



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

**Version 2.0**

**December 2, 2011**

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



This page is intentionally left blank.

## Revision History

Document Version	Document Date	Revision Details
<b>Version 1.0</b>	November 10, 2009	<ul style="list-style-type: none"><li>• Initial publication of the document, including:<ul style="list-style-type: none"><li>◦ Chapter 1: Introduction</li><li>◦ Chapter 2: Overview of ICAM</li></ul></li><li>• Part A: ICAM Segment Architecture<ul style="list-style-type: none"><li>◦ Chapter 3: ICAM Segment Architecture</li><li>◦ Chapter 4: ICAM Use Cases</li><li>◦ Chapter 5: Transition Roadmap and Milestones</li></ul></li></ul>
<b>Version 2.0</b>	December 2, 2011	<ul style="list-style-type: none"><li>• Revised to include new Part B: Implementation Guidance:<ul style="list-style-type: none"><li>◦ Chapter 6: ICAM Implementation Planning</li><li>◦ Chapter 7: Initiative 5: Streamline Collection and Sharing of Digital Identity Data</li><li>◦ Chapter 8: Initiative 6: Fully Leverage PIV and PIV-I Credentials</li><li>◦ Chapter 9: Access Control Convergence</li><li>◦ Chapter 10: Initiative 7: Modernize PACS Infrastructure</li><li>◦ Chapter 11: Initiative 8: Modernize LACS Infrastructure</li><li>◦ Chapter 12: Initiative 9: Implement Federated Identity Capability</li></ul></li><li>• Inclusion of Glossary appendix.</li><li>• Minor revisions to existing Part A chapters to include:<ul style="list-style-type: none"><li>◦ Document overview updated to reflect additional chapters.</li><li>◦ Editorial and formatting corrections.</li><li>◦ Terminology updates to maintain consistency between Parts A and B.</li><li>◦ Updates to content related to the Federal Public Key Infrastructure to reflect infrastructure upgrades since original publication.</li></ul></li></ul>

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<sup>1</sup> cites the development of the federal ICAM segment architecture and recognizes the importance of the effort in promoting federation and interoperability. It states 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.<sup>||</sup> OMB has further recognized the importance of the ICAM segment

---

<sup>1</sup> [Fiscal Year Budget](#), The Office and Management and Budget (OMB).

architecture to successfully continuing implementation of HSPD-12 through the release of M-11-11,<sup>2</sup> which requires that agencies align with the architecture and guidance provided in the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance.

## 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<sup>3</sup> 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

---

<sup>2</sup> [M-11-11](#), Continued Implementation of Homeland Security Presidential Directive (HSPD) -12-Policy for a Common Identification Standard for Federal Employees and Contractors, OMB, February 3, 2011. [M-11-11]

<sup>3</sup> 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 [SP 800-63](#), E-authentication Guidance, Version 1.0.2, NIST, April 2006. [SP 800-63] PIV-interoperable specifications do not apply to individuals for whom HSPD-12 policy is applicable per [M-05-24](#), Implementation for Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employees and Contractors, OMB, August 5, 2005. [M-05-24] (i.e., federal employees and contractors with long-term access to federal facilities and information systems).

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 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

<b>Revision History</b> .....	i
<b>Executive Summary</b> .....	iii
<b>Table of Contents</b> .....	vii
<b>List of Figures</b> .....	xiii
<b>1. Introduction</b> .....	1
1.1. Background .....	1
1.2. Purpose .....	2
1.3. Scope .....	3
1.4. Document Overview .....	4
<b>2. Overview of Identity, Credential, and Access Management</b> .....	7
2.1. ICAM in the Federal Government.....	7
2.1.1. <i>Identity Management</i> .....	9
2.1.2. <i>Credential Management</i> .....	10
2.1.3. <i>Access Management</i> .....	12
2.1.4. <i>ICAM Intersection</i> .....	13
2.2. ICAM Goals and Objectives .....	14
2.2.1. <i>Goal 1: Comply with Federal Laws, Regulations, Standards, and Governance Relevant to ICAM</i> .....	14
2.2.2. <i>Goal 2: Facilitate E-Government by Streamlining Access to Services</i> .....	15
2.2.3. <i>Goal 3: Improve Security Posture across the Federal Enterprise</i> .....	16
2.2.4. <i>Goal 4: Enable Trust and Interoperability</i> .....	17
2.2.5. <i>Goal 5: Reduce Costs and Increase Efficiency Associated with ICAM</i> .....	18
2.3. ICAM Governance .....	19
2.3.1. <i>Governing Authorities</i> .....	19
2.3.2. <i>Federal Policies and Key Initiatives Impacting ICAM Implementation</i> .....	20
<b>PART A: ICAM Segment Architecture</b> .....	23
<b>3. ICAM Segment Architecture</b> .....	25
3.1. Developing the ICAM Segment .....	25
3.2. ICAM Architectural Layers .....	26
3.2.1. <i>Performance Architecture</i> .....	27
3.2.2. <i>Business Architecture</i> .....	28
3.2.3. <i>Data Architecture</i> .....	31
3.2.4. <i>Service Architecture</i> .....	33
3.2.5. <i>Technical Architecture</i> .....	37
<b>4. ICAM Use Cases</b> .....	47
4.1. Create and Maintain Digital Identity Record for Internal User.....	49
4.1.1. <i>As-is Analysis</i> .....	49
4.1.2. <i>Target Analysis</i> .....	52
4.1.3. <i>Gaps</i> .....	56
4.2. Create and Maintain Digital Identity Record for External User .....	58
4.2.1. <i>As-is Analysis</i> .....	58
4.2.2. <i>Target Analysis</i> .....	60
4.2.3. <i>Gaps</i> .....	63
4.3. Perform Background Investigation for Federal Applicant.....	64
4.3.1. <i>As-is Analysis</i> .....	65
4.3.2. <i>Target Analysis</i> .....	68
4.3.3. <i>Gaps</i> .....	71
4.4. Create, Issue, and Maintain PIV Card .....	73

4.4.1. <i>As-is Analysis</i> .....	73
4.4.2. <i>Target Analysis</i> .....	80
4.4.3. <i>Gaps</i> .....	84
4.5. Create, Issue, and Maintain PKI Credential.....	86
4.5.1. <i>As-is Analysis</i> .....	86
4.5.2. <i>Target Analysis</i> .....	91
4.5.3. <i>Gaps</i> .....	92
4.6. Create, Issue, and Maintain Password Token .....	93
4.6.1. <i>As-is Analysis</i> .....	93
4.6.2. <i>Target Analysis</i> .....	96
4.6.3. <i>Gaps</i> .....	97
4.7. Provision and De-provision User Account for an Application.....	98
4.7.1. <i>As-is Analysis</i> .....	98
4.7.2. <i>Target Analysis</i> .....	100
4.7.3. <i>Gaps</i> .....	103
4.8. Grant Physical Access to Employee or Contractor.....	105
4.8.1. <i>As-is Analysis</i> .....	105
4.8.2. <i>Target Analysis</i> .....	107
4.8.3. <i>Gaps</i> .....	111
4.9. Grant Visitor or Local Access to Federally-Controlled Facility or Site.....	113
4.9.1. <i>As-is Analysis</i> .....	113
4.9.2. <i>Target Analysis</i> .....	116
4.9.3. <i>Gaps</i> .....	121
4.10. Grant Logical Access.....	122
4.10.1. <i>As-is Analysis</i> .....	122
4.10.2. <i>Target Analysis</i> .....	124
4.10.3. <i>Gaps</i> .....	128
4.11. Secure Document or Communication with PKI.....	130
4.11.1. <i>As-is Analysis</i> .....	130
4.11.2. <i>Target Analysis</i> .....	130
4.11.3. <i>Gaps</i> .....	133
4.12. Application of the ICAM Use Cases.....	134
4.12.1. <i>IEE: User Management</i> .....	134
4.12.2. <i>G2G: Emergency Responders</i> .....	136
4.12.3. <i>G2B: Medical Information Exchange</i> .....	137
4.12.4. <i>G2C: Citizen Services</i> .....	139
<b>5. Transition Roadmap and Milestones .....</b>	<b>141</b>
5.1. Performance Improvement Recommendations .....	141
5.2. Initiatives and Milestones .....	143
5.2.1. <i>Government-wide Level Governance Initiatives</i> .....	144
5.2.2. <i>Agency-level Implementation Initiatives</i> .....	147
5.2.3. <i>Implementation Sequencing Plan</i> .....	151
5.3. Performance Metrics .....	152
<b>PART B: Implementation Guidance .....</b>	<b>159</b>
<b>How to Read and Use Part B: Implementation Guidance .....</b>	<b>161</b>
<b>6. ICAM Implementation Planning .....</b>	<b>165</b>
6.1. Program Organization and Management.....	165
6.1.1. <i>Program Governance</i> .....	165
6.1.2. <i>Program Stakeholders</i> .....	168
6.1.3. <i>Program Management</i> .....	176
6.1.4. <i>Performance Reporting</i> .....	184
6.2. Incorporating ICAM into Existing Agency Processes.....	185

6.2.1. <i>Management Accountability and Control</i> .....	185
6.2.2. <i>Capital Planning</i> .....	186
6.2.3. <i>Enterprise Architecture</i> .....	189
6.2.4. <i>IT Security and Risk Management</i> .....	189
6.3. Privacy Considerations.....	194
6.3.1. <i>Applying the FIPPs</i> .....	194
6.3.2. <i>Programmatic Support</i> .....	196
<b>7. Initiative 5: Streamline Collection and Sharing of Digital Identity Data</b> .....	<b>197</b>
7.1. Enterprise Digital Identity.....	197
7.1.1. <i>Core Identity Attributes</i> .....	198
7.1.2. <i>Authoritative Data Sources</i> .....	200
7.1.3. <i>Managing Digital Identity Records</i> .....	204
7.2. Digital Identity Process Integration .....	209
7.2.1. <i>Streamlining HR Processing</i> .....	211
7.2.2. <i>Streamlining Background Investigation Processing</i> .....	213
7.2.3. <i>Streamlining Contractor Processing</i> .....	215
7.3. Authoritative Digital Identity Attribute Exchange.....	217
7.3.1. <i>Elements of Attribute Exchange</i> .....	218
7.3.2. <i>AAES Architecture</i> .....	219
7.3.3. <i>AAES Solution Components</i> .....	220
7.3.4. <i>AAES Common Design Characteristics</i> .....	224
7.3.5. <i>AAES Implementation Considerations</i> .....	225
7.3.6. <i>Leveraging Existing Identity Attribute Exchange Capabilities</i> .....	227
<b>8. Initiative 6: Fully Leverage PIV and PIV-I Credentials</b> .....	<b>231</b>
8.1. Credential Overview .....	231
8.1.1. <i>PIV Card</i> .....	232
8.1.2. <i>PIV-I Card</i> .....	234
8.1.3. <i>PIV Infrastructure</i> .....	236
8.1.4. <i>Leveraging the PIV Infrastructure for Exceptional Scenarios</i> .....	238
8.2. Authentication.....	244
8.2.1. <i>PIV and PIV-I Authentication Mechanisms</i> .....	244
8.2.2. <i>PKI Credential Validation</i> .....	247
8.3. PIV Card Usage Challenges.....	251
8.3.1. <i>Card Issuance Lead Time</i> .....	252
8.3.2. <i>Printed Information</i> .....	255
8.3.3. <i>Administrator Access Privileges</i> .....	259
8.3.4. <i>Reasonable Accommodations</i> .....	260
8.3.5. <i>PIV Card Management</i> .....	262
8.4. Interagency Federation Using the PIV Card .....	267
8.4.1. <i>Common Scenarios for Interagency Federation</i> .....	268
8.4.2. <i>Implementation Considerations</i> .....	268
8.5. Value-added Applications.....	269
8.5.1. <i>Encryption</i> .....	269
8.5.2. <i>Digital Signatures</i> .....	270
<b>9. Access Control Convergence</b> .....	<b>273</b>
9.1. Resource Attribute Management.....	273
9.1.1. <i>Resource Discovery and Inventory</i> .....	273
9.1.2. <i>Collecting and Organizing Resource Information</i> .....	275
9.2. Privilege Management.....	277
9.2.1. <i>Entitlement Attributes</i> .....	278
9.2.2. <i>Privilege Management Lifecycle</i> .....	280
9.2.3. <i>Automated Provisioning Capability</i> .....	280
9.3. Authorization .....	285

9.3.1. <i>Access Control Models</i> .....	286
9.3.2. <i>Policy Management</i> .....	290
9.4. Auditing and Reporting .....	292
<b>10. Initiative 7: Modernize PACS Infrastructure .....</b>	<b>297</b>
10.1. Physical Access Implementation Planning .....	298
10.1.1. <i>Program Governance</i> .....	298
10.1.2. <i>Facility Risk Assessments</i> .....	303
10.1.3. <i>Program Funding</i> .....	305
10.1.4. <i>Schedule Planning</i> .....	307
10.2. Physical Access Architecture and Design .....	312
10.2.1. <i>Solution Architecture</i> .....	312
10.2.2. <i>Solution Components</i> .....	314
10.2.3. <i>Common Design Characteristics</i> .....	316
10.3. Physical Access Technical Implementation.....	318
10.3.1. <i>Automated Provisioning to PACS</i> .....	318
10.3.2. <i>Common Physical Access Scenarios</i> .....	321
10.4. Local Facility Access .....	327
10.5. Visitor Access.....	327
<b>11. Initiative 8: Modernize LACS Infrastructure .....</b>	<b>331</b>
11.1. Logical Access Implementation Planning .....	332
11.1.1. <i>Program Governance</i> .....	332
11.1.2. <i>Program Funding</i> .....	334
11.1.3. <i>Schedule Planning</i> .....	338
11.2. Logical Access Architecture and Design .....	346
11.2.1. <i>Solution Architecture</i> .....	346
11.2.2. <i>Solution Components</i> .....	351
11.2.3. <i>Common Design Characteristics</i> .....	354
11.3. Logical Access Technical Implementation.....	355
11.3.1. <i>System Configuration</i> .....	356
11.3.2. <i>LACS Enterprise Solution Integration</i> .....	358
11.3.3. <i>Common Logical Access Scenarios</i> .....	362
<b>12. Initiative 9: Implement Federated Identity Capability .....</b>	<b>365</b>
12.1. Federation Overview .....	365
12.1.1. <i>Why Federate?</i> .....	367
12.1.2. <i>Federation Trust Topologies</i> .....	368
12.2. Federal Trust Framework .....	369
12.2.1. <i>Federal PKI (FPKI)</i> .....	371
12.2.2. <i>Open Identity Initiative</i> .....	372
12.3. Provisioning Users External to the Federal Government.....	377
12.3.1. <i>Provisioning Scenarios</i> .....	378
12.3.2. <i>Provisioning Process for External Users</i> .....	381
12.3.3. <i>Provisioning Implementation Patterns</i> .....	385
12.3.4. <i>Considerations for Provisioning Non-Federal Users</i> .....	387
12.4. Federated Access Using Third-Party Credentials.....	389
12.4.1. <i>Determining Acceptable Credentials</i> .....	390
12.4.2. <i>Identity Providers</i> .....	392
12.4.3. <i>Federation Governance</i> .....	394
12.4.4. <i>Federated Access Implementation Considerations</i> .....	395
<b>Appendix A        Acronym List .....</b>	<b>399</b>
<b>Appendix B        Glossary.....</b>	<b>405</b>
<b>Appendix C        Policy List .....</b>	<b>419</b>

<b>Appendix D</b>	<b>Risk Registry .....</b>	<b>425</b>
<b>Appendix E</b>	<b>ICAM Segment Architecture Development Approach Details .....</b>	<b>433</b>
<b>Appendix F</b>	<b>ICAM Data Standards and Guidance .....</b>	<b>437</b>
<b>Appendix G</b>	<b>ICAM Technical Standards and Guidance .....</b>	<b>441</b>
<b>Appendix H</b>	<b>Decision Trees for Component Migration Decisions .....</b>	<b>449</b>
<b>Appendix I</b>	<b>Existing Identity Exchange Models .....</b>	<b>453</b>
<b>Acknowledgements .....</b>		<b>459</b>

This page is intentionally left blank.

## List of Figures

Figure 1: ICAM Conceptual Diagram .....	8
Figure 2: FSAM Asset Mapping to FICAM Roadmap Chapters .....	26
Figure 3: Segment Architecture Layers .....	27
Figure 4: Business Value Chain Summary .....	29
Figure 5: ICAM Use Case Overview .....	30
Figure 6: Cross Government Repositories and Systems .....	32
Figure 7: Services Framework .....	34
Figure 8: Agency As-Is Conceptual Diagram .....	39
Figure 9: Federal PKI Architecture .....	40
Figure 10: HSPD-12 Conceptual Diagram .....	41
Figure 11: Agency Target Conceptual Diagram .....	42
Figure 12: Federal Enterprise Target Conceptual Diagram .....	43
Figure 13: Federal Enterprise Target Conceptual Diagram: Cross-Agency Access .....	44
Figure 14: Federal Enterprise Target Conceptual Diagram, Citizen Access .....	45
Figure 15: Use Case Functional Overview .....	47
Figure 16: Identity Record Creation by System and User Type .....	51
Figure 17: Use Case 1 As-is Architecture Details .....	52
Figure 18: Use Case 1 Target Process Diagram .....	55
Figure 19: Use Case 1 Target Architecture Details .....	56
Figure 20: Use Case 2 As-is Architecture Details .....	60
Figure 21: Use Case 2 Target Process Diagram .....	62
Figure 22: Use Case 2 Target Architecture Details .....	63
Figure 23: Use Case 3 As-is Architecture Details .....	68
Figure 24: Use Case 3 Target Process Diagram .....	70
Figure 25: Use Case 3 Target Architecture Details .....	71
Figure 26: Use Case 4 As-is Architecture Details .....	79
Figure 27: Use Case 4 Target Process Diagram .....	82
Figure 28: Use Case 4 Target Architecture Details .....	84
Figure 29: Mapping of PKI Credential and Identity Assurance Levels .....	86
Figure 30: Use Case 5 As-is Architecture Details .....	90
Figure 31: Use Case 5 Target Process Diagram .....	92
Figure 32: Use Case 6 As-is Architecture Details .....	95
Figure 33: Use Case 7 As-is Architecture Details .....	100
Figure 34: Use Case 7 Target Process Diagram .....	102
Figure 35: Use Case 7 Target Architecture Details .....	103
Figure 36: Use Case 8 As-is Architecture Details .....	107
Figure 37: PIV Authentication Mechanisms .....	108
Figure 38: Use Case 8 Target Process Diagram .....	110
Figure 39: Use Case 8 Target Architectural Analysis Details .....	111
Figure 40: Use Case 9 As-is Architectural Analysis Details .....	116
Figure 41: Use Case 9 Target Process Diagram .....	119
Figure 42: Use Case 9 Target Architectural Analysis Details .....	121
Figure 43: Use Case 10 As-is Architecture Details .....	124
Figure 44: Use Case 10 Target Process Diagram .....	127
Figure 45: Use Case 10 Target Architecture Details .....	128
Figure 46: Use Case 11 Target Process Diagram (Encryption) .....	132

Figure 47: Use Case 11 Target Process Diagram (Digital Signature) .....	132
Figure 48: Use Case 11 As-is Architecture Details .....	133
Figure 49: ICAM Performance Improvement Recommendation Summary .....	143
Figure 50: Initiative 1 Transition Activity Summary.....	145
Figure 51: Initiative 2 Transition Activity Summary.....	146
Figure 52: Initiative 3 Transition Activity Summary.....	146
Figure 53: Initiative 4 Transition Activity Summary.....	147
Figure 54: Initiative 5 Transition Activity Summary.....	149
Figure 55: Initiative 6 Transition Activity Summary.....	149
Figure 56: Initiative 7 Transition Activity Summary.....	150
Figure 57: Initiative 8 Transition Activity Summary.....	151
Figure 58: Initiative 9 Transition Activity Summary.....	151
Figure 59: ICAM Performance Metrics (* indicates inclusion in the Data.gov data stream).....	157
Figure 60: Federal ICAM Initiative Stakeholders .....	173
Figure 61: Agency-level ICAM Stakeholders.....	175
Figure 62: Examples of ICAM Workstream Responsibilities .....	177
Figure 63: Sample ICAM PMO Structure .....	178
Figure 64: Sample ICAM Program Communications.....	179
Figure 65: Sample ICAM Program Risks and Mitigations.....	181
Figure 66: ICAM Considerations within the CPIC Process.....	187
Figure 67: OMB Budget Guidance .....	188
Figure 68: ICAM Cost Categories Summary .....	189
Figure 69: Summary of the Risk Management Framework .....	191
Figure 70: NIST SP 800-53 Control Families and Relation to ICAM .....	193
Figure 71: Applying the FIPPs to ICAM.....	195
Figure 72: Core Person Model Attributes .....	199
Figure 73: Common Characteristics of Authoritative Data Sources .....	201
Figure 74: Common Digital Identity Process Integration Steps .....	210
Figure 75: Common Protocols for Sharing Identity Data .....	218
Figure 76: AAES Reference Architecture.....	220
Figure 77: Alternative Approaches for Implementing an Authoritative Attribute Manager .....	223
Figure 78: Common AAES Design Characteristics .....	224
Figure 79: Comparison of Existing Identity Attribute Exchange Capabilities .....	229
Figure 80: PIV Card Standard Physical Elements.....	233
Figure 81: PIV Card Digital Certificates.....	234
Figure 82: Comparison of PIV and PIV-I .....	235
Figure 83: PIV Infrastructure Components .....	237
Figure 84: Credential Types and Characteristics .....	240
Figure 85: Summary of Identification and Authentication Requirements by Credential Type .....	243
Figure 86: PIV Card Authentication Mechanisms and Procedures Summary .....	246
Figure 87: Examples of PD-Val Technologies.....	249
Figure 88: Benefits and Limitations of Validation Models .....	249
Figure 89: Benefits and Limitations of CRLs and OCSPs .....	251
Figure 90: Resource Information Sources.....	275
Figure 91: Sample Resource Information Components .....	276
Figure 92: Privilege Management Lifecycle .....	280
Figure 93: Benefits of Employing Automating Provisioning Capabilities .....	282
Figure 94: Common Characteristics of an Automated Provisioning Capability.....	283

Figure 95: Common Access Control Models .....	289
Figure 96: Policy Management Lifecycle .....	292
Figure 97: Common Access Control Reports .....	294
Figure 98: Sample PACS Governance Efforts .....	302
Figure 99: Common Risk Management Steps .....	304
Figure 100: Common PACS Acquisition Considerations .....	306
Figure 101: Planning Phase Sample Activities .....	308
Figure 102: Requirements and Design Phase Sample Activities .....	309
Figure 103: Build Phase Sample Activities .....	310
Figure 104: Implement Phase Sample Activities .....	311
Figure 105: Operate and Maintain Phase Sample Activities .....	312
Figure 106: Physical Access Solution Architecture .....	313
Figure 107: Common PACS Design Characteristics .....	318
Figure 108: Comparison of Automated Provisioning Techniques .....	320
Figure 109: Benefits and Limitations of CHUID Authentication in PACS .....	322
Figure 110: Benefits and Limitation of CAK Authentication in PACS .....	323
Figure 111: Benefits and Limitations of PKI Authentication in PACS .....	324
Figure 112: Benefits and Limitations of Biometric Authentication in PACS .....	325
Figure 113: Common VMS Design Characteristics .....	330
Figure 114: Sample LACS Governance Efforts .....	334
Figure 115: Common LACS Funding Considerations .....	336
Figure 116: Planning Phase Sample Activities .....	339
Figure 117: Requirements and Design Phase Sample Activities .....	340
Figure 118: Build Phase Sample Activities .....	341
Figure 119: Implement Phase Sample Activities .....	342
Figure 120: Operate and Maintain Phase Sample Activities .....	343
Figure 121: Logical Access Solution Architecture .....	347
Figure 122: Benefits and Limitations of Enterprise Authentication and Authorization .....	348
Figure 123: Benefits and Limitations of Decentralized Authorization Approaches .....	349
Figure 124: Benefits and Limitations of Decentralized Authentication Approaches .....	350
Figure 125: Benefits and Limitations of Decentralized Authentication and Authorization Approaches .....	350
Figure 126: Common LACS Design Characteristics .....	355
Figure 127: LACS Solution Component Deployment Considerations .....	361
Figure 128: Overview of Federal Trust Framework Components .....	370
Figure 129: TFPAP Process Overview .....	373
Figure 130: TFPAP Privacy Principles .....	376
Figure 131: Overview of Identity Scheme Adoption Process Steps .....	377
Figure 132: Benefits and Limitations of Automatic Information Collection .....	382
Figure 133: Benefits and Limitations of Prompted Information Collection .....	383
Figure 134: Benefits and Limitations of Deferred Information Collection .....	384
Figure 135: Benefits and Limitations of Hybrid Information Collection Approaches .....	385
Figure 136: Overview of Provisioning Implementation Patterns .....	387
Figure 137: Common Steps for Determining Acceptable Third-Party Credentials .....	390
Figure 138: Adopted Schemes and E-Authentication Levels of Assurance .....	391
Figure 139: Levels of Architecture .....	433
Figure 140: FSAM Implementation Steps .....	435
Figure 141: Tailored FSAM Outputs for the Federal ICAM Segment .....	436
Figure 142: PACS Server Migration .....	450

Figure 143: PACS Control Panel Migration .....	451
Figure 144: PACS Reader Migration .....	452

## 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,<sup>4</sup> have highlighted that the Federal Government must do more to address these threats. The Government Accountability Office (GAO)<sup>5</sup> recently found that most agencies have not implemented the necessary security controls to prevent and detect unauthorized access to federal information technology (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, which discusses recommendations such as improving authentication strength for individuals and devices, increasing the use of privacy-enhancing technologies, and extending the availability of identity management capabilities. 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<sup>6</sup> 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,<sup>7</sup> 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

---

<sup>4</sup> [Cyberspace Policy Review](#), Assuring a Trusted and Resilient Information and Communications Infrastructure, Executive Office of the President, May 29, 2009.

<sup>5</sup> [GAO-09-701](#), Agencies Make Progress in Implementation of Requirements, but Significant Weaknesses Persist, Government Accountability Office, May 19, 2009.

<sup>6</sup> [GAO-05-49](#), Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices, Government Accountability Office, November 2004.

<sup>7</sup> [GAO-06-612](#), Guidance and Standards Are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts, Government Accountability Office, May 2006.

reliable ICAM capabilities across the entire Federal Government are a critical factor in the success of all government mission work. A common, standardized, trusted basis for digital identity and access management within the federal sector is needed to provide a consistent approach to deploying and managing appropriate identity assurance, credentialing, and access control services. The 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<sup>8</sup> 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<sup>9</sup> cites the development of the federal ICAM segment architecture and recognizes the importance of the effort in promoting federation and interoperability. It states 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.|| OMB has further recognized the importance of the ICAM segment architecture to successfully continuing implementation of HSPD-12 through the release of M-11-11,<sup>10</sup> which requires that agencies align with the architecture and guidance provided in the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance.

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

---

<sup>8</sup> [The Federal PKI program](#) is a core component of the Federal Trust Framework as a set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs. This program is managed by the [Federal PKI Management Authority \(FPKIMA\)](#). [FPKIMA]

<sup>9</sup> [Fiscal Year Budget](#), The Office and Management and Budget(OMB).

<sup>10</sup> [M-11-11](#), Continued Implementation of Homeland Security Presidential Directive (HSPD) -12-Policy for a Common Identification Standard for Federal Employees and Contractors, OMB, February 3, 2011. [M-11-11]

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 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 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.

The Roadmap addresses unclassified<sup>11</sup> 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 Personal Identity Verification (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.

---

<sup>11</sup> National security systems are not covered by this document, but unclassified systems within Defense and Intelligence agencies are.

- **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.
- **PART B: Implementation Guidance**
  - **Chapter 6: ICAM Implementation Planning.** Discusses planning considerations for ICAM programs and how an agency can align their ICAM program strategies to realize synergies and avoid common management pitfalls.
  - **Chapter 7: Initiative 5: Streamline Collection and Sharing of Digital Identity Data.** Discusses approaches for improving the lifecycle management of digital identity records, including processes for establishing, maintaining, and exchanging identity data in a secure manner.
  - **Chapter 8: Initiative 6: Fully Leverage PIV and PIV-I Credentials.** Discusses approaches for effectively using PIV and PIV-I credentials in agency operations. Offers guidance for addressing common implementation challenges.
  - **Chapter 9: Access Control Convergence.** Discusses how to apply various access control models to enforce policies for an agency’s resources related to user privileges. Describes the design and functionality of an automated provisioning capability.
  - **Chapter 10: Initiative 7: Modernize PACS Infrastructure.** Discusses the activities associated with planning, designing, and implementing a PACS that meets relevant policy and technology requirements.
  - **Chapter 11: Initiative 8: Modernize LACS Infrastructure.** Discusses the activities associated with planning, designing, and implementing a LACS that meets relevant policy and technology requirements.
  - **Chapter 12: Initiative 9: Implement Federated Identity Capability.** Discusses environments external to the Federal Government where an agency can leverage the government-wide federated identity framework to reduce redundancies in their ICAM programs.

This page is intentionally left blank.

## 2. Overview of Identity, Credential, and Access Management

This section provides an introduction to ICAM. The primary compliance drivers relative to ICAM have historically been the Electronic Authentication<sup>12</sup> (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 the 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 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.

---

<sup>12</sup> 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 Governmentwide Policy and Federal CIO Council as part of the ISIMC activities.

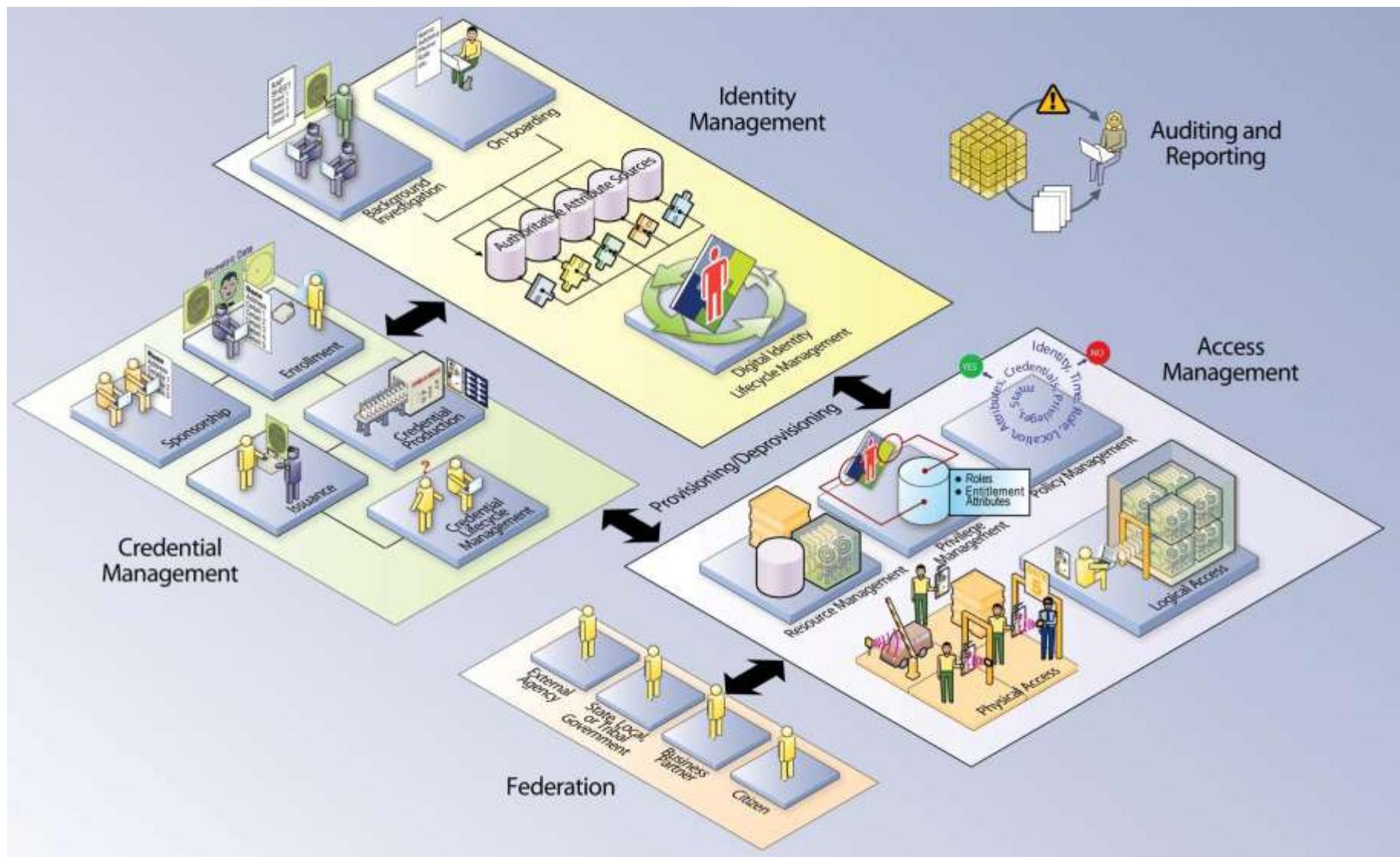


Figure 1: ICAM Conceptual Diagram

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**

Identity management is the combination of technical systems, policies, and processes that create, define, govern, and synchronize the ownership, utilization, and safeguarding of 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.<sup>13</sup> Identity management includes the processes for maintaining and protecting the identity data of an individual over its life cycle. 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. 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

---

<sup>13</sup> [Identity Management Task Force Report](#), National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management, 2008. [Identity Management Task Force Report]

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 single digital representation of themselves that 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 often 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 de-provisioned when access is no longer required. While the term —on-boarding<sup>14</sup> 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 life cycle 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 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),<sup>14</sup> a credential is, —an object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.<sup>15</sup> Credential management supports the life cycle of the credential itself. In the Federal Government, examples of

<sup>14</sup> [SP 800-63](#), Electronic Authentication Guideline, Version 1.0.2, NIST, April 2006. [SP 800-63]

<sup>15</sup> 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 U.S. Federal PKI Common Policy Framework](#), Version 3647 – 1.6, February 11, 209. [COMMON]

credentials 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 Publication 201 [FIPS 201], NIST SP 800-73,<sup>16</sup> 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.<sup>17</sup> 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 life cycle, which might include revocation, reissuance/replacement, re-enrollment, expiration, personal identification number (PIN) reset, suspension, or re-instatement.

A key distinction in the lifecycle management of credentials versus identities is that credentials expire. The attributes which form your digital identity may change or evolve over time, but your identity does not become invalid or terminated from a system perspective. 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.

---

<sup>16</sup> [SP 800-73, Interfaces for Personal Identity Verification –Part 1: End-Point PIV Card Application Namespace, Data Model and Representation, NIST, February 2010. \[SP 800-73\]](#)

<sup>17</sup> 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 or denied 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.<sup>18</sup> 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 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 requires access control. 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. These attributes represent features of an individual that can be used as the basis for determining access decisions to both physical and logical resources. 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<sup>19</sup> also supports making the decision to grant/deny access to individuals. Common factors include:

---

<sup>18</sup> [FIPS Publication 201](#), Personal Identity Verification (PIV) of Federal Employees and Contractors, Introduction, Pg. 1, March 2006. [FIPS 201]

<sup>19</sup>—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 (ROI) 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. This approach enables an Access Management initiative to promote security and trust and meet business needs while achieving the envisioned value.

#### **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 ROI 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 Officials (F/ERO) that support emergency preparedness and response; 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 [G2G], Government-to-Business [G2B], Government-to-Citizen [G2C], and Internal Effectiveness and Efficiency [IEE]) at all levels of assurance as defined in OMB M-04-04.<sup>20</sup>

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 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 G2G, G2B, and 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.

---

<sup>20</sup> [M-04-04](#), E-Authentication Guidance for Federal Agencies, OMB, December 16, 2003. [M-04-04]

### **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 (FISMA) and supporting NIST SP 800-53<sup>21</sup> and 800-37,<sup>22</sup> by promoting the use of strong identity solutions appropriate to the environment. ICAM further supports the policy and guidance established by the Interagency Security Committee (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<sup>23</sup> 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.

---

<sup>21</sup> [SP 800-53](#), Recommended Security Controls for Federal Information Systems and Organizations, NIST, August 2009. [SP 800-53]

<sup>22</sup> [SP 800-37](#), Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, NIST, February 2010. [SP 800-37]

<sup>23</sup> [SP 800-116](#), A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), NIST, November 2008. [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 Federal 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 General Services Administration (GSA) Office of Governmentwide Policy (OGP), and direct oversight from the Office of Management and Budget (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 Subcommittee (SPMSC), which coordinates with other standing cross agency efforts and advises on FISMA reporting tools and security policy;
- Security Acquisitions Subcommittee (SASC), which recommends Security Contract Language changes and reviews Supply Chain Activities; and
- Network and Infrastructure Security Subcommittee (NISC), 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 [NSS], OMB, and the Office of Science and Technology Policy [OSTP]), 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 (E.O.) 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 6.1.2.1 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 Appendix C 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 [SSN]).
- **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 OMB, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes.
- **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 identification (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 Federal 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 (GPEA).** 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 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 PII 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 primary 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.

Agencies are to 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. The ICAM segment architecture has been adopted as an approved segment within the FEA, which agencies are required to implement. Additionally, OMB has recognized the value of the ICAM segment architecture and has instructed agencies to ensure that their ICAM programs align with the government-wide segment architecture.<sup>24</sup>

#### 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<sup>25</sup> (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

---

<sup>24</sup> [M-11-11](#)

<sup>25</sup> [Federal Segment Architecture Methodology](#) (FSAM), Version 1.0, Executive Office of the President, December 12, 2008. [FSAM]

implemented separately. Additionally, as part of the capital planning process, each agency is to use the information provided by the ICAM segment architecture to make the appropriate budget requests for ICAM initiatives for all budget cycles going forward (as enforced 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 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
<b>Chapter 2: Overview of Identity, Credential, and Access Management</b>	<ul style="list-style-type: none"> <li>• Policy Map</li> <li>• Business Challenges Analysis</li> <li>• Business Drivers, Goals &amp; Objectives</li> </ul>
<b>Chapter 3: ICAM Segment Architecture</b>	<ul style="list-style-type: none"> <li>• Segment Architecture Purpose Statement</li> <li>• Business Value Chain Analysis</li> <li>• Inventory of Government-wide Data Sources &amp; Data Elements</li> <li>• As-Is System Interface Diagram</li> <li>• Target System Interface Diagram</li> <li>• Services Framework</li> </ul>
<b>Chapter 4: ICAM Use Cases</b>	<ul style="list-style-type: none"> <li>• As-is Use Cases</li> <li>• Target Use Cases</li> <li>• Target Information Flow Diagrams</li> </ul>
<b>Chapter 5: Transition Roadmap and Milestones</b>	<ul style="list-style-type: none"> <li>• Recommendation Implementation Overview</li> <li>• Implementation Sequencing Plan</li> <li>• Transition Plan Milestones</li> <li>• Performance Metrics</li> </ul>
<b>Chapter 6: ICAM Implementation Planning</b>	<ul style="list-style-type: none"> <li>• Stakeholder List</li> </ul>
<b>Appendix D: Risk Registry</b>	<ul style="list-style-type: none"> <li>• Risk Registry</li> </ul>

Figure 2: FSAM Asset Mapping to FICAM Roadmap 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 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.

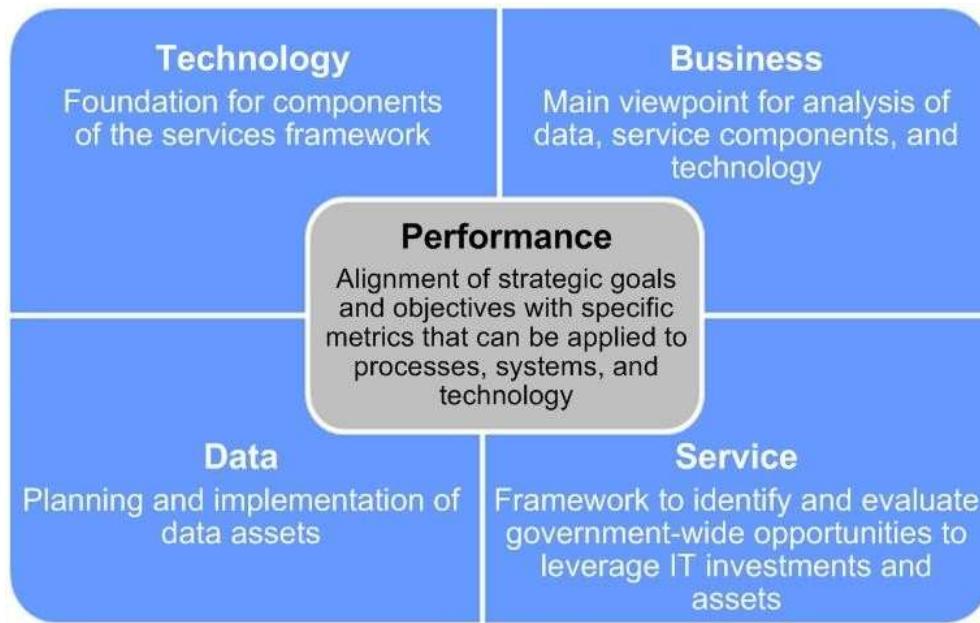


Figure 3: Segment Architecture Layers

The following subsections describe each layer in greater detail and present the 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.** Provides 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 (PIV-I) credential to access Federal Government resources, whereas a citizen may use an alternate third-party credential).

The following figure provides a summary of some of the common user populations within each E-Government sector and the respective credential types that support ICAM transactions.

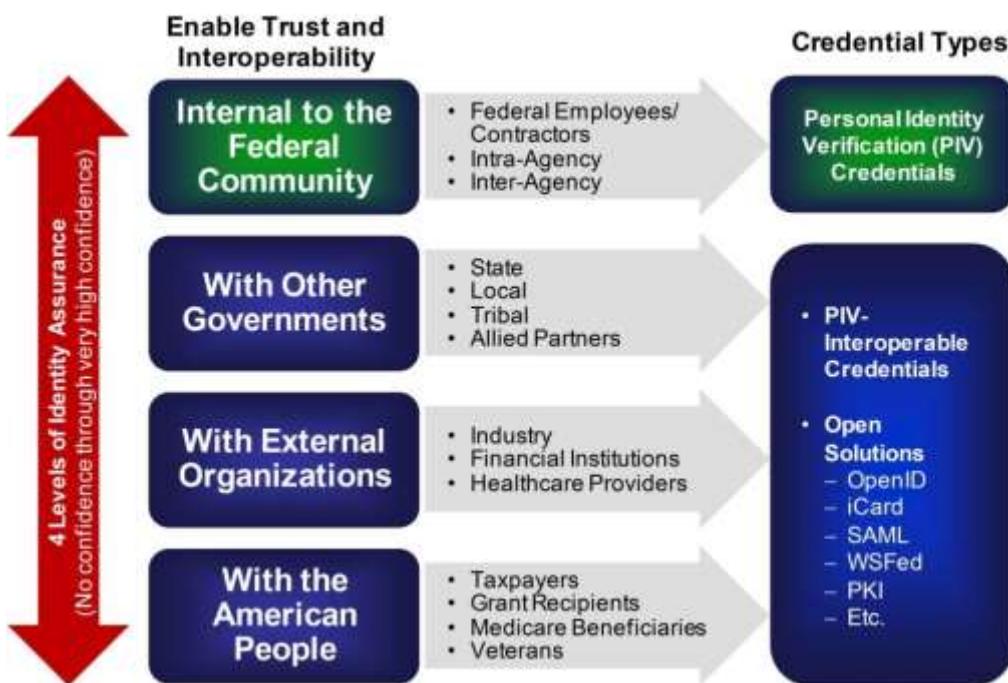


Figure 4: Business Value Chain Summary

### 3.2.2.2. Use Cases Overview

As the main component of the ICAM business architecture, the Roadmap Development Team (RDT) identified common use cases that capture the main 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 5 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 life cycle 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 life cycle in compliance with Federal PKI standards.
Create, issue, and maintain password token	✓	✓	✓	✓	Provides the high-level process steps for creating, issuing, and maintaining a password token over the credential life cycle.
Provision and de-provision user account for an application	✓	✓	✓	✓	Provides the high-level process steps for provisioning and de-provisioning 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 5: 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 enterprise architecture (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 6 includes an overview of the principal cross-government repositories or systems identified across the use cases.

Repository or System	Description	Data Types					E-Gov Alignment				
		Personal Info	Biometrics	Access Rules	Privileges	Suitability	Roles	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 (SSNs).	✓							✓	✓	✓
Central Verification System (CVS)	An Office of Personnel Management (OPM) 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.	✓			✓	✓		✓	✓	✓	✓
Federal/Emergency Response Official Repository (F/ERO)	The F/ERO repository is managed by Federal Emergency Management Agency (FEMA) in accordance with Public Law 110-53 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 F/ERO 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 6: 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 Appendix F ICAM Data Standards and Guidance

### 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
- International Organization for Standardization (ISO)/International Electrotechnical Commission (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 7 shows the resulting ICAM Services Framework.

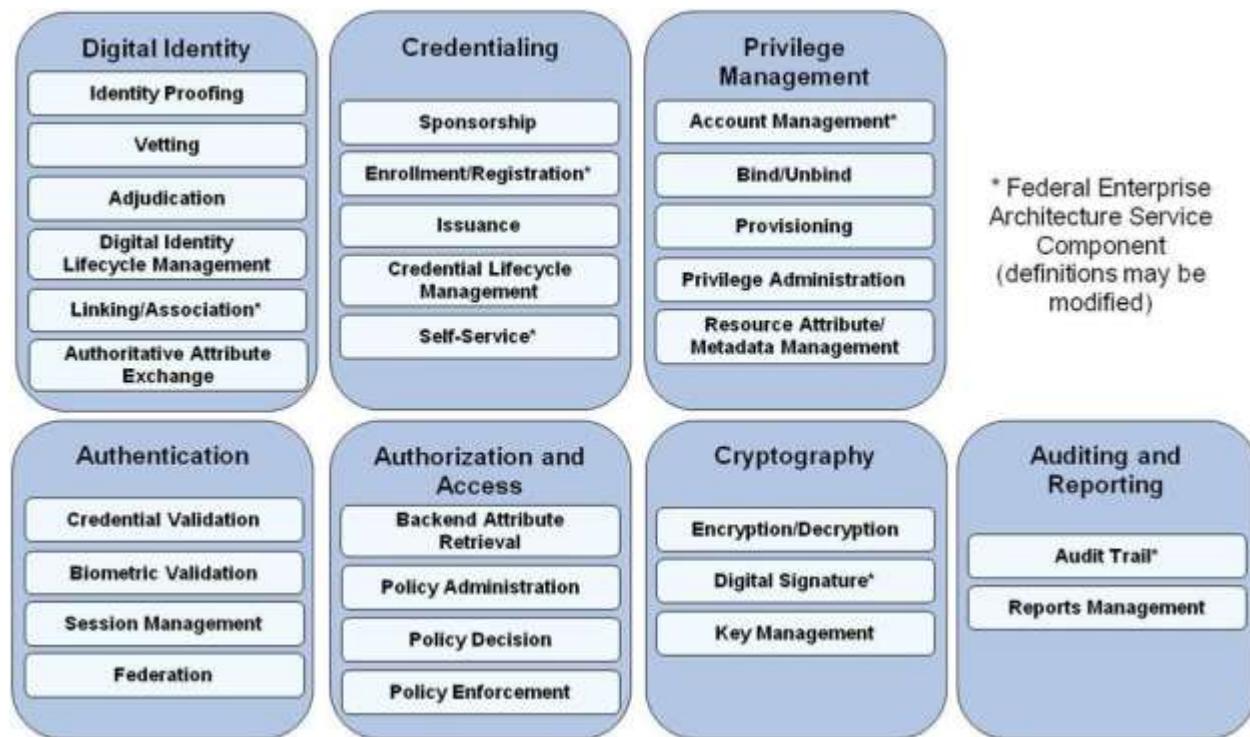


Figure 7: Services Framework

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 representation of identity in a digital environment. 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 life cycle.

Service Component	Description
Identity Proofing	Process that vets and verifies the information (e.g., identity history, credentials, documents) that is used to establish the identity of a system entity; initiates

Service Component	Description
	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 evaluating 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 and/or eligible for particular privileges.
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 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	Capability that performs discovery and mapping of attributes from authoritative source repositories and enables sharing of these attributes.

### **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 non-person entity (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	Process of maintaining a credential and associated support over the life cycle; common processes include renewal, reissuance, suspension, blocking and unblocking, revocation, etc. Life cycle support activities vary depending on the credential type, and may include a Self Service component.
Self-Service	Capability to 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** comprises the set of processes for establishing and maintaining the entitlement or privilege attributes that comprise an individual's access profile. These attributes are features of an individual that can be used as the basis for determining access decisions to both physical and logical resources. It governs the management of the data that constitutes the user's privileges and other attributes, including the storage, organization and access to information.

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.

Service Component	Description
Account Management	Processes of requesting, establishing, issuing, and closing user accounts; tracking users and their respective access authorizations; and managing these functions
Bind/Unbind	Process of building or removing a relationship between an entity's identity and further attribute information on the entity (e.g., properties, status, or credentials).
Provisioning	Capability of 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	Process that 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 (Secure Socket Layer)/TLS (Transport Layer Security), the validation of digital signatures, or other non-biometric and non-cryptographic mechanisms.
Biometric Validation	Capability 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	Capability that 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	Capability to support a trust relationship between discrete digital identity Providers 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	Capability that acquires additional information not found in the authenticated credential that is required by a relying party to make an access based decision.
Policy Administration	Process of creating, disseminating, modifying, managing, and maintaining hierarchical rule sets to control digital resource management, utilization, and protection in a standard policy exchange format.
Policy Enforcement	Capability that restricts access to specific systems or content in accordance with policy decisions that are made.
Policy Decision	Capability that 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	Capability of an asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection.
Key Management	Processes involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.

### **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	Capability to capture and maintain a chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result.
Reports Management	Capability to collect detailed information about system entities, usage activity, and identity audit events and presented it in a meaningful way.

## **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:

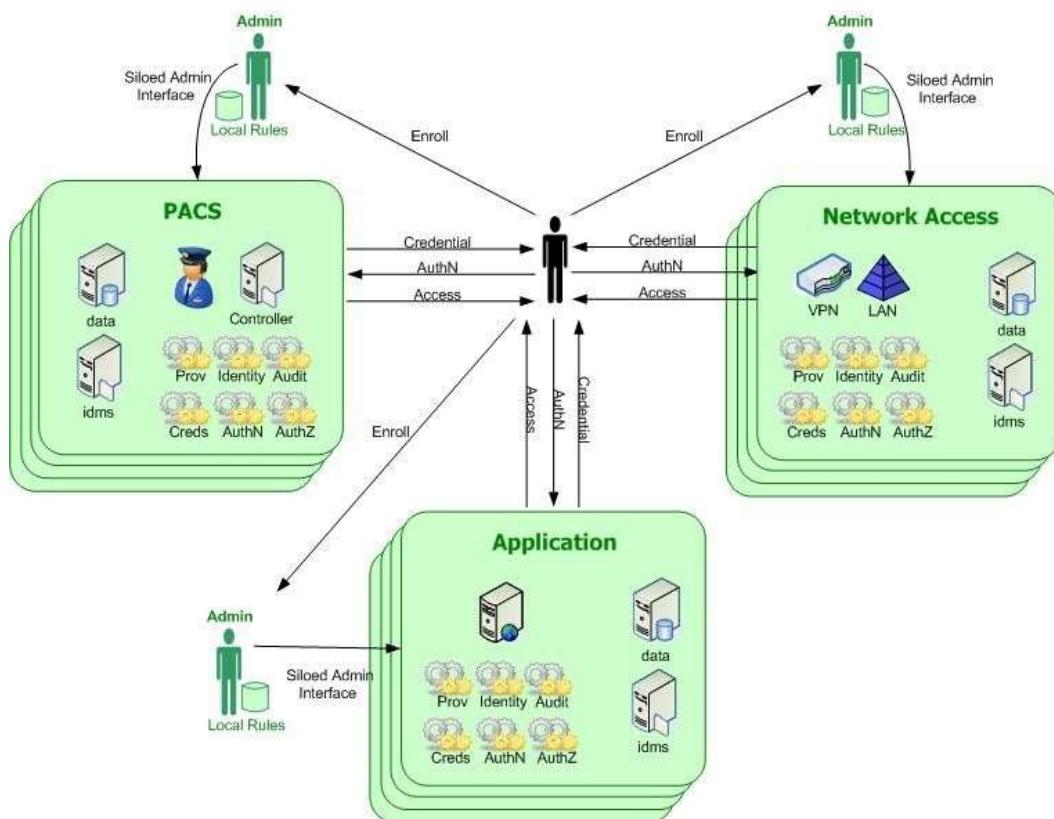
- As-is System Interface Diagrams. Provide a depiction of the as-is —conceptual solution architecture,|| which shows the existing systems and services in the as-is state and identifies the relationships between them. This component is provided in Section 3.2.5.1 below.
- Target System Interface Diagrams. 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 8: Agency As-Is Conceptual Diagram**

The figure above shows ICAM functions performed independently by Physical Access Control Systems (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-credentialled, identity proofed, and provisioned in each system across the federal enterprise.

Figure 9 and Figure 10 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 9 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 Certification Authority (FCPCA), represented by the light orange boxes in the diagram.

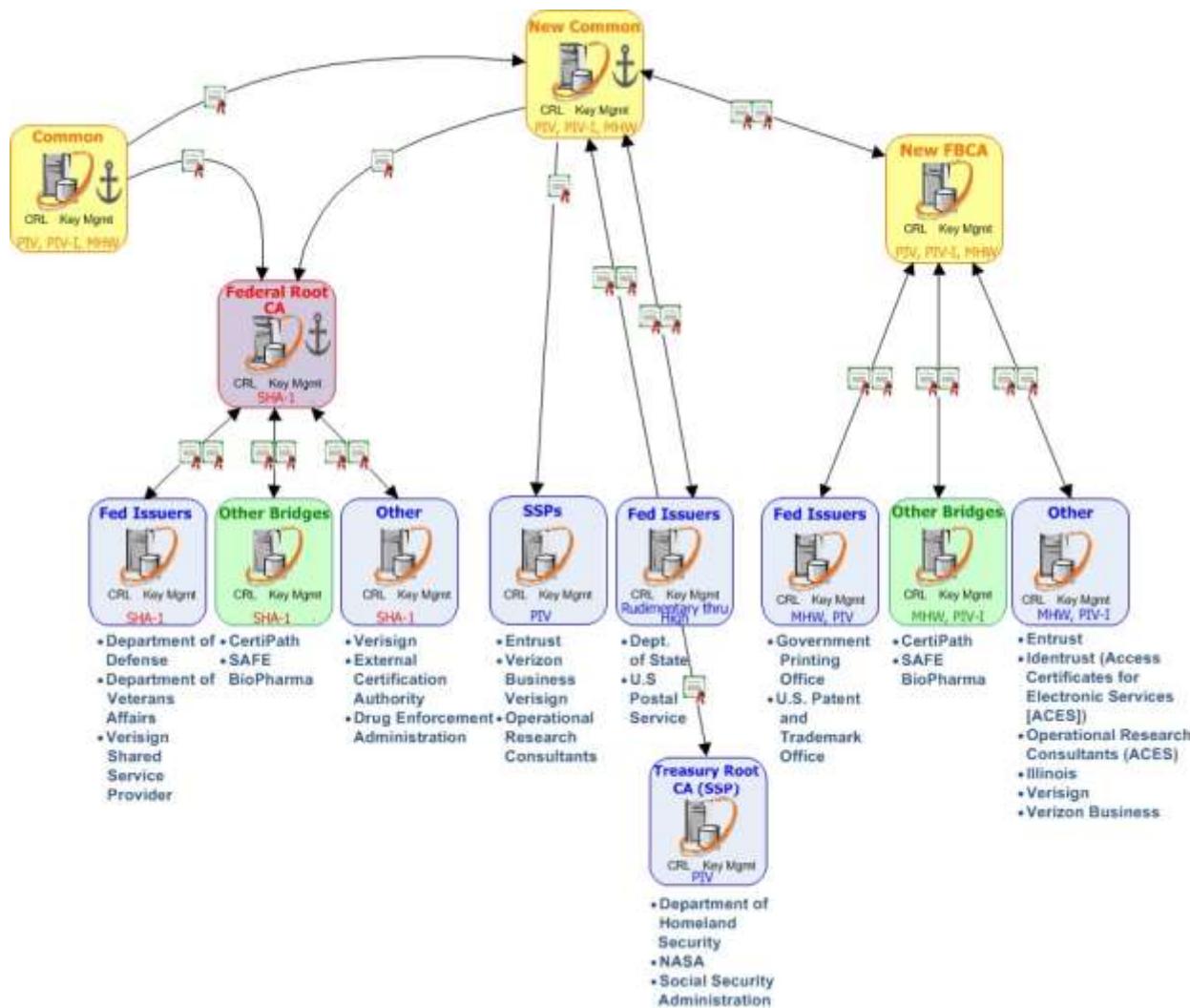


Figure 9: Federal PKI Architecture

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, organized to support the pharmaceutical industry and the Certipath Bridge, organized to support 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 Shared Service Providers (SSP). Federal agencies that do not operate a legacy PKI can acquire PKI services that comply with Federal policy requirements from the SSPs. The FCPCA encompasses two CAs, one to support validation of digital signatures and signed objects by legacy users of SHA-1 and another to support users of SHA-2. The SHA-1 infrastructure will be phased out by the end of 2013. 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 Research & Education Bridge Certification Authority (REBCA) organized to support the educational community.

Enabling the appropriate level of identity assurance for non-federal users, as defined in 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 user ID/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. As illustrated above, the New FBCA requires medium hardware assurance for federal and other bridges. 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 10 shows a generic solution architecture for an agency PIV credentialing system.

