN for validation by the PIV card. The PIV card validates the PIN and activates the card. The PACS validates the PIV Authentication Certificate. The PACS validates the digital signature of the certificate via challenge/response.
    f. **CAK + BIO-A:** This includes an integration of the steps from options B and D. The verification of the PIN can be trusted because the PIV card is authenticated by the CAK.
3. Upon successful verification, the panel notifies the locking mechanism, the entry point opens, and the Cardholder is granted access to the facility/area. If verification is unsuccessful, the access attempt is denied and the locking mechanism remains locked.
4. The PACS creates a record of the access event.

The figure below shows the data interchanges and information flow as described in the processes outlined above. The hexagonal figures represent the various services that are employed throughout the process. Repositories and actors are also depicted. This graphical depiction of the process should illustrate the architecture needed to support this target state use case.

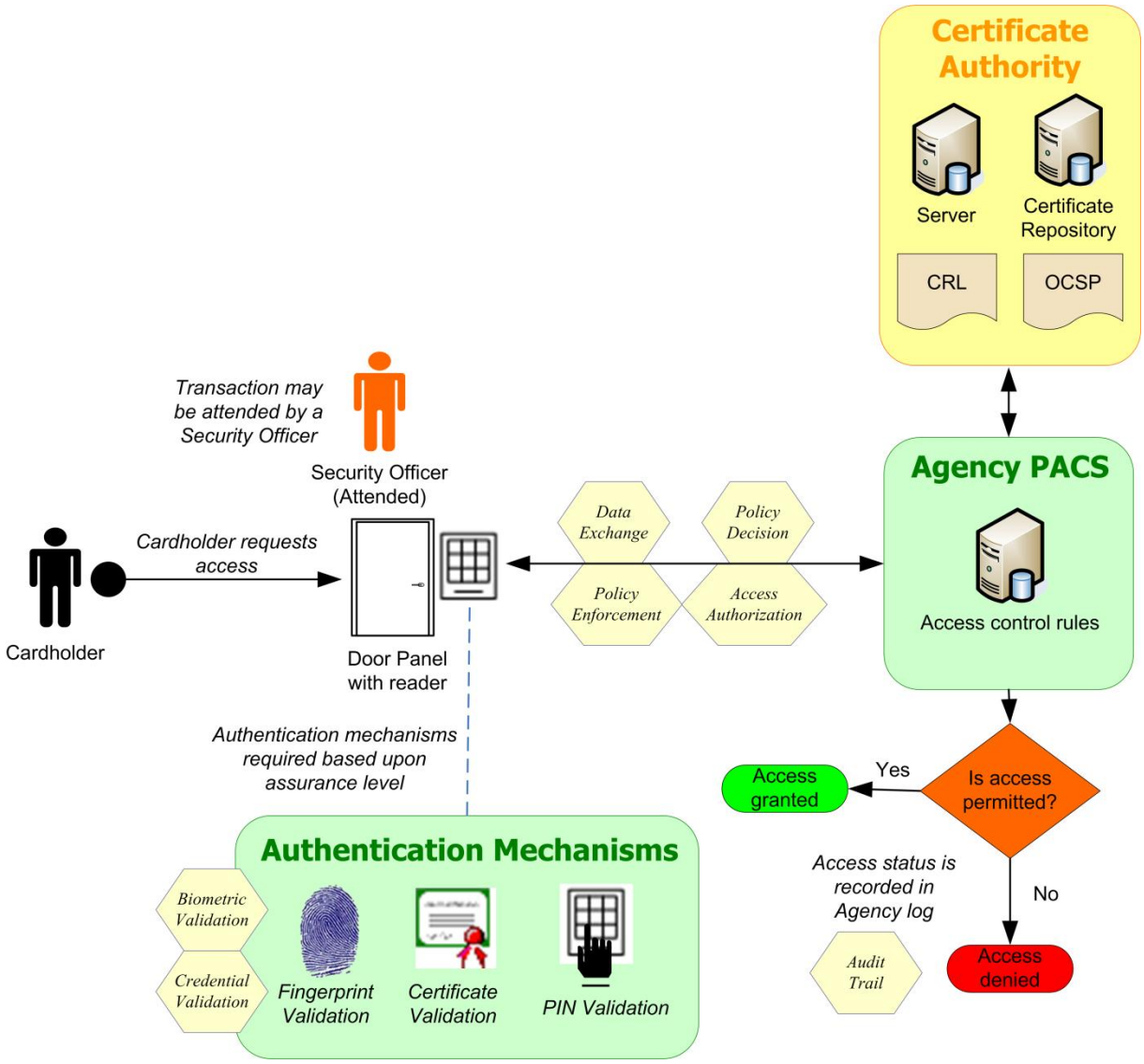

Figure 37: Use Case 8 Target Process Diagram

4.8.2.2. Architecture Analysis

The following table provides details for the Business, Data, Service, and Technology Layers of the ICAM segment architecture in support of this use case in the target state. An overview of the segment architecture layers can be found in Chapter 4.

Architecture Layer	Architecture Details
Business	• **E-Government Alignment:** IEE • **Trigger:** Cardholder requests access to a facility • **Actors:** Cardholder, Security Officer • **Endpoint:** Cardholder granted or denied access
Data	**Data Elements** • PIV Card Physical Data ○ Security Object ○ First, Middle, and Last Name ○ Facial Image/Photo ○ Employee Affiliation ○ Organizational Affiliation ○ Expiration Date ○ Issuing Authority emblem or ID ○ Agency Card Serial Number ○ Issuer Identification • PIV Card Logical Data ○ PIN ○ CHUID ○ CAK Authentication Data ○ Fingerprint Templates **Data Repositories/Systems** • PACS
Service	• Access Authorization • Data Exchange • Resource Attribute/Metadata Management • Policy Enforcement • Policy Decision • Biometric Validation • Credential Validation
Technology	**Hardware/Software** • Card – contact or contactless • Panel • Reader –13.56 MHz • PACS Server **Standards** • ISO/IEC 7810 (card physical structure) • ISO/IEC 10373 (card physical structure) • ANSI 322 (card physical structure) • ISO/IEC 7816 (contact card specification) • ISO/IEC 14443 (contactless card specification) • ISO/IEC 7811 (magnetic stripe specification) • RFC 3852 • SP800-73 • SP800-78 • SP800-116 • FIPS140 (crypto module for generating cryptographic keys) • SP800-76 (biometrics)

Figure 38: Use Case 8 Target Architectural Analysis Details

4.8.3. Gaps

This section provides a summary of the high-level gaps between the as-is and target states for this use case. Gaps may focus on Data, Technology, Business and/or Service Layer activities. Explanations about the drivers and impact of each gap are also provided.

- **Inability of many installed PACS technologies to meet new requirements for electronic authentication outlined in NIST SP800-116.** Current technologies and processes must be upgraded to ensure electronic authentication of PIV cards and multi-factor authentication as defined in NIST SP800-116 (as needed based on risk and maturity models). Agencies should adopt an approach to managing physical access across the enterprise that links individual PACS via a federated network wherever possible.
- **Lack of integration between PACS and other ICAM systems (provisioning and credentialing systems).** Enabling PACS in this manner requires linking with centralized or federated systems that can provide user attributes and credential information from authoritative data sources.
- **Need to determine which PIV features are required to adequately mitigate the inherent risks associated with physical access control for agency facilities.** SP 800-116 PACS authentication mechanisms are to be implemented based on risk-based assessments of the facilities and access points for each agency. Agencies must use completed facility risk assessments or conduct new assessments if they have not been done in order 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

This use case provides the high-level process steps necessary to authenticate and authorize a visitor or an individual who requires local physical access to federally-controlled facilities and sites. 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, etc.). Both groups are addressed in this use case and it is expected that they may be granted access through different processes with multiple ID types.

This use case is also closely related to the processes of digital identity creation (Use Case 2), credentialing (Use Case 4), and provisioning (Use Case 7). These processes are sometimes performed at a localized level within this use case, depending on the type of individual attempting access.

4.9.1. As-is Analysis

Today 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. Current challenges include:

- Inability of current infrastructure to validate external agency identity credentials.
- Lack of automated mechanisms used to collect visitor data prior to their arrival at an agency facility/site.
- No standardization around the types of credentials issued for visitor or facility access.

Key assumptions for this use case include:

- No data is being provisioned in the PACS in the as-is state.
- Agency-specific processes for access to restricted or higher clearance areas/facilities are considered out of the scope of this use case.
- All visitor access is substantiated by a sponsor, who validates the visitor's need to access the facility or area.
- A visitor management system in place. In the as-is state, it is noted that this may be an electronic system or a system of manual logs used to track visitor access.

4.9.1.1. Process Flow

This use case is divided into two parts: 1) granting access to an agency visitor and 2) granting access to an individual requiring extended local facility access.

Part 1: Grant access to an agency visitor

1. A Visitor identifies a need to access an agency's facility. The Visitor contacts his Sponsor and/or the security office directly to initiate a visitor request form, if required.
2. The Sponsor, in consultation with the Visitor, completes the visitor request form and submits it to the agency's security office. The form may include (but is not limited to) the following data:

a. Name
b. SSN
c. Citizenship
d. Date and time of visit
e. Affiliation
f. Campus/building/room to be visited
g. Entry point of visitor
h. Point of contact's name, phone number and email
i. Point of contact's campus/building/room
j. Escort name and contact number
k. Purpose of visit
l. Clearance required

3. A Security Officer enters visitor request form into the Visitor Management System (in the case of a manual form). The Security Officer confirms the data submitted is valid. Officer also determines if the visitor requires any additional screening or an escort per agency or facility security policy.
4. The Visitor is notified (via phone or email) of access request approval/rejection.
5. The Visitor arrives at the facility to which he needs access. If a visitor access form was not required or completed in advance, the Security Officer may collect some or all of the same information from Step 2 above in person and enters it into the Visitor Management System. Where manual visitor management systems are in place, the Visitor may enter this information himself into a paper log.
6. The Visitor presents some form of physical identification (e.g., driver's license or ID card from another agency). The Security Officer inspects and validates the identification and confirms the access request upon successful validation.
7. The Security Officer issues a visitor badge to the Visitor. Depending on the agency, this may be a paper form or an electronic badge processing system. Some badges may also include additional security features such as a facial image or UV inks. Some badges may have the ability to provide electronic access, but these are pre-provisioned in the PACS with no specific identity information tied to them. If a Visitor possesses an ID card from another agency, it may be used in lieu of a visitor badge.
8. The Visitor may be required to follow other security measures such as walking through a metal detector or leaving his cell phone behind.
9. If an escort is required, the Security Officer contacts the escort and informs him that the visitor is waiting and needs to be signed-in/confirmed. Depending upon the agency, the escort may be required to provide his own identification and/or sign the access log book.

10. Upon exiting the facility, the Visitor returns his badge and may also be required to sign-out in the access log book. If an escort was required, the escort may also be required to show his identification or to sign-out the visitor.

Part 2: Grant local facility access to an individual

1. An agency determines that an individual requires local facility access.
2. The individual undergoes an identity proofing process commensurate with his position or relationship with the agency. These processes are considered agency- or facility-specific and may vary widely (e.g., a child care worker versus another non-agency tenant in a facility).
3. The individual is issued an ID card to be used for physical access. This card may be the same as or similar to a legacy (i.e., non-PIV) agency ID card.
4. On each occasion that the individual arrives to the facility to gain access, the Security Officer follows an agency- or facility-specific process for validating the credential and granting or denying access. This process may resemble the process for granting access to an agency employee or contractor (outlined in Use Case 8) or may more closely align with some of the process steps for granting access to a visitor (as defined in Part 1 above).

4.9.1.2. Architecture Analysis

The following table provides details for the Business, Data, Service, and Technology Layers of the ICAM segment architecture in support of this use case in the as-is state. An overview of the segment architecture layers can be found in Chapter 4.

Architecture Layer	Architecture Details
Business	• **E-Government Alignment:** IEE, G2G, G2C, G2B • **Trigger:** A Visitor requires access to a facility • **Actors:** Visitor, Sponsor, Security Officer • **Endpoint:** temporary access granted to facility/building
Data	**Data Elements** • Access Request Form ○ Visitor Name ○ SSN ○ Citizenship ○ Affiliation ○ Date and time of visit ○ Campus/building/room to be visited ○ Entry point of visitor ○ Point of contact's name, phone number and email ○ Point of contact's campus/building/room ○ Escort name and contact number ○ Purpose of visit ○ Clearance required • Access Log Book ○ Visitor Name ○ Date ○ Sign-in time ○ Sign-out time ○ Visitor Signature ○ Agency/Company representing ○ Sponsor signature

Architecture Layer	Architecture Details

	• Temporary/Visitor Badge/Card
	  ○ Facial Image/Photo
	  ○ Organizational Affiliation
	  ○ Temporary/Visitor identification
	  ○ Agency Card Serial Number
	  ○ Issuer Identification
	  ○ Unique identifier (if card provides electronic access)
	• Other forms of identification
	  ○ Driver's license
	  ○ Military ID
	  ○ Other agency identity card (see Use case 8 architecture analysis for more specific data elements)
	Data Repositories/Systems
	• Visitor Management System
	• NCIC

Service	• Account Management • Bind/Unbind • Provisioning • Privilege Lifecycle Management • Sponsorship • Credential Validation • Access Authorization • Policy Administration • Policy Enforcement • Policy Decision • Audit Trail
Technology	**Hardware/Software** • Badge • Badge processing system/software • Metal detector or other security mechanisms • GUI Interface to Management System **Standards** • ISO/IEC 7810 (card physical structure) • ISO/IEC 10373 (card physical structure) • ANSI 322 (card physical structure) • ISO/IEC 7816 (contact card specification)

Figure 39: Use Case 9 As-is Architectural Analysis Details

4.9.2. Target Analysis

In the target state, it is expected that agencies will continue to manage visitor access processes in accordance with agency policy and security requirements; however, target 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, the target state will standardize on the use of PIV credentials for access and will incorporate the ability to provision outside PIV cards credentials into the PACS and perform electronic authentication.

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), subject to agency or facility security policies. A FAC is

an ID card that is technically compatible with, but physically and electronically distinct from,[42] the PIV card. The FAC should be interoperable with PIV cards and allow for access to local facilities through electronic authentication mechanisms.

Key assumptions for this use case include:

- An electronic visitor management system in place.
- An infrastructure is in place to support cross-agency use and acceptance of PIV cards (e.g., federation).

It is useful to note that the functionality described in the target state may be established by a common service provider across agencies. Using a shared service provider for visitor access control can greatly improve the efficiency and effectiveness of the target state. Rather than each agency developing its own solutions, it would be more efficient for common provider(s) to develop a set of protocols to standardize the data exchanged between agencies for electronic visit requests.

4.9.2.1. Process Flow

This use case is divided into two parts: 1) granting access to an agency visitor and 2) granting access to an individual requiring extended local facility access.

Part 1: Grant access to an agency visitor

1. A Visitor identifies a need to access an agency's facility. The Visitor contacts his Sponsor and/or the security office directly to initiate a visitor request form, if required.
2. The Visitor enters the required data into or completes an online visitor request form and submits it to the agency's security office, if required. The security form is saved to the agency's Visitor Management System. The form includes the same data as described in the as-is state.
    a. Alternatively, if the visitor is invited by a sponsoring party, it is possible to have this information pre-populated from authoritative data sources. In this case, the visitor would simply accept the invitation.
3. If the visitor is a PIV or PIV-interoperable cardholder, he may register his credential for expedited access upon arrival at the facility.
4. The electronic visitor request form is routed to the Visitor's Sponsor for approval, if required. This information may be automatically rerouted for additional screening where applicable.
5. Security Officer receives an electronic notification to review the new access request. Upon approval, an email notification is automatically generated and sent to the visitor approving the access request.
6. The Visitor arrives at the facility to which he needs access. If a visitor access form was not required or completed in advance, the Security Officer may collect some or all of the same information from Step 2 of the visitor request form above in person and enter it into the Visitor Management System.

[42] as required by OMB Memorandum M-05-24, "HSPD-12 Implementation Guidance for Federal Departments and Agencies"

7. The Visitor provides some form of physical identification, which is validated using one of the following methods:
    a. If the Visitor does not possess a PIV or PIV-interoperable card, the Security Officer inspects and validates the identification and confirms the access request upon successful validation. The Security Officer then issues a visitor badge to the Visitor.
    b. If the Visitor possesses a PIV or PIV-interoperable card, it should be electronically authenticated using the mechanisms outlined in Use Case 8. This access attempt may be performed in the presence of the Security Officer but does not necessarily require human intervention. If the Visitor used a PIV or PIV-interoperable card, it may also be inserted into a reader that checks against either a CRL or OCSP via the Federal Bridge infrastructure. If the card was not and the card is validated and provisioned into the PACS in advance of the Visitor's arrival, it may be done at this time.
8. The Visitor may be required to follow other security measures such as walking through a metal detector or leaving his cell phone behind.
9. If an escort is required, the escort is notified by automatic means that the visitor is waiting and needs to be signed-in/confirmed. Depending upon the agency, the escort may be required to scan his PIV card against the reader to validate in the PACS that he is the visitor's escort for that visit. To enter a specific facility or doorway, the visitor first scans his badge at a reader, and then the escort scans his own badge prior to the door opening.
10. Upon exiting the facility the visitor and/or the escort may be required to scan the reader with their badges to show the visitor has completed his visit. If a badge was issued to the visitor for the duration of the visit, the badge is returned, disassociated with the user and deactivated in the PACS. Visitor PIV cards provisioned in the PACS will lose any privileges beyond the agreed upon timeframe.

Part 2: Grant local facility access to an individual

1. An agency determines that an individual requires local facility access.
2. The individual undergoes an identity proofing process commensurate with his position or relationship with the agency. These processes are considered agency- or facility-specific.
3. The agency issues the individual a Facility Access Card to be used for physical access.
4. On each occasion that the individual arrives to the facility to gain access, the FAC should be authenticated using electronic mechanisms using the PACS, which grants or denies the access attempt. Unless agency or facility policy requires an escort for the individual, it is anticipated that this process will closely resemble the process for granting access to an agency employee or contractor (outlined in Use Case 8).

The figure below shows the data interchanges and information flow as described in the processes outlined above. The hexagonal figures represent the various services that are employed throughout the process. Repositories and actors are also depicted. This graphical depiction of the process should illustrate the architecture needed to support this target state use case.

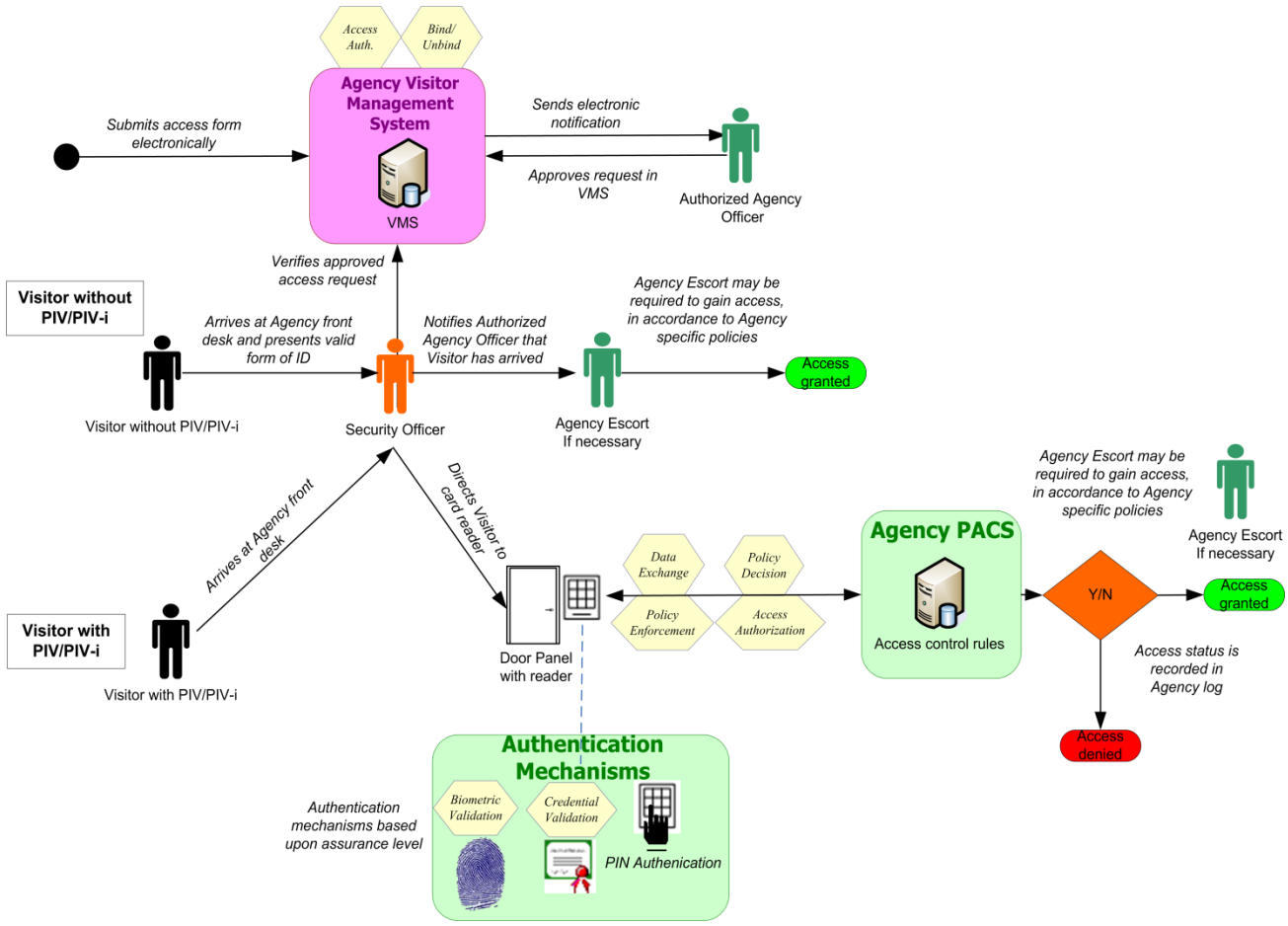

Figure 40: Use Case 9 Target Process Diagram

4.9.2.2. Architecture Analysis

The following table provides details for the Business, Data, Service, and Technology Layers of the ICAM segment architecture in support of this use case in the target state. An overview of the segment architecture layers can be found in Chapter 4.