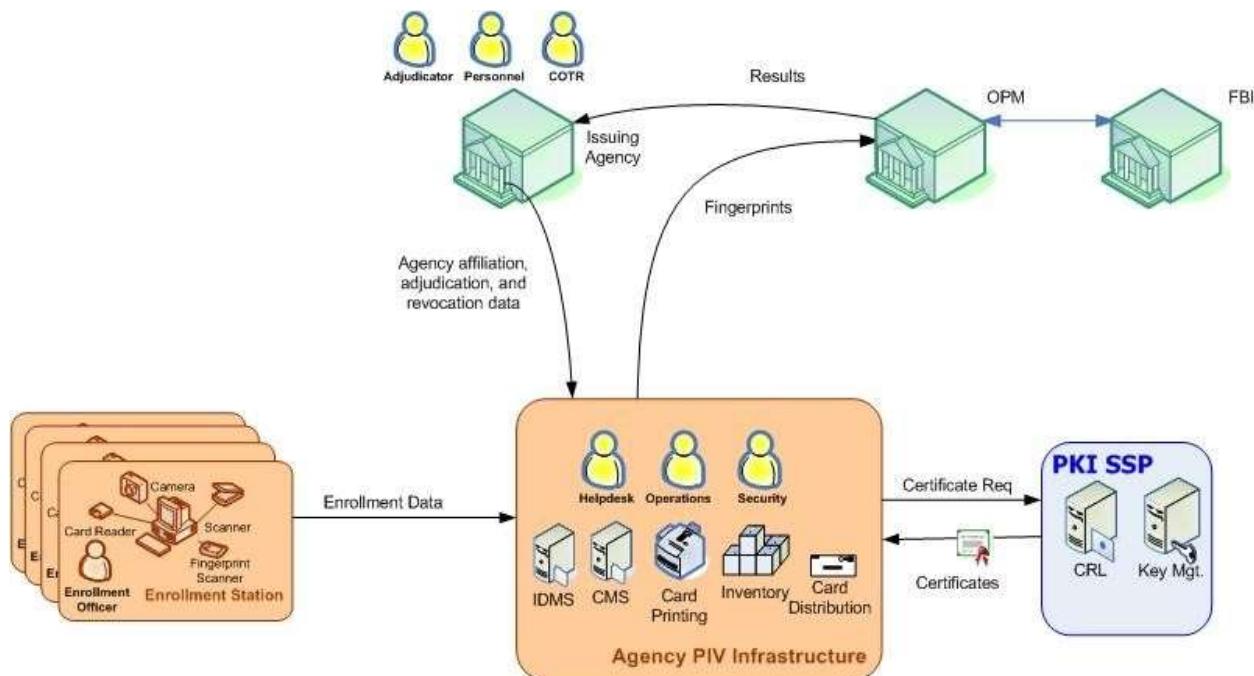


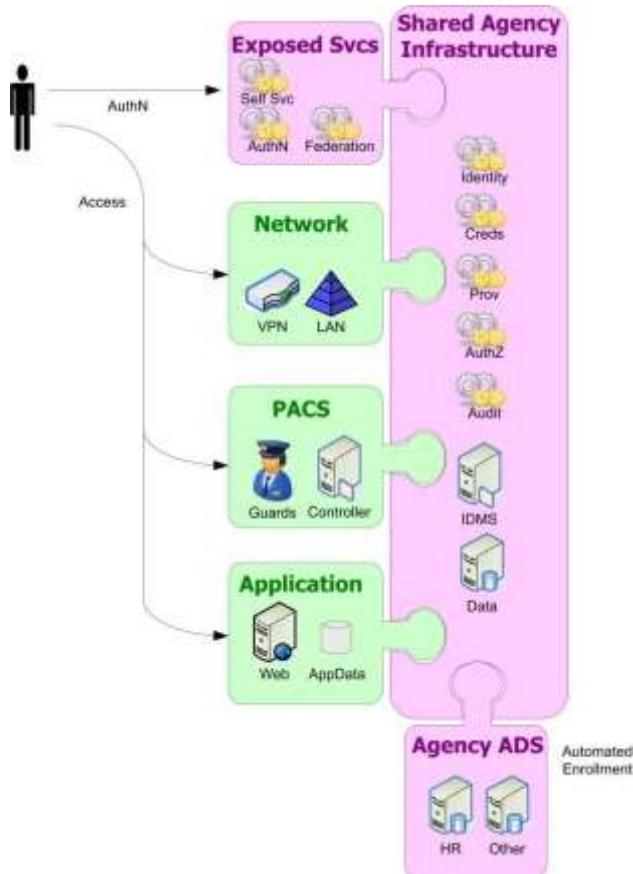
Figure 10: HSPD-12 Conceptual Diagram

In the target state, it is envisioned that agencies will use the PIV credentials for PACS and Logical Access Control Systems (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 11 shows the target system interfaces at the agency level, as viewed from the user perspective.



**Figure 11: 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 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 the 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 authoritative data sources 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 users will have access to data within infrastructure based on attributes.

In addition, the shared agency infrastructure shown in Figure 11 will connect to a shared federal infrastructure that provides common, government-wide ICAM services as depicted in Figure 7.

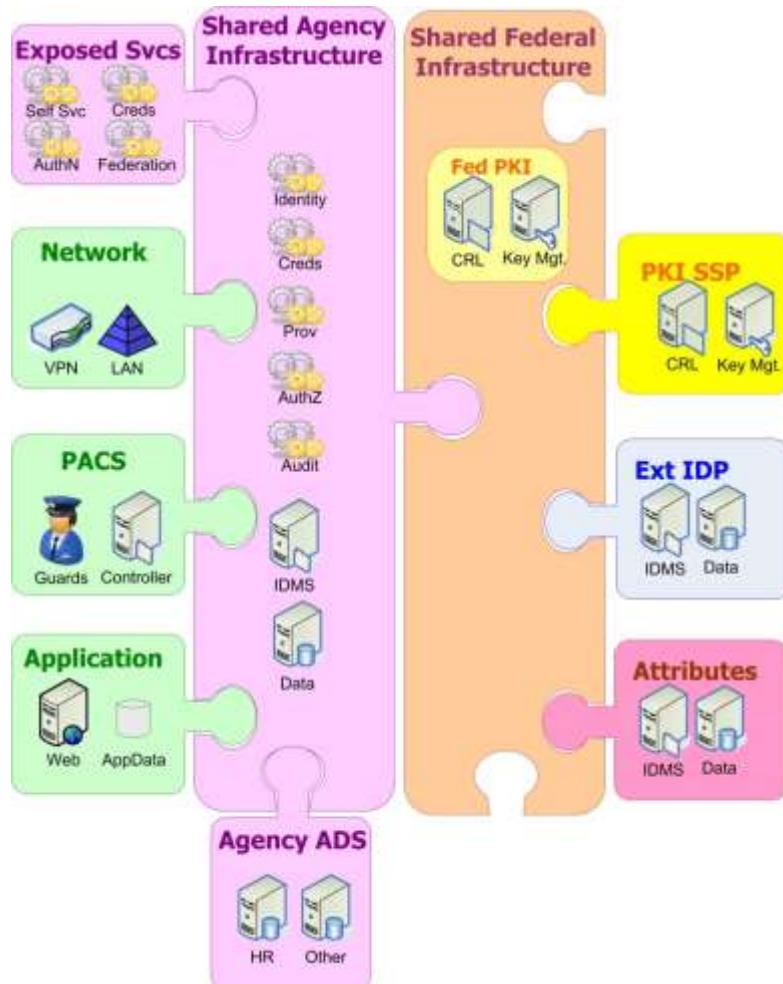
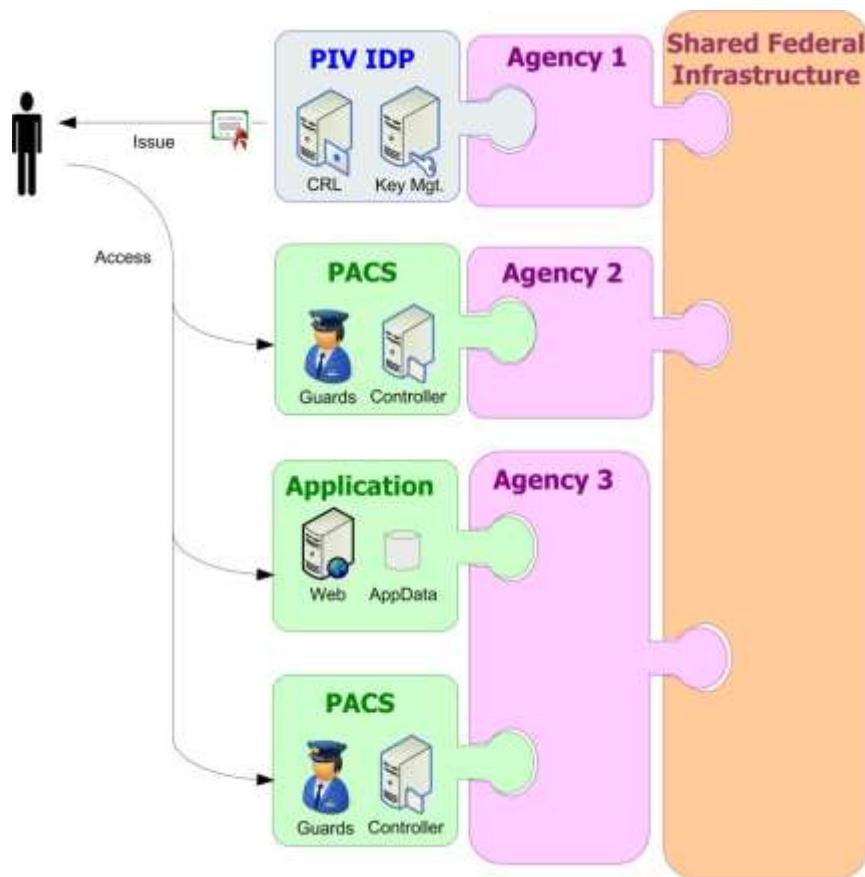


Figure 12: Federal Enterprise Target Conceptual Diagram

The shared federal infrastructure will provide interfaces to PKI SSPs, Identity Providers, 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 13 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 13: 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 14 shows the scenario where an external user authenticates via an external Identity Provider in order to access services at several different agencies. The external Identity Provider is integrated with the Shared Federal Infrastructure, enabling access to multiple agencies.

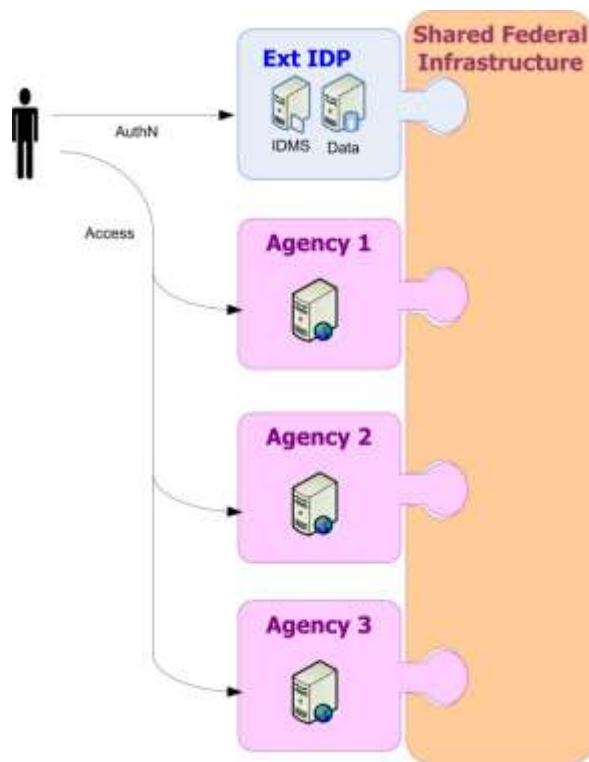


Figure 14: Federal Enterprise Target Conceptual Diagram, Citizen Access

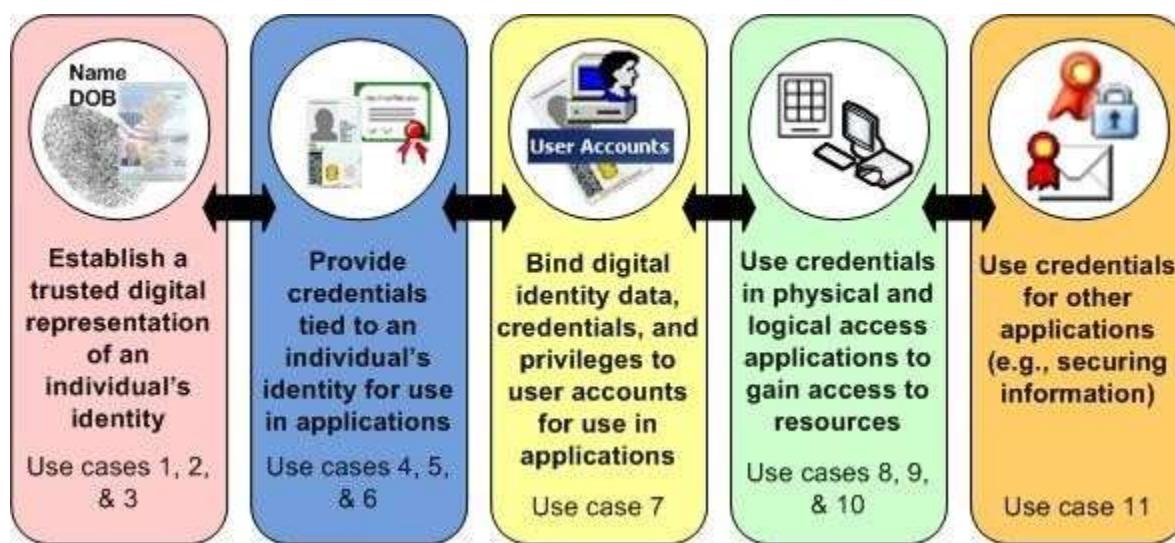
This page is intentionally left blank.

## 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 main 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 Part B of this document. Figure 15 illustrates the high-level functionality encompassed by the use cases in this section.



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-I 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 transactions that occur as part of routine operations 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 the representation of identity in a digital environment. 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.<sup>26</sup>

### 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 helps 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).

---

<sup>26</sup> 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 Inspector General (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:<sup>27</sup>

System Type	Identity Data Stored	Internal User Type
HR System	Biographical, affiliation, citizenship, benefits	Employee
Personnel Security System <sup>28</sup>	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 (PACS)	Biographical, affiliation, security/clearance, biometric, role, credential	Employee, Contractor, Affiliate
Logical Access Control System (LACS)	Biographical, security, biometric, personal identification number (PIN)	Employee, Contractor, Affiliate

**Figure 16: 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 Section 3.2.

---

<sup>27</sup> 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.

<sup>28</sup> 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
<b>Business</b>	<ul style="list-style-type: none"> <li>• <b>E-Government Alignment:</b> IEE</li> <li>• <b>Trigger:</b> <ul style="list-style-type: none"> <li>◦ Part 1: An individual becomes affiliated with an agency</li> <li>◦ Part 2: An individual's identity data changes, requiring an update to his digital identity record</li> </ul> </li> <li>• <b>Actors:</b> Individual/Internal User, Data Administrator, Authorized User</li> <li>• <b>Endpoints:</b> <ul style="list-style-type: none"> <li>◦ Part 1: Identity record created</li> <li>◦ Part 2: Change made to identity record</li> </ul> </li> </ul>
<b>Data</b>	<p><b>Data Elements</b></p> <ul style="list-style-type: none"> <li>• Identifier</li> <li>• Core attributes</li> <li>• Context specific attributes</li> <li>• Affiliations</li> <li>• Biometrics</li> <li>• Role information</li> <li>• Benefit data</li> <li>• Salary data</li> <li>• Clearance/Suitability/Fitness/Credential Eligibility data</li> <li>• Contract data</li> </ul> <p><b>Data Repositories/Systems</b></p> <ul style="list-style-type: none"> <li>• Human Resources (HR) System</li> <li>• Personnel Security System</li> <li>• Payroll System</li> <li>• Contract/Contractor Management System</li> <li>• eVerify</li> <li>• Physical Access Control System (PACS)</li> <li>• Logical Access Control System (LACS)</li> <li>• Other agency systems</li> </ul>
<b>Service</b>	<ul style="list-style-type: none"> <li>• Digital Identity Lifecycle Management</li> <li>• Linking/Association</li> </ul>
<b>Technology</b>	<p><b>Hardware/Software</b></p> <ul style="list-style-type: none"> <li>• Database Management System, servers to support systems</li> <li>• Directory Services</li> <li>• USAJobs (portal software)</li> <li>• Electronic Questionnaires for Investigations Processing (e-QIP) (portal software)</li> </ul> <p><b>Standards</b></p> <ul style="list-style-type: none"> <li>• eXtensible Markup Language (XML)</li> </ul>

Figure 17: 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, an individual's identity record may be drawn from multiple systems that store different component data elements; however, only one system should be authoritative for each individual identity attribute. 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 authoritative identity data from 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.

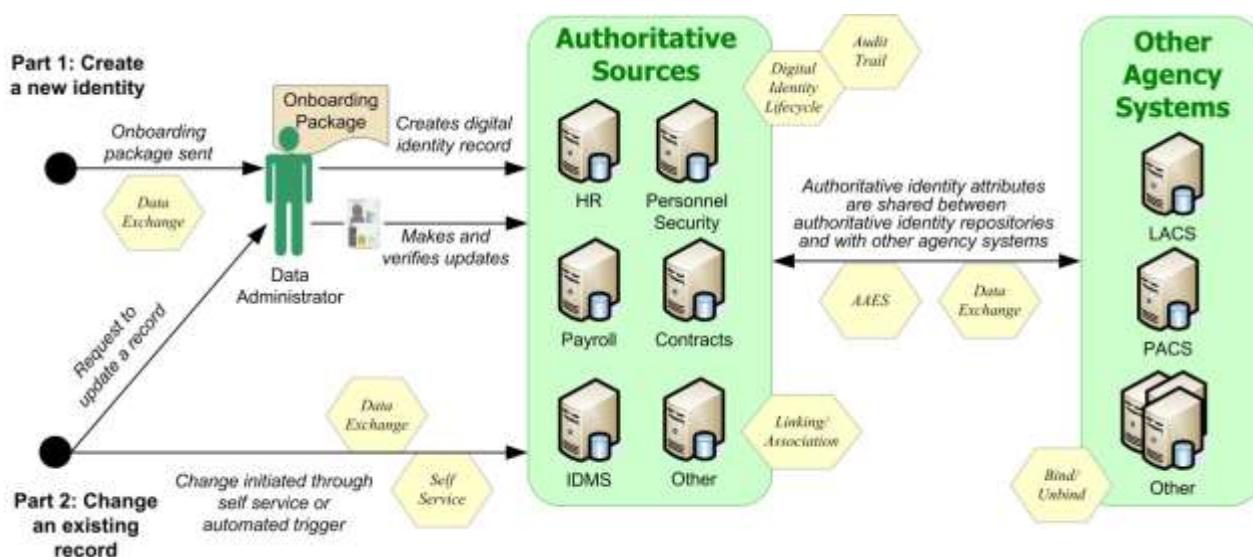


Figure 18: Use Case 1 Target Process Diagram

#### 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 Section 3.2.

Architecture Layer	Architecture Details
<b>Business</b>	<ul style="list-style-type: none"> <li><b>E-Government Alignment:</b> IEE</li> <li><b>Trigger:</b> <ul style="list-style-type: none"> <li>Part 1: An individual becomes affiliated with an agency</li> <li>Part 2: An individual's identity data changes, requiring an update to his digital identity record</li> </ul> </li> <li><b>Actors:</b> Individual/Internal User, Data Administrator, Authorized User</li> <li><b>Endpoints:</b> <ul style="list-style-type: none"> <li>Part 1: Identity record created</li> <li>Part 2: Change made to identity record</li> </ul> </li> </ul>
<b>Data</b>	<p><b>Data Elements</b></p> <ul style="list-style-type: none"> <li>Identifier</li> <li>Core attributes</li> <li>Context specific attributes</li> <li>Affiliations</li> <li>Biometrics</li> <li>Role information</li> <li>Benefit data</li> <li>Salary data</li> <li>Clearance/Suitability/Fitness/Credential Eligibility data</li> <li>Contract data</li> </ul> <p><b>Data Repositories/Systems</b></p> <ul style="list-style-type: none"> <li>Human Resource (HR) System</li> <li>Personnel Security System</li> <li>Payroll System</li> <li>Contract/Contractor Management System</li> <li>Physical Access Control System (PACS)</li> <li>Logical Access Control System (LACS)</li> <li>Other agency systems</li> </ul>

Architecture Layer	Architecture Details
<b>Service</b>	<ul style="list-style-type: none"> <li>• Authoritative Attribute Exchange (AAES)</li> <li>• Digital Identity Lifecycle Management</li> <li>• Linking/Association</li> <li>• Data Exchange</li> <li>• Bind/Unbind</li> <li>• Self-Service</li> <li>• Audit Trail</li> </ul>
<b>Technology</b>	<p><b>Hardware/Software</b></p> <ul style="list-style-type: none"> <li>• Database Management System, servers to support systems</li> <li>• Directory Services</li> <li>• USAJobs (portal software)</li> <li>• Electronic Questionnaires for Investigations Processing (e-QIP) (portal software)</li> </ul> <p><b>Standards</b></p> <ul style="list-style-type: none"> <li>• eXtensible Markup Language (XML)</li> <li>• Simple Object Access Protocol (SOAP)</li> <li>• Secure Socket Layer (SSL)</li> <li>• Security Assertion Markup Language (SAML) 2.0</li> </ul>

**Figure 19: 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 de-provisioning, 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 [SSA], 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 is 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 Section 3.2.

Architecture Layer	Architecture Details
<b>Business</b>	<ul style="list-style-type: none"> <li>• <b>E-Government Alignment:</b> IEE, G2G, G2C, G2B</li> <li>• <b>Trigger:</b> <ul style="list-style-type: none"> <li>○ Part 1: Applicant requests account for government application</li> <li>○ Part 2: User requests update to digital identity record attribute(s)</li> </ul> </li> <li>• <b>Actors:</b> Applicant/User, Application Administrator</li> <li>• <b>Endpoint:</b> <ul style="list-style-type: none"> <li>○ Part 1: Identity record created</li> <li>○ Part 2: Change made to identity record</li> </ul> </li> </ul>
<b>Data</b>	<p><b>Data Elements</b></p> <ul style="list-style-type: none"> <li>• Identity data</li> <li>• Mission-specific data</li> </ul> <p><b>Data Repository/System</b></p> <ul style="list-style-type: none"> <li>• Agency applications</li> </ul>
<b>Service</b>	<ul style="list-style-type: none"> <li>• Digital Identity Lifecycle Management</li> <li>• Linking/Association</li> <li>• Self-Service</li> <li>• Identity Proofing</li> </ul>

Architecture Layer	Architecture Details
<b>Technology</b>	<b>Hardware/Software</b> <ul style="list-style-type: none"> <li>• Database Management System</li> <li>• Mission applications</li> <li>• Directory Services</li> </ul> <b>Standards</b> <ul style="list-style-type: none"> <li>• eXtensible Markup Language (XML)</li> </ul>

Figure 20: 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 Applicant. 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 the Applicant 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 a User'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 a User'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 User 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.

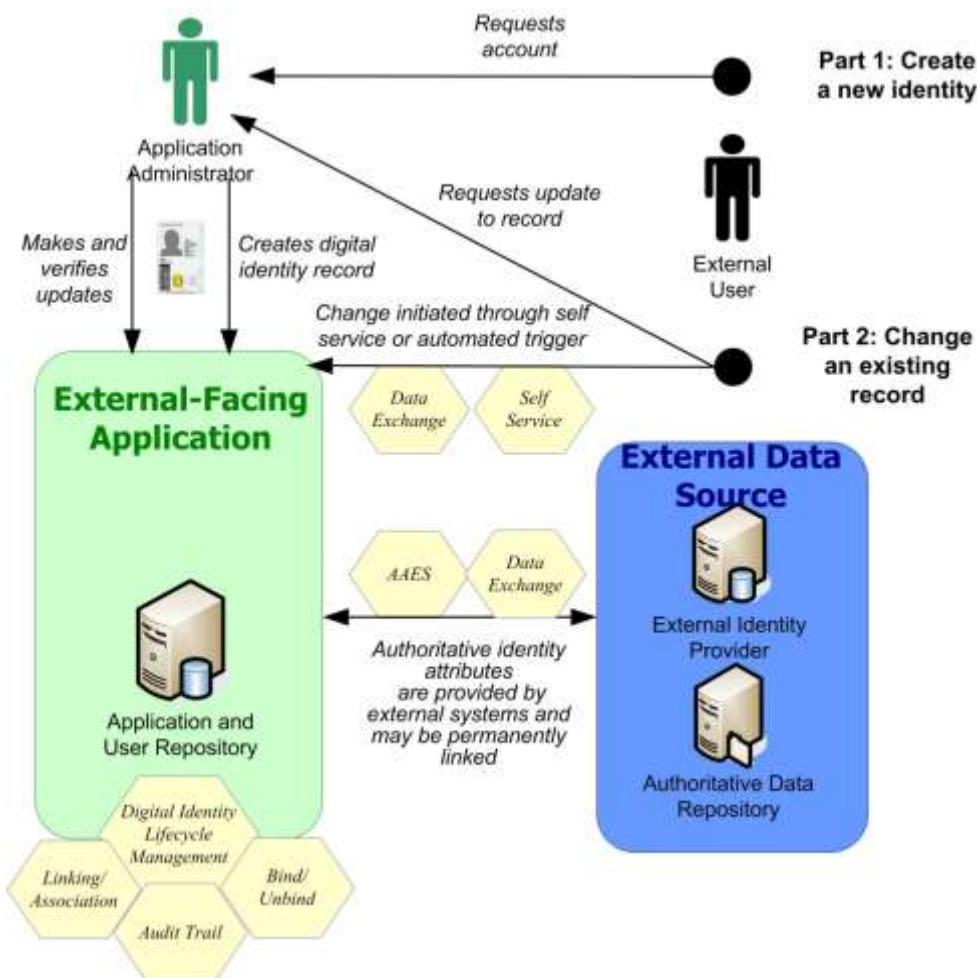


Figure 21: Use Case 2 Target Process Diagram

#### 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 Section 3.2.

Architecture Layer	Architecture Details
<b>Business</b>	<p><b>E-Government Alignment:</b> IEE (in the case of conditional hires or job applicants), G2G, G2C, G2B</p> <ul style="list-style-type: none"> <li><b>Trigger:</b> <ul style="list-style-type: none"> <li>Part 1: Applicant requests account for government application</li> <li>Part 2: User requests update to digital identity record attribute(s)</li> </ul> </li> <li><b>Actors:</b> Applicant/User, Application Administrator</li> <li><b>Endpoint:</b> <ul style="list-style-type: none"> <li>Part 1: Identity record created</li> <li>Part 2: Change made to identity record</li> </ul> </li> </ul>

Architecture Layer	Architecture Details
<b>Data</b>	<p><b>Data Elements</b></p> <ul style="list-style-type: none"> <li>• Identifier</li> <li>• Core attributes</li> <li>• Context specific attributes</li> <li>• Affiliations</li> </ul> <p><b>Data Repositories/Systems</b></p> <ul style="list-style-type: none"> <li>• Mission delivery applications (e.g., grant/loan applications)</li> <li>• Other agency systems</li> </ul>
<b>Service</b>	<ul style="list-style-type: none"> <li>• Digital Identity Lifecycle Management</li> <li>• Linking/Association</li> <li>• Bind/Unbind</li> <li>• Self-Service</li> <li>• Data Exchange</li> <li>• Authoritative Attribute Exchange (AAES)</li> <li>• Audit Trail</li> </ul>
<b>Technology</b>	<p><b>Hardware/Software</b></p> <ul style="list-style-type: none"> <li>• Database Management System</li> <li>• Directory Services</li> <li>• Online Certificate Status Protocol (OCSP)/Certificate Revocation List (CRL)/Server-based Certificate Status Protocol (SCVP)</li> </ul> <p><b>Standards</b></p> <ul style="list-style-type: none"> <li>• eXtensible Markup Language (XML)</li> <li>• Secure Socket Layer (SSL)</li> <li>• X.509</li> </ul>

**Figure 22: 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
<b>Adjudication<sup>29</sup></b>	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: <ul style="list-style-type: none"> <li>• suitable for Government employment;</li> <li>• eligible for logical and physical access;</li> <li>• eligible for access to classified information;</li> <li>• eligible to hold a sensitive position; or</li> <li>• fit to perform work for or on behalf of the Government as a contractor employee.</li> </ul>
<b>Credentialing Determination</b>	Determination of whether or not an individual is eligible <sup>30</sup> to receive a Personal Identity Verification (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 FIPS 201 Section 2, and additional Office of Personnel Management (OPM) requirements as applicable: <ol style="list-style-type: none"> <li>1. 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.</li> <li>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.</li> </ol>
<b>Suitability Determination<sup>31</sup></b>	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.
<b>Fitness Determination</b>	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

<sup>29</sup> As defined 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, The White House, June 30, 2008.[E.O. 13467]

<sup>30</sup> This document uses the term eligibility to describe an individual's eligibility to receive a PIV credential

<sup>31</sup> As defined in the [Code of Federal Regulations](#), Title 5 Volume 2, Government Printing Office, January 1, 2005.

Term	Definition
	employee.
<b>Security Clearance Determination</b>	Determination of whether or not an individual is eligible for access to sensitive or classified information. <sup>32</sup>

### 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 Federal Bureau of Investigation (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<sup>33</sup> engender little trust or reciprocity across agencies; and
- A long delay between the initiation of a background investigation<sup>34</sup> 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:

---

<sup>32</sup> "Classified information" means information that has been determined pursuant to [Executive Order 12958](#), Classified National Security Information, The White House , 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.), Nuclear Regulatory Commission, to require protection against unauthorized disclosure.

<sup>33</sup> OPM determines the minimum investigation required to support reciprocity, and currently conducts the NACI as the minimum standardized investigation for PIV credential applicants.

<sup>34</sup> Based upon [GAO-07-842T](#), Delays and Inadequate Documentation Found for Industry Personnel, GAO, May 2007.

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, Contract Officer's Technical Representative, or Program Officer triggers the background investigation, often in conjunction with the Facility Security Officer 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 Central 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 card 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 card, the Agency Representative may exercise discretion to deny a PIV card. 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 card 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 the FBI or OPM to check for criminal history in the Integrated Automated Fingerprint Identification System (IAFIS). The 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 Section 3.2.

Architecture Layer	Architecture Details
<b>Business</b>	<ul style="list-style-type: none"> <li>• <b>E-Government Alignment:</b> IEE</li> <li>• <b>Trigger:</b> An Applicant needs a background investigation due to the Applicant's status as a federal employee or contractor.</li> <li>• <b>Actors:</b> Applicant, Agency Representative, Investigative Service Provider, Adjudicator</li> <li>• <b>Endpoint:</b> A background investigation has been completed and adjudicated.</li> </ul>
<b>Data</b>	<p><b>Data Elements<sup>35</sup></b></p> <ul style="list-style-type: none"> <li>• Applicant biographic data</li> <li>• Applicant employment history for previous 5 years</li> <li>• Applicant education attained during previous 5 years including highest degree verified</li> <li>• Applicant place of residence for previous 5 years</li> <li>• Applicant Citizenship status</li> <li>• Applicant references</li> <li>• Applicant law enforcement check for previous 5 years</li> <li>• Applicant National Agency Checks (NACs)</li> <li>• Applicant fingerprint samples</li> <li>• Agency data</li> </ul> <p><b>Data Repositories/Systems</b></p> <ul style="list-style-type: none"> <li>• Central Verification System (CVS)</li> <li>• Personnel Investigations Processing System (PIPS)</li> <li>• Joint Personnel Adjudication System (JPAS)</li> <li>• Federal Bureau of Investigation Integrated Automated Fingerprint Identification System (FBI IAFIS)</li> <li>• Fingerprint Transaction System (FTS)</li> <li>• Agency Human Resources (HR) database</li> <li>• Agency Personnel Security database</li> </ul>

<sup>35</sup> 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
	<ul style="list-style-type: none"> <li>• Other agency-specific databases</li> </ul>
<b>Service</b>	<ul style="list-style-type: none"> <li>• Adjudication</li> <li>• Digital Identity Lifecycle Management</li> </ul>
<b>Technology</b>	<p><b>Hardware/Software</b></p> <ul style="list-style-type: none"> <li>• Electronic Questionnaires for Investigations Processing (e-QIP)</li> <li>• Database Management System, servers for primary systems</li> </ul> <p><b>Standards</b></p> <ul style="list-style-type: none"> <li>• FIPS 201</li> <li>• American National Standards Institute (ANSI)/National Institute of Standards and Technology Information Technology Lab (NIST-ITL) 1-2000</li> </ul>

Figure 23: 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 capability within CVS to view background investigation adjudication results 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, Contract Officer's Technical Representative, or Program Officer triggers the background investigation, often in conjunction with the Facility Security Officer 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 card 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 card. 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 card 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.<sup>36</sup>
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 credential 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 ISP 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.

<sup>36</sup> Federal risk levels and associated background investigations are currently being revised by OPM.

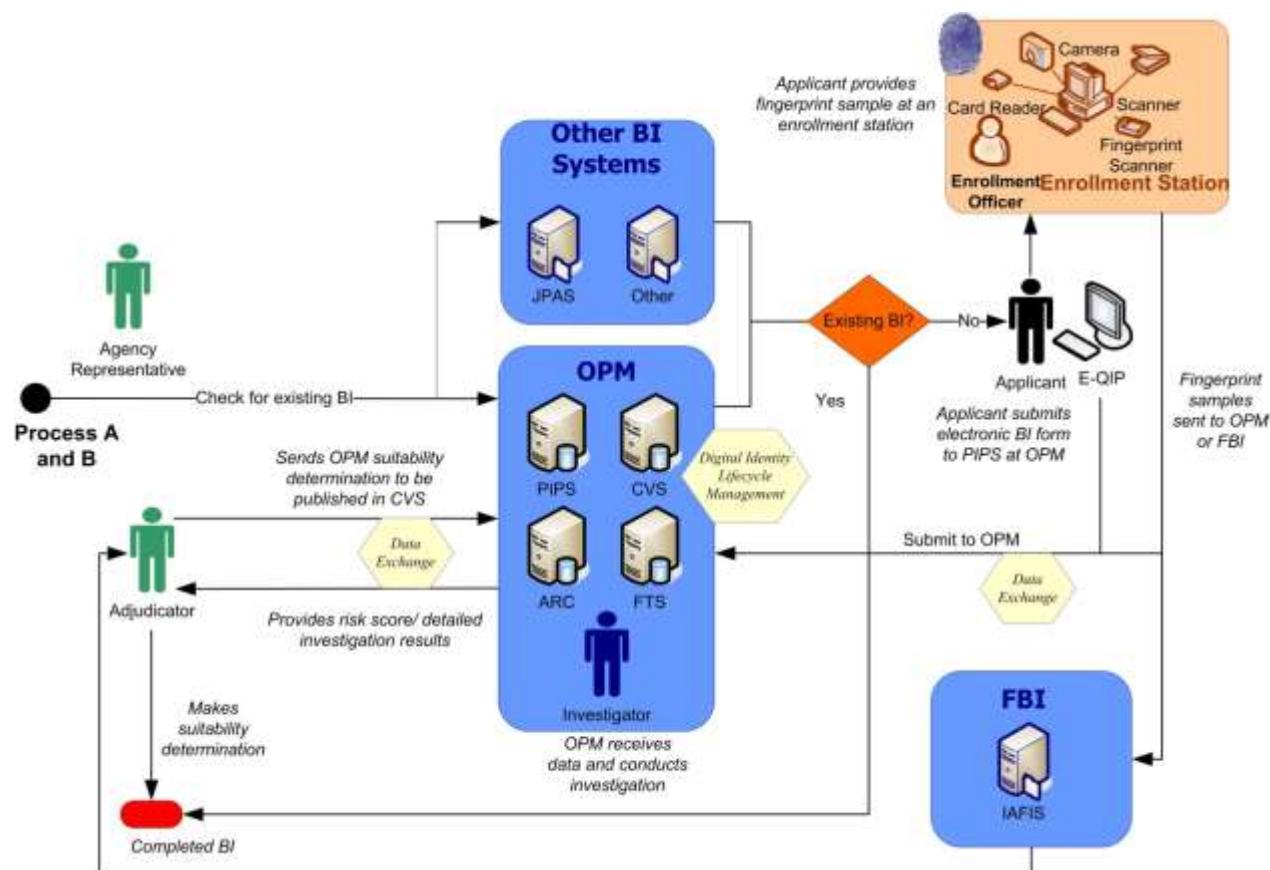


Figure 24: Use Case 3 Target Process Diagram

#### 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 Section 3.2.

Architecture Layer	Architecture Details
<b>Business</b>	<ul style="list-style-type: none"> <li><b>E-Government Alignment:</b> IEE</li> <li><b>Trigger:</b> An Applicant needs a background investigation due to the Applicant's status as a federal employee or contractor.</li> <li><b>Actors:</b> Applicant, Agency Representative, Investigative Service Provider, Adjudicator</li> <li><b>Endpoint:</b> A background investigation has been completed and adjudicated.</li> </ul>

Architecture Layer	Architecture Details
<b>Data</b>	<p><b>Data Elements</b> (can vary by the type of investigation required)</p> <ul style="list-style-type: none"> <li>• Applicant biographic data</li> <li>• Applicant employment history for previous 5 years</li> <li>• Applicant education attained during previous 5 years including highest degree verified</li> <li>• Applicant place of residence for previous 5 years</li> <li>• Applicant Citizenship status</li> <li>• Applicant references</li> <li>• Applicant law enforcement check for previous 5 years</li> <li>• Applicant National Agency Check (NAC)</li> <li>• Applicant fingerprint samples</li> <li>• Agency data</li> </ul> <p><b>Data Repositories/Systems</b></p> <ul style="list-style-type: none"> <li>• Central Verification System (CVS)</li> <li>• Central Contractor Registration (CCR) database</li> <li>• Personnel Investigations Processing System (PIPS)</li> <li>• Joint Personnel Adjudication System (JPAS)</li> <li>• Federal Bureau of Investigation Integrated Automated Fingerprint Identification System (FBI IAFIS)</li> <li>• Fingerprint Transaction System (FTS)</li> <li>• Agency Human Resources (HR) database</li> <li>• Agency Personnel Security database</li> <li>• Other agency-specific databases</li> </ul>
<b>Service</b>	<ul style="list-style-type: none"> <li>• Data Exchange</li> <li>• Adjudication</li> <li>• Digital Identity Lifecycle Management</li> </ul>
<b>Technology</b>	<p><b>Hardware/Software</b></p> <ul style="list-style-type: none"> <li>• Electronic Questionnaires for Investigations Processing (e-QIP)</li> <li>• Database Management System, servers for primary systems</li> </ul> <p><b>Standards</b></p> <ul style="list-style-type: none"> <li>• FIPS 201</li> <li>• Secure Socket Layer (SSL)</li> <li>• American National Standards Institute (ANSI)/National Institute of Standards and Technology Information Technology Lab (NIST-ITL) 1-2000</li> </ul>

**Figure 25: 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<sup>37</sup> prescribe government-wide reciprocity requirements, agencies must work to honor reciprocity of background investigations to reduce costs and administrative burden, wherever possible.<sup>38</sup>

<sup>37</sup> [Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12](#), Office of Personnel Management, July 31, 2008.

<sup>38</sup> [M-06-21](#), Reciprocal Recognition of Existing Personnel Security Clearances, OMB, July 17, 2006.

- **Need for common interface standards to conduct automated record checks.** Agencies should identify authoritative sources at the agency level and other cross-agency 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 life cycle 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,<sup>39</sup> 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-I credentials; however, the scope of this use case is limited to the PIV card, the common identification credential for federal employees and contractors.

### 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 PIV 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 Identity Management System (IDMS), either on an individual basis, or as part of a group in a

---

<sup>39</sup> HSPD-12 applies to federal employees, contractors, and affiliates requiring long-term access to federal facilities and information systems in accordance with [M-05-24](#), Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employees and Contractors, OMB, August 5, 2005. [M-05-24] Applicability to affiliates, which may include foreign nationals and other parties, is an agency-level risk-based decision.

batched process (batch processing may be handled in various ways at individual agencies).

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 a PIV credential.
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 one-to-many (1:n) 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 PIV 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/ M-05-24.<sup>40</sup>
4. Full background check information is typically collected via related background investigation processes associated with on-boarding (see Use Case 3). The Adjudicator

---

<sup>40</sup> [M-05-24](#)

provides a final PIV 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 PIV card production for the credential on an interim (six-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 National Agency Check with Written Inquiries (NACI) Indicator to show full approval (the NACI Indicator is located on the PIV Authentication Certificate). This process is handled differently 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 PIV card certificates.
6. The certificates<sup>41</sup> and PIN are loaded onto the PIV 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 card life cycle. 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 PIV 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

---

<sup>41</sup> The digital certificates issued as part of the PIV card must be compliant with the [COMMON](#).

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.)

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 Certification Authority (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 PIV 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 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 six 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 PIV card (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 PIV card is terminated in IDMS.
5. The digital credentials on the PIV card are revoked.
6. Revocation status is propagated to applicable provisioning software or individual applications, notifying them of PIV 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 Section 3.2.

Architecture Layer	Architecture Details
<b>Business</b>	<ul style="list-style-type: none"> <li>• <b>E-Government Alignment:</b> IEE</li> <li>• <b>Trigger:</b> <ul style="list-style-type: none"> <li>◦ Part 1: A sponsor requests a PIV card for an employee or contractor.</li> <li>◦ Part 2: A Cardholder's PIV card requires a maintenance activity.</li> </ul> </li> <li>• <b>Actors:</b> Applicant /Cardholder, Sponsor, Registrar/Enrollment Official, Adjudicator, Issuer, Card Management System Administrator, Subscriber, Key Recovery Officer, Local Registration Agent (LRA), Key Recovery Agent (KRA)</li> <li>• <b>Endpoint:</b> <ul style="list-style-type: none"> <li>◦ Part 1: A PIV card is issued.</li> <li>◦ Part 2: A PIV card is maintained and ultimately expires/is revoked.</li> </ul> </li> </ul>
<b>Data</b>	<p><b>Data Elements</b></p> <ul style="list-style-type: none"> <li>• PIV Sponsor <ul style="list-style-type: none"> <li>◦ Name</li> <li>◦ Organization</li> <li>◦ Contact Information</li> </ul> </li> <li>• Applicant <ul style="list-style-type: none"> <li>◦ Name</li> <li>◦ Date of birth (DOB)</li> <li>◦ Position</li> <li>◦ Contact Information</li> <li>◦ Digitally Captured Facial Image</li> <li>◦ Fingerprints</li> <li>◦ Background Investigation Results</li> <li>◦ I-9 Source Identity Documentation Data</li> <li>◦ Document title</li> <li>◦ Document issuing authority</li> <li>◦ Document number</li> <li>◦ Document expiration date (if any)</li> <li>◦ Cardholder Unique Identifier (CHUID)/Federal Agency Smart Credential Number (FASC-N)</li> <li>◦ Personal identification number (PIN)</li> <li>◦ Cryptographic Key Pairs</li> <li>◦ Cryptographic Key Pairs Certificates</li> <li>◦ PIV Credential Holder signature</li> </ul> </li> </ul>

Architecture Layer	Architecture Details
	<ul style="list-style-type: none"> <li>• PIV Registrar <ul style="list-style-type: none"> <li>◦ Name</li> <li>◦ Contact Information</li> <li>◦ Completed &amp; signed PIV Request</li> <li>◦ Completed &amp; signed Standard Form (SF) 85 (or equivalent)</li> </ul> </li> <li>• PIV Issuer <ul style="list-style-type: none"> <li>◦ Name</li> <li>◦ Contact Information</li> <li>◦ Completed &amp; formally authorized PIV request</li> <li>◦ Approval notice from PIV Registrar</li> <li>◦ Agency Card Serial Number</li> <li>◦ Signed acceptance form from PIV credential holder</li> </ul> </li> </ul> <p><b>Data Repositories/Systems</b></p> <ul style="list-style-type: none"> <li>• Identity Management System (IDMS)</li> <li>• Card Management System</li> <li>• Certificate Revocation List (CRL)</li> <li>• Audit Log System</li> </ul>
<b>Service</b>	<ul style="list-style-type: none"> <li>• Sponsorship</li> <li>• Enrollment</li> <li>• Adjudication</li> <li>• Issuance/Activation</li> <li>• Credential Lifecycle Management</li> <li>• Digital Signature</li> <li>• Audit Trail</li> </ul>
<b>Technology</b>	<p><b>Hardware/Software</b></p> <ul style="list-style-type: none"> <li>• See the <a href="#">GSA Approved Products List (APL)</a> supported by the Homeland Security Presidential Directive 12 (HSPD-12) Evaluation Program:</li> <li>• Card Printer Station</li> <li>• CHUID Reader (Contact)</li> <li>• CHUID Reader (Contactless)</li> <li>• Cryptographic Module</li> <li>• Electromagnetically Opaque Sleeve</li> <li>• Electronic Personalization (Product)</li> <li>• Electronic Personalization (Service)</li> <li>• Facial Image Capturing (Middleware)</li> <li>• Facial Image Capturing Camera</li> <li>• Fingerprint Capture Station</li> <li>• Graphical Personalization</li> <li>• OCSP Responder</li> <li>• PIV Card</li> <li>• PIV Middleware</li> <li>• Single Fingerprint Capture Device</li> <li>• Template Generator</li> <li>• Template Matcher</li> <li>• Transparent Reader</li> </ul> <p><b>Standards</b></p> <ul style="list-style-type: none"> <li>• FIPS 140</li> <li>• FIPS 201</li> <li>• SP 800-73</li> <li>• SP 800-76</li> <li>• SP 800-78</li> <li>• SP 800-79</li> <li>• SP 800-96</li> <li>• SP 800-104</li> </ul>

Figure 26: 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, which 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 de-provisioning 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 F/ERO 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.<sup>42</sup>
  - Process step: if a PIV card Applicant is approved to be assigned a F/ERO status, the PIVAUTH Certificate and the appropriate attribute assigned to that individual must be sent to FEMA upon PIV card issuance and updated on a periodic 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:

---

<sup>42</sup> This is a mandate arising from House Resolution 12.

- Part 1, Enrollment, Step 6
- Part 1, Adjudication, Steps 4 and 5
- Part 1, Issuance, Step 5
- 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.

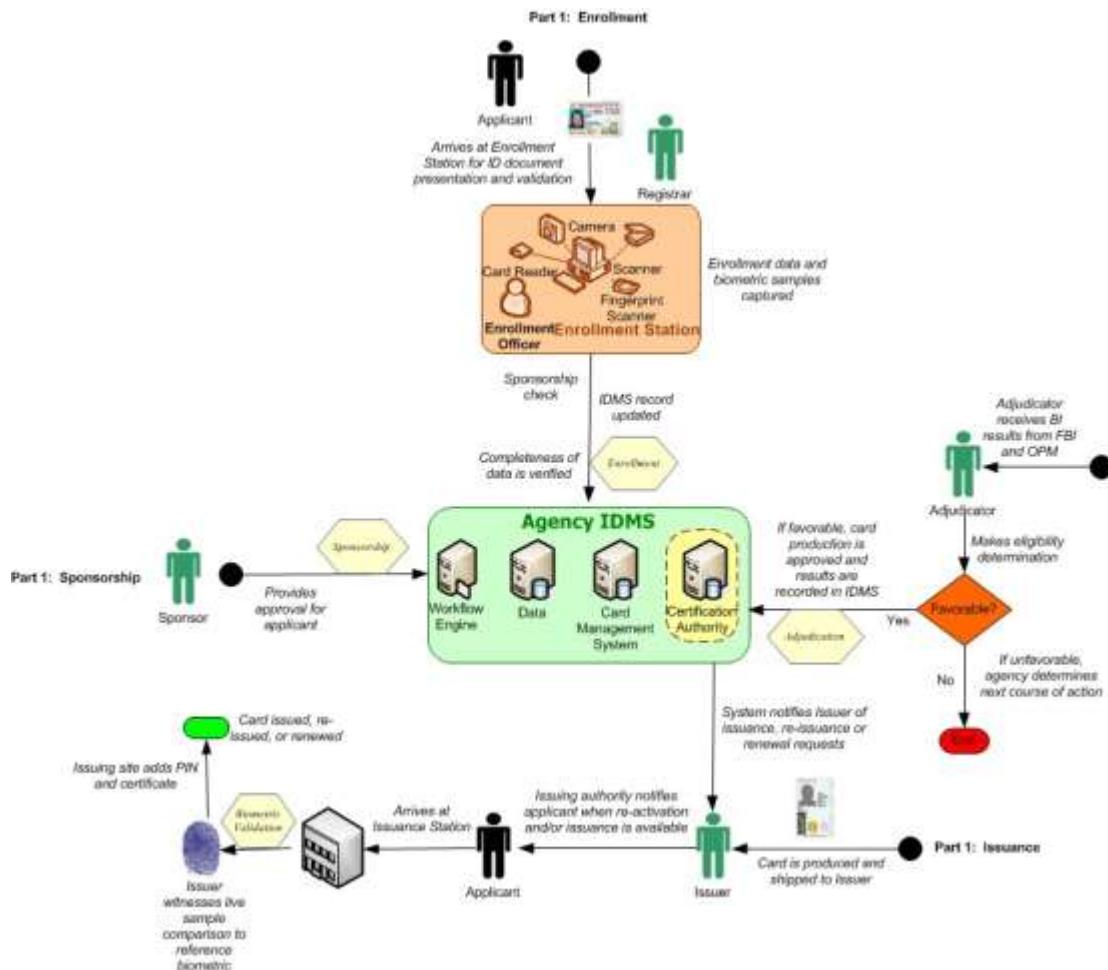


Figure 27: Use Case 4 Target Process Diagram

#### 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 Section 3.2.

Architecture Layer	Architecture Details
<b>Business</b>	<ul style="list-style-type: none"> <li><b>E-Government Alignment:</b> IEE</li> <li><b>Trigger:</b> <ul style="list-style-type: none"> <li>Part 1: An employee or contractor requests a PIV card.</li> <li>Part 2: A Cardholders PIV card requires a maintenance activity.</li> </ul> </li> <li><b>Actors:</b> Applicant /Cardholder, Sponsor, Registrar/Enrollment Official, Adjudicator, Issuer, Card Management System Administrator, Subscriber, Key Recovery Officer, Local Registration Agent (LRA), Key Recovery Agent (KRA)</li> <li><b>Endpoint:</b> <ul style="list-style-type: none"> <li>Part 1: A PIV card is issued.</li> <li>Part 2: A PIV card is maintained and ultimately expires/is revoked.</li> </ul> </li> </ul>

Architecture Layer	Architecture Details
<b>Data</b>	<p><b>Data Elements</b></p> <ul style="list-style-type: none"> <li>• PIV Sponsor <ul style="list-style-type: none"> <li>◦ Name</li> <li>◦ Organization</li> <li>◦ Contact Information</li> </ul> </li> <li>• Applicant <ul style="list-style-type: none"> <li>◦ Name</li> <li>◦ Date of birth (DOB)</li> <li>◦ Position</li> <li>◦ Contact Information</li> <li>◦ Digitally Captured Facial Image</li> <li>◦ Fingerprints</li> <li>◦ Background Investigation Results</li> <li>◦ I-9 Source Identity Documentation Data</li> <li>◦ Document title</li> <li>◦ Document issuing authority</li> <li>◦ Document number</li> <li>◦ Document expiration date (if any)</li> <li>◦ Cardholder Unique Identifier (CHUID)/Federal Agency Smart Credential Number (FASC-N)</li> <li>◦ Personal identification number (PIN)</li> <li>◦ Cryptographic Key Pairs</li> <li>◦ Cryptographic Key Pairs Certificates</li> <li>◦ PIV Credential Holder signature</li> </ul> </li> <li>• PIV Registrar <ul style="list-style-type: none"> <li>◦ Name</li> <li>◦ Contact Information</li> <li>◦ Completed &amp; signed PIV Request</li> <li>◦ Completed &amp; signed Standard Form (SF) 85 (or equivalent)</li> </ul> </li> <li>• PIV Issuer <ul style="list-style-type: none"> <li>◦ Name</li> <li>◦ Contact Information</li> <li>◦ Completed &amp; formally authorized PIV request</li> <li>◦ Approval notice from PIV Registrar</li> <li>◦ Agency Card Serial Number</li> <li>◦ Signed acceptance form from PIV credential holder</li> </ul> </li> </ul> <p><b>Data Repositories/Systems</b></p> <ul style="list-style-type: none"> <li>• Identity Management System (IDMS)</li> <li>• Card Management System</li> <li>• Certificate Revocation List (CRL)</li> </ul>
<b>Service</b>	<ul style="list-style-type: none"> <li>• Sponsorship</li> <li>• Enrollment</li> <li>• Adjudication</li> <li>• Issuance</li> <li>• Credential Lifecycle Management</li> <li>• Digital Signature</li> <li>• Key Management</li> <li>• Audit Trail</li> </ul>

Architecture Layer	Architecture Details
<b>Technology</b>	<p><b>Hardware/Software</b></p> <ul style="list-style-type: none"> <li>• See the <a href="#">GSA Approved Products List (APL)</a> supported by the Homeland Security Presidential Directive 12 (HSPD-12) Evaluation Program:</li> <li>• Card Printer Station</li> <li>• CHUID Reader (Contact)</li> <li>• CHUID Reader (Contactless)</li> <li>• Cryptographic Module</li> <li>• Electromagnetically Opaque Sleeve</li> <li>• Electronic Personalization (Product)</li> <li>• Electronic Personalization (Service)</li> <li>• Facial Image Capturing (Middleware)</li> <li>• Facial Image Capturing Camera</li> <li>• Fingerprint Capture Station</li> <li>• Graphical Personalization</li> <li>• Online Certificate Status Protocol (OCSP) Responder</li> <li>• PIV Card</li> <li>• PIV Middleware</li> <li>• Single Fingerprint Capture Device</li> <li>• Template Generator</li> <li>• Template Matcher</li> <li>• Transparent Reader</li> </ul> <p><b>Standards</b></p> <ul style="list-style-type: none"> <li>• FIPS 140</li> <li>• FIPS 201</li> <li>• SP 800-73</li> <li>• SP 800-76</li> <li>• SP 800-78</li> <li>• SP 800-79</li> <li>• SP 800-96</li> <li>• SP 800-104</li> </ul>

Figure 28: 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 card 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 card 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 life cycle 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. Alternatively, PKI certificates can be issued 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<sup>43</sup> (COMMON), the policy governing the PKI component of the FEA, 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 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 Level of Assurance (LOA) 3 and 4<sup>44</sup> and may be used to provide authentication, digital signature and encryption functionality. PKI certificates that are to be used at LOA 4 must be installed on a hardware token, while soft certificates are acceptable at LOA 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 LOA 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 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
<b>FBCA Basic Assurance</b>	X	
<b>FBCA Medium Assurance</b>	X	
<b>FBCA Medium Hardware</b>	X	X
<b>FBCA High Assurance</b>	X	X
<b>COMMON (Software)</b>	X	
<b>COMMON_Hardware</b>	X	X
<b>COMMON_High</b>	X	X

Figure 29: Mapping of PKI Credential and Identity Assurance Levels

<sup>43</sup> [COMMON](#)

<sup>44</sup> As defined in [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 the Federal Government.
- Rules and guidance for Key Escrow are not well-defined across the Federal 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 Registration Authority (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 (DOB), 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.
- c. 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.
  - d. 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 life cycle. 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 Section 3.2.

Architecture Layer	Architecture Details
<b>Business</b>	<ul style="list-style-type: none"> <li><b>E-Government Alignment:</b> IEE, G2G, G2B, G2C</li> <li><b>Trigger:</b> User requests a PKI certificate</li> <li><b>Actors:</b> Certification Authority (CA), Certificate Status Servers, Registration Authority (RA), Applicant/Subscriber, Authorized Sponsoring Agency Employee</li> <li><b>Endpoints:</b> <ul style="list-style-type: none"> <li>Part 1: A PKI certificate is issued.</li> <li>Part 2: PKI Maintenance activity is successfully completed.</li> </ul> </li> </ul>
<b>Data</b>	<p><b>Data Elements</b></p> <p>RA</p> <ul style="list-style-type: none"> <li>The identity of the person performing the identification</li> <li>A signed declaration by that person that he verified the identity of the Applicant</li> <li>Unique identifying number(s) from the ID(s) of the Applicant, or a facsimile of the ID(s)</li> <li>Applicant's biometric data</li> <li>The date and time of the verification</li> <li>A declaration of identity signed by the Applicant using a handwritten signature and performed in the presence of the person performing the identity authentication</li> </ul> <p>Sponsor</p> <ul style="list-style-type: none"> <li>Contact information to enable the CA or RA to communicate with the Sponsor when required</li> </ul> <p><b>Data Repositories/Systems</b></p> <ul style="list-style-type: none"> <li>CA</li> </ul>
<b>Service</b>	<ul style="list-style-type: none"> <li>Identity Proofing</li> <li>Credential Lifecycle Management</li> <li>Sponsorship</li> <li>Enrollment/Registration</li> <li>Adjudication</li> <li>Issuance</li> <li>Self Service</li> <li>Digital Signature</li> <li>Key Management</li> <li>Audit Trail</li> </ul>
<b>Technology</b>	<p><b>Hardware/Software</b></p> <ul style="list-style-type: none"> <li>Smart card (hard tokens)</li> <li>PKI issuance software</li> </ul> <p><b>Standards</b></p> <ul style="list-style-type: none"> <li>Federal PKI Common Policy</li> <li>Federal Bridge Certificate Authority (FBCA) Certificate Policy</li> <li>FIPS 186</li> <li>FIPS 180</li> <li>eXtensible Markup Language (XML)</li> <li>SP 800-67</li> <li>SP 800-78</li> <li>International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 18033-3:2005</li> <li>X.509 Certificate Revocation Lists (CRLs)</li> <li>Online Certificate Status Protocol (OCSP)</li> </ul>

Figure 30: 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 life cycle 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 LOA 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 CAs cross-certified with the Federal Bridge.
- Implementation of key history practices at the CA.
- Increased directory mappings to allow certificates issued from CAs 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.

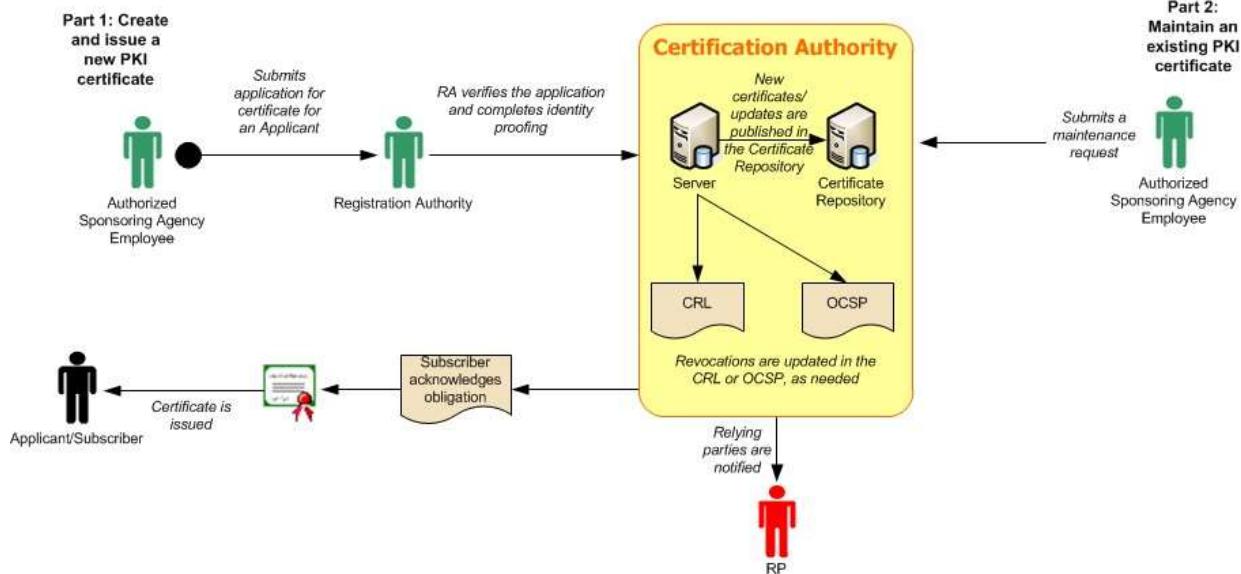


Figure 31: Use Case 5 Target Process Diagram

#### 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 credential 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 LOA 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<sup>45</sup> 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*

---

<sup>45</sup> 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. LOA 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).
  - b. 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 DOB.
    - 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 Section 3.2.