Architecture Layer	Architecture Details
Business	• **E-Government Alignment:** IEE, G2G, G2B, G2C • **Trigger:** Visitor needs to access a facility • **Actors:** Visitor, Sponsor, Security Officer • **Endpoint:** Temporary access granted
Data	**Data Elements** • Access Request Form (some combination of) ○ Visitor Name ○ SSN ○ Citizenship ○ Affiliation ○ Date and time of visit ○ Campus/building/room to be visited ○ Entry point of visitor ○ Point of contact's name, phone number and email ○ Point of contact's campus/building/room

Architecture Layer	Architecture Details
	○ Escort name and contact number ○ Purpose of visit ○ Clearance required • Temporary/Visitor Badge/Card (some combination of) ○ Facial Image/Photo ○ Organizational Affiliation ○ Temporary/Visitor identification ○ Agency Card Serial Number ○ Issuer Identification ○ Unique identifier (if card provides electronic access) • Other forms of identification ○ Driver's license ○ Military ID ○ Employee ID Card ○ Other agency badge/card (see Use case 8 architecture analysis for more specific data elements) • PIV Card Physical Data ○ First, Middle, and Last Name ○ Facial Image/Photo ○ Employee Affiliation ○ Organizational Affiliation ○ Expiration Date ○ Agency Card Serial Number ○ Issuer Identification • PIV Card Logical Data ○ Unique Identifier ▪ Electronic Proprietary Unique Identifier OR ▪ CHUID ▪ CAK Certificate ▪ PIV Auth Certificate **Data Repositories/Systems** • Visitor Management System • NCIC • PACS
Service	• Account Management • Bind/Unbind • Provisioning • Privilege Lifecycle Management • Resource Attribute/Metadata Management • Sponsorship • Credential Validation • Access Authorization • Policy Administration • Policy Enforcement • Policy Decision • Audit Trail • Credential Validation • Federation • Self-Service
Technology	**Hardware/Software** • Badge • Badge processing system/software • Metal detector or other security mechanisms **Standards** • ISO/IEC 7810 (card physical structure) • ISO/IEC 10373 (card physical structure) • ANSI 322 (card physical structure)

Architecture Layer	Architecture Details
	• ISO/IEC 14443 (contactless card specification) • RFC 3852 (Asymmetric Digital Signature Syntax) • SP800-78 (Asymmetric Signature algorithm and key size requirements)

Figure 41: Use Case 9 Target Architectural Analysis Details

4.9.3. Gaps

This section provides a summary of the high-level gaps between the as-is and target states for this use case. Gaps may focus on Data, Technology, Business and/or Service Layer activities. Explanations about the drivers and impact of each gap are also provided.

- **Lack of automation and consistency in agency processes/systems used for visitor access control.** 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). Additionally, software should be implemented to enforce escort rules at access points.
- **Inability to electronically authenticate and accept PIV and PIV-interoperable credentials from visitors.** PACS should make use of PIV and PIV-interoperable credentials (including certificate checks for level 4 access points) 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. This use case also relies upon completion of digital identity creation (Use Cases 1 and 2), credentialing (Use Cases 4 and 5), and provisioning (Use Case 7) processes in advance of the logical access attempt. Logical access processes consume the credentials and identities already established in previous use cases. In implementation, centralized systems or software employed in target scenarios may service logical access systems, physical access systems, and support the provisioning workflow without distinguishing between those functions.

4.10.1. 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. As was discussed in Use Case 6, a user ID/password combination is most prevalent in the as-is state. Other types of tokens currently in use at an agency for granting logical access include:

- A onetime password generator
- An approved and internally-issued PKI soft certificate
- Biometric matching
- A trusted smart card
- USB tokens and other hardware tokens holding PKI certificates
- A trusted externally issued PKI soft cert
- A trusted third party credential (independently provided identity assertion)

Access to both support- and mission-focused systems are typically granted at the application level. As a result, LACS systems in the current state are in many cases synonymous with the built-in individual application access mechanisms. Some notable exceptions, such as Windows logon, are in most cases centrally managed and provisioned in the as-is state. Once a user has been granted access to the network, however, individual applications both within and outside the agency require additional identity authentication frequently using additional unique user IDs and usually requiring additional unique passwords. This model requires users to possess or remember numerous credentials in order to carry out daily functions.

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, resulting in an inability to manage user accounts or privileges centrally.
- **Lack of trust.** Authentication of user credentials and assertions across applications is based on a network of trust. The framework for trusting external identity and credential providers for access to local applications is not yet established, even within an agency. Also, many applications do not accept externally issued credentials due to an inability to establish and enforce common minimum standards.

- **Redundant and incompatible authentication mechanisms.** Selection and issuance of credentials have historically been managed by individual application owners, resulting in a wide array of proprietary, single use credentials and authentication protocols.

Key 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.
- The high-level steps for performing authentication and authorization are similar, regardless of the credential type used. Detailed methods that are specific to a particular credential type are outside the scope of this use case.
- Applications referred to in the process flow should be considered general representations of any logical resource within the agency. The processes to determine risk for a particular application and establish different authentication mechanisms and security features are considered outside the scope of this use case.
- Use of the PIV card for logical access is considered a future state process and is outside of the scope of the as-is process flow.
- Access to unrestricted applications is outside the scope of this use case.

4.10.1.1. Process Flow

This as-is use case for granting logical access includes the following steps:

1. A User attempts to access an agency network or application, which prompts user authentication.
2. The User presents the designated credential.
3. The application validates the credential using the appropriate authentication techniques.
4. Once the User has been successfully authenticated, the application verifies the User's permissions based on business rules and internal directories to determine if the requested access is allowable.
5. The application makes an access control decision and approves or denies the access attempt. The application records the access event.

4.10.1.2. Architecture Analysis

The following table provides details for the Business, Data, Service, and Technology Layers of the ICAM segment architecture in support of this use case in the as-is state. An overview of the segment architecture layers can be found in Chapter 4.

Architecture Layer	Architecture Details
Business	• **E-Government Alignment:** IEE, G2G, G2C, G2B • **Trigger:** User requests access to a logical resource • **Actors:** User, Application • **Endpoint:** Approval/denial of User Access Request
Data	**Data Elements** • One time password data • Biometric data • Attribute and privilege data • Contact Card Logical Data

Architecture Layer	Architecture Details
	○ Unique Identifier ○ Electronic Proprietary Unique Identifier **Data Repositories/Systems** • LACS • Domain Controller • Local Application
Service	• Credential Validation • Biometric Validation • Session Management • Data Exchange • Access Authorization • Policy Administration • Policy Decision • Policy Enforcement
Technology	**Hardware/Software** • Smart Card – contact • Information Card or other third party credentials • PKI certificates ○ USB tokens containing PKI certificates ○ Soft Certificates ○ PKI certificates on PIV cards • One time password generators • Directory Services • Domain Controller • Card reader • Computer terminal ○ LACS Server ○ Network and other Applications **Standards** • ISO/IEC 7816 (contact card specification) • RFC 3852 (Asymmetric Digital Signature Syntax) • Interface specifications between the service and IDPs • LDAP v.2 and v.3 • Security Assertion Markup Language (SAML) • eXtensible Access Control Markup Language (XACML) • Windows NT 4.0 networking APIs (Net APIs) • Replication Simple Mail Transfer Protocol (SMTP)

Figure 42: Use Case 10 As-is Architecture Details

4.10.2. 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 reuse 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 SP800-63.

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 the 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 are 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.

4.10.2.1. Process Flow

This use case is divided into two parts: 1) granting access to a federal agency employee or contractor and 2) granting access to an external user.

Part 1: Grant access to a federal agency employee or contractor

1. A User attempts to access an agency network or application. The LACS prompts the User to provide his credential to perform user authentication.
2. The User inserts his PIV card into a card reader. In order to allow access to certain authentication mechanisms available on the contact chip, the User inputs his PIN.
3. The LACS validates the PIV using one or a combination of the following authentication mechanisms available on the card and the appropriate authentication techniques:[43]
    a. PIV Authentication Key
    b. Card Authentication Key

[43] A detailed description of how authentication is performed using the PIV mechanisms can be found in SP800-73 Part 1, Appendix B

c. Biometric Check

A separate authentication may be bypassed in instances where a current session has been established based upon previous authentication events.

4. The LACS determines the business rules needed to approve access to the application, including scheme translation, required attributes, and access control policies. Once the User has been successfully authenticated, the LACS sends an assertion that includes any required attributes to the application that the User is trying to access.
5. The application verifies the User's permissions and approves or denies the access attempt based on business rules and internal directories. (Depending on how the LACS is deployed, this step may alternatively be performed by a authorization service component.)
6. The LACS records the access event.

Part 2: Grant logical access to external users

1. An External User (hereafter referred to as the User) requests access to an application in one of two ways:
   a. The request is initiated at the IDP. In this case the User communicates to the IDP information that identifies the application requested after authentication has been performed.
   b. The request is initiated at the application home page and the user is redirected to the IDP to validate the credential.
2. The IDP prompts the User to provide his credential to perform user authentication. The User provides the requested credential.
3. The IDP validates the credential using the appropriate authentication mechanisms and techniques.
4. Once the User has been successfully authenticated, the IDP sends an assertion that includes any required attributes to the LACS service governing access to the application.
5. The LACS decrypts the assertion (as needed) and verifies it.
6. The LACS verifies the User's permissions and approves or denies the access attempt based on business rules and internal directories.
7. The LACS records the access event.

The figure below shows the data interchanges and information flow as described in the processes outlined above. The hexagonal figures represent the various services that are employed throughout the process. Repositories and actors are also depicted. This graphical depiction of the process should illustrate the architecture needed to support this target state use case.

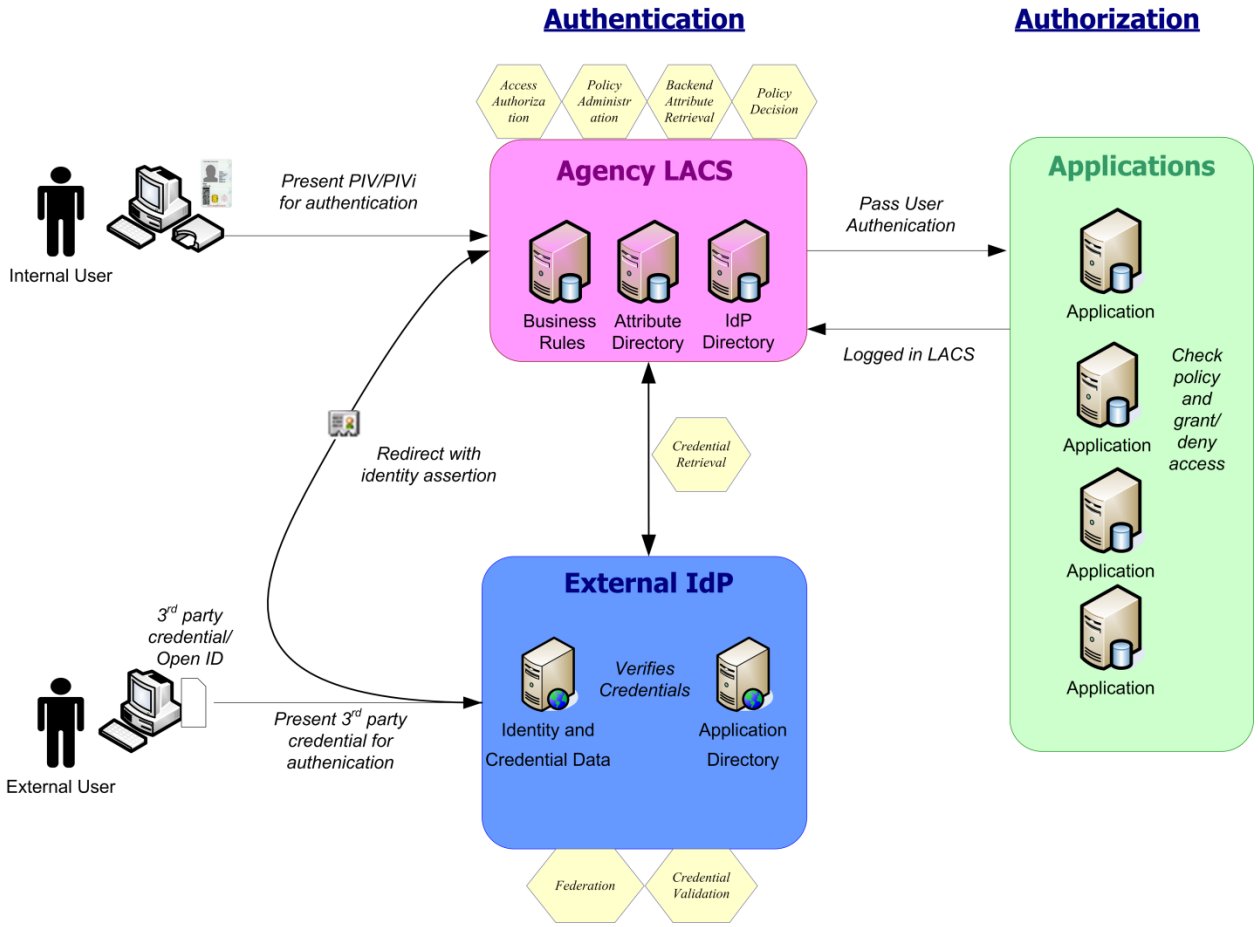

Figure 43: Use Case 10 Target Process Diagram

4.10.2.2. Architecture Analysis

The following table provides details for the Business, Data, Service, and Technology Layers of the ICAM segment architecture in support of this use case in the target state. An overview of the segment architecture layers can be found in Chapter 4.

Architecture Layer	Architecture Details
Business	• **E-Government Alignment:** IEE, G2G, G2C, G2B • **Trigger:** User requests access to a logical resource • **Actors:** User, Credential or Identity Providers, RA, Trust Brokers, Attribute Authorities • **Endpoint:** Approval of User Access Request

Data	**Data Elements**
	• Unique Identifier
	  ○ PKI: PIV Authentication or Card Authentication certificates
	  ○ Biometric Templates
	Data Repositories/Systems
	• LACS
	• Attribute databases

Service	• Resource Attribute/Metadata Management • Credential Retrieval • Backend Attribute Retrieval • Credential Validation

Architecture Layer	Architecture Details
	• Biometric Validation • Session Management • Federation • Access Authorization • Data Exchange • Policy Administration • Policy Decision • Policy Enforcement

Technology	**Hardware/Software**
	• A list of Executive branch applications using a form of identity based access control can be requested from NSTC. This data call was held in support of the National Science and Technology Council Subcommittee on Biometrics and Identity Management IdM Task Force Report
	• Smart Card – contact
	• PKI certificates
	  ○ USB tokens containing PKI certificates
	  ○ Soft Certificates
	  ○ PKI certificates on PIV cards
	• One time password generators
	• PDAs
	• Locally managed PC/MAC
	• Externally hosted PC/MAC
	• Unknown IP network devices
	• UNIX boxes and other servers
	• Domain Controller
	• Card reader
	• Computer terminal
	• LACS Server
	• Network and other Applications
	Standards
	• ISO/IEC 7816 (contact card specification)
	• RFC 3852 (Asymmetric Digital Signature Syntax)
	• SP800-78 (Asymmetric Signature algorithm and key size requirements)
	• Interface specifications between the service and IDPs
	• LDAP v.2 or newer
	• Security Assertion Markup Language (SAML)
	• eXtensible Access Control Markup Language (XACML)
	• Windows NT 4.0 networking APIs (Net APIs) or newer
	• Replication Simple Mail Transfer Protocol (SMTP)
	• Interface specifications between the service and IDPs, TBD
	• (BAE) Interface Specifications
	• Secure Socket Layer (SSL)
	• HTTPS
	• WS-Security
	  ○ SOAP

Figure 44: Use Case 10 Target Architecture Details

4.10.3. Gaps

This section provides a summary of the high-level gaps between the as-is and target states for this use case. Gaps may focus on Data, Technology, Business and/or Service Layer activities. Explanations about the drivers and impact of each gap are also provided.

- **Lack of ability to accept externally issued credentials.** The Federal Government needs federation processes such as direct relationships with trusted IDPs, working with Trust

Broker services, or by entering into a federation of trust. Agencies should also enable relevant applications to accept external third party credentials.

- **Lack of adoption of PIV technologies and processes.** Agencies should adopt the authentication mechanisms of the PIV credential for logical access authentication at all assurance levels for internal users, and upgrade their systems to enable PIV use.
- **Need for enterprise-wide access management capability at the agency level.** Complete an upgrade of current application infrastructures to allow for centralized workflow management for logical access. Determine architecture at the agency level to provide centralized workflows (e.g., implementation of enterprise-wide LACS application).
- **Need for enhanced role and attribute data to perform situational access control. The use of attributes for LACS decisions.** Agencies should 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. Part of this capability will rely on the use of backend attribute exchange across departments to allow for real time access decisions or prior provisioning based on user attributes.

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. A digital signature is the result of a cryptographic transformation of data in order to provide origin authentication, data integrity, and signatory non-repudiation. While encryption and digital signature capabilities are traditionally considered information security processes, they are important security applications of PKI credentials and have therefore been included within the ICAM segment architecture. Securing a document with PKI through encryption and digital signatures relies upon the completion of the PKI credential issuance use cases (Use Cases 4 and 5).

4.11.1. As-is Analysis

In the as-is state, the use of PKI for encryption and digital signature purposes is oftentimes inconsistently applied. For this reason, this use case is considered to be a future state process and no process flow is provided in the as-is state.

4.11.2. Target Analysis

In the target state for internal users, the PIV card will be used as the PKI source for digital signatures and encryption. Also, the target state will provide guidance and best practices by which users can uniformly apply encryption and digital signatures to secure documents and communications.

In the target state, it is envisioned that the issues preventing widespread application of encryption and digital signatures in the current state will be addressed through the following:

- 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. The number of commonly available technologies (e.g., Adobe PDF) available to support PIV PKI certificates must be increased.
- 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 used 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 by an application to recognize a PKI certificate have been completed in advance of the start of the process flow.
- Infrastructure and applications for processing encryption and digital signatures have been implemented in advance of the start of this use case.

- The processes described use PKI certificates. 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 will be performed on behalf of the user by an appropriate application and will be largely transparent from the end user perspective.

4.11.2.1. Process Flow

Encrypting and digitally signing data are two separate processes; therefore, the process flow for this use case has been divided into two parts: 1) encrypting and decrypting a file and 2) digitally signing a file or communication.

Part 1: Encryption and decryption of a file

1. The User obtains the public key for the intended recipient in one of the following ways:
   a. Directory look up (LDAP proxy)
   b. Provided in a prior communication with the recipient
   c. Pulled from a directory published by the CA
2. The User opens the application that will be used to apply encryption and selects the appropriate certificate to use.
3. The application encrypts the file using the public key of the intended recipient of the data.
4. The User transmits the file to the intended recipient. The recipient then decrypts the file using his private key and an appropriate application.

Part 2: Digitally signing a file or communication

1. The User opens the application that will be used to digitally sign the data.
2. The User inserts his PIV card into card reader, in the case of a federal employee or contractor, or selects the appropriate alternate private key, in the case of an external user. If the certificate has been pre-registered, the application may automatically select the appropriate certificate.
3. The User selects the option to digitally sign the data.
4. The application hashes the data and uses the User's private key to encrypt the resulting message digest, thus creating the digital signature.
5. The User transmits the original data (which may or may not be encrypted) along with the digital signature to the intended recipient.
6. The Recipient opens the file and verifies signature. The Recipient first duplicates the creation of the message digest. Then he decrypts the digital signature using the User's public key and compares it to the duplicated message digest. If the two match, the document has not been altered and was signed using the User's private key.

The figures below show the data interchanges and information flow as described in the processes outlined above. The hexagonal figures represent the various services that are employed throughout the process. Repositories and actors are also depicted. This graphical depiction of the process should illustrate the architecture needed to support this target state use case.

Figure 45 represents Part 1 of the process flow.

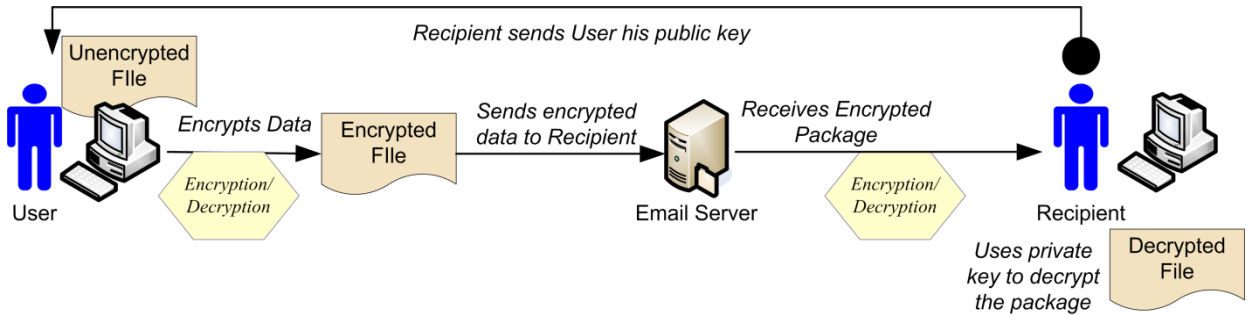

Figure 45: Use Case 11 Target Process Diagram (Encryption)

Figure 46 represents Part 2 of the process flow.