Architecture Layer	Details
<b>Business</b>	<ul style="list-style-type: none"> <li>• <b>E-Government Alignment:</b> IEE, G2G, G2C, G2B</li> <li>• <b>Trigger:</b> <ul style="list-style-type: none"> <li>◦ Part 1: User requests access to a logical resource</li> <li>◦ Part 2: User is required or desires to change password</li> </ul> </li> <li>• <b>Actors:</b> User, Application Administrator, Help Desk</li> <li>• <b>Endpoint:</b> Issuance of password token</li> </ul>
<b>Data</b>	<p><b>Data Elements</b></p> <ul style="list-style-type: none"> <li>• Personal Data           <ul style="list-style-type: none"> <li>◦ Name</li> <li>◦ Date of birth (DOB)</li> <li>◦ Address</li> <li>◦ Other personal information</li> <li>◦ Unique Identifiers (to the system/application consuming the password)</li> <li>◦ Usernames</li> <li>◦ Passwords</li> </ul> </li> </ul> <p><b>Data Repositories/Systems</b></p> <ul style="list-style-type: none"> <li>• Logical Access Control System (LACS)</li> <li>• Local Application</li> </ul>
<b>Service</b>	<ul style="list-style-type: none"> <li>• Identity Proofing</li> <li>• Account Management</li> <li>• Enrollment/Registration</li> <li>• Issuance</li> <li>• Credential Lifecycle Management</li> <li>• Self Service</li> </ul>
<b>Technology</b>	<p><b>Hardware/Software</b></p> <ul style="list-style-type: none"> <li>• Domain Controller</li> <li>• Computer terminal</li> <li>• LACS Server</li> <li>• Network and other Applications</li> <li>• Directory Services</li> </ul> <p><b>Standards</b></p> <ul style="list-style-type: none"> <li>• Interface specifications between the service and Identity Providers</li> <li>• Lightweight Directory Access Protocol (LDAP) v.2 and v.3</li> <li>• Security Assertion Markup Language (SAML) 1.0 and 2.0 for transmission between Identity Providers</li> <li>• Secure Socket Layer (SSL)</li> </ul>

**Figure 32: 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, or Identity Providers, that issue identity tokens to user communities and then provide identity assertions to local applications. The local applications trust the Identity Provider'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 SP 800-63 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 credential 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 Identity Provider 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 implementation plans and begin utilizing them in lieu of password logon.

## **4.7. Provision and De-provision User Account for an Application**

This use case provides the high-level process steps for provisioning and de-provisioning 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 privilege (or 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
- De-provision 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.

De-provisioning 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 de-provisioning 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 (SOD).** Manual processes for granting permission lack visibility across applications and resources to determine if access permissions violate SOD 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).<sup>46</sup>
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: De-provision a user account*

---

<sup>46</sup>This generic title represents a number of individuals within an agency who may have authority to approve account creation or 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 Section 3.2.

Architecture Layer	Architecture Details
<b>Business</b>	<ul style="list-style-type: none"> <li>• <b>E-Government Alignment:</b> IEE, G2G, G2B, G2C</li> <li>• <b>Triggers:</b> <ul style="list-style-type: none"> <li>◦ Part 1: A User requires access to an application</li> <li>◦ Part 2: A User's access need has changed</li> <li>◦ Part 3: A User no longer requires access to the application</li> </ul> </li> <li>• <b>Actors:</b> Individual/User, Privilege Manager, Application Administrator</li> <li>• <b>Endpoints:</b> <ul style="list-style-type: none"> <li>◦ Part 1: A user account is created for the user with the appropriate access privileges</li> <li>◦ Part 2: The user's access privileges are updated to reflect a change in access need</li> <li>◦ Part 3: The user account is deactivated or removed from the application</li> </ul> </li> </ul>
<b>Data</b>	<p><b>Data Elements</b></p> <ul style="list-style-type: none"> <li>• Username</li> <li>• Position</li> <li>• Membership</li> <li>• Authentication Credential</li> <li>• Access Permission</li> </ul> <p><b>Data Repository/System</b></p> <ul style="list-style-type: none"> <li>• Application-specific user database</li> </ul>
<b>Service</b>	<ul style="list-style-type: none"> <li>• Account Management</li> <li>• Bind/Unbind</li> <li>• Provisioning</li> <li>• Privilege Administration</li> <li>• Policy Administration</li> <li>• Audit Trail</li> </ul>
<b>Technology</b>	<p><b>Hardware/Software</b></p> <ul style="list-style-type: none"> <li>• Application administrator Global Unique Identifier (GUID)</li> </ul>

Figure 33: Use Case 7 As-is Architecture Details

#### **4.7.2. Target Analysis**

The underlying business need and function for provisioning and de-provisioning 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 de-provisioning:

- **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 de-provisioning processing time once access is no longer required. Automated 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: De-provision a user account*

1. A request to de-provision 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 de-provisioning 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.

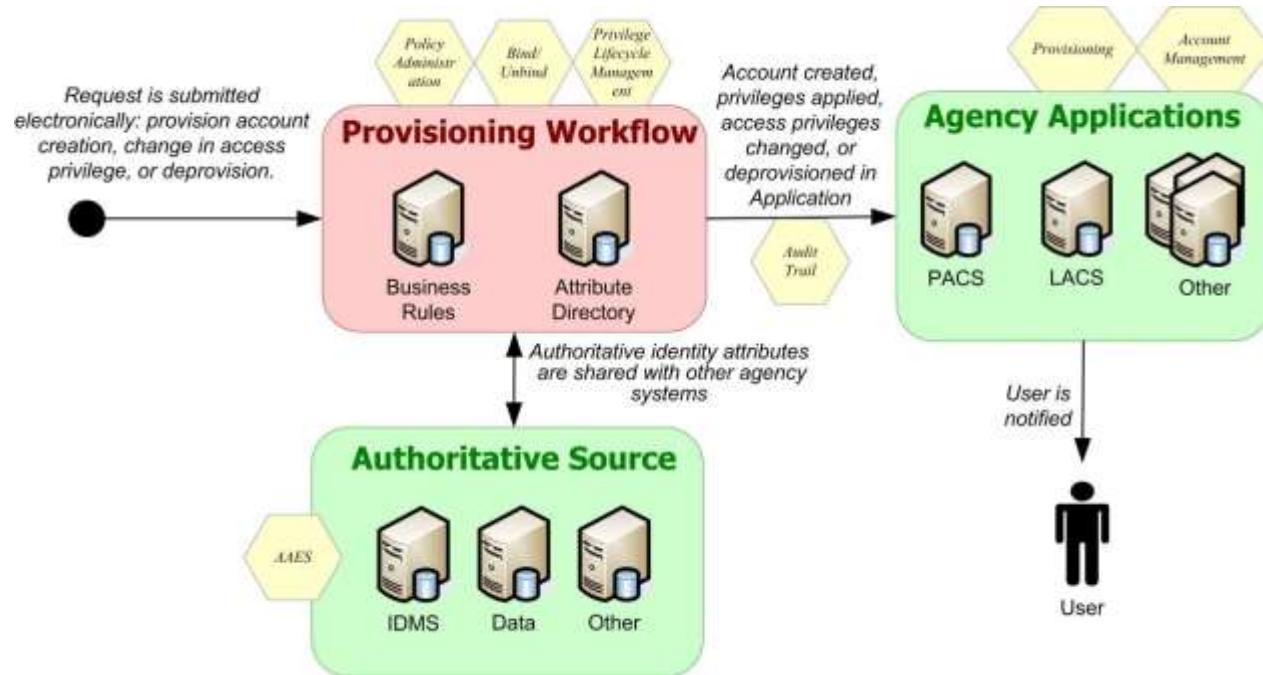


Figure 34: Use Case 7 Target Process Diagram

#### 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 Section 3.2.

Architecture Layer	Architecture Details
<b>Business</b>	<ul style="list-style-type: none"> <li>• <b>E-Government Alignment:</b> IEE, G2G, G2B, G2C</li> <li>• <b>Trigger:</b> <ul style="list-style-type: none"> <li>◦ Part 1: A user requires access to an application</li> <li>◦ Part 2: A user's access need has changed</li> <li>◦ Part 3: A user no longer requires access to the application</li> </ul> </li> <li>• <b>Actors:</b> Individual/User, Privilege Manager, Provisioning Workflow</li> <li>• <b>Endpoint:</b> <ul style="list-style-type: none"> <li>◦ Part 1: A user account is created for the user with the appropriate access privileges</li> <li>◦ Part 2: The user's access privileges are updated to reflect a change in access need</li> <li>◦ Part 3: The user account is deactivated or removed from the application</li> </ul> </li> </ul>
<b>Data</b>	<p><b>Data Elements</b></p> <ul style="list-style-type: none"> <li>• Username</li> <li>• Position</li> <li>• Membership</li> <li>• Access Permission</li> <li>• Roles and Attributes</li> </ul> <p><b>Data Repositories//Systems</b></p> <ul style="list-style-type: none"> <li>• Authoritative agency identity repositories</li> <li>• Application-specific user database</li> </ul>
<b>Service</b>	<ul style="list-style-type: none"> <li>• Authoritative Attribute Exchange (AAES)</li> <li>• Resource Attribute/Metadata Management</li> <li>• Account Management</li> <li>• Bind/Unbind</li> <li>• Provisioning</li> <li>• Privilege Administration</li> <li>• Backend Attribute Retrieval</li> <li>• Policy Administration</li> <li>• Audit Trail</li> </ul>
<b>Technology</b>	<p><b>Hardware/Software</b></p> <ul style="list-style-type: none"> <li>• Standards based provisioning engines</li> </ul> <p><b>Standards</b></p> <ul style="list-style-type: none"> <li>• Backend Attribute Exchange (BAE) Specifications</li> <li>• Lightweight Directory Access Protocol (LDAP) v.2 and v.3;</li> <li>• eXtensible Markup Language (XML)</li> <li>• Security Assertion Markup Language (SAML) 2.0</li> <li>• Service Provisioning Markup Language</li> <li>• Web Services Description Language</li> <li>• Web Service-Federation/Identity –Web Services Framework</li> <li>• Web Services-Interoperability Basis Security Profile</li> </ul>

Figure 35: 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 de-provision users based on established business rules such that a single push can provision/change/de-provision multiple access control points or a user access request can trigger pull-based queries to provision/change/de-provision 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 routine 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 (ACL), 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 ACL 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 Section 3.2.

Architecture Layer	Architecture Details
<b>Business</b>	<ul style="list-style-type: none"> <li>• <b>E-Government Alignment:</b> IEE</li> <li>• <b>Trigger:</b> Cardholder requests access to a facility</li> <li>• <b>Actors:</b> Cardholder, Security Officer</li> <li>• <b>Endpoint:</b> Cardholder granted or denied access</li> </ul>
<b>Data</b>	<p><b>Data Elements</b></p> <ul style="list-style-type: none"> <li>• Agency ID Card Physical Data <ul style="list-style-type: none"> <li>◦ First, Middle, and Last Name</li> <li>◦ Facial Image/Photo</li> <li>◦ Employee Affiliation</li> <li>◦ Organizational Affiliation</li> <li>◦ Expiration Date</li> <li>◦ Agency Card Serial Number</li> <li>◦ Issuer Identification</li> </ul> </li> <li>• Contact or PIV Card Logical Data <ul style="list-style-type: none"> <li>◦ Unique Identifier</li> <li>◦ Electronic Proprietary Unique Identifier</li> </ul> </li> </ul> <p><b>Data Repositories/Systems</b></p> <ul style="list-style-type: none"> <li>• Physical Access Control System (PACS)</li> </ul>
<b>Service</b>	<ul style="list-style-type: none"> <li>• Access Authorization</li> <li>• Data Exchange</li> <li>• Policy Enforcement</li> <li>• Policy Decision</li> <li>• Audit Trail</li> </ul>
<b>Technology</b>	<p><b>Hardware/Software</b></p> <ul style="list-style-type: none"> <li>• Card – contact or contactless</li> <li>• Panel</li> <li>• Reader – 125 kHz or 13.56 MHz</li> <li>• PACS Server</li> </ul> <p><b>Standards</b></p> <ul style="list-style-type: none"> <li>• International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 7810 (card physical structure)</li> <li>• ISO/IEC 10373 (card physical structure)</li> <li>• American National Standards Institute (ANSI) 322 (card physical structure)</li> <li>• ISO/IEC 7816 (contact card specification)</li> <li>• ISO/IEC 14443 (contactless card specification)</li> <li>• ISO/IEC 7811 (magnetic stripe specification)</li> </ul>

Figure 36: 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 NIST SP 800-116.<sup>47</sup> 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

<sup>47</sup> [SP 800-116](#)

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 37 provides a list of PIV authentication mechanisms and their authentication factors.

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

**Figure 37: 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.<sup>48</sup>
- 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<sup>49</sup> 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.
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:

<sup>48</sup> A list of authentication mechanism combinations can be found in Appendix C of [SP 800-116](#).

<sup>49</sup> [SP 800-76](#), Biometric Data Specification for Personal Identity Verification, NIST, January 2007. [SP 800-76]

- a. **CHUID + VIS:** The card reader reads the CHUID from the PIV card and matches it against the ACL. The system also validates the asymmetric signature of the CHUID. In order to achieve single factor authentication, the CHUID read is performed in the presence of the Security Officer to confirm possession of the card.
  - b. **CAK:** Authentication of the PIV 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. **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.
  - d. **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.*
  - e. **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.
  - 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.

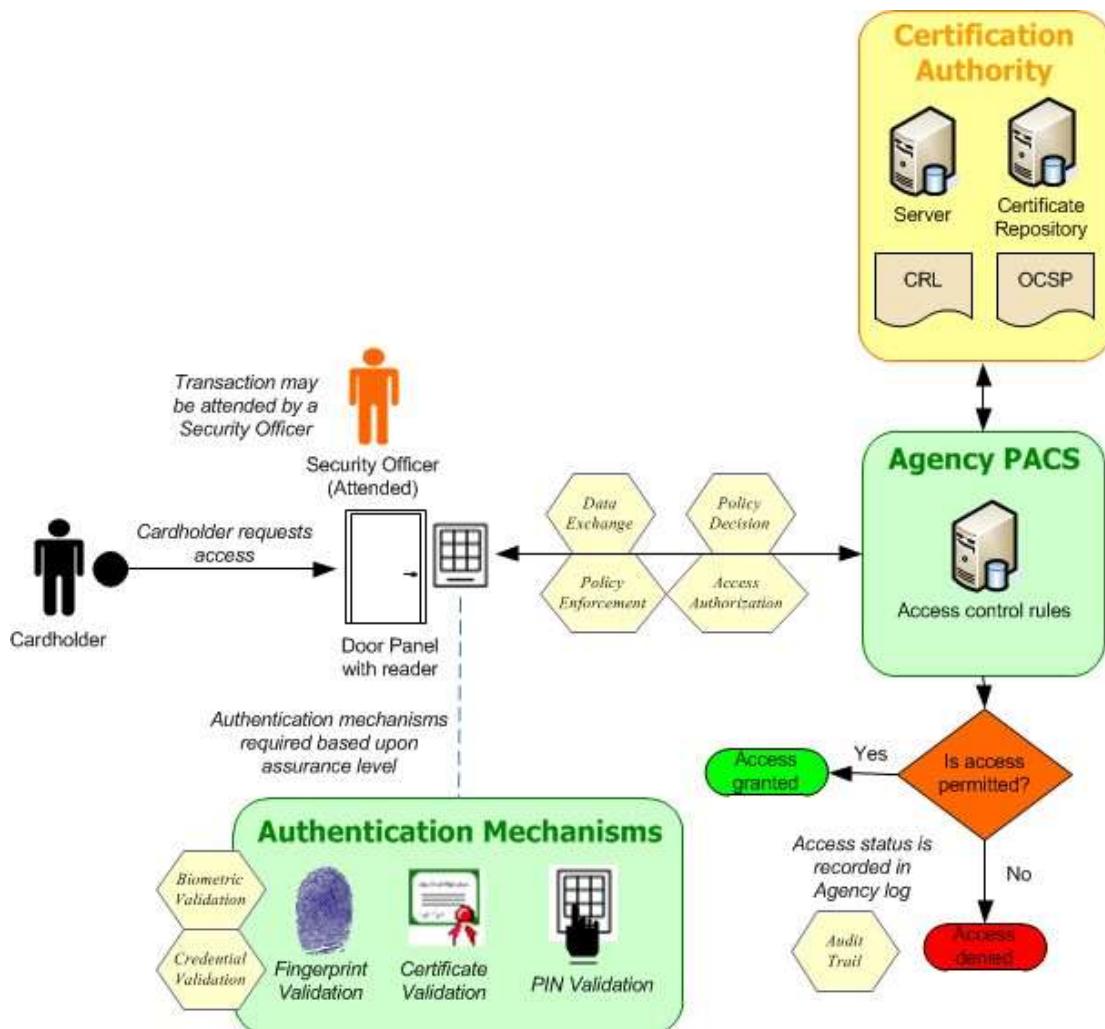


Figure 38: Use Case 8 Target Process Diagram

#### 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 Section 3.2.

Architecture Layer	Architecture Details
<b>Business</b>	<ul style="list-style-type: none"> <li><b>E-Government Alignment:</b> IEE</li> <li><b>Trigger:</b> Cardholder requests access to a facility</li> <li><b>Actors:</b> Cardholder, Security Officer</li> <li><b>Endpoint:</b> Cardholder granted or denied access</li> </ul>
<b>Data</b>	<p><b>Data Elements</b></p> <ul style="list-style-type: none"> <li>PIV Card Physical Data <ul style="list-style-type: none"> <li>○ Security Object</li> <li>○ First, Middle, and Last Name</li> <li>○ Facial Image/Photo</li> <li>○ Employee Affiliation</li> <li>○ Organizational Affiliation</li> <li>○ Expiration Date</li> <li>○ Issuing Authority emblem or ID</li> </ul> </li> </ul>

Architecture Layer	Architecture Details
	<ul style="list-style-type: none"> <li>○ Agency Card Serial Number</li> <li>○ Issuer Identification</li> <li>● PIV Card Logical Data           <ul style="list-style-type: none"> <li>○ Personal identification number (PIN)</li> <li>○ Cardholder Unique Identifier (CHUID)</li> <li>○ Card Authentication Key (CAK) Authentication Data</li> <li>○ Fingerprint Templates</li> </ul> </li> </ul> <p><b>Data Repositories/Systems</b></p> <ul style="list-style-type: none"> <li>● Physical Access Control System (PACS)</li> </ul>
<b>Service</b>	<ul style="list-style-type: none"> <li>● Access Authorization</li> <li>● Data Exchange</li> <li>● Resource Attribute/Metadata Management</li> <li>● Policy Enforcement</li> <li>● Policy Decision</li> <li>● Biometric Validation</li> <li>● Credential Validation</li> </ul>
<b>Technology</b>	<p><b>Hardware/Software</b></p> <ul style="list-style-type: none"> <li>● Card – contact or contactless</li> <li>● Panel</li> <li>● Reader – 13.56 MHz</li> <li>● PACS Server</li> </ul> <p><b>Standards</b></p> <ul style="list-style-type: none"> <li>● International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 7810 (card physical structure)</li> <li>● ISO/IEC 10373 (card physical structure)</li> <li>● American National Standards Institute (ANSI) 322 (card physical structure)</li> <li>● ISO/IEC 7816 (contact card specification)</li> <li>● ISO/IEC 14443 (contactless card specification)</li> <li>● ISO/IEC 7811 (magnetic stripe specification)</li> <li>● Request for Comments (RFC) 3852</li> <li>● FIPS 140 (crypto module for generating cryptographic keys)</li> <li>● SP 800-73</li> <li>● SP 800-76</li> <li>● SP 800-78</li> <li>● SP 800-116</li> </ul>

Figure 39: 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 requirements for electronic authentication outlined in SP 800-116.** Current technologies and processes must be upgraded to ensure electronic authentication of PIV cards and multi-factor authentication as defined in SP 800-116 (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 card 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 (VMS) is 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 the visitor request form into the VMS (in the case of a manual form). The Security Officer confirms the data submitted is valid. The Security 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 VMS. Where manual VMS are in place, the Visitor may enter this information himself into a paper log.
  6. The Visitor presents some form of physical ID (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 Section 3.2.

Architecture Layer	Architecture Details
<b>Business</b>	<ul style="list-style-type: none"> <li>• <b>E-Government Alignment:</b> IEE, G2G, G2C, G2B</li> <li>• <b>Trigger:</b> A Visitor requires access to a facility</li> <li>• <b>Actors:</b> Visitor, Sponsor, Security Officer</li> <li>• <b>Endpoint:</b> temporary access granted to facility/building</li> </ul>
<b>Data</b>	<p><b>Data Elements</b></p> <ul style="list-style-type: none"> <li>• Access Request Form <ul style="list-style-type: none"> <li>◦ Visitor Name</li> <li>◦ Social Security Number (SSN)</li> <li>◦ Citizenship</li> <li>◦ Affiliation</li> <li>◦ Date and time of visit</li> <li>◦ Campus/building/room to be visited</li> <li>◦ Entry point of visitor</li> <li>◦ Point of contact's name, phone number and email</li> <li>◦ Point of contact's campus/building/room</li> <li>◦ Escort name and contact number</li> <li>◦ Purpose of visit</li> <li>◦ Clearance required</li> </ul> </li> <li>• Access Log Book <ul style="list-style-type: none"> <li>◦ Visitor Name</li> <li>◦ Date</li> <li>◦ Sign-in time</li> <li>◦ Sign-out time</li> <li>◦ Visitor Signature</li> <li>◦ Agency/Company representing</li> <li>◦ Sponsor signature</li> </ul> </li> <li>• Temporary/Visitor Badge/Card <ul style="list-style-type: none"> <li>◦ Facial Image/Photo</li> <li>◦ Organizational Affiliation</li> <li>◦ Temporary/Visitor identification</li> <li>◦ Agency Card Serial Number</li> </ul> </li> </ul>

Architecture Layer	Architecture Details
	<ul style="list-style-type: none"> <li>○ Issuer Identification</li> <li>○ Unique identifier (if card provides electronic access)</li> <li>● Other forms of identification           <ul style="list-style-type: none"> <li>○ Driver's license</li> <li>○ Military ID</li> <li>○ Other agency identity card (see Use case 8 architecture analysis for more specific data elements)</li> </ul> </li> </ul> <p><b>Data Repositories/Systems</b></p> <ul style="list-style-type: none"> <li>● Visitor Management System (VMS)</li> <li>● NCIC</li> </ul>
<b>Service</b>	<ul style="list-style-type: none"> <li>● Account Management</li> <li>● Bind/Unbind</li> <li>● Provisioning</li> <li>● Privilege Lifecycle Management</li> <li>● Sponsorship</li> <li>● Credential Validation</li> <li>● Access Authorization</li> <li>● Policy Administration</li> <li>● Policy Enforcement</li> <li>● Policy Decision</li> <li>● Audit Trail</li> </ul>
<b>Technology</b>	<p><b>Hardware/Software</b></p> <ul style="list-style-type: none"> <li>● Badge</li> <li>● Badge processing system/software</li> <li>● Metal detector or other security mechanisms</li> <li>● Graphical User Interface to Management System</li> </ul> <p><b>Standards</b></p> <ul style="list-style-type: none"> <li>● International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 7810 (card physical structure)</li> <li>● ISO/IEC 10373 (card physical structure)</li> <li>● American National Standards Institute (ANSI) 322 (card physical structure)</li> <li>● ISO/IEC 7816 (contact card specification)</li> </ul>

**Figure 40: 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 credentials into the PACS and perform electronic authentication.

For individuals who require 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 an alternate card type, subject to agency or facility security policies. It is desirable that this alternate card be technically compatible with, but physically and electronically distinct from,<sup>50</sup> the PIV card to allow for access to local facilities through electronic authentication mechanisms.

<sup>50</sup> As required by [M-05-24](#).

Key assumptions for this use case include:

- An electronic VMS is 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 SSP 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 VMS. 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-I 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 VMS.
7. The Visitor provides some form of physical ID, which is validated using one of the following methods:
  - a. If the Visitor does not possess a PIV or PIV-I 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-I 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-I card, it may also be inserted into a reader that checks against either a CRL or OCSP via the Federal Bridge infrastructure. If the PIV 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 an alternate card type to be used for physical access.
4. On each occasion that the Individual arrives to the facility to gain access, the alternate card type 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.

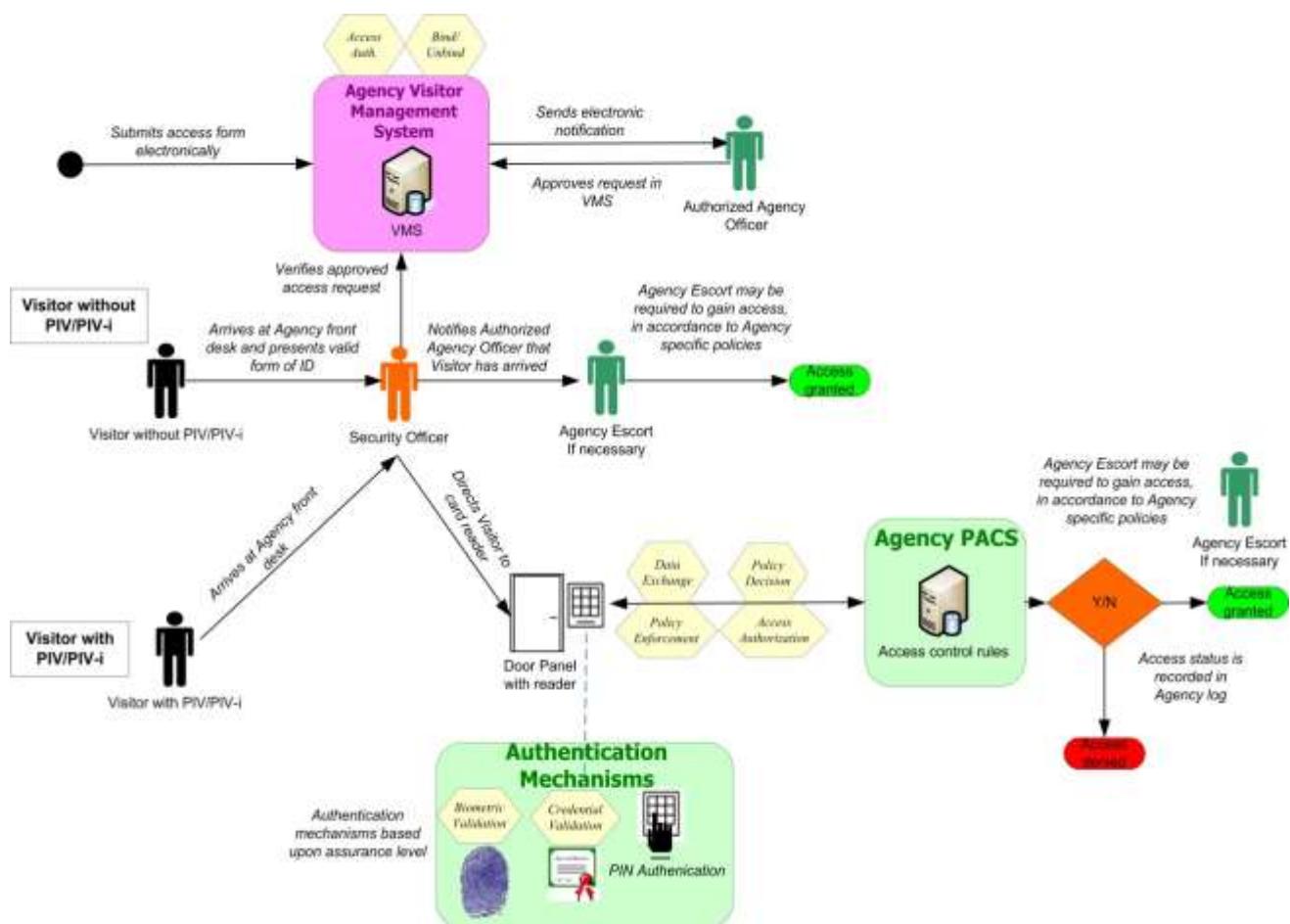


Figure 41: Use Case 9 Target Process Diagram

#### 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 Section 3.2.

Architecture Layer	Architecture Details
<b>Business</b>	<ul style="list-style-type: none"> <li><b>E-Government Alignment:</b> IEE, G2G, G2B, G2C</li> <li><b>Trigger:</b> Visitor needs to access a facility</li> <li><b>Actors:</b> Visitor, Sponsor, Security Officer</li> <li><b>Endpoint:</b> Temporary access granted</li> </ul>
<b>Data</b>	<p><b>Data Elements</b></p> <ul style="list-style-type: none"> <li>Access Request Form (some combination of)             <ul style="list-style-type: none"> <li>Visitor Name</li> <li>Social Security Number (SSN)</li> <li>Citizenship</li> <li>Affiliation</li> <li>Date and time of visit</li> <li>Campus/building/room to be visited</li> <li>Entry point of visitor</li> <li>Point of contact's name, phone number and email</li> <li>Point of contact's campus/building/room</li> <li>Escort name and contact number</li> <li>Purpose of visit</li> </ul> </li> </ul>

Architecture Layer	Architecture Details
	<ul style="list-style-type: none"> <li>○ Clearance required</li> <li>● Temporary/Visitor Badge/Card (some combination of)             <ul style="list-style-type: none"> <li>○ Facial Image/Photo</li> <li>○ Organizational Affiliation</li> <li>○ Temporary/Visitor identification</li> <li>○ Agency Card Serial Number</li> <li>○ Issuer Identification</li> <li>○ Unique identifier (if card provides electronic access)</li> </ul> </li> <li>● Other forms of identification             <ul style="list-style-type: none"> <li>○ Driver's license</li> <li>○ Military ID</li> <li>○ Employee ID Card</li> <li>○ Other agency badge/card (see Use case 8 architecture analysis for more specific data elements)</li> </ul> </li> <li>● PIV Card Physical Data             <ul style="list-style-type: none"> <li>○ First, Middle, and Last Name</li> <li>○ Facial Image/Photo</li> <li>○ Employee Affiliation</li> <li>○ Organizational Affiliation</li> <li>○ Expiration Date</li> <li>○ Agency Card Serial Number</li> <li>○ Issuer Identification</li> </ul> </li> <li>● PIV Card Logical Data             <ul style="list-style-type: none"> <li>○ Unique Identifier                     <ul style="list-style-type: none"> <li>■ Electronic Proprietary Unique Identifier OR</li> <li>■ Cardholder Unique Identifier (CHUID)</li> <li>■ Card Authentication Key (CAK) Certificate</li> <li>■ PIV Authentication Certificate</li> </ul> </li> </ul> </li> </ul> <p><b>Data Repositories/Systems</b></p> <ul style="list-style-type: none"> <li>● Visitor Management System (VMS)</li> <li>● National Crime Information Center (NCIC)</li> <li>● Physical Access Control System (PACS)</li> </ul>
<b>Service</b>	<ul style="list-style-type: none"> <li>● Account Management</li> <li>● Bind/Unbind</li> <li>● Provisioning</li> <li>● Privilege Lifecycle Management</li> <li>● Resource Attribute/Metadata Management</li> <li>● Sponsorship</li> <li>● Credential Validation</li> <li>● Access Authorization</li> <li>● Policy Administration</li> <li>● Policy Enforcement</li> <li>● Policy Decision</li> <li>● Audit Trail</li> <li>● Credential Validation</li> <li>● Federation</li> <li>● Self-Service</li> </ul>
<b>Technology</b>	<p><b>Hardware/Software</b></p> <ul style="list-style-type: none"> <li>● Badge</li> <li>● Badge processing system/software</li> <li>● Metal detector or other security mechanisms</li> </ul> <p><b>Standards</b></p> <ul style="list-style-type: none"> <li>● International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 7810 (card physical structure)</li> <li>● ISO/IEC 10373 (card physical structure)</li> <li>● American National Standards Institute (ANSI) 322 (card physical structure)</li> <li>● ISO/IEC 14443 (contactless card specification)</li> </ul>

Architecture Layer	Architecture Details
	<ul style="list-style-type: none"><li>• Request for Comments (RFC) 3852 (Asymmetric Digital Signature Syntax)</li><li>• SP 800-78 (Asymmetric Signature algorithm and key size requirements)</li></ul>

Figure 42: 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-I credentials from visitors.** PACS should make use of PIV and PIV-I credentials (including certificate checks for level 4 access points) for cross-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 one-time password generator;
- An approved and internally-issued PKI soft certificate;
- Biometric matching;
- A trusted smart card;
- Universal serial bus (USB) tokens and other hardware tokens holding PKI certificates;
- A trusted externally issued PKI soft certificate; and
- 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 (SSO) 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 Section 3.2.

Architecture Layer	Architecture Details
<b>Business</b>	<ul style="list-style-type: none"> <li>• <b>E-Government Alignment:</b> IEE, G2G, G2C, G2B</li> <li>• <b>Trigger:</b> User requests access to a logical resource</li> <li>• <b>Actors:</b> User, Application</li> <li>• <b>Endpoint:</b> Approval/denial of User Access Request</li> </ul>
<b>Data</b>	<p><b>Data Elements</b></p> <ul style="list-style-type: none"> <li>• One-time password data</li> <li>• Biometric data</li> <li>• Attribute and privilege data</li> <li>• Contact Card Logical Data</li> </ul>

Architecture Layer	Architecture Details
	<ul style="list-style-type: none"> <li>○ Unique Identifier</li> <li>○ Electronic Proprietary Unique Identifier</li> </ul> <p><b>Data Repositories/Systems</b></p> <ul style="list-style-type: none"> <li>● Logical Access Control System (LACS)</li> <li>● Domain Controller</li> <li>● Local Application</li> </ul>
<b>Service</b>	<ul style="list-style-type: none"> <li>● Credential Validation</li> <li>● Biometric Validation</li> <li>● Session Management</li> <li>● Data Exchange</li> <li>● Access Authorization</li> <li>● Policy Administration</li> <li>● Policy Decision</li> <li>● Policy Enforcement</li> </ul>
<b>Technology</b>	<p><b>Hardware/Software</b></p> <ul style="list-style-type: none"> <li>● Smart Card – contact</li> <li>● Information Card or other third-party credentials</li> <li>● PKI certificates           <ul style="list-style-type: none"> <li>○ Universal serial bus (USB) tokens containing PKI certificates</li> <li>○ Soft Certificates</li> <li>○ PKI certificates on PIV cards</li> </ul> </li> <li>● One-time password generators</li> <li>● Directory Services</li> <li>● Domain Controller</li> <li>● Card reader</li> <li>● Computer terminal           <ul style="list-style-type: none"> <li>○ LACS Server</li> <li>○ Network and other Applications</li> </ul> </li> </ul> <p><b>Standards</b></p> <ul style="list-style-type: none"> <li>● International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 7816 (contact card specification)</li> <li>● Request for Comments (RFC) 3852 (Asymmetric Digital Signature Syntax)</li> <li>● Interface specifications between the service and Identity Providers</li> <li>● Lightweight Directory Access Protocol (LDAP) v.2 and v.3</li> <li>● Security Assertion Markup Language (SAML)</li> <li>● eXtensible Access Control Markup Language (XACML)</li> <li>● Windows NT 4.0 networking application programming interfaces (APIs)</li> <li>● Replication Simple Mail Transfer Protocol (SMTP)</li> </ul>

Figure 43: 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 card authentication digital credential, to grant access to applications at all levels of assurance. A key goal is enabling SSO 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 provider. Over time, it is anticipated that certain external users within the G2G and G2B sectors will possess PIV-I 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 M-04-04 and SP 800-63.

Achieving the target state goals requires the following architectural changes:

- Implementing LACS. A flexible centrally managed agency LACS is required to layer attributes and permissions, and map those to the authentication mechanism to make access decisions for all agency applications, including legacy.
- Enabling Federation. The target state will require agreement on versions, technologies, formats, and oversight mechanisms to transfer and trust identities and credentials across agency boundaries and with external entities. Establishing Trusted Identity Providers and similar mechanisms will enable service providers to make access decisions based on defined levels of trust.
- Fully enabling use of the PIV and PIV-I 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-I 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 credential using one or a combination of the following authentication mechanisms available on the card and the appropriate authentication techniques:<sup>51</sup>

---

<sup>51</sup> A detailed description of how authentication is performed using the PIV mechanisms can be found in [SP 800-73-3](#), Part 1, Appendix B.

- a. PIV Authentication Key
- b. 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 an 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 Identity Provider (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.

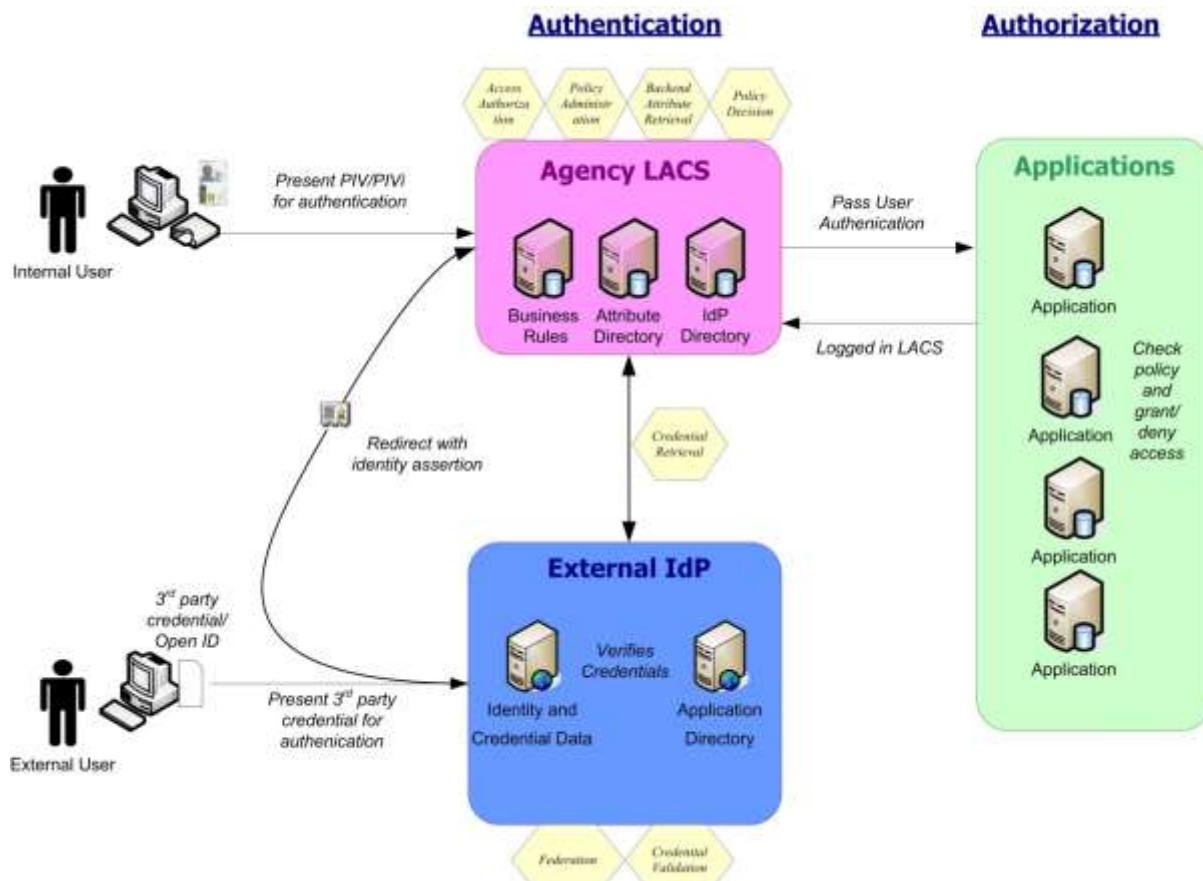


Figure 44: Use Case 10 Target Process Diagram

#### 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 Section 3.2.

Architecture Layer	Architecture Details
<b>Business</b>	<ul style="list-style-type: none"> <li><b>E-Government Alignment:</b> IEE, G2G, G2C, G2B</li> <li><b>Trigger:</b> User requests access to a logical resource</li> <li><b>Actors:</b> User, Credential or Identity Providers (IdPs), Registration Authority (RA), Trust Brokers, Attribute Authorities</li> <li><b>Endpoint:</b> Approval of User Access Request</li> </ul>
<b>Data</b>	<p><b>Data Elements</b></p> <ul style="list-style-type: none"> <li>Unique Identifier           <ul style="list-style-type: none"> <li>PKI: PIV Authentication certificate</li> <li>Biometric Templates</li> </ul> </li> </ul> <p><b>Data Repositories/Systems</b></p> <ul style="list-style-type: none"> <li>Logical Access Control System (LACS)</li> <li>Attribute databases</li> </ul>
<b>Service</b>	<ul style="list-style-type: none"> <li>Resource Attribute/Metadata Management</li> <li>Credential Retrieval</li> <li>Backend Attribute Retrieval</li> <li>Credential Validation</li> <li>Biometric Validation</li> <li>Session Management</li> </ul>

Architecture Layer	Architecture Details
	<ul style="list-style-type: none"> <li>• Federation</li> <li>• Access Authorization</li> <li>• Data Exchange</li> <li>• Policy Administration</li> <li>• Policy Decision</li> <li>• Policy Enforcement</li> </ul>
<b>Technology</b>	<p><b>Hardware/Software</b></p> <ul style="list-style-type: none"> <li>• 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 Task Force Report</li> <li>• Smart Card – contact</li> <li>• PKI certificates <ul style="list-style-type: none"> <li>◦ Universal serial bus (USB) tokens containing PKI certificates</li> <li>◦ Soft Certificates</li> <li>◦ PKI certificates on PIV cards</li> </ul> </li> <li>• One-time password generators</li> <li>• Personal digital assistants</li> <li>• Locally managed computer</li> <li>• Externally hosted computer</li> <li>• Unknown Internet Protocol (IP) network devices</li> <li>• Server(s)</li> <li>• Domain Controller</li> <li>• Card reader</li> <li>• Computer terminal</li> <li>• LACS Server</li> <li>• Network and other Applications</li> </ul> <p><b>Standards</b></p> <ul style="list-style-type: none"> <li>• International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 7816 (contact card specification)</li> <li>• Request for Comments (RFC) 3852 (Asymmetric Digital Signature Syntax)</li> <li>• SP 800-78 (Asymmetric Signature algorithm and key size requirements)</li> <li>• Interface specifications between the service and Identity Providers</li> <li>• Lightweight Directory Access Protocol (LDAP) v.2 or newer</li> <li>• Security Assertion Markup Language (SAML)</li> <li>• eXtensible Access Control Markup Language (XACML)</li> <li>• Windows NT 4.0 networking application programming interfaces (APIs) or newer</li> <li>• Replication Simple Mail Transfer Protocol (SMTP)</li> <li>• Backend Attribute Exchange (BAE) Interface Specifications</li> <li>• Secure Socket Layer (SSL)</li> <li>• Hypertext Transfer Protocol (HTTP)</li> <li>• Web Service (WS)-Security <ul style="list-style-type: none"> <li>◦ Simple Object Access Protocol (SOAP)</li> </ul> </li> </ul>

**Figure 45: 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 Identity Providers, 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 card 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 (BAE) 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 GPEA 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 (Lightweight Directory Access Protocol [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 46 represents Part 1 of the process flow.

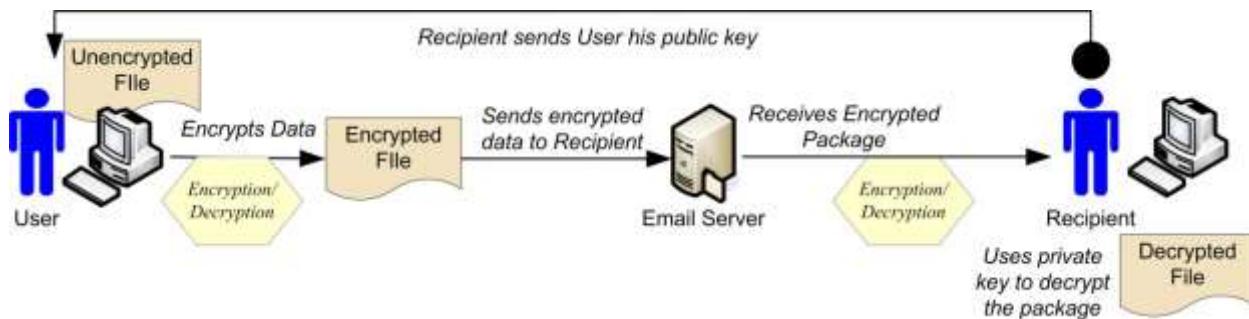


Figure 46: Use Case 11 Target Process Diagram (Encryption)

Figure 47 represents Part 2 of the process flow.

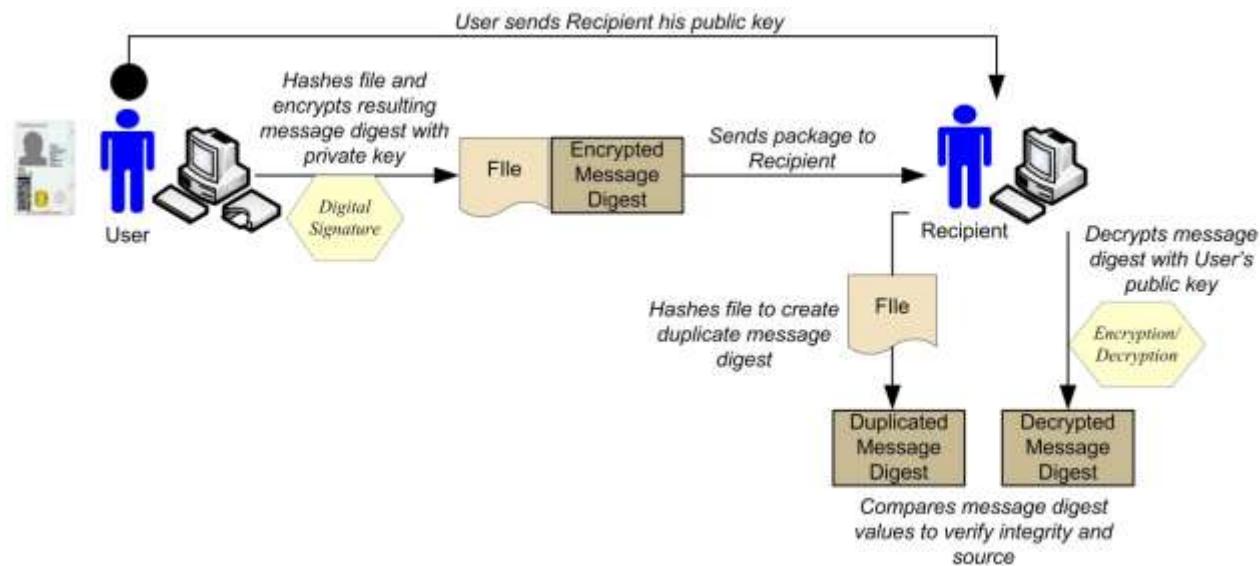


Figure 47: Use Case 11 Target Process Diagram (Digital Signature)

#### 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 Section 3.2.

Architecture Layer	Architecture Details
<b>Business</b>	<ul style="list-style-type: none"> <li><b>E-Government Alignment:</b> IEE, G2G, G2B, G2C</li> <li><b>Trigger:</b> User must sign or encrypt a document or message</li> <li><b>Actors:</b> Certification Authority (CA), Sender (Signatory), Receiver (Verifier)</li> <li><b>Endpoint:</b> Receiver decrypts document or verifies digital signature</li> </ul>
<b>Data</b>	<p><b>Data Elements</b></p> <ul style="list-style-type: none"> <li>PKI Certificates and Keys</li> <li>Hashes</li> <li>Security Object</li> </ul> <p><b>Data Repositories/Systems</b></p> <ul style="list-style-type: none"> <li>PKI directories</li> <li>Local Application Certificate Cache</li> </ul>

Architecture Layer	Architecture Details
<b>Service</b>	<ul style="list-style-type: none"> <li>• Encryption/Decryption</li> <li>• Digital Signature</li> <li>• Path Discovery and Validation (PDVAL)</li> <li>• Key Management</li> <li>• Audit Trail</li> </ul>
<b>Technology</b>	<p><b>Hardware/Software</b></p> <ul style="list-style-type: none"> <li>• Federal Bridge Certification Authority (FBCA)</li> <li>• Email applications</li> <li>• Document applications enabled to be used with external encryption</li> </ul> <p><b>Standards</b></p> <ul style="list-style-type: none"> <li>• Federal Bridge Common Policy</li> <li>• FIPS 186</li> <li>• FIPS 180</li> <li>• eXtensible Markup Language (XML)</li> <li>• Triple Data Encryption Standard (Triple DES)</li> <li>• Advanced Encryption Standard (AES)</li> <li>• SP 800-67</li> <li>• SP 800-78</li> <li>• Elliptic Curve Digital Signature Algorithm (ECDSA)</li> <li>• Secure Hash Algorithms (SHA)</li> <li>• Rivest, Shamir and Adleman (RSA)</li> <li>• International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 18033-3:2005</li> <li>• X.509 Certificate Revocation Lists (CRLs)</li> <li>• Online Certificate Status Protocol (OCSP)</li> </ul>

**Figure 48: 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 fundamental 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 HR. 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:** HR personnel, Personnel Security Office, Provisioning Engine, Authoritative Attribute Exchange Service (AAES), Agency Contractor/New Employee, PIV Office Personnel, Security Officer at the local facility

#### **Process Flow:**

1. An offer to hire is proffered to an Agency Contractor (hereafter referred to as a New Employee).
2. HR 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 AAES 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 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 credential as a Federal employee.
13. Applications such as SharePoint and Virtual Private Network (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 Security Officer at the local facility 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 AAES.

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 AAES 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 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-I credentials. Some responders will use a PIV credential (in this case, the Department of Defense (DoD) Common Access Card or CAC) while others will use a PIV-I card (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 Hazardous Waste Operations 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-I 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 smart card reader, thus provisioning the user accounts into the perimeter access control system. The Headquarters Guard applied all the approved rights and attributes 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 BAE 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-I 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 DoD) 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 LOA 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. The first application requires a level 3 token to access and report official trial data. The second application requires level 1 authentication as it is only used to create a personalized search page of public data not otherwise requiring authentication for access. In addition, the first application requires 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 Organizational 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 —softPKI 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.<sup>52</sup>

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 LOA 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, a real-time verification against the medical partner's user data, using the BAE 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).

#### **4.12.4. G2C: Citizen Services**

**Scenario:** A citizen leverages an existing external 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. The user

---

<sup>52</sup> 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.

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™.

**Actors:** Citizen, Provisioning Engine, MySpace™, 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 Research Website.
3. The Research 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™ 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™ authentication services.
6. When authenticating to the grant application in the future, the application requires that the MySpace™ system verify the password token. The agency application (relying party) accepts assertions from MySpace™ (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™ 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 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 going forward in their budget submissions.
- **Performance Metrics.** Defines government-wide performance metrics, a main 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 Backend Attribute Exchange (BAE) common data elements or other shared attribute exchange models to support data sharing of common, mission-specific identity attributes outside of the 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 Attribute Exchange Service (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 for a 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 process 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 card 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 de-provision 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 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 (PIV-I) credentials from visitors.	Enable the use of PIV and PIV-I 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 BAE 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 credential to further encryption and digital signature usage.

**Figure 49: 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 primary 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 National Information Exchange Model (NIEM) or Universal Core (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-Shared Infrastructure Provider [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 Backend Attribute Exchange (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 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 the PIV credential 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, Controlled Unclassified Information (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 Authoritative Attribute Exchange Service (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 non-person entities (NPEs).	RDT	12/31/2009
1.17	Engage privacy community, DOJ, and industry groups to address any perceived liability associated with Identity Provider services.	ICAMSC	03/31/2010

Figure 50: 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 a 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 the scheme adoption process for authentication technologies acceptable at Levels of Assurance (LOA) 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 51: 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 the SP 800-116 maturity model into the transition plan template for ICAM tracking/reporting.	OMB	12/31/2009
3.2	Create an 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 (e.g., PIV-interoperable) credentials.	RDT and ISC Convergence Committee	12/31/2009
3.6	Develop Performance Reference Model (PRM) mapping for ICAM performance architecture.	RDT	03/30/2010

Figure 52: 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 Central Verification System (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 card 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 53: 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-I 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-I 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 LACS 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 may be tracked using the ICAM Transition Plan template being developed as part of government-wide activity 3.2. OMB reserves the right to request periodic updates on implementation progress. 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 the Backend Attribute Exchange (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 Authoritative Attribute Exchange Service (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 card 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 54: 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-I 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 use of PIV credentials.	Federal Executive Branch Agencies	12/31/2010
6.2	Develop guidance recommending the use of PIV credentials for authentication at all levels by internal users and requiring agencies to issue internal policy on the use of PIV credentials.	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 (PACS) 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-I 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-I issuers.	AWG	12/31/2009

**Figure 55: 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<sup>53</sup> 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 Physical Access Control System (PACS) process and technology upgrades to ensure electronic authentication of PIV cards and multi-factor authentication as defined in 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 Universal Core or National Information Exchange Model (NIEM) to increase interoperability.	Federal Executive Branch Agencies	9/30/2011
7.7	Using the guidance provided in 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-I credentials into PACS, following the SP 800-116 guidance.	Federal Executive Branch Agencies	9/20/2011

Figure 56: 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

<sup>53</sup> [Section 508](#) of the Rehabilitation Act.

Activity No.	Transition Activity	Activity Owner	Implementation Milestone Date
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
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 57: 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 58: Initiative 9 Transition Activity Summary

#### **5.2.3. Implementation Sequencing Plan**

The sequencing plan provides an aggregated view of key life cycle activities and associated duration estimates for two of the key activity areas for the target state, modernizing PACS and LACS. Sections 10.1.4 and 11.1.3 provide the sequencing plans for PACS and LACS solutions, respectively. The ICAM sequencing plan provides a baseline, which encompasses common activities across a standard system development life cycle. It is expected that agencies will need to tailor the sequencing plan into a detailed work breakdown structure based on their specific implementation approach, technology factors, and organizational size and objectives.

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, going forward.

### **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 Physical Access Control System (PACS) and Logical Access Control System (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 de-provision 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

Item No.	Strategic Goal Supported	Objectives Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	End State Target
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%
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 (for Revocation and Suspension (measured from the certification authority's [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%

Item No.	Strategic Goal Supported	Objectives Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	End State Target
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%
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 PACS implemented in accordance with SP 800-116.	100%

Item No.	Strategic Goal Supported	Objectives Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	End State Target
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%
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 personal identification number (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

Item No.	Strategic Goal Supported	Objectives Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	End State Target
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%
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 59: 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.

This page is intentionally left blank.

## How to Read and Use Part B: Implementation Guidance

Part A of this document introduces the ICAM segment architecture, which provides federal agencies with a standards-based approach that outlines a cohesive target state to ensure clarity and interoperability across agency-level initiatives. As stated in OMB M-11-11, agency transition plans for requiring the use of the PIV credentials as the common means of authentication to facilities, networks, and information systems must align with the ICAM segment architecture. Alignment involves modifying or applying new business processes, program administration, and technology solutions across an agency. Part B dedicates a chapter to each of the agency-level initiatives described in Chapter 5 and explains the activities required to align with the ICAM segment architecture and meet the target state.

This section of the document addresses elements to help read, understand, and apply the guidance provided in Part B.

### Content Covered

Part B provides guidance on a broad range of topics to enable a holistic approach for alignment with the ICAM segment architecture. The discussions in Part B are based on industry and government best practices as well as examples from agency ICAM programs. In each chapter, the guidance addresses the following specific areas:

- **Program planning and management.** Planning and management are critical to the execution of any initiative and, as such, are a main focus of Part B. Chapter 6 addresses general ICAM implementation planning considerations while each subsequent chapter discusses the key decision points and activities across the life cycle of the individual efforts, for example, PACS modernization.
- **Sample solution architectures for key ICAM capabilities.** An agency may need to modify an existing technology solution or implement a new technology capability to fulfill the activities identified in the segment architecture. To assist ICAM implementers in this effort, Part B provides solution architectures and outlines the supporting components and common design characteristics for the sample solutions.
- **Implementation patterns and considerations.** To add specificity to high-level concepts and help an agency make appropriate ICAM-related decisions, Part B discusses common approaches for achieving the target state and outlines the associated factors for consideration throughout its ICAM implementation.
- **Approaches for resolving common implementation challenges.** As agencies have begun executing their ICAM programs, they have identified a variety of technical and process implementation challenges. Part B provides guidance and lessons learned that an agency may leverage as they tackle some of the common challenges.

### Content Presentation

The guidance provided in Part B covers a broad range of topics and includes a great deal of content to adequately assist ICAM implementers in addressing each of the agency-level initiatives. In order to make the guidance easier to navigate, Part B contains structural tools and techniques to help direct and focus the reader's attention, including:

- **Specific audiences.** As noted in Section 1.2, the primary audience for the FICAM Roadmap is Federal Government ICAM implementers at all stages of program planning,

design, and implementation. This is a broad audience, encompassing individuals with a wide variety of background knowledge and job responsibilities. For this reason, many of the sections in Part B have been developed to focus on content more relevant to a specific role, such as program leadership or technical resources. In these cases, the particular audience and the key topics addressed are identified in the beginning of the section.

- **References to other efforts and relevant documentation.** As part of the government-wide level governance initiatives (See Section 5.2.1), the ICAMSC and its supporting working groups have undertaken multiple efforts to supplement ICAM policy and guidance to agencies and develop processes and specifications to support interoperability and trust. In order to manage the length of this document, the guidance addresses these efforts by reference, describing how to use those work products in the context of the broader guidance and providing citations and links to the source where appropriate.
- **Use of call out boxes.** The narrative portions of the guidance in Part B are high-level and focus on sample solutions and implementation patterns to help an agency with its decision making. To clarify the general concepts throughout the document or provide specific, real-world examples of particular programs, approaches, or decisions that have been successful in agency implementations, Part B uses call out boxes. There are six different types of call out boxes, each with a different focus, including: Implementation Tip, Lesson Learned, Terminology, Privacy Tip, Frequently Asked Question (FAQ), and return on investment (ROI). Look for call out boxes like this one throughout Part B:

FAQ	What is the difference between General Services Administration (GSA) Schedules and the Approved Products List (APL)? GSA Schedules are purchasing vehicles for a broad range of products and services. The resources available on the GSA Schedules have pre-approved vendors and pre-negotiated rates. The APL is a list of Homeland Security Presidential Directive 12 (HSPD-12) related products and services that have been tested per an approved NIST test procedure. An agency can use the GSA Schedules to purchase a resource that is included on the APL.	?
-----	--	---

- **Inclusion of benefits and limitations.** Where more than one approach may be viable to meet the requirements of the ICAM target state, the document summarizes the benefits and limitations of each approach presented. This allows an agency to make informed decisions and choose approaches that are a good fit with their ICAM program.

## Use of Terminology

Part B includes several words that may have multiple meanings or connotations in common use or other contexts; however, they are intended to convey a specific meaning with relation to the execution of the ICAM segment architecture. In order to prevent confusion when reading the guidance, the following definitions should be observed:

- **Enterprise.** Refers to a department or agency. A key characteristic of the target state is the implementation of streamlined, common ICAM services at the agency level. Many of the concepts and capabilities throughout the guidance are referred to as —enterprise-wide. In these instances, it is expected that an agency will coordinate and streamline the functionality across an agency’s bureaus/components to the extent practicable to support efficiencies and cost savings.

- **ICAM Program.** Refers to the structure and activities within an agency that support alignment with the functional areas of the ICAM segment architecture. These functional areas and individual efforts may be managed via a single program structure or within multiple offices/management structures, so long as they are managed in a coordinated way.
- **Project or Initiative.** Refers to a discrete effort to produce a particular ICAM service or achieve a particular agency-level initiative in support of an agency's overall ICAM program (e.g., the modernization of LACS). An agency may have a separate management team and investment funding to execute a project, depending on how the ICAM program is structured.
- **Should vs. Must.** This document provides guidance and recommendations to assist agencies in aligning with the ICAM segment architecture. As such, the document uses the word —should— to denote a preferred approach or a leading best practice where an agency has multiple options to complete an agency-level initiative. Where the guidance addresses existing policy or technical requirements, it uses the word —must— to denote that the approach described is not optional.