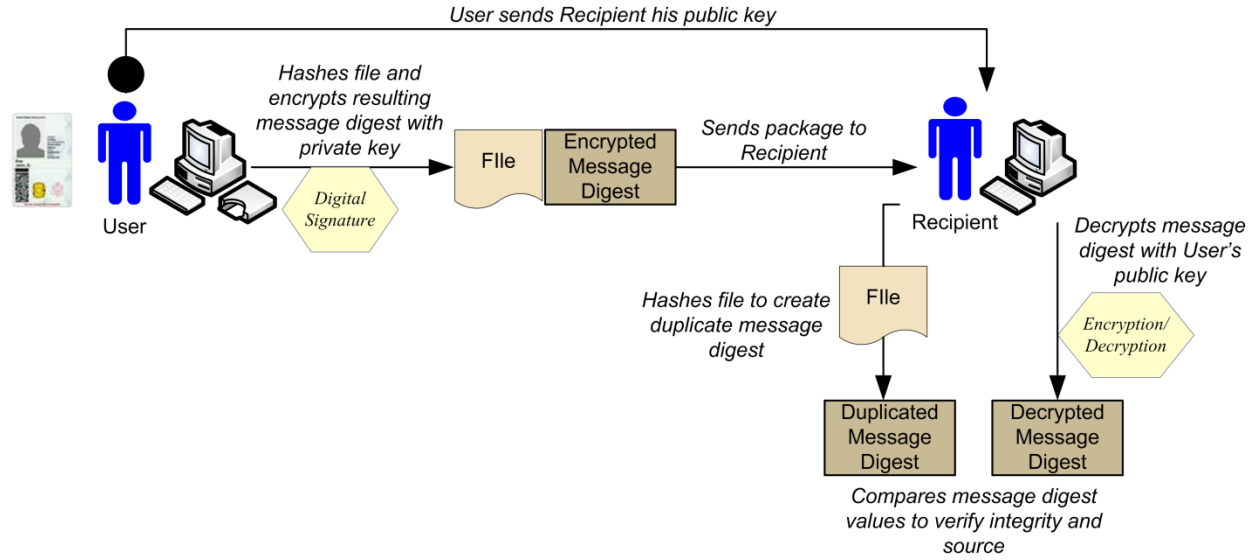

Figure 46: Use Case 11 Target Process Diagram (Digital Signature)

4.11.2.2. Architecture Analysis

The following table provides details for the Business, Data, Service, and Technology Layers of the ICAM segment architecture in support of this use case in the target state. An overview of the segment architecture layers can be found in Chapter 4.

Architecture Layer	Architecture Details
Business	• **E-Government Alignment:** IEE, G2G, G2B, G2C • **Trigger:** User must sign or encrypt a document or message • **Actors:** Certification Authority, Sender (Signatory), Receiver (Verifier) • **Endpoint:** Receiver decrypts document or verifies digital signature
Data	**Data Elements** • PKI Certificates and Keys • Hashes • Security Object **Data Repositories/Systems** • PKI directories • Local Application Certificate Cache

Architecture Layer	Architecture Details
Service	• Encryption/Decryption • Digital Signature • PDVAL • Key Management • Audit Trail
Technology	**Hardware/Software** • Federal Bridge Certification Authority • Email applications • Document applications enabled to be used with external encryption **Standards** • Federal Bridge Common Policy • FIPS186 • FIPS 180 • XML • Triple Data Encryption Algorithm (Triple DES), including two and three Triple DES • Advanced Encryption Standard (AES) • NIST Special Publication 800-67 • NIST Special Publication 800-78 • Elliptic Curve Digital Signature Algorithm (ECDSA) • Secure Hash Algorithms (SHA) • RSA • ISO/IEC 18033-3:2005 • X.509 CRLs • OCSP

Figure 47: Use Case 11 As-is Architecture Details

4.11.3. Gaps

This section provides a summary of the high-level gaps between the as-is and target states for this use case. Gaps may focus on Data, Technology, Business and/or Service Layer activities. Explanations about the drivers and impact of each gap are also provided.

- **Lack of government-wide guidance regarding use of encryption and digital signatures.** Currently, there is no implementation guidance for when to use encryption and digital signatures. Policy must provide standards for using PKI to secure emails, encrypt Controlled Unidentified Information (CUI) materials, and applicability for signing legal documents.
- **Lack of adoption of PKI technologies and processes.** Applications used for documentation and email exchanges must be enabled to use PIV PKI.
- **Lack of government-wide guidance for key history management.** Key history is needed to recover documents that have been encrypted using keys now expired or revoked.

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 analysis on their systems and processes so that their ICAM architectures are specific to their own business processes. It is envisioned that 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. Target state business processes will typically encompass multiple use cases; the use cases defined in Chapter 4 are not meant to limit ICAM functionality to only eleven areas nor to imply that each use case must be implemented such that it is wholly self-contained. As a corollary, many technologies may be implemented to fully support two, three, or more of the target use cases. Supporting multiple business processes through technology and service reuse is a core goal of segment architecture.

This section provides several examples of how an agency might leverage the high-level use case framework from Sections 4.1-4.11 to support a mission specific function. Several of the functions described reflect hypothetical Target State capabilities. Further, these scenarios identify how services and technologies may be reused to simplify the business process. There is an example scenario for each of the four E-Government sectors.

4.12.1. 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 she works, and will already have her 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 where she was a contractor, but must switch to a new physical location. The contractor must re-enroll or be reissued a federal PIV credential to indicate her change in status. Likewise, many legacy application logins and Active Directories were based on the contractor's old username and her 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 she had access, and then reinstating her access rights to these or other applications using new credentials.

Actors: Human Resource personnel, Personnel Security Office, provisioning engine, automated attribute exchange service, agency contractor/new employee, PIV Office personnel, local physical access officer

Process Flow:

1. An offer to hire is proffered to an agency contractor (hereafter referred to as a new employee).
2. Human Resource personnel in charge of the hiring process check to see whether the individual is known to the agency; they determine that as a contractor, certain information about the new employee is already available and stored within the Procurement Office (contractor) database.

3. HR requests the personnel security office to verify that existing background or suitability/fitness checks are valid and adequate.
4. HR personnel update the new location designation to the contractor profile. HR then asks the new hire to verify that the information in the contractor database is correct through an online link to a user profile page.
5. The new employee confirms all information in her existing record and saves the profile.
6. Upon submission, the system transfers the contractor profile information into the employee authoritative source repository. The legacy contractor user account is changed to inactive.
7. The automated attribute exchange service is employed to update all links to the new employee's peripheral attributes, such as trainings and clearance level that are not stored with the core identity profile.
8. The provisioning engine links unique identifiers within the Global Address List (GAL) and Active Directory to the original account.
9. The email address listserv creates a new, non-contractor email address for the new federal employee. The provisioning engine associates the email address to the previous email address and the user's unique profile/ user record.
10. Legacy contractor identifiers and email address are deactivated but still affiliated with the user record for audit purposes.
11. HR notifies the new employee to receive a new PIV credential showing her Federal employee status.
12. The new employee makes an appointment at the PIV Office, verifies her biometric, and is issued a new PIV badge as a Federal employee.
13. Applications such as SharePoint and VPN, to which the new employee should retain access, are provisioned using the new credential's information via the automated provisioning engine.
14. Physical access to her previous office building is not reestablished. Rather, the provisioning engine uses her new location code to assign access rights to her new office and provides this information to the local physical security officer.
15. The local physical security officer then approves the privileges requested by the provisioning engine, allowing the new employee access to the building.

This scenario focuses on the transfer and linkage of identity information within an agency, and the subsequent mapping of privileges to the user's new status. From the new employee's perspective, she has been asked to perform maintenance activities for her identity information (Use Case 1) and her PIV credential (Use Case 4). However, many more activities have been performed in the back-end. Many of these involve the correlation and exchange of attributes between databases. These exchanges should be performed using common services and interfaces as described in Use Cases 1, 4, 7, 9 and 10. It also avoids the need to perform a redundant background investigation (Use Case 3) and training. For example, Step 3 above requires that links are created to the user's security clearance status within the Personnel Security Office. Likewise, Step 7 requires a link to databases such as mandatory training completion information

from the Training Office. These links are important to maintain the user's full profile, some of which may be maintained outside of the HR database, and the information transfer could be accomplished through use of an Authoritative Attribute Exchange service.

Many of the interfaces and systems involved can support more than one Use Case as defined in this document. In fact, the mechanisms used for logical access remains the same through the use of an automatic rule based provisioning engine, which enables for the link the new user profile to the old user access rights (Use Case 7). An authoritative attribute exchange service maps the old attributes to the new employee profile (Use Case 1).

4.12.2. G2G: Emergency Responders

Scenario: 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 (in this case, the DoD Common Access Card or CAC) while others will use a PIV-interoperable card (the First Responder Access Card or FRAC).

Actors: Incident Commander, Army Reserve Personnel, Fire Fighters, Resource Supervisors, Perimeter Guard, Headquarters Guard

Process Flow:

1. The incident commander requests resources with appropriate HAZWOPER and clearance attributes using the regional emergency response system.
2. The system searches for suitable responders among state, local, and federal responders in that region.
3. The system identifies four responders with appropriate attributes that are posted nearby, two Army Reserve and two Fire Department personnel.
4. The incident commander creates an official request for these resources, using a digital signature to allow the recipients, the resource supervisors, to validate the sender of the request.
5. The resources' supervisors are notified and approve the request through the automated request service. The incident commander is also notified that his requests have been approved and is given a full list of the anticipated responders.
6. The requested personnel arrive at the perimeter and report to the incident commander.
7. Two users present a DoD CAC while two present a PIV-interoperable First Responder Access Card (FRAC), which the incident commander or his/her designee validate electronically using PIN and biometric checks to assure that they were the requested persons.

8. Upon verification, the incident commander approves the addition of the personnel to the perimeter "white list" and assigns the level and areas of access to these users, firmly associating the users with specified access rights.
9. A headquarters guard then reads the PIV-AUTH certificates from the Army CAC and Fire Fighter FRAC credentials using a handheld smartcard reader, thus provisioning the user accounts into the perimeter access control system. The headquarters guard applied all the approved rights and attributed within the perimeter access control system.
10. A second perimeter security guard authenticates the credentials using a handheld device each time the responders request access.
11. The guard grants access to the restricted area based on successful credential authentication through use of the PIN and a biometric validation, and verification of the user's access privileges.

The first responder activities outlined in the steps above utilize and depend upon many of the business flows and architecture as outlined within several of the Use Cases found in this chapter. For example, the search for suitable resources listed in Step 2 (above) requires that the organizations for the respective individuals collect identity data that can be shared in this scenario (Use Cases 1 and 2). Both the DoD and Fire Fighter personnel will have had information collected from them and populated into the regional request system, either manually or through an automatic push. This user data should be associated with any applicable background investigations performed prior to the event taking place (Use Case 3). For example, army personnel will have undergone the DoD sponsored investigations needed prior to being issued a common access card (CAC). Career Fire Fighters will have undergone different background checks based on their positions as well as meet the minimum check to receive a FRAC. (Other attributes associated with responders are based on training and qualifications. These attributes, stored in DoD and local firefighter databases, must be available via a real-time be reach back capability using the Backend Attribute Exchange protocol.)

Likewise, credentials must have been issued to the responders and the incident commander. The national guardsmen and the firemen were issued PIV and PIV-interoperable credentials; the DoD follows a full PIV model as specified in Use Case 4, while the Firefighters undergo a similar process as outlined in the document "PIV Interoperability for Non Federal Issuers." The action in Step 3 above requires that PKI certificates were issued to the incident commander prior to his use of them, as described in Use Case 5. The site commander was issued a soft certificate through an issuer cross-certified with the Federal Bridge (the Department of Defense) that is stored on his laptop for the express use of signing emails and other communications. PKI soft certificates issued in accordance with the Federal Bridge Common Policy can be accepted at assurance level 3. When the incident commander creates an official request using a digital signature, allowing the recipient to validate the sender of the request, Use Case 11 directly applies.

Provisioning and access control activities described above touch upon several more of this document's use cases. Prior to the emergency responders arriving at the site of the incident, the incident commander would have provisioned these responders a user account (Use Case 7), as described in Steps 7, 8, and 9 above. Then when Steps 10 and 11 above occur, the process looks very similar to the Visitor Access Control Use Case 9.

4.12.3. 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 partner organization to a federal agency, a hospital, is requesting access to clinical trial information conducted by others, and is also attempting to report results for a clinical trial they have conducted using federal funds. The user requires access to two applications from clinicaltrials.gov. Application number one requires a level 3 token to access and report official trial data; application number two 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 an appropriate proof that the user is an authorized representative of a trusted partner organization.

Actors: medical professional, organizational sponsor, application #1, application #2

Process Flow:

1. To begin, the medical professional requests access to the trial data reporting application. The medical professional provides proof of identity and organizational affiliation through an online application form to the reporting application including name, organizational affiliation, and other relevant data.
2. The information collected is mapped to verify whether the user is already known to the agency. The medical professional is unknown to the agency and is a first-time user.
3. The user's information is saved and correlated within the agency authoritative databases, creating a new user profile.
4. The application request is processed automatically and the organizational sponsor for the hospital receives an email request to verify that the individual is a current and appropriate hospital representative with need to input trial data into the agency application.
5. The sponsor approves the request and validates the affiliation through an online link. This enables the privileges for the application to be associated with the medical professional's profile and begins the process for a PKI certificate to be issued.
6. At the same time that the medical professional is granted privileges within the application, a trusted issuer of PKI certificates associated with the organization is sent a sponsored request for a certificate for the user.
7. The medical professional undergoes identity proofing and is issued a "soft" PKI certificate to his work computer.
8. The user's information, both identity and credential, is provisioned in necessary databases.
9. To facilitate the research process, the professional signs up for a second service that will remember his recent searches and sends updates and new research links to him or her based on keyword searches (application #2).
10. The application requests basic information about the user and compares this information to the internal core identity repository. It determines that this individual is already known to the agency and has a PKI certificate issued to the user.

11. The application form requests that the medical professional sign up for various groups (e.g. radiologists, epidemiologists).
12. Upon login to application #1, the application performs real time validation during each access attempt to verify both the PKI certificate is valid and that the professional is still a valid employee with proper rights to access the medical information.
13. Upon login to application #2, the medical professional uses the PKI certificate already issued to authenticate into the application.
14. Once the user has been authenticated, application #2 displays all information related to the user's customized searches and self-identified groups[44].

In this scenario, an external user follows through Use Cases 2, 5, 7, and 10. The process of account creation and mapping between applications (Use Case 2) happens in two distinct ways—one for a new user and one for a user profile already established. However, in both cases the profile is linked to a single user credential, a PKI certificate, which is reused for multiple applications at different assurance levels.

The PKI certificate isn't actually issued by the Federal agency—it is issued by a third party PKI supplier affiliated with the medical professional's organization that is cross certified with the Federal Bridge. However, the application begins the request cycle, and the organizational sponsor acts both the verifier of the user's affiliation and as the sponsor for the PKI certificate. Although not controlled internal to the agency, this process follows exactly the steps found within Use Case 5. Provision engine associates the newly issued credential with the appropriate application (Use Case 7).

The credential holder can use this certificate to log onto the agency application at assurance level three; this is needed to protect sensitive information from the clinical trial. The application is able to validate the certificate's status through the services of the PKI federal bridge (Use Case 10). In addition, an "attribute based access control" real-time verification against the medical partner's user data, using the Backend Attribute Exchange protocol is performed directly to the hospital database. Based on a current and valid organizational affiliation, and a valid PKI certificate check, the user is allowed access to application #1 and can update clinical trial information.

In the As-Is state, users requesting access to application #2 would be issued a username and password as described in Use Case 6. However, application #2 allows the medical professional to sign into the application using his or her trusted PKI certificate, even though the service does not require level three authentication. Use of higher authentication credentials is enabled through using a step-down service supported by the credential issuer, who provides a link to public facing agency applications through which the PKI certificate is validated. The PKI issuer then sends an assertion that is accepted by application #2 in lieu of a password or other level one authentication token. This is one method of enabling federation for logical access (Use Case 10).

[44] It is important to note that this is provided as a high level process flow. A number of additional federal requirements would determine if the individually identifiable health information held by or on behalf of the Federal Government could be used or disclosed in the manner described.

4.12.4. G2C: Citizen Services

Scenario: A citizen leverages 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 a level one or higher assurance credential to access the application.[45] The user has not had previous dealings with the agency, so he or she must provide basic information to the agency to create a user profile. They are then able to use a password issued by a trusted member of a federated identity community (OpenID) for whom they are already a user, MySpace$_{TM}$.

Actors: citizen, provisioning engine, MySpace$_{TM}$, research website

Process Flow:

1. The citizen user navigates to a research website, but does not have a login. The user requests access and begins the process by providing very basic information about himself.
2. The user's information is compared to existing user data using a central service and found not to have a duplicate. The service then creates a new profile for the user based on the information collected by the website.
3. The website asks the user if they have an existing account with any of several suitable password providers, including various telephone companies, software institutions, and several email account service providers.
4. The applicant chooses the option of using an existing password issued from MySpace$_{TM}$ as the mechanism to log into the government application upon future visits.
5. The application forwards this selection to the central provisioning engine, which then creates a link on the user's account to the MySpace$_{TM}$ authentication services.
6. When authenticating to the grant application in the future, the application requires that the MySpace$_{TM}$ system verify the password token. The agency application (the relying party) accepts assertions from MySpace$_{TM}$ (the credential issuer) that the citizen's credentials are valid.

In the As-Is state, a government website that requires a password would normally create a new user profile and then issue a password only for that single application (Use Case 5). In the Target state this process will be eclipsed through the reuse of third party credentials and authentication tokens, such as the MySpace$_{TM}$ password.

The reuse of external credentials requires that many complex interactions be supported in order for the scenario to function properly; centralized provisioning must be able to correlate user records across the agency (Use Case 2) and then link them to a federation of credential providers (Use Case 7). Once linked, the application must be able to accept a third party assertion in lieu of an actual password. Federated logical access is a Target state described in Use Case 10.

5. Transition Roadmap and Milestones

The goal of the ICAM Transition Roadmap is to define a series of logical steps or phases that enable the implementation of the target ICAM segment architecture. The Transition Roadmap provides a comprehensive view across ICAM initiatives to demonstrate the ways in which they work together to achieve the target strategic priorities and vision, 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 the process improvement areas (gaps) identified through the development of the ICAM use cases (see Chapter 4). The implementation recommendations span the implementation of the target performance, business, data, service, and technical layers of the segment architecture as described in the previous chapters.
- **Initiatives and Milestones.** Prioritizes the implementation recommendations into a sequencing plan. The sequencing plan is a summary of investment activities required to achieve the target architecture and includes activity owners and implementation milestones. Agencies are encouraged to include the activities in Section 5.2 in their FY11 budget submissions.
- **Performance Metrics**. Defines government-wide performance metrics, a core part of the performance architecture, through which achievement of strategic improvement opportunities will be measured. The purpose of the performance metrics is to create a reporting framework to measure the success of the activities and investments within the ICAM segment.

The sequencing plan in Section 5.2.3 includes activities and milestones to be completed at both the government-wide and the individual agency levels. Agencies are expected to incorporate the improvement activities, milestones, and metrics identified as part of this ICAM segment architecture into their respective agency-specific architectures and transition roadmaps. Each roadmap should include the specific strategies or activities to close the gaps between the agency-specific current state baseline and the target state vision outlined in the ICAM segment architecture.

5.1. Performance Improvement Recommendations

Each of the use cases in Chapter 4 includes a summary of the gaps between the as-is and target states in meeting the objectives that have previously been defined for ICAM. These gaps span a variety of issues, from outdated technologies, to poor business process fit, to redundancies, etc. Based upon the gap analysis, a set of high-level recommendations has been created to drive business performance improvements. These recommendations are captured in the following table. In some cases, a single gap spanned multiple use cases, or multiple gaps addressed a single or similar challenge; these have been combined in the table below.

Item No.	Performance Gap	Performance Improvement Recommendation
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.
2	Need for common definitions of additional identity attributes required for mission-specific functions.	Implement 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.
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	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.
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.
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.
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.
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.
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.
10	Lack of integration between PIV systems and FEMA Emergency Response Official repository.	Integrate PIV systems with F/ERO database to provide required data.
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.
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.
13	Lack of government-wide approach and guidance for managing key history.	Provide guidance on the management of key history.
14	Lack of product adoption for path discovery and validation.	Implement path discovery and validation products.
15	Administrative and user burden associated with managing and remembering numerous Federally-issued stand-alone 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.
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.

Item No.	Performance Gap	Performance Improvement Recommendation
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.
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.
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.
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.
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.
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.
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.
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.
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.
26	Lack of adoption of PKI technologies and processes.	Fully enable the use of the PIV to further encryption and digital signature usage.

Figure 48: ICAM Performance Improvement Recommendation Summary

In order to provide an actionable transition plan, the high-level performance improvement recommendations must be further developed into specific activities that address business process re-engineering, systems integration, establishment of formal partnerships, and policy development or other transformational approaches for achieving the target ICAM architecture. These specifics are captured in the initiative descriptions and sequencing plan provided in the next section.

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. In order to provide an integrated view of the performance and schedule milestones for the segment, the transition activities have been organized within nine core initiatives that support the goals and objectives of the ICAM segment. The success of the government-wide ICAM strategy is dependent on the completion of activities by both the governance entities at the government-wide level and the agencies themselves. As a result, the nine initiatives within this section have been divided further into the initiatives that are primarily the responsibility of the ICAM governance authorities and the initiatives that are primarily the responsibility of the agencies. In a few instances, activities that have been assigned at the agency level have been included in the government-wide level initiatives and vice versa based upon the best alignment for that activity to the initiatives. Individual owners have been identified in association with specific activities, as appropriate.

5.2.1. Government-wide Level Governance Initiatives

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

- **Initiative 1: Augment policy and implementation guidance to agencies**
  Includes a wide range of policy and guidance that is either currently lacking or is newly required as a result of changes outlined in the target ICAM architecture.
- **Initiative 2: Establish federated identity framework for the Federal Government**
  Includes continued outreach to business partners and service consumers to determine the right approach and resolve interoperability issues associated with federated identity management. Agencies are then expected to implement the recommendations outlined in the government-wide framework, once made available.
- **Initiative 3: Enhance performance measurement and accountability within ICAM initiatives**
  Includes activities designed to mitigate the lack of adoption and performance issues that have plagued legacy ICAM programs and to help ensure strong, consistent performance across agencies.
- **Initiative 4: Provide government-wide services for common ICAM requirements**
  Includes the ongoing or planned creation of government-wide services to reduce redundancy and promote consistency across ICAM needs that are common to all agencies.

5.2.1.1. Initiative 1: Augment policy and implementation guidance to agencies

The following table details the transition activities, activity owner(s), and milestone dates associated with the augmentation of policy and implementation guidance to agencies:

Activity No.	Transition Activity	Activity Owner	Implementation Milestone Date
1.1	Conduct survey to collect existing data standards from agencies in order to help determine a common baseline of digital identity data elements and formats.	Architecture Working Group (AWG)	10/31/2009
1.2	Conduct review of data elements/models for government-wide identity data repositories to help ensure interoperability across multiple repositories.	Federation Interoperability Working Group (FIWG) or AWG	12/12/2009
1.3	Review existing Federal data standards such as NIEM or UCore to determine feasibility of reuse in common digital identity standard.	AWG	11/12/2009
1.4	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 (leverage prior work on Agency-SIP interface).	NIST with input from AWG	03/12/2010
1.5	Issue guidance to agencies following publication of final digital identity data specification.	NIST	4/26/2010
1.6	Provide further implementation guidance on implementation of the BAE specification based on pilot work at DHS and DoD.	RDT	9/28/2009

Activity No.	Transition Activity	Activity Owner	Implementation Milestone Date
1.7	Develop technical guidance for management of key history associated with use of key management certificates on PIV cards (via updates to NIST SP 800-73).	NIST	10/31/2009
1.8	Issue agency/department level policy on the use of PIV credentials for both physical and logical access in accordance with HSPD-12 guidance.	Federal Executive Branch Agencies	3/31/2010
1.9	Promote understanding of OMB requirements for the use of PIV within each agency.	ICAMSC	12/31/2009
1.10	Develop implementation guidance for the use of encryption and digital signatures; including scenarios for securing emails, CUI materials, and signing legal documents.	ICAMSC, RDT	12/31/2009
1.11	Expand the ICAM glossary such that the terms are formalized to provide a standard Federal vocabulary to facilitate inter-Agency agreement and standardization.	ICAMSC, RDT	03/30/2010
1.12	Provide further detail supporting the technical and data layers of the ICAM segment. Develop a government-wide technical architecture that includes common elements of government-wide infrastructure.	AWG	03/30/2010
1.13	Based on the government-wide technical architecture (Activity 1.12), determine whether additional consolidation of ICAM services is feasible for government-wide consumption.	RDT and AWG	5/30/2010
1.14	Develop and publish an interface specification to facilitate the use the AAES for exchange of digital identity data across Agencies.	AWG	5/30/2010
1.15	Develop guidance on use of alternative biometric modalities for use with PIV.	NIST, ICAMSC	6/30/2010
1.16	Develop guidance on the applicability of ICAM to NPEs.	RDT	12/31/2009
1.17	Engage privacy community, DOJ, and industry groups to address any perceived liability associated with IDP services.	ICAMSC	03/31/2010

Figure 49: Initiative 1 Transition Activity Summary

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

The following table details the transition activities, activity owner(s), and milestone dates associated with establishing a federated identity framework for the Federal Government:

Activity No.	Transition Activity	Activity Owner	Implementation Milestone Date
2.1	Develop document outlining the recommendations for mechanisms to accept externally-issued credentials for application authentication of external users.	Citizen Outreach Focus Group (COFG)	10/30/2009
2.2	Complete scheme adoption process for authentication technologies acceptable at assurance levels 1, 2, and 3 and publish on idmanagement.gov.	AWG	7/30/2009

Activity No.	Transition Activity	Activity Owner	Implementation Milestone Date
2.3	Determine and document approach for provisioning logical access for external users at all assurance levels.	COFG/AWG/FIWG	3/31/2010
2.4	Establish and document processes related to accepting and trusting externally issued credentials to support streamlining logical access at all assurance levels.	COFG/AWG/FIWG	3/31/2010
2.5	Establish and document certification process for federated credential and identity providers.	ICAMSC/AWG/FPKIPA	3/12/2010
2.6	Augment existing ICAM framework and provide further guidance on authentication of external entities and decentralized identity provider models to support business with external communities.	ICAMSC, COFG	06/30/2010

Figure 50: Initiative 2 Transition Activity Summary

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

The following table details the transition activities, activity owner(s), and milestone dates associated with the enhancement of performance measurement and accountability across ICAM initiatives:

Activity No.	Transition Activity	Activity Owner	Implementation Milestone Date
3.1	Incorporate SP 800-116 maturity model into the transition plan template for ICAM tracking/ reporting.	OMB	12/31/2009
3.2	Create updated transition plan template for agencies to use to track compliance with ICAM segment architecture.	OMB, RDT	12/31/2009
3.3	Develop recommendations for ICAM maturity models, with specific goals for access control, credentialing, and identity data management.	ICAMSC, RDT	9/30/2010
3.4	Develop gaps and transition plan to align agency architecture with the federal ICAM segment architecture across mission areas and traditionally stove-piped programs.	Federal Executive Branch Agencies	3/31/2010
3.5	Develop measurable performance metrics to evaluate support for and usage of third party (PIV-interoperable) credentials.	RDT and ISC Convergence Committee	12/31/2009
3.6	Develop Performance Reference Model mapping for ICAM performance architecture.	RDT	03/30/2010

Figure 51: Initiative 3 Transition Activity Summary

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

The following table details the transition activities, activity owner(s), and milestone dates associated with the provision of government-wide services for common ICAM requirements:

Activity No.	Transition Activity	Activity Owner	Implementation Milestone Date
4.1	Complete upgrade to CVS to include additional functionality to support reciprocity.	OPM	TBD
4.2	Enable reciprocity by communicating additional guidance and procedures, as deemed necessary, to facilitate trust amongst agencies.	OPM	TBD
4.3	Establish a mechanism to enable referencing completed background investigations based upon fingerprints in order to tie an individual claiming an identity to a previously vetted identity.	FBI	6/30/2010
4.4	Determine the feasibility of a service for contractor PIV issuance that transcends agency boundaries; implement, if feasible.	GSA	3/30/2011
4.5	Establish government-wide procurement vehicles for provisioning/ workflow technologies.	GSA	9/30/2010
4.6	Complete upgrades to Federal PKI to support increased capacity expected as a result of PIV implementation maturity.	GSA	9/30/2010

Figure 52: Initiative 4 Transition Activity Summary

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**
  Includes activities required to eliminate redundancies in the collection and maintenance of identity data and mitigate the inefficiencies and security and privacy risks associated with current identity data management processes.
- **Initiative 6: Fully leverage PIV and PIV-interoperable credentials**
  Includes a wide variety of activities required to meet the intent of HSPD-12 for the usage of PIV credentials, as well as activities to leverage externally-issued credentials that are compliant with PIV-interoperable specifications and can be trusted by the Federal Government at E-authentication level 4.
- **Initiative 7: Modernize PACS infrastructure**
  Includes activities required to update physical security processes and systems for routine access for PIV cardholders and visitor access for individuals with other acceptable credentials.
- **Initiative 8: Modernize LACS infrastructure**
  Includes activities associated with upgrading logical access control systems to fully leverage the PIV card, make better use of cryptographic capabilities, and automate and streamline capabilities to increase efficiency and improve security.
- **Initiative 9: Implement federated identity capability**
  Includes the activities to support streamlined service delivery to external consumers and reduce redundancy in ICAM programs by leveraging a government-wide federated identity framework.

It is important to note that while implementation milestone dates have been provided for each agency-level initiative, these dates are provided as a guideline only. Agencies will be given the

opportunity to establish completion milestones in collaboration with OMB based on the maturity of their as-is state. Agency-specific milestones will be reported and tracked using the ICAM Transition Plan template being developed as part of government-wide activity 3.2. For those agency-level activities that reflect requirements outlined prior to the introduction of the ICAM segment architecture in an agency's HSPD-12 Implementation Plan with OMB, the agency is expected to comply with the previously established dates.

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

The following table details the transition activities, activity owner(s), and milestone dates associated with streamlining the collection and sharing of digital identity data. Note that collection and reuse of digital identity data is subject to all applicable privacy laws and regulations.

Activity No.	Transition Activity	Activity Owner	Implementation Milestone Date
5.1	Implement government-wide digital identity data standard such that data can be easily exchanged. Specify data standard for procurement/ development of new identity management systems	Federal Executive Branch Agencies	9/8/2010
5.2	Use BAE common data elements to support sharing of data elements for use in shared mission or business areas (e.g., ISE).	FIWG working with Communities of Interest	3/31/2010
5.3	Complete an inventory of authoritative data sources for each of the data elements defined as part of the government-wide digital identity specification.	Federal Executive Branch Agencies	6/10/2010
5.4	Establish an agency AAES to enable discovery and sharing of digital identity data between agency systems/resources. Develop interfaces with other repositories that are authoritative for individual data elements, as necessary.	Federal Executive Branch Agencies	1/01/2011
5.5	Enable processes and technologies for synchronization of updates to digital identity data to and from the authoritative sources across all applicable consumers of this information.	Federal Executive Branch Agencies	6/29/2011
5.6	Evaluate the need for a government-wide approach for creating and maintaining contractor and affiliate identity data, including feasibility/desire for government-wide contractor database.	ICAMSC	1/15/2010
5.7	Transition all transmission of biographic data and biometrics used to conduct background investigations to electronic processes.	Federal Executive Branch Agencies	12/31/2009
5.8	Minimize collection of biographic data and utilize AAES for sharing authoritative biographic data where necessary.	Federal Executive Branch Agencies	6/29/2011
5.9	Eliminate paper processes wherever possible and determine mechanisms to share with appropriate agency partners under specific scenarios.	FIWG, Federal Executive Branch Agencies	03/31/2010
5.10	Populate identity data required as part of the PIV sponsorship and enrollment processes through digital identity data captured in authoritative repositories.	Federal Executive Branch Agencies	9/8/2010
5.11	Incorporate First Responder requirements into PIV systems, including standardization of Responder designations and development of any required interface to the FEMA Emergency Response Official database.	Federal Executive Branch Agencies	10/8/2010

Activity No.	Transition Activity	Activity Owner	Implementation Milestone Date
5.12	Modify processes as necessary to ensure that fingerprints captured for conducting the background investigation are captured as part of PIV enrollment.	Federal Executive Branch Agencies	6/30/2010
5.13	Establish business rules for sharing identity/access record data as needed between agencies in order to provision access.	FIWG	9/30/2010
5.14	Enable the use of BAE across departments to allow for real time access decisions based on user attributes.	FIWG/AWG	3/31/2010

Figure 53: Initiative 5 Transition Activity Summary

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

The following table details the transition activities, activity owner(s), and milestone dates associated with fully leveraging existing PIV and PIV-interoperable credentials across agencies:

Activity No.	Transition Activity	Activity Owner	Implementation Milestone Date
6.1	Reduce or eliminate the creation and issuance of separate soft certificates to Federal Executive Branch Agency users. Standardize on PIV credentials.	Federal Executive Branch Agencies	12/31/2010
6.2	Develop guidance recommending the use of PIV for authentication at all levels by internal users and requiring agencies to issue internal policy on the use of PIV.	RDT	10/30/2009
6.3	Implement use of PIV credentials for internal user access and eliminate separate username/password tokens wherever possible.	Federal Executive Branch Agencies	9/30/2010
6.4	Employ standard lease agreements at federal facilities by requiring the use of FIPS 201 compliant or FIPS 201 interoperable credentials as the basis for attaining authorization for unescorted access into facilities employing physical access control systems across the Federal enterprise.	Federal Executive Branch Agencies	9/30/2010
6.5	Include language in procurements requiring that logical and physical authentication systems support PIV-compliant identity credentials.	GSA/ Agencies	12/31/2009
6.6	Begin enabling relevant applications to accept PIV cards from other Executive Branch Agencies and PIV-interoperable cards.	Federal Executive Branch Agencies	10/30/2009
6.7	Leverage the results from FIPS 199 assessments to inventory systems/applications and prioritize for PIV enablement.	Federal Executive Branch Agencies	1/30/2010
6.8	Implement applications to support the use of encryption, digital signature, and PKI authentication technology.	Federal Executive Branch Agencies	12/31/2009
6.9	Expand the use of digital signatures in lieu of manual, paper-based signing processes.	Federal Executive Branch Agencies	12/31/2009
6.10	Establish capability for recovery of data encrypted with expired/lost credentials (in accordance with guidance provided based on Activity 1.7).	Federal Executive Branch Agencies	12/31/2009
6.11	Complete implementation of path discovery and validation products.	Federal Executive Branch Agencies	12/31/2009
6.12	Establish the minimum certification process by which external organizations become trusted PIV-interoperable issuers.	AWG	12/31/2009

Figure 54: Initiative 6 Transition Activity Summary

5.2.2.3. Initiative 7: Modernize PACS infrastructure

The following table details the transition activities, activity owner(s), and milestone dates associated with the modernization of the PACS infrastructure. Please note that many agency facilities may require critical PACS upgrade activities not covered by the ICAM architecture, such as incorporation of Section 508 accessibility requirements. Implementation best practices for PACS modernization will be discussed in Part B of this document.

Activity No.	Transition Activity	Activity Owner	Implementation Milestone Date
7.1	Plan PACS process and technology upgrades to ensure electronic authentication of PIV cards and multi-factor authentication as defined in NIST SP 800-116; develop business case and incorporate into funding request/cycle via budget process.	Federal Executive Branch Agencies	9/14/2009, 9/2010
7.2	Adopt an agency-wide approach to managing physical access that links individual PACS via a federated network wherever possible.	Federal Executive Branch Agencies	6/30/2010
7.3	Upgrade current technology to ensure it supports PIV cards and more stringent authentication assurance.	Federal Executive Branch Agencies/ GSA	9/30/2011
7.4	Populate PACS user attributes and credential information from authoritative data sources.	Federal Executive Branch Agencies	9/30/2011
7.5	Document and develop interfaces to support PIV PKI certificate checks as it relates to physical access privileges, where applicable based on risk assessment.	Federal Executive Branch Agencies	9/30/2011
7.6	Leverage common Federal data standards such as UCore or NIEM to increase interoperability.	Federal Executive Branch Agencies	9/30/2011
7.7	Using the guidance provided in NIST SP 800-116, determine which authentication mechanisms are required at each facility access point.	Federal Executive Branch Agencies	9/30/2011
7.8	Upgrade technologies to support secure, automated processes for requesting and provisioning visitor access.	Federal Executive Branch Agencies	3/30/2012
7.9	Define and implement a process for supporting externally issued credentials.	Federal Executive Branch Agencies	9/30/2011
7.10	Provide for the functionality to provision other agency issued PIV and third party PIV-interoperable credentials into PACS, following the NIST 800-116 guidance.	Federal Executive Branch Agencies	9/20/2011

Figure 55: Initiative 7 Transition Activity Summary

5.2.2.4. Initiative 8: Modernize LACS infrastructure

The following table details the transition activities, activity owner(s), and milestone dates associated with the modernization of agency LACS infrastructures:

Activity No.	Transition Activity	Activity Owner	Implementation Milestone Date
8.1	Adopt an agency-wide approach to managing logical access that links individual applications to a common access management infrastructure wherever possible.	Federal Executive Branch Agencies	12/31/2009
8.2	Complete an upgrade of the logical access infrastructure within the agency to allow for centralized provisioning and workflow management for logical access.	Federal Executive Branch Agencies	12/31/2011

Activity No.	Transition Activity	Activity Owner	Implementation Milestone Date
8.3	Establish business rules by which the provisioning workflows are managed for both internal and external users.	Federal Executive Branch Agencies	12/31/2011
8.4	Upgrade current processes by investing in provisioning/workflow management technologies; develop business case and incorporate into next funding request/cycle via budget process.	Federal Executive Branch Agencies	10/1/2010
8.5	Tie all relevant applications/systems into the automated workflow where feasible; upgrade legacy systems as needed.	Federal Executive Branch Agencies	3/30/2012

Figure 56: Initiative 8 Transition Activity Summary

5.2.2.5. Initiative 9: Implement federated identity capability

The following table details the transition activities, activity owner(s), and milestone dates associated with the implementation of federated identity capabilities:

Activity No.	Transition Activity	Activity Owner	Implementation Milestone Date
9.1	Issue agency-specific policy addressing recognition of externally-issued credentials that follow the trust framework processes established by the Federal CIO Council.	Federal Executive Branch Agencies	3/30/2012
9.2	Implement guidance on consuming external credentials and identity records	Federal Executive Branch Agencies	3/30/2012
9.3	Begin reducing the creation and maintenance of password tokens by Federal Executive Branch Agencies for external users through acceptance of externally issued credentials.	Federal Executive Branch Agencies	10/30/2009
9.4	Enable public facing applications to accept third party credentials, as appropriate.	Federal Executive Branch Agencies	11/26/2011
9.5	Incorporate upgraded CVS functionality into business processes for checking adjudication of prior background investigations for an individual.	Federal Executive Branch Agencies	6/30/2010

Figure 57: Initiative 9 Transition Activity Summary

5.2.3. Implementation Sequencing Plan

The sequencing plan provides an aggregated cross-agency view of current and planned efforts required to achieve the target architecture. The ICAM sequencing plan has been developed as a Microsoft Project schedule template and will be provided to agencies as part of the ICAM Transition Plan template being developed as Activity 3.2 of this Roadmap.

It is expected that agencies will translate their required activities into a detailed work breakdown structure (WBS) within their own ICAM segment architecture. Agencies should take into consideration their existing ICAM implementation baselines and unique considerations that might dictate additional or different steps to achieve the government-wide objectives. Agency-specific sequencing plans should also provide additional information on the deliverables that are required for implementation; the specific IT investment(s), system(s), or program(s) supporting the activity; and any dependencies and constraints impacting implementation. Agencies will be required to provide specific completion dates in order to support performance measurement and accountability at the government-wide level. In the near-term, agencies should use this section to

forecast and request funding for out-year costs associated with the initiative activities, beginning with the FY2011 budget cycle.

5.3. Performance Metrics

The performance metrics in this section cover a wide range of systems, technologies, processes, activities and outcomes within the ICAM segment. Gathering metrics across the layers of the segment creates a line of sight from IT investment performance up to the ICAM strategic goals and objectives.

The performance metrics provided below standardize a number of metrics that are currently being tracked at one or multiple agencies for individual ICAM programs. They also include new metrics that are being introduced to address new aspects within the target ICAM segment architecture. It is intended that agencies will streamline the tracking and reporting of their ICAM programs against this common set of metrics. This list does not preclude the measurement of additional metrics deemed important by an individual agency; however, the introduction of a common set of metrics is intended to allow ICAM governance entities to compare programs consistently in order to gain a more comprehensive and consistent view of progress against ICAM objectives across the Federal Government.

The performance metrics in this section include an end state target that aligns with achievement of the target state ICAM segment architecture. Agencies are expected to set their own interim performance targets for each fiscal year based on the maturity of their current ICAM programs in collaboration with OMB and measure and report their performance for each metric in one of three reporting locations:

1. Exhibit 300: In cases where an agency has existing or planned investments specific to ICAM as a result of capital planning processes, the agency should include the performance metrics outlined in this section within its Exhibit 300(s). The inclusion of ICAM metrics within the agency's Exhibit 300 submissions should be referenced in the ICAM Transition Plan.
2. Agency ICAM Transition Plan: The Transition Plan template (reference Activity 3.2) will include a segment for annual reporting against these metrics along with agency-specific targets year-over-year. In cases where an agency does not have any capital investments related to ICAM, it should use the Transition Plan to report progress against the performance metrics.
3. Data.gov: Four metrics have been identified for public reporting on Data.gov via agency websites (identified in the below table with asterisks). Due to the high priority of ICAM and its relevance to national initiatives such as cybersecurity, the reporting of high value metrics is relevant and appropriate for achieving transparency in government.

The measurement areas and measurement groupings are drawn from the FEA Performance Reference Model (PRM) and support the performance line of sight.

The performance metrics are provided in the following table.