## ***Utilizing the Implementation Guidance***

Part B provides high level guidance and considerations that are regarded as applicable at any agency to help achieve the target state defined in the ICAM segment architecture. It is acknowledged that each agency will differ in its specific needs, mission, and ICAM program maturity, which will affect the decisions it makes when implementing the ICAM segment architecture. As such, Part B was developed to include a variety of approaches that can be tailored by an agency to make the appropriate decisions for its ICAM program. The following list provides some of the ways that an agency can get the most out of Part B:

- **Disseminate guidance across functional areas.** Part B provides guidance on activities and considerations that affect many different projects and stakeholders throughout an agency. To fully utilize Part B, an agency should share the guidance with implementers in the various functional areas that support an agency's ICAM program. This will allow all relevant stakeholders to be aware of their responsibilities and the role they play in helping their agency align with the ICAM segment architecture.
- **Determine steps to align with the guidance.** Part B provides holistic guidance to complete the agency-level initiatives in the ICAM segment architecture. It is expected that each agency is at a different stage of program maturity and likely has existing projects and investments related to the guidance provided. An agency should determine the degree to which their agency is currently in alignment and identify the necessary steps to close gaps where they exist.
- **Perform analysis to select the best approach.** As mentioned throughout this section, Part B provides a number of options for how an agency can achieve the target state. Because every agency is different in its needs and mission, an agency should perform analysis (e.g., cost/benefit) to determine the most suitable approach.
- **Make decisions and drive change.** Part B is offered to serve as catalyst for agencies to identify and take the necessary steps to improve efficiency and security in their ICAM program. An agency should strive to quickly implement the changes to management approaches, business processes, and technologies to move on the appropriate migration path towards the target state defined in the ICAM segment architecture.

This page is intentionally left blank.

## 6. ICAM Implementation Planning

This chapter provides guidance for planning and establishing an ICAM program within a federal agency. It is expected that agencies have general lifecycle methodologies that they employ to plan and execute programs. The guidance provided in this chapter is intended to supplement these life cycle methodologies and introduce ICAM specific agency-level planning considerations that drive the overall success and adoption of the ICAM segment architecture within the Federal Government.

Chapter 6 has been divided into three elements:

- **Program Organization and Management.** This section discusses the establishment of ICAM governance bodies to manage and oversee complex ICAM programs within an agency; suggests stakeholder management and communication strategies for engaging and collaborating with the wide array of stakeholders involved in ICAM implementations; and provides risk management guidance proven to successfully mitigate the level of risk to agencies implementing ICAM programs.
- **Incorporating ICAM into Existing Agency Processes.** This section discusses how agencies should integrate ICAM into the capital planning, accountability, acquisition, and security processes that are performed for all government programs.
- **Privacy Considerations.** This section discusses privacy as one of the key drivers behind the ICAM initiative and introduces guidance for ensuring the privacy of sensitive information that is inherently contained within the various programs that fall under ICAM.

### 6.1. Program Organization and Management

ICAM is a key enabler across the federal enterprise and within specific agency programs and mission areas; therefore, it is imperative that federal agencies properly organize and manage ICAM efforts. This section provides guidance on how an agency can establish effective governance structures, collaborate with stakeholders, provide program management, and report performance to executive leadership to ensure that these programs are implemented successfully across the organization and to minimize any negative impact of ICAM on the agency's mission. The information and guidance presented in this section is intended to assist agencies in providing answers to several common program organization and management questions, including:

- How can I establish governance to ensure ICAM alignment at the agency level?
- What groups are considered ICAM stakeholders?
- What are the best practices for supporting implementation of individual ICAM projects?

#### 6.1.1. Program Governance

Goal 1 of the Federal ICAM Initiative, as identified in Section 2.2.1, is to align and coordinate all of the laws, standards, regulations, and policies that ICAM programs must adhere to, and establish and enforce accountability for ICAM implementations within federal governance bodies. Achieving this goal at the Federal Government level will allow supervisory bodies to evaluate the compliance of agency level programs as a unified ICAM program, as opposed to examining each of the ICAM component projects independently. In order to ensure that ICAM programs at the agency level are compliant, each agency should have a formal governance

structure, either by leveraging an existing program structure or by establishing new governance as necessary. This structure is responsible for aligning and consolidating the agency's various ICAM investments, monitoring these programs for alignment with organizational objectives, and ensuring broad awareness and understanding. Program governance should also establish goals, mission priorities, organization, accountability, metrics, and management controls within an agency.

### Lesson Learned

It is important for an ICAM governance structure to account for the interdependencies between its project management, investment management, and capital planning components. Health and Human Services enhanced its ICAM program governance by applying its Enterprise Performance Life Cycle framework, which incorporates structured investment processes, distinguished project management principles, and industry best practices.



Establishing a formal governance structure within a federal agency refers to both the creation and assignment of a specific group or entity to provide oversight and management, and development and enforcement of agency-specific policies, processes, and performance measures. Governance encompasses the relationship between the oversight effort, mechanisms put in place to ensure compliance, the enterprise's overall business direction, and the accountability framework to encourage desirable behavior. It also encompasses all of the decision-making roles and responsibilities involved in executing the program across the agency enterprise. The governance needs to be structured in a way that facilitates coordination between the Department and bureau/component level and promotes stakeholder buy-in. Program Governance involves identifying individuals, such as an Executive Sponsor, to champion the ICAM program and establishing coordinated governance groups at the Department and bureau/component levels, such as an ICAM Executive Steering Committee (ESC), addressed in the following section.

#### **6.1.1.1. ICAM Executive Steering Committee**

An ESC is one of the means by which an agency can provide oversight for its ICAM program. The ESC is chartered by the agency's executive leadership to govern and align the ICAM program with its agency's mission. Typically, the ESC is comprised of departmental heads, bureau/component leadership, business owners, and application owners. The ESC's charter should specify the group's authority to enforce changes, when necessary, to align ICAM technology, policy and execution with the agency's overall mission.

An ESC provides an agency with the ability to resolve many of the internal issues common to ICAM by employing a top-down approach for managing implementation. For example, gaining the support and buy-in necessary to ensure wide-scale enterprise adoption is often difficult given the broad reach and technical nature of ICAM. ESCs help mitigate this risk by providing end-users with a consistent message from their senior executives on how ICAM solutions can streamline access to resources that support their mission work. Additionally, many of the ESC participants are leaders within the stakeholder community, and as such, facilitate collaboration between the diverse groups that contribute to successful ICAM implementation. Properly chartered, an ESC will establish performance measurement and accountability mechanisms to ensure that ICAM implementations comply with federal laws and regulations and fulfill the desired goals and objectives. These specific performance mechanisms are discussed in Section 6.1.4.

### Implementation Tip

Documenting and understanding key performance metrics and the expected performance improvements as a result of implementing ICAM are an excellent way to demonstrate program value to leadership and gain the support of the members of an agency's Executive Steering Committee (ESC). Being able to demonstrate incremental, quantifiable benefits helps maintain program momentum.



As previously noted, the role and responsibilities of each agency's ESC are typically governed by its charter. The following list describes some of the typical responsibilities that might be assigned to an ESC:

- Provide a means through which changes to the ICAM program or disputes between ICAM and individual program offices are resolved;
- Provide direction and counsel to the ICAM Program Management Office (PMO), if applicable;
- Ensure proper resource allocation to ICAM programs and projects;
- Review and approve the program business architecture;
- Provide input for, or participate in, the critical development stages of the ICAM program;
- Take responsibility for overall stakeholder management to include internal and external stakeholders;
- Provide strategic guidance for cost, schedule, performance and technical solutions to ensure program success;
- Review post-implementation evaluations to ensure that forecasted benefits and outcomes of the ICAM program are met;
- Provide program status information to oversight organizations such as the Office of Management and Budget (OMB), Office of Inspector General (OIG), and Government Accountability Office (GAO), upon request; and
- Establish collaboration to provide guidance, identify common agency challenges, identify best practices, and share solutions.

Each of the responsibilities listed above contributes to an overarching level of governance and support that is critical to ensuring the successful implementation of ICAM within an agency. ESCs provide agencies with a means to ensure agency-wide adoption through strong executive buy-in and support, ensure alignment with the organization's business need and mission, and enforce compliance with applicable laws, regulations, and policies.

#### **6.1.1.2. Bureau/Component Governance**

Some agencies are made up of subgroups, typically called bureaus or components, which operate in a decentralized manner. For agencies with this dynamic, it may be beneficial to create a governance structure at the bureau/component level by way of an interdisciplinary team. This team should be authorized and recognized by department-level leadership to enhance communication and promote cohesion among the various subgroups within an agency. Obtaining leadership buy-in at the department-level is an advantageous way to build the foundation of a strong and recognized ICAM program. The mission of the bureau/component interdisciplinary team is to provide ICAM-related recommendations to the department's ESC and help drive the success of the ICAM program. These teams are typically comprised of working-level roles and employ a bottom up approach for managing implementation. An interdisciplinary team at the bureau/component level plays an important risk mitigation role by providing insight into the

implementation effort from a functional point of view. This information helps the ESC understand the impact certain decisions may have on program executors and ultimately promote buy-in across various stakeholders.

## FAQ

### What groups should be represented in ICAM governance?

Governance structures should be made up of individuals that have a diverse blend of skills and experience; for example, business process operators, business process end users, administrative roles, security, privacy, legal and audit, information technology (IT), and financial groups. Inclusion of a variety of groups in the ICAM governance will ensure that different needs and opinions are represented and addressed, which contributes to the success of the program.



## 6.1.2. Program Stakeholders

A stakeholder is an individual or organization that is either actively involved in a program or who might be affected by the program's execution or completion. It is critical to identify all stakeholders, and not just those who may be positively affected by the project, in order to understand the needs, responsibilities, and potential impacts of program decisions. Once the stakeholders have been identified, an agency can work to engage its stakeholders in support of the success of the program/project.

This section identifies key ICAM stakeholders, both at the government-wide level (associated with the ICAM segment<sup>54</sup> and the Federal ICAM Initiative) and the agency level (associated with an agency's ICAM program and supporting projects). It then introduces approaches for managing and engaging stakeholders to support ICAM program success.

### 6.1.2.1. Government-wide ICAM Segment Stakeholders

An early step in developing the ICAM segment architecture was identifying the stakeholders related to the ICAM segment. The following table provides an overview of the stakeholders who were identified as part of this process. The table lists many of the federal stakeholders for ICAM but is not intended to be an exhaustive 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. The stakeholders all contribute to or are impacted by the Federal ICAM Initiative.

Stakeholder Group	Stakeholder Name	Role
<b>Federal Governance Bodies</b>	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.

<sup>54</sup> ICAM is included the Federal Enterprise Architecture. Information on the other segments can be found in the [Enterprise Architecture Segment Report \(EASR\), Interim Version 1.3, Executive Office of the President, September 2009](#). [EASR]

Stakeholder Group	Stakeholder Name	Role
	The Federal Chief Information Officers (CIO) Council	Serves as the principal interagency forum for improving practices in the design, modernization, use, sharing, and performance of Federal Government agency information resources. Chartered the work of the Federal Identity Credentialing Committee (FICC), E-authentication initiative, and the Federal PKI Policy Authority, which have been consolidated into the newly chartered Information Security and Identity Management Committee (ISIMC) and Identity Credential and Access Management Subcommittee (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.
	Department of Homeland Security (DHS)	Oversees government-wide and agency-specific cybersecurity implementation and reporting with respect to information systems that fall under FISMA to provide adequate, risk-based, and cost-effective cybersecurity. Develops analyses for OMB in support of the FISMA annual report, oversees agencies' cybersecurity operations and incident response; and reviews agencies' cybersecurity programs annually. <sup>55</sup>
	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 Homeland Security Presidential Directive 12 (HSPD-12) deployment. Provides the USAccess Homeland Security Presidential Directive 12 (HSPD-12) Managed Service Offering.

<sup>55</sup> DHS government-wide cybersecurity role and responsibilities established by OMB in [M-10-28](#), Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS), July 6, 2010.

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 Human Resources (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 uniform and consistent policies and procedures to ensure the effective, efficient, and timely completions of investigations and adjudications relating to determination of suitability and eligibility for logical and physical access. 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. <sup>56</sup>
	Suitability and Security Clearance Performance Accountability Council	Interagency body established by Executive Order (E.O.) 13467 <sup>57</sup> and supported by OPM to develop and implement uniform and consistent policies and procedures related to suitability, fitness, and clearance determination activities and processes. The Suitability and Security Clearance Performance Accountability Council serves as the most senior policy-making entity for the security and suitability reform effort and provides final determinations for resulting reports, such as the Security and Suitability Process Reform, Initial Report dated April 30, 2008 <sup>58</sup> and the Federal Investigative Standards. <sup>59</sup>
	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 (E.O.) 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 (NSTC)	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.
	Federal Enterprise Architecture (FEA) Interagency Group	Community of federal enterprise architects that support the development of the FEA practices, models and other assets.

<sup>56</sup> 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, The White House, June 30, 2008. [E.O. 13467]

<sup>57</sup> [E.O. 13467](#)

<sup>58</sup> [Security and Suitability Process Reform Initial Report](#), Joint Security and Suitability Reform Team, April 30, 2008.

<sup>59</sup> [Federal Investigative Standards](#), Joint Security and Suitability Reform Team, December 2008.

Stakeholder Group	Stakeholder Name	Role
	Office of the National Coordinator for Health IT	Provides counsel to the Secretary of Health and Human Services (HHS) and departmental leadership for the development and nationwide implementation of an interoperable health IT 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 Cloud Computing Advisory Council	Provides oversight to the Cloud Computing Initiative and Program Management Office (PMO), formerly ITI LOB PMO. Goal is to achieve an optimized, cost-effective, government-wide IT 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 (IPC) formerly the Information Sharing Council	Council first established under E.O.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.
	National Security Staff (NSS)	The merged National Security Council (NSC) and Homeland Security Council (HSC). The mission of the NSS is to advise and assist the President on national security and foreign policies.
	Committee of National Security Systems (CNSS)	Provides a forum for the discussion of policy issues in regards to the protection of national security systems. <sup>60</sup> The committee has representation from 21 U.S. Government Executive Branch Departments and Agencies.
Internal standards body	National Institute of Standards and Technology (NIST)	Non-regulatory federal agency within the 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 the Federal Information Security Management Act (FISMA). NIST is an American National Standards Institute (ANSI) accredited standards development organization to develop biometric format standards.
External industry guidance and standards bodies	ASIS International	ASIS International is the preeminent organization for End-User physical security professionals. Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests.
	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.

<sup>60</sup> Although national security systems are outside the scope of this document, the NSS and CNSS have been included as stakeholders because they coordinate with OMB and the ISIMC in areas where the ICAM initiative relates to national security efforts.

Stakeholder Group	Stakeholder Name	Role
	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.
	OpenID Foundation	Organization formed to help promote, protect and enable the OpenID technologies and community. The OpenID Foundation manages intellectual property, brand marks as well as fostering vital growth and global participation in the proliferation of OpenID.
	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 Assertion Markup Language (SAML) and WS-* <sup>61</sup> ) needed in e-business and Web services applications.
	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.
	Smart Card Alliance	Not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. The Smart Card Alliance 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.
	Transglobal Secure Collaboration Program (TSCP)	Government-industry partnership specifically focused on facilitating solutions for Aerospace and Defense issues. Currently working on identity federation issues in international defense and aerospace programs.
<b>Internal ICAM Service Providers</b>	Department of the Treasury	A provider of PKI services and digital certificates for trusted identity authentication across the Federal Government and with external bodies.
	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.
<b>External ICAM Service Providers</b>	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 Global Federated Identity and Privilege Management (GFIPM).
	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 with the most appropriate services based on the needs of our customers and the state of the industry. Also includes Identity and Trust Providers.
	Industry PKI Service Providers	Providers of PKI services and digital certificates for trusted identity authentication across the Federal Government and with external bodies.

<sup>61</sup> WS-\*(WS-SEC, Web Services Security, WSS): A family of web service standards/specifications published by OASIS WS-Security.

Stakeholder Group	Stakeholder Name	Role
<b>Internal Service Consumers</b>	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	Primary recipient of Personal Identity Verification (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 ICAM initiatives.
<b>External Service Consumers</b>	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 (G2C) and Government-to-Business (G2B). 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 (DHS) to develop the First Responder Access Card (FRAC) identity credential).

**Figure 60: Federal ICAM Initiative Stakeholders**

#### **6.1.2.2. Agency-level ICAM Program Stakeholders**

ICAM programs are large, complex initiatives that often span across several agency bureaus/components; as such, it is critical to define the program objectives, boundaries, and stakeholders early in the planning process. Identifying and managing the stakeholders responsible for ICAM business processes and systems is critical to achieving a fully integrated ICAM portfolio.

The following table provides an overview of many agency-level stakeholders within an agency-level ICAM program. For each stakeholder, the table includes role descriptions identifying their overarching role or mission within the agency and their relevance to the ICAM program. The table is not intended to be an exhaustive list of agency-level stakeholders for all federal organizations, but rather to highlight the most common groups that are involved in or impacted by ICAM implementations.

Stakeholder Name	Role
Agency Employees	Employees of a federal agency. Employees comprise a large percentage of an agency's total user population. Employees consume ICAM services by using their PIV cards to gain access to agency facilities and information systems.

Stakeholder Name	Role
Agency Partners and Affiliates	Includes contractors working on behalf of the Federal Government and affiliates that do business with or consume the services provided by federal agencies. Portions of this population utilize the PIV card to access agency facilities and information systems, while others utilize non-PIV cards and require only occasional access to agency assets.
Business Process/System Owners	Individuals within an agency responsible for managing a set of activities, programs, and systems that are critical to operations and use ICAM services.
General Counsel	Responsible for providing legal oversight over an agency's ICAM program, administering security clearance review programs, and ensuring that ICAM programs abide by all applicable laws and regulations through use of an Inspector General (IG) led audit and accountability program.
Human Resources (HR)	Responsible for conducting agency-level recruitment, on-boarding, wage, and benefit activities, and establishing personnel policies and regulations. As on-boarding officials, HR offices are generally responsible for collecting and managing biographical information on federal employees, which results in creation of a digital identity within the agency's HR application. HR works closely with Personnel Security during the recruiting and on-boarding processes to ensure that an appropriate background investigation is conducted for each new hire.
Office of the Chief Financial Officer (OCFO)	Responsible for administering the agency's budget, and reviewing and submitting budgetary/investment requests to OMB. OCFO is also responsible for developing and implementing fiscal planning activities to ensure alignment with the agency's strategic and operational ICAM goals and objectives. OCFO plays a significant role in processing and submitting budget requests for ICAM investments and ensuring that ICAM requirements and tools are leveraged across the agency's investments.
Office of the Chief Information Officer (OCIO)	Responsible for maintaining the agency's overall information security posture, defining and ensuring compliance with the agency's enterprise architecture (EA), and planning for technology investments to meet current and future requirements. The CIO typically coordinates with the agency's Chief Financial Officer (CFO) to assure that the IT programs and activities are executed in a cost-effective manner. OCIO is heavily involved in ICAM implementations by ensuring that appropriate security controls are applied, determining how the ICAM solution will impact the security of existing applications, and incorporating ICAM into the agency's EA.
Office of the Chief Information Security Officer (OCISO) <sup>62</sup>	Responsible for developing, employing, and publishing security policies, programs, and standards to guard the agency's personnel, property, facilities, and information. Overseeing projects related to credentials, badges, emergency signaling devices, etc. OCISO has leadership and authority over security policy and programs within the agency and can coordinate with the Personnel Security and Physical Security divisions.
Personnel Security	Responsible for coordinating with managers HR departments to determine position sensitivity levels for each position occupied within the agency, and coordinating with OPM to ensure that an appropriate background investigation and/or periodic reinvestigation is conducted for all agency employees and contractors.
Physical Security	Responsible for managing and maintaining the security of agency buildings, including: resolving conflicts concerning entry to facilities, and verifying that those seeking to gain access to federal buildings are appropriately authorized to do so (including visitors).

<sup>62</sup> The Office of the Chief Information Security Officer is the naming convention used by various Federal Government agencies, although similar naming structure can be found as well such as The Office of the Chief Security Officer.

Stakeholder Name	Role
PIV Credentialing Program	Responsible for managing and maintaining the PIV card issuance process and infrastructure.
Privacy Office	Responsible for administering policy to govern the use, collection, storage, and dissemination of Personally Identifiable Information (PII) for all agency employees, contractors, and affiliates. Privacy Offices are also responsible for maintaining an agency's System of Records Notices (SORNs), and supporting Privacy Impact Assessments (PIAs) for all IT investments, including ICAM.
Solution Providers	Industry partners and/or system integrators that provide ICAM services to federal agencies.
Unions	Responsible for representing the interests of its federal employee members and conducting collective bargaining on their behalf. As representatives for federal employees, the unions are frequently involved in matters related to ICAM processes that collect personal information or introduce additional requirements for background investigations.

Figure 61: Agency-level ICAM Stakeholders

#### **6.1.2.3. Stakeholder Management Strategies**

Traditionally, ICAM programs have been managed in stove-pipes, which has led to challenges in involving all relevant stakeholders. Stakeholder management, as it relates to ICAM, involves coordination, collaboration, and communication with numerous entities within the agency. Each of these entities often has a distinct mission requirement and performs a specific set of duties in support of the overall agency mission. As such, these stakeholders all have important ties to ICAM, but are not necessarily bound together by a single agency program or project. These stakeholders will have different viewpoints that may conflict with one another or the overarching ICAM program objectives. Furthermore, decisions made in one program area may impact another; therefore, the ability to communicate and coordinate across stakeholder groups, leveraging their inputs to the benefit of all, becomes increasingly important to the success of the overall ICAM program. This section presents some high-level considerations for involving stakeholders and promoting collaboration across an agency's ICAM portfolio to help overcome many of the challenges typically associated with ICAM.

Collaboration is both a process and an outcome in which shared interest or conflict is addressed by a group of key stakeholders. The collaborative process involves a synthesis of different stakeholder perspectives to better understand complex problems. In the case of ICAM, the stakeholder perspectives will range from business process owners needing access to data and services to the agency end user needing gate access and access to data and services in order to successfully perform his job. The benefits provided by streamlining agency processes using ICAM solutions cannot be realized without close collaboration and consideration of all stakeholder requirements.

Collaboration is usually achieved through the development of expert problem-solving teams, such as working groups that are established to address issues and present solutions. Although members of these groups have individual accountability, they come together to share information and perspectives and produce shared work products. The success of these groups is heavily reliant on participation and involvement from stakeholders across the program in order to ensure that all requirements are considered. Within an agency's ICAM program, for example, each bureau/component might assemble an interdisciplinary working group responsible for expressing the concerns and interests of its business and system owners and users. These representatives

work with the group to incorporate their needs into agency-wide program capabilities and requirements. Working groups of this nature are an excellent forum for identifying and escalating business and technical challenges that may not be known at the enterprise level but could impede ICAM implementation throughout the agency. Working groups are also used as a forum for sharing implementation lessons learned across bureaus/components or individual programs in order to reduce overall ICAM program risk and increase speed and efficiency in implementation.

In addition to working groups, an agency may choose to stand up smaller focus groups or tiger teams for the purpose of resolving specific program issues or providing direct support for implementation. This technique helps improve stakeholder buy-in associated with enterprise approaches and services by promoting better understanding and a sense of inclusion and ownership in the program. It also improves consistency across an agency's ICAM implementation, a key goal when implementing the ICAM segment architecture. For example, an agency's ICAM program management staff could leverage small focus groups with expertise in the agency's enterprise ICAM program and tools to consult with and support implementation efforts at the bureau/component level.

### 6.1.3. Program Management

In addition to setting up an ICAM governance structure, an agency needs to establish a mechanism for supporting execution and operations of the projects and workstreams within the ICAM program. This section examines a Program Management Office (PMO) as one possible alternative for providing ICAM program support; however, an agency should evaluate potential program management alternatives and select the option that best fits its needs.

#### Implementation Tip

In order for a Program Management Office (PMO) to be effective, it must be chartered to perform the functions as needed, have the support of executive leadership, be allowed to use resources as required, and have the skills and expertise to implement the ICAM program.



An ICAM PMO serves a complementary role to the ESC and while establishing both an ESC and a PMO may not be strictly necessary, larger organizations may see the need to separate governance and operational responsibility within their ICAM program. A PMO helps ensure that the individual projects and investments that comprise the ICAM program run smoothly and achieve the expected results within the defined budgetary and schedule constraints. In addition, an ICAM PMO provides an agency with a single coordination point for streamlining management of ICAM programs at an operational level. This position allows the PMO to facilitate close cooperation and synchronization between an agency's ICAM stakeholders and the individual ICAM component activities to ensure alignment across the organization. The PMO will typically be responsible for the supporting functions discussed throughout Section 6.1, including:

- Planning and coordinating implementation efforts across various ICAM stakeholders and component programs (e.g., credentialing, physical access control, logical access control, personnel security, etc.);
- Maintaining an enterprise ICAM perspective to ensure alignment of all component programs with organizational objectives;
- Serving as a centralized point of contact for ICAM questions, issues, and concerns;

- Planning for and securing program funding to execute ICAM capabilities;
- Handling communications and outreach to both internal and external stakeholders; and
- Managing program risks and issues to resolution across agency office/component/bureau boundaries.

FAQ	<b>What is the difference between an Executive Steering Committee (ESC) and a Program Management Office (PMO)?</b> ESCs traditionally provide top-down leadership support and guidance across the programs within an agency and PMOs provide operational support for the day-to-day execution of a specific implementation.	
-----	--	---

To further promote the successful execution of the ICAM program initiatives, an ICAM PMO may decide to assign separate workstreams to individuals who already have an active and steadfast involvement in a particular area outside of the program. These —champions,|| as the title implies, must have the passion to drive the success of their piece of the ICAM puzzle and make it their personal mission to achieve the performance outcomes defined for the ICAM target state. Additionally, a workstream task lead manages the day-to-day activities of his/her individual workstream and provides the ICAM PMO with critical and timely information related to the planning, development, deployment, and activities of their initiatives.

	Workstream Name	Responsibilities
Administrative Workstreams	Outreach and Communications	Responsible for developing and executing the ICAM program's Communications Plan, including: <ul style="list-style-type: none"> <li>Defining communication message types, media, target audience, and timing.</li> <li>Communicating ICAM program concepts, activities, and progress to promote support for the implementation of improved ICAM capabilities.</li> </ul>
	Policy	Responsible for setting the direction for the ICAM program and developing or finalizing all policies and standard operating procedures related to the ICAM program.
	Budget	Responsible for developing, managing, monitoring, and reporting on the ICAM program budget. The Budget Workstream will have key interfaces with an agency's OCFO during the budget development and submission cycles.
	Performance Management	Responsible for tracking, managing, and reporting on overall ICAM program performance and metrics.
Project Workstreams	Identity Management	Responsible for ICAM processes and systems related to the management of digital identity data. This includes management and oversight of efforts to modernize the management of digital identities, such as HR modernization, in accordance with the ICAM target state initiatives.
	Credential Management	Responsible for ICAM processes and systems related to credential lifecycle management activities. Separate workstreams may be identified for various credential types, including agency PIV cards and local facility access cards.
	Physical Access	Responsible for ICAM processes and systems related to physical access control, including modernization efforts in accordance with the ICAM target state initiatives.
	Logical Access	Responsible for ICAM processes and systems related to logical access control, including modernization efforts in accordance with the ICAM target state initiatives.

**Figure 62: Examples of ICAM Workstream Responsibilities**

A PMO has many characteristics that make it a viable method for providing ICAM program management. PMOs generally follow standardized project management policies, processes, and methods. Within ICAM, a PMO provides opportunities to share lessons learned both within an agency and across agencies. It may serve as an advisor to other agency offices or programs impacted by the ICAM program (see Section 6.2) on addressing ICAM as appropriate within other agency-wide capabilities. Additionally, an ICAM PMO acts as a single, centralized point of contact for the agency's ICAM program. Finally, the PMO is the primary authority for performing acquisition planning tasks and making procurement decisions. As a result, an ICAM PMO can offer an agency the following benefits:

- Enhanced efficiency
- Streamlined overhead costs
- Minimized redundancy of ICAM-related processes
- Validated alignment with architecture and technical standards
- Fostered communication and cooperation between interrelated programs
- Consistent messaging to both internal and external stakeholders
- Timely and accurate reporting
- Minimized confusion
- Facilitated agency-wide adoption
- Minimized risk

Figure 63 represents a sample ICAM PMO structure. An agency should design its ICAM PMO structure in a way that fosters communication, coordinates efforts, and appropriately aligns with the agency's overall organizational structure.

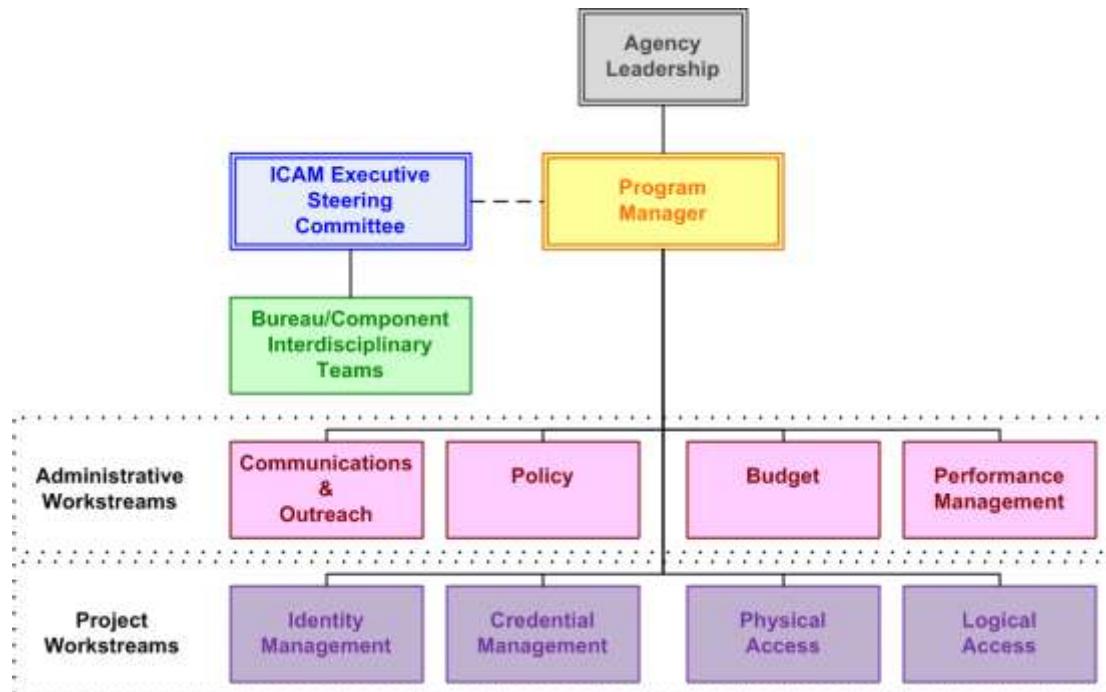


Figure 63: Sample ICAM PMO Structure

Because program communications, risk management, and acquisition planning are critical functions of the ICAM PMO, these functions are discussed further in the following sections.

#### 6.1.3.1. Program Communications

Effective communication at all levels is key to the success of any program, in order to facilitate support with stakeholders at various levels in the agency. In order to communicate consistently and effectively, a Communications Plan should be developed early in the program life cycle for programs such as ICAM. A Communications Plan will outline the objectives, goals, themes and approach of the overall program. Some goals of the plan include the distribution of project information, management of stakeholders' expectations and communication of project performance. The following table provides a summary of some of the common communications that an agency might incorporate as part of its ICAM program.

Communication Description	Target Audience	Delivery Media
ICAM program awareness materials explaining key program features and milestones	User population	Brochure, posters, video
ICAM program website containing resources for stakeholders and users	Various stakeholder groups	Website
Ad hoc updates for system rollout events and changes	User population	E-mail, newsletter bulletin
Leadership briefing highlighting program objectives and status	Agency leadership	Slide presentation, meeting
Lessons learned workshops	ICAM implementers	Meeting, teleconference, webinar
Messages from Leadership	ICAM implementers, user population	Memo, e-mail
ICAM conference or All-hands	ICAM implementers, user population	Meeting, teleconference, webinar

**Figure 64: Sample ICAM Program Communications**

When creating a Communications Plan, agencies should analyze the stakeholders that make up their audience and tailor the message and delivery media in such a way that will produce the desired response. The goal of this plan is to keep stakeholders regularly informed and involved by providing appropriate and well-structured communications, ultimately helping to foster and maintain stakeholder support and reduce risk.

#### Lesson Learned

Process or system changes that will impact users need to be communicated early and often in order to promote adoption. As many agencies learned when introducing the new PIV credential, employees and contractors needed to be made aware of the new requirements, processes, and their benefits before enrollments started to increase.



#### 6.1.3.2. Program Risk Management

Risk management involves the identification of policies, procedures, and practices, as well as the analysis, assessment, control, and avoidance of threats to the continuing efficiency, profitability and success of program operations. Due to the complexity of ICAM and its cross-departmental involvement, risks that threaten the success of an agency's ICAM program can have sweeping effects. Therefore, proactive risk management is paramount within an agency's ICAM program. This requires the involvement of the entire program management team and active maintenance of issues. Other typical characteristics of a successful risk management program include:

- Stakeholders at all levels within a project can identify a risk;

- Processes exist to analyze, prioritize, and determine mitigation approaches for identified risks;
- Procedures are in place for assigning owner(s) of a risk and defining risk ownership responsibilities;
- A defined escalation path exists for flagging and resolving risks up to and including executive leadership, as necessary;
- There is an ability to track the resolution efforts and their effectiveness; and
- Report on risk status to organizational leadership.

ICAM implementers should develop a Risk Management Plan that defines the way risks are measured for the ICAM program, provides a process for identification and appropriate response, and assigns roles and responsibilities for various stages in the process. Tools are available commercially to help manage and track risks for a program. ICAM implementers should determine if their agency has risk management tools that could be leveraged within the ICAM program.

Another leading practice in ICAM Risk Management is the use of a Risk Registry (sometimes referred to as a Risk Log), which aides in managing, assigning and tracking risk events. The Risk Registry usually includes the description of the risk event, the date that the event occurred, how the event was resolved, whether the resolution was effective, and the owner of the event. Review and updating of the Risk Registry should be incorporated into ongoing management processes. A Risk Registry was developed as part of the ICAM segment architecture to identify and track risks for the Federal ICAM Initiative and can be found in Appendix D Risk Registry. The following table summarizes some of the common risks faced within an agency ICAM program and sample mitigation approaches.

Item No.	Risk Description	Mitigation Plan
1	If agency plans and budgets do not include ICAM activities, adequate funding may not be available for modernization efforts, the agency will not be able to meet target state requirements and deadlines for the ICAM segment architecture.	Develop consolidated ICAM business case and funding request to secure funding beginning in FY12. Communicate funding needs to the agency OCFO and explore existing funding sources within the agency. Determine if internal funding can be routed to ICAM efforts, for example, working capital.
2	If the agency's ICAM transition plan does not gain support and adoption at the Assistant/Deputy Secretary level, including required compliance, the agency will not receive coordination and support from the necessary stakeholders in order to move forward with implementation.	Support institution of governance structure for ICAM (to include the ESC). Develop and implement Communications Plan.
3	If the agency doesn't meet the scheduled transition activity milestone dates, funding for ICAM and other agency systems may be impacted.	Based on agency ICAM segment architecture analysis, provide realistic completion targets for ICAM activities to OMB in the ICAM Transition Plan template.
4	If the bureaus/components fail to adopt enterprise ICAM services in a timely manner, overall agency ICAM implementation and compliance will be delayed.	Dedicate ICAM program management resources and program funding to gain stakeholder buy-in and support bureau/component-level implementation requirements and efforts.
5	If the agency is unable to staff dedicated resources with the necessary technical knowledge, the agency will be unable to successfully execute technical implementation and the program schedule will lag.	Leverage cross-agency ICAM expertise via working groups and outreach in order to supplement staff knowledge. Incorporate staff augmentation in the ICAM acquisition plan in order to ensure necessary skill sets.

Item No.	Risk Description	Mitigation Plan
6	If the ICAM effort is unable to gain acceptance by the user population, the agency will not be able to meet target state requirements and deadlines.	Dedicate additional ICAM program management resources and program funding to increase the communication effort and promote awareness.
7	If the ICAM solution vendor(s) goes out of business, the agency may experience program delays or incur additional costs to migrate to new solutions.	Include supply chain risk management in ICAM program Acquisition Plan and identify alternative solution component sources. Where possible, use approved vendors and products from established acquisition vehicles. Include activities for compiled software escrow and source code escrow.

**Figure 65: Sample ICAM Program Risks and Mitigations**

One area that can introduce risk to a program is procurement. It is imperative that an agency plan an approach for the acquisition of ICAM-related products and services that is cost and time effective in order to minimize the overall impact on the program. This is addressed further in the following section.

#### **6.1.3.3. Acquisition Planning**

When planning for the acquisition of products and services for its ICAM program, an agency must comply with specified regulations and policies, the main system of regulations being the Federal Acquisition Regulation<sup>63</sup> (FAR). The FAR sets forth the rules governing the federal acquisition process and includes several clauses specifically relevant to an agency's ICAM program, as discussed later in this section. When purchasing products and services for its HSPD-12 implementation, an agency must also follow OMB M-06-18<sup>64</sup> and leverage the Federal Information Processing Standards 201 (FIPS 201) Evaluation Program Approved Products List (APL). In addition to the requirements governing federal acquisitions, an agency has other resources at its disposal to support acquisition for its ICAM program, including the GSA Schedules, also addressed in this section.

FAQ	What is the difference between General Services Administration (GSA) Schedules and the Approved Products List (APL)?	
	GSA Schedules are purchasing vehicles for a broad range of products and services. The resources available on the GSA Schedules have pre-approved vendors and pre-negotiated rates. The APL is a list of Homeland Security Presidential Directive 12 (HSPD-12) related products and services that have been tested per an approved National Institute of Standards and Technology (NIST) test procedure. An agency can use the GSA Schedules to purchase a resource that is included on the APL.	

M-6-18 provides guidance to federal agencies related to the acquisition of products and services for HSPD-12 implementations. It introduced several amendments to the FAR, which were codified in 48 C.F.R. Subpart 4.13,<sup>65</sup> that require an agency to comply with HSPD-12 and FIPS 201 for contractors who require routine logical or physical access and include language to this

<sup>63</sup> [Federal Acquisition Regulation](#) (FAR), Volume 1, March 2005.

<sup>64</sup> [M-06-18](#) Acquisition of Products and Services for Implementation of HSPD-12, OMB, June 30, 2006. [M-06-18]

<sup>65</sup> [FAR Subpart 4.13- Personal Identity Verification. \[FAR Subpart 4.13\]](#)

effect<sup>66</sup> in applicable solicitations and contracts. The addition to the FAR also requires that agencies purchase only approved products and services in support of their HSPD-12 implementations. The FIPS 201 Evaluation Program was developed to organize and define a standardized approval process for these products and services. All required NIST validation and GSA testing must be met to be an approved product or service for HSPD-12 purchases. Approved products and services, which have been demonstrated to meet NIST validation and GSA testing and have been qualified by the Evaluation Program, can be found on the FIPS 201 APL.

ROI	
Agencies are strongly encouraged to institute processes to include language in solicitations and contracts, where applicable, requiring use of the PIV card where encryption and digital signature services are provided. This language would supplement the existing FAR requirements related to using the PIV card for contractor access. This approach not only promotes government-wide consistency in providing these security services, but also supports a greater return on investment (ROI) in leveraging the agency's existing PIV infrastructure.	

The APL is continuously updated to reflect new products and technologies that have been assessed and approved. It is an agency's responsibility to stay current on these changes and incorporate them into agency planning during regular technology refresh cycles as part of the capital planning and budget process. A complete inventory of Government Certified and Approved Services and Products Listings, including the FIPS 201 APL, Certified PKI (public key infrastructure) Shared Service Providers (SSP) List,<sup>67</sup> and Qualified HSPD-12 Service Providers List, can be found on GSA's website.<sup>68</sup>

In addition to the APL, there are several other activities underway in the Federal ICAM Initiative to identify and recognize specific categories of products and services that meet advertised criteria to support other functions within an agency's ICAM program. These include:

- The Path Discovery and Validation (PDVAL) products approval process using the Public Key Interoperability Test Suite (PKITS) to ensure compatibility and interoperability of solutions within the Federal Bridge Certification Authority (FBCA);
- The Trust Framework Provider Adoption Process (TFPAP), which outlines the process that the ICAM community uses to certify organizations that assess commercial Identity Providers for use by the Federal Government (discussed further in Section 12.1.1); and
- The Personal Identity Verification Interoperability (PIV-I) for Non-Federal Issuers (NFI) guidance<sup>69</sup> and supporting processes for approving an NFI.

<sup>66</sup> [48 C.F.R. 52.204-9](#), Personal Identity Verification of Contractor Personnel, September 2007.

<sup>67</sup> As required by Streamlining Authentication and Identity Management within the Federal Government, OMB, July 3, 2003.

<sup>68</sup> [GSA FIPS 201 Evaluation Program Approved Products List \(APL\)](#), General Services Administration. [APL]

<sup>69</sup> [Personal Identity Verification Interoperability for Non-Federal Issuers](#), Version 1.1, CIO Council, July 2010. [Personal Identity Verification Interoperability for Non-Federal Issuers]

### Implementation Tip

Purchasing products off of the Homeland Security Presidential Directive 12 (HSPD-12) Approved Products List (APL) does not ensure interoperability or appropriateness for your agency's implementation. Products bought from the APL must be properly integrated and configured to be interoperable with other ICAM programs and services. Furthermore, prior to acquiring, agencies should determine if the products are appropriate for the risk level and/or design of the ICAM solution.



Though not a required acquisition tool, GSA Schedules provide quick, flexible, cost-effective procurement solutions and assist in compliance by including approved products. Overall, the benefits offered by schedules result in reduced risk and, when applied to an agency ICAM program, allow agencies to achieve the ICAM objectives of cost-effectiveness and efficiency. There are two GSA Schedules that are relevant to the ICAM effort: IT Schedule 70 and Schedule 84.

IT Schedule 70 is under the Multiple Award Schedule (MAS) program and gives agencies direct access to commercial experts who are able to address the needs of the government IT Community through a series of Special Item Numbers (SINs). These SINs cover most of the general purpose commercial IT hardware, software and services and should be used by agencies as needed to meet their mission objectives as well as ICAM initiatives. Within IT Schedule 70, GSA has set up SINs 132-60 through 132-62, which can help an agency meet the procurement needs of its ICAM program, including electronic credentials, PKI services, and HSPD-12 products and services. With regard to HSPD-12, M-06-18<sup>70</sup> promotes the use of IT Schedule 70, SIN 132-62 and notes that agencies purchasing HSPD-12 products and services through acquisition vehicles other than GSA IT Schedule 70 bear the responsibility for ensuring that they comply with the applicable federal standards and requirements. In addition to IT Schedule 70, ICAM implementations often require acquisition of security products and services, particularly items related to Physical Access Control Systems (PACS). These items may be procured using Schedule 84, which includes a full suite of solutions for law enforcement, security, facilities management, fire, rescue, clothing, marine craft, and emergency/disaster response.

Agency procurement personnel may purchase resources off of both schedules to meet their ICAM implementation needs. For example, an agency trying to modernize their PACS could purchase new PIV card readers for access control points off of Schedule 84 and purchase services from the system integrator off of Schedule 70. Additionally, state and local governments are authorized to purchase products and services through GSA Schedules 70 and 84 by way of the Cooperative Purchasing Program. This arrangement may help achieve interoperability in Government-to-Government (G2G) ICAM interactions in the target state.

<sup>70</sup> [M-06-18](#)

## FAQ

### Why are some products and services not represented by a category on the FIPS 201 Product/Service category list?

The FIPS 201 Evaluation Program assesses and approves only products and services for which there are direct requirements specified in FIPS 201. Although they are not part of the Evaluation Program, GSA has also developed qualification requirements and a list of qualified vendor services for other products and services that may be necessary for Homeland Security Presidential Directive 12 (HSPD-12) systems and deployments but have no direct requirements in FIPS 201 (e.g., integration services, contractor managed services and solutions). These can be found at [www.idmanagement.gov](http://www.idmanagement.gov).



Using the resources discussed in this section offers an agency the following benefits when purchasing products and services to support its ICAM program:

- **More competitive rates and potentially lower implementation costs.** Regardless of the method used to access Schedules 70 and 84, GSA has already negotiated fair and reasonable prices for these products and services. It is prepared to help agencies leverage both contracts to maximize the value for the materials and services purchased.
- **Shorter procurement time.** GSA Schedules offer streamlined procurement over agency-negotiated contracts, which can be cumbersome and costly. Additionally, tools such as eBuy<sup>71</sup> and GSA Advantage<sup>72</sup> are available to assist in ordering from both Schedules. These websites specifically provide procurement specialists with an extensive selection of approved products and services from GSA contracts.
- **Reduced complexity and effort required to perform due diligence.** Agencies purchasing products not included on the GSA APL are responsible for ensuring that the products and services procured meet all applicable federal standards and requirements, ensuring conformance to applicable federal standards for the life cycle of the components, and maintaining a written plan for ensuring ongoing conformance to applicable federal standards for the life cycle of the components.<sup>73</sup> This effort can be expensive, burdensome, and time consuming.
- **Elimination of non-compliance with standards and requirements.** If the GSA Schedules and the APL are not used, an agency also runs the risk of potential non-compliance if its conformance processes are incomplete or do not keep pace with changes within the GSA Evaluation Program.

### 6.1.4. Performance Reporting

Performance measures are essential for successful program management and oversight. Assigning performance measurements to an agency's ICAM program provides decision makers and stakeholders with a useful tool to monitor progress, determine program effectiveness, and identify areas that need more funding or process improvement. As shown in Figure 62, an agency may choose to assign a dedicated workstream to the important task of measuring and reporting performance.

<sup>71</sup> [www.ebuy.gsa.gov](http://www.ebuy.gsa.gov)

<sup>72</sup> [www.gsaadvantage.gov](http://www.gsaadvantage.gov)

<sup>73</sup> FAR Subpart 4.13

### Implementation Tip

It is important to make leadership and management feel ownership and accountability for the success of their agency's ICAM program. One way to accomplish this is to tie any outcomes and accomplishments of the ICAM program specifically to the responsible individual's yearly performance plan.



Performance reporting for ICAM programs has traditionally been focused on external reporting requirements (e.g., OMB HSPD-12 implementation status reports). In addition to mandatory reporting requirements, agencies should determine ways to leverage performance reporting to improve alignment with the ICAM segment architecture and drive progress on ICAM programs internal to the agency. Section 5.3 of the ICAM segment architecture specifies 32 performance metrics that align with achieving the target state. These serve as a starting point for agencies to measure the performance of their ICAM program and report the results to executive leadership. It is recommended that agencies incorporate the ICAM metrics into their ICAM program management practices and project reporting practices. Additionally, agencies should incorporate relevant metrics into their Exhibit 300 business case submissions for any ICAM investments as a means of tracking pertinent information and demonstrating investment results and value to the agency.

At the end of FY 2010, agencies were required to complete their plans for implementing the use of the PIV credential within the agency and an ICAM Reporting Template was provided for this purpose (available on [www.max.omb.gov](http://www.max.omb.gov)). In addition, there is mandatory reporting via the Cyberscope process for agency use of PIV credentials for physical and logical access.

## 6.2. Incorporating ICAM into Existing Agency Processes

In addition to planning specific to an ICAM program, there are numerous other systems and processes within an agency that are impacted by the implementation of the ICAM segment architecture. Each of the following subsections discusses an existing agency process or program, the impacts of the ICAM target state on that program, and guidance for addressing ICAM considerations. The information and guidance presented in this section is intended to assist agencies in providing answers to several common questions related to incorporating ICAM into existing agency processes, including:

- What criteria should be used to evaluate ICAM implementations?
- How can my agency incorporate ICAM requirements into its Capital Planning and Investment Control (CPIC) processes?
- How do ICAM systems impact and how are they impacted by IT security and risk management processes?

### 6.2.1. Management Accountability and Control

Management accountability, as defined by OMB Circular A-123,<sup>74</sup> is the expectation that managers are responsible for the quality and timeliness of program performance, increasing productivity, controlling costs and mitigating adverse aspects of agency operations, and assuring that programs are managed with integrity and in compliance with applicable law. Management

<sup>74</sup> [Circular A-123](#), Management's Responsibility for Internal Control, OMB, December 21, 2004. [OMB Circular A-123]

controls (i.e., organization policies and procedures) are tools to help program and financial managers achieve results and safeguard the integrity of their programs.

In order to improve the ability to assess alignment with the ICAM segment architecture, it is recommended that agencies leverage ICAM-specific evaluation criteria for use by agency independent evaluators for evaluating ICAM implementations.<sup>75</sup> These criteria should leverage the characteristics of the ICAM target state architecture as a model for controlling ICAM program costs and increasing efficiency. The performance architecture, as discussed in Section 3.2.1, defines clear areas for managing and evaluating alignment of programs with the ICAM target state. In particular, the performance metrics identify quantitative measures for evaluating ICAM program success. Some common topic areas that could be included in evaluation criteria are:

- Elimination of manual, paper-based processes for the collection of identity data;
- Compliance with acquisition guidance for PIV card products and services as a component of acquisition assessments;
- Adoption of standards-based, commercially available products and technologies in ICAM modernization efforts;
- Streamlining of provisioning and authentication services through enterprise capabilities; and
- Coordinated ICAM program management and investment across supporting projects.

In addition OMB Circular A-123 includes, as a control, separation of duties for various functions. An enterprise Logical Access Control System (LACS) service can support this required control by detecting the conflict and allowing the corrective action. Additionally, an automated enterprise auditing capability across agency applications offers enhanced visibility to more easily control access to systems and sensitive information. This capability could be used to support evaluating compliance with policy and applicable law.

### **6.2.2. Capital Planning**

The Clinger-Cohen Act of 1996<sup>76</sup> was enacted to improve the acquisition and management of information resources by the Federal Government. It introduces a structured, integrated approach to selecting and managing investments called Capital Planning and Investment Control (CPIC). CPIC 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 (EA), privacy, security, budgeting, portfolio management, procurement, and acquisition management of capital assets. The primary product of the CPIC process is the Exhibit 300, which is defined by OMB Circular A-11. Exhibit 300s are constructed and reviewed on an annual basis for both new and existing capital investments.

Traditionally, agencies have submitted separate Exhibit 300 investment requests for various ICAM activities (e.g., HSPD-12, E-authentication). In future budget submissions, however, agencies may consider coordinating their capital planning efforts closely across individual ICAM projects and Exhibit 300 business cases. The goal of this coordination effort is to ensure

---

<sup>75</sup> ICAM-specific evaluation criteria for use by agency independent evaluators are under development by the ICAMSC.

<sup>76</sup> [The Clinger-Cohen Act of 1996](#)

alignment throughout the organization to consolidate and/or eliminate redundant ICAM investments across agency components/bureaus. This supports collaboration across ICAM projects and systems and will improve visibility and accountability of the agency's spending on ICAM-related investments. ICAM implementers will need to evaluate their agency's specific needs to determine the appropriate and most cost efficient Exhibit 300 submission approach.

In addition to updating the agency's approach to its ICAM investments, agencies should also work to incorporate ICAM requirements, such as the need to use the PIV card as the authentication mechanism for employees accessing agency systems, into its CPIC and investment request processes. This will require identifying key criteria for an investment to be considered aligned with the ICAM target state, incorporating that criteria into CPIC processes and guidance, and communicating any changes to the relevant stakeholders and CPIC process participants.

Furthermore, collaboration between all relevant stakeholders during each phase of the CPIC process is critical to ensure that the overlapping elements of different ICAM activities are addressed. The following figure highlights several of the key ICAM considerations relevant to each phase of the standard CPIC process.

CPIC Phase	Phase Objective	ICAM Considerations
<b>Pre-Select</b>	Assess the business needs and resource requirements for the investment.	<ul style="list-style-type: none"> <li>Investment business plans should state use of the PIV card for authentication within the security planning.</li> <li>Educate Investment Review Board on ICAM requirements.</li> </ul>
<b>Select</b>	Ensure the selection of investments that best supports the mission and approach.	<ul style="list-style-type: none"> <li>Review investment for alignment with agency's ICAM segment architecture relative to accounts, authentication, access control, and auditing capabilities.</li> <li>Investment data architecture should be evaluated to guard against the redundant collection of identity data.</li> </ul>
<b>Control</b>	Take actions to ensure investments will deliver the projected benefits through quality control and executive review.	<ul style="list-style-type: none"> <li>Ensure that investment is properly integrated and aligned with the agency's ICAM infrastructure.</li> <li>Oversee development of investment and integration with enterprise ICAM services.</li> </ul>
<b>Evaluate</b>	Evaluate and analyze if investments have delivered what was expected, while remaining cost effective.	<ul style="list-style-type: none"> <li>Investment should document and demonstrate return on investment (ROI) realized through use of ICAM infrastructure security services.</li> <li>Determine opportunities to improve efficiency and update investment as enterprise ICAM capabilities mature.</li> </ul>

**Figure 66: ICAM Considerations within the CPIC Process**

As part of the FY11 budget submission cycle, OMB provided additional guidance to agencies related to their ICAM program and the use of PIV cards across all IT investments. The following table summarizes this guidance.

Fiscal Year	OMB Guidance
<b>2010</b>	<p>Complete detailed transition plans documenting efforts to align with the FICAM Roadmap. Plans should address use of electronic capabilities of HSPD-12 credentials to improve the agency's security posture.</p> <p>All new (unclassified) logical and physical access control systems must be enabled to accept HSPD-12 credentials for authenticating federal employees and contractors.</p>

Fiscal Year	OMB Guidance
<b>2011</b>	Agencies must use Development, Modernization, and Enhancement (DME) and/or Operations and Maintenance (O&M) funding to upgrade existing Physical Access Control Systems (PACS) and Logical Access Control Systems (LACS) to use HSPD-12 credentials.
<b>2012</b>	Agencies shall not spend DME and/or O&M funding on systems unless they use HSPD-12 credentials.

**Figure 67: OMB Budget Guidance**

As a result of this guidance, agencies must implement use of the PIV card for authentication within all IT systems (as defined in the ICAM target state architecture) in order to receive future investment funding from OMB. This begins with new investments in FY10 and extends to funding for existing investments in FY12. The guidance also requires agencies to begin detailed planning for aligning their investments with the ICAM segment architecture.<sup>77</sup> These requirements are reinforced by OMB M-11-11,<sup>78</sup> which provides guidance on the continued implementation of HSPD-12.

Agencies need to incorporate planning for PIV-enablement and alignment with the ICAM segment architecture when completing capital planning activities and preparing their budget submissions. As part of its adoption into the Federal Enterprise Architecture (FEA), the ICAM segment architecture was added and assigned a segment code in the Enterprise Architecture Segment Report (EASR).<sup>79</sup> Agencies must code relevant ICAM costs to the ICAM segment code and report them as part of their budget submissions via the Exhibit 53. The following figure provides a summary of multiple common ICAM-related cost categories, which an agency can leverage to help determine and report their ICAM costs in an organized manner.

Cost Category	Description
<b>New User Identity Proofing</b>	Costs associated with proofing the identity of new users at the necessary level of assurance .
<b>Integration</b>	Integration costs from contractor services and additional software/hardware required for integration and testing.
<b>Software</b>	Cost of software including licenses and maintenance fees that could be decommissioned or redeployed across all environments for development, testing, and production.
<b>PKI software</b>	Licensing costs for PKI software as well as vendor maintenance fees to support all environments for development, testing, and production.
<b>Help desk calls</b>	Costs associated with the number of password related calls received by an agency.
<b>Hardware</b>	Cost of hardware that could be decommissioned or redeployed across all environments for development, testing, and production.
<b>IT Operations Services</b>	Costs of backups, monitoring, new development, enhancements, etc. across all environments for development, testing, and production.
<b>Training</b>	Costs associated with training and creating/acquiring materials for new software and services installation, integration, maintenance, business processes, and end user support.

<sup>77</sup> The ICAM segment architecture (Part A of this document) has been adopted as part of the Federal Enterprise Architecture (FEA), as an agency requirement. The FEA Framework was created in response to [Executive Order 13011](#), ‘Federal Information Technology,’ The White House, July 16, 1996. [E.O. 13011]

<sup>78</sup> [M-11-11](#), Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors, OMB, February 3, 2011. [M-11-11]

<sup>79</sup> [EASR](#)

Cost Category	Description
<b>Policy Compliance</b>	Costs associated with bringing the system into compliance with applicable ICAM policies.

Figure 68: ICAM Cost Categories Summary<sup>80</sup>

### 6.2.3. Enterprise Architecture

In general, 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||). Successful EA enables an agency to maximize the contribution of its resources, IT investments, and system development activities to achieve its performance goals. The FEA 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.

The development of the ICAM 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 budget submissions going forward. Agencies must develop a work plan for completing the transition activities and achieving the target state identified therein, as required by M-11-11.<sup>81</sup> In addition, the ICAM segment architecture and the agency detailed work plan should be thoroughly reviewed when determining which investments to submit for funding through the annual budget cycle.

Many agencies have already taken steps to integrate the ICAM segment architecture into their own agency EA programs. Such adoption of the ICAM segment architecture and its use 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. Additionally, conformance with the ICAM Segment Architecture will minimize the risk associated with an agency's IT security program.

### 6.2.4. IT Security and Risk Management

IT Security involves protecting the confidentiality, integrity and availability of information. Agencies are required to perform a risk assessment on a system to determine the extent of potential threats associated with it. Risk assessments assist agencies in determining the proper security mechanisms for information systems commensurate with their level of risk. According to NIST SP 800-30,<sup>82</sup> —Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the information systems and data that support their organization's mission.||

Since ICAM includes the management of identity data, accounts, and access, it is intrinsically linked to an agency's IT security program. As a result of this linkage, ICAM solutions are capable of supporting innovative approaches for IT risk management, ICAM implementations also offer the ability to support required information system security controls using common

<sup>80</sup> Cost category information has been adapted from the Agency E-Authentication Cost Template

<sup>81</sup> [M-11-11](#)

<sup>82</sup> [SP 800-30](#), Risk Management Guide for Information Technology Systems, NIST, July 2002. [SP 800-30]

services for the entire organization, significantly streamlining the accreditation process. The following subsections discuss, in greater detail, the ways in which ICAM systems impact and are impacted by IT security and risk management processes.

ROI	Implementing proactive security controls, such as those offered by enterprise ICAM services, can save an agency money through risk avoidance. The average organizational cost of a data breach in 2010 was \$7.2 million, an average of \$214 per compromised account. Proactive measures cost organizations significantly less, with the average cost for detection and escalation being \$13 per record and \$51 during ex-post response. <sup>83</sup>	
-----	---	--

#### **6.2.4.1. Risk Management Framework for Information Systems**

Information systems implemented as part of an agency's ICAM program must meet all relevant Federal Information Security Management Act (FISMA) requirements, including application of the IT Risk Management Framework (RMF) defined in NIST SP 800-37.<sup>84</sup> The RMF is a security life cycle approach that was designed to help agencies build information security capabilities into their information systems, better monitor the real-time security status of those systems, and provide relevant information to agency leadership to enable risk-based decisions associated with their operation. The RMF includes six steps, which an agency must apply to its ICAM systems in order to select, implement, assess, and authorize the appropriate system security controls and adequately monitor the effectiveness of those controls on an ongoing basis to support responsibility and accountability in the overall security of the system.

FAQ	What is the difference between the Certification and Accreditation (C&A) process and the Risk Management Framework (RMF)?  The six-step RMF fundamentally transformed the previous C&A process to allow an organization to track the security state of an information system on an ongoing basis and maintain the security authorization for the system over time. The C&A process was not an on-going, multi-step approach like the RMF life cycle process. This life cycle gives agencies the flexibility to alter, enhance, or reassess the security controls employed in their information systems continuously and easily.	
-----	---	--

The six steps in the RMF life cycle are summarized in the following figure. The RMF framework allows agencies to move from and between steps as needed and allocate resources to each step as they deem appropriate; however, equal emphasis should be placed on each step.

Step	Step Description	Objectives
1	<b>CATEGORIZE Information System</b>	<ul style="list-style-type: none"> <li>• Categorize information and information systems based on mission and business objectives of the agency</li> <li>• Describe each information system, including: full name with acronym, location of the system, version number, types of information held in the system, system owner, and other specific agency requirements</li> <li>• Register the information system within specified program offices</li> </ul>

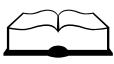
<sup>83</sup> 2010 Annual Study: U.S. Cost of a Data Breach, Compliance pressures, cyber attacks targeting sensitive data drive leading IT organizations to respond quickly and pay more, March 2011.