Item No.	Strategic Goal Supported	Objectives Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	End State Target
1	Goal 5: Reduce Costs and Increase Efficiency Associated with ICAM	3.2, 3.3, 5.1, 5.2	Customer Results	Service Accessibility	Access	Average time to provision initial PACS and LACS access to an internal user (specifically, the time between the point when the approval for an access privilege has been granted to the point that the privilege is granted to an individual for physical and logical access).	Less than 2 hours from the point when the need for an access privilege has been identified to the point that the privilege is granted to an individual.
2	Goal 3: Improve Security Posture across the Federal Enterprise	3.2, 3.3, 5.1, 5.2	Mission and Business Results	Administrative Management	Security Management	Average time to deprovision internal user from PACS and LACS upon separation from the agency (specifically, the time between the last hour worked by the employee to the point that the access privilege has been revoked).	Less than 2 hours from the point when the need for revocation of an access privilege has been identified to the point that the privilege is removed from the system.
3*	Goal 3: Improve Security Posture across the Federal Enterprise	3.1, 3.2, 3.3, 5.1, 5.2, 5.3	Processes and Activities	Security and Privacy	Security	Number of physical access transactions that electronically authenticate internal and external user's PIV card for routine access divided by the number of physical access transactions supported for internal and external Agency users (expressed as a percentage).	100%
4	Goal 5: Reduce Costs and Increase Efficiency Associated with ICAM	5.1	Customer Results	Timeliness and Responsiveness	Delivery Time	Number of business days from applicant registration to PIV card issuance (not including time associated with background investigation).	7 days
5	Goal 5: Reduce Costs and Increase Efficiency Associated with ICAM	5.1	Processes and Activities	Productivity	Productivity	Average PIV Enrollment Time (includes applicant provision of demographic data, fingerprints, photo, and all other data required to complete enrollment per FIPS 201).	10 minutes
6	Goal 5: Reduce Costs and Increase Efficiency Associated with ICAM	5.1	Processes and Activities	Productivity	Productivity	Average PIV Activation Time (not including local printing).	10 minutes
7	Goal 5: Reduce Costs and Increase Efficiency Associated with ICAM	3.2, 3.3, 5.1, 5.2, 5.3	Processes and Activities	Productivity	Efficiency	Percentage of PIV cardholder records from which data is automatically populated into PACS during provisioning upon issuance.	100%

Item No.	Strategic Goal Supported	Objectives Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	End State Target
8	Goal 5: Reduce Costs and Increase Efficiency Associated with ICAM	3.3, 5.1, 5.2, 5.3	Processes and Activities	Productivity	Efficiency	Percentage of PIV cardholder records from which data is automatically populated into LACS during provisioning upon issuance.	100%
9	Goal 3: Improve Security Posture across the Federal Enterprise	3.3	Technology	Efficiency	System Response Time	PKI Certificate Response Time (PKI CRT) for Revocation and Suspension (measured from the CA's perspective).	2 hours to respond, 18 hours to publish
10*	Goal 2: Facilitate E-Government by Streamlining Access to Services	2.1, 3.2, 3.3, 5.1, 5.2, 5.3	Customer Results	Service Accessibility	Automation	Percentage of government applications accessible to federal employees and contractors using PIV credentials for authentication.	100%
11	Goal 5: Reduce Costs and Increase Efficiency Associated with ICAM	3.3, 5.1, 5.2, 5.3	Processes and Activities	Productivity	Efficiency	Percentage of agency applications integrated into the automated provisioning workflow.	100%
12	Goal 5: Reduce Costs and Increase Efficiency Associated with ICAM	5.1	Processes and Activities	Productivity	Efficiency	Number of manual processes divided by the total number of ICAM-related processes.	0
13	Goal 5: Reduce Costs and Increase Efficiency Associated with ICAM	3.3, 5.1, 5.2	Processes and Activities	Productivity	Efficiency	Percentage of PIV-holders for whom fingerprint templates were collected once and used both for background investigations and the PIV enrollment process in order to maintain the chain of identity.	100%
14	Goal 1: Comply with Federal Laws, Regulations, Standards, and Governance Relevant to ICAM	3.3	Processes and Activities	Security and Privacy	Security	Percentage of employees and contractors with PIV-compliant background checks.	100%
15*	Goal 1: Comply with Federal Laws, Regulations, Standards, and Governance Relevant to ICAM	3.2, 3.3, 5.1, 5.2	Processes and Activities	Management and Innovation	Risk	Percentage of employees/contractors/affiliates who have been issued PIV cards.	100%

Item No.	Strategic Goal Supported	Objectives Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	End State Target
16	Goal 1: Comply with Federal Laws, Regulations, Standards, and Governance Relevant to ICAM	1.1, 3.3, 4.4	Processes and Activities	Security and Privacy	Security	Percentage of relevant systems for which accreditation of PIV Credential Issuer and systems in accordance with SP 800-37, 800-53 and 800-79 standards has been successfully achieved.	100%
17	Goal 5: Reduce Costs and Increase Efficiency Associated with ICAM	5.1	Technology	Efficiency	Technology Improvement	Number of PIV sponsorship records that are electronically populated from existing authoritative identity data sources divided by the total number of sponsorship records populated (expressed as a percentage).	100%
18	Goal 5: Reduce Costs and Increase Efficiency Associated with ICAM	3.3	Processes and Activities	Productivity	Efficiency	Number of internal agency applications integrated with provisioning tool divided by the total number of applications planned for provisioning integration.	100%
19	Goal 4: Enable Trust and Interoperability	2.1, 4.1, 4.2, 4.3	Technology	Efficiency	Interoperability	Number of external agency applications enabled to accept third party credentials for authentication and authorization divided by the number of applications that require authentication / authorization for external users.	100%
20	Goal 1: Comply with Federal Laws, Regulations, Standards, and Governance Relevant to ICAM	1.1, 3.3, 4.4	Processes and Activities	Management and Innovation	Risk	Percentage of agency applications whose access control policies and processes are consistent with M-04-04 requirements.	100%
21	Goal 1: Comply with Federal Laws, Regulations, Standards, and Governance Relevant to ICAM	1.1, 3.2, 3.3, 4.4	Processes and Activities	Security and Privacy	Security	Percentage of physical access control systems implemented in accordance with 800-116.	100%
22	Goal 1: Comply with Federal Laws, Regulations, Standards, and Governance Relevant to ICAM	1.2, 3.1, 4.2, 4.3, 4.4	Processes and Activities	Cycle Time and Timeliness	Timeliness	Percentage of milestones met in accordance with transition plan	100%

Item No.	Strategic Goal Supported	Objectives Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	End State Target
23	Goal 5: Reduce Costs and Increase Efficiency Associated with ICAM	5.1	Mission and Business Results	Administrative Management	Help Desk Services	Number of help desk calls requiring PIN/password resets divided by the total number of enterprise users.	Significant decrease over time as provisioning is extended to applications. Goal is <5%.
24	Goal 3: Improve Security Posture across the Federal Enterprise	2.2	Processes and Activities	Security and Privacy	Privacy	Percentage of end users who believe that their privacy is adequately protected as a direct result of the Agency's ICAM-related processes.	>95%
25	Goal 3: Improve Security Posture across the Federal Enterprise	3.3	Processes and Activities	Management and Innovation	Risk	Number of orphaned accounts remaining in Agency applications as a result of inadequate / manual de-provisioning processes.	0
26	Goal 3: Improve Security Posture across the Federal Enterprise	5.1, 5.2, 5.3	Processes and Activities	Security and Privacy	Privacy	Number of digital identities maintained per federal user.	1
27*	Goal 4: Enable Trust and Interoperability	2.1, 3.3, 4.2, 4.3	Technology	Effectiveness	IT Contribution to Process, Customer, or Mission	Number of electronic transactions conducted with external businesses and citizens using third party credentials divided by the total number of e-Gov transactions conducted with external businesses and citizens (expressed as a percentage).	100%
28	Goal 5: Reduce Costs and Increase Efficiency Associated with ICAM	5.1, 5.2, 5.3	Processes and Activities	Financial	Savings and Cost Avoidance	Help desk costs avoided as a result of consolidating ICAM infrastructure.	Varies
29	Goal 5: Reduce Costs and Increase Efficiency Associated with ICAM	5.1, 5.2, 5.3	Processes and Activities	Financial	Savings and Cost Avoidance	Operations & maintenance costs avoided as a result of consolidating application services through automation of provisioning and identity lifecycle management.	Varies
30	Goal 5: Reduce Costs and Increase Efficiency Associated with ICAM	4.4, 5.1, 5.2, 5.3	Mission and Business Results	General Government	Central records and statistics management	Number of identity attributes that have a single recognized authoritative source divided by the total number of attributes used to comprise a digital identity (expressed as a percentage).	100%

Item No.	Strategic Goal Supported	Objectives Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	End State Target
31	Goal 1: Comply with Federal Laws, Regulations, Standards, and Governance Relevant to ICAM	1.2, 3.1, 4.2	Processes and Activities	Cycle Time and Timeliness	Timeliness	Percentage of Transition Plans submitted on time.	100%
32	Goal 5: Reduce Costs and Increase Efficiency Associated with ICAM	5.1	Processes and Activities	Productivity	Productivity	Average time taken for resetting the PIN for Agency PIV cards.	<20 minutes

Figure 58: ICAM Performance Metrics (* indicates inclusion in the Data.gov data stream)

This page is intentionally left blank.

PART B: Implementation Guidance

This part of the document provides guidance to agencies for planning and implementing ICAM programs and the 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.

This page is intentionally left blank.

6. ICAM Implementation Planning

This chapter serves as a primer on implementation planning related to ICAM programs. It is expected that agencies have general life cycle methodologies they employ to plan and execute programs within their agency. The purpose of this chapter is to pick up where an agency's general life cycle methodologies leave off, identifying specific planning considerations common across Identity, Credential, and Access Management programs. This section is intended to help agencies to align their programs and realize synergies and increased benefits across the three disciplines.

Due to its close ties with the remaining Implementation Guidance (Chapters 7-12), the majority of this chapter will be drafted as part of Phase 2 of the effort and will be included in version 2.0 of this document; however, three outputs from Phase 1 of the effort are included in this version: the ICAM Stakeholders List, the ICAM Risk Registry, and information regarding the link between Enterprise Architecture and the budget cycle.

6.1. Program Stakeholders

6.1.1. Collaboration and Stakeholder Management

A stakeholder is an individual or organization that is either actively involved in the project or who might be affected by the project's execution or completion. It is critical to identify all stakeholders, and not just those who may be positively affected by the project. The stakeholders affected may include employees, unions, application owners, industry partners, system integrators, user populations, solution providers, and other affiliates and partners. Traditionally, ICAM programs have been managed in stovepipes, which have led to challenges in involving all relevant stakeholders. This section presents some high-level considerations for involving stakeholders and promoting collaboration to assist agencies in overcoming the challenges typically associated with ICAM programs.

Stakeholder management, as it relates to ICAM, is the management of numerous stakeholders within ICAM that are not necessarily bound by a single program. ICAM programs are large, complex initiatives that often span across multiple endeavors across several departmental organizations; as such it is critical to define the program objectives, boundaries, and stakeholders early in the planning process. This could include identifying and simultaneously managing the stakeholders of an HSPD-12 credentialing system, a new Physical Access Control System, a Logical Access Control System, and several other programs related to ICAM. These stakeholders will likely have very different viewpoints and often these may conflict with one another or the program objectives. Furthermore, decisions made in one program may impact another program so it may be critical in gaining buy-in so that a specific program or technology is supported by leadership and adopted by users. Discussions of the impacts of these programs may also highlight the opportunity to leverage existing programs and investments, thus improving efficiency. Implementing ICAM programs may also have legal implications, particularly within the privacy community, which provides additional reasons for collaboration. Therefore, stakeholder management and collaboration is essential to incorporate a holistic approach for ICAM implementation.

Collaboration is both a process and an outcome in which shared interest or conflict that cannot be addressed by any single individual is addressed by key stakeholders. This process is unique with ICAM not only because of the large number of stakeholders, but the way that these stakeholders overlap into other programs. ICAM crosses many interagency boundaries and obstacles that other programs do not, as such, nearly the entire population will have some interest in the ICAM implementation. As an example, from a user perspective, ICAM impacts the way everyone in the agency is to be identified and gain access to the resources that they may need to do their job. Each stakeholder group will also have a unique viewpoint and unique interest in the ICAM implementation. The collaborative process involves a synthesis of these different perspectives to better understand complex problems.

The result of collaboration is the development of integrative solutions that go beyond an individual vision to a productive resolution that could not be accomplished by any single person or organization. For example, when stakeholders collaborate to identify overlaps between programs, redundant processes across various ICAM programs may be eliminated. The segment architecture provides an example with the creation of a digital identity. The creation of a digital identity with various data elements that span across multiple systems will require the collaboration of many different stakeholders within traditionally stove-piped programs. In the target state, digital identity data is intended to be leveraged to reduce redundant data collection processes that may occur within different programs. Another example of an overlap is between the stakeholders of a credentialing program and the stakeholders of physical/logical access management programs. Collaboration between these two stakeholder groups is critical to the overall success of ICAM because of the dependencies that they have with one another.

Communication and outreach to the stakeholders that are affected by ICAM is another essential part of successful ICAM implementation. Effective communication is key to the success of any program and is especially relevant in programs as far reaching as ICAM implementations. In order to communicate consistently and effectively a Communication Plan should be developed early in the program life cycle. ICAM implementation requires the efforts and cooperation of diverse stakeholders to form a cohesive to guide and maintain the various identity, credential, and access management programs. It is up to the agency to plan and decide which stakeholder would best manage each of the different programs associated with ICAM, as different stakeholders may have different strengths that can be leveraged more effectively in a particular program.

6.1.2. ICAM Stakeholders

The following table provides an overview of the stakeholders related to the ICAM segment. The table lists many of the federal stakeholders for ICAM, but is not intended to be a detailed list of non-federal stakeholders. The role descriptions provided for each stakeholder identify their overarching role or mission and their relevance to the ICAM segment.

Stakeholder Group	Stakeholder Name	Role
Federal Governance Bodies	Office of Management and Budget (OMB)	• Assists the President in overseeing the preparation of the federal budget and supervises its administration in Executive Branch agencies. Provides policy, direction, and oversight for the implementation of ICAM initiatives. The lead agency with respect to E-Government implementation.

Stakeholder Group	Stakeholder Name	Role
	Office of the National Coordinator for Health IT (ONCHIT)	• Provides counsel to the Secretary of Health and Human Services and departmental leadership for the development and nationwide implementation of an interoperable health information technology infrastructure. • Use of this infrastructure will improve the quality, safety and efficiency of health care and the ability of consumers to manage their health information and health care.
	Federal Enterprise Architecture Interagency Group	• Community of federal enterprise architects that support the development of the Federal Enterprise Architecture practices, models and other assets.
	The Federal CIO Council	• Serves as the principle interagency forum for improving practices in the design, modernization, use, sharing, and performance of Federal Government agency information resources. Chartered the work of the FICC, E-authentication initiative, and the Federal PKI Policy Authority, which have been consolidated into the newly chartered ISIMC and ICAMSC. Also includes the Privacy Committee.
	Information Security and Identity Management Committee (ISIMC)	• Serves as the principal interagency forum for identifying high priority security and identity management initiatives and developing recommendations for policies, procedures, and standards to address those initiatives that enhance the security posture and protection afforded to Federal Government networks, information, and information systems.
	Identity Credential and Access Management Subcommittee (ICAMSC)	• Subcommittee of the ISIMC focused on initiatives related to Identity, Credential, and Access Management.
	Privacy Committee	• The Privacy Committee is the principal interagency forum to improve agency practices for the protection of privacy. The Privacy Committee serves as the interagency coordination group for Senior Agency Officials for Privacy and Chief Privacy Officers in the Federal Government that provides a consensus-based forum for the development of privacy policy and protections throughout the Federal Government by promoting adherence to the letter and spirit of laws and best practices advancing privacy.
	General Services Administration (GSA) NOTE: GSA is also an Internal Service Provider	• Managing partner for ICAM initiatives. • Provides government building space, acquisition solutions for government organizations and the military, and management best practices and efficient government operations. • Establishes and maintains acquisition vehicles and approved products for HSPD-12 deployment. • Provides the USAccess HSPD-12 Managed Service Offering.

Stakeholder Group	Stakeholder Name	Role
	Office of Personnel Management (OPM) NOTE: OPM is also an Internal Service Provider	• Supports the Federal Government's workforce by shaping HR management systems to effectively recruit, develop, manage and retain a high quality and diverse workforce and through technical assistance, employment information, pay administration, and benefits delivery for personnel. • Develops and implements policies and procedures for investigations and adjudications, and conducts personnel background investigations as part of the screening process. • Owns the automated systems to support investigative processing. • Serves as the suitability executive agent for the Federal Government.[46]
	Joint Security and Suitability Reform Team	• Interagency body supported by OPM to examine the processes and technologies that support security clearance, investigation, and suitability determination activities and provide recommendations for improvement to meet the goals of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). • Published the Security and Suitability Process Reform, Initial Report dated April 30, 2008[47] and the Federal Investigative Standards.[48]
	The Federal PKI Policy Authority	• Interagency body set up under the CIO Council to enforce digital certificate standards for trusted identity authentication across the federal agencies and between federal agencies and outside bodies, such as universities, state and local governments and commercial entities.
	Interagency Security Committee (ISC)	• Committee established by Executive Order 12977,which is responsible for developing standards, policies and best practices for enhancing the quality and effectiveness of physical security in, and the protection of, nonmilitary federal facilities in the United States. The ISC provides a permanent body to address continuing government-wide security for federal facilities.
	National Science and Technology Council	• This Cabinet-level Council is the principal means within the executive branch to coordinate science and technology policy across the diverse entities that make up the Federal research and development enterprise. • The NSTC Subcommittee on Biometrics and Identity Management provides leadership and federal coordination for ICAM issues.
	Background Investigation Stakeholder Group (BISG)	• Comprised of senior security officers and managers and provides recommendations on standardization and develops long-term strategies regarding the enhancement of investigative processes for the Federal Government.

[46] In accordance with responsibilities and duties outlined in Executive Order 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, June 30, 2008.

[47] Security and Suitability Process Reform Initial Report, Joint Security and Suitability Reform Team, April 30, 2008.

[48] Federal Investigative Standards, Joint Security and Suitability Reform Team, December 2008.

Stakeholder Group	Stakeholder Name	Role
	Federal Cloud Computing Advisory Council	• Provides oversight to the Cloud Computing Initiative and PMO (formerly ITI LOB PMO). • Goal is to achieve an optimized, cost-effective, government-wide information technology infrastructure that supports agency mission, while providing reliability and security in service delivery.
	Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC)	• The government's primary policy coordination body for secured global information and communications infrastructure. • Its focus is to achieve an assured, reliable, secure, and survivable global information and communications infrastructure and related capabilities, and is the policy forum for cybersecurity matters.
	Information Sharing and Access Policy Interagency Policy Committee (formerly the Information Sharing Council)	• Council first established under Executive Order 13356 to review matters related to the improvement of sharing terrorism information. • The IPC holds responsibilities to advise the President and the Program Manager on the development of Information Sharing Environment (ISE) policies, procedures, guidelines, and standards, and to ensure proper coordination among federal agencies participating in the ISE.
Internal standards body	National Institute of Standards and Technology (NIST)	• Non-regulatory federal agency within the U.S. Department of Commerce that promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology. • The NIST Computer Security Division has developed extensive standards that impact implementation of ICAM programs and their underlying IT systems under the statutory responsibilities of FISMA • NIST is an ANSI accredited standards development organization to develop biometric format standards.
External industry guidance and standards bodies	Smart Card Alliance (SCA)	• Not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. • SCA has authored numerous white papers that provide best practices in the area of credential management.
	TechAmerica	• High-tech industry association active in Federal Information Security policy issues.
	Security Industry Association (SIA)	• Non-profit international trade association representing electronic and physical security product manufacturers, distributors, integrators, and service providers. American National Standards Institute (ANSI)-approved Standards Development Organization involved in developing systems integration and equipment performance standards.
	Kantara Initiative/Liberty Alliance	• Global body working to enable a networked world based on open standards where consumers, citizens, businesses and governments can more easily conduct online transactions while protecting the privacy and security of identity information.
	Transglobal Secure Collaboration Program (TSCP)	• Government-industry partnership specifically focused on facilitating solutions for Aerospace and Defense (A&D) issues. Currently working on identity federation issues in international defense and aerospace programs.

Stakeholder Group	Stakeholder Name	Role
	Organization for the Advancement of Structured Information Standards (OASIS)	• Not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society. • OASIS develops security standards (e.g., Security Assertions Markup Language (SAML) and WS*) needed in e-business and Web services applications.
	OpenID Foundation (OIDF)	• Organization formed to help promote, protect and enable the OpenID technologies and community. • The OIDF manages intellectual property, brand marks as well as fostering vital growth and global participation in the proliferation of OpenID.
	Information Card Foundation (ICF)	• The ICF is a non-profit foundation whose mission is to advance simpler, more secure and more open digital identity on the Internet, increasing user control over personal information while enabling mutually beneficial digital relationships between people and businesses.
	Institute of Electrical and Electronics Engineers (IEEE)	• Non-profit organization for the advancement of technology and enterprise-wide strategic planning process,
Internal ICAM Service Providers	Federal Bureau of Investigation (FBI)	• Protects and defends the United States against terrorist and foreign intelligence threats, upholds and enforces the criminal laws of the United States, and provides leadership and criminal justice services to federal, state, municipal, and international agencies and partners. • Conducts national fingerprint and criminal history checks.
	Department of the Treasury	• A provider of PKI services and digital certificates for trusted identity authentication across the Federal Government and with external bodies.
External ICAM Service Providers	Industry Identity Access Management (IAM) providers	• The issuers of electronic credentials to user communities. Similarly, providers of authentication technologies are stakeholders in assisting the government to the most appropriate services based on the needs of our customers and the state of the industry. • The Identity Providers (IDPs) and being a Trust Provider.
	Cooperative groups and initiatives	• Partnerships formed to share information, the ability to authenticate across boundaries, or other ICAM function such as the Four Bridges Forum and GFIPM.
	Industry PKI Service Providers	• Providers of PKI services and digital certificates for trusted identity authentication across the Federal Government and with external bodies.
Internal Service Consumers	Cross-agency shared service system owners	• Accept and trust electronic assertions of identity in respective electronic or web-based systems.
	Federal Agency Application Owners	• Will accept and trust electronic assertions of identity in respective electronic or web-based systems. Also referred to as Relying Parties.
	Federal Employees	• Core recipient of PIV credentials and holders of legacy E-Authentication credentials. • Require access and user privileges for both physical and logical access. • A subset of federal employees also serves as implementers of FICAM initiatives.

Stakeholder Group	Stakeholder Name	Role
External Service Consumers	American Public and Businesses	• The individuals and businesses that require access to government systems and resources. • Government-wide approach to ICAM must address the varying needs of these communities, focusing particularly on the characteristics of the two user segments: Government-to-Citizen and Government-to-Business. The Federal Government provides ICAM services to universities and contractors as business partners.
	Privacy Community	• People and organizations that support privacy practices and regulation. Members can be users of government services and advocate for the secure handling of that data.
	State, Local, Foreign and Tribal Governments	• Transact business on behalf of their government or its constituency. • Partner with the Federal Government in identity management initiatives (e.g., State and Local partnership with the Department of Homeland Security to develop the First Responder Access Card identity credential).

Figure 59: ICAM Stakeholders

The development of a new Federal ICAM architecture will invariably affect partners outside the Federal Government. To the extent possible, the standards and practices already implemented in those forums, many mentioned above, were incorporated. In addition, several working groups that support the ICAMSC have performed outreach to gather inputs for this architecture. Where possible, the Roadmap Development Team will work with stakeholders to address implementation concerns and consider architectural modifications.

6.2. Risk Management

The Risk Registry that was developed as part of the ICAM segment architecture can be found in Appendix D Risk Registry.

6.3. Capital Planning

Capital Planning and Investment Control (CPIC) is a structured, integrated approach to selecting and managing investments. It supports alignment of investments to the agency's mission and supports business needs while reducing risks and increasing returns throughout the investment's life cycle. The CPIC process as a whole integrates strategic planning, enterprise architecture, privacy, security, budgeting, portfolio management, procurement, and acquisition management of capital assets. The primary product of the CPIC process is the OMB Circular A-11 defined Exhibit 300 (E-300). E-300's are constructed and reviewed on an annual basis.

Federal agencies should include ICAM in their CPIC portfolios. Typically, agencies have separate Exhibit 300s for various ICAM programs. However, agencies may choose to consolidate traditionally stove-piped programs into an agency-wide Exhibit 300 addressing ICAM, in which component/bureau investments link to the agency-wide exhibit. This would ensure collaboration and may help incorporate a holistic approach to ICAM. Furthermore, collaboration between all relevant stakeholders during each phase of the CPIC process is critical to ensure that the overlapping elements of different ICAM programs are addressed, particularly during the Select and Control phases. More information on CPIC processes should be available through agencies' Office of Chief Information Officer (OCIO).

The sub-sections below provide specific ICAM guidance and lessons learned with respect to the Capital Planning process.

6.3.1. Acquisition Resources

To be provided in version 2.0 of this document.

6.3.2. Accreditation

Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls.[49] Accreditation provides accountability for adverse impacts that might occur as a result of a security breach, thus challenging responsible parties to implement the most effective security controls allowable within resource constraints. In order to perform accreditation, agencies must periodically perform detailed reviews of the management, operational, and technical security controls[50] in an information system, a process typically called certification. As a result of certification, an agency may need to reassess or modify a system's security controls in order to maintain an acceptable level of risk prior to accreditation.

Accreditation is an important aspect of any ICAM initiative not only because of the security and regulatory requirements, but also because of the scheduling and cost impacts resulting from the process. As such, additional time may need to be built into an implementation schedule early in the planning process to avoid costly delays. The amount of time necessary to successfully accredit an information system is based uniquely on each application's Confidentiality, Integrity, and Availability ratings (Low, Moderate, or High).[51] Failure to properly account for the duration of the accreditation process during the implementation planning phase may result in significant delays during an ICAM implementation.

6.3.2.1. Accreditation of PIV Systems

Due to the privacy, data security, and trust concerns around the credentials and information processed by PIV systems, these applications are subject to unique accreditation requirements in addition to the requirements placed on all IT systems. These PIV specific requirements are outlined in NIST Special Publication 800-79-1.[52] The purpose behind adopting additional accreditation requirements for PIV Card Issuers (PCI) is to establish and maintain a level of trust in the credentials that are issued. This guidance is particularly relevant when planning PIV rollout as part of an ICAM implementation since additional time will need to be built into the implementation schedule beyond what is normally required for accreditation purposes on other programs. Credentialing systems not accredited at the NIST High baseline should not be used to issue credentials to access a NIST High baseline system.

---

[49] Per NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004.

[50] As defined in NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, June 2009

[51] Explanations behind these ratings and general guidance for classifying an information system are provided in FIPS 199.

[52] NIST SP 800-79-1, Guidelines for the Accreditation of Personal Identity Verification Card Issuers, June 2008.

6.3.2.2. Accreditation of PACS

Historically, agencies have viewed PACS as independent from their IT enterprise based on the localized nature of many legacy implementations. Advancements in PACS technologies and the increasing adoption of enterprise models for PACS architecture with significant touch points to agency networks have underscored the fact that PACS are an integration of security and information systems. As such, they are subject to the accreditation process and conformance with the security controls applicable to all other information systems.

6.3.3. Enterprise Architecture

In general, enterprise architecture (EA) is a strategic management tool that helps organizations view the relationships among missions, information, technology, and transitional processes through depictions of current environments (termed "As-is") and future environments (termed "Target"). The Federal Government has adopted a federated architecture approach. The Federal Enterprise Architecture (FEA) describes the top level of the federation and provides broad guidance for explaining a common approach for EA development applicable across the Federal Government. Department-specific architectures must map back to the FEA to demonstrate alignment and allow for investment management across the entire Federal Government enterprise.

Successful enterprise architecture enables an agency to maximize the contribution of its resources, IT investments, and system development activities to achieve its performance goals. Architecture describes clear relationships from strategic goals and objectives through investments to measurable performance improvements for the entire enterprise or a portion (segment) of the enterprise. As such, enterprise architecture and supporting segment architectures should be thoroughly reviewed when determining which investments to submit for funding through the annual budget cycle.

Chapters 3, 4, and 5 present a common, government-wide segment architecture specific to ICAM. The development of the segment architecture was accelerated in order to allow agencies to incorporate the target state vision for federal ICAM, including the detailed initiative and milestone activities, into their FY11 budget submission. Use of the segment architecture in requesting investment funding will help ensure that IT investments are aligned with the common vision for ICAM and that agencies can begin taking steps to eliminate redundancies and realize synergies between individual ICAM investments.

6.4. Security Considerations

To be provided in version 2.0 of this document.

6.5. Privacy Considerations

To be provided in version 2.0 of this document.

This page is intentionally left blank.

Appendix A Acronym List

Acronym	Description
AAES	Authoritative Attribute Exchange Service
ADS	Authoritative Data Source
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AWG	Architecture Working Group
BAE	Backend Attribute Exchange
CA	Certification Authority
CHUID	Cardholder Unique Identifier
CIO	Chief Information Officer
COFG	Citizen Outreach Focus Group
COMMON	Federal PKI Common Policy Framework
CPIC	Capital Planning and Investment Control
CRL	Certificate Revocation List
CSP	Credential Service Provider
CUI	Controlled Unclassified Information
CVS	Clearance Verification System
DA	Data Administrator
DBMS	Database Management System
DHS	Department of Homeland Security
DOB	Date of Birth
DoD	Department of Defense
EA	Enterprise Architecture
ECDSA	Elliptic Curve Digital Signature Algorithm
e-QIP	Electronic Questionnaires for Investigations Processing
ESIGN	Electronic Signatures In Global and National
FAC	Facilities Access Card
FASC-N	Federal Agency Smart Credential Number
FBCA	Federal Bridge Certification Authority
FBI	Federal Bureau of Investigation
FBI CJIS	Federal Bureau of Investigation Criminal Justice Information System
FCIOC	Federal Chief Information Officer Council
FCPCA	Federal Common Policy Certification Authority
FEA	Federal Enterprise Architecture
FEMA	Federal Emergency Management Agency
F/ERO	Federal/Emergency Response Official
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FIWG	Federation Interoperability Working Group
FRAC	First Responder Access Card
FSAM	Federal Segment Architecture Methodology
FSO	Facilities Security Officer
G2B	Government-to-Business
G2C	Government-to-Citizen
G2G	Government-to-Government
GPEA	Government Paperwork Elimination Act
GSA	General Services Administration
GSA MSO	General Services Administration Managed Service Office
GUI	Global Unique Identifier
HSPD-12	Homeland Security Presidential Directive 12

Acronym	Description
HR	Human Resources
IAFIS	Integrated Automated Fingerprint Identification System
IAM	Identity Access Management
ICAM	Identity, Credential & Access Management
ICAMSC	Identity, Credential and Access Management Subcommittee
ID	Identification
IDMS	Identity Management System
IDP	Identity Provider
IEE	Internal Effectiveness & Efficiency
IRS	Internal Revenue Service
ISC	Interagency Security Committee
ISE	Information Sharing Environment
ISIMC	Information Security and Identity Management Committee
ITAA	Information Technology Association of America
JPAS	Joint Personnel Adjudication System
KRA	Key Recovery Agent
LACS	Logical Access Control Systems
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Agent
NCES	Net-Centric Enterprise Services
NCIC	National Crime Information Center
NIEM	National Information Exchange Model
NIST SP	National Institute of Standards and Technology Special Publication
NPE	Non-Person Entity
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
OIDF	OpenID Foundation
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PACS	Physical Access Control Systems
PIN	Personal Identification Number
PIPS	Personnel Investigations Processing System
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RA	Registration Authority
RDT	Roadmap Development Team
SAML	Security Assertions Markup Language
SCA	Smart Card Alliance
SHA	Secure Hash Algorithm
SIA	Security Industry Association
SIP	Shared Infrastructure Provider
SF	Standard Form
SOAP	Simple Object Access Protocol
SRM	Service Component Reference Model
SSA	Social Security Administration
SSP	Shared Service Provider
Triple DES	Triple Data Encryption Algorithm
TSCP	Transglobal Secure Collaboration Program
XML	eXtensible Markup Language

Appendix B Glossary

Term	Definition
Adjudicator	Provides adjudication of background check information to determine eligibility of the applicant to receive a credential, access rights, or be able to work for the Government as an employee or contractor.
Adjudication	Evaluation of pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether a covered individual is: • suitable for Government employment; • eligible for logical and physical access; • eligible for access to classified information; • eligible to hold a sensitive position; or • fit to perform work for or on behalf of the Government as a contractor employee.
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.
Application Administrator	The party responsible for the maintenance and implementation of access control rights. Application Administrators should not be the approvers due to separation of duties.
Attribute Authorities	An entity recognized as having the authority to verify the association of attributes to an identity.
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.
Authenticator	A memory, possession, or quality held by a person that can serve as proof of identity when presented to a verifier.
Authoritative Attribute Exchange Service (AAES)	Service that performs discovery and mapping of attributes from authoritative source repositories.
Authoritative Data Source	The repository or system that contains the data and attributes about an individual that are 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.
Authorizer	Approves or denies access to applications or facilities based on business rules.
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.
Cardholder/Credential Holder	An individual possessing an issued token, PKI certificate, PIV Card or other authentication device.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.
Certificate Revocation List (CRL)	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.
Certificate Status Servers	The counterpart to the Certification Authority that passes revocation and expiration status to relying parties in real time.
Clearance Verification System (CVS)	A Federal repository for authorized personnel to determine whether an appropriate background investigation has been performed.
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.

Term	Definition
Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.
Credentialing Determination	Determination of whether or an individual is eligible to receive a PIV credential as either a federal employee or contractor.
Data Administrator (DA)	Party responsible for maintaining an organization's data and establishing relationship between authoritative data repositories. May also be an application administrator responsible for managing local data.
Domain Controller	The server(s) that manages passwords and authentication requests for a set of applications.
Digital Identity	The representation of Identity in a digital environment.[53]
E-Authentication Assurance Level (EAAL)	Evaluation categories by which authentication mechanisms are measured based on SP800-63. The lowest level assurance is 1; the highest assurance level is 4.
Enhanced Electronic Questionnaires for Investigations Processing (e-QIP)	An automated tool for processing standard investigative questionnaires.
Enrollment Officer	The individual who initiates the chain of trust for identity proofing and provides trusted services to confirm employer sponsorship, bind an Applicant to his biometric, and validate identity documentation. The Enrollment Officer delivers a secured enrollment package to the IDMS for adjudication.
eVerify	An Internet based system operated by the Department of Homeland Security (DHS) in partnership with the Social Security Administration (SSA) that allows participating employers to electronically verify the employment eligibility of their newly hired employees.
External Identity Provider (IDP)	A service or system that establishes an individual's identity and links the identity to a physical or electronic credential or token. IDP's validate the identity of the individual using the credential or token issued and pass along verification of the individual's identity to a relying party, usually through a SAML assertion. Within this Use Case, External IDPs are agency systems, other than the agency performing the validation. External IDP's are those systems or services that are not directly controlled or managed by the agency.
External System or Third Party Application	Resources maintained and operated by a separate federal agency, the private sector, or another third party outside of the agency.
External User	Any individual attempting or requesting access to agency facilities or systems that is not an employee, contractor, or primary affiliate of the agency. External users may be PIV holders from another agency, business partners, or private citizens.
Fitness Determination	A decision by an agency that an individual has or does not have the required level of character and conduct necessary to perform work for or on behalf of a Federal agency as an employee in the excepted service (other than in an excepted service position where the incumbent can be noncompetitively converted to competitive service) or as a contractor employee.
Global Federated Identity and Privilege Management (GFIPM) framework	An initiative that provides the justice community and partner organizations with a standards-based approach for implementing federated identity management using the concept of globally understood metadata. GFIPM utilizes direct trust across participating agencies.
Integrated Automated Fingerprint Information System (IAFIS)	A national fingerprint and criminal history system maintained by the FBI, Criminal Justice Information Services (CJIS) Division that provides automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

[53] "Identity Management Task Force Report 2008." National Science and Technology Council, Subcommittee on Biometrics and Identity Management, Pg. G-5.

Term	Definition
Identity	The unique biological person defined by DNA; the physical being.[54]
Identity Management (IdM)	The combination of technical systems, rules, and procedures that define the ownership, utilization, and safeguard of personal identity information.[55]
Identity Management System (IDMS)	An automated system of hardware (servers) and software (programs) that provides the workflow management (services) of identity functions, as normatively described in FIPS 201. An IDMS is separately layered and/or compartmentalized within one system and/or a modular component of an agency's centralized system/enterprise. The IDMS will be encapsulated in an environment that is secure, auditable and protect the privacy of personal information. The IDMS establishes the centralized Chain-of Trust that is then integrated into the components of a FIPS 201 enterprise.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Internal/Agency/Local Application or System	A logical system, software or other application to which access is controlled by a particular agency. Internal systems are those hosted, managed, or otherwise controlled by the agency. These systems may only be available within the agency networks and behind agency firewalls.
Internal Actors	Individuals (users, applicants, credential holders, etc.) that primarily consist of employees and contractors of an agency, but also include any fellows, interns, researchers or other individuals tightly affiliated with an agency. These are users who have a primary affiliation to the agency, and for whom the agency typically collects digital identity records and provides credentials such as PIV cards.
Investigative Service Provider (ISP)	An entity responsible for collecting and processing personal investigative data, performing various checks, and providing investigative results to the requesting agency.
Investigator	An authorized individual who performs background investigations on behalf of an Investigative Service Provider.
Issuer	The entity that issues a credential to the Applicant after all identity proofing, background checks, and related approvals have been completed, especially for PIV and PKI credentials.
Joint Personnel Adjudication System (JPAS)	The Department of Defense personnel security system, which provides information regarding clearance, access, and investigative status to authorized DoD security personnel and other interfacing organizations.
Law Enforcement Information Sharing Program (LEISP)	Program that supports a collaborative process involving senior leadership from DOJ component agencies and representatives from across the national law enforcement community. This program supports a Trusted Broker and information exchange protocol currently in use across several domains.

[54] "Task Force Report." Pg. G-5.

[55] "Task Force Report." Pg. G-5

Term	Definition
Logical Access Control System (LACS)	An automated system that controls an individual's ability to access one or more computer system resources such as a workstation, network, application, or database. A logical access control system requires validation of an individual's identity through some mechanism such as a PIN, card, biometric, or other token. It has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.
Mission Systems	Applications and systems required to perform agency mission goals, such as census data collection systems within the Census Bureau, grant management systems within the Department of Education, and mission control applications in NASA.
National Crime Information Center (NCIC)	A computerized index of criminal justice information maintained by the FBI that is commonly used to verify suitability of visitors prior to granting access to facilities.
Non-Person Entity (NPE)	Any type of non-human device (e.g., routers, servers, switches, firewalls, sensors) or software object.
Password Token	A password linked to a user identity that provides some level of confidence in the identity of the password owner. A password token may be used to grant access to more than one application.
Physical Access Control System (PACS)	An automated system that manages the passage of people or assets through an opening (s) in a secure perimeter (s) based on a set of authorization rules.
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.
Registrar	An entity that establishes the identity of an Applicant prior to credential issuance (also referred to as an Enrollment Official). In the PIV process, the Registrar authenticates the Applicant's identity by checking identity source documents and identity proofing and ensures a proper background check has been completed before the PIV credential is issued. In a PKI process, the Registrar is referred to as a RA.
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.
Security Clearance Determination	Determination of whether or not an individual is eligible for access to sensitive or classified information.
Sponsor	Actors that verify that applicants have a need for a credential and initiate the credential enrollment and issuance process, especially for PKI and PIV credentials.
Suitability Determination	A decision by OPM or an agency with delegated authority that a person is suitable or is not suitable for employment in the competitive service, in the excepted service where the incumbent can be noncompetitively converted to competitive service, or career appointment in the Senior Executive Service.
Support Systems	Applications and systems that support cross agency functionality typically aligned to a line of business (LOB), such as Payroll, Contract Management or HR systems.
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.

Term	Definition
User	An individual that is utilizing services provided by an agency. Users may be credential holders, applicants, or employees. This definition is specific to the Use Case. General term is applied to an individual who is at one stage an Applicant and who becomes a Cardholder or other status.
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.
Visitor	An external user (see definition above) that is requesting short term access to an agency facility.

This page is intentionally left blank.

Appendix C Policy List

GROUP	DOCUMENT NAME	DESCRIPTION
Joint Security and Suitability Reform Team	Federal Investigative Standards	This document 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-00-10	This document provides Executive agencies with the guidance required under Sections 1703 and 1705 of the GPEA, P. L. 105-277, Title XVII. GPEA requires agencies, by October 21, 2003, to provide for the (1) option of electronic maintenance, submission, or disclosure of information, when practicable as a substitute for paper; and (2) use and acceptance of electronic signatures, when practicable. GPEA specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form.
OMB	M-04-04	This guidance requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. It establishes and describes four levels of identity assurance for electronic transactions requiring authentication. Assurance levels also provide a basis for assessing CSPs on behalf of Federal agencies. This document will assist agencies in determining their E-Government authentication needs. 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	This memo requires the use of an SSP to mitigate the risk of commercial managed services for public key infrastructure (PKI) and electronic signatures.
OMB	M-05-22	This memorandum and its attachments provide guidance to the agencies to ensure an orderly and secure transition from Internet Protocol Version 4 (IPv4) to Version 6 (IPv6).
OMB	M-05-24	This memorandum provides implementing instructions for HSPD-12 and FIPS 201.
OMB	M-06-16	The memorandum directs all Federal Agencies and departments to "encrypt all sensitive data on their mobile computers/devices."
OMB	M-06-18	This memorandum provides updated direction for the acquisition of products and services for the implementation of HSPD-12 “Policy for a Common Identification Standard for Federal Employees and Contractors” and also provides status of implementation efforts.
OMB	M-07-06	This memorandum discusses validation and monitoring agency issuance of Personal Identity Verification (PIV) compliant identity credentials.
OMB	M-07-16 (esp. Attachment 1)	As part of the work of the Identity Theft Task Force, this memorandum requires agencies to develop and implement a breach notification policy within 120 days.
OMB	M-07-20	This memorandum provides instructions for completing your agency’s annual E-Government Act report as required by the E-Government Act of 2002 (Pub. L. No. 107-347) (Act).
OMB	M-08-01	This memorandum serves as a reminder for agencies to complete background investigations and issue credentials as required for the implementation of HSPD-12.
Presidential Directive	HSPD-5	The purpose of this directive is to enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system.

GROUP	DOCUMENT NAME	DESCRIPTION
Presidential Directive	HSPD-7	This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.
Presidential Directive	HSPD-8	The purpose of this directive is to "establish policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and local entities."
Presidential Directive	HSPD-12	HSPD-12 calls for a mandatory, government-wide standard for secure and reliable forms of ID issued by the Federal Government to its employees and employees of federal contractors for access to federally-controlled facilities and networks.
Presidential Directive	HSPD-24	"This directive establishes a framework to ensure that Federal executive departments and agencies use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under United States law."
DOJ	The Privacy Act of 1974	This act protects certain Federal Government records pertaining to individuals. In particular, the Act covers systems of records that an agency maintains and retrieves by an individual's name or other personal identifier (e.g., social security number).
DHS	REAL ID Act of 2005	This statute requires minimum performance standards to improve the integrity and security of state-issued driver's licenses and identification cards. (Regulations were promulgated by DHS).
OPM	Final Credentialing Standards	Formally titled *Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12,* this memorandum provides final government-wide credentialing standards to be used by all Federal departments and agencies in determining whether to issue or revoke personal identity verification (PIV) cards to their employees and contractor personnel, including those who are non-United States citizens.
TSA	Maritime Transportation Safety Act	The Maritime Transportation Safety Act of 2002 requires the prevention of individuals from gaining access to a secure area of a vessel or facility unless authorized to be the area and requires that individual to hold a transportation security card unless escorted (Regulations were promulgated by DHS, and resulted in the Transportation Worker Identification Credential).
N/A	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	HIPAA protects the privacy of individually identifiable health information. The Act also provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information.
N/A	Government Paperwork Elimination Act of 1998 (GPEA)	GPEA requires Federal agencies, by October 21, 2003, to allow individuals or entities that deal with the agencies the option to submit information or transact with the agency electronically, when practicable, and to maintain records electronically, when practicable. The Act specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form, and encourages Federal Government use of a range of electronic signature alternatives.
N/A	E-Government Act of 2002	This act is intended to enhance the management and promotion of electronic Government services and processes by establishing a Federal CIO within the Office of Management and Budget, 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.

GROUP	DOCUMENT NAME	DESCRIPTION
N/A	Electronic Signatures In Global and National (ESIGN) Commerce Act of 2000	This act was intended to facilitate the use of electronic records and signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically.
N/A	Federal Information Security Management Act (FISMA) of 2002	This act 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	Federal Government Intelligence Reform and Terrorism Prevention Act of 2004	This act contains a variety of measures designed to reform the intelligence community and the intelligence and intelligence-related activities of the United States Government.
N/A	Public Law No: 110-53, The Implementing the 9/11 Commission Recommendations Act of 2007	This law provides for the implementation of the recommendations of the National Commission on Terrorist Attacks Upon the United States.
N/A	Executive Order 12977	Established the ISC to develop standards, policies and best practices for enhancing the quality and effectiveness of physical security in, and the protection of, nonmilitary federal facilities in the United States.
N/A	Executive Order 13467	Established to ensure an efficient, practical, reciprocal, and aligned system for investigating and determining suitability for Government employment, contractor employee fitness, and eligibility for access to classified information.

This page is intentionally left blank.

Appendix D Risk Registry

Segment Name / ID		Federal Identity Credential and Access Management (FICAM) Segment					Risk List
Purpose of Risk List:		The Risk List is used to track and manage risks to the FICAM segment.					
ID	Risk Label	Risk Description	Risk Category	Severity	Probability	Risk Score	Mitigation Plan
Unique tracking number for each risk	Brief label for the Risk	Detailed description of the Risk including the expected impact if the risk occurs	Category description (i.e., type) of the risk	Severity of the risk to the project scope, schedule, and resources if it occurs	Likelihood that the risk may occur	Overall scoring of the risk (=severity x probability)	The overall plan to reduce the probability or effect of the risk.
1	Segment Cost Impacts	Agency plans and budgets may not include ICAM activities; as a result, adequate funding may not be available.	Cost	High	High	High	Development of transition plan including milestones and priorities to guide Agency budget requests. Agencies must ensure that sufficient resources are available for ICAM activities, and should submit budget request for funds to address relevant ICAM transition activities.
2	ICAM compliance and alignment	Agencies may resist compliance with ICAM segment architecture (both business and technology framework), perpetuating inefficiencies and threatening success of government-wide ICAM vision.	Governance	High	High	High	Incorporate the 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.