<sup>84</sup> [SP 800-37](#), Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, NIST, February 2010. [SP 800-37]

Step	Step Description	Objectives
2	<b>SELECT Security Controls</b>	<ul style="list-style-type: none"> <li>Select the appropriate security controls for the information system and document the controls in the security plan</li> <li>Develop a continuous monitoring strategy to determine the ongoing effectiveness of security controls and any changes to information systems</li> <li>Review the proposed security controls; ensure that the security plan has identified any possible risk to the agency</li> </ul>
3	<b>IMPLEMENT Security Controls</b>	<ul style="list-style-type: none"> <li>Implement security controls from the security plan (created in step 2)</li> <li>Document the implementation of the security controls in the security plan</li> </ul>
4	<b>ASSESS Security Controls</b>	<ul style="list-style-type: none"> <li>Create and approve a security assessment plan of the security controls and ensure assessors follow the documented procedures in the plan</li> <li>Document any problems or recommendations from the assessment in an assessment report and adjust appropriate security controls, if needed</li> </ul>
5	<b>AUTHORIZE Information System</b>	<ul style="list-style-type: none"> <li>Create a plan of action based on findings from the security assessment report; when completed, submit to the authorizing agency official for review</li> <li>The authorizing official reviews and determines the risk to the organizational operations, such as mission or assets</li> </ul>
6	<b>MONITOR Security Controls</b>	<ul style="list-style-type: none"> <li>Review and determine the security impact of any changes to the information system</li> <li>Make updates to the security plan, security assessment report, and plan of actions as needed during the continuous monitoring process</li> <li>Following the monitoring strategy set forth, report the security status on a continual basis</li> </ul>

**Figure 69: Summary of the Risk Management Framework**

As an agency implements ICAM, many other IT risk requirements and controls are achieved. For example, the final step in the RMF is monitoring security controls. Several of the enterprise services provided by ICAM (see Services Framework in Section 3.2.4), including automated auditing and reporting, can be used to implement an agency's continuous monitoring capability. These services provide a common control across an agency's information systems, which in turn support the RMF objective of leveraging inherited common controls to the maximum extent possible. This allows an agency to increase the consistency, effectiveness, and timeliness of security control implementation within its information security program and more effectively manage risk.

Terminology	
<b>Continuous monitoring</b> – One of six steps in the Risk Management Framework (RMF) described in NIST SP 800-37. The objective of a continuous monitoring program is to determine if the complete set of planned, required, and deployed security controls within an information system (including its environment of operation) or inherited by the system continue to be effective over time in light of the inevitable changes that occur.	

Due to the privacy, data security, and trust concerns associated with the credentials and information processed by PIV credential systems, HSPD-12 applications are subject to additional assessment and authorization requirements in addition to the requirements placed on all information systems. For example, PIV Card Issuers (PCI) are subject to additional assessment of security requirements and controls to establish and maintain a known level of trust in the

credential issuing processes, so that trust can be extended to the authenticity of the credential. The PIV card specific requirements are found in NIST SP 800-79,<sup>85</sup> including:

- **Organizational Preparedness.** Relates to the overall level of engagement of senior management regarding the formation and operation of the PCI. Roles and responsibilities must be clearly identified, and policies and procedures must be defined, documented, and put in place.
- **Security Management & Data Protection.** Concerns the provisioning of adequate measures (e.g., management procedures, operational controls, technical protections) to ensure that privacy requirements are addressed, the rights of individuals are acknowledged, and personal data are protected.
- **Infrastructure Elements.** Represents the sum of the activities required to procure, deploy, and maintain the PCI information system components. PCI information system components (e.g., PKI, biometrics, and card production) must meet the technical specifications defined in FIPS 201 and related documents. Additionally, information systems used within the PCI need to be assessed and authorized under SP 800-37 for FISMA compliance.
- **Processes.** Classes of functions that collectively span the entire PIV card life cycle activities such as sponsorship, enrollment/identity proofing, adjudication, card production, card activation/issuance and maintenance.

Advancements in PACS technologies, the emergence of enterprise models for PACS, and increasing interconnectivity with agency networks have highlighted the fact that PACS are comprised of components from both physical security and information systems. As such, they are subject to the RMF process and conformance with the security controls applicable to information systems.

#### **6.2.4.2. Security Controls**

The RMF provides the process for selecting, implementing, assessing, and monitoring security controls. An agency must incorporate considerations for these controls throughout the life cycles of information systems supporting its ICAM program. Additionally, many of the control families identified in NIST SP 800-53<sup>86</sup> incorporate ICAM in their execution. Due to this interrelationship, an ICAM implementation contributes to the FISMA compliance of a wide variety of information systems. This impact affects both the FISMA reporting process and the security of every application that the ICAM solution interacts with. Figure 70 below describes the key SP 800-53 control families that are related to and impacted by ICAM implementations:

Control Family	Description	Relationship to ICAM
<b>Access Control (AC)</b>	Controls falling under the AC category ensure that proper restrictions are in place to limit access to authorized users with a need to know.	<ul style="list-style-type: none"> <li>• IT resources use the ICAM program as their primary means of access control.</li> <li>• ICAM strengthens access control methods through the use of centralized account management, Role-Based Access Control (RBAC), etc.</li> </ul>

<sup>85</sup> [SP 800-79](#), Guidelines for the Accreditation of Personal Identity Verification Card Issuers, NIST, June 2008. [SP 800-79]

<sup>86</sup> [SP 800-53](#), Recommended Security Controls for Federal Information Systems and Organizations, NIST, August 2009. [SP 800-53]

Control Family	Description	Relationship to ICAM
<b>Audit and Accountability (AU)</b>	Controls falling under the AU category ensure that applications properly record and review records of specific user actions.	<ul style="list-style-type: none"> <li>ICAM presents agency implementers the opportunity to eliminate redundancy and increase accountability across the enterprise by centralizing audit capabilities within the ICAM.</li> <li>Centralized audit capabilities enable the recording of actions at the user level for all IT resources that interact with the ICAM solution.</li> <li>The redundancy from having all IT resources maintain separate audit logs is reduced.</li> <li>Security is increased by providing a broader, centralized view of user actions across multiple applications.</li> <li>ICAM implementers should determine an agency's individual audit requirements and design ICAM audit capabilities to meet these individual needs.</li> </ul>
<b>Security Assessment and Authorization (CA)</b>	Controls falling under the CA are in place to ensure that an agency has the necessary processes in place to monitor the needed security controls.	<ul style="list-style-type: none"> <li>ICAM implementers need to meet annual FISMA CA requirements.</li> <li>ICAM implementers can leverage the parent control system interface connections to enable identity data sharing.</li> </ul>
<b>Identification and Authentication (IA)</b>	IA controls are in place to ensure that users and devices are properly authenticated prior to allowing access to an IT resource.	<ul style="list-style-type: none"> <li>ICAM implementations will simplify compliance with IA controls for all applications as agencies standardize on the PIV credential for internal users.</li> <li>ICAM implementations will simplify compliance with IA controls as agencies enhance security and trust in authentications by incorporating electronic identification techniques.</li> </ul>
<b>Physical and Environmental Protection (PE)</b>	Controls falling under the PE family are in place to ensure that an agency and its applications have proper processes and technology in place to prevent intrusion and damage to the physical environment (buildings, secured rooms, etc.), provide emergency resources, and monitor physical access of personnel and visitors.	<ul style="list-style-type: none"> <li>The authentication support provided by ICAM implementations mentioned in the IA control family applies equally to authenticating people to a physical environment.</li> </ul>
<b>Risk Assessment (RA)</b>	Controls falling under the RA family are in place to ensure that an agency has the proper processes in place to adhere to their risk policies and adjust as risks change.	<ul style="list-style-type: none"> <li>ICAM implementers should formally document their risk assessment policies and coordinate among components within the agency.</li> <li>ICAM implementers should regularly review and update their current risk assessments.</li> </ul>

**Figure 70: NIST SP 800-53 Control Families and Relation to ICAM**

In addition to the specific control families mentioned above there are numerous other security controls that are interrelated with identity management. ICAM solutions have the potential to provide the means to execute many of these controls when properly designed. Involving security personnel throughout the ICAM implementation planning and design phases will not only impact the security of the ICAM solution itself, but also opens up the opportunity to support the agency's overall security mission.

## 6.3. Privacy Considerations

ICAM programs have significant privacy implications for federal agencies and must be treated accordingly. These implications must be carefully considered by agencies to mitigate potential privacy risks, while still providing the security intended for the identity management systems (IDMS). Therefore, privacy should be considered an essential component and mission critical objective for all ICAM implementations and agency implementers should understand and integrate privacy principles into ICAM programs early in the design stage. This section introduces the Fair Information Practice Principles (FIPPs) and discusses how they can be appropriately integrated into an agency's ICAM program. The information and guidance presented in this section is intended to assist agencies in providing answers to several common ICAM-related privacy questions, including:

- What are the Fair Information Practice Principles and how do they apply to my agency's ICAM program?
- What processes must my agency complete in order to meet applicable privacy requirements?

### 6.3.1. Applying the FIPPs

Since ICAM programs involve the collecting, storing, sharing, and maintenance of Personally Identifiable Information (PII), federal agencies must implement solutions that actively support privacy protections and the widely-recognized FIPPs. Under the Privacy Act, which is based on the FIPPs, agencies are required to have certain processes and procedures governing their use of PII in place. Agencies should first assess those processes and procedures and determine whether the implementation of an ICAM program constitutes a new use of PII that requires adjustment of existing processes and procedures. The following figure provides a description of each of the FIPPs and discusses practical implementation considerations for applying them within an ICAM program.

Fair Information Practice Principle	Description	ICAM Implementation Considerations
<b>Individual Participation</b>	Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.	Agencies that currently interact with the public in a face-to-face context and/or engage in paper/telephone transactions must recognize that there will continue to be individuals who will not feel comfortable adopting technological processes. They should continue to offer physical alternatives for processes that are not inherently technology-based. Agencies should also provide redress mechanisms in accordance with the Privacy Act that allow individuals to report and correct information that is inaccurate, lost, or compromised and damages resulting from incorrect authentication or unauthorized access. Redress mechanisms help enhance confidence in the program and promote individual participation.
<b>Transparency</b>	Agencies should be transparent with respect to the information they collect and share, and provide notice to the individual regarding collection, use, dissemination, and maintenance of PII.	A foundational principle in federal privacy law is that an individual has the right to know what information the government collects and retains about him and, to a great extent, the right to control how that information is being used. When building ICAM programs, agencies should, first and foremost, consider this principle and ensure the following prior to each

Fair Information Practice Principle	Description	ICAM Implementation Considerations
<b>Purpose Specification</b>	Agencies should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.	<p>occurrence of information collection and/or transmission:</p> <ul style="list-style-type: none"> <li>• The user is clearly informed what information elements will be collected</li> <li>• The user understands who will receive the information</li> <li>• The user is clearly informed of how the information will be used</li> <li>• The user must affirmatively choose to participate before any information is transmitted</li> </ul>
<b>Data Minimization</b>	Agencies should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).	Agencies should only collect the information necessary to carry out ICAM business functions. Wherever possible, agencies should use assertions of an individual's identity in lieu of identifying data elements. For example, if an application has an age limitation, the program should ask for proof of age rather than the exact birth date. Agencies should also determine how long specific categories of information associated with ICAM processes will be retained and implement procedures for destruction of the information at the end of the retention period.
<b>Use Limitation</b>	Agencies should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.	The Privacy Act generally requires that once an individual consents to the collection of his information for a specific, stated purpose, that information can only be used for that purpose. This is particularly important to remember when considering the sharing of information between programs. If the programs have different purposes, such sharing will likely not be permissible without additional consent from the user. Agencies should carefully consider this limitation when crafting their privacy notices for ICAM programs.
<b>Security</b>	Agencies should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.	Agencies must ensure the security of information at all stages (collection, transmission, storage, destruction) in accordance with various legal and policy requirements (e.g., FISMA and OMB M-07-16). <sup>87</sup> Examples of techniques for securing data are encryption, strong authentication procedures, time out functionality, and minimum security controls to make information unusable by unauthorized individuals.
<b>Data Quality and Integrity</b>	Agencies should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.	Agencies should identify and implement means to ensure that PII is accurate, relevant, timely, and complete, including providing mechanisms for individuals to correct inaccuracies in their information.
<b>Accountability and Auditing</b>	Agencies should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.	ICAM implementers should establish accountability measures to ensure that each of the FIPPs is appropriately applied and effectively protect users' privacy. Such measures can include ICAM program audits and reviews by agency privacy and security officials. Agencies should address accountability for specific requirements, such as the M-07-16 requirement for annual certification of training for employees who handle PII. Clear accountability will promote confidence in ICAM programs.

**Figure 71: Applying the FIPPs to ICAM**

<sup>87</sup> [M-07-16](#), Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007. [M-07-16]

Adopting the FIPPs to support privacy-protecting ICAM solutions requires deliberate effort. One example of such an effort is the development of the privacy requirements of the TFPAP, which aims to enable the Federal Government to leverage third-party credentials that citizens already have for other purposes. In order for an external entity to be certified to provide credentials for use by the Federal Government, it must demonstrate compliance with a rigorous set of privacy requirements built around the FIPPs. This topic is discussed in greater detail in Chapter 12.

### 6.3.2. Programmatic Support

All programs that collect, retain, or use personal information are required to complete and maintain program documents to support these activities. Such processes for determining policies and rules around collection and use of information ensure that agencies are not creating an unnecessary burden on individuals; nor are they collecting or using information for purposes that are not consistent with the intent of the program. Agencies should be extremely clear and thorough when developing the documentation to support the collection, use, and retention of personal information. Below are processes that agencies must complete in order to meet key privacy requirements:

- **System of Records Notice (SORN).** A notice published by an agency in the Federal Register to notify the public of a system of record, a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier assigned to the individual. The SORN includes basic information about the system, including system name, categories of individuals covered by the system, and categories of records in the system and addresses the policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system.
- **Privacy Impact Assessment (PIA).** The process used to evaluate the potential ramifications to the protection of privacy within IT systems. The resulting document includes information related to the data in the system, access to the data, attributes of the data, and maintenance of administrative controls for protecting it. An agency must complete a PIA whenever a new system is being introduced or an existing system is substantially modified.
- **Establishment of redress procedures.** Procedures to allow an individual to review his record in an IT system upon request and permit the individual to request amendment of a record pertaining to him. In addition to enabling an agency to meet the requirements of the Privacy Act of 1974, redress procedures also help enhance transparency, raise the awareness of the mission, and promote user confidence.

#### Privacy Tip

It is encouraged that ICAM implementers provide redress mechanisms even when not required by the Privacy Act. Enabling users to file complaints and comments regarding an ICAM program and rectify this if their information is inaccurate, lost, or compromised will promote confidence in their interaction with the government.



## 7. Initiative 5: Streamline Collection and Sharing of Digital Identity Data

Initiative 5 of the ICAM Transition Roadmap, as discussed in Section 5.2.2, is an agency-level ICAM implementation initiative that includes activities required to eliminate inefficiencies and redundancies in the collection and maintenance of identity data. It also aims to mitigate security and privacy risks associated with current identity data management processes. Digital identity, a foundational component of ICAM, is an electronic representation of an individual that is composed of identity attributes. The transition activities associated with Initiative 5 require that agencies eliminate the manual, redundant, and often paper-based collection of identity attributes in favor of implementing an automated method of collecting identity data once, storing it in authoritative source systems, and sharing when necessary to support the agency's mission. Additionally, agencies are expected to establish an Authoritative Attribute Exchange Service (AAES), as defined in the ICAM Services Framework (Section 3.2.4), to enable secure electronic sharing of identity attributes.

This chapter is organized into the following three core sections:

- **Enterprise Digital Identity.** This section defines the enterprise digital identity and discusses the concepts of core identity attributes and unique person identifiers. It also provides guidance for identifying the authoritative sources, which house attributes that comprise the enterprise digital identity.
- **Digital Identity Process Integration.** This section provides guidance for streamlining and integrating business processes for establishing and managing the digital identity life cycle.
- **Authoritative Digital Identity Attribute Exchange.** This section provides guidance for implementing an AAES capability, which enables secure electronic sharing of digital identity attributes. It also discusses how an agency might leverage existing data exchange models to support effective sharing of digital identity data.

### 7.1. *Enterprise Digital Identity*

An agency collects digital identity data for individuals (i.e., employees, contractors, and individuals with staff-like access<sup>88</sup>) in order to support the agency's core business operations, issue credentials, and administer access to an agency's physical and logical resources. Therefore, in order to ensure that access control decisions across the agency are based on accurate and current information, digital identity data must be reliably managed over time. To support this need, the ICAM segment architecture emphasizes the importance of an enterprise digital identity. The enterprise digital identity is a single digital representation of an individual's identity, maintained at an enterprise level, which leverages attributes from authoritative source systems. As discussed in Section 4.1, this target state vision differs from most agency environments, where agencies typically rely on locally managed user identity accounts comprised of redundantly collected identity attributes.

---

<sup>88</sup>These individuals have access to similar internally facing applications and resources that employees and contractors may have and subsequently go through a comparable process to gain this access.

This section provides guidance for defining identity attributes that make up a digital identity and, if needed, employing a unique person identifier to bind those attributes to an individual. This section also discusses how to determine authoritative sources of identity data and take necessary steps to leverage these data sources. The information in this section seeks to provide answers to several common digital identity questions, including:

- How do I determine what identity attributes are needed to identify a person within my agency?
- How do I discover or locate authoritative data sources for particular identity data attributes in my agency?
- How are authoritative data sources designated and protected?
- What approaches exist to help my agency manage digital identities more effectively?

### 7.1.1. Core Identity Attributes

An agency typically collects a wide variety of data elements about its users. Within this data set, smaller subsets of attributes enable an agency to uniquely identify an individual within the organization and supports execution of meaningful access control decisions. Use Case 1, Create and Maintain Digital Identity Record for Internal User (Section 4.1), defines this data subset as the core digital identity. A key enabler for agencies to move toward the target state approach for core digital identities is the development of a common government-wide Core Person Model needed to manage and share digital identity records.

As part of Initiative 1: Augment Policy and Implementation Guidance to Agencies, the ICAM Subcommittee developed the government-wide Core Person Model (also referred to as the digital identity data specification in Section 5.2.1.1) for use by agencies working to align with the ICAM segment architecture. This specification was developed through an analysis of numerous existing agency person models and a collaborative consensus process within the ICAM Subcommittee. As shown in Figure 72, the Core Person Model provides a common definition for the attributes that comprise a digital identity record within the Federal Government. An agency should use the Core Person Model when working to establish enterprise digital identities.

Attribute	Description
Person Identifier	Uniquely identifies an individual within a specified domain in which the person exists (e.g., Locally Unique Identifier [LUID] associated with the Backend Attribute Exchange [BAE] <sup>89</sup> )
Name	An individual's name, typically including first, middle, last, and display names.
Set of Biometrics	Represents a measured biological or behavioral characteristic of an individual (e.g., electronic fingerprint template, facial image).
Physical Description	Describes an individual's physical characteristics (e.g., height, eye color, hair color, sex).
Birth Record	Pertains to the place (city, state, and country) and date of an individual person's birth record.
Contact Information	Includes an individual's phone number(s) and work mailing address.
Set of Credentials	Relates to one or more identity credentials possessed by an individual (e.g., credential sponsor, FASC-N, serial number(s), issuer, revocation uniform resource identifier [URI], etc.).

<sup>89</sup> As specified in the [BAE Version 2.0 Overview Document](#).

Attribute	Description
Set of Citizations	Corresponds to an individual's country or countries of citizenship, commonly expressed as a digraph or trigraph.
Set of Email Addresses	Corresponds to an individual's current and historical email addresses.
Set of Clearances	Corresponds to an individual's background investigation and/or clearance history (e.g., investigation type, completion date, status, etc.).
Set of Affiliations	Corresponds to an individual's affiliation with an organization (e.g., employee status, business relationship, etc.).
Social Security Number (SSN)	An individual's SSN or other national ID with a corresponding country code for foreign nationals.

**Figure 72: Core Person Model Attributes**

The attributes identified in the government-wide Core Person Model are intended to serve as a baseline. It is expected that agencies may need to supplement the model with additional attributes that support the agency's mission-specific business needs. Although these additional attributes are not addressed directly in this chapter, an agency should work to streamline and consolidate the processes for storing and managing them wherever possible. In order to fully leverage the Core Person Model, an agency should consider the following:

- **Identify where each data element is collected and stored.** Among the first steps that an agency will need to take when adopting the Core Person Model is determining where each attribute is stored within the agency. This often involves determining which offices or groups within the agency are responsible for collecting and maintaining those data elements. The data elements may be located in multiple, redundant locations. Guidance related to resolving conflicts between source systems is discussed in Section 7.1.3.
- **Map agency data to the model.** Once an agency identifies the location of each data element, it should map its data model to the Core Person Model to tailor it for agency use.
- **Determine additional core data elements, if necessary.** As noted previously, an agency may find that additional attributes are necessary to support its implementation of the Core Person Model. These additional attributes should be limited to those elements that are needed to uniquely identify an individual within the organization and support the agency's specific mission needs. Additional identity attributes may be collected to support enhanced access control scenarios; however, these attributes are considered entitlement attributes,<sup>90</sup> not part of the basic digital identity record.
- **Identify opportunities for process integration.** A key driver for establishing a core digital identity is the ability to eliminate redundant collection and maintenance of digital identity data. An agency should identify redundancies in data collection associated with the Core Person Model and determine opportunities to integrate and streamline these business processes by leveraging existing identity data.

Managing a digital identity at an enterprise level by leveraging core digital identities can provide agencies with a number of benefits, including:

- **Eliminating redundant identity data creation.** Establishing enterprise digital identity records allows an agency to reduce or eliminate the need for excess business processes that may collect redundant identity data for specific application use.

---

<sup>90</sup> Collection and use of application-specific entitlement attributes are covered in Chapter 9.

- **Enabling interoperability and more robust identity attribute sharing.** Aligning with the Core Person Model for digital identity data at the enterprise level provides an agency with a common basis for sharing identity attributes across an agency. When combined with the establishment of attribute management and distribution services, this enables an agency to offer enhanced attribute sharing capabilities for use by programs and applications across the organization.<sup>91</sup>
- **Streamlining identity life cycle management.** Establishing an enterprise digital identity and processes for maintaining data as it is updated in authoritative sources greatly reduces the administrative burden associated with identity life cycle management while improving data quality and accuracy.
- **Increasing the accuracy and reliability of provisioned identities.** The basic data associated with a user account should be established and updated based on enterprise digital identity data (see Section 9.2.3 for additional information). This approach provides consistency across enterprise identities and improves the accuracy of user account data established through automated provisioning workflows.

### 7.1.2. Authoritative Data Sources

The ICAM target state calls for agencies to end redundant collection and maintenance of identity data and to focus on leveraging accurate and reliable data stored within authoritative data sources. An authoritative data source for identity is a repository or system that contains attributes about an individual and is considered to be the primary or most reliable source for this information. In the case that two or more systems have mismatched or conflicting data, the data within the authoritative data source is considered to be the most accurate. Within many federal agencies, authoritative identity data is dispersed across a number of different systems that are often independently managed. Some agencies, however, may operate a single centralized repository of identity data, such as an Identity Management System (IDMS). While an agency is not required to have a single repository of identity data, it is expected that agencies will designate an authoritative data source for each data element in the Core Person Model and work to minimize the number of data sources used to collect and maintain the same identity information. In cases where an agency houses identity data elements across several authoritative data sources, it is recommended that it share or map identifiers between the data sources in order to avoid collisions and errors, as discussed in Section 7.1.2.

#### Lesson Learned

Sometimes identifying an authoritative source can lead to other efficiencies. Treasury identified HRConnect as its authoritative source of core identity data for employees and contractors. As a result, Treasury was able to establish HRConnect as the originator of the Treasury Unique Identifier (TrUID), which is used to link users in USAcces, Treasury Enterprise Directory, and bureau Identity Management Systems (IDMS) through the user's lifecycle. This approach is envisioned to dramatically improve the data quality within the agency and reduce the amount of redundant data collection.



<sup>91</sup> See Section 7.3.2 for a sample Authoritative Attribute Exchange Service solution design and architecture.

### 7.1.2.1. Authoritative Data Source Identification

One of the first hurdles that many agencies encounter is determining which systems/resources are authoritative for specific identity attributes. This authoritative source discovery process involves determining where identity attributes are first recorded and updated. In order to accomplish this, agencies must first determine where identity data is stored within the organization and then perform an analysis to identify which of those source systems should be designated as authoritative. As part of complying with HSPD-12, many agencies have already identified authoritative data sources for the data elements that are required as part of the PIV enrollment and issuance process. It is likely, however, that an agency will need to conduct additional authoritative source discovery in order to identify an authoritative source for each of the data elements contained in the Core Person Model.

#### Implementation Tip

Many agencies maintain an inventory of systems and applications that house Personally Identifiable Information, often referenced in Systems of Records Notices (SORNs). This inventory can provide a starting point for determining which agency systems can serve as authoritative data sources for identity attributes. As a SORN specifies the permissible, or routine, uses of the data in a particular system of records, it will need to be modified if the information will be used in a different way than originally anticipated.



In general, many authoritative data sources share a number of common characteristics that agencies should look for as part the discovery process. Figure 73 provides a description of these characteristics.<sup>92</sup>

Characteristic	Description
Primary Source	A data source where an identity data element originates. The data is not received from another system or resource.
Legal Authority to Collect	A data source that generally operates with a legal authority to collect certain data elements as part of the organization's mission (e.g., HR has the legal authority to collect identity data within federal agencies).
Data Accuracy	A data source that is generally considered to be accurate and reliable for a specific identity attribute(s) at any given time.
Data Freshness	A data source that contains the most up-to-date data available and is generally the first system to be updated when data changes.
Data Accessibility	A data source that limits the availability of certain data elements to those individuals or groups that have a need to know.
Data Protection	A data source that has restrictions in place that limit the ability to change stored data to a select group of users.
Data Ownership	A data source that is generally owned and maintained by groups that own the data itself and can vouch for its authenticity.
Data Modification	A data source that performs modification of data originated elsewhere (e.g., updating identity attributes for use in downstream processes, data normalization) and becomes authoritative by virtue of performing the modification.

Figure 73: Common Characteristics of Authoritative Data Sources

During the process of identifying and designating authoritative data sources, an agency should document and map core digital identity data elements based on how the data is originated, types of transformations that occur to the data, and where the data is stored. It is possible for one

<sup>92</sup> Characteristics of authoritative data sources have been abstracted from [NIST IR 7657](#), A Report on the Privilege (Access) Management Workshop, March 2010. [NIST IR 7657]

system to be authoritative for data element creation and a second system to be authoritative for data element modification. For example, an employee's initial building and room number may be created in the PACS, whereas subsequent changes to building a room may be handled in an employee locator system. It is still important to ensure that there is only one authoritative source for data creation and only one for data modification.

Identifying and designating authoritative data sources will help agencies understand where their identity data is input and how they are used throughout the enterprise. This mapping should be extended to downstream processes to streamline the flow of identity data (e.g., name and work address data are required downstream by the mail application). It will also help to understand where data needs to be shared across the agency. Once an agency has analyzed its data sources using the characteristics discussed in Figure 73 and determined which source(s) are authoritative for each attribute, it can begin preparing its identity data for consumption throughout the enterprise.

#### **7.1.2.2. Authoritative Sources Data Preparation**

Data preparation and cleanup is needed to remove redundancies and discrepancies in the data housed within authoritative data sources. The analysis discussed in the previous section should help identify where data is collected and identify any redundancies. If an agency has multiple authoritative sources, it should evaluate the merits of consolidating data sources where appropriate. As identity data from authoritative data sources is shared with downstream processes, further data preparation requirements will evolve (e.g., ensuring employment status information can be read by both LACS and PACS to trigger de-provisioning workflows).

An agency should perform real-time or periodic data synchronization in the authoritative data source as well as areas where the data is shared to ensure that identity data is current. For example, if the data attribute for an employee's bureau/component affiliation changes in the authoritative source, the change should be synchronized in other systems that use this data element. This is an important step in cases where identity attributes are used to determine access privileges on a resource.

Ideally, each identity data attribute within the Core Person Model should only be modified in one place. Applications and processes reliant on authoritative data should not have the capability to manipulate authoritative data. Instead, they should only consume data and make business decisions based on them. An agency should determine the logical place for updating each data attribute based upon the business processes that typically initiate the change (e.g., an agency personnel security system is a logical place for updates to background investigation status data).

An agency should define its processes such that the most accurate and recent identity data resides in the authoritative source. There may be cases in which a downstream application has more recent data than the data housed in the authoritative source. In such cases, an agency should be capable of processing and approving out-of-band change requests in order to ensure that the data in the authoritative data source is appropriately updated.

#### **7.1.2.3. Authoritative Data Source Security and Privacy Considerations**

Authoritative data sources, like all other federal information systems, are subject to the security and privacy requirements in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the Privacy Act of 1974. Section 6.2.4 provides guidance on applying

FISMA security requirements and associated security controls to ICAM programs and systems. Given the sensitive nature of the information contained within authoritative identity data sources, an agency should closely observe the requirements outlined in FISMA and consider implementing optional enhancements to provide an additional measure of security, if justified based on the information system risk classification. Potential enhancements include:

- **Enforce strict access permissions.** In the ICAM target state, authoritative identity data is used across the organization to support a variety of ICAM programs and business operations, and as such, data integrity is of paramount concern. A loss of data integrity within authoritative data sources can significantly impact the level of trust that consumer applications and external partners will place on the agency's identity data. Agencies should take steps to ensure that the information contained within authoritative data sources cannot be manipulated or changed without strict rules and enforcement mechanisms.
- **Appropriateness of data usage.** All IT systems are subject to some degree of audit and reporting requirements under FISMA; however, agencies should take additional measures to ensure that data usage or exchange stemming from authoritative data sources can be recorded and audited as a means of ensuring that data is accessed, used, and shared in accordance with security and privacy policies. The ICAM reporting and auditing capabilities discussed in Section 9.4 provide agencies with an opportunity to leverage existing investments to provide this level of functionality.
- **Employ security enhancements.** In order to take full advantage of the security requirements and capabilities outlined under FISMA, agencies should consider applying the security enhancements associated with high-impact systems, outlined in SP 800-53,<sup>93</sup> to authoritative identity data sources. Doing so requires that additional security controls are put in place to protect the system and its data.
- **Verify authoritative source authenticity.** It may be desirable for downstream applications that rely on identity data from authoritative sources to validate the attributes provided by the source. This typically includes verifying the identity of the source and the time at which it validated the attribute values. This can be accomplished by verifying a digital signature placed by the authoritative source around selected groups of attribute-value pairs or through the use of a real-time verification service.
- **Provide redress capability.** In accordance with the Privacy Act of 1974, an agency should ensure that users have redress capabilities to rectify errors associated with identity records. This capability not only improves the accuracy and freshness of authoritative data, but also provides a level of transparency for end-users and consumers of identity data.

#### Implementation Tip

Partially automating requests for redress within the standard IT environment can help speed up the processing time and improve data quality. However, requests for redress should never be processed without human review, because of the risk of falsification of identity details.



<sup>93</sup> [SP 800-53](#)

### 7.1.3. Managing Digital Identity Records

As discussed in the previous sections, adopting and implementing the Core Person Model and defining an authoritative data source for each of the specified attributes enables an agency to create enterprise digital identities based on accurate and reliable data. Full achievement of the ICAM target state, however, requires that agencies eliminate duplicate and/or redundant digital identity records to ensure that each federal user has only a single digital identity. Managing a single digital identity record for each user within the organization requires that an agency establish a process to link or bind identity attributes to the appropriate record. There are several common techniques for accomplishing this, which are discussed in the sub-sections that follow. An agency should evaluate each of these approaches and determine which method best meets its needs and aligns with existing or planned capabilities.

#### 7.1.3.1. Unique Person Identifiers

A unique person identifier is an alphanumeric string attribute that identifies or selects exactly one individual from a defined community (e.g., the current and former employees of an Executive Branch agency or department) in order to distinguish his/her enterprise digital identity from others, even in cases where the underlying identity attributes may be the same (e.g., two employees with the same name). Unique person identifiers are best utilized when performing direct access lookups of digital identities (e.g., provisioning user accounts), reconciling collisions between identity attributes that occur as a result of automated matching processes, and limiting data discrepancies when binding identity data to an individual across multiple agency systems. In cases where an agency chooses to implement a single enterprise system for managing identity data, unique person identifiers should be used to correlate identity data in advance of the implementation in order to ensure that the system is populated with accurate data. Despite any changes to an individual's role within the organization (e.g., a contractor becomes a federal employee), these identifiers are generally assigned to an individual as part of the initial on-boarding process and persist throughout the digital identity life cycle.

#### Lesson Learned

By integrating its State Global Identifier Database (SGID) directly into its HR Integrated Personnel Management Suite (IPMS) the Department of State is able to assign unique person identifiers immediately to all agency direct hires and ensure that all of the Department's HR systems use the same unique identifier for an individual when transferring data. This provides an increased level of data accuracy across the Department's systems and reduces the amount of time required to provision identities.



Agencies are not required to establish unique person identifiers in order to achieve alignment with the ICAM target state; however, doing so can significantly help streamline the processes required to manage digital identity and support the implementation of other ICAM programs, such as physical and logical access modernization efforts. Additional benefits of establishing a unique person identifier system within an agency include:

- **Mitigating data discrepancies.** Unique person identifiers provide agencies with the ability to correlate identity data for the same individual across multiple systems. Data collisions can occur when multiple systems contain different values for the same attribute or data element. Using a unique person identifier helps to easily detect and resolve conflicts between different sources of identity attribute data and helps to ensure the uniqueness of an identity across the enterprise.

### Implementation Tip

Place a strong emphasis on data quality and accuracy. As an agency moves toward leveraging an enterprise digital identity record, the accuracy of the underlying identity data becomes increasingly important in order to prevent propagation of data errors. Ensuring the accuracy of the digital identity data to which unique person identifiers are bound enables an agency to maximize their effectiveness and achieve the associated process efficiencies.



- **Streamlining digital identity creation.**<sup>94</sup> Binding identity attributes to a unique person identifier streamlines the processes for reconciling those attributes into a single digital identity by eliminating the need to manually correlate attributes across various source systems.
- **Enabling modernized access control.** Using a unique person identifier provides an agency with a greater degree of confidence when provisioning user access in an automated fashion because the identity attributes that are used to support authentication and authorization decisions are bound to an individual's digital identity through the unique identifier.
- **Streamlining federated identity management.** Establishing a unique person identifier provides agencies with a key through which identities can be correlated across agency boundaries, as appropriate. In a federated environment, this can be accomplished through the use of parallel person identifiers, in which two agencies share their unique person identifiers to correlate identity data between the two organizations. Alternatively, an agency can append an agency-specific code to its unique person identifier or choose to have its own agency-specific code appended to another organization's unique person identifier to extend the attribute's uniqueness and reciprocity across the broader Federal Government community.
- **Visibility into identity data.** The ability to uniquely identify a user allows an agency to better understand the user's role and entitlements across the enterprise. This data can be analyzed within an agency or between agencies for the purpose of account auditing, threat identification, privilege correlation, and compliance (e.g., detection of segregation of duties violations).

### Privacy Tip

Unique person identifiers, when used inappropriately, could be used to track or profile a user's access patterns across an organization. In order to mitigate this risk, an agency should work with its Privacy Office to establish agency-level policies or guidance around the appropriate use and consumption of unique person identifiers.



When implementing a system to create and manage unique person identifiers, an agency should take steps to ensure that these attributes are randomly generated, according to a common standard, algorithm, or naming convention, in a fashion where the identifier cannot be easily guessed by a third party. The identifier itself should not be based on commonly available information about the individual, such as date and place of birth, and such information about the user should not be able to be obtained by manipulation or reverse engineering.

<sup>94</sup> More detailed information can be found in Section 7.1.3.2.

### Implementation Tip

Request for Comments (RFC) 4122,<sup>95</sup> A Universally Unique Identifier (UUID) Uniform Resource Namespace, offers agencies a standardized approach for creating unique person identifiers using time-based, name-based, or random number algorithms. Leveraging an approach like RFC 4122 is the preferred approach to creating identifiers, as it results in an infinitesimally small chance of collision without the need for a managed identifier namespace.



Unique identifiers should not be derived from or linked to data that is subject to change, such as user biographic data or credential-specific numbers. For example, the Federal Agency Smart Credential Number (FASC-N) or optional Universally Unique Identifier (UUID) of the PIV card should not be used as a person's enterprise unique identifier if the intended use is to link the identity record to the user's active credential. These numbers are linked to a specific credential and change with each consecutive card issued to the same cardholder. Use of a card identifier may be a viable option for generating a unique person identifier if an agency is only seeking an authoritative originator for its unique numbers and the identifier will be able to persist across the user's digital identity life cycle. As an alternative, an agency should establish a separate unique person identifier attribute (i.e., not linked to a credential) that is specifically intended to support digital identity management for managed identities that will span multiple credentials.

### Lesson Learned

When implementing its Electronic Data Interchange Personal Identifier (EDIPI), DoD established a rule set to govern how this attribute could be used within the organization. The Department determined early on that such a rule set was critical to ensuring the effectiveness of EDIPI and helping to mitigate potential privacy risks associated with inappropriate user and activity tracking.



Although there may be multiple authoritative sources containing different sets of data about an individual, the unique identifier should be generated from one originator. Doing so eliminates the possibility of collision or conflict between identifiers issued from different sources. In some cases, it may make sense for an agency to generate a unique identifier with an existing system that houses digital identity data (e.g., HR or PIV card enrollment). Some of these systems, however, only contain identity data for a portion of the total user population and should be extended to include the entire intended user population if they will be used to create unique identifiers. It is also important that unique identifiers be reconciled on a regular basis to ensure there are neither redundant identifiers nor the same identities with different identifiers. If fraudulent enrollment is a concern, an agency can leverage one-to-many (1:n) biometric matching against the entire enrolled community to detect duplicate enrollments and reconcile individuals who may have more than one identifier.

<sup>95</sup> [RFC 4122](#), A Universally Unique Identifier (UUID) URN Namespace, Internet Engineering Task Force, July 2005.

### Implementation Tip

Treasury's HRConnect has been identified as the authoritative source of core identity data for employees and contractors within Treasury. As a result, HRConnect is the originator of the Treasury Unique Identifier (TrUID), which is used to link users in USAccess, Treasury Enterprise Directory, and bureau Identity Management Systems (IDMS) through the user's lifecycle. This approach dramatically improves data quality and reduces redundant collection of data.



An agency should also consider the life cycle of unique person identifiers and establish a policy to govern if and when identifiers for identities that are no longer valid can be recycled and reused. An agency's policy for the life cycle of unique person identifiers should seek to address the following:

- **Identifier longevity.** The length of the identifier (number of alphanumeric digits) and the size of the namespace may impact the amount of time that an identifier should remain active. An agency should set a life span (years) that must expire before an identifier could be recycled, which at a minimum should be at least as long as the potential life span of any archived records associated with the user.
- **Management of identifiers.** In addition to the regular management of identifiers that are in use, an agency should determine how identifiers will be managed for a user that has become inactive but may reinitiate his/her affiliation with the agency in the future. Doing so ensures that an identifier is not made available for re-use during the defined life span.
- **Temporary users.** In many cases, a portion of the user population may consist of temporary users that are not expected to return at any point in the future. An agency should determine if these users will obtain unique identifiers from the same system/process as other users or if a secondary namespace with lower longevity is needed.

#### 7.1.3.2. Multi-attribute Keys

In some cases, it may not be feasible or desirable for an agency to implement a single unique person identifier attribute for managing enterprise digital identity records. This approach would likely require an agency to modify existing systems and processes or stand up a new system to create and manage unique person identifiers. It is possible for an agency to achieve similar results and benefits to those described in Section 7.1.3.1 using a multi-attribute key to manage digital identities across the enterprise.

A multi-attribute key is a combination of identity attributes that can be bound to serve as an identifier for user records across multiple systems. This approach allows an agency to take advantage of data that is already available to the agency and would likely require less modification to existing systems. Additionally, multi-attribute keys provide a layer of redundancy, which can help address an error in a single attribute that is part of the key. If an error is present, an agency can analyze the other identity attributes within the key to reconcile the key to the record of the correct individual. This may be desirable to some agencies to mitigate the risks associated with poor data quality.

In order to establish a multi-attribute key, an agency must designate an attribute set (two or more identity attributes) to serve as key fields within its relational database system(s). An agency should choose attributes which, when combined, are sufficient to disambiguate among users within their agency community. For example, a combination such as name, date of birth (DOB),

entrance on duty date, and home telephone number is likely to be sufficient to differentiate between individuals that might share a common attribute (e.g., the same name). Once a multi-attribute key has been established, the database system will then enforce this property as new records are added across the database. When duplicate identifiers are compared, these key fields will be analyzed to further refine the search and identify the correct record. When selecting attributes to form a multi-attribute key, an agency should evaluate the use of attributes that are considered PII. PII is generally subject to use restrictions, which could affect the availability of a multi-attribute key that includes a PII data element.

#### **7.1.3.3. Manual Identity Attribute Correlation**

In cases where unique person identifiers or multi-attribute keys are not used, it is likely that an agency will need to apply additional processes to bind identity attributes for an individual. Correlating identity attributes can typically be accomplished in two ways: through development of a correlation algorithm that must be manually applied by an administrator through a batch (or similar) process; and/or through manual linking by an administrator using a pre-defined rule set. Within an agency or organization, each application may potentially have different naming standards for user account creation. Without a unique identifier or multi-attribute key to serve as the primary key, it may be necessary to develop unique correlation algorithms for every application in the enterprise. In addition to requiring additional development time, this process may also introduce additional risk in successfully identifying related records during correlation activities. In order to resolve these errors, administrators would then spend additional time manually verifying identities, attributes, and entitlements and reconciling each account within the application.

#### **Lesson Learned**

A federal agency with a large user base began a LACS modernization effort, initially relying on manual attribute correlation techniques to bind identity attributes to digital identities. Early in the implementation, the agency determined that the time and effort associated with resolving data collisions manually had significant impacts to the cost and schedule of the overall effort. To mitigate this, the agency implemented a unique person identifier system, which offered a more efficient approach to identity correlation.



Regardless of the approach, this type of attribute correlation is often labor and time intensive, particularly in a large, dispersed agency with many sources of identity data. In addition, use of manual attribute correlation can result in a diminished ability to detect and resolve security and audit issues that may arise in identity records and user accounts (e.g., creation of duplicate entries for the same individual as a result of status or affiliation changes). This can also affect downstream agency applications in the form of duplicate user accounts and identity records. Duplicate user accounts can drive up software licensing costs on some applications, depending on licensing terms and agreements, and the accounts may not get detected and terminated when a user leaves the agency. Despite these challenges, an agency might pursue this approach following a cost/benefit analysis as there is only a minimal need to change business processes and upgrade or procure technology. This might also serve as a transitional approach until regular technology refresh cycles allow an agency to implement a more automated solution to achieve greater levels of efficiency.

## 7.2. Digital Identity Process Integration

As discussed in Use Case 1, Create and Maintain Digital Identity Record for Internal User (Section 4.1), agencies collect identity data through a number of disparate processes that are conducted by offices and groups throughout the organization. These include new hire on-boarding, background investigation processing, credentialing, and access control administration. Typically, each of these processes is a manual, separate, and often redundant point for obtaining identity data.

The ICAM target state seeks to streamline and integrate digital identity management processes and minimize the number of collection points for identity data while reducing or eliminating the use of paper-based forms as identity data collection methods. These improvements are expected to help agencies achieve greater process efficiency and improve the security and privacy around the collection and maintenance of digital identity data. The information and guidance presented in this section is intended to assist agencies in providing answers to several common digital identity process integration questions, including:

- What steps can my agency take to streamline and integrate the backend processes that are used to collect and manage digital identity data?
- What can my agency do to streamline and integrate the HR and on-boarding processes that are used to collect identity data?
- How can my agency better integrate the background investigation process to eliminate redundant data collection?
- What steps can my agency take to streamline the processes for managing contractor identity data?

### Privacy Tip

Electronic security methods (e.g., encryption, role-based access control, etc.), when deployed as part of an agency's overall security program, can be more efficient, more reliable, and less expensive than traditional methods (e.g., locked rooms, filing cabinets, etc.) for protecting sensitive data. However, these electronic methods still require strict adherence to privacy laws, directives, and policies. An agency should, therefore, consult with its Privacy Office to ensure that appropriate privacy protections are implemented.



Once the core person attributes are established and authoritative sources are defined, agencies should analyze the backend processes that are used to obtain identity data to determine where processes can be enhanced and improved. Per OMB Circular A-123, management is responsible for establishing and maintaining internal control to achieve the objectives of effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations.<sup>96</sup> This responsibility is also held by ICAM implementers, who are accountable for improving the effectiveness, quality, and productivity of federal programs and operations. The goals of OMB Circular A-123, further discussed in Section 6.2.1, closely align with the effort to improve the processes within an agency that collect identity data, described below in Figure 74.

<sup>96</sup> [Circular A-123](#)

Process Integration Step	Description	Key Considerations
<b>Step 1: Identify</b>	Conduct internal information gathering with business process owners to identify all of the processes within the core business areas that involve collection of identity	<ul style="list-style-type: none"> <li>• Use specific criteria to define what constitutes a core business process</li> <li>• Take steps to ensure successful engagement and participation of relevant process owners</li> <li>• Take steps to ensure the availability of process and related data element information gathered</li> </ul>
<b>Step 2: Analyze</b>	Examine these processes and document the collection methods and types of identity information that is collected.	<ul style="list-style-type: none"> <li>• Identify inefficiencies</li> <li>• Determine which process steps provide value and which do not</li> <li>• Take note of process frequency</li> <li>• Inventory the data sources</li> <li>• Understand how long both the entire process and each step/section takes</li> <li>• Perform quality checks to determine accuracy and completeness of information</li> </ul>
<b>Step 3: Align</b>	Use information from the data analysis to identify and prioritize improvement opportunities for inclusion in an implementation plan.	<ul style="list-style-type: none"> <li>• Isolate redundancies in process steps, forms, and data elements</li> <li>• Identify paper-based collection methods that can be automated</li> <li>• Identify manual data entry points</li> </ul>
<b>Step 4: Improve</b>	Provide implementation plan to business process owners and provide recommendations on how to streamline, automate, and enhance identity data collection.	<ul style="list-style-type: none"> <li>• Integrate similar, redundant processes</li> <li>• Minimize duplicative information collection</li> <li>• Replace paper-based collection processes with electronic methods, as appropriate</li> <li>• Automate manual processes, as appropriate</li> </ul>
<b>Step 5: Implement</b>	Business process owners put the implementation plan into action.	<ul style="list-style-type: none"> <li>• Implement relevant metrics for digital identity processes</li> <li>• Establish training needs</li> <li>• Make updates to relevant process documentation, etc.</li> </ul>
<b>Step 6: Control</b>	Develop methods for continuously monitoring and measuring success of the process improvement effort.	<ul style="list-style-type: none"> <li>• Conduct surveys to track end-user satisfaction</li> <li>• Conduct surveys to track support staff productivity and satisfaction</li> <li>• Capture process efficiency, data quality, and cost savings</li> <li>• Establish governance and reporting requirements</li> <li>• Create a process control board</li> <li>• Review audit logs and workflow of sensitive information flows</li> </ul>

**Figure 74: Common Digital Identity Process Integration Steps**

By performing a thorough analysis of backend processes and taking steps to achieve a tighter integration across the digital identity landscape, agencies can expect to see a number of benefits, including:

- **Increased levels of process efficiency.** As more and more agency processes move toward sharing and reusing authoritative identity data, the need to manually collect and manage that data significantly decreases. This allows agencies to focus on core business functions and significantly reduces the administrative burden associated with digital identity management.

Lesson Learned	
<p>Effectively increasing the efficiency of digital identity lifecycle management is dependent on achieving tight integration between various systems and processes, which requires input and involvement from many groups within an agency, including the CIO, personnel security, HR, procurement, etc. With the establishment of its On-Boarding Initiative (OBIN) in 2010, The National Aeronautics and Space Administration (NASA) determined that most delays in the on-boarding process were caused by “hand-off” issues in which the person responsible for taking the next step was unaware that action was needed. Through the initiatives implemented as part of OBIN NASA was able to reduce the average time to on-board an employee by half.</p>	

- **Cost savings.** By tightly integrating the process used to collect and manage digital identity data, agencies can recognize cost savings through a reduction in the number of person hours spent collecting, managing, and reconciling identity data at a local level. Additionally, cost savings can be achieved through integration since fewer systems and processes are required for storing and maintaining identity data.
- **Enhanced security and privacy.** Integrating digital identity creation processes results in fewer collection points. By allowing agencies to take advantage of this technology, it directly translates to fewer opportunities for data leakage and/or theft through automated access control to identity data. Furthermore, eliminating paper-based collection methods also reduces additional security and space requirements associated with storing and securing paper files.
- **Enhanced compliance with Federal regulations and guidance.** By achieving the ICAM target state for digital identities and aligning with the ICAM segment architecture, the tight integration of the digital identity creation processes and elimination of paper-based collection methods helps agencies comply with the Government Paperwork Elimination Act (GPEA).<sup>97</sup>

### 7.2.1. Streamlining HR Processing

Within many agencies, the Human Resources (HR) department is typically the primary source of person data for federal employees. The guidance in this section is equally applicable to streamlining the processes used to collect identity data for contractors and individuals with staff-like access, although this data may be housed separately from employee data. HR is usually the first group within an agency to receive an individual’s identity information, often through the job application and employee on-boarding processes. By targeting integration and streamlining of these HR processes, an agency can see significant benefits from initial reconciliation of users to user life cycle management. There are several specific steps that agencies can take to achieve this, including:

- **Streamlining data exchange.** Agencies should seek to integrate the systems used for recruiting, including both systems owned and managed by the agency and government-wide applications, such as OPM’s USA Jobs program, with the agency’s HR systems. This integration can be used to enable pre-population of on-boarding and HR data from the data provided by the applicant as part of the recruiting process.

<sup>97</sup> [Implementation of the Government Paperwork Elimination Act](#), OMB. [GPEA]

- **Digitizing the on-boarding process.** Agencies should establish an on-boarding solution that will allow new employees to complete their HR forms online and track the progress of the on-boarding process.
- **Integrating various HR systems.** An agency's HR department may use a variety of systems to manage their business processes, such as recruiting, on-boarding, and training. Separate systems may also be operated at the bureau/component level to perform the same functions. An agency should seek to connect or consolidate these systems to eliminate redundant collection and management of data.

### Lesson Learned

An HR modernization effort can be the catalyst for process integration. The Department of State is implementing the Integrated Personnel Management System (IPMS) to replace the aging stove-piped HR applications with modern technology and Commercial-Off-The-Shelf (COTS) products. The IPMS is comprised of four integrated HR systems that together reduce transaction processing overhead, enhance enterprise-wide data sharing, improve data integrity and quality, and empower employees/supervisors to manage their personal information independently through the introduction of online workflow processes.



- **Leveraging digital signatures.** Many HR forms require a signature from the employee and other approval authorities. The process of manually collecting and verifying documents with wet signatures can be time-intensive and burdensome. The use of digital signatures enables an agency to more easily detect instances of forgery or tampering by verifying that a form was created by a known individual and was not altered during transit. Agencies should accept digital signatures for HR forms to the greatest extent possible.<sup>98</sup> Use of digital signatures leveraging the PIV card is further discussed in Section 8.4.2.
- **Establishing an employee self-service portal.** The administrative burden on HR professionals within an agency can be greatly reduced by allowing employees to proactively manage select identity information. Agencies should seek to leverage an online capability that allows employees to securely update their data, such as address, emergency contacts, and direct deposit account information. Applicable data changes from this portal would ideally be populated downstream to reliant systems.

### Lesson Learned

Enable agency employees to manage their own information, wherever possible. Within NASA's IdMAX, there is a self-service portal that allows users to modify their own profile. This includes making changes to their name or email address in the directory and requesting a PIV card renewal. This feature has increased the level of customer satisfaction within NASA as users can easily update their identity information without having to ask an HR specialist to act on their behalf. Furthermore, NASA was able to reduce the administrative costs and time associated with HR managing each information change transaction.



<sup>98</sup> As indicated in [Circular A-130, Appendix II](#), Implementation of the Government Paperwork Elimination Act, OMB, 2000.

## 7.2.2. Streamlining Background Investigation Processing

Agencies perform background investigations most commonly to determine an individual's suitability/fitness for federal employment or fitness to perform work as a contractor, as discussed in Section 4.3. While the background investigation process is not typically viewed as an act of creating a digital identity, the data collected readily contains an individual's core digital identity. By targeting integration and streamlining of personnel security and background investigation processes, agencies have the potential to dramatically improve the processes around creating and populating the digital identity. Agencies have several opportunities to accomplish this, including:

- **Leveraging data captured during the PIV enrollment process.** Capturing data once and reusing it creates process efficiencies and a limited number of data collection points enhances data privacy. For example, many biographic data elements (e.g., name, DOB) are required elements for both background investigations and obtaining a PIV credential. If data is collected for PIV enrollment first, agencies should seek to electronically share this data with the systems supporting background investigation processing to eliminate redundancy.

ROI	
By leveraging the electronic fingerprints captured during PIV card enrollment to support the fingerprinting requirement for background investigations, one large federal agency was able to reduce the time associated with completing required criminal history checks and eliminate the need for the cardholder to appear in-person for multiple fingerprinting events.	

- **Integrating background investigation processing into other processes.** Agencies should seek to minimize the steps necessary to initiate a background investigation by integrating this process with other existing business processes. For example, instead of requiring a personnel security specialist to manually track the due dates for periodic reinvestigations, an agency could build a workflow that automatically tracks reinvestigation dates and prompts the personnel security specialist to initiate reinvestigations at the appropriate time. Doing so can reduce investigation time, enhance customer service, improve security, and minimize administrative burden within the agency.
- **Leveraging authoritative sources of identity information.** Agencies often rely on redundant collection and manual re-entry of biographical information to initiate and process background investigations. To achieve the target state, an agency should seek to leverage its internal authoritative sources of identity data (e.g., HR systems) and share this information with the systems and applications that are used to track and conduct investigations (e.g., OPM's e-QIP). Doing so can significantly minimize the amount of identity data that an agency or an individual must manually re-enter during the background investigation process.
- **Eliminating paper-based investigative forms.** Agencies are required to use OPM's e-QIP application to allow applicants to electronically enter, update, and transmit their personal investigative data over a secure Internet connection.<sup>99</sup> Agencies should also

<sup>99</sup> Use of e-QIP was mandated jointly by OMB, OPM, and the Office of the Director of National Intelligence in the [E-Government Act of 2002, P.L. 107-347](#).

strive to eliminate the use of paper forms and manual processes to support investigation processing through OPM. Agencies should utilize automated electronic processing solutions, such as OPM's electronic Agency Delivery of investigative results.

ROI	
By taking advantage of OPM's electronic Agency Delivery option for investigative results, a large defense agency was able to completely eliminate the unnecessary reproduction and certified mailing of paper-based investigative records. In addition to eliminating the need to reproduce these files on paper, the agency was able to save approximately \$40,000 per month in costs related to mailing records.	

- **Honoring reciprocity for investigations performed by other agencies.** Agencies are required to exercise reciprocity for investigations and adjudications, when appropriate.<sup>100</sup> The ICAM segment architecture identifies the lack of reciprocity in accepting background investigations completed by or on behalf of another agency as a key gap in performing background investigations. An agency should utilize the capabilities provided within Central Verification System (CVS) to report and view background investigation adjudication results to reduce the costs and administrative burden associated with conducting a redundant investigation.

The President signed the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004,<sup>101</sup> which provided a formal need to create an integrated, secure database for information related to security clearance, suitability, and access decisions for military, civilian, and government contractor personnel. Under IRTPA, the Office of Personnel Management (OPM) was given the responsibility of establishing and maintaining this database, referred to as the CVS.<sup>102</sup> Under guidance issued by OMB<sup>103</sup> in 2005, OPM modified CVS to also house data related to credentialing determinations under HSPD-12, suitability or fitness for federal employment, fitness for contractor employees, and eligibility for access to classified information to facilitate reciprocity.

An agency's responsibilities with regard to use of CVS include the following:<sup>104</sup>

- Upon adjudicating an individual's investigative results, report all adjudicative decisions on background investigations to OPM.
- Supply records and HSPD-12 information to CVS in bulk via transaction files through the OPM Secure Portal, or through individual entries through the Personnel Investigations Processing System (PIPS) Agency Menu.
- Submit daily updates to their information in CVS to report any changes, such as: adding new clearances, noting revocations, denials, suspensions, and those clearances which were administratively withdrawn. In addition, agencies are required to fully refresh their CVS clearance data at least monthly.

<sup>100</sup> As required by [E.O. 13467](#).

<sup>101</sup> [Intelligence Reform and Terrorism Prevention Act of 2004](#).

<sup>102</sup> Clearances granted by the Department of Defense (DoD) are not maintained in CVS, and will be verified by checking DoD's Joint Personnel Adjudication System (JPAS).

<sup>103</sup> Office of Management and Budget, [Reciprocal Recognition of Existing Personnel Security Clearances](#), December 12, 2005.

<sup>104</sup> As described in, [Notice No. 10-04](#), Enhancements to the Central Verification System (CVS) for Reciprocity, Office of Personnel Management, Federal Investigative Services Division March 18, 2010.

- Prior to initiating a new background investigation request, consult CVS to determine if an existing investigation exists that is sufficient to meet the agency's needs.
- Take steps to ensure the accuracy and maintenance of the information provided to CVS, as OPM does not own this information and other agencies may rely on it to make credentialing decisions.
- Ensure that the appropriate data elements are entered into CVS for each applicable record (e.g., name, DOB, investigation, clearance level, status, etc.).<sup>105</sup>

### 7.2.3. Streamlining Contractor Processing

Along with managing employee identity data for credential and access management, an agency also manages this identity data for contractors. Although contractors may require similar access to federal employees, the methods and locations for collecting and maintaining their identity data are often very different. Digital identities for the contractor population can be challenging to manage due to a number of factors, including:

- Managing identity data for individual contractors has traditionally not been required to support contracting business functions, unless required based on the nature of the contract.
- Where it is collected to support access, contractor information is often obtained through a variety of disparate processes and managed separately for individual resources.
- Many agencies do not have existing authoritative source(s) for contractor identity data.
- The contractor population is fluid as individuals often change the projects, bureau/component, or agencies with which they are affiliated.

In order to overcome these challenges, an agency should take steps to establish a robust process for managing contractor identity data for those contractors who require identity credentials and access to agency resources. By doing this, agencies can achieve similar efficiencies and cost savings associated with improved employee data management. An agency should consider the following when streamlining the processes for collecting contractor identity data:

- **Enhanced on-boarding process.** Agencies should take steps to establish a well-defined and streamlined process for accepting individuals as contractors that leverages digital methods wherever possible. This process should be communicated to and followed by all relevant parties so that there is no ambiguity in the way contractors are introduced into the agency. This improved on-boarding process should replace manual, paper-based forms and processes with more efficient and secure electronic options, such as digital signature and online portals.
- **Single collection point.** Within the streamlined on-boarding process, agencies should minimize the points at which contractor data is collected. If possible, there should be one step in the on-boarding process where contractors provide their identity data. Agencies should examine the on-boarding process to determine the most logical place to collect contractor information. This might require agencies to begin collecting identity data at a point in which they were not previously collecting identity data. For example, agencies could establish the background investigation process as the single location for collecting

---

<sup>105</sup> An agency should refer to its internal Personnel Security Office and OPM for an up-to-date and complete list of Central Verification System (CVS) data elements.

contractor identity data. A single collection point will help eliminate redundancy, increase efficiency, and ease management of contractor information.