Segment Name / ID		Federal Identity Credential and Access Management (FICAM) Segment					Risk List
Purpose of Risk List:		The Risk List is used to track and manage risks to the FICAM segment.					
ID	Risk Label	Risk Description	Risk Category	Severity	Probability	Risk Score	Mitigation Plan
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.	Governance	High	Medium	High	Identify reasons for non-compliance. Seek executive buy-in to achieve alignment. Incorporate requirements into FISMA/ATO processes and sign-off. Conduct outreach to Inspector General (IG)/Government Accountability Office (GAO) to help ensure audit plans incorporate requirements.
4	Role Authentication	Lack of ability to authenticate role information for individuals could threaten success of G2B interactions, where the identity of the end user is less important than their role within a company (i.e., can an employee legally commit his firm?)	Governance	Low	High	Medium	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.	Governance	Low	Low	Low	"PIV capable" requirement incorporated into investment approval, and FISMA/ATO requirements. Conduct outreach to Inspector General (IG)/Government Accountability Office (GAO) to help ensure audit plans incorporate requirements.

Segment Name / ID		Federal Identity Credential and Access Management (FICAM) Segment					Risk List
Purpose of Risk List:		The Risk List is used to track and manage risks to the FICAM segment.					
ID	Risk Label	Risk Description	Risk Category	Severity	Probability	Risk Score	Mitigation Plan
6	Organizational trust	Consistent approach for negotiating organizational trust lags behind standards for trusted credentials and transaction-based identity authentication.	Governance	Medium	Medium	Medium	Additional guidance/use cases for establishing organizational trust relationships between service providers and consumers.
7	Citizen Outreach Traction	The Federal Government will not achieve effective service delivery and Return on Investment (ROI) on Citizen Outreach efforts unless offerings attract a sufficient number of users to provide value and gain traction with the public at large (i.e., network effect).	Performance	Medium	Medium	Medium	ICAM initiatives must include deliberate action to drive applications or credentials to critical mass. Targets should be high value applications within specific Communities of Interest to drive rapid adoption.
8	Performance Tracking	Without appropriate tracking and consequences, Agencies may not meet ICAM segment performance metrics.	Performance	Medium	Medium	Medium	Implement controls to track performance.
9	IDP Liability	Commercial entities may be unwilling to serve as an IDP to the government over liability concerns, threatening successful federation models.	Policy/Guidance	Medium	Medium	Medium	Engage privacy community, DOJ, and industry groups to provide solutions that mitigate this risk.
10	Digital Signature Traction	Agencies may resist adoption of digital signature applications based upon historical behavior.	Policy/Guidance	Low	Low	Low	Enhanced digital signature guidance.

Segment Name / ID		Federal Identity Credential and Access Management (FICAM) Segment					Risk List
Purpose of Risk List:		The Risk List is used to track and manage risks to the FICAM segment.					
ID	Risk Label	Risk Description	Risk Category	Severity	Probability	Risk Score	Mitigation Plan
11	Exposure of PII	Driving an increase in e-Government creates additional points of electronic exposure for personally identifiable information (PII), increasing the risk of data compromise.	Privacy	High	Low	Medium	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.	Privacy	Low	Medium	Low	Single centralized architectural components should be avoided, where possible. Attention should be paid to prevent an easily traceable "trail" left behind by authentication solutions (e.g., OpenID Uniform Resource Identifiers, Social Security Numbers, etc) Privacy principles must be incorporated into solution level architecture.
13	Claims Assurance	Poor authorization decisions may result if FICAM focus is limited to identity authentication without incorporation of claims like attributes, privileges, roles, etc.	Security	Medium	High	High	New guidance around attribute authorities. Potential guidance on binding claims to identities. Incorporate claims delivery and trust into FICAM conceptual solution architecture.

Segment Name / ID		Federal Identity Credential and Access Management (FICAM) Segment					Risk List
Purpose of Risk List:		The Risk List is used to track and manage risks to the FICAM segment.					
ID	Risk Label	Risk Description	Risk Category	Severity	Probability	Risk Score	Mitigation Plan
14	Visual Authentication	Agencies continue to rely on visual authentication of PIV credentials for physical access, which fails to comply with HSPD-12 and could undermine the enhanced security enabled through electronic authentication.	Security	Medium	High	High	Implementation of the maturity model identified in SP 800-116 with oversight and tracking by Agency IG.
15	Undiscoverable federal trust graph	As new mechanisms such as bridges and inter-federation are employed, it may become difficult to deterministically discover every IDP trusted (directly and indirectly) by the government	Technology	Medium	High	High	Architectural solutions should address.
16	Non-PIV solution alignment	Related credentialing efforts in other sectors (e.g., FRAC, TWIC, eHealth) may not align with PIV or FEDERAL PKI standards, affecting credential interoperability and service delivery.	Technology	Medium	High	High	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.	Technology	Medium	Medium	Medium	Requires multi-tiered interoperability approach, including industry testing, deployment testing, scheme adoption lifecycle, implementation guidance, etc.

Segment Name / ID		Federal Identity Credential and Access Management (FICAM) Segment					Risk List
Purpose of Risk List:		The Risk List is used to track and manage risks to the FICAM segment.					
ID	Risk Label	Risk Description	Risk Category	Severity	Probability	Risk Score	Mitigation Plan
18	Digital identity schema incompatibilities	Lack of common standards for digital identity data and incompatibilities between existing schemas and commercial products could prevent interoperability and the use of desired standards/products (e.g., SAML products).	Technology	Medium	Medium	Medium	Define government-wide standards for identity data schemas. Coordinate with vendors through interoperability lab to find solutions.
19	Lack of approved technologies in emerging areas of ICAM	Interoperability could be compromised if an approved set of technologies and vendors is not specified for technologies in new and rapidly evolving areas.	Technology	Medium	Medium	Medium	Coordinate existing approved products mechanisms (including SIN 132-6X) and procurement vehicles (schedules) across ICAM initiatives.
20	COTS PD-VAL	COTS support for Path Discovery and Validation (PD-Val) is not widespread, resulting in relying party on third applications that don't work properly with government identity credentials.	Technology	Low	High	Medium	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.	Technology	Low	Medium	Low	ICAM segment architecture transition plan should include approach to provide coordination with solution providers and other solution consumers.

Segment Name / ID		Federal Identity Credential and Access Management (FICAM) Segment					Risk List
Purpose of Risk List:		The Risk List is used to track and manage risks to the FICAM segment.					
ID	Risk Label	Risk Description	Risk Category	Severity	Probability	Risk Score	Mitigation Plan
22	Availability/ interoperability of alternate biometric modalities	Lack of common, standardized alternative biometrics could prevent interoperability for exceptional use cases across Agencies (primarily for PIV and PIV-I).	Technology	Low	Medium	Low	Additional guidance/standards regarding alternate biometrics pending. Identify authoritative source for government biometrics.

This page is intentionally left blank.

Appendix E ICAM Segment Architecture Development Approach Details

Architectures within the FEA may be developed at the enterprise, segment, or solution level. The levels address different business perspectives, varying the level of detail and addressing related but distinct concerns. Figure 60, provided in the FEA Practice Guidance document,[56] depicts the hierarchical relationships between enterprise, segment, and solution architectures.

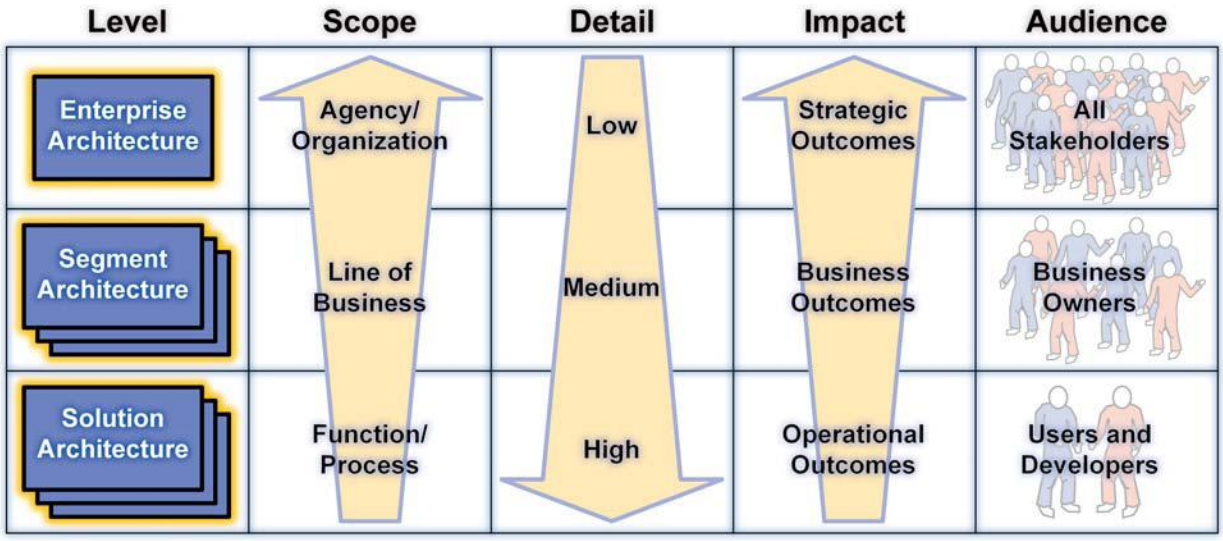

Figure 60: Levels of Architecture

A segment architecture defines a simple roadmap for a core mission area, business service, or enterprise service. Of the three types, ICAM is considered an enterprise service segment, but it supports and functions across mission areas (e.g., providing for student loans) and business services (e.g., Human Resources Line of Business). The ICAM segment falls within the overall framework established by the FEA but has been extended and specialized extensively to address the unique aspects of ICAM enterprise services. Where common data, business processes, investments, and technologies defined at the federal enterprise level are applicable to ICAM, they have been included and reused in the segment.

In order to complete the development work necessary for the segment architecture, working groups were developed along with leadership appointed to facilitate the effort over time. These four new entities included:

- **Roadmap Development Team Lead**. The team lead facilitates the activities of the project team. The team lead is responsible for coordinating resolution of development team comments and contributions, serving as a point of contact for all government and contractor members of the Roadmap Development Team, coordinating activities with the Lead Architect and supporting working groups, and reporting to the ICAMSC on the progress of the initiative.

[56] FEA Practice Guidance, Federal Enterprise Architecture Program Management Office, OMB, November 2007. http://www.whitehouse.gov/omb/assets/fea_docs/FEA_Practice_Guidance_Nov_2007.pdf

- **Roadmap Development Team.** Representatives from all FCIOC organizations with experience in ICAM projects. The Roadmap Development Team is responsible for providing support for development of the roadmap through participation in bi-weekly meetings to review and provide comments on drafts of the roadmap, providing relevant documentation from their agency to support development of the roadmap, and coordinating enterprise architecture inputs from practitioners at their respective agencies.
- **Lead Architect**. Senior Enterprise Architecture practitioner who helps business owners identify the business issues to be addressed by the segment and the expected results of the work products. The Lead Architect guides the Core Team and serves as a subject matter expert for the development of the ICAM segment architecture.
- **Core Team.** A subset of the larger Roadmap Development Team, this group includes key subject matter experts from select agencies responsible for hands on development of the roadmap and resolving components of the ICAM segment architecture. The Core Team is responsible for participating in ad hoc content development and consensus sessions related to specific content areas and reaching back to resources at their agencies as needed to provide expertise.

The Federal CIO Council and the ISIMC provided primary oversight during the development effort with support from the ICAMSC. In developing the segment architecture, the Roadmap Development Team worked closely with several working groups under the ICAMSC, including the Architecture Working Group (AWG) and the Citizen Outreach Focus Group (COFG). The AWG was specifically tasked with supporting the development of the ICAM Technical and Data architectures.

The Roadmap Development Team leveraged existing agency identity management architectures extensively in the creation of the ICAM segment architecture. This approach allowed the team to benefit from the best aspects of work that has already been performed across the Federal Government, both improving the quality and alignment of the architecture and allowing for development of the architecture within the aggressive timeframe allotted.

The development of the ICAM segment architecture was conducted in accordance with the guidance provided by OMB in the ICAM Roadmap Architecture Development Approach document.[57] That guidance states that the ICAM segment architecture and roadmap should 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?

[57] Identity, Credential and Access Management Roadmap: Applying a Segment Architecture Approach to Streamlining, Consolidating and Enhancing Authentication and Credentialing Capabilities within the Federal Government, OMB, February 10, 2009.

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.** Includes the initial steps to identify and engage the appropriate participants, define the purpose of the segment, and establish a project management foundation for the effort.
- **Step 2: Define the Segment Scope and Strategic Intent.** Includes activities to define the scope, goals, and objectives and identify the strategic improvement opportunities for the segment. Activities in the later FSAM process steps seek alignment with the strategic intent defined in Step 2.
- **Step 3: Define Business and Information Requirements.** Includes activities to analyze the segment business and information environments and determine the business and information improvement opportunities that will achieve the target performance architecture. The business and data architectures are developed at the end of this step.
- **Step 4: Define the Conceptual Solution Architecture.** Includes steps to develop the conceptual solution architecture, an integrated view of the combined systems, services, and technology architectures that support the target performance, business, and data architectures developed in the preceding process steps.
- **Step 5: Author the Modernization Blueprint.** Includes actions to create a series of validated implementation recommendations to transition from the as-is to the target state articulated through sequencing and transition plans.

The following figure, provided in the FSAM, illustrates the process steps of the methodology and their relationships to enterprise and solution level architectural efforts.

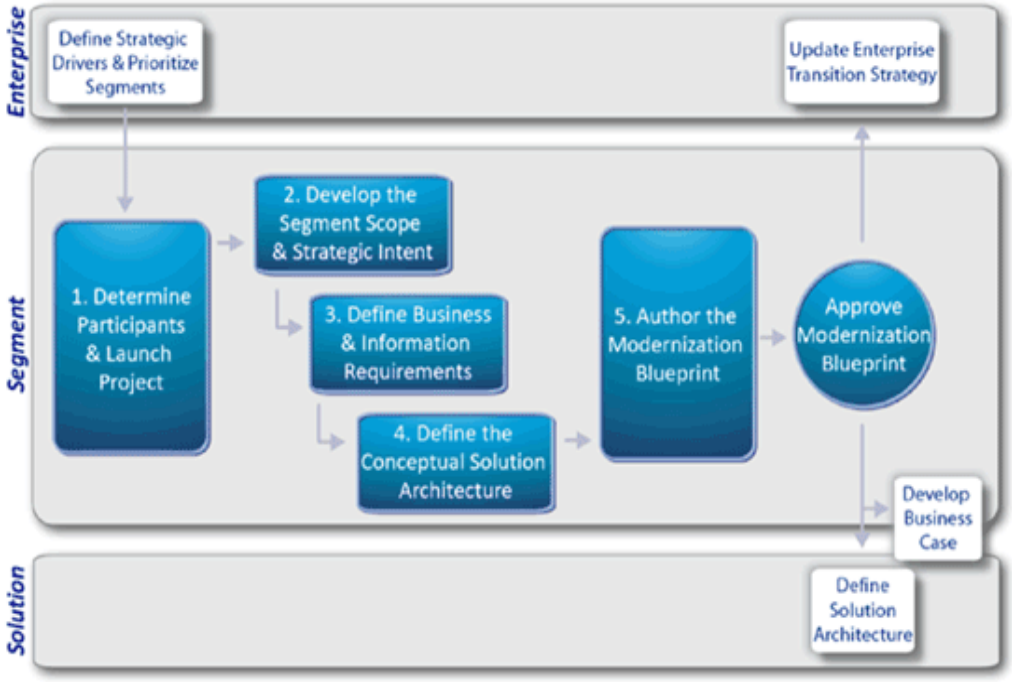

Figure 61: FSAM Implementation Steps

The following table details the activities that were performed and the outputs that were created for each process step during the development of the ICAM segment architecture.

	Step 1: Determine Participants and Launch 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
Activities	• Determine the executive sponsor • Develop the purpose statement for the segment • Solicit core team members • Create core team charter and project plan • Establish the communications strategy	• Establish segment scope and context • Identify and prioritize strategic improvement opportunities • Define segment strategic intent • Validate and communicate the scope and strategic intent	• Determine current business and information environment associated with strategic improvement opportunities • Determine business and information improvement opportunities • Define target business and data architectures • Validate and communicate target business and data architectures	• Assess systems and technology environment for alignment with performance, business, and information requirements • Define the target conceptual solution architecture • Identify and analyze system and service transition dependencies • Validate and communicate the conceptual solution architecture	• Perform cost / value / risk analysis to develop implementation recommendations • Develop draft blueprint and sequencing plan • Review and finalize the blueprint and sequencing plan • Brief core team and obtain approval
Outputs	• Segment Architecture Purpose Statement • Core Team Roster • Roles & Responsibilities • Project Plan	• Stakeholder List • Policy Map • Risk Registry • Business Challenges Analysis • Business Drivers, Goals, & Objectives • Performance Metrics	• Business Value Chain Analysis • As-is Use Cases • Inventory of Authoritative Data Sources & Data Elements • Target Use Cases • Target Information Flow Diagram	• As-is System Interface Diagram • Target System Interface Diagram • Services Framework	• Recommendation Implementation Overview • Implementation Sequencing Plan • Transition Plan Milestones • Comments Matrix

Figure 62: Tailored FSAM Outputs for the Federal ICAM Segment

The outputs shown in Figure 62 were created and reviewed as stand-alone assets during the development of the ICAM segment. They have since been aligned to the chapters throughout this document in a manner that provides structure and supports a logical progression to the reader for using the architecture.

Appendix F ICAM Data Standards and Guidance

GROUP	DOCUMENT NAME	DESCRIPTION
AWG	HSPD-12 Shared Component Infrastructure Interface Specification Common Elements	This document provides Extensible Markup Language (XML) elements common to [Agency-SIP] and [ESP-SIP].
AWG	HSPD-12 Shared Component Infrastructure Metadata Management	This document describes SCI metadata management. It captures assumptions the AWG has made about the full lifecycle of SCI metadata (definition, distribution, configuration, use, and maintenance).
AWG	Finalization Service Provider to System Infrastructure Provider Interface	This document describes the interface for Finalization Service Provider (FSP) and Systems Infrastructure Provider (SIP) data exchange. It is a standard, re-usable shared service for Federal government-wide use, per [SCI Architecture]. Therefore, one should read [SCI Architecture] before reading this document.
AWG	System Infrastructure Provider and Production Service Provider Interface Specification	This document provides the interface specification for Systems Infrastructure Provider (SIP) and Production Service Provider (PSP) data exchange. It is a standard, re-usable shared service specification for Federal government-wide use, per [SCI Architecture]. Therefore, one should read [SCI Architecture] before reading this specification.
AWG	System infrastructure Provider to Federal PKI Shared Service Provider Interface Specification	This document provides the interface specification for Systems Infrastructure Provider (SIP) and Federal Public Key Infrastructure (PKI) Shared Service Provider (SSP) data exchange. It is a standard, re-usable shared service specification for Federal government-wide use, per [SCI Architecture]. Therefore, one should read [SCI Architecture] before reading this specification.
NIST	SP 800-73	This document specifies the PIV data model, command interface, client application programming interface and references to transitional interface specifications.
NIST	SP 800-73, Parts 1, 2, 3, and 4	This document contains technical specifications to interface with the smart card to retrieve and use the identity credentials. The specifications reflect the design goals of interoperability and PIV Card functions. The goals are addressed by specifying a PIV data model, card edge interface, and Application Programming Interface (API). Moreover, SP 800-73 enumerates requirements where the standards include options and branches. The specifications go further by constraining implementers' interpretations of the normative standards. Such restrictions are designed to ease implementation, facilitate interoperability, and ensure performance, in a manner tailored for PIV applications.
NIST	SP 800-76	This document contains technical specifications for biometric data mandated in [FIPS]. These specifications reflect the design goals of interoperability and performance of the PIV Card. This specification addresses image acquisition to support the background check, fingerprint template creation, retention, and authentication. The biometric data specification in this document is the mandatory format for biometric data carried in the PIV Data Model (Appendix A of SP 800-73-1). Biometric data used only outside the PIV Data Model is not within the scope of this standard.

GROUP	DOCUMENT NAME	DESCRIPTION
NIST	SP 800-87	This document provides the organizational codes for federal agencies to establish the FASC-N that is required to be included in the FIPS 201 Card Holder Unique Identifier. SP 800-87 is a companion document to FIPS 201.
NIST	SP 800-103	This document provides the broadest possible range of identity credentials and supporting documents insofar as they pertain to identity credential issuance. Priority is given to examples of primary and secondary identity credentials issued within the United States. Part 2 of this document will provide an Extensible Markup Language (XML) schemas, as a framework for retention and exchange of identity credential information.
NIST	SP 800-104	The purpose of this document is to provide additional recommendations on the Personal Identity Verification (PIV) Card color-coding for designating employee affiliation. The recommendations in this document complement FIPS 201 in order to increase the reliability of PIV card visual verification.
NIST	SP 800-122	The purpose of this document is to assist Federal agencies in protecting the confidentiality of a specific category of data commonly known as personally identifiable information (PII). This document provides practical, context-based guidance for identifying PII and determining what level of protection is appropriate for each instance of PII. The document also suggests safeguards that may offer appropriate levels of protection for PII and provides recommendations for developing response plans for breaches involving PII.
NIST	FIPS 199	FIPS Publication 199 develops standards for categorizing information and information systems. Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the Federal Government, promotes: (i) effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and (ii) consistent reporting to the Office of Management and Budget and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.
NIST	FIPS 201-1	This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems.
GSA	E-Authentication Federation Adopted Scheme	This interface specification provides guidance on how to use SAML 2.0 SSO Profile using HTTP POST specifically for Federation purposes.
IAB	Technical Implementation Guidance Smart Card Enabled Physical Access Control Systems	The purpose of this guidance is to define specifications and standards required to enable agencies to procure and implement hardware and software for PACS, such that these systems will: Operate with the Federal Agency Smart Credential (FASC), such as NIST standards based Personal Identity Verification (PIV) cards; Facilitate cross-agency, federal enterprise interoperability; Allow existing legacy PACS to operate with FASC compatible card readers until the time comes for its upgrade.

GROUP	DOCUMENT NAME	DESCRIPTION
UCore	UCore	Universal Core (UCore) is a federal initiative that supports the National Information Sharing Strategy and all associated Departmental / Agency strategies. UCore enables information sharing by defining an implementable specification (XML Schema) containing agreed upon representations for the most commonly shared and universally understood concepts of Who, What, When, and Where.
NIEM	NIEM	NIEM, the National Information Exchange Model, is a partnership of the U.S. Department of Justice and the Department of Homeland Security. It is designed to develop, disseminate and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation.
NIST	ANSI/NIST-ITL 1-2000, and 2006	ANSI/NIST-ITL 1-2000: Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information An approved ANSI standard for describing the fingerprint data interchange format used by Law Enforcement agencies (e.g., FBI, State and Local Police) Currently being updated with a number of changes, including an XML representation. This update, commonly referred to as ANSI/NIST-ITL 1-2006, has not yet been approved. A proposed draft is currently in review. EFTS: Electronic Fingerprint Transmission Specification. A specific implementation of the ANSI/NIST-ITL 1-2000 standard, describing how to communicate with the FBI IAFIS. Will be updated to reflect changes in ANSI/NIST-ITL 1-2006 and renamed to EBTS: Electronic Biometric Transmission Specification.
ISO/IEC	ISO/IEC 24727	ISO/IEC 24727 defines interoperable programming interfaces to integrated circuit cards (and other identity credential types). In its entirety, ISO/IEC 24727 defines a secure, distributed, adaptive implementation of a high-level identity API, the Service Access Layer. Programming interfaces are defined for all card lifecycle stages and for use with integrated circuit cards. ISO/IEC 24727 is written with sufficient detail and completeness that independent implementations of each component are interchangeable and can interoperate with independent implementations of the other components.

This page is intentionally left blank.

Appendix G ICAM Technical Standards and Guidance

GROUP	TYPE	NAME	DESCRIPTION
ANSI/SIA	Standards	OSIPS-01: 2008, Framework	This document provides requisite definitions including interface infrastructure requirements and special interfaces for shared activities such as event reporting, schedules exchange and other common elements. It is designed to enable the open integration of different types of components within an enterprise system.
ANSI/SIA	Standards	OSIPS-ACR-200x	This document describes identity authentication and calculating access authentication factors that are presented in an access transaction seeking approval of a grant of access to an Accessible Component Collection.
ANSI/SIA	Standards	OSIPS-APC:200x	This document describes the access point and credentials presented to field devices at the access point controller.
ANSI/SIA	Standards	OSIPS-IDM:200x	This document describes identities and carrier claims of identity that are authenticated by comparing reference authentication factors with presented credentials.
AWG	Guidance	HSPD-12 Shared Component Infrastructure Trust Model	This document describes the Trust Model (TM) for the HSPD-12 shared component infrastructure (SCI). It captures assumptions the AWG has made on how architectural components will trust each other.
AWG	Guidance	HSPD-12 Shared Component Architecture	This document describes the SCA and captures AWG decisions based on relevant business processes and derived use cases. Decisions captured include: What architectural components are required; How and when architectural components interoperate to support all use cases; and how architectural components are technically constructed
AWG	Guidance	HSPD-12 Shared Component Infrastructure Technical Interoperability Model	This document describes the Technical Interoperability Model (TIM) for the HSPD-12 shared component infrastructure (SCI). It captures assumptions the AWG has made on how architectural components will technically interoperate with each other.
AWG	Guidance	Agency to System Infrastructure Provider Interface Specification	This document provides the interface specification for agency system and Systems Infrastructure Provider (SIP) data exchange. It is a standard, re-usable shared service specification for Federal government-wide use, per [SCI Architecture].
AWG	Guidance	Enrollment Service Provider to System Infrastructure Provider Interface Specification	This document provides the interface specification for Enrollment Service Provider (ESP) and Systems Infrastructure Provider (SIP) data exchange. It is a standard re-usable shared service specification for Federal government-wide use, per [SCI Architecture].
AWG	Guidance	HSPD-12 Fingerprint Process Considerations & Research	The following research and analysis was conducted as a part of the HSPD-12 AWG effort to develop standard interfaces for the Enrollment Service Providers.

GROUP	TYPE	NAME	DESCRIPTION
AWG	Guidance	Backend Attribute Exchange Architecture and Interface Specification	This document's primary objective is to define an interoperable model and interface for government-wide BAE. This document provides a high-level description of BAE business use cases, BAE business processes, the BAE architectural model, and standards-based BAE interface specifications. Some sections are normative (e.g., interface specification), while other sections are informational or recommendations (e.g., governance).
AWG	Guidance	HSPD-12 Implementation Architecture Working Group Concept Overview	This document briefly covers concepts that are critical to understanding the shared component architecture.
NIST	Guidelines	SP 800-53 (parts)	This is the first major update of Special Publication 800-53 since its initial publication in December 2005. This document provides significant improvements to the security control catalog. In addition, the changing threat environment and growing sophistication of cyber attacks necessitated specific changes to the allocation of security controls and control enhancements in the low-impact, moderate-impact, and high-impact baselines. Lastly, this document has added new security controls to address organization-wide security programs and introduced the concept of a security program plan to capture security program management requirements for organizations.
NIST	Guidelines	SP 800-63	This document supplements OMB guidance, by providing technical guidelines for the design of electronic systems for the remote authentication of citizens by government agencies. The revision represents an expansion and reorganization of the original document, broadening the discussion of technologies available to agencies, and giving a more detailed discussion of assertion technologies. Changes intended to clarify the pre-existing requirements are also included in the revision. The bulk of the changes since the previously posted draft of SP 800-63 concern assertion technologies and Kerberos.
NIST	Guidelines	SP 800-67	This publication specifies the Triple Data Encryption Algorithm (TDEA), including its primary component cryptographic engine, the Data Encryption Algorithm (DEA). When implemented in an SP 800-38 series-compliant mode of operation and in a FIPS 140 compliant cryptographic module, TDEA may be used by Federal organizations to protect sensitive unclassified data. Protection of data during transmission or while in storage may be necessary to maintain the confidentiality and integrity of the information represented by the data. This recommendation precisely defines the mathematical steps required to cryptographically protect data using TDEA and to subsequently process such protected data. The Triple Data Encryption Algorithm (TDEA) is made available for use by Federal agencies within the context of a total security program consisting of physical security procedures, good information management practices, and computer system/network access controls.

GROUP	TYPE	NAME	DESCRIPTION
NIST	Guidelines	SP 800-73, Parts 1, 2, 3, and 4	This document contains technical specifications to interface with the smart card to retrieve and use the identity credentials. The specifications reflect the design goals of interoperability and PIV Card functions. The goals are addressed by specifying a PIV data model, card edge interface, and Application Programming Interface (API). Moreover, SP 800-73 enumerates requirements where the standards include options and branches. The specifications go further by constraining implementers' interpretations of the normative standards. Such restrictions are designed to ease implementation, facilitate interoperability, and ensure performance, in a manner tailored for PIV applications.
NIST	Guidelines	SP 800-76	This document contains technical specifications for biometric data mandated in [FIPS]. These specifications reflect the design goals of interoperability and performance of the PIV Card. This specification addresses image acquisition to support the background check, fingerprint template creation, retention, and authentication. The goals are addressed by citing biometric standards normatively and by enumerating requirements where the standards include options and branches. In such cases, a biometric profile can be used to declare what content is required and what is optional. This document goes further by constraining implementers' interpretation of the standards. Such restrictions are designed to ease implementation, assure conformity, facilitate interoperability, and ensure performance, in a manner tailored for PIV applications. The biometric data specification in this document is the mandatory format for biometric data carried in the PIV Data Model (Appendix A of SP 800-73-1). Biometric data used only outside the PIV Data Model is not within the scope of this standard. This document does however specify that any biometric data in the PIV Data Model shall be embedded in the Common Biometric Exchange Formats Framework (CBEFF) structure of section 6. This document provides an overview of the strategy that can be used for testing conformance to the standard.
NIST	Guidelines	SP 800-78	This document contains the technical specifications needed for the mandatory and optional cryptographic keys specified in FIPS 201 as well as the supporting infrastructure specified in FIPS 201 and the related Special Publications 800-73, Interfaces for Personal Identity Verification [SP800-73], and SP 800-76, Biometric Data Specification for Personal Identity Verification [SP800-76], that rely on cryptographic functions.
NIST	Guidelines	SP 800-85 A	This document's revisions include the additional tests necessary to test some of the optional features added to the PIV Data Model and Card Interface as well as the PIV Middleware through specifications SP 800-73 Parts 1, 2 and 3.
NIST	Guidelines	SP 800-85 B	This test guidance document specifies the derived test requirements, detailed test assertions, and conformance tests for testing the data elements of the PIV system as per specifications laid out in FIPS201, SP80073, SP80076, and SP80078.

GROUP	TYPE	NAME	DESCRIPTION
NIST	Guidelines	SP 800-96	The purpose of this document is to present recommendations for Personal Identity Verification (PIV) card readers in the area of performance and communications characteristics to foster interoperability. This document is not intended to re-state or contradict requirements specifically identified in Federal Information Processing Standard 201 (FIPS 201) or its associated documents. It is intended to augment existing standards to enable agencies to achieve the interoperability goal of HSPD-12. The document provides requirements that facilitate interoperability between any card and any reader. Specifically, the recommendations are for end-point cards and readers designed to read end-point cards.
NIST	Guidelines	SP 800-116	The purpose of this document is to describe a strategy allowing agencies to PIV-enable their PACS, and migrate to government-wide interoperability. Specifically, the document recommends a risk-based approach for selecting appropriate PIV authentication mechanisms to manage physical access to Federal Government facilities and assets.
NIST	Federal Standards	FIPS 140	This publication provides a standard that will be used by Federal organizations when these organizations specify that cryptographic-based security systems are to be used to provide protection for sensitive or valuable data. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. This standard specifies the security requirements that will be satisfied by a cryptographic module. The standard provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.
NIST	Federal Standards	FIPS 180	This Standard specifies a Secure Hash Algorithm, SHA-1, for computing a condensed representation of a message or a data file. When a message of any length < 264 bits is input, the SHA-1 produces a 160-bit output called a message digest. The message digest can then be input to the Digital Signature Algorithm (DSA) which generates or verifies the signature for the message. Signing the message digest rather than the message often improves the efficiency of the process because the message digest is usually much smaller in size than the message. The same hash algorithm must be used by the verifier of a digital signature as was used by the creator of the digital signature.
NIST	Federal Standards	FIPS 186	This Standard specifies a suite of algorithms that can be used to generate a digital signature. Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature in proving to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation, since the signatory cannot repudiate the signature at a later time.

GROUP	TYPE	NAME	DESCRIPTION
NIST	Federal Standards	FIPS 201-1	This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems. The standard contains two major sections. Part one describes the minimum requirements for a Federal personal identity verification system that meets the control and security objectives of HSPD-12, including personal identity proofing, registration, and issuance. Part two provides detailed specifications that will support technical interoperability among PIV systems of Federal departments and agencies. It describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card. The physical card characteristics, storage media, and data elements that make up identity credentials are specified in this standard.
Federal CIO Council	Guidance	Personal Identity Verification Interoperability for Non-Federal Issuers	This document advocates a set of minimum requirements for non-federally issued identity cards that can be trusted by the Federal government, and details solutions to the four barriers to interoperability that currently preclude Federal government trust of non-federally issued identity cards. Credentials issued according to PIV-interoperable specifications meet the minimum vetting requirements at E-authentication level 4 as indicated in NIST SP 800-63. PIV-interoperable credentials are not intended for individuals to whom HSPD-12 applies per OMB M-05-24.
GSA	Guidance	E-Authentication Federation Governance	This document improves the internal management of the Federal Government by defining governance structure, Federation change management, waivers, dispute resolution, and business standards.
GSA	Guidance	E-Authentication Federation Operational Standards	This document defines operational standards for Federation Members. The standards defined herein leverage both Federally-mandated standards and commercial best practices and ensure that the best interests of the Federation, specifically the Integrity of the operating environment are maintained. This document is intended to improve the internal management of the Federal Government.
GSA	Guidance	E-Authentication Federation Technical Approach	This document sets the technical direction and approach for the ASC. It describes the architectural framework under which the PMO implements technologies, products and technical standards to meet its program objectives. In addition, it provides a methodology for graceful adoption of new identity schemes as they emerge.
GSA	Guidance	E-Authentication Federation Architecture Interface Specification	This interface specification provides guidance on how to use SAML 2.0 SSO Profile using HTTP POST specifically for Federation purposes.
GSA	Guidance	U.S. E-Authentication Identity Federation Approved Product List (APL)	This document contains a list of products listed herein have demonstrated basic interoperability in the E-Authentication Interoperability Lab using the E-Authentication Security Assertion Markup Language (SAML) 1.0 and 2.0 Interface Specification in a federated environment.

GROUP	TYPE	NAME	DESCRIPTION
GSA	Guidance	E-Authentication Certificate Credential Assessment Profile	This profile specifies the criteria for certificate-based Credential Services (CSs) that authenticate public key certificates. It is based upon guidance specified in National Institute of Standards and Technology (NIST) Special Publication 800-63, version 1.0.1
FPKIA	Guidance	Bridge-Enabling Web Servers	This document discusses technical steps necessary to enable a web server to accept PKI based user credentials and validate them through a certificate bridge (e.g., the FBCA).
FPKIA	Guidance	Functional Requirements for Path Validation Systems	This document specifies requirements for PKI clients used in the Federal PKI. Requirements are specified for path validation, path discovery, and auditing. This document considers two basic scenarios for implementing these requirements: PKI client functionality may be performed locally or delegated entirely to a trusted server. Supplemental requirements are specified for clients and servers for the special case of delegated PKI processing.
FIPS 201 Evaluation Program	Guidance	Product/Services Category List	This document contains a FIPS-201 products list, and a description of each
FIPS 201 Evaluation Program	Guidance	Card to Reader Interoperability Requirement Guideline	The purpose of this document is to define and validate a suite of performance, interoperability and security requirements for PIV Card and Reader interface associated with a Personal Identity Verification (PIV) System consistent with Federal Information Processing Standards (FIPS) Publication 201 and its associated documents. Section two provides requirements that facilitate interoperability between any card and any reader (physical or logical operating environment). Performance-based requirements that enable rapid electronic authentication are listed in section three and requirements pertaining to security in a moderate risk environment are listed in section four.
FIPS 201 Evaluation Program	Guidance	Configuration Management Plan	The purpose of this document is to provide a CM Plan that illustrates the methodology that will be used for project deliverable management, vendor product/service equipment management, and Lab and testing documentation management. This CM Plan will allow the Project Team, Lab, and GSA to proceed with deliverable and documentation development and updates as needed.
FIPS 201 Evaluation Program	Guidance	Test Procedures - Card Printer Station	This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the Card Printer Station (henceforth referred to as the Product) against the subset of applicable requirements that need to be tested for this category.
FIPS 201 Evaluation Program	Guidance	Test Procedures - Electromagnetically Opaque Sleeve	This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the Electromagnetically Opaque Sleeve (henceforth referred to as the Product) against the subset of applicable requirements that need to be electronically tested for this category.
FIPS 201 Evaluation Program	Guidance	Test Procedures - Electronic Personalization	This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the Electronic Personalization Product or Service against the subset of applicable requirements that need to be electronically tested for this category.
FIPS 201 Evaluation Program	Guidance	Test Procedures - Facial Image Capturing Camera	This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the Facial Image Capturing Camera (henceforth referred to as the Product) against the subset of applicable requirements that need to be electronically tested for this category.

GROUP	TYPE	NAME	DESCRIPTION
FIPS 201 Evaluation Program	Guidance	Test Procedures - Facial Image Capturing Middleware	This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the Facial Image Capturing Middleware by testing the INCITS 385 Facial Image profile against the subset of applicable requirements that need to be electronically tested for this category.
FIPS 201 Evaluation Program	Guidance	Test Procedures - Graphical Personalization	This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the Graphical Personalization Service Provider (henceforth referred to as the Service) against the subset of applicable requirements that need to be tested for this category.
FIPS 201 Evaluation Program	Guidance	Test Procedures - PIV Card	This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the PIV Card (henceforth referred to as the Product) against the subset of applicable requirements that need to be electronically tested for this category.
FIPS 201 Evaluation Program	Guidance	Test Procedures - PIV Card Reader - Authentication Key	This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the Authentication Key Reader (henceforth referred to as the Product) against the subset of applicable requirements that need to be electronically tested for this category.
FIPS 201 Evaluation Program	Guidance	Test Procedures - PIV Card Reader - Biometric	This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the Biometric Reader (henceforth referred to as the Product) against the subset of applicable requirements that need to be electronically tested for this category.
FIPS 201 Evaluation Program	Guidance	Test Procedures - PIV Card Reader - CHUID Authentication (Contact)	This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the CHUID Authentication Reader (Contact) (henceforth referred to as the Product) against the subset of applicable requirements that need to be electronically tested for this category.
FIPS 201 Evaluation Program	Guidance	Test Procedures - PIV Card Reader - CHUID Authentication (Contactless)	This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the CHUID Authentication Reader (Contactless) (henceforth referred to as the Product) against the subset of applicable requirements that need to be electronically tested for this category.
FIPS 201 Evaluation Program	Guidance	Test Procedures - PIV Card Reader - CHUID (Contact)	This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the CHUID Reader (Contact) (henceforth referred to as the Product) against the subset of applicable requirements that need to be electronically tested for this category.
FIPS 201 Evaluation Program	Guidance	Test Procedures - PIV Card Reader - CHUID (Contactless)	This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the CHUID Reader (Contactless) (henceforth referred to as the Product) against the subset of applicable requirements that need to be electronically tested for this category.
FIPS 201 Evaluation Program	Guidance	Test Procedures - PIV Card Reader - Transparent	This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the Transparent Reader (henceforth referred to as the Product) against the subset of applicable requirements that need to be electronically tested for this category.
FIPS 201 Evaluation Program	Guidance	Test Procedures - Template Generator	This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the Template Generator (henceforth referred to as the Product) against the subset of applicable requirements that need to be electronically tested for this category.

GROUP	TYPE	NAME	DESCRIPTION
N/A	Standard	Security Assertion Markup Language (SAML)	Security Assertion Markup Language (SAML) 2.0 is an industry standard for web SSO and web services authentication, attribute exchange, and authorization. SAML-based federation is the basis for Level 1 and Level 2 authentication under the E-Authentication framework.
N/A	Standard	Extensible Markup Language (XML)	Extensible Markup Language, abbreviated XML, describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them. XML is an application profile or restricted form of SGML, the Standard Generalized Markup Language [ISO 8879]. By construction, XML documents are conforming SGML documents. XML documents are made up of storage units called entities, which contain either parsed or unparsed data. Parsed data is made up of characters, some of which form character data, and some of which form markup. Markup encodes a description of the document's storage layout and logical structure. XML provides a mechanism to impose constraints on the storage layout and logical structure.
N/A	Standard	Lightweight Directory Access Protocol (LDAP)	The Lightweight Directory Access Protocol (LDAP) is an Internet protocol for accessing distributed directory services that act in accordance with X.500 data and service models.
N/A	Standard	Simple Object Access Protocol (SOAP)	SOAP is a lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. It uses XML technologies to define an extensible messaging framework providing a message construct that can be exchanged over a variety of underlying protocols. The framework has been designed to be independent of any particular programming model and other implementation specific semantics.
N/A	Standard	Hypertext Transfer Protocol Secure (HTTPS)	Combines Hypertext Transfer Protocol and a cryptographic protocol
NIST	Standard	Advanced Encryption Standard (AES)	The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.
N/A	Standard	Online Certificate Status Protocol (OCSP)	The Online Certificate Status Protocol (OCSP) enables applications to determine the (revocation) state of an identified certificate. OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and may also be used to obtain additional status information. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate in question until the responder provides a response.
N/A	Standard	Extensible Access Control Markup Language (XACML)	XACML was chartered "to define a core schema and corresponding namespace for the expression of authorization policies in XML against objects that are themselves identified in XML.

GROUP	TYPE	NAME	DESCRIPTION
N/A	Standard	Simple Mail Transfer Protocol (SMTP)	The objective of Simple Mail Transfer Protocol (SMTP) is to transfer mail reliably and efficiently. SMTP is independent of the particular transmission subsystem and requires only a reliable ordered data stream channel.
N/A	Standard	Secure Socket Layer (SSL)	SSL is a security protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
NIST/NSA	Standard	Secure Hash Algorithms (SHA)	The Secure Hash Algorithm (SHA), developed by NIST, along with the NSA, for use with the Digital Signature Standard (DSS) is specified within the Secure Hash Standard (SHS) [National Institute of Standards and Technology (NIST). FIPS Publication 180: Secure Hash Standard (SHS). May 1993.].
ISO	Standard	ISO/IEC 7810 (card physical structure)	ISO/IEC 7810:2003 is one of a series of standards describing the characteristics of identification cards. It is the purpose of ISO/IEC 7810:2003 to provide criteria to which cards shall perform and to specify the requirements for such cards used for international interchange. It takes into consideration both human and machine aspects and states minimum requirements.
ISO	Standard	ISO/IEC 18033-3:2005	ISO/IEC 18033-3:2005 specifies block ciphers. A block cipher is a symmetric encipherment system with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext.
NIST	Standard	Elliptic Curve Digital Signature Algorithm (ECDSA)	The ECDSA ds algorithm is a FIPS approved cryptographic algorithm for digital signature generation and verification. ECDSA is the elliptic curve analogue of the DSA. ECDSA is described in ANSI X9.62.

This page is intentionally left blank.

Appendix H Acknowledgements

This 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. Part A comprises a segment architecture for ICAM that is provided to agencies for planning and considerations. Part B comprises implementation guidance to provide agencies with information and tools to realizing the goals of ICAM. The ICAMSC wishes to thank their colleagues who reviewed drafts of this document and contributed to its development.

The ICAMSC extends special thanks to the following individuals who comprise the Core Architecture Team:

- 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 ICAMSC would also like to acknowledge and appreciate the support and collaboration of the following members of the Roadmap Development Team, who also helped develop and review drafts of this document:

- 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
- 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

We also would like to express appreciation to the many additional agency personnel and support staff and the members of the Interagency Security Committee (ISC) who reviewed and provided comments to drafts of this document.

This page is intentionally left blank.