- **Gaps in contractor data.** Once agencies have established where contractor information will be collected, they should compare the data elements to the Core Person Model in Section 7.1.1 and identify discrepancies. It is beneficial for agencies to have consistent attributes across all groups within their population, so agencies should ensure that they collect similar information from contractors when creating their digital identity.
- **Authoritative source.** As discussed in Section 7.1.2, authoritative sources are a key element of successful management of digital identities. Typically, agencies do not have a single authoritative source for contractors, which can make management of their data challenging. Agencies should take steps to establish an authoritative source for contractors by either creating a separate repository or tying it into an existing system that holds employee data (e.g., IDMS).
- **Data retention.** Contractors typically begin and end many different contracts throughout their affiliation with an agency; therefore, agencies should carefully analyze their options for retaining contractor data after the contract ends. Agencies should determine a length of time for maintaining contractor data in their systems that is cost-effective and compliant with the Fair Information Privacy Principle of data minimization.
- **Account and status changes.** Because the contractor population is variable, maintaining information that is accurate and up-to-date can be challenging. Agencies should establish a specified process for making changes to contractor information that incorporates current workflows and business processes. Agencies could also consider implementing a self-service portal that allows authorized individuals to make changes to their identity information and status. This option could improve data integrity and reduce the burden on the agency's support staff.

### Lesson Learned

Allowing a user to enter his/her own information during on-boarding to create a user account can improve the quality of the data collected and improve privacy protections. For example, NASA has initiated an "invitation process" to collect digital identity data from the individual. The invitation process allows the individual to securely enter sensitive information such as Social Security Number (SSN) and date of birth (DOB), resulting in more accurate and current data while limiting unnecessary exposure of Personally Identifiable Information (PII).



- **Enhanced off-boarding process.** Agencies should take steps to establish a well-defined and streamlined process for managing contractor identity records as they end their affiliation with the agency. This process should be communicated to and followed by all relevant parties so that there is no ambiguity in the way contractors are released from the agency. The responsibility for completing this off-boarding process should be assigned to a specific person (e.g., sponsor) or office (e.g., personnel security). For example, the National Aeronautics and Space Administration (NASA) assigns a separation date to all contractors that is aligned with the end date of the assignment or contract. Off-boarding workflows notify civil servant sponsors, security, and IT services when a separation date takes place to appropriately rescind access.
- **PIV card collection.** One important ICAM-specific element that should be incorporated into the contractor off-boarding process is the collection of the contractor's PIV card. When contractors fail to turn in their PIV card, it can have a number of negative impacts

on the agency including security risks, inaccurate information on the status of their contractor population, and unnecessary costs for the management of their PIV card (an estimated \$3 per month per card for the GSA Managed Service Office).

- **Contract requirement.** To help enforce the collection of PIV cards from contractors, a requirement should be incorporated into contracts requiring that all government property, including PIV cards, be relinquished at the completion of the contract.
- **Policy.** Agencies should establish a policy that details the approach for collecting and managing contractor identity data. This policy should be communicated across the agency and included in all contracts. A contractor policy can help ensure understanding of and compliance with the procedures for handling contractors and ultimately the agency's achievement of the ICAM target state.

#### Lesson Learned

After analyzing their processes for collecting contractor identity data, the United States Department of Agriculture (USDA) determined that the best way to manage contractors' digital identity would be to establish a separate authoritative source for contractor information. This approach provides USDA with streamlined and integrated processes for collecting and maintaining contractor data and results in an up-to-date and accurate resource for contractor information.



### 7.3. Authoritative Digital Identity Attribute Exchange

As noted previously, agencies have a common need to collect and share basic identity data within their organization to support credential issuance, provisioning of user accounts, and access control administration. The ICAM Services Framework introduces an AAES capability as the means to securely share authoritative identity attributes within an agency. An AAES is a technical solution that provides agencies with the capability to connect various authoritative data sources and share identity and other attributes with the shared enterprise infrastructure. This chapter has already discussed a number of steps that should be taken to ensure that the agency is fully prepared to implement an AAES capability, including establishment of an enterprise digital identity model, identification of authoritative data sources, and streamlining of the processes used to populate those authoritative sources. The AAES capability allows agencies to link their authoritative sources of identity information with consumers of identity data across the agency, thus eliminating the need to redundantly collect identity data at each point where it is used.

#### Implementation Tip

Look for ways to provide easily accessible identity data to relying parties. Treasury's PIV Data Synchronization solution includes a Data Management Service (DMS) that is designed to correlate identity data from multiple authoritative sources (e.g., HRConnect for core identity, USAccess for credential information, etc.) and provide synchronization with relying party systems. By allowing up-to-date identity data to be readily available to relying party systems, the DMS will reduce redundant data collection and improve data accuracy throughout the agency.



This section provides guidance necessary to help agencies understand and establish an AAES capability within their organization and take full advantage of their authoritative data sources. The information and guidance presented in this section is intended to assist agencies in providing answers to several common authoritative digital identity attribute exchange questions, including:

- What are the core components of effectively sharing identity data?

- What is an AAES and what does it do?
- How would an AAES fit within my agency’s ICAM architecture and what components are necessary to support it?
- What should I consider when designing and implementing my agency’s AAES capability?
- What information and lessons learned can I leverage from existing data sharing capabilities when I begin to develop my agency’s AAES?

### 7.3.1. Elements of Attribute Exchange

When seeking to electronically share attribute data between authoritative source systems and relying parties, there are three core elements that must be addressed to support the attribute exchange:

- **Protocol.** The technical means by which identity attributes are exchanged. The attribute provider and relying party involved in the exchange must agree upon the protocol that will be used.
- **Payload.** The digital identity attributes that are exchanged between the parties; typically involves attribute contracts to define what is included and how it is formatted.
- **Policy.** The governance processes and mechanisms that are put into place to manage and operate the exchange and adjudicate any issues that may arise.

The following sub-sections discuss each of these core elements in greater detail and include guidance for agencies on aligning their attribute exchange capabilities with the ICAM segment architecture and the processes and requirements associated with the Federal Trust Framework (addressed further in Section 12.2).

#### 7.3.1.1. Protocol

Defining a common exchange protocol is the element of attribute exchange that enables the involved parties to communicate using the same language and set of rules. When establishing an attribute sharing capability, an agency should select a protocol that meets the technical and operational needs of both the Identity Provider and Relying Party. Selecting an appropriate protocol is also dependent on the type of connection that is desired between the parties, as different types of connections may not be equally supported by all approved protocols. Figure 8 contains a sampling of several common protocols used for exchanging identity data.

Protocol	Description
<b>LDAP/s</b>	Lightweight Directory Access Protocol is used to read and/or edit directories. Traffic to and from the directory should be encrypted (i.e., TLS, SSL, Internet Protocol Security [IPSec]). Access control should be in place to ensure data is provided to only those authorized to view it.
<b>DSML</b>	Directory Service Markup Language provides directory service information in an XML syntax. Data traverses across HTTP/s.
<b>SAML</b>	Security Assertion Markup Language is used to exchange authentication and authorization data in XML.
<b>SPML</b>	Service Provisioning Markup Language is an open standard that uses an XML-based framework for the integration and interoperation of service provisioning requests.

Figure 75: Common Protocols for Sharing Identity Data

### 7.3.1.2. Payload

A critical component of any identity attribute exchange capability involves defining what attributes are to be exchanged between the parties and how those attributes are to be formatted. Defining attribute syntax (e.g., format) helps ensure that identity attributes are received in such a manner that they are usable within a relying party application. This is most often accomplished through the establishment of an attribute contract. When streamlining the exchange and management of identity data within an agency, it is expected that the payload will align with the government-wide Core Person Model, discussed in Section 7.1.1. However, an agency may opt to include additional attributes based on its specific mission and business needs.

#### Terminology

**Attribute Contract** – A document that extensively describes the agreement on the set of, and syntax of, attributes that members of a federation have to abide by on the “payload.”



### 7.3.1.3. Policy

Establishing governance is important to maintaining the ongoing operation of identity attribute sharing arrangements and providing a framework to help ensure that both the Identity Provider and Relying Party(s) operate within the confines of the arrangement. An agency implementing an internally-focused attribute sharing capability should establish agency policies governing the appropriate use of identity data that is made available through the solution. This can often alleviate the need for point-to-point agreements between groups within the organization. When seeking to establish an identity attribute exchange capability external to the agency, additional governance considerations apply, as discussed in Section 12.4.3.

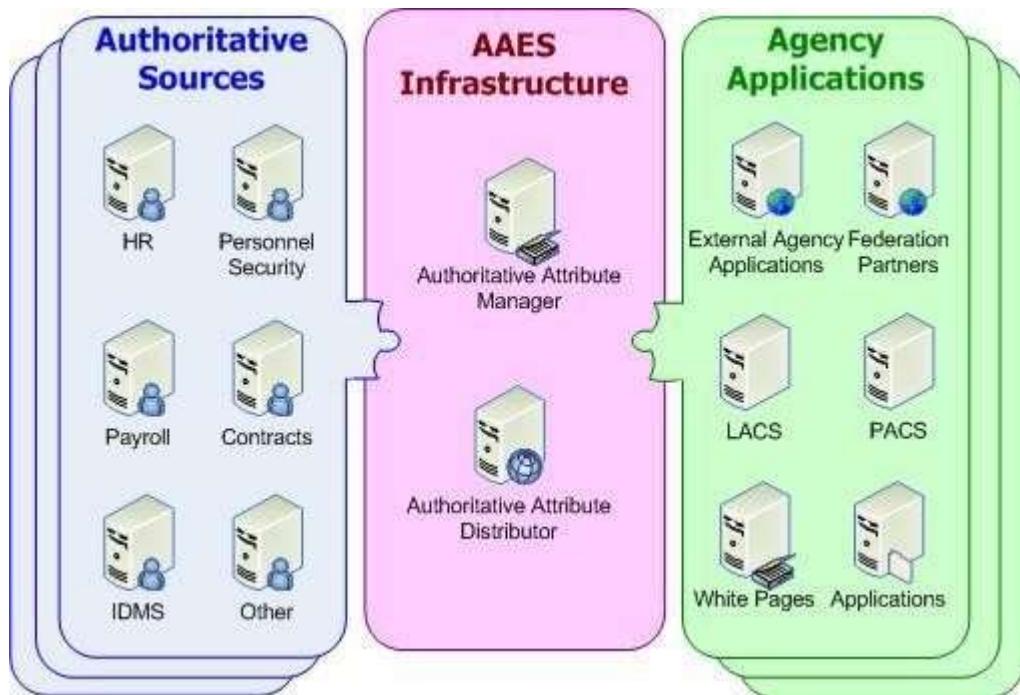
#### Privacy Tip

Implementing an attribute sharing capability provides an agency with a number of benefits and process efficiencies; however, one goal of this effort is to avoid collecting and/or sharing more PII than is necessary for the intended use. Therefore, only those attributes that are minimally necessary should be shared with a relying party. To achieve this, agencies should consider establishing attribute agreements or attribute practice statements to address which attributes will be shared and the manner in which they will be conveyed, to ensure privacy and security.



## 7.3.2. AAES Architecture

Designing an AAES solution architecture requires agencies to consider the capabilities presented in the ICAM target state, existing ICAM investments (e.g., logical access solutions), and the agency’s overall IT infrastructure. The objective of this effort is to determine how an AAES capability will integrate with the agency’s IT infrastructure and provide digital identity attribute sharing services, as defined in the ICAM Services Framework (Section 3.2.4). This section provides a high-level AAES solution architecture diagram illustrating the services and capabilities introduced in the ICAM segment architecture.



**Figure 76: AAES Reference Architecture**

The diagram above is intended to serve as a high-level depiction of the ICAM target state for an AAES capability, which supports achievement of Transition Activity 5.4 as discussed in Section 5.2.2.1. Figure 76 is representative of the solution variations/designs that an agency may choose to implement. The solution components within the AAES Infrastructure are represented generically and could be implemented using a variety of Commercial Off-The-Shelf (COTS) or purpose-built products. Agencies should evaluate their existing ICAM and infrastructure investments and select the approach that best meets their needs.

As depicted in Figure 76, an AAES provides a consolidated mechanism for securely and electronically exchanging digital identity attributes between authoritative data sources and the agency applications that consume those attributes. In many cases, this data is spread across multiple authoritative sources within an agency, thereby complicating the challenge of exchanging attributes between sources and consumers. The Authoritative Attribute Manager provides the capability to present a single, authoritative view of that data by reconciling and aggregating attributes from the various sources.<sup>106</sup> The Authoritative Attribute Distributor is the component that integrates with attribute consumers and conducts the data exchange. The following sub-sections discuss the two AAES Infrastructure components in greater detail.

### 7.3.3. AAES Solution Components

This section describes the functionality and approaches for implementing the AAES Infrastructure components, the Authoritative Attribute Manager and the Authoritative Attribute Distributor. In some cases it may be possible to achieve the functionality described for both the Authoritative Attribute Manager and Authoritative Attribute Distributor by implementing a

<sup>106</sup> See Section 7.1 for a detailed discussion of the steps that are necessary to define a core set of identity attributes and identify and leverage the authoritative sources for those attributes within an agency.

single product or tool. Conversely, it is also possible that multiple products and/or purpose-built applications could be integrated to create a single AAES solution. Each agency should evaluate their existing and planned ICAM investments as well as the agency’s infrastructure and select an implementation approach that best meets the business needs and mission requirements of the agency.

#### **7.3.3.1. Authoritative Attribute Manager**

The Authoritative Attribute Manager is designed to correlate identity attributes from the various authoritative data sources within an agency and provide a single authoritative source of digital identity. The Manager functions as a central hub of attributes by aggregating data from the various sources through either resource connectors or web services. When aggregating data from the authoritative data sources to form an enterprise digital identity, the Manager de-conflicts discrepancies that exist in the same attribute between multiple sources. As previously discussed, an agency should seek to define a single authoritative data source for each identity attribute in the Core Person Model; however, that may not always be possible. For example, it may be necessary to combine data from different HR systems (e.g., from two agency bureaus) for a single individual. Additional data normalization may be necessary to ensure that the various identity attributes are formatted in a way that is consumable by the applications and users that receive authoritative identity data through the AAES. The Authoritative Attribute Manager is also capable of extending the schema for an identity, should additional attributes be required that are not included in the agency’s implementation of the Core Person Model; this may be the case with entitlement attributes used to support user authorization decisions.

By aggregating and correlating identity data in the Manager, attributes can be found in one central location, which improves consistency of attribute data because there is a single source that is treated as authoritative. Additionally, the Manager provides an agency with the opportunity to support a number of enhanced capabilities, including support for multiple access control models at the application level that operate based on a variety of digital identity data elements.<sup>107</sup> This capability enables agencies to make more secure, accurate, and reliable access control decisions and enforce access controls at a much more granular level.

#### **Lesson Learned**

Treasury’s PIV Data Synchronization solution includes a Data Management Service (DMS) that correlates identity data from multiple authoritative sources (e.g., HRConnect for core identity data and USAcces for credential information) and provides synchronization with relying systems. By making up-to-date identity data easily available to relying party systems, the DMS reduces redundant data collection and improves data accuracy throughout the enterprise.



The Authoritative Attribute Manager can be implemented in several ways, based on an agency’s existing investments and infrastructure requirements, including:

- **Virtual directory.** A virtual directory service aggregates and normalizes identity attributes dynamically, without the need to store them in a physical repository and regularly synchronize them with the authoritative data sources. When requested, the virtual directory queries the authoritative data sources and provides the normalized

<sup>107</sup> See Section 9.3.1 for an in-depth discussion of access control models.

attributes to the attribute consumer. In some cases it may also be possible for a virtual directory product to serve as both the Authoritative Attribute Manager and Distributor.

- **Metadirectory.** A metadirectory is similar to a virtual directory in that it aggregates and normalizes identity attributes from multiple authoritative sources; however, this approach involves physically storing the results of the data aggregation and synchronizing with the authoritative data stores at regular intervals.
- **Identity Manager.** The Identity Manager component of a modernized logical access control system (LACS), discussed in Section 11.2.2.1, is capable of providing the identity attribute aggregation and normalization capabilities of the Authoritative Attribute Manager. Agencies choosing to implement an Identity Manager as part of their LACS modernization effort should consider this a preferred approach in order to avoid redundant investment in this capability.

#### Privacy Tip

When determining an appropriate approach to implementing an Authoritative Attribute Manager, an agency should work with its Privacy Office to determine whether there is an existing Systems of Record Notice (SORN) in place or whether a new SORN needs to be developed, and whether a Privacy Impact Assessment (PIA) is required. If a new or updated PIA and/or SORN are necessary, then they must be in place before the approach can be developed and implemented.



Each agency should perform an analysis to determine which of the alternatives for implementing an Authoritative Attribute Manager described above best meets the agency's business needs and mission while balancing the need to leverage existing investments, wherever possible. There are a number of benefits and limitations associated with each of the approaches that agencies should consider as part of this analysis, which are outlined in Figure 77.

Approach	Benefits	Limitations
<b>Virtual Directory</b>	<ul style="list-style-type: none"> <li>• Attributes are queried in real-time and results are dynamically provided to relying parties</li> <li>• No requirement to physically store identity data eliminates privacy concerns associated with systems of record</li> <li>• Ability to develop custom views for each relying party ensures that identity data is not shared inappropriately</li> <li>• Ability to easily support a large number of authoritative data sources</li> <li>• Data provided to consumer applications is always up-to-date with authoritative sources</li> </ul>	<ul style="list-style-type: none"> <li>• Dynamic querying places an additional performance load on authoritative source systems but can be addressed through data caching</li> <li>• Some authoritative data sources for identity data may not be built to support dynamic querying</li> <li>• Pushing authoritative identity data to consumer applications requires an additional tool (Authoritative Attribute Distributor)</li> <li>• AAES and consumer systems may be unable to pull data when the authoritative source is unavailable but can be addressed through data caching</li> </ul>
<b>Metadirectory</b>	<ul style="list-style-type: none"> <li>• Minimal impact to performance of authoritative data sources</li> <li>• Queries by relying parties can be responded to faster due to local storage of data</li> <li>• Minimally invasive to source systems that may have more complicated or proprietary data stores</li> </ul>	<ul style="list-style-type: none"> <li>• Data is physically stored locally, which is redundant with authoritative data sources and creates a new system of record</li> <li>• Local data storage requires that appropriate security and privacy controls are in place</li> <li>• Metadirectory may not be up-to-date with authoritative sources given synchronization schedule</li> <li>• Pushing authoritative identity data to</li> </ul>

Approach	Benefits	Limitations
		additional tool (Authoritative Attribute Distributor)
<b>Identity Manager</b>	<ul style="list-style-type: none"> <li>• Opportunity to leverage an existing LACS investment</li> <li>• Natively provides an ability to push identity data to consumers without the need for an additional (Authoritative Attribute Distributor) component</li> <li>• Streamlined integration with access control components</li> <li>• Provides a number of enhanced capabilities, including provisioning, workflows to augment/enhance attributes, and user self-service</li> </ul>	<ul style="list-style-type: none"> <li>• Requires that agencies procure an Identity Manager (if one is not already owned)</li> <li>• Some Identity Manager products may require that attributes be stored in a physical directory after aggregation</li> </ul>

**Figure 77: Alternative Approaches for Implementing an Authoritative Attribute Manager**

Regardless of the implementation approach selected, an agency must appropriately protect the Authoritative Attribute Manager due to the types and amount of data that it contains. In order to do so, an agency should ensure that agreements are in place to govern the exchange of identity attributes between these source systems and the Authoritative Attribute Manager. The Authoritative Attribute Manager itself is not directly accessed by systems or humans that request attributes, rather it partners with the Authoritative Attribute Distributor, discussed in Section 7.3.3.2, which serves as the interface point for requesting applications. This provides an additional layer of security that prevents requesting parties from directly accessing the attributes, which could potentially lead to unauthorized disclosure.

### **7.3.3.2. Authoritative Attribute Distributor**

The Authoritative Attribute Distributor is designed to integrate with the Authoritative Attribute Manager to provide attributes, by request, to consumer applications (i.e., applications that use identity data for downstream processes), both internal and external to the agency. The Distributor can also be used to synchronize user data with user accounts or local directories, based on the agency's requirements. The Authoritative Attribute Distributor serves as the primary communication point for consumer applications in that it both receives and responds to requests for attributes by pulling the appropriate attributes from the Authoritative Attribute Manager. This capability provides applications with streamlined access to the requested attributes while shielding the Authoritative Attribute Manager (and its connected authoritative sources) from direct access from users and consumer applications, which would increase the complexity of protecting the security and privacy of the data.

As discussed in Section 7.3.3.1 above, the Authoritative Attribute Distributor component can be the same product as the Authoritative Attribute Manager. This is most commonly achieved through implementation of an Identity Manager product. The Identity Manager acts as both a Manager and Distributor by consolidating identity attributes, protecting those attributes at rest, and exposing a secure interface to push and/or pull those attributes to consumers through resource adapters and web services. The Authoritative Attribute Distributor can also be a separate product from the Manager. In this case, a physical or virtual directory can be the

Authoritative Attribute Manager, and a service layer may be built to serve as the Distributor and share identity attributes with consumers.

In order to ensure the security and integrity of the AAES, both users and consumer applications must interface with the service through a proxy or secure protocol following successful authentication. The Authoritative Attribute Distributor should be capable of exposing a wide range of secure communications protocols in order to meet the needs of the agency's consumer applications. These protocols are discussed further in Section 7.3.1. The integration of each consumer application with the Distributor should be governed by an agreement that defines the specific attributes that will be provided and specifies data usage, distribution, and synchronization requirements. Although individual consumer applications may have access to different data, it is important for the AAES to have a common access management component to provide a consistent level of protection.

#### 7.3.4. AAES Common Design Characteristics

In order to successfully build and deploy an AAES capability, as defined in the target state ICAM segment architecture, it is necessary to understand the common characteristics that the solution should include in order to meet the objectives of the ICAM target state. These common characteristics are identified in Figure 78; however, it is also important for agencies to consider their specific needs when designing an AAES.

AAES Characteristic ID	AAES Solution Characteristics
<b>AAES 1</b>	Provides aggregation of identity attributes.
<b>AAES 2</b>	Supports deployment of connectors and service interfaces to retrieve identity attributes for distributed sources.
<b>AAES 3</b>	Utilizes a unique person identifier to distinguish between identities.
<b>AAES 4</b>	Provides transformation of identity attributes from authoritative source data storage format to a standardized format to present data externally.
<b>AAES 5</b>	Provides correlation of identity attributes from distributed sources of identity information.
<b>AAES 6</b>	Provides the capability to reconcile differences between different sources of identity attributes.
<b>AAES 7</b>	Provides an interface to request identity attributes over common protocols such as LDAP/s, DSML, SAML, and SPML.
<b>AAES 8</b>	Provides security to protect data against unauthorized access and logging to facilitate audits.
<b>AAES 9</b>	Provides various views of identity attributes and display them only to users or systems that are authorized to view those attributes.
<b>AAES 10</b>	Provides the ability to request identity data based on a variety of methods (name, globally unique identifier, email, DOB).
<b>AAES 11</b>	Provides reports of identity attributes.
<b>AAES 12</b>	Provides the capability to push or pull identity attributes including the ability to distribute new identities and updates to existing identity attributes.
<b>AAES 13</b>	Provides the capability to protect data at rest.
<b>AAES 14</b>	Provides the capability to sign attribute assertions.

Figure 78: Common AAES Design Characteristics

### 7.3.5. AAES Implementation Considerations

Deploying an AAES capability requires considerable planning, support, and coordination from various groups within an agency. Specific planning and coordination considerations include the following:

- **Data quality.** The Authoritative Attribute Manager is used to consolidate identity data. However, the source identity data must be stored in a consistent and defined format prior to implementing the Manager. Furthermore, the data must be complete and up-to-date.<sup>108</sup> The data quality of the source systems is a pre-requisite to an AAES solution. If the quality of the data is poor coming into the AAES, then the data shared from the AAES will also be poor quality (e.g., name spelled incorrectly in the authoritative data source).
- **Defining identities.** The Authoritative Attribute Manager uses built-in queries to aggregate identity attributes from different sources. In some cases, there may be multiple sources for digital identity data. When this occurs, the Attribute Manager should be capable of determining which source is authoritative and be used to define the enterprise digital identity. For example, if there are two different sources the following scenarios could be present:
  - Identity exists in both sources and consists of mutually exclusive attributes;
  - Identity exists in both sources and consists of overlapping attributes; or
  - Identity exists in one source but not the other.
- **Flexible authoritative attribute source selection.** Most agencies do not have a central location to create, update, and store all attributes utilized throughout the enterprise. Therefore, in a case that there may be conflicting values from different sources for the same attribute, it is important to develop a process for identifying and selecting the most accurate value. These processes may range from identifying which record was most recently updated to comparing multiple sources and selecting the value which appears most often.
- **Correlation of identity attributes.** Given the number of potential sources for identity attributes, an agency should determine a mechanism for correlating those attributes into a single digital identity within the Attribute Manager. That is, each individual needs to be uniquely identified and attributes of the same identity from different sources should be correlated to the same enterprise digital identity. As discussed in Section 7.1.3, attributes can be correlated using a unique person identifier or a combination of attributes (i.e., a multi-attribute key). If a reliable correlation key does not exist, a mechanism must be developed for accurately correlating identity information, perhaps involving human review of potentially conflicting records.
- **Normalization.** Normalization creates a common and consistent taxonomy for attributes. It provides a mapping between different attribute types and values. For example, one bureau/component’s organization attribute can be equivalent to another’s division attribute. Establishing a process for normalizing these attributes (e.g., data modeling) across an agency is critical to enabling effective attribute sharing.
- **Reconciliation of identity attributes.** During the course of correlating attributes to an identity, there may be scenarios where different authoritative sources have a discrepancy

---

<sup>108</sup> Guidance related to data cleansing and formatting is provided in Section 7.1.2.2 with regards to implementing the Core Person Model.

regarding the same attribute of an identity, or where an attribute is missing completely. An agency may experience difficulty determining which attributes are correct if there are discrepancies with a single identity. In this case, a process must be put in place to correct the discrepancy and store the correct attribute in the Authoritative Attribute Manager. This will often require use of an offline process involving human review of the attributes. It must be determined how to fix the problem upstream. This can be achieved by either creating a data scanning utility to check for error conditions prior to populating the Authoritative Attribute Manager, or by building a process to notify the appropriate personnel to correct the source data manually.

- **Sensitivity of data.**<sup>109</sup> Aside from mission critical data, identity and privilege data can be some of the most sensitive data used within an agency. Due to the sensitivity of the data, it is extremely important to ensure that proper access controls are in place. The various technologies used to implement an AAES can provide enhanced security and privacy for an individual's PII. For example, specific views can be created based on a user's role to limit access to sensitive data elements, such as Social Security Number (SSN). This can be a good method to satisfy various users with different reporting requirements while protecting sensitive data from those who lack a need to know it. Views can be dynamically created based on the authorization information or the views can be stored and invoked on a regular basis.

#### Privacy Tip

Electronic mechanisms such as role-based access control enforcement and data encryption provide an enhanced means for protecting sensitive data. However, all of the privacy concerns and requirements cannot be addressed through technology. An agency should leverage its Privacy Office to ensure that questions about the need, use, and retention of sensitive data (e.g., date of birth [DOB], Social Security Number [SSN], etc.) are accurately answered and that appropriate privacy protections are in place.



- **Securing the AAES.** Access controls alone are not sufficient protection. An in depth defensive approach should be taken by implementing other security mechanisms to protect the AAES from being compromised. This includes ensuring that traffic travels through firewalls to filter application and network layer attacks. Data should be protected while at rest and while in transit by using encryption. Furthermore, AAES implementations should include a comprehensive logging mechanism that provides for periodic security audits; this feature can be used to revise access controls as needed to comply with agency privacy policies. Monitoring mechanisms should also be in place to ensure the integrity of the AAES solution has not been compromised.
- **Access to the AAES.** As discussed in Section 7.3.3.2, the requesting party should never have direct access to the attributes contained within the Authoritative Attribute Manager component of the AAES. It is expected that the majority of attribute consumers will be other agency IT applications that will obtain attributes from the Authoritative Attribute Distributor based on a defined attribute agreement or Memorandum of Understanding.<sup>110</sup>

<sup>109</sup> The examples provided in this bullet are not intended to be comprehensive. An agency should conduct a risk assessment in accordance with [SP 800-37](#) and refer to related FISMA guidance provided by NIST for a complete inventory of access controls related to ensuring data security.

<sup>110</sup> More information on the use of authoritative attributes in physical and logical access systems can be found in Chapters 10 and 11, respectively.

This is recommended because it makes it more difficult for an attacker to compromise the Attribute Manager because the attacker does not know the true address of the Attribute Manager and only has access to an intermediary device. Additional security measures (e.g., XML security gateways) can serve as an extra layer of protection for the AAES.

- **Access control groups.** For the purpose of streamlining the process of interfacing with the AAES, attributes can be grouped based on sensitivity (e.g., public, confidential, confidential PII) or business level roles (e.g., HR, benefits administration, access control administration, etc.). Applications and requesting parties may then be able to request a group of attributes based on the underlying need and usage criteria.
- **Integration into system development life cycle (SDLC).**<sup>111</sup> As more systems interface with the AAES and use it to obtain identity attributes, an agency should consider integrating a step into its SDLC to ensure that new applications consider how to integrate with and use the AAES. This may involve providing a standardized method for requesting applications to provide justification, get approved, and sign a governance agreement for receiving the data. This may also involve establishing a process for quickly creating new access control groups and/or attribute views as they are requested.
- **Push versus pull.** Consumer applications have a wide variety of requirements for how identity data is obtained. Both pushing and pulling of data should be accounted for during implementation in order to accommodate the varying capabilities of legacy systems that will consume the attributes. Pulling data refers to consumers making requests for data using the Authoritative Attribute Distributor's service layer. Pushing data refers to the Distributor synchronizing user data back to authoritative sources as well as downstream applications.
- **Use of attribute service for more than identity.** The scope of this section has been focused on identity attributes. However, a similar architecture (or the same AAES) can be implemented or expanded upon to include entitlement attributes.<sup>112</sup>
- **Governance of attribute sharing.** Agencies should consider establishing guidelines to protect against unauthorized disclosure of identity information, which may include establishing an attribute agreement or Memorandum of Understanding/agreement to define which attributes will be made available to specific attribute consumers via the AAES infrastructure. Taking this step ensures that attribute consumers are provided with the information necessary to effectively make authorization decisions while limiting the exposure of unnecessary information. These agreements and memorandums can be updated over time, as business needs change, to accommodate additional attributes that may be required.

### 7.3.6. Leveraging Existing Identity Attribute Exchange Capabilities

For some time now Federal, state and local governments have recognized the value that stems from the ability to securely and reliably share information. Through a number of interagency partnerships, several pilot programs have been developed to address the need to share information electronically in order to better support specific mission critical business functions. While each of these programs was designed to address the needs of a specific mission or

---

<sup>111</sup> More information can be found in [SP 800-37](#), [SP 800-53](#), and [SP 800-64](#), Security Considerations in the System Development Life Cycle, Revision 2, NIST, October 2008.

<sup>112</sup> Entitlement attributes are discussed in-depth in Section 9.2.1.

business area, an agency can leverage the work done in support of these efforts in order to develop its AAES capability. The key exchange capabilities available for agency consideration include:

- **Backend Attribute Exchange (BAE).** A standards based architecture and interface specification to securely obtain attributes of subjects (e.g., PIV card holders, federation members), from authoritative sources, to make access control decisions and/or to do provisioning. The BAE is designed to support any community-defined attribute contract; as such, an agency could use this approach to exchange a wide variety of identity attributes in support of improved identity life cycle management. A BAE could provide attribute management and distribution capabilities as discussed in Section 7.3.3.1 and 7.3.3.2 respectively, using an XML gateway managed web service for authentication and access to a virtual directory.
- **National Information Exchange Model (NIEM).** A model to provide enhanced sharing of data with state, local, and tribal governments for daily business as well as emergency or disaster situations. NIEM provides a common vocabulary set to enable data sharing between multiple authorities and allows for seamless, repeatable communications without the need to enforce stringent technology requirements.
- **Global Federated Identity and Privilege Management (GFIPM).** An access model to enable streamlined federated access to law enforcement applications by provisioning local user accounts through trusted attribute sharing. Participating agencies interact on a peer-to-peer level, disclosing only their local security policies and having the ability to decide with whom they wish to interact based on their community of interest. This flexible structure allows GFIPM to adapt as the community's needs change.

The capabilities described above can be leveraged by an agency for its own identity data sharing needs because they provide a foundation for implementing the basic elements of attribute exchange (i.e., protocol, payload, and policy), as discussed earlier in Section 7.3.1. The following figure summarizes the capabilities with regard to these elements.

Capability	Protocol	Payload	Policy
<b>BAE</b>	<ul style="list-style-type: none"> <li>• Supports both direct exchange and brokered exchange models using the ICAM Security Assertion Markup Language (SAML) 2.0 profile of BAE</li> <li>• Supports a batch and occasionally connected model using the ICAM SPML profile of BAE</li> <li>• Attribute exchange functionality is agnostic to the authentication mechanism used</li> <li>• Supports both Web Applications and Web Services</li> <li>• Interactions occur in the</li> </ul>	<ul style="list-style-type: none"> <li>• Indifferent to the payload being exchanged</li> <li>• Allows organizations and communities of interest to define their attribute contracts or leverage existing contracts (e.g., Global Federated Identity and Privilege Management [GFIPM] Attribute Contract)</li> </ul>	<ul style="list-style-type: none"> <li>• Includes specific governance and operational rules that will be managed by the Federation Operator<sup>113</sup></li> </ul>

<sup>113</sup> Currently being defined as part of the BAE v2 specifications.

Capability	Protocol	Payload	Policy
	"back-channel"		
<b>NIEM</b>	<ul style="list-style-type: none"> <li>Cross-organizational use requires agreement on exchange protocol between the Identity Provider and Relying Party</li> </ul>	<ul style="list-style-type: none"> <li>Large potential data set organized and managed within clearly defined domains</li> <li>Well-defined core data set available for reuse within mission or business-specific domains</li> </ul>	<ul style="list-style-type: none"> <li>No common governance framework defined</li> </ul>
<b>GFIPM</b>	<ul style="list-style-type: none"> <li>Utilizes its own SAML 2.0 Web SSO profile (different from the adopted ICAM profile)</li> <li>Uses SAML Identity Provider Functionality and Authentication Assertion Functionality for cross-domain authentication</li> <li>Uses SAML Attribute Assertion functionality to pass the attributes of the authenticated user</li> <li>Interactions occur in the "front-channel"</li> </ul>	<ul style="list-style-type: none"> <li>Leverages the attribute set established by NIEM</li> <li>Requires use of the GFIPM Attribute Contract / Metadata to be part of the federation</li> </ul>	<ul style="list-style-type: none"> <li>Independent governance model<sup>114</sup> that is not currently adopted through the ICAM Trust Framework Provider model</li> </ul>

**Figure 79: Comparison of Existing Identity Attribute Exchange Capabilities**

Each attribute exchange capability has been presented individually in order to allow for a comparison of their respective approach to the protocol, payload, and policy elements. However, in implementation, it is expected that an agency might combine the various aspects from two or more of the attribute exchange capabilities to fulfill its attribute exchange requirements. For example, an agency might choose a combination of front-channel web SSO attribute assertions (e.g., GFIPM payload) with a back-channel attribute provider (e.g., BAE exchange). An agency should carefully consider its mission objectives when deciding the appropriate aspects to leverage in the implementation of its attribute exchange capability.

<sup>114</sup> <http://www.gfipm.net/guidelines.html>

This page is intentionally left blank.

## 8. Initiative 6: Fully Leverage PIV and PIV-I Credentials

Initiative 6, as introduced in Section 5.2.2, is an agency-level ICAM implementation initiative that includes activities required to use PIV and PIV-Interoperable (PIV-I) credentials for both the required access control uses and other value-added applications. As a result of the Homeland Security Presidential Directive 12 (HSPD-12) mandate, agencies have issued PIV cards to their employees and contractors and are working toward enabling their use to access physical and logical resources. Through this effort, agencies have identified numerous challenges in the lifecycle management of the credentials as well as technical and procedural requirements related to the operations of an HSPD-12 program. In addition, PIV and PIV-I cards have capabilities beyond access control that agencies can leverage to achieve additional value out of the significant investment they have made in their PIV infrastructure. The guidance in this chapter provides examples how an agency can successfully tackle the operational aspects of credential usage through instances where agencies have identified improvements that can be shared at the implementation level as well as some of the ways in which an agency can fully leverage PIV and PIV-I credentials to get additional return on their investment.

This chapter has been organized into the following five main sections:

- **Credential Overview.** This section discusses the PIV card and the elements of the data model that are available for agency use. It also introduces PIV-I and discusses the activities required to accept it. Finally, it provides an overview of the PIV infrastructure and the components that support agency use of PIV and PIV-I credentials.
- **Authentication.** This section discusses the different ways an agency can use the features of the PIV and PIV-I credentials to authenticate to systems and applications and the common requirements for path and certificate validation.
- **Card Usage Challenges.** This section discusses the aspects of PIV card management and usage related to the HSPD-12 program.
- **Interagency Federation.** This section discusses use of the PIV card for access across agency boundaries, provides an overview of common interagency federation scenarios, and includes considerations for enabling federation between two or more agencies.
- **Value-added Applications.** This section discusses how an agency can leverage PIV and PIV-I cards for use beyond physical and logical access, including encryption and digital signature, to see additional return on the investment in the credential.

### 8.1. Credential Overview

In order for agencies to achieve Initiative 6: Fully Leverage PIV and PIV-I Credentials (introduced in Section 5.2.2), ICAM implementers must understand these credentials and the features, characteristics, and supporting infrastructure that enable their use. The features of PIV and PIV-I cards and supporting infrastructure allow agencies to meet the ICAM goals of improved security, privacy, and interoperability when controlling access to physical and logical resources. They also provide opportunities for usage beyond access control applications.

### Implementation Tip

Work closely with your agency's credential vendors and manufacturers to stay abreast of changes in PIV and PIV-I card technology and ensure that current printing procedures and methods, digital components (e.g., certificates), and security features are being leveraged. As the use of these credentials increases, so will the technological developments that are available to the Federal Government. Visit idmanagement.gov regularly for additional helpful links and references related to PIV and PIV-I.



The information and guidance presented in this section is intended to assist an agency in providing answers to several common PIV and PIV-I credential questions, including:

- What are the features of the PIV and PIV-I cards and what functions do they provide?
- What are the differences between PIV and PIV-I cards?
- What are the components that comprise the PIV infrastructure and how can they be leveraged to provide efficiencies and cost savings for an agency?

#### 8.1.1. PIV Card

The goals of PIV implementation include increased efficiency, improved security and privacy protection, and interoperability. Many of the design features and data elements on the PIV card enable enhanced security and privacy when used to verify a claimed identity. Furthermore, the PIV card supports interoperability through the deployment of a common identification credential with a standard set of minimum requirements. The features of the PIV card can be broken out into two main categories: physical card features, including security features and visual card topography, and the data objects stored electronically on the embedded integrated-circuit chip (ICC).

While PIV card applications leverage the logical credentials stored on the card, the PIV card also serves as a visual identification card in some limited target state usage scenarios. Standardization in the physical card elements enhances visual card authentication. Figure 80 describes the common mandatory physical elements on the PIV card, as outlined in FIPS 201.<sup>115</sup>

Element Type	Description	Standard Element
<b>Security Features</b>	The PIV Card shall contain, at a minimum, one security feature that aids in reducing counterfeiting, is resistant to tampering, and provides visual evidence of tampering attempts. Examples of such security features are given in the 'Standard Element' box.	<ul style="list-style-type: none"><li>• Optical varying structures</li><li>• Optical varying inks</li><li>• Laser etching and engraving</li><li>• Holograms</li><li>• Holographic images</li><li>• Watermarks</li></ul>

<sup>115</sup> [FIPS Publication 201](#), Personal Identity Verification (PIV) of Federal Employees and Contractors, National Institute of Standards and Technology, March 2006. [FIPS 201]

Element Type	Description	Standard Element
<b>Visual Card Topography</b> <sup>116</sup>	The visual card topography for the PIV card specifies the information that is mandatory and optional and defines a common design for the placement of printed components.	<b>Front of Card</b> <ul style="list-style-type: none"> <li>• Photograph</li> <li>• Name</li> <li>• Employee Affiliation</li> <li>• Organizational Affiliation</li> <li>• Expiration Date</li> </ul> <b>Back of Card</b> <ul style="list-style-type: none"> <li>• Agency Card Serial Number</li> <li>• Issuer Identification</li> </ul>

**Figure 80: PIV Card Standard Physical Elements**

Most applications for the PIV card leverage the logical data elements on the card to perform electronic verification of a claimed identity. These data elements are defined as part of the PIV card data model, outlined in NIST SP 800-73.<sup>117</sup> The PIV card data objects provide graduated levels of identity assurance and allow an agency the opportunity to select appropriate levels of security for applications being accessed with the PIV card. The following elements comprise the mandatory objects of the PIV card data model:<sup>118</sup>

- **Card Capability Container.** An object that holds data sets and supports minimum capacity for retrieval of the Data Model. The Card Capability Container allows each PIV card to carry the information needed for software to communicate with the card.
- **Cardholder Unique Identifier (CHUID).** A data element used by the card to prove the identity of the cardholder to an external entity. The CHUID includes a 16 byte Global Unique Identifier (GUID), a 25-byte Federal Agency Smart Credential Number (FASC-N), which uniquely identifies each card, expiration date, and issuer digital signature.
- **Certificate for PIV Authentication.** A certificate used with its associated private key to authenticate the card and the cardholder.
- **Cardholder fingerprints.** Primary and secondary fingerprint templates stored on the card for performing authentication.
- **Security Object.** Signed data object that enforces the integrity of unsigned information (and optionally all PIV data objects, excluding digital certificates).

In addition to the mandatory data objects, the PIV card data model includes 28 optional data objects for interoperable use. Of particular note are the optional certificates that further support authentication and expanded uses, including encryption and digital signing. Digital certificates are a primary tool for performing electronic verification for logical access applications (discussed further in Chapter 11) and for modernization of physical access applications (discussed further in Chapter 10). Figure 81 provides additional detail regarding the certificates available for the PIV card.

<sup>116</sup>The mandatory visual elements are also represented in digital form on the ICC of the card.

<sup>117</sup>[SP 800-73-3](#), Interfaces for Personal Identity Verification – Part 1: End-Point PIV Card Application Namespace, Data Model and Representation, National Institute of Standards and Technology, February 2010. [SP 800-73]

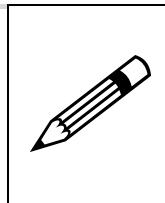
<sup>118</sup>It is anticipated that additional data elements will be made mandatory for the PIV card in future revisions to [FIPS 201](#).

Digital Certificate	Mandatory/Optional	Description	Practical Use(s)
Certificate for PIV Authentication	Mandatory	A certificate used with its associated asymmetric (private) key to authenticate the card and the cardholder.	<ul style="list-style-type: none"> <li>Authentication (with PIN)</li> <li>Verification of status of the subject's background investigation at the time of card issuance<sup>119</sup></li> </ul>
Certificate for Card Authentication	Optional	A certificate used either with an asymmetric (private) or symmetric (secret) Card Authentication Key (CAK) to support physical access.	<ul style="list-style-type: none"> <li>Physical access</li> <li>Authentication</li> </ul>
Certificate for Digital Signature	Optional	A certificate used with its associated asymmetric (private) key for Digital Signature and its associated private key support the use of digital signatures for the purpose of document signing.	<ul style="list-style-type: none"> <li>Digital signature (with PIN)</li> <li>Supports non-repudiation</li> <li>Message integrity</li> </ul>
Certificate for Key Management	Optional	A certificate used with its associated asymmetric (private) key, supports the use of encryption for the purpose of confidentiality.	<ul style="list-style-type: none"> <li>Digital encryption</li> <li>Message confidentiality</li> </ul>

Figure 81: PIV Card Digital Certificates<sup>120</sup>

### Implementation Tip

Although FIPS 201 only requires inclusion of the PIV Authentication Key on the card, an agency should strongly consider including the optional certificates as well. Since many vendor pricing models are on a “per seat” basis, there is often no additional cost for the optional certificates, and they allow an agency to leverage additional functions, such as digital signing and encryption, while increasing interoperability with other agencies using the optional certificates.



### 8.1.2. PIV-I Card

As deployment and usage of PIV cards has expanded, the desire arose to issue credentials that are interoperable with federal PIV infrastructure. This capability also supports the objectives of the ICAM segment architecture by allowing an agency to achieve strong security in their interactions with external business partners and customers while eliminating credential management costs for these populations. The PIV card is, as defined, an identification credential issued by a federal agency to its employees and contractors. Additionally, the PIV card standards include several requirements that can only be met by a federal issuer. The specification —Personal Identity Verification Interoperability for Non-Federal Issuers<sup>121</sup> resolves these challenges and defines a common set of minimum requirements for a PIV-I credential<sup>122</sup> that meets the PIV technical specifications for interoperability with PIV infrastructure elements and is issued in a manner that can be trusted by the Federal Government.

The following figure compares the key characteristics of the PIV-I card to the PIV card.

<sup>119</sup> This feature might be removed in future revisions of [FIPS 201](#).

<sup>120</sup> Additional mandatory elements on the PIV card may be included in the revision to [FIPS 201](#), which is currently under revision.

<sup>121</sup> [Personal Identity Verification Interoperability for Non-Federal Issuers](#), Version 1.1, CIO Council, July 2010.

<sup>122</sup> For more information on PIV-I, see [Personal Identity Verification Interoperable \(PIV-I\) Frequently Asked Questions \(FAQ\)](#), Version 1.0, June 28, 2010.

Characteristic	PIV	PIV-I
<b>Terminology</b>	An identity card that is fully conformant with federal PIV standards. Only cards issued by federal entities can be fully conformant. Federal standards ensure that PIV cards are interoperable with and trusted by all Federal Government relying parties.	An identity card that meets the PIV technical specifications to work with PIV infrastructure elements such as card readers, and is issued in a manner that allows Federal Government relying parties to trust the card.
<b>Visual Card Topology</b>	<ul style="list-style-type: none"> <li>Fully conforms to the PIV card visual topology defined in FIPS 201 and SP 800-106.</li> <li>Contains all mandatory items on the front and back of the card.</li> <li>All optional items are formatted and placed in accordance with the standard, if used.</li> </ul>	<ul style="list-style-type: none"> <li>Must be visually distinct from PIV card topology to ensure no suggestion of attempting to create a fraudulent PIV card.<sup>123</sup></li> <li>Must contain, at a minimum: <ul style="list-style-type: none"> <li>Issuing/Sponsoring Organization (e.g., company name)</li> <li>Card holder Photograph</li> <li>Card holder Full Name</li> <li>Card Expiration Date</li> </ul> </li> </ul>
<b>Technical Requirements</b>	Fully conformant with federal PIV standards (i.e., FIPS 201 and related documentation).	Must conform to the NIST technical specifications for a PIV Card as defined in SP 800-73 <sup>124</sup> and meet the cryptographic requirements of FIPS 140 and SP 800-78.
<b>Identifier(s)</b>	<ul style="list-style-type: none"> <li>Mandatory CHUID data object conformant with requirements in SP 800-73.</li> <li>Unique Federal Agency Smart Credential Number (FASC-N) assigned to each individual.</li> <li>Conformant GUID present in the CHUID.</li> </ul>	<ul style="list-style-type: none"> <li>Valid RFC 4122 generated Universally Unique Identifier (UUID), in accordance with SP 800-73, in the GUID field of the CHUID.</li> <li>FASC-N with Agency Code equal to 9999, System Code equal to 9999, and Credential Number equal to 999999, indicating that the UUID is the primary credential identifier.</li> </ul>
<b>Identity Proofing and Background Investigation</b>	<ul style="list-style-type: none"> <li>Identity proofing satisfies SP 800-63, Level of Assurance (LOA) 4.</li> <li>NACI background investigation or equivalent.</li> </ul>	<ul style="list-style-type: none"> <li>Identity proofing satisfies SP 800-63, LOA 4.</li> <li>No background investigation required.</li> </ul>
<b>Digital Certificate Issuance</b>	PIV certificates are issued in direct compliance with federal certificate policies (i.e., COMMON). <sup>125</sup>	PIV-I certificates are issued under their own policies that are cross-certified at the Federal Bridge at specific assurance levels and may be honored by relying agencies at those levels.
<b>Card Authentication Key (CAK)</b>	The CAK is optional on PIV cards.	The CAK is mandatory on PIV-I cards.

**Figure 82: Comparison of PIV and PIV-I**

In addition to understanding the technical and physical requirements of the PIV-I credential, agencies should consider a number of policy and process decisions before fully leveraging PIV-I credentials, including:

- Credential applicability.** A PIV-I card cannot be issued or accepted in the place of a PIV card for individuals who fall under the applicability guidance outlined in OMB M-05-24.<sup>126</sup>

<sup>123</sup> At a minimum, images or logos on a PIV-I card shall not be placed entirely within Zone 11, Agency Seal, as defined by [FIPS 201](#).

<sup>124</sup> [SP 800-73](#)

<sup>125</sup> [X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework](#), Version 3647 – 1.6, February 11, 2009. [COMMON]

- **Agency issuance.** There are certain situations in which a federally-issued PIV-I credential can address the unique needs of a specific group within an agency's population. If an agency chooses to issue PIV-I credentials, they must fully comply with all applicable PIV-I specifications and policies. Additionally, an agency should seek to leverage its existing PIV infrastructure (e.g., existing PKI services and card stock) and ensure that its PIV-I credential is interoperable with the PIV-enabled infrastructure and systems for both physical and logical access.
- **Acceptance and use of PIV-I credentials.** While PIV-I credentials are technically interoperable with the PIV infrastructure, an agency needs to decide if any additional requirements or processes should be required for acceptance and use of the PIV-I card. For example, an agency may choose to limit the physical access of PIV-I cardholders to access points for common areas within a facility.
- **Technical interoperability.** Although the GSA ICAM Lab performs testing<sup>127</sup> to make sure that card issuers conform to PIV-I requirements, an agency should establish a process for determining if an external entity's PIV-I card is interoperable with its systems and applications. Technical interoperability of PIV-I credentials can be affected by the way in which optional aspects of the technical standards and specifications are implemented by the credential issuer.
- **Lifecycle processes.** An agency should define the procedures that support the management and maintenance of a cardholder's PIV-I. These process decisions should be explicitly stated in the contract and/or federation agreement. Key considerations include: How are changes in card status handled and communicated? What is the termination and card collection process? And how will access be provisioned and de-provisioned?

## FAQ

### How can an agency be sure that the external entity issuing a PIV-I followed sound security practices?

Agencies that leverage PIV-I credentials can be assured, with a high level of confidence, that PIV-I issuers follow sound security and privacy practices because they must cross certify with the Federal Bridge Certification Authority (FBCA). In order to be cross certified, external entities must meet extensive control requirements, comply with the X.509 Certificate Policy,<sup>128</sup> and annually demonstrate compliance with certificate policies and procedures.



### 8.1.3. PIV Infrastructure

An agency's PIV infrastructure is comprised of various hardware and software elements that work together to enable the authentication of the PIV card to PACS and LACS, as described in Chapters 10 and 11, respectively. As previously mentioned, agencies have made a significant investment in these components and therefore can greatly benefit from accepting external credentials (e.g., PIV-I) that are interoperable with their existing PIV infrastructure. The

<sup>126</sup> [M-05-24](#), Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, OMB, August 2005. [M-05-24]

<sup>127</sup> Testing performed in support of PIV-I conformance is addressed in the [Personal Identity Verification Interoperable \(PIV-I\) Certification Process](#), Federal PKI Policy Authority Certificate Policy Working Group, Version 1.0, March 8, 2011.

<sup>128</sup> [COMMON](#)

following figure provides an overview of the different components that make up the PIV Infrastructure and provides examples of how an agency can use them with PIV-I cards.

Component	Description	PIV-I Use
<b>Smart Card Readers</b>	Hardware components and associated device drivers necessary to access data stored on the smart card. Readers can be attached to desktop or laptop computers, usually via universal serial bus (USB) cable, and are often installed in expansion slots in laptops.	An agency can configure its smart card readers to read the PKI certificates stored on the PIV-I card.
<b>Middleware</b>	A software component that facilitates interactions between a workstation and a PIV card. PIV middleware interprets the data stored on the PIV card and provides a uniform interface for use by other software that relies on PIV data, such as logical access control and digital signing and encryption applications. <sup>129</sup>	An agency can configure its middleware to communicate between the PIV-I card, the reader, and workstation.
<b>Approved Card Stock (ACS)</b>	The form factor that contains an embedded integrated-circuit chip (ICC) for electronically storing data objects. PIV card stock comes from vendors that are included on the FIPS 201 APL. This card stock can be purchased through GSA Schedule 70 and meets specific requirements, such as durability and inclusion of tamper proofing characteristics. <sup>130</sup>	An agency can use existing PIV card stock to create PIV-I cards.
<b>Directory Services</b>	Provide a means of linking PIV cards to a user's authority to access computer systems, networks and applications. Associating a user's PIV card to their account(s) allows the PIV card to be used for user authentication, providing a higher level of security than username/password.	An agency can provide PIV-I card holders an account within the directory service for authentication to systems, networks, and applications.

**Figure 83: PIV Infrastructure Components**

At each stage of the credential lifecycle, from enrollment to finalization, there are entities and services supplying and supporting the components that comprise the PIV infrastructure. An agency should seek to extend existing services in place for their PIV implementation to support additional functionality (e.g., issuance or acceptance of PIV-I credentials) and achieve economies of scale. The following list provides an overview of the types of PIV service providers that can potentially be leveraged:

- **PIV Enrollment Service Providers.** Provide local presence at agency sites to support the enrollment of PIV applicants.
- **PIV Systems Infrastructure Providers.** Provide an agency with the software functionality (IDMS and Card Management System) to manage PIV credentials.
- **PIV Production Service Providers.** Produce and personalize PIV cards for agency use.
- **PIV Finalization Service Providers.** Provide local presence at agency sites to complete the issuance to the applicant and finalize the personalization of PIV cards.
- **Federal Public Key Infrastructure Shared Service Provider.** Issues digital certificates that are stored on the PIV card and used to authenticate users.

<sup>129</sup> For detailed information regarding approved products, see the [APL](#).

<sup>130</sup> For detailed information regarding approved products, see the [APL](#).

### Implementation Tip

Work with procurement to incorporate PIV-enablement requirements in all solicitations. For example, an agency can require that all computers acquired are equipped with smart card readers or that new applications have built-in PIV capabilities. Ensuring that the products an agency purchases meet PIV requirements up front saves time and money over upgrading or adding onto a solution later.



### 8.1.4. Leveraging the PIV Infrastructure for Exceptional Scenarios

The ICAM target state calls for agency employees and contractors to use the PIV credential for physical and logical access control. As an agency migrates toward enterprise-wide adoption of the PIV card it is likely that it will encounter scenarios in which a user requires access but does not possess a PIV card. These individuals fall into one of the two following groups:

- **PIV cardholders not currently in possession of an active PIV card.** This group includes employees and contractors that fall under the scope of HSPD-12 but do not have an active PIV card in their possession for some period of time during which physical and/or logical access is required. This is commonly the case in agencies where there is a delay between card enrollment and issuance (e.g., to conduct the background investigation or to accommodate card production and delivery). Another common example is the case of users whose PIV credential has been damaged, lost, stolen, or compromised<sup>131</sup> and a replacement card has not yet been received.
- **Individuals for whom a PIV card is not required.** This group includes individuals who are not employees or contractors of an agency within the Executive Branch of the Federal Government but require access to agency resources. It also includes agency employees and contractors who are either short-term (i.e., employed less than 6 months) or fall into a special category (e.g., guest researchers, volunteers, interns, etc.) and will not be issued a PIV card following a risk-based decision process. There are also some individuals who fall under the scope of HSPD-12 but for whom the PIV processes cannot successfully be completed (e.g., individuals with less than three years of residency in the United States needed to perform a NACI investigation).<sup>132</sup>

In order to maintain an acceptable level of security for physical and logical access, an agency should consider providing these users with credentials that leverage the existing PIV infrastructure and meet applicable resource security requirements. It is recommended that an agency determine the characteristics of any user groups that will require a non-PIV credential, including the security requirements and assurance level of the resources to which they require access, in order to determine which non-PIV credential type is most appropriate. The following subsections introduce several types of credentials that can address access for these individuals and the characteristics for when to apply them.

#### 8.1.4.1. Non-PIV Credential Types Interoperable with Existing PIV Infrastructure

There are a number of non-PIV credential types that are available for an agency to issue to individuals who require physical and/or logical access but do not have a PIV card. This section

<sup>131</sup> A detailed discussion on lost or stolen credentials can be found in Section 8.3.5.3.

<sup>132</sup> Additional details and guidance for credentialing individuals with less than three years of residency in the United States can be found in the Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12, July 31, 2008.

introduces and describes each of the non-PIV credential types, which leverage FIPS 201-compliant Approved Card Stock (ACS) and digital certificates defined under the Federal PKI Common Policy Framework (COMMON), which promotes reuse and interoperability with existing PIV infrastructure investments. The credential types vary with regard to card topography requirements, required identity proofing, and the level of assurance supported.<sup>133</sup> These differences are described further below:

- **PIV-I credential.** This non-PIV credential type provides very high confidence in the asserted identity's validity (Level of Assurance [LOA] 4) and is therefore a good option for federal issuance to groups who require access to environments where risks and consequences of data compromise are moderate. PIV-I credentials leverage existing PIV infrastructure, which can provide an agency with cost and process efficiencies. PIV-I credentials, however, may need to be printed off-site because they have specific topography requirements.<sup>134</sup> This introduces a delay in issuance and therefore may not be the best option for those scenarios that require instant credentials. PIV-I credentials are described in further detail in Section 8.1.2.

#### Implementation Tip

To the greatest extent possible, an agency should seek to leverage externally-issued PIV-I cards before issuing new ones. To prevent issuing duplicate credentials, an agency should determine if externally-issued PIV-I cards are available in the target community before issuing a separate PIV-I card. This supports the ICAM objective of cost savings and efficiency and allows the Federal Government to leverage the investment commercial entities are making in this space.



- **ACS + Medium Hardware Certificate.**<sup>135</sup> This non-PIV credential type provides very high confidence in the asserted identity's validity (LOA 4) and is therefore a good option for issuance to groups who require access to environments where threats to data are high or the consequences of the failure of security services are high. Unlike a PIV-I credential, an ACS + Medium Hardware Certificate credential does not have topography requirements, so it can be printed quickly and locally to address scenarios in which users need immediate credentials. This approach requires in-person proofing, which might not be viable for all of the potential user scenarios.
- **ACS + Basic Certificate.** This non-PIV credential type provides high confidence in the asserted identity's validity (LOA 3). This credential could be a good option for federal issuance to groups who need access to areas and systems where there are risks and consequences of data compromise, but they are not considered to be of major significance. An ACS + Basic Certificate credential also does not have topography requirements, so it can be printed quickly and locally to address scenarios in which users need immediate credentials. This approach can be achieved with remote identity proofing, which may be more suitable for users who cannot feasibly complete in-person proofing requirements.

<sup>133</sup> As defined in [SP 800-63](#).

<sup>134</sup> [Personal Identity Verification Interoperability For Non-Federal Issuers](#)

<sup>135</sup> [Medium Hardware Policy](#), Federal PKI Policy Authority, September 12, 2006.

- **ACS + Rudimentary Certificate.** This non-PIV credential provides the lowest degree of assurance concerning identity of the individual. Because an ACS + Rudimentary Certificate can be issued at LOA 1 or LOA 2, the identity proofing varies (LOA 1 requires no identity proofing, LOA 2 requires minimal identity proofing). This level is relevant to environments in which the risk of malicious activity is considered to be low; it is not suitable for transactions requiring authentication and is primarily intended for use to provide data integrity to signed information. An ACS + Rudimentary Certificate credential does not have topography requirements, so it can be printed quickly and locally to address scenarios in which users need immediate credentials.

Each of these non-PIV credential types are compliant for use in the ICAM target state because they leverage ACS from the GSA APL, meet PIV technical interoperability requirements, and include PKI credentials that are covered under the FBCA. Additionally, each of these non-PIV credentials have a different level of assurance based on the strength of the binding between the public key and the individual whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.<sup>136</sup>

#### Implementation Tip

An agency may decide that a local credentialing solution is more cost-efficient or better addresses the needs of its users who will not receive a PIV card than the non-PIV credentials described in this section. For example, users who only require physical access to low risk areas may not require a certificate-based credential. This decision to pursue a local credentialing solution should be made after thoughtful analysis, and the chosen approach should seek to minimize multiple, incompatible credentials and leverage existing infrastructure as much as possible.



Figure 84 provides a summary of the credential types and characteristics described in the paragraphs above.

Type	Level of Assurance (LOA)	Topography Requirements	Identity Proofing Requirements
PIV-I Credential	4	✓	In-person identity proofing required.
ACS + Medium Hardware Certificate	4		In-person identity proofing required.
ACS + Basic Certificate	3		Remote or in-person identity proofing allowed.
ACS + Rudimentary Certificate	1, 2		Requires little or no identity proofing.

Figure 84: Credential Types and Characteristics

#### 8.1.4.2. Establishing Trust

An important aspect of issuing and accepting non-PIV credentials is trust. As such, an agency should take into consideration the degree of confidence it has in the enrollment, identity

<sup>136</sup>The level of assurance language in this subsection is derived from [COMMON](#).

proofing, and issuance processes required to obtain each of the existing non-PIV credentials.

Figure 86 compares the identity proofing requirements between each of the non-PIV Credentials.<sup>137</sup>

FBCA Identification and Authentication Process	Description	PIV-I Card	ACS + MHW	ACS + Basic	ACS + Rudimentary
<b>Authentication of Human Subscriber<sup>138</sup></b>	<p>Identity shall be established no more than 30 days before initial certificate issuance.</p> <p>The following information shall be recorded for issuance of each certificate:</p> <ul style="list-style-type: none"> <li>• The identity of the person performing the identification;</li> <li>• A signed declaration by that person that he or she verified the identity of the applicant;</li> <li>• A unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s) (in-person identity proofing);</li> <li>• The date of the verification; and</li> <li>• A declaration of identity signed by the applicant.</li> </ul>	✓	✓		
	<p>An entity certified by a State or Federal Entity as being authorized to confirm identities may perform in-person authentication on behalf of the Registration Authority.</p>	✓	✓	✓	
	<p>The following biometric data shall be collected :</p> <ul style="list-style-type: none"> <li>• An electronic facial image - a new facial image shall be collected each time a card is issued; and</li> <li>• Two electronic fingerprints.</li> </ul>	✓			
	<p>Applicant may apply and receive a certificate by providing his or her e-mail address.</p>				✓
	<ul style="list-style-type: none"> <li>• Identity may be established by in-person proofing before a Registration Authority or Trusted Agent; or remotely verifying information provided by applicant including ID number and account number through record checks.</li> <li>• Confirms that: name, DOB, address and other personal information in records are consistent with the application and sufficient to identify a unique individual.</li> <li>• Address may be confirmed if the credential is issued in a manner that confirms the address of record supplied by the applicant or confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice.</li> </ul>			✓	

<sup>137</sup> See the [COMMON](#) for more information.

<sup>138</sup> Addressed in Section 3.2.3.1 of [COMMON](#).

FBCA Identification and Authentication Process	Description	PIV-I Card	ACS + MHW	ACS + Basic	ACS + Rudimentary
	<p>Identity shall be established by in-person proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy.<sup>139</sup></p> <p>Credentials required are:</p> <ul style="list-style-type: none"> <li>• One Federal Government-issued picture ID;</li> <li>• One REAL ID Act compliant picture ID, or</li> <li>• Two Non-Federal Government IDs, one of which shall be a photo ID (e.g., Non-REAL ID Act compliant Driver's License).</li> <li>• Any credentials presented must be unexpired.</li> </ul> <p>Credentials required are:</p> <ul style="list-style-type: none"> <li>• Two identity source documents in original form from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification.</li> <li>• At least one document shall be a valid State or Federal Government-issued picture ID.</li> <li>• The use of an in-person antecedent is not applicable (Note: because biometrics must be collected, in-person proofing is required).</li> </ul> <p>A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement.</p>	✓	✓		
<b>Non-Verified Subscriber Information<sup>140</sup></b>	Information that is not verified shall not be included in certificates.	✓	✓	✓	
<b>Identification and Authentication for Routine Re-key<sup>141</sup></b>	Identity may be established through use of current signature key.				✓
	Identity shall be reestablished through initial registration process at least once every 15 years.			✓	
	Identity shall be reestablished through initial registration process at least once every 9 years.	✓	✓		
<b>Enrollment Process and Responsibilities<sup>142</sup></b>	All communications shall be authenticated and protected.	✓	✓	✓	✓
	<p>If databases or other sources are used to confirm Subscriber attributes, then these sources and associated information sent to a Certification Authority (CA) shall require:</p> <ul style="list-style-type: none"> <li>• When information is obtained through one or more information sources, an auditable chain of custody must be in place.</li> <li>• All data received be protected and securely exchanged in a confidential and tamper evident manner, and protected from unauthorized access.</li> </ul>	✓	✓	✓	✓

<sup>139</sup> Addressed in Section 3.2.3.1 of [COMMON](#).

<sup>140</sup> Addressed in Section 3.2.4 of [COMMON](#).

<sup>141</sup> Addressed in Section 3.3.1 of [COMMON](#).

<sup>142</sup> Addressed in Section 4.1.2 of [COMMON](#).

FBCA Identification and Authentication Process	Description	PIV-I Card	ACS + MHW	ACS + Basic	ACS + Rudimentary
<b>Certificate Application Processing</b> <sup>143</sup>	Information in certificate applications must be verified as accurate before certificates are issued.	✓	✓	✓	✓
<b>CA Actions During Certificate issuance</b> <sup>144</sup>	Verify the source of a certificate request before issuance	✓	✓	✓	✓
<b>Processing Certificate Modification Requests</b> <sup>145</sup>	Proof of all subject information changes must be provided and verified before the modified certificate is issued.	✓	✓	✓	✓
<b>Private Key Delivery to Subscriber</b> <sup>146</sup>	When CAs or RAs generate keys on behalf of the Subscriber, then the private key must be delivered securely to the Subscriber.	✓	✓	✓	✓
	The Entity CA must maintain a record of the subscriber acknowledgement of receipt of the token.	✓	✓	✓	✓
<b>Other Aspects of Activation Data</b> <sup>147</sup>	In the event activation data must be reset, a successful biometric 1:1 match of the applicant against the biometrics collected is required.	✓			

Figure 85: Summary of Identification and Authentication Requirements by Credential Type

#### 8.1.4.3. *Implementation Considerations*

There are a number of factors that contribute to an agency's decision of which non-PIV credential to issue. For some scenarios, more than one type of non-PIV credential may be viable based on the requirements. In addition, if an agency has multiple user populations that do not have PIV credentials it may be possible to select different solutions based upon these scenarios. An agency should carefully consider the requirements of the population while providing cost effective solutions that meet security requirements. To assist an agency in this process, the following list describes considerations for an agency to address when selecting and implementing a non-PIV solution:

- **Compatibility of non-PIV credential with existing infrastructure.** An important aspect of leveraging existing investments, technologies, and processes includes determining the ability of the non-PIV credential to support requirements of an agency's

<sup>143</sup> Addressed in Section 4.2 of [COMMON](#).

<sup>144</sup> Addressed in Section 4.3.1 of [COMMON](#).

<sup>145</sup> Addressed in Section 4.8.3 of [COMMON](#).

<sup>146</sup> Addressed in Section 6.1.2 of [COMMON](#).

<sup>147</sup> Addressed in Section 6.4.3 of [COMMON](#).

access control system. For example, an agency may decide not to issue PIV-I credentials to a user population if its PACS uses the FASC-N to make access decisions.<sup>148</sup>

- **Issuance lead-time of non-PIV credential types.** Certain non-PIV credential types may take longer to issue than others due to registration, processing, or production requirements. An agency should analyze the lead-time of each to determine which option best addresses the needs of each of the non-PIV issuance scenarios.
- **Establishment of policies and processes.** A Federal Issuer is responsible for meeting all requirements for the type of certificate that is being used on the non-PIV card, including affiliation and identity proofing. An agency should implement policies and processes that address the issuance of non-PIV credentials. These requirements should be consistent with the ICAM target state and support the goals of cost savings, enhanced security, and efficiency.
- **Vetting requirements.** None of the non-PIV credential types includes any background investigation for issuance. Therefore, when implementing the desired non-PIV approach for individuals who are not employees or contractors,<sup>149</sup> an agency should determine if any additional requirements or processes should be required for acceptance and use of the non-PIV credential. If the individual will be given access to resources similar to PIV cardholders, it is recommended that additional security controls be considered to make security commensurate.

## 8.2. Authentication

As defined in the ICAM Services Framework (see Section 3.2.4), authentication is the process of verifying that a claimed identity is genuine and based on valid credentials. This section outlines the mechanisms available on the PIV and PIV-I card that allow an agency to authenticate the identity of the cardholder and subsequently make appropriate access-related decisions. It also provides more detailed implementation guidance for performing authentication using the PKI credentials on the card. The information and guidance presented in this section is intended to assist an agency in providing answers to several common authentication questions, including:

- How do I authenticate PIV and PIV-I cards?
- How are the certificates on PIV and PIV-I cards validated?

### 8.2.1. PIV and PIV-I Authentication Mechanisms

An agency may utilize several of the PIV and PIV-I card features to perform authentication. This approach was intended to allow an agency the opportunity to select an authentication mechanism with sufficient strength to meet the appropriate level of assurance for the applications being accessed with the PIV card. The following figure summarizes the PIV authentication mechanisms available on the card and their associated authentication procedures. Implementation of these methods within particular physical and logical access usage scenarios is addressed in further detail in Sections 10.3 and 11.3, respectively.

---

<sup>148</sup> For a description of the identifiers present on the PIV-I card, see Section 8.1.2.

<sup>149</sup> Employees and contractors fall under the background investigations requirements outlined in FIPS 201 and related HSPD-12 policy memoranda.

Authentication Mechanism	Authentication Procedure <sup>150</sup>
PIV Visual Credentials (VIS)	<ul style="list-style-type: none"> <li>• The cardholder presents credential to Guard/Verifier;</li> <li>• The Guard/Verifier performs counterfeiting and forgery check and verifies that credential has not been tampered with;</li> <li>• The Guard/Verifier performs visual inspection of card characteristics (e.g., facial image) to authenticate Cardholder;</li> <li>• The Guard/Verifier examines credential expiration date; and</li> <li>• Authentication complete.</li> </ul>
PIV CHUID	<ul style="list-style-type: none"> <li>• The cardholder presents credential to card reader;</li> <li>• The card reader electronically reads the CHUID on the PIV card;</li> <li>• The PIV application checks the digital signature on the CHUID to ensure the CHUID was signed by a trusted source and is unaltered;</li> <li>• The PIV application checks the expiration date on the CHUID to ensure that the card has not expired;</li> <li>• The PIV application uses a unique identifier (e.g., Federal Agency Smart Credential Number [FASC-N]) within the CHUID as input to the authorization check to determine whether the cardholder should be granted access; and</li> <li>• Authentication complete.</li> </ul>
PIV Biometrics (BIO)/PIV Biometrics Attended (BIO-A)	<ul style="list-style-type: none"> <li>• The cardholder presents credential to card reader;</li> <li>• The card reader electronically reads the CHUID on the PIV card;</li> <li>• The PIV application checks the expiration date in the CHUID to ensure the card has not expired;</li> <li>• The PIV application prompts the cardholder to submit a PIN, activating the PIV card and in the case of BIO-A, the PIN entry is done in the view of an attendant;</li> <li>• The PIV application reads the biometric from the card;</li> <li>• The PIV application verifies the signature on the biometric to ensure the biometric is intact and comes from a trusted source;</li> <li>• The PIV application prompts the cardholder to submit a live biometric sample and in the case of BIO-A, the biometric sample is submitted in the view of an attendant;</li> <li>• If the biometric sample matches the biometric read from the card, the cardholder is authenticated to be the owner of the card;</li> <li>• The PIV application compares the FASC-N in the CHUID with the FASC-N in the Signed Attributes field of the external digital signature on the biometric;</li> <li>• The PIV application uses the FASC-N as input to the authorization check to determine whether the cardholder should be granted access; and</li> <li>• Authentication complete.</li> </ul>
Match-on-Card Biometric Comparison <sup>151</sup>	<ul style="list-style-type: none"> <li>• The cardholder presents their card to a contactless biometric reader;</li> <li>• The cardholder presents their finger to the biometric scanner;</li> <li>• The host establishes a secure session with the card;</li> <li>• The host prepares an encrypted template containing the fingerprint (image or minutia) and transmits it via contactless interface to the card;</li> <li>• The card decrypts the template and compares it with the reference template stored on the card;</li> <li>• The card returns signed result (i.e., Yes/No) to the host; and</li> <li>• Authentication complete.</li> </ul>
PIV Authentication Key (PIV AUTH)	<ul style="list-style-type: none"> <li>• The cardholder presents credential to card reader;</li> <li>• The card reader electronically reads the PIV Authentication Key certificate from the PIV card;</li> <li>• The PIV application prompts the cardholder to submit a PIN;</li> <li>• The submitted PIN is used to activate the card;</li> </ul>

<sup>150</sup> As defined in [FIPS 201](#).

<sup>151</sup> For information on the match-on-card biometric comparison, reference [NIST Interagency Report 7452](#): Secure Biometric Match-on-Card Feasibility Report, November 2007. As of publication of the FICAM Roadmap and Implementation Guidance, FIPS 201 is under revision, with the match-on-card biometric comparison anticipated to be added as a PIV authentication mechanism.

Authentication Mechanism	Authentication Procedure <sup>150</sup>
	<ul style="list-style-type: none"> <li>• The card reader issues a challenge string to the card and requests an asymmetric operation in response;</li> <li>• The PIV card responds to the previously issued challenge by signing it using the PIV authentication private key;</li> <li>• The PIV application verifies the response signature and conducts a standards-compliant PKI path validation;</li> <li>• The PIV application checks the related digital certificate to ensure that it is from a trusted source;</li> <li>• The PIV application checks the revocation status of the certificate to ensure current validity;</li> <li>• The PIV application validates the response as the expected response to the issued challenge;</li> <li>• The card reader extracts the Subject Distinguished Name and unique identifier (e.g., FASC-N) from the authentication certificate and passes this data as input to the access control decision; and</li> <li>• Authentication complete.</li> </ul>
Asymmetric Card Authentication Key (PKI-CAK)	<ul style="list-style-type: none"> <li>• The cardholder presents credential to card reader;</li> <li>• The card reader reads the Card Authentication Key (CAK) certificate from the PIV card;</li> <li>• The card reader issues a challenge string to the card and requests a response encrypted with PKI;</li> <li>• The PIV application verifies the response signature and conducts a standards-compliant PKI path validation;</li> <li>• The PIV application checks the related digital certificate to ensure that it is from a trusted source and if the PKI certificate is expired;</li> <li>• The PIV application checks the revocation status of the certificate to ensure current validity;</li> <li>• The PIV application validates the response as the expected response to the issued challenge;</li> <li>• The card reader extracts the FASC-N from the card authentication certificate and passes the data as input to the access control decision; and</li> <li>• Authentication complete.</li> </ul>
Symmetric Card Authentication Key (CAK)	<ul style="list-style-type: none"> <li>• The cardholder presents credential to card reader;</li> <li>• The card reader electronically reads the CHUID from the PIV card;</li> <li>• The PIV application checks the digital signature on the CHUID to ensure the CHUID was signed by a trusted source and is unaltered;</li> <li>• The PIV application checks the expiration date on the CHUID to ensure that the card has not expired;</li> <li>• The card reader issues a challenge string to the card and requests a response;</li> <li>• The PIV card responds to the previously issued challenge by signing it using the symmetric card authentication key;</li> <li>• The PIV application validates the response as the expected response to the issued challenge;</li> <li>• The card reader extracts a unique identifier (e.g., FASC-N) within the CHUID and passes the data as input to the authorization check to determine whether the cardholder should be granted access; and</li> <li>• Authentication complete.</li> </ul>

**Figure 86: PIV Card Authentication Mechanisms and Procedures Summary**

Many of the authentication mechanisms and associated procedures for the PIV-I card are similar to those of the PIV card. There are, however, some differences and considerations that ICAM implementers should understand and address before accepting PIV-I credentials, including:

- **Visual (VIS).** PIV and PIV-I cards are visually distinct from one another. An agency should ensure that security guards are properly trained on how to authenticate an

individual based on the PIV-I card's visual characteristics. It is also likely that the visual characteristics of PIV-I cards will vary based on the issuing entity, which can complicate a guard's ability to perform VIS. Due to the weakness of visual authentication, it is strongly recommended that agencies seek to use some form of electronic validation for PIV-I cards in conjunction with or in place of VIS.

- **CHUID.** The CHUID is part of the FASC-N, which in the PIV-I data model is partially populated with all 9s. Because of this, an agency is unable to ensure uniqueness and authenticate PIV-I card holders using the CHUID. An agency should, therefore, use the UUID to authenticate PIV-I card holders in scenarios where the CHUID would be used for PIV authentication.
- **PKI Certificates.** PIV and PIV-I cards use different PKI certificate policies for the certificates on the card. The basic authentication steps are the same for both; however, an agency's applications need to be able to differentiate between the certificates.

As noted in the Figure 86, a key step in authenticating a PKI certificate is determining if the certificate is valid. This process involves additional implementation considerations, which are addressed in greater detail in the following section.

## 8.2.2. PKI Credential Validation

An important authentication service component within the ICAM Services Framework (see Section 3.2.4) is the credential validation service capability. Credential validation is important because it establishes trust in PIV and PIV-I credentials. The following sections discuss the two main aspects of credential validation: trust path discovery and revocation checking.

### 8.2.2.1. Trust Path Discovery

Certificate validation begins with trust path discovery, a process to determine the chain of Certification Authority (CA) certificates and cross-certificates that run from a relying party's trust anchor to the certificate on the credential. Trust paths can be discovered at the time of the transaction or created once and cached. After a trust path has been established, the trust path must be validated. Trust path validation involves an assessment of the certificates that make up the trust path to determine each certificate's validity status at that moment. Certificates in a trust path that is cached are validated in real-time at the beginning of each transaction.

An agency should take special care to ensure proper validation of certificates. The Federal Trust Infrastructure provides a number of essential functions that can be leveraged by an agency for validation, but an agency may expose themselves to significant risk of unauthorized access if applications are not configured to properly leverage the Federal Trust Infrastructure. The principle functions provided by the Federal Infrastructure are:

- **Standard policies.** Policies describe how a certificate is issued, identifying requirements such as identity proofing, cryptographic strength, and whether particular tokens such as smart cards are used. When a CA issues a certificate, the certificate includes an Object Identifier (OID) that indicates which policy was followed. OIDs registered through NIST for the purpose of certificate issuance are not only reflected in the certificates themselves, but also included in written policy documents such as the Common Policy,<sup>152</sup> where the

---

<sup>152</sup> [COMMON](#)

circumstances under which the certificates were issued are defined. Standard Federal PKI policies are managed by the Federal PKI Policy Authority and are captured in RFC 3647 Certificate Policies. A given certificate policy can define multiple policies for certificate issuance. Government-wide policies are defined in the Common Policy CP and the Federal Bridge Certificate Policy. A given CA may issue certificates under multiple policies, so a critical part of the validation process should require that PIV-reliant applications evaluate the policy OID of each certificate to determine whether a certificate should be trusted for a given application.

- **Certification of trusted issuers.** The Federal PKI Policy Authority reviews the policies and practices of CAs to determine whether they can be trusted by federal agencies. The Federal PKI Management Authority (MA) enables trust of valid issuers by issuing cross-certificates to approved CAs or PIV-I issuers. These cross-certificates indicate which standard policies should be considered valid for the issuer. It is trivial for an attacker to establish a rogue CA or PIV-I issuer and to create valid digital certificates. The only way to identify trusted issuers is to check for certification from the Federal PKI MA and inspect the policy OIDs.

Relying party validation of trusted issuers, policy OIDs, and revocation data is generally referred to as Path Discovery and Validation (PD-Val).<sup>153</sup> Proper use of certificate-based credentials, such as the PIV and PIV-I cards, requires that systems be capable of performing PD-Val. Systems capable of PD-Val must also be configured with the policy OIDs that should be trusted for a given application.<sup>154</sup> An agency should consider the following when deploying PD-Val solutions:

- **COTS limitations.** Most COTS products do not fully implement PD-Val natively. An agency should not assume that applications supporting certificate authentication properly implement PD-Val. Additional integration work may be required to achieve the desired functionality.
- **Shared infrastructure.** An agency should implement shared certificate processing capabilities consistent with the ICAM Services Framework (see Section 3.2.4) and the agency conceptual target technical architecture (see Figure 11 in Part A) so that PD-Val capable software can be leveraged by multiple applications. For example, an Online Certificate Status Protocol (OCSP) service established at the enterprise level that is shared by multiple organizations to validate PIV cards.
- **Use of proper trust anchor.** A trust anchor is a self-signed certificate issued by a CA that serves as the source of trust for other CAs. The trust anchor for the Federal Government is the Federal Common Policy Root,<sup>155</sup> which is managed by the Federal PKI Management Authority (FPKIMA). PD-Val engines should be configured to use the Common Policy root certificate as a Trust Anchor to ensure certificates by un-trusted issuers cannot be used to access federal systems.
- **Specified policy OIDs.** PD-Val engines should be configured to specify which certificate policy OIDs are trusted to ensure low assurance certificates from trusted issuers cannot

---

<sup>153</sup> More detailed information on PD-Val, including software test suites, is available from the ICAMSC and their work groups.

<sup>154</sup> The ICAMSC and NIST have established requirements and test tools for software implementing PD-Val, including the [Public Key Interoperability Test Suite](#) (PKITS).

<sup>155</sup> The Federal Common Policy Root is not the trust anchor for agencies with self-certifying legacy PKI's (e.g., State Department), but these agencies are cross-certified to the Federal Bridge Certificate Authority.

be used to access federal systems. The policy OIDs for PIV credentials include [id-fpki-common-authentication], [id-fpki-common-hardware], and [id-fpki-common-cardAuth].

There are a variety of tools and technologies available to an agency for performing PD-Val. Before implementing this type of tool, an agency should perform a risk-based analysis to determine which option best meets their specific needs. The following table provides an overview of PD-Val tools and technologies:

Description	
<b>SCVP</b>	Server-based Certificate Validation Protocol (SCVP) is an Internet protocol used to determine the path between a X.509 digital certificate and a trusted root (Delegated Path Discovery) and to validate that path (Delegated Path Validation) according to a specific validation policy. SCVP makes it easier for an agency to deploy PIV-enabled applications by reducing the burden and overhead on agency applications performing certification path validation and centralizing the management of validation policies.
<b>TAMP</b>	Trust Anchor Management Protocol (TAMP) is a protocol used to manage the trust anchors and community identifiers contained in a trust anchor store.
<b>PRQP</b>	The PKI Resource Query Protocol (PRQP) is an Internet protocol used for obtaining information about services associated with a X.509 Certification Authority. It was created to solve interoperability and usability issues among PKIs, specifically addressing certain problems associated with finding services and data repositories associated with a CA.

**Figure 87: Examples of PD-Val Technologies**

Where agency system limitations prevent proper certificate processing using full PD-Val, an agency may make a local risk-based decision to manually configure local trust anchors as an alternative (i.e., locally store a Root CA certificate). This approach, typically referred to as direct trust, has substantial risks and generally should only be used as a transition state after careful consideration. Similarly, an agency may make a local risk based decision to perform PD-Val functions when a credential is enrolled or provisioned rather than each time they are used. This approach also has significant risks, but may improve system performance or provide transitional capabilities.

The following figure describes the benefits and limitations of the different validation methods available to an agency. This list is not intended to be comprehensive; an agency must do a thorough risk analysis when choosing to adopt one validation model over the other.

Benefits		Limitations
<b>PD-Val</b>	<ul style="list-style-type: none"> <li>Provides real time validation resulting in the most up-to-date information</li> <li>Does not require systems to be reconfigured if the trust path changes</li> </ul>	<ul style="list-style-type: none"> <li>Requires connection to a network</li> <li>Many products that are currently available may not properly support PD-Val</li> <li>May require more time than direct trust to process trust paths</li> </ul>
<b>Direct Trust</b>	<ul style="list-style-type: none"> <li>Provides faster processing of trust paths than PD-Val</li> <li>Does not need to be connected to a network</li> </ul>	<ul style="list-style-type: none"> <li>Requires systems to be reconfigured if the trust path is modified and the potential impacts of this are significant</li> <li>If a certificate in the path is revoked, a relying party may not know about the revocation until the trust path is manually updated (or until the CRLs are updated, if the product checks CRLs)</li> </ul>

**Figure 88: Benefits and Limitations of Validation Models**

### 8.2.2.2. Revocation Checking

Trusted CAs that issue certificates are required to publish a list of all certificates that have been revoked. Certificates can be revoked for a variety of reasons including compromise, termination, etc. Before trusting a certificate, an agency should first verify that the certificate has not been revoked. CA revocation data is published to online repositories, whose locations are specified in the certificate. Revocation data is signed by the issuer to ensure that it cannot be spoofed or altered. Updated revocation data is published regularly. The FPKIMA also publishes revocation data for certificates to trusted issuers. An agency should check this revocation data as part of certificate processing. Federal PKI (FPKI) provides two methods for obtaining revocation data to validate the certificates on PIV and PIV-I credentials:

- **Certificate Revocation Lists (CRLs).**<sup>156</sup> A CRL is a list that is published by the CA at defined intervals and contains certificates that have not yet expired, but which are identified as invalid (revoked). Certificates may be revoked for a number of reasons, including a change in the information contained in the certificate or a suspected compromise of the private key associated with the public key in the certificate.
- **Online Certificate Status Protocol (OCSP).** An OCSP is an Internet protocol used to obtain the revocation status of a digital certificate via an Internet connection in real-time. OCSP is often referred to as —OCSP Responder|| because of the request/response format of the certificate checking messages.

When determining which certificate validation method to implement to support its ICAM functions, an agency should perform an analysis of both CRLs and OCSPs. To assist in this decision-making process, Figure 89 provides a high-level overview of the general benefits and limitations of CRLs and OCSPs based on the common characteristics of each validation method. The statements included in the figure may vary in applicability for an agency, based on the way in which the approach is implemented, an agency’s PKI infrastructure (e.g., legacy, shared services, etc.), the size of an agency’s user population, and the type of product(s) used to support the certificate validation method.

	Benefits	Limitations
CRL	<ul style="list-style-type: none"> <li>• Typically easier to manage for small numbers of users</li> <li>• Supported by most products</li> <li>• Provides rapid certificate status validation from cached CRL</li> <li>• Allows off-line certificate status validation using cached information</li> <li>• Typically leverages existing infrastructure and can therefore be easier and less expensive to implement than OCSP</li> </ul>	<ul style="list-style-type: none"> <li>• Typical CRLs grow bigger with time and can likely become too large for workstations to continually cache or for clients/relying parties to download</li> <li>• Limitations on wireless communication bandwidth may affect the suitability of CRLs for use with mobile devices</li> <li>• In a federated environment, the number of CRLs required to perform validation is greatly increased</li> <li>• In general, CRL downloads for updates or because of expiration can place a significant burden on network bandwidth</li> </ul>

<sup>156</sup> For more information on the format and semantics of certificates and CRLs, refer to RFC 3280.

	Benefits	Limitations
OCSP	<ul style="list-style-type: none"> <li>Typically less burdensome on networks than CRLs</li> <li>Provides on-line certificate status validation to relying parties on demand</li> <li>Relying parties are not required to download and store certificate data</li> <li>Can be updated more frequently with less overhead than typical CRLs</li> </ul>	<ul style="list-style-type: none"> <li>May require multiple queries to validate the entire certificate chain</li> <li>An OCSP's revocation data is based on information in CRLs, so data from OCSP is not as up-to-date as CRLs</li> <li>Not as widely supported as CRLs</li> <li>Network performance impacts the responsiveness of OCSP</li> <li>OCSP can be more complex and costly to implement than CRLs</li> </ul>

Figure 89: Benefits and Limitations of CRLs and OCSPs

Lesson Learned	
<p>Certificate checking capabilities can be integrated with other access control processes. The Department of Health and Human Services (HHS) established enterprise software to manage and streamline security identities, compliance, and security events across disparate physical security systems. This system checks the validity of the card holder's certificates every 18 hours and immediately restricts physical access through all connected PACS servers if the system discovers revoked or suspended certificates.</p>	

### 8.3. PIV Card Usage Challenges

Agencies have identified numerous technical and process implementation challenges as they have worked to issue and manage PIV cards for their employees and contractors. Due to the extensive progress that has been made in the issuance of PIV cards, many agencies are now looking to mature and improve their agency-specific processes and procedures that support the PIV credentialing effort in order to improve the end-user experience. Additionally, in order for agencies to fully leverage PIV cards to enable access to their resources, it is essential to resolve PIV card usage challenges in order to provide robust life cycle support for PIV credential management. As PIV card usage increases, lifecycle management and technology migration over time become increasingly critical components of the agency's ICAM program. A key characteristic of the ICAM target state is the implementation of policies and procedures at the enterprise-level; therefore, an agency should consider addressing these PIV card usage challenges with agency-wide solutions and approaches. This section provides guidance and lessons learned to address some of the common challenges and process improvement efforts that an agency may pursue as they work to fully leverage the PIV credential.

Privacy Tip	
<p>When taking steps to enhance the credentialing process to create a better end-user experience (e.g., automated notifications), an agency should coordinate with their Privacy Office early and often throughout the improvement effort. Privacy Officers can help ICAM implementers identify potential privacy enhancements (e.g., use of privacy screens on enrollment workstations) and ensure that individuals' Personally Identifiable Information (PII) is protected in compliance with applicable privacy laws and regulations.</p>	

The information and guidance presented in this section is intended to assist an agency in providing answers to several common PIV card usage questions, including:

- How can my agency decrease the time between enrollment and issuance of the PIV card?
- What are some considerations around information printed on the face of the PIV card?

- How can my agency leverage the PIV for card holders that have administrator access privileges?
- What are some reasonable accommodations that my agency can provide to individuals with physical disabilities?

### 8.3.1. Card Issuance Lead Time

FIPS 201 defines a clear set of process requirements for enrolling and issuing PIV cards in order to meet the security objectives of HSPD-12. In some cases, these requirements are more rigorous than previous processes and thus have increased the issuance time from what was customary for legacy badging operations. As such, agencies have been faced with the challenge of getting PIV cards into the hands of their employees and contractors fast enough so as not to impede the individual's ability to work. The following list describes some of the process areas an agency should address to minimize the time between an individual's first day of work and PIV card issuance as they fully leverage PIV and PIV-I credentials.

#### 8.3.1.1. Sponsorship

Sponsorship is the first step in the PIV credentialing process and therefore plays a key role in how quickly an individual can be issued a PIV card. An agency should ensure that this process is streamlined, roles are well-defined, and applicants fully understand their responsibilities. Some considerations to make this process more effective to support timely issuance of a PIV credential are as follows:

- **Integration with HR processes.** Sponsorship can be integrated with existing HR and on-boarding processes so that the individual is already well into the credentialing process on his first day of work. For example, individuals can fill out required PIV forms at the same time as they are completing other employment forms, such as payroll information.
- **Process automation.** An agency can automate the supporting activities within sponsorship. For example, the information required for sponsorship can be populated from other authoritative sources. This effort reduces the amount of time it takes for a sponsorship request to be created, reduces the redundancy of an applicant submitting the same information multiple times, and minimizes the potential for human error by reducing the amount of information the Sponsor has to manually input into the system.

#### Lesson Learned

Integrating HR processes can help improve employee satisfaction while promoting efficiency and productivity within an agency. Treasury's PIV Data Synchronization solution integrates HR processes with USAccess to automatically populate the UPN and email address in the PIV card certificates. This simplifies the employee's on-boarding process and enables them to log onto the agency's network and email on their first day of employment.



#### 8.3.1.2. Background Investigation

Per FIPS 201, agencies must complete a minimum background investigation for PIV cardholders. This requirement creates two groups of applicants: those who have an existing investigation on file and those who need an appropriate background investigation initiated. In addition, the following are some considerations an agency should address to support the timely issuance of a PIV credential:

- **Condition of employment.** Some agencies require that employees have a completed background investigation before being hired for the job. Although this might not be possible for all agencies, this approach ensures that employees can start the credentialing process on or before the first day of employment and get their PIV card produced and issued to them immediately following enrollment.
- **Process automation.** An agency should, to the greatest extent possible, automate the processes required to obtain the individual's background investigation information (e.g., form submission and fingerprints) and report the results to the necessary systems and applications, as discussed in Section 7.2.2.
- **Direct integration with OPM.** An agency should seek to integrate the background investigation process with the PIV card enrollment process. For example, an agency can send the fingerprints collected during enrollment to the OPM for processing. Not only can this effort reduce the redundancy of taking an applicant's fingerprints twice, it can speed up the entire credentialing process. Minimally, the fingerprints used to support a background investigation must be captured during the same enrollment session as the fingerprints for the PIV card.
- **Timely adjudication.** An agency should establish streamlined processes to adjudicate an applicant's record. If possible, an agency should automate this process so that an applicant's records are not delayed in a queue awaiting human intervention. In cases where human intervention (i.e., adjudication) is required, an agency can make a risk-based decision to issue a PIV credential based on the results of a criminal history check before the results of the completed NACI are made available.

#### Privacy Tip

Agencies are required by the Privacy Act to ensure that information in their systems is accurate, complete, and current. This obligation is applicable to the information held in systems used to perform adjudications. An agency should implement quality reviews on the information in these systems and establish a redress process for individuals to identify and remediate errors in a timely manner. Not only will these efforts help ensure compliance with the Privacy Act, but it can also improve the effectiveness of the adjudication process.



#### 8.3.1.3. Card Distribution

One area of the credentialing process that can significantly impact the time it takes for an individual to be issued a PIV card is card distribution. This process includes the steps to produce the PIV card and deliver it to the appropriate issuance location. An agency should analyze its end-to-end card distribution model to remove delays and expedite card issuance. An agency should consider the following factors to improve card distribution:

- **Printing frequency.** An agency can decrease the time it takes to issue a card to its end users by establishing a printing schedule that is appropriate for the card issuance volume and desired issuance timeline. Maintaining a regular printing schedule can help improve customer service by providing a predictable production timeline. More frequent printing may incur additional costs, which should be factored in when determining the appropriate schedule.
- **Timely shipping.** An agency can decrease the time it takes to get a card issued to end users by improving upon the shipping process. For example, an agency can have the

printing schedule aligned with the shipping schedule so that PIV cards are sent out immediately after they are created.

- **Tracking.** An agency should establish a process for tracking the creation and distribution of PIV cards. This allows the status of the PIV card to be monitored so that issues can be identified and resolved quickly to minimize the negative impact on issuance lead time and customer service.

If an agency receives card distribution services from a shared service provider, the factors discussed above will likely be determined by the provider. In this case, an agency should work closely with its shared service provider to ensure that its card distribution requirements are met.

#### **8.3.1.4. Notifications**

Although many of the activities involved in the credentialing process happen —behind the scenes,|| applicants have a few key responsibilities. In order to ensure that the PIV card is issued as soon after sponsorship as possible, applicants must be properly notified of required actions and relevant information.

- **Accurate contact information.** An agency should leverage trusted authoritative sources to ensure that the email address being entered in the system is accurate and active to ensure notifications are received.
- **Automatic emails.** An agency should automate the notification process so that emails are sent to the applicant in a timely fashion. For example, an enrollment notification should be sent to the applicant as soon as their Sponsor submits the sponsorship request, and an issuance notification should be sent to the applicant as soon as their card is available for activation.
- **Specific process information.** Applicant notifications should contain clear and concise information about the process, a description of their responsibilities (e.g., requirement to bring two forms of I-9 identity documentation, including a photo ID to enrollment), and next steps.
- **Detailed scheduling instructions.** Applicant notifications should include specific directions on how to schedule their credentialing appointment. This includes details around the enrollment/issuance location (directions, contact information, hours of operation) and what process they should follow if they are unable to keep their existing appointment. An agency should consider employing an online scheduling system that is robust and user-friendly. Effective appointment scheduling is important not only to ensure cards are issued to users in a timely fashion, but also because scheduling errors can decrease productivity and be inconvenient for those applicants who must travel to credentialing stations.

#### **Privacy Tip**

Although an agency should ensure that email notifications contain adequate information, they should take steps to minimize the Personally Identifiable Information (PII) included in email communications. If the nature of the communication requires PII to be in the email, it should be encrypted.



### 8.3.2. Printed Information

One of the goals of HSPD-12 is to establish a credential that is visually consistent across the Federal Government. FIPS 201 describes mandatory and optional printed information to achieve a common PIV card appearance while allowing an agency the flexibility to alter the card based on specific needs. On top of the direction provided in FIPS 201 and SP 800-104, agencies have had to make their own decisions around how to ensure the correct information is printed on the card, the processes for changing that information, what optional information to print on the PIV card, and how individuals get special designations printed on their credential. The following list describes some areas an agency should address in relation to the information that is printed on the PIV card.

#### Implementation Tip

The inclusion of optional data elements on the face of the PIV card should be kept to the minimal amount possible. The PIV card topography, as described in FIPS 201 and SP 800-104, provide optional data elements for agency-specific data to customize the face of the PIV card (e.g., bureau/component affiliation, clearance level, special facility privileges). Printing extra information on the card reduces privacy and introduces additional card reprinting costs due to data elements that frequently change.



#### 8.3.2.1. Leveraging Information Stored Electronically on the Card

While printed information can provide some value, most applications for the PIV card leverage the logical data elements stored on the credential. Taking advantage of the capability offered by this technology can provide a number of benefits to an agency including efficiency, reduced costs, and increased privacy. In addition to these benefits, an agency should consider the following when using information stored electronically on the PIV card:

- **Desired level of interoperability.** It is expected that an agency will perform authentication by electronic means. To that end, an agency should seek to utilize the existing logical data elements on the PIV card's chip to enhance the opportunities for interagency federation (see Section 8.4). In addition, an agency that chooses to use optional information on its PIV cards should store the data electronically instead of printing it on the face of the PIV card. These efforts allow an agency to support interoperability by securely sharing authoritative information electronically via methods such as BAE (see Section 7.3).
- **Increased privacy.** Limiting the data printed on the face of the card can prevent unintended disclosure of personal data in environments where the PIV card is required to be visibly displayed per physical security policy. Most importantly, an agency must ensure that certain sensitive information is not printed on the face of the card (e.g., Social Security Number [SSN] and date of birth [DOB]). In addition, PIV cardholders should store their PIV cards while not in use to minimize unintended exposure of printed information.
- **Cost savings.** Some of the data typically printed on the face of the PIV card (e.g., bureau/component affiliation, position or rank) are dynamic attributes that may change multiple times prior to the planned expiration date of the card. The more cardholder information that is printed on the PIV card, the greater the chance that an individual will require a new card prior to the end of their card's useful life. This increases the costs an agency spends on cardstock, printing fees, and manpower required to support the PIV

card reprinting process. On the other hand, changing information that is stored electronically requires little effort and does not result in a card reprint.

### Lesson Learned

Limiting the amount of data printed on the face of the PIV card doesn't have to impact access control decisions. When NASA first began issuing PIV cards, Center designators were printed on the cards to conform with past practices. Over time, NASA realized that the Center designator information was not necessary for making efficient access control decisions. NASA was able to reduce the need for additional card reprints by removing the Center designation as a printed field from their PIV cards.



#### 8.3.2.2. Change Process

The information printed on the face of the PIV card is subject to change due to a variety of circumstances. It is important to the integrity of an agency's ICAM program for information on the PIV card and in associated systems to be accurate and up-to-date. Therefore, agencies should establish a well-defined process for how changes are made to an individual's PIV card information. The following are some considerations around establishing an effective change process:

- **Request initiation.** An agency should determine how to initiate a request to change information printed on the PIV card. To the greatest extent possible, an agency should integrate this process with other existing processes so that updates made to information in one location automatically create a change request in the PIV system. For example, if an individual changes their last name in the payroll system, the PIV system receives a request to update the last name field.
- **Request verification.** An agency should establish a process for ensuring the validity of updated information. For example, if an agency prints rank information on their PIV card, it would be appropriate to verify an individual's request to change their credential to display a higher rank. An agency could require that change requests come from specific authoritative sources that would definitively know this information (i.e., Human Resources).
- **Enrollment requirements.** An agency should ensure that its re-issuance workflows address whether or not a cardholder must complete the entire identity proofing and registration process as a result of a change request. No re-enrollment is required if the cardholder can be reconnected to the chain-of-trust record by performing a 1:1 biometric match against the biometric reference data on the card. The entire identity proofing and registration process must be completed if the cardholder cannot be matched to his/her chain-of-trust record.

#### 8.3.2.3. Name

FIPS 201 states that the full name should be printed on the PIV card. At issuance, the PIV Issuer (or an authorized delegate) validates that the name on the source identity document matches the picture and name on the new PIV credential being personalized. As such, it is important that an agency establish clear policies and procedures to ensure that the name on the credential is accurate and consistent with identity source documents. The following are some considerations around the name that is printed on the PIV card:

- **Full name.** FIPS 201 requires that the full name be printed on the PIV card and be composed of a Primary Identifier (i.e., surname or family name) and a Secondary Identifier (i.e., pre-name or given name). When establishing policies and procedures around the name that appears on the PIV card, an agency should consider the effect that the naming convention will have on other systems and processes. For example, the name that is used in the applicant’s PIV record may be used to initiate a background investigation and should therefore be consistent with the applicant’s legal name. An agency should also establish a standardized approach for abbreviating conventional prefixes and using other special symbols in names (e.g., apostrophes and hyphens). In addition, when determining the approach for printing names that exceeds the allotted name space, an agency should be mindful of the fact that many individuals are sensitive to the way their names appear on the PIV card.
- **Nicknames and pseudonyms.** Some individuals may prefer or need to have a name printed on their PIV card that is different from the name they were given at birth. Although the use of nicknames is not discussed in FIPS 201, agencies should establish policies and procedures to address nicknames being printed on an individual’s PIV card that adhere to the intent and integrity of HSPD-12. For example, an agency may consider requiring that an individual provide identity documentation that reflects their preferred name and meets the identity proofing requirements of the PIV card. For those individuals who have been authorized to use a pseudonym, the agency should issue a PIV card reflecting this name only after the individual has provided evidence that the pseudonym is authorized by the agency.
- **Inconsistent identity information.** Some identity documents for the same individual might have different name information. For example, an individual might be Joseph John Smith, JR on one identity document and Joe J. Smith on another. An agency should establish policies for accepting and verifying name information that varies from one identity document to the other, independent of how slight the difference.
- **Name changes.** There are a number of reasons an individual might need to change the name on record in the PIV system. One common reason an individual might need to change their name on the PIV card is due to changes in marital status. In this case, the individual must provide evidence of a formal name change (e.g., marriage certificate, divorce decree, judicial recognition of a name change) and re-enroll to receive a new PIV card that reflects the attribute change.

#### **8.3.2.4. Special Designations**

The PIV card topography as described in FIPS 201 provides space for special designations of an individual to be printed on the face of the card. Some examples of these designations include Federal Emergency Response Official (F/ERO), access privileges (e.g., 24 hour access), and authorization to carry special equipment (e.g., weapons).

## Terminology

**Federal Emergency Response Official (F/ERO)** – is a federal employee or contractor who is responsible for the execution of the National Response Framework (NRF), National Infrastructure Protection Plan (NIPP), National Continuity Policy Implementation Plan (NCPIP), and/or National Incident Management System (NIMS). These Emergency Responders are those employees who are designated to restore and/or maintain continuity of operations after a disaster. The requirements and restrictions for Emergency Responders are typically included in agency continuity plans and this designation is indicated on the individual's PIV card by a red stripe at the bottom front of the card.



The following are some considerations around printing special designations on an individual's PIV card:

- **Validation of special designations.** An agency should be moving towards electronic validation of the PIV card data elements, wherever possible. However, the PIV card data model does not include a corresponding digital element for special designations, which makes electronic validation unavailable. An agency should take this into account when assigning special designations and take steps to ensure these attributes are properly validated before granting access. In some cases an agency may be able to leverage an existing BAE to obtain and electronically validate attributes from authoritative sources in order to make access control decisions and for provisioning user access, as discussed in Appendix I.
- **Standardized approval process.** An agency should establish clear and well-defined processes for assigning and authorizing individuals to be assigned special designations. How is the request initiated? Who approves the request? What, if any, documentation is required? What qualifications and/or certifications should be required of the individual? Is there a renewal requirement for qualifications and certifications? Are there any populations that are exempt from this designation? How can registration officials verify the applicant's special designation request?
- **Special designation repository.** An agency should create an authoritative source that maintains the information of individuals with special designations within their agency. This repository should be one of the authoritative sources that populate sponsorship information so that the appropriate individuals are identified as requiring special designations. In particular, an agency has the responsibility to link their inventory of F/ERO identity and attributes (qualifications, authorizations, certifications, and/or privileges) with FEMA's F/ERO database.<sup>157</sup> FEMA's system has the capability to support electronic validation of F/EROS which strengthens the decision process for entry into incident scenes, allows for expedited entry and exit from the scenes, and provides secure electronic records of those who respond to emergencies.
- **Standardized revocation process.** An agency should establish clear and well-defined processes for revoking an individual's special designation. What circumstances require the designation to be removed? Who is accountable for revoking the designations?

<sup>157</sup> In response to Title IV of [Public Law \(PL\) 110-53](#), —Implementing Recommendations of the 9/11 Commission Act of 2007,|| FEMA established an F/ERO database that links with agency HSPD-12 and local emergency response systems to be the authoritative source of responder identities and attributes.

### 8.3.3. Administrator Access Privileges

There are individuals who, because of the role they hold within their agency, require special network privileges (e.g., system and database administrators). Typically, these individuals will be assigned an administrator account in addition to their basic user account, which allows them to have heightened access to the agency's network and resources. Because of the security implications associated with privileged access, these users are encouraged to minimize the amount of time they spend logged onto agency networks with their administrative accounts. As a result, these users often move between their basic and administrative account multiple times in one session. HSPD-12 requires use of the PIV card to authenticate to logical resources; however, certain versions of operating systems commonly used within the Federal Government have technical limitations that do not allow multiple network accounts to be mapped to a single PIV card.

In the ICAM target state, all users will authenticate to logical resources using one PIV card; however, it is anticipated that there will be a transition period as an agency works to get all systems modernized to meet the target state requirements. Due to the sensitivity of the access of these user types, it is recommended that an agency take deliberate action during this transition, which includes the following activities:

- **Migrate to technologies that support PIV-enablement for administrator accounts.** Currently, there are versions of several vendor products available that allow multiple user accounts to be associated to a single PIV card. Where these vendor products are in use, an agency should plan for and execute migration to the upgraded version.
- **Work with product vendors to include necessary functionality into future product versions.** Where current operating systems and vendor products do not support the use of a single PIV card for multiple user accounts, an agency should work with their vendors to ensure that this functionality is incorporated into future versions of their product. Driving vendors to incorporate the necessary capabilities will allow an agency to move towards the target state in a timely manner without having to replace existing investments.
- **Use secure credentials throughout the transition.** As an agency migrates toward these new vendor products, they will face a transitional period. An agency in the transition period must still meet applicable requirements based on the system's security categorization and level of assurance. One option for meeting these requirements is issuing a second credential to administrators that leverages the PIV infrastructure.<sup>158</sup> While this approach introduces additional credential issuance and maintenance costs for these users, it satisfies the target state objective of using the PIV card for logical access. Where an agency has another token infrastructure (e.g., USB, one-time password tokens) already in operation, it would be acceptable to continue using these technologies until the migration is completed; however, an agency should not stand up a new alternative credential infrastructure if one is not already in place.

---

<sup>158</sup> See Section 8.1.2 for more information around the PIV-Icard.

## FAQ

### Can my agency issue username and password credentials for authenticating to administrator accounts?

No, this is not considered a viable transition approach. This approach is not consistent with current policy,<sup>159</sup> which requires use of a PIV card for authentication to logical access control systems (LACS). Additionally, username and password does not provide sufficient identity assurance for the types of transactions performed by privileged users.



## 8.3.4. Reasonable Accommodations

There are individuals who, due to physical disabilities or limitations, may need special accommodations to assist them during the credentialing process and to support ongoing PIV card usage. Many of the PIV card challenges experienced by individuals with physical limitations can be addressed through an agency's compliance with Section 508,<sup>160</sup> an amendment to the Rehabilitation Act of 1973, which requires that federal agencies' electronic and information technology is accessible to people with disabilities. In addition to meeting the requirements of Section 508, the following subsections describe some of the areas that an agency should address to alleviate the physical challenges associated with PIV usage that some individuals within their user population may face.

### 8.3.4.1. Biometric Collection

A key component of the enrollment process is the collection of biometrics in the form of fingerprints and a photo. There are certain circumstances in which a registration official is unable to capture fingerprints because of availability or quality. Additionally, certain disabilities may prevent an individual from achieving or maintaining the physical positions required to capture fingerprints or the photo. The following are some considerations around addressing challenges of biometric collection:

- **Reasonable accommodations officials.** An agency should consider involving these individuals in the development and improvement of the agency's credentialing process. They can help identify additional requirements and accommodations that might need to be in place for those with physical challenges.
- **Training.** It is recommended that registration officials take disability awareness and sensitivity training.<sup>161</sup> This training should prepare registration officials to handle the needs of physically challenged individuals during the biometric collection process in order to ensure that the process is comfortable and clear to the individual.
- **Equipment modification.** An agency should make sure that, to the greatest extent possible, equipment is mounted in a way that the person is able to maneuver it to facilitate the biometric collection. For example, if a person is unable to move into a particular position for the photo capture, the camera should be able to be moved to varying positions to compensate.

<sup>159</sup> [M-11-11](#)

<sup>160</sup> For additional information, visit the [Section 508 website](#).

<sup>161</sup> Government-wide disability and sensitivity awareness training is provided through the [United States Access Board](#).

- **Alternative biometrics.** An agency should standardize a process for handling applicants who do not have viable fingerprint biometrics. This process should be in accordance with the FIPS 201 and SP 800-76 documents.<sup>162</sup>
- **Adjudication of records without fingerprints.** An agency should consult OPM, the Suitability Executive Agent, for established policies and procedures related to determining the suitability of an individual that does not have usable fingerprints.
- **Visual information.** An agency should provide an audio option for items during enrollment or issuance that need to be read. For example, the user agreement signed as part of issuance should be read out loud for visually-impaired applicants.

#### Implementation Tip

Be proactive in making schedule accommodations for individuals with physical challenges. For example, an agency can create flexibility in their PIV card schedules to allow more time for those who need special accommodations. An agency with online scheduling systems can include an option for an individual to request an accommodation. This could alert the system to automatically schedule a longer session.



#### 8.3.4.2. Card Usage

Once an applicant has been issued their PIV card, the requirement is to use the credential to access physical and logical resources. Individuals with physical disabilities may face some challenges when using the credential for these applications. An agency should take special care to understand these obstacles and make accommodations to assist these individuals. The following are some considerations around addressing physical challenges of PIV card usage.

- **Physical card usage.** Applications that use the contact interface of the PIV card require that the card be entered into the reader chip-end first and with the front side of the card facing upwards. For individuals with certain physical disabilities, determining which end of the card contains the chip and which side of the card is the front can be difficult.<sup>163</sup> Potential accommodations in this situation could include additional training, specially-designed equipment, or designation of an assistant to help with PIV card use.
- **Colors identifiers.** An agency has the option to use Zone 18, Affiliation Color Code, to assist individuals who are colorblind. When exercised, the affiliation color code —B| for Blue (Foreign Nationals) or —G| for Green (Contractor) shall be printed in a white circle in Zone 15.<sup>164</sup>
- **Visual usage instructions.** Individuals with impaired vision will have challenges reading the instructions for PIV use that appear on their computer screen. For instance, after the PIV card is inserted, there will be a prompt for the user to input their PIN. Agencies should provide accommodations for these individuals, such as screen reader software.

<sup>162</sup> NIST is in the process of updating the [FIPS 201](#) and [SP 800-76](#) documents to reflect how agencies should handle alternate biometric modalities for PIV users lacking usable fingerprints. The FICAM Roadmap and Implementation Guidance will be updated when these revisions are published.

<sup>163</sup> It is anticipated that the [FIPS 201](#) revision will address methods by which proper card orientation can be correctly detected by touch.

<sup>164</sup> [SP 800-104](#), Scheme for PIV Visual Card Topography, NIST, June 2007.

### 8.3.5. PIV Card Management

Throughout the life of a PIV card, there will be various situations that affect the card's status. An agency should establish streamlined processes and provide clear guidelines to cardholders so that the status of the card is up-to-date in systems. Failure to do so could have serious security implications. For example, if an on-site contractor's project has come to an end and their PIV card is not collected, then the individual could use the PIV card to gain unauthorized access to facilities and networks until the card reaches its expiration date. The following list describes some of the areas an agency should address in relation to PIV card management as they seek to fully leverage PIV and PIV I-credentials.

#### 8.3.5.1. Termination

The final step in the PIV card lifecycle is termination of the PIV card. The PIV card must be relinquished upon ending employment or affiliation with the agency, for whatever reason. Automation can improve an agency's ability to terminate access privileges in a timely fashion. However, it is essential that an agency properly manage this process so that credentials do not remain in the hands of individuals no longer associated with the agency. The following are considerations around addressing PIV card termination as it relates to PIV card management:

- **Streamlining termination.** An agency should create streamlined processes for terminating an individual's record in the PIV system. This process, to the greatest extent possible, should be integrated with other HR processes so that a termination in other systems voids the record in the PIV system. It is important to note that terminations in other systems do not always require an action to terminate the record in the PIV system. For example, if an individual changes roles and no longer requires access to a particular job-related system, this would not require their PIV card to be terminated in the PIV system. When terminating a PIV record, cardholder information is only to be retained for the duration required per National Archives and Records Administration (NARA) General Records Schedules.<sup>165</sup>
- **De-provisioning access.** An agency should integrate processes such that the termination of a PIV card automatically updates other systems and removes the individual's access to physical and logical resources. An agency should thoroughly examine workflows of automatic provisioning in systems to ensure that records are properly removed from only appropriate systems. For example, if a PIV card is terminated due to an individual moving to a different bureau within an agency, the individual's record may not need to be voided in all systems.
- **Card collection.** An agency should require that card collection be included as a key step of the out-processing performed on the last day of employment. A specific individual should have accountability for ensuring that this action is completed and a process should be established for situations in which the card is not collected.

---

<sup>165</sup> For more information see the NARA General Records Schedules [website](#).

### Privacy Tip

An agency should have processes in place so cardholders can address incorrect/inadvertent termination or changes in access. Redress is a necessary consideration when discussing lifecycle issues such as termination and access rights.



#### 8.3.5.2. Certificate Expiration

Per FIPS 201 and the Common Policy, PIV cards are valid up to a maximum of five years and the certificates on the PIV card are valid up to a maximum of three years. This means that new certificates may need to be obtained prior to card expiration. The following are considerations around addressing certificate expiration as it relates to PIV card management:

- **Timing of expiration.** An agency should perform a cost/benefit analysis to make decisions on when to update certificates. An agency might find value in a certificate expiration date that is earlier than the maximum three years or in requiring that the PIV card and certificate expiration dates match.
- **Card holder training.** A majority of the cardholder population may be unfamiliar with the concept of digital certificates. This lack of understanding can create challenges for the end user when their certificates expire. An agency should provide adequate training to PIV cardholders so that they are aware of the digital certificates on their card, the fact that they will expire, and that they will need to take action to update the certificates.
- **Notification of certificate expiration.** An agency should establish an automatic system that sends email notifications to cardholders before their certificates are going to expire at scheduled renewal times (90, 60, or 30 days). These emails should include information on the process they should follow to update their certificates and what will happen if they do not update their certificates before the expiration date.
- **Certificate update method.** The certificate renewal process can be performed by the user from a desktop through a secure self-service portal or the agency may choose to issue new PIV cards before the card's expiration date.
- **Key recovery.** Once a PIV card holder's certificates have expired, he/she will be unable to access emails and files that were encrypted with their previous certificates. As suggested in SP 800-73,<sup>166</sup> an agency should strongly consider the option of loading retired key management key(s) onto the PIV card. This allows for the decryption of data that have been previously encrypted with active/valid keys, but which are now retired, by storing the corresponding certificates on the PIV card application or an online repository. SP 800-73 allows a maximum of 20 retired key management keys.

### ROI

Setting the PIV card's expiration date to the maximum allowable time period is not necessarily the most cost effective approach. After performing a cost analysis, the Social Security Administration (SSA) decided to synchronize the card expiration with the certificate expiration at three years. This will save SSA \$68 per card over a ten year cycle, as many cards need to be replaced due to data changes or wear and tear before their expiration date.



<sup>166</sup> [SP 800-73](#)

### 8.3.5.3. PIV Card Unavailability

There may be circumstances that affect the availability of a PIV card to its cardholder, including PIV cards that have been forgotten, lost, stolen, or damaged. As agencies move toward fully leveraging PIV credentials, it becomes increasingly imperative to have solutions to address these events. An agency should establish policies and procedures to minimize the frequency of these circumstances as well as adequately handle the adverse impact to the cardholder when they do occur. The following are considerations around addressing PIV card unavailability as it relates to PIV card management:

- **End-user training.** Many cardholders may not understand the nuances of the PIV card and the associated expenses. An agency should take the necessary steps to educate their user population on what makes the PIV card different from legacy identification cards; the impact of forgetting, losing, or damaging the card; and proper handling instructions. For example, cardholders should be instructed to keep their PIV card in its protective sleeve when not in use to prevent damage and unintended exposure of the individual's information.
- **Reporting processes.** An agency should establish a streamlined process for reporting cards that are forgotten, lost, stolen, or damaged. This process should follow OMB guidance on reporting breaches of Personally Identifiable Information (PII),<sup>167</sup> clearly identify the appropriate points of contact, and be publicized and well-known to both cardholders and PIV process role holders. In addition, there should be automation in the process of suspending or disabling the PIV card once the responsible party reports the change in status.
- **Temporary access.** An agency should create policies and processes for obtaining temporary access to physical and logical resources when a PIV card is reported as forgotten, lost, stolen, or damaged. The policy should include an established length of time that the individual can maintain this temporary access, and access should be automatically revoked after the specified time period. Likewise, cardholders should be aware that this process is acceptable only as a temporary alternative in special circumstances, not as an alternative to using their PIV card.
- **PIV card replacement.** An agency should standardize the process for obtaining a replacement card if the original PIV card is lost or stolen. Decisions should be made around whether a reprint should be ordered for the unavailable PIV card or if the individual should re-enroll.<sup>168</sup>

### 8.3.5.4. Algorithm and Key Migration

PIV card management requires support for key management and the migration of cryptographic algorithms and key lengths over time. These migrations are typically triggered as a result of known or potential algorithm breaks or the availability of more powerful computing techniques that could compromise the keys. Due to the reliance on cryptographic keys to perform authentication, an agency must adequately plan for key migrations to ensure that the ability of agency applications to validate the PIV card is not affected. NIST SP 800-78 and SP 800-

---

<sup>167</sup> Contact your privacy office if you are unsure about OMB reporting requirements.

<sup>168</sup> The current revision process of [FIPS 201](#) is expected to address PIV card replacement.

131A<sup>169</sup> specify approved algorithms and key lengths to achieve a particular security strength and the time frames during which the algorithms and key lengths are considered acceptable for use. An agency should refer to this guidance to identify and plan for future algorithm and key length migrations.

### Implementation Tip

An agency should carefully evaluate the potential limitations associated with maintaining legacy public key infrastructures when planning for future algorithm and key length migrations. Maintaining a legacy infrastructure may be more costly than fully migrating and may limit interoperability with organizations that no longer operate a legacy infrastructure.



The transition from SHA-1 to SHA-256<sup>170</sup> for generating and verifying digital signatures is an excellent case study in the need for an agency to have established plans for migration to stronger algorithm technology as required for security reasons. Per the requirements in SP 800-78 and SP 800-131A, SHA-1 was designated for acceptable use through the end of 2010; however, many agencies were not prepared for the transition.

As a result, NIST and the Federal PKI Policy Authority<sup>171</sup> (FPKIPA) worked to develop an adapted transition plan and interim infrastructure support to ease the transition to SHA-256 over a longer period of time. The main goal of the transition is to maintain interoperability with limited security risk to ensure the federal community is able to transition to SHA-256 without unnecessary disruption in service to subscribers. The following list includes some of the key components of the transition plan developed by the FPKIPA to ease the transition for an agency:

- Continued operation of the current Federal Bridge Certification Authority (FBCA) and Common Policy CAs, which ran through March 31, 2011 in order to maintain support during the transition to the new SHA infrastructure,
- Creation of a parallel SHA-1 infrastructure (SHA-1 Federal Root Certification Authority [FRCA]) within the FPKI to be operational during the transition period that will issue SHA-1 cross-certificates under differentiated Object Identifiers (OID), and
- Changes to the FPKI Certificate Policies that allow the use of SHA-1 to sign revocation information for certificates issued before 12/31/2010, to define the SHA-1 differentiated OIDs, and to allow SHA-1 for signing revocation information for SHA-1 certificates until 12/31/2013.

The Federal Government is beginning to plan for the transition to new algorithm technology that is more difficult to break than existing algorithms. An example of a future algorithm that is being considered is Elliptic Curve Cryptography (ECC), which would require the transition of one or more of the PIV keys to elliptic curve keys.

<sup>169</sup> [SP 800-131A](#), Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, NIST, January 2011.  
[SP 800-131A]

<sup>170</sup> Detailed requirements and lessons learned associated with this transition can be found in [SHA-256 Transition Lessons Learned, Federal Public Key Infrastructure Policy Authority, Version 1.0, May 21, 2011](#).

<sup>171</sup> The [FPKIPA](#) is an 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.

## Terminology

**Elliptic Curve Cryptography (ECC)** – An approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. This algorithm technology can provide exponentially stronger security with a smaller bit size than current algorithms in use (e.g., SHA-256).



To be well-prepared for this and other future algorithm and key migrations, an agency should consider the following:

- **Effective life cycle management.**<sup>172</sup> An agency should actively maintain awareness of upcoming requirements and incorporate plans for migration into existing lifecycle processes. Being proactive and agile allows an agency to accommodate changes without disrupting current process flows and systems. Additionally, planning in steps to accommodate migration early gives an agency the opportunity to build in new requirements and ample time for testing to ensure proper functionality.
- **Subject matter experts.** An agency’s transition plan should include the establishment and coordination of personnel who are knowledgeable in the technologies that support the PIV and PIV-I infrastructure. For example, in order to understand changes in key length and strength, there needs to be people with expertise in PKI. Subject matter experts should have a vested interest in keeping up with changing technology and evaluating how those changes might impact agency applications.
- **Inventory of PIV-enabled applications.** An agency’s transition plan should describe a streamlined process to inventory existing applications that use certificates for authentication, digital signature, and/or encryption. As a part of this inventory process, there should be ways to determine which applications are at risk of being unable to process the new algorithm technology by working with vendors/manufacturers.
- **Testing support.** An agency’s transition plan should include a test plan for all PKI/PIV-enabled applications. An agency should request test CA certificates that are signed with the new algorithm technology to determine each application’s capability to accept PIV certificates and CRLs and process data that is signed with the new algorithm technology and produce signatures with the new algorithm technology.
- **Scope of change.** An agency should also consider the scope of the change in terms of the impact to PIV-enabled applications. The change might have a vast effect or the scope may be more contained. For example, in the case of SHA-2, the fact that a PKI may issue SHA-2 signed validation data (e.g., CRLs) could immediately impact an application’s ability to validate all existing SHA-1 certificates throughout the agency because not all objects in the chain are at SHA-1.
- **Report results.** An agency’s transition plan should describe which parties need to be aware of the test results and what actions need to be taken to address the report findings. The testing results can be shared and leveraged across the agency to support synergy and help enable a successful transition.
- **Communication.** An agency’s transition plan should include a detailed process to communicate important information, such as dependencies and impacts from other

<sup>172</sup> See [M-10-15](#), FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, OMB, April 21, 2010 for information. [M-10-15]

technology deployments, test results, and next steps across the bureaus/components. Timing is also an important factor in communications. For example, bureaus/components with PIV-enabled applications should be informed of cryptographic changes and the impacts of transition timelines to operations well in advance of their implementation.

- **Vendor support.** An agency should involve vendors early and often and have advance awareness of the capability of its vendors to deliver new solutions that are technically compliant with upcoming changes. An agency may not be able to control a vendor's release schedule for fixes, which could extend beyond the time needed to configure, test and implement.

#### Lesson Learned

Timing is everything. An agency planning to test infrastructure in response to an upcoming technology change need to understand the necessary tools and resources and how long it will take to get them. For example, the time it takes to get test cards from vendors has a significant impact on the time it takes to perform the appropriate tests, configure the applications, and release the fix into production.



#### 8.4. Interagency Federation Using the PIV Card

Across the Federal Government, agencies and their users often have the need to access resources and information systems owned and managed by another agency. In the past, providing access to another agency's users has been accompanied by the issuance of separate credentials that are managed by the organization that owns the application/data. However, the process for accomplishing this is streamlined in the ICAM target state, as discussed in Section 4.10, through government-wide standardization on use of the PIV card as the common credential for the federal workforce. Government-wide PIV implementation provides agencies with a common trust and technology infrastructure that can be used to trust digital identities and authenticate PIV cards that have been created and issued by another agency.

#### Implementation Tip

To meet the intent of HSPD-12, agencies must consider the need for interoperability when designing and implementing PIV infrastructure. An agency may customize aspects of its PIV program to suit its specific needs; however, complex customization can inhibit PIV interoperability across agency boundaries. As such, the need to authenticate another agency's users and enable another agency to authenticate your users should be paramount during the design process.



Use of the PIV across agency boundaries, referred to as interagency federation, is required by the policies related to the implementation of HSPD-12<sup>173</sup> to minimize the redundant collection of identity data and issuance of alternative credentials. The commonality provided by the PIV infrastructure allows an agency to trust a user from another agency either by directly authenticating his PIV using the mechanisms discussed in Section 8.2.2 or choosing to accept an authentication performed by another agency and consuming an identity assertion (e.g., SAML).

<sup>173</sup> M-11-11

## FAQ

### How does interagency federation differ from external (G2G, G2B, G2C) federations?

Interagency federation occurs within the Federal Government for PIV cardholders while external federations include other individuals who will not be issued a PIV card and have some other means of authentication. Within interagency federation, trust is inherent due to the policies, processes, and technical standards that exist as part of the PIV infrastructure. Additional information and guidance with regard to external federation can be found in Chapter 12.



The information presented in this section is intended to assist an agency in providing answers to several common interagency federation questions, including:

- What are the most common scenarios in which my agency will need to trust and grant access to a user from another agency?
- What should my agency consider when preparing to accept another agency's PIV cards or identity assertions?

#### 8.4.1. Common Scenarios for Interagency Federation

The justification for granting access to another agency's users is based primarily on the agency's mission and business function and the services that it provides. The following list describes the primary scenarios that may require federated access within the Federal Government:

- **Applications that service the government-wide community.** Within the Federal Government, there are a number of applications that provide an array of services to federal users. This includes applications that serve as information sharing and knowledge repositories (e.g., OMB's Max.gov site) as well as those that provide human resources and personnel security services and information (e.g., Employee Express, CVS, etc.).
- **Shared/managed service provider applications.** Similar to applications that serve the government-wide community, shared and managed services typically provide support to subscriber agencies and have smaller external user bases than government-wide applications.
- **Applications that support specific mission or business functions.** Includes applications with users from two or more agencies that share a common mission or business goal and have a need to share or exchange related information (e.g., law enforcement).

#### 8.4.2. Implementation Considerations

Enabling an agency's applications to trust another agency's credentials is an undertaking that requires planning, support, and coordination from various groups within an agency and with the agency's external partners. Chapter 12 discusses these efforts in the context of federation with parties external to the Federal Government; however, many of those considerations apply to interagency federation (e.g., management of data for external users, provisioning, de-provisioning, federation agreements). The following list describes the planning and coordination considerations that apply specifically to interagency federation:

- **Trust basis for PIV cards.** The common standards and policies related to HSPD-12 establish the basis for trust in PIV cards and the digital identities to which they have been

bound.<sup>174</sup> This common trust fabric simplifies the processes and burden associated with establishing a trusted relationship with another agency; however, an agency should confirm that its agency partners are currently compliant with established policies and technical specifications when establishing federation relationships.

- **Determine the appropriate authentication method.** For each interagency federation scenario, an agency will need to grant access to another agency's users based on the authentication of the PIV card or the information in an identity assertion sent by that agency. The approach an agency takes is based on the specific business scenario, the application the agency is trying to grant access to, and the available infrastructure. For example, an application may be configured for assertion-based federation. In this situation, it may be more advantageous for the application to federate the user with an assertion derived from the authentication of the user's PIV card rather than directly authenticating the PIV card.
- **Determine additional information requirements to grant access.** The PIV card allows for a level of trust in the identity and validity of the user. However, the information on the PIV often is not enough to make an access decision. Therefore, an agency should determine what additional information, if any, is needed to support its access control scenarios to properly grant access to users from another agency. Further discussion around access control policies can be found in Section 9.3.

## **8.5. Value-added Applications**

In addition to the required use of the PIV card for physical and logical access, an agency may be able to achieve a greater return on the investment they have made in their PIV infrastructures by leveraging the card for additional uses.<sup>175</sup> In particular, Use Case 11 of the ICAM segment architecture (see Section 4.11) promotes the use of the PIV, and in extension, PIV-I, card for encryption and digital signature. Agencies may wish to use the PIV for additional value-added applications; however, these types of applications are out of scope for this guidance. If an agency chooses to pursue adding other value added applications to its PIV card, it is important to ensure that such implementations do not invalidate the FIPS 140 and FIPS 201 certifications, which could compromise use of the PIV card for required access applications.

The information in this section provides guidance to assist an agency in providing answers to several common questions around value-added applications, including:

- How can my agency use the encryption capabilities that are available on my PIV card to secure data?
- When should my agency leverage digital signature capabilities to automate approval workflows that are available today?

### **8.5.1. Encryption**

In the target state, the PIV and PIV-I card will be used as the PKI source for encryption and as such, an agency should establish policies and procedures that support their users in uniformly

---

<sup>174</sup> More information around trust in the card issuance process can be found in [SP 800-79](#).

<sup>175</sup> A detailed security checklist for the PIV card can be found at [M-06-16](#), Protection of Sensitive Agency Information, OMB, June 23, 2006. [M-06-16]

applying encryption to secure documents and communications.<sup>176</sup> Using the PIV and PIV-I card for encryption provides an agency with not only the opportunity to get more value out of their investment of the PIV and PIV-I card, but also increase security and privacy and reduce costs associated with unauthorized access to data. The following list includes some considerations around using encryption as a way to get more value out of the PIV and PIV-I card.

- **Policy and guidelines.** If an agency is going to get more value out of their investment in the PIV card by using it for encryption, they need to establish appropriate policies and guidelines to reflect this intent. These policies and guidelines should be well-communicated to the user population and compliance should be monitored. Furthermore, before an agency moves forward with initiatives to encrypt with PIV or PIV-I, there should be a plan in place for key histories and a method for delivering old encryption keys to end-users, as discussed in Section 8.3.5.2.
- **When to encrypt data.** Although encryption is a successful way to secure information, not all documents and emails need to be encrypted. If every user encrypted every transmission of information, the agency's network would be inundated. An agency promoting encryption should provide users with guidance and policy around which type of information requires encryption, based on risk. Furthermore, there are some situations that prohibit the use of encryption. For example, NARA does not allow federal permanent records to be encrypted at time of transfer of legal custody to NARA.
- **Controlled Unclassified Information (CUI).** An agency should include in their policy the processes and storage requirements of CUI, which prohibit disclosure to and modification by unauthorized internal and external parties. An agency must store and protect CUI in accordance with E.O. 13556.<sup>177</sup> The encryption capabilities provided as part of the PIV credential enable an agency to meet the data protection requirements of E.O. 13556. An agency should develop internal policies and guidance to address the use of PIV-based encryption.

### 8.5.2. Digital Signatures

In the target state, the PIV and PIV-I card will be used as the PKI source for digital signatures and as such, an agency should establish policies and procedures that support their users in uniformly applying digital signatures to secure documents and communications. Digital signatures can help an agency streamline business processes and transition manual processes to more automated online transactions. Additionally, digital signatures can provide mitigation for a variety of security vulnerabilities, such as phishing, by providing authentication, non repudiation, and integrity. The following list includes some considerations around using digital signatures as a way to get more value out of the PIV and PIV-I card.<sup>178</sup>

---

<sup>176</sup> Encryption guidelines are discussed in [M-06-16](#) and [M-07-16](#).

<sup>177</sup> [E.O 13556](#), Controlled Unclassified Information, The White House, November 4, 2010.

<sup>178</sup> For more information, see SP 800-25, Federal Agency Use of Public Key Technology for Digital Signatures and Authentication, NIST, October 2000.

ROI	
Implementing digital signatures to convert paper-based approval forms into electronic can help an agency achieve significant cost savings. An estimated 40 percent of the costs of bringing a new drug to market are related to paper-based approval processes. This was one of the drivers behind the National Cancer Institute partnering with a global biopharmaceutical company to enable digital signatures on electronic documents. This effort is estimated to save the National Cancer Institute more than \$48,000 per 100 users annually and dramatically reduce the cost of clinical trials in the pharmaceutical industry.	

- **Government Paperwork Elimination Act (GPEA).**<sup>179</sup> The GPEA requires that, when practicable, federal agencies use electronic forms, electronic filing, and electronic signatures to conduct official business with the public. It also states that electronic documents and signatures should not be treated less favorably than paper electronic documents and signatures or denied legal effect, validity, or enforceability. The GPEA recognizes digital signatures as one of the valid forms of electronic signatures and strongly encourages its acceptance by federal agencies.
- **Determine appropriateness of digital signature.** Not all documents and transactions require a digital signature. To evaluate the suitability of electronic signature alternatives for a particular application, an agency must perform both a risk-based and cost-benefit analysis. The goals of the assessment are to determine whether an electronic signature solution is appropriate to supplement or replace an existing paper-based process, and if so, to identify the particular technologies, practices, and management controls best suited to minimize the risk and cost to acceptable levels while maximizing the benefits to the parties involved.
- **Support for background investigation processing.** An agency should consider leveraging digital signatures to streamline and improve the security and efficiency of the background investigation initiation process, as discussed in Section 7.2.2.
- **Establish supporting policies and guidance.** An agency should consider creating a policy around the use of digital signatures. For example, an agency might require that all emails sent from an agency-owned system or account, which contains an embedded hyperlink and/or attachment, use digital signatures. The policy should also include guidelines for acceptance of digital signatures from other entities.

Implementation Tip	
An agency should address the appropriate use of PIN caching in its agency-level policy related to digital signature. <sup>180</sup> In some situations (e.g., bulk signing of email messages), it is impractical for the user to input his PIN for each digital signature, and PIN caching may be appropriate with associated compensating controls. In order to preserve the value of PIN entry as a security control, the card-accepting device should only supply cached PINs for authorized, local use; PINs may only be entered, cached, and supplied under the supervision of the cardholder; and/or cached PIN entries should be cleared after a specified time period.	

<sup>179</sup> For more information see the [GPEA](#).

<sup>180</sup> The agency decision regarding PIN caching applies to the Digital Signature Key in support of signing functions. This excludes caching for other purposes such as access control (e.g., PACS).

- **Provide training for users.** An agency should educate their user population around how to identify transactions that require digital signatures and how to properly digitally sign documents and emails.
- **Determine process and system capability.** An agency should take appropriate action to ensure that business processes and systems relying on digital signatures are capable of gathering, retaining, and making available pertinent transactional information, such as date and time, identity, and location.
- **Identify processes that could leverage timestamps.** Digital signatures provide the added benefit of including a timestamp on digitally signed data that can be used to identify when something was signed with a high level of accuracy. An agency should identify which processes could benefit from or leverage timestamps and implement digital signatures, as appropriate.

**FAQ**

**What is the difference between an electronic signature and a digital signature?**

“Electronic signature” is the term used in all of the E-Transaction Laws. It is a generic, technology-neutral term that refers to the universe of all of the various methods by which one can “sign” an electronic record. “Digital signature,” on the other hand, is a term for a technology-specific process often used to authenticate identity and/or to verify the integrity of electronic records by mapping the digital signature back to digital certificates (PKI). The term “digital signature” is not used in the E-Transaction Laws.



## 9. Access Control Convergence

Physical and logical access control are intended to allow entry to or use of resources to authorized users and entities based on an established set of rules that define appropriate access permissions. Access control convergence refers to the common processes and technologies that enable both physical and logical access control. As described in the target state of the ICAM segment architecture, agencies should be moving toward providing access control services at the enterprise level, which in turn necessitates the convergence of many physical and logical access management activities and business processes. Enabling enterprise access control requires management of information about the resources being protected, the users attempting to access those resources, and the policies governing access control decisions. Improvement in these process areas, as discussed in the following subsections, supports achievement of the target state and enables more effective interoperability and information sharing.

Chapters 10 and 11, which address the modernization of PACS and LACS respectively, address specific implementation considerations for many of the topics discussed throughout this chapter in the context of the technical solutions and systems.

### 9.1. Resource Attribute Management

Resource Attribute/Metadata Management, as defined in the ICAM Services Framework, is the process for establishing and maintaining data (such as rules for access, credential requirements, etc.) for a resource/asset. This data defines the access, protection, and handling controls for a resource. Resources may be both physical (campus sites, buildings, individual offices/areas, etc.) or logical (IT applications, data, services, etc.). The information and guidance presented in this section is intended to assist agencies in providing answers to several common resource management questions, including:

- Where might I find information about the resources within my agency that must be protected?
- Where can I find lists of these resources and information about them?
- How can resources be organized or grouped to streamline access control for users that require access to a set of common resources?

FAQ	Isn't resource management the management of supplies, hardware, software, and other personal property?	?
No, not in the context of ICAM. Agencies are responsible for managing numerous types of resources, assets, and property under their custody. Within the context of ICAM, however, resource management refers specifically to managing information about resources that require access control. Some agencies also call this process asset management.		?

#### 9.1.1. Resource Discovery and Inventory

When implementing access control solutions, an agency should maintain a complete inventory of all resources that need to be protected (both physical and logical). This may require aggregating information from multiple existing resource inventories because the processes used to identify, track, and catalog resources are often distributed across multiple programs and systems within an agency. Each program or system typically collects and manages information about a subset of

the agency’s resources in order to support a specific business function. For example, agencies are required under FISMA to have a complete, current inventory of IT systems. ICAM implementers must be able to retrieve information about these resources quickly and efficiently in order to effectively manage access to them in a coordinated fashion. Additionally, physical and logical resources typically are managed separately from each other within an agency.

Terminology	
<b>Metadata</b> – Structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata is often called data about data or information about information. <sup>181</sup> Physical and logical access control systems often rely on metadata to accurately and reliably grant user access to protected resources.	

For many existing resources, an agency has likely already determined which resources require protection and the necessary level of protection. Guidance for determining protection requirements for information systems, devices, and infrastructure is outlined in many existing policy and guidance documents (e.g., M-04-04, FIPS 199, M-06-16).<sup>182</sup> Guidance for determining levels of protection for facilities and work sites which require electronic security systems is provided by the Interagency Security Committee (ISC).<sup>183</sup> It can be expected that an agency’s physical security group will have previously evaluated all existing facilities and sites within the agency’s custody and determined physical protection requirements; however, for geographically dispersed organizations, this information may be managed locally. Figure 90 discusses several common programs and functions that collect and manage this information, and may therefore provide a starting point for ICAM implementers.

Agency Function	Information Available	Resource Type
Facility Management Group / Physical Security Group	Information regarding resources that must be secured using Physical Access Control System (PACS).	Physical
Real Property Group	Information regarding land, building, and improvements that are owned or leased by a federal agency.	Physical
Capital Planning and Investment Control (CPIC) Program	Investment information for capital assets submitted by a federal agency to OMB for funding.	Physical Logical
Helpdesk/Trouble Ticket Solutions and Records	Often contain lists of resources and/or targets of privilege/access management requests, as they are frequently sources of problems and issues for users.	Physical Logical
Enterprise Data Warehouse	Enterprise Architecture (EA) repository of electronically stored data about an organization’s resources and data, commonly maintained to facilitate reporting and analysis.	Physical Logical
Information Resources Catalog (IRC)	Some agencies may have an existing IRC, which is a comprehensive catalog of resources and resource information.	Physical Logical

<sup>181</sup> Understanding Metadata, National Information Standards Organization (NISO), 2004.

<sup>182</sup> [M-04-04](#), E-Authentication Guidance for Federal Agencies, OMB, December 23, 2003.[M-04-04]

[FIPS Publication 199](#), Standards for Security Categorization of Federal Information and Information Systems, NIST, February 2004. [FIPS 199]

[M-06-16](#)

<sup>183</sup> ISC Physical Security Criteria for Federal Facilities, The Interagency Security Committee, 2010.

Agency Function	Information Available	Resource Type
IT System Inventory	Inventory of IT applications and security compliance and reporting information.	Logical
Change Control Board (CCB) and/or Change Management System	Maintains the software, hardware, and application baselines for resources within the enterprise as a means of supporting change/upgrade efforts.	Logical

**Figure 90: Resource Information Sources**

Developing a comprehensive view of all agency resources (physical and logical) is reliant upon locating and reconciling existing sources of information. Several agencies have taken steps to create consolidated resource tracking solutions for the purpose of gathering the information necessary to make informed access management decisions in a timely manner. While this is not a requirement of ICAM, it is an example of a centralized repository of resource information to help ICAM implementers streamline the development and deployment process.

#### Implementation Tip

Don't wait until a complete agency inventory is in an automated system to begin developing access policies and tying resources into enterprise access control capabilities. Developing a complete inventory is a time-consuming process, and efficiency benefits and return on investment (ROI) can be realized by integrating even a small number of resources with automated ICAM capabilities once a representative sampling of major resource types has been identified.



#### 9.1.2. Collecting and Organizing Resource Information

Collecting, analyzing, and understanding the information about a resource that leads to determining the necessary level of protection is critical to establishing effective access control policies. An essential component in determining access control policy is a resource's risk profile. Risk profiles are indicators of the potential impact on the organization in terms of the loss of confidentiality, integrity, or availability for logical assets, and the impact of loss due to specific vulnerabilities for physical assets. Risk assessments are commonly performed for many agency resources as part of existing security compliance processes. Risk assessments for physical resources are governed by the Facility Risk Assessment process, outlined in the ISC's Physical Security Criteria for Federal Facilities, which is discussed further in Chapter 10. Risk assessments for logical resources are governed by the FISMA process. The resulting risk profiles can be leveraged for access control purposes without creating an additional burden for resource owners.

Risk profiles provide ICAM implementers with a baseline from which to determine the primary access control requirements. However, additional information about a resource can be used to develop more granular access controls to further increase the security and realize the efficiencies that can be obtained through deployment of access control systems.

FAQ	
<b>Are there any tools available to help determine the level of authentication risk associated with my information systems?</b> <p>Yes, the eAuthentication Risk and Requirements Assessment (e-RA) tool can be leveraged to assist in determining logical access control risks and appropriate levels of assurance, as defined in M-04-04. e-RA is available on the Federal Government's identity management website.<sup>184</sup> Additional guidance for conducting overall security risk assessments is provided in FIPS 199.<sup>185</sup></p>	

Contextual information about a resource is often required to support access control decisions. This information can often be obtained by reviewing resource documentation and meeting with resource owners/administrators to discuss how and why access is currently controlled. Chapter 11 also introduces the process for conducting application assessments, a best practice for supporting the integration of applications with LACS, which can serve as an additional means for gathering contextual information about logical resources. Examples of contextual information that can be used to support access control are provided in Figure 91.

Information Component	Description
Time-based access restriction	Access to the resource is restricted during particular hours or certain times of the day, week, or year based upon resource requirements.
Certification-based access restriction	Access to the resource requires possession of a particular certification or permit.
Organizational affiliation restriction	Resource access requires a particular affiliation with the organization (e.g., IT systems for federal employee access only), or affiliation with a particular bureau/component/office, etc.
Location-based restriction	Access to the resource is restricted based on geographical location for both physical and logical resources, and/or Internet Protocol (IP) and Media Access Control (MAC) address for IT resources and data.
Resource-based restriction	Access to certain data or information is dependent upon it being accessed through a particular resource, thereby preventing direct access.
Data sensitivity restriction	Certain IT resources or data elements may require that users possess a level of public trust or clearance (National Agency Check with Written Inquiries [NACI], Public Trust, Secret, etc.) before being accessed.

**Figure 91: Sample Resource Information Components**

The examples in Figure 91 are not intended to be comprehensive; however, they can be used to help implementers as they begin considering the additional information about a resource that is needed to develop access control policies. They also help define the types of entitlement information that an agency might need about its users in order to support access control decisions, discussed further in Section 9.2.1. Developing access control policies is a multi-step process to determine what access controls can be employed to improve security and create added value for the organization. The steps involved in developing robust access control policies are discussed in greater detail in Section 9.3.2.

Resources can be grouped based on common criteria as a means of providing baseline privileges in an automated fashion. This is accomplished by examining the resource attributes, such as the examples provided in Figure 91, that determine how users are granted access and looking for

<sup>184</sup> [GSA eAuthentication Risk and Requirements Assessment](#) (e-RA)

<sup>185</sup> [FIPS 199](#)

similarities that drive access control decisions. Resources may be grouped in several ways, including:

- **Physical Location.** Many agencies with multiple offices/buildings in metropolitan areas often grant access to all facilities within that area as a means of ensuring that personnel can easily attend meetings in nearby offices, this may also extend to network/system access associated with a geographic location.
- **Project/Program Affiliation.** Projects or programs that rely on a small subset of information systems or specified work locations can group those resources and grant access based upon affiliation with the project or program rather than granting each person access to each individual resource.
- **Organizational Relationship.** Within an agency there may be components or bureaus that grant access to resources based upon organizational affiliation (i.e., a component/bureau specific information sharing tool).
- **Function/Purpose.** Similar to Project/Program affiliation, certain resources may support a common function or purpose within an organization (i.e., HR systems, accounting systems, etc.).

In order to manage access control an agency must manage information about the individuals and entities attempting to access its resources. The processes for supporting this are discussed in the following section.

## **9.2. Privilege Management**

Privilege management, as defined in the ICAM segment architecture, refers to a set of processes for establishing and maintaining the entitlement or privilege attributes that comprise an individual's access profile. Privilege management supports updates to privileges over time as an individual's access needs change. Entitlement attributes are features of an individual that are used as the basis for determining access decisions to both physical and logical resources. The authorization decision relies on the presence or absence of one or more specific entitlement attributes. Across the Federal Government, access privileges are managed using an array of disparate processes and systems. Often, information about a person or entity is collected and stored numerous times in multiple locations and managed by administrators at a local resource level. This approach places a significant burden on local administrators to maintain user data, and often leads to considerable security risks in the form of orphaned accounts<sup>186</sup> and inappropriate access based on out-of-date entitlement information.

---

<sup>186</sup> Orphaned accounts is defined within Section 9.2.3.

## Terminology

<p><b>Privilege Management</b> – A set of processes for establishing and maintaining the entitlement or privilege attributes that comprise an individual's access profile. These attributes are features of an individual that can be used as the basis for determining access decisions to both physical and logical resources.</p> <p>There are several other commonly used definitions of privilege management that include definition of access policies or even real-time execution of access control. These concepts are included in the ICAM Services Framework<sup>187</sup> as "Authorization and Access" services and are addressed in this chapter.</p>	
--	---

Agencies should begin working to streamline and secure their existing privilege management processes by mapping and correlating entitlement attributes based upon common resource access needs and automatically provisioning<sup>188</sup> these attributes from authoritative sources to the appropriate resources. This section discusses the impacts of the ICAM segment architecture on traditional privilege management processes and introduces the automated provisioning capability that is outlined in the target state. Additionally, this section seeks to answer several common privilege management questions, including:

- What steps and activities are involved in managing privileges throughout the access management lifecycle?
- How can privilege management processes be improved by correlating similar information and access needs into defined roles?
- What does the automated provisioning capability do and what benefits does this approach provide over current techniques?

### 9.2.1. Entitlement Attributes

Attributes about an individual can be broken down into two primary categories for the purposes of access control, identity attributes and entitlement attributes. Identity attributes are characteristics about a person that make it possible to uniquely identify them as an individual. The creation, management, and use of identity attributes are discussed in great detail in Chapter 7. Entitlement attributes are those characteristics about an individual that are used to determine access privileges. Privileges, when combined with access control policies and resource access rules, are used to make intelligent access control (authorization) decisions.

Currently, entitlement attributes are obtained through a variety of user-reported paper-based and technology-based workflows at a local resource level within federal agencies. This often results in duplicative data collection and creates inefficiencies in which individual resource owners or administrators are responsible for ensuring the accuracy and validity of each user's entitlement attributes. The ICAM target state advocates minimizing the duplicative collection of this information by automatically populating existing attribute data from authoritative sources within the organization. Authoritative sources are typically repositories where there is an existing business purpose for information to be regularly updated to ensure that the data is accurate, current, and valid.

<sup>187</sup> The ICAM Services Framework can be found in Section 3.2.4.

<sup>188</sup> Target state ICAM provisioning capabilities are discussed in detail in Use Case 7, Section 4.7.2 of Part A. Achievement of the ICAM target state is discussed in Section 9.2.3.

### Implementation Tip

Defining the most commonly used entitlement attributes across multiple resources within your agency and automating sharing and use of this information will yield near term benefits while you continue to work on identifying additional attributes and making them available for sharing.



Generally speaking, there are several common categories of information about an individual used to make decisions regarding access privileges, including:<sup>189</sup>

- **Employer Details.** Information about an individual's employer and employment affiliation, which defines how an individual is —mapped within the organization. For internal users, this would likely include the bureau/component or even the division an individual supports, as well as the employee type (e.g., permanent, contractor, volunteer). For external users, this could include employer name and other relevant designations linked to a particular partner/customer organization.
- **Location.** Information related to the physical location of the individual. This typically includes regional designation, city or metropolitan area, and facility/site assignment. Location information can note an individual's permanent work location or temporary travel or detail assignments.
- **Job Duties.** Information regarding an individual's job designation and responsibilities. These attributes help define the resources, data, and sites that an individual requires access to in order to carry out his job. For federal employees, this includes common occupational series and job classification descriptions. This also includes job-related authorities, such as management level, direct reports, and approval authorities.
- **Special Qualifications.** Information about special designations, skills, or certifications an individual possesses. This includes security clearances, certifications/licenses, education, etc. These attributes are related less to an individual's mapping and responsibilities within the organization and more to a special skill or prerequisite condition for access to restricted resources, sites, or data.

### ROI

By managing access control using up-to-date entitlement attributes provided through an enterprise privilege management service, agencies can achieve process efficiencies and enhance overall security. These technologies are capable of rapidly granting or revoking access based upon changes to a user's entitlement attributes, the operational environment, and established access control policies. This reduces the administrative burden associated with manually managing access control and eliminates the vulnerabilities associated with unnecessary user access.



Within each of the above categories there are a variety of entitlement attributes that can be used to support access control decisions. Each attribute provides a unique piece of information about the individual, which, when combined with information about a resource, is capable of supporting a more granular level of authorization than is generally possible in most current systems. Entitlement attributes can be organized in a variety of ways, several of which are discussed in Section 9.3.1, for the purpose of streamlining the access control process. Most often,

<sup>189</sup> The descriptions in this section are adapted from [Defining User Attributes for Authority-Based Access Control](#), Waterman, K. Krasnow and Patricia K. Hammar, May 15, 2007.

collections of certain entitlement attributes are combined to develop access roles. Individuals in a particular role share similar information needs and as a result they likely share similar entitlement attributes. Use of roles or similar attribute groupings significantly reduces the complexity involved in managing user privileges. User roles are further discussed in Section 9.3.2.

### 9.2.2. Privilege Management Lifecycle

As previously discussed, privileges must be defined and managed over time to ensure that access decisions are based upon the most accurate and up-to-date information available. An individual's entitlement attributes must be refreshed periodically to reflect job/role changes, updated certifications, temporary assignments, etc. This section introduces a multi-stage privilege management lifecycle, which has been designed to help agencies fill this need. The activities discussed in Figure 92 should be tailored to suit the unique needs of an agency based upon existing business processes and technical architecture.

Life Cycle Phase	Description	Common Activities
Attribute Definition	Examining source systems to determine available entitlement attributes and select those that are necessary to determine access privileges.	<ul style="list-style-type: none"> <li>Identify attribute stores</li> <li>Determine if stores are authoritative</li> <li>Examine available entitlement attributes</li> <li>Select attributes necessary to enable access control</li> </ul>
Provision Access	Create user access accounts and assign access privileges associated with selected agency resources.	<ul style="list-style-type: none"> <li>Provision user access to protected resources</li> <li>Automate provisioning</li> </ul>
Periodic Review	Implement mandatory control mechanisms to re-validate access levels and modify entitlements at regular intervals. Access privileges may require adjustment based on promotions, job changes, role changes, situational variations, etc.	<ul style="list-style-type: none"> <li>Establish periodic review criteria</li> <li>Assess existing access privileges</li> <li>Modify privileges as necessary (revoke access if not required)</li> </ul>
De-provision Access	Removal of user access privileges to resources when access is no longer required to complete job duties or when the individual leaves the organization.	<ul style="list-style-type: none"> <li>De-provision user access rights from protected resources</li> <li>Remove user from authoritative sources (if leaving the organization)</li> <li>Retain and archive access records for de-provisioned users, if applicable</li> </ul>

**Figure 92: Privilege Management Lifecycle**

At a general level, each of the phases described above is essential to ensuring that privileges are managed consistently and accurately across the organization. Attributes should be defined and leveraged from existing authoritative sources to eliminate redundant collection and use at a local resource level. In order to maintain the integrity of the privilege management system, user privileges need to be periodically re-validated to accommodate changes to an individual's access requirements. Re-validation along with de-provisioning helps eliminate orphaned accounts within resources and prevents individuals from having access to resources that are not required to complete their job duties.

### 9.2.3. Automated Provisioning Capability

As defined in the ICAM Services Framework, Section 3.2.4.3, provisioning is the process of creating user access accounts and assigning privileges or entitlements within the scope of a

defined process or interaction. Provisioning provides users with access rights to applications and other resources that may be available in an environment, and may include the creation, modification, deletion, suspension, or restoration of a defined set of access privileges. Provisioning, as referred to in this document, includes the process for permanently removing an individual's access to particular agency resources when it is no longer required to perform job functions. This process is often referred to as de-provisioning.

## Terminology

**Orphaned Account** – An account belonging to a user that has left the organization or no longer requires access to the resource. Orphaned accounts are most often the result of ineffective de-provisioning processes wherein user access privileges are not removed immediately upon a user leaving the organization. These accounts create security vulnerabilities, which may be exploited by individuals seeking to do harm.



In the current environment, provisioning to PACS differs slightly from provisioning user privileges to other IT systems. Currently, automated provisioning capabilities that are integrated with PACS solutions typically provision user identity data for the purpose of establishing a user account, while entitlement privileges (e.g., access to specific sites or doors) are managed and controlled within the PACS solution itself. In the ICAM target state, however, agencies should develop automated provisioning capabilities that enable the provisioning of desired baseline physical access privileges (e.g., access to building common areas for all agency cardholders) to the PACS solution as part of the initial account creation process.

Throughout the majority of the Federal Government, provisioning is currently performed via an array of manual processes that create new instantiations of a user's identity within each resource, often employing paper-based approval workflows. This heavily manual process greatly reduces the ability to remove access when it is no longer needed (de-provision), in a timely fashion. This arrangement creates a great administrative burden for local resource owners and administrators, and is labor and time intensive. Additionally, the inability to efficiently and rapidly revoke access can inadvertently allow users to retain access to information or sites unnecessarily, or result in the existence of orphaned accounts. The target state ICAM segment architecture proposes the use of automated provisioning capabilities as a means of reducing redundant collection and use of digital identity data and streamlining the process of pairing identities and resources.

## ROI

The National Aeronautics and Space Administration (NASA) performed an analysis of its logical resources to determine what basic resource entitlements should be granted to new users. A provisioning capability was deployed to automatically grant new users access privileges to these resources immediately upon record finalization by Human Resources (HR). This has resulted in significant administrative and time savings for resource owners and allowed new users to gain access to resources immediately upon beginning employment.



Automated provisioning tools leverage existing, authoritative sources of digital identity data to automatically link those identities to agency resources based on an analysis of the entitlement privileges. This capability standardizes the provisioning process across an organization for all protected resources. Figure 93 illustrates the numerous efficiencies that can be achieved by deploying an enterprise-wide automating provisioning capability.

Benefit Category	Example Benefits
User Experience	<ul style="list-style-type: none"> <li>• Reduced manual account linking</li> <li>• Automated account linking and reconciliation</li> <li>• Elimination of per-application paper-based workflow</li> <li>• Access provisioning when required by role</li> <li>• Reduced sign-on applications</li> <li>• Faster access to resources</li> </ul>
Operational Efficiency	<ul style="list-style-type: none"> <li>• Streamlined provisioning of accounts for new users</li> <li>• Ability to establish foundational provisioning capabilities</li> <li>• Reduction in per application account administration</li> <li>• Automated reconciliation response workflow</li> <li>• Attribute synchronization</li> <li>• Business friendly workflow for approvers and/or administrators</li> </ul>
Security	<ul style="list-style-type: none"> <li>• Ability to easily automate detection, reporting, and response to orphaned accounts</li> <li>• Ability to detect and resolve excessive access privileges across multiple resources</li> <li>• Elimination of custom account linking code</li> <li>• Ability to centralize audit and access reporting</li> <li>• Standardized provisioning</li> <li>• Ability to digitally sign access approvals</li> <li>• Ability to automate use of enterprise digital identity<sup>190</sup></li> <li>• Visibility into PII reduced based on business and job requirements</li> <li>• Centralized preventative policy enforcement</li> </ul>

**Figure 93: Benefits of Employing Automating Provisioning Capabilities**

An effective provisioning framework has a strong foundation comprised of standardized, easily deployable, and repeatable approaches that simplify processes, eliminate infrastructure stovepipes, and streamline access control within agencies. Provisioning capabilities should be tightly integrated with an agency’s overall ICAM architecture and remain flexible enough to accommodate resource-specific approval processes.

#### Privacy Tip

Using technology to automate manual paper-based provisioning processes does not eliminate the privacy requirements associated with the manual process. Privacy protections, such as approvals from required personnel, must be embedded into new electronic applications or processes that are replacing a paper format (e.g., a paper request form), in order to prevent additional privacy risk. Agencies should build these protections into the automated workflow from the initial design.



#### 9.2.3.1. Common Design Characteristics

In order to successfully build and deploy an automated provisioning capability, as defined in the target state ICAM segment architecture, it is necessary to understand the common characteristics that the solution should include in order to meet the objectives of the ICAM target state. These common characteristics are identified in Figure 94; however it is also important for agencies to consider their specific needs when designing a provisioning tool.

Characteristic ID	Automated Provisioning Characteristics
Provisioning 1	The automated provisioning service includes resource requirements for creating a valid resource user account.

<sup>190</sup> See Section 7.1 for additional information on enterprise digital identity.

Characteristic ID	Automated Provisioning Characteristics
<b>Provisioning 2</b>	The automated provisioning service includes network configuration requirements between provisioning component and resource user store.
<b>Provisioning 3</b>	The automated provisioning service includes workflows for provisioning resource accounts (including accounts for Physical Access Control System [PACS] solutions).
<b>Provisioning 4</b>	The automated provisioning service includes forms for requesting access to a protected resource (including physical sites, buildings, rooms, etc.).
<b>Provisioning 5</b>	The automated provisioning service includes approvals required for granting authorization to protected resources.
<b>Provisioning 6</b>	The automated provisioning service includes requirements for how the identity management component will create/modify/delete authorization.
<b>Provisioning 7</b>	The automated provisioning service includes any data schema attributes needed for provisioning for each protected resource.
<b>Provisioning 8</b>	The automated provisioning service includes any notifications that will be triggered during the provisioning workflow.
<b>Provisioning 9</b>	The automated provisioning service includes audit/reporting requirements for provisioning workflows.
<b>Provisioning 10</b>	The automated provisioning service includes workflows for de-provisioning resource accounts.
<b>Provisioning 11</b>	The automated provisioning service includes the ability to map identities to resource accounts.
<b>Provisioning 12</b>	The automated provisioning service includes the ability to retrieve and evaluate authoritative attributes from other agency systems to make provisioning decisions.
<b>Provisioning 13</b>	The automated provisioning service includes the ability to detect and act on attribute changes to provision and de-provision access.
<b>Provisioning 14</b>	The automated provisioning service includes any resource account lifecycle management requirements.
<b>Provisioning 15</b>	The automated provisioning service includes any user interface requirements for provisioning workflows and providing help desk support.
<b>Provisioning 16</b>	The automated provisioning service includes the ability to detect, prevent, and resolve conflicts with established segregation of duties (SOD) policies.

Figure 94: Common Characteristics of an Automated Provisioning Capability

### 9.2.3.2. *Implementation Considerations*

Deploying an automated provisioning capability is an undertaking that requires planning, support, and coordination from various groups within an agency. Specific planning and coordination considerations include the following:

- **Understand current workflows.** Awareness of current provisioning workflows and technologies allows integrators to fully understand which resources require which information, while at the same time allowing integrators to analyze these needs and streamline, where applicable.

Lesson Learned	
When configuring automated provisioning workflows, consider leveraging a small set of baseline workflows to start. The workflows can then be modified and customized over time to support additional resource-specific needs or as mission and/or business needs change. The National Aeronautics and Space Administration (NASA) found that a single baseline workflow with several alternate approval options enabled rapid deployment of provisioning services to the majority of its resources.	

- **Determine approval requirements.** Knowing resource authorization requirements facilitates the mapping of roles and entitlements to access privileges. Providing an escalation path when approvals (or denials) are not given in a defined timeframe can significantly decrease the overall time taken to provision a user and improve the end user experience.
- **Develop technical requirements.** Define the development, test, and production environment configurations in which the automated provisioning system will run, including the solution architecture and configuration specifications for hardware processing nodes, automated provisioning component deployment, communications interfaces and protocols, network interfaces, and disk storage.
- **Define de-provisioning processes.** A key benefit to automated provisioning solutions is the ability to accurately and reliably de-provision user access when it is no longer needed. Currently, many agencies have fewer triggers to review and remove access than for providing access. An agency can see significant efficiencies and security benefits by carefully defining rules for de-provisioning users, whether temporarily (suspend access) or permanently (revoke access).
- **Determine appropriate logging and auditing requirements.** Logging defined approval and provisioning steps is critical in establishing who has been given access to what and by whom. Agencies should determine appropriate auditing requirements and ensure that the provisioning solution is designed to log the appropriate events.
- **Define user reports or dashboards.** Automated provisioning provides the ability to capture information regarding account requests, approvals, and assigned permissions. Agencies should determine requirements for user reports or dashboard capabilities using this information to make the user management process more transparent to business and application owners.

## ROI

Automated provisioning capabilities support an enhanced level of transparency and a more accurate understanding of the number of required active user accounts for a given resource. Upon implementing its provisioning solution, a federal agency was able to significantly reduce its software licensing costs at the resource level by eliminating unnecessary user licenses for duplicate or orphaned accounts.



- **Determine technology needs.** There are a wide variety of technology solutions that can provide an agency with an automated provisioning capability. An agency should analyze available workflow products, the ability to modify existing investments, and custom provisioning capabilities to determine which solution best suits the overall needs of the organization in the most cost effective manner.
- **Determine appropriate provisioning architecture.** Provisioning architectures typically operate in one of two ways: by initiating the transmission of identity data (attributes, roles, privileges, etc.) through data feeds at predetermined time intervals or based on events; or by allowing relying parties (resources) to initiate the transmission of identity data from LACS components by request, when needed. Agencies should assess the business needs and technical constraints of the resources that will be integrated with the provisioning solution and define the appropriate architecture.
- **Gain approval and seek funding.** Regardless of the technology path chosen, agency implementers will need to gain investment approval from ICAM decision makers and secure funding if existing investments are not feasible sources.

- **Link user identifiers to an enterprise digital identity.** User identifiers often vary from resource to resource. As part of implementing an automated provisioning capability, these unique identifiers should be mapped to the user's enterprise digital identity to provide visibility into user permissions across the organization. This concept is further discussed in Chapter 7.
- **Maintain data privacy.** Provisioning involves transmitting and/or sharing user data with integrated resources to facilitate account creation and access control. Agencies must ensure that appropriate controls are in place to maintain data privacy and prevent unauthorized disclosure.
- **Communicate and train the user population.** As with all other organizational changes, an agency should ensure that the changes are communicated to the user population and that appropriate training is provided. In provisioning, this is especially important for personnel holding a sponsor or approver role.

#### Implementation Tip

When establishing automated provisioning workflows, it is important to evaluate current process steps and maintain necessary approval steps that are not inherently managed through the automated workflow (i.e., human intervention) to ensure that resource access is appropriately provisioned. In many cases, provisioning automation may allow an agency to streamline the account request steps. For example, approvals that were previously performed by sequentially signing a paper form may be approved concurrently, where appropriate, and offer non-repudiation of the approval through use of digital signatures.



In addition to planning considerations discussed above, implementation and enablement considerations for automated provisioning solutions are provided for PACS and LACS solutions in Chapters 10 and 11, respectively. Once an organization has a privilege management process in place to grant access privileges to individuals and an automated provisioning capability, the next step is correlating these access privileges with access rules that are intended to protect resources. The resulting access control policies are then used to control access to protected resources based on individual access privileges and may be reused with future resources. Authorization models for streamlining access control and the process through which access control policies are developed and enforced are discussed in detail in the following section.

### 9.3. Authorization

Authorization is the enforcement of access policies to ensure that the correct individuals and entities are granted access to only the resources and information that they require. This relies heavily on the —principle of least privilege,|| which states that users should only be authorized to access whatever is needed to do their job. In order to achieve successful authorization decisions, agencies must define policies that specify how information about resources, users, and the environmental context should be combined in order to determine when to grant or deny access. The combination of all of these elements comprise authorization.

## FAQ

### What is the difference between authentication and authorization?

Authentication<sup>191</sup> is the process of verifying that a claimed identity is genuine and based on valid credentials. In contrast, authorization is the process of granting or denying specific requests for access to resources. These two processes are tightly aligned and together support access control.<sup>192</sup>



The responsibility for determining the appropriate access control policies typically rests with the relying party resource (i.e., with the system owner or facility security manager). As agencies move toward the target state ICAM architecture and enterprise approaches, models, and services for access control, it is important to work with resource owners to understand and incorporate the appropriate resource-specific workflows and policies. This offers agencies the ability to streamline existing authorization processes and improve consistency, security, and reliability without giving up local control of resource access criteria.

This section discusses the impacts that the ICAM segment architecture has on existing authorization processes, introduces various models for evaluating attributes to make access decisions, and examines the processes for managing access control policies throughout their life cycle. Additionally, this section seeks to answer several common questions about authorization, including:

- What are access control models and how are they used to streamline access control within an agency?
- What should I consider when evaluating the various access control models for my agency?
- How are access control policies defined and enforced within ICAM solutions, and what benefits do digital access control policies offer?

### 9.3.1. Access Control Models

Successfully managing access to resources relies on pairing certain elements of information about the resource (discussed in Section 9.1) with information about the user (discussed in Section 9.2) within the appropriate context to make an access decision. An agency can employ various access control models to determine how user and resource attributes should be handled within access control transactions. Access control models are conceptual ways to express how an access control system implements specific policies using its underlying infrastructure components and security mechanisms. This section discusses common access control models, their benefits and limitations, and examines when a particular model could be employed based upon the needs of the agency. Many of the definitions and characteristics of various access control models within this section are drawn from NIST IR 7657.<sup>193</sup>

Many systems today rely on access control lists (ACLs), a basic method for performing access control that grants access based on a list of the authorized entities and the actions they are allowed to perform. ACLs offer a simple approach to managing access and require minimal

<sup>191</sup> PIV-based authentication is discussed in detail in Chapter 8 – Fully Leveraging PIV and PIV-I Credentials.

<sup>192</sup> A detailed discussion of authentication and authorization, and the role that they play in supporting access control is available in [SP 800-12, An Introduction to Computer Security: NIST Handbook, NIST, October 1995, \[SP 800-12\]](#)

<sup>193</sup> [NIST IR 7657](#)

infrastructure; as such, they have been implemented widely across numerous applications. Maintaining ACLs for individual resources or an enterprise can be time-consuming and prone to errors. Additionally, approval processes for adding a user to an ACL often involve personal knowledge of the individual, such as by a supervisor approving the request. Over time, as a user's role or access needs change, it can be difficult to identify and remove access that is no longer needed.

## Terminology

**Situational Access Control** – An approach for adapting access control decisions for a resource to support the current operational environment. In this approach, the attributes about a user or resource typically do not change; however, their relevance to the situation impacts the access control decision. For example, an individual may be granted access to a location that he/she does not routinely have access to during an emergency situation based on his/her designation as an Emergency Response Official.



Situational Access Control is not a separate access control model but may be supported by several of the more robust access control models (e.g., Role-Based Access Control (RBAC), Policy-Based Access Control (PBAC), Attribute-Based Access Control (ABAC), and Risk-Adaptable Access Control RAdAC)<sup>194</sup> available.

As agencies move toward enterprise approaches to access control in the ICAM target state, many ICAM implementers are looking for more flexible, granular approaches for managing access. Several additional access control models are available that automate access based upon user attributes and contextual resource information, including Attribute-Based Access Control (ABAC), Role-Based Access Control (RBAC), Policy-Based Access Control (PBAC), and Risk-Adaptable Access Control (RAdAC). Figure 95 describes each of these access control models and discusses the benefits and limitations inherent to each model.

Access Control Model	How Access Determinations are Made	Benefits	Limitations
<b>Access Control List (ACL)</b>	Access to resources is granted on a resource-by-resource basis, based upon an individual's inclusion and corresponding privileges, as noted on the resource's ACL.	<ul style="list-style-type: none"> <li>• Simple framework which does not require pre-existing infrastructure.</li> <li>• Supported by common operating systems.</li> <li>• Widely used and accepted throughout the Federal Government.</li> <li>• Controlled locally at the resource level.</li> </ul>	<ul style="list-style-type: none"> <li>• Ability to evaluate individual access privileges becomes extremely complex as the list grows larger over time.</li> <li>• Criteria for access and individual role/job duties are fluid over time, thereby placing a significant administrator burden on resources owners.</li> <li>• Nearly impossible to manage at an enterprise level due to the sheer volume of resources and ACLs.</li> <li>• Requires manual changes to ACL, a time consuming and error prone process.</li> <li>• Revocation of access privileges may be delayed due to non-automated communication methods (e.g., word of mouth, e-mail, paper form distribution, etc.).</li> </ul>

<sup>194</sup> See Figure 95 for a description of these access control models.

Access Control Model	How Access Determinations are Made	Benefits	Limitations
<b>Role-Based Access Control (RBAC)</b>	<p>Individuals are assigned to various roles within an organization, down to the resource level based upon certain identity and entitlement attributes.</p> <p>Access is determined by having a particular role assignment that corresponds to one or more resources.</p>	<ul style="list-style-type: none"> <li>• Supports groupings of individuals with particular roles based upon well-defined and trusted attributes.</li> <li>• Can accommodate centralized management.</li> <li>• Can be implemented at various levels within an organization, as long as a valid role is defined.</li> <li>• Supported by common operating systems and capable of group support as well.</li> </ul>	<ul style="list-style-type: none"> <li>• Can be difficult to manage as each protected resource generally has unique role requirements, thereby resulting in large numbers of potential role assignments within an organization.</li> <li>• Difficult to manage granular access of individuals due to the rigid nature of role assignments.</li> <li>• Difficult to implement in a highly distributed agency (not centrally managed).</li> <li>• Requires significant level of effort to determine appropriate alignment of privileges for users not linked to the agency's organizational structure.</li> </ul>
<b>Attribute-Based Access Control (ABAC)</b>	<p>Focuses on characteristics that describe people, resources and environments. The requester provides attributes which are compared to those documented as requirements for granting or denying access, at which point a decision is made.</p>	<ul style="list-style-type: none"> <li>• Requires no advance knowledge of requestors.</li> <li>• An individual's attributes can be correlated from multiple sources to create a unified identity.</li> <li>• Highly adaptable to changing needs; efficient for agencies where individuals come and go frequently.</li> </ul>	<ul style="list-style-type: none"> <li>• Lengthy implementation time due to the need to correlate information and attributes from multiple sources for all potential users.</li> <li>• Reliant on authoritative identity/entitlement data – difficulty managing attribute conflicts between source systems.</li> <li>• Not natively supported by common operating systems.</li> <li>• Not appropriate for all environments (i.e., those with significant changes in risk level).</li> </ul>
<b>Policy-Based Access Control (PBAC)<sup>195</sup></b>	<p>Determines access using rule sets, which consider the circumstances of the transaction and the policy.</p>	<ul style="list-style-type: none"> <li>• Promotes compliance with standardized access controls.</li> <li>• Flexible in not being linked to only one type of access control.</li> <li>• Adapts quickly to new policy rules.</li> </ul>	<ul style="list-style-type: none"> <li>• PBAC requires the design, deployment, and seamless integration of enterprise level systems (databases, directory services, etc.).</li> <li>• Policies must be absolutely unambiguous to avoid unintentional, unauthorized access.</li> <li>• Entire enterprise must use the same attributes for access and those attributes must be authoritative.</li> <li>• Not natively supported by common operating systems.</li> </ul>

<sup>195</sup> PBAC may also be referred to as Rule-Based Access Control.

Access Control Model	How Access Determinations are Made	Benefits	Limitations
<b>Risk-Adaptable Access Control (RAdAC)</b>	Amount of information required of requesters to verify their identity depends on the current threat level, information includes personal trustworthiness and environmental factors.	<ul style="list-style-type: none"> <li>• Has the ability to make real time access control available.</li> <li>• Can control multiple diverse systems- including digital policies as some systems may require different authentication levels for the same user based transactions.</li> <li>• Supports flexible situations.</li> </ul>	<ul style="list-style-type: none"> <li>• Cannot always be automatic, user judgments are needed.</li> <li>• Integrated systems must use standardized data exchange formats.</li> <li>• Policies must be unambiguous to avoid unintentional, unauthorized access.</li> <li>• Extensive considerations in adhering to policy and law – involves great care to be taken to ensure compliance.</li> <li>• Not natively supported by common operating systems.</li> </ul>

**Figure 95: Common Access Control Models**

The elements described above are intended to help agencies better understand access control models and the value that they can provide. However, implementers should recognize that no single model is perfect in all situations. There are several important considerations that ICAM implementers should consider when evaluating access control models for a particular agency, including:<sup>196</sup>

- **Complexity vs. Simplicity.** Agencies should seek to achieve a balance between complexity and simplicity of the access control system's underlying architecture. Simpler architectures are easier to manage and maintain; however, they may offer comparatively fewer enhanced capabilities. Implementers should consider the agency's unique situation in terms of its user base, resources, infrastructure, and attribute stores in order to determine which model balances complexity with simplicity. Additionally, an agency may begin with a simple architecture that is designed for extension to a more complex model over time, which can be an effective way to support achievement of short and long-term objectives.
- **Performance.** Agencies should consider their mission needs and operating requirements and evaluate against the access control system's ability to process user requests within a time that is consistent with the needs of the enterprise. This can be accomplished by examining the complexity of the decision-making algorithm, as well as through process modeling and prototyping.
- **Policy Support.** Access control models should support the organization's overall access control policies, such as mandatory access control, discretionary access, separation of duties, workflows, etc. Certain models may also be capable of combining various policies to achieve enhanced capabilities, should they be desired.
- **Ease of Administration.** Agencies should consider the level of administrative and technical support necessary to manage the access control system. For example, the need to support special languages and capabilities represents a significantly higher administrative burden than use of a simple graphical user interface to compose and administer access control policy.

<sup>196</sup> [NIST IR 7657](#)

## FAQ

### Isn't there one access control model that is the best?

Each of the access control models is a conceptual approach for how to use resource, user, and environmental data to drive the appropriate types of access control policies. In practice, agencies should review their access requirements and choose the model or a combination of the capabilities of several models in order to best suit their needs. More robust access control models, such as role-based access control or policy-based access control, can help an agency achieve the automation and efficiency goals and enhanced security capabilities associated with the target state ICAM segment architecture.



Each access control model has been presented individually in order to allow for a comparison of the benefits and limitations. In implementation, however, it is likely that many agencies will utilize some type of hybrid approach that combines various aspects of multiple access control models depending on the requirements of the resource. For example, RBAC often provides a sufficient level of granularity to define access policies for many agency resources; however, an application that has an extensive remote user population may require additional access mechanisms capable of handling RAdAC contextual information. In this case, when a user from an unknown location attempts to gain access, they may be prompted for additional information for verification. Several of the access control models in this section provide efficiencies or more granular security that is not possible in the current environment. The following section discusses how these models may be applied to define and manage access control policies within an agency.

### 9.3.2. Policy Management

Access control policies are used throughout the Federal Government and serve as the linchpin that enables successful authorization decisions to both physical and logical resources, supports security audit capabilities, and controls access to information. These policies are the rules that specify how to use resource and entitlement attributes to make an access control decision.

## FAQ

### What is the difference between Policy-Based Access Control (PBAC) and Access Control Policies?

While both terms include the word “policy,” PBAC is just one of several access control models, which are used to describe how access control decisions are made within an access control system. Access control policies, on the other hand, are the specific rules that are executed by an access control system that define what users should be granted access to what resources. Policies are found in association with each of the various access control models discussed in the previous section.



Creation of secure, implementable access control policies hinges on having accurate, reliable, and timely information about the resources that you are protecting, and the users and devices that require access to them. Pairing this information results in the creation of rules/policies that define what attributes a person must have in order to access a particular resource. Strategies for managing access control policies vary widely within the Federal Government; however, it often occurs at a local/resource level within federal agencies, where administrators modify policy to

suit local operational requirements. At a general level, policy management can be broken down into a multi-step life cycle, as depicted in Figure 96 below:<sup>197</sup>

Life Cycle Phase	Description	Common Activities
<b>Policy Definition</b>	Process which defines the access control policy scope and requirements for a target asset or resource. The following considerations and inputs influence the access control policy definition process, including but not limited to: environment, users, unauthorized access risks; and existing policies, rules or internal processes which currently govern access to the resource or asset. The Policy Definition phase is usually facilitated by several interviews and working sessions.	<ul style="list-style-type: none"> <li>• Identify the asset or resource requiring discrete access control</li> <li>• Discover the environment in which access control policies will be developed and applied</li> <li>• Discover the users affected by the access control policies</li> <li>• Discover and document the risks associated with unauthorized access risks based on government standards (e.g., SP 800-63,<sup>198</sup> M-04-04, etc.)</li> <li>• Discover and document the relevant policies, rules or internal processes which influence the access to the asset or resource</li> </ul>
<b>Policy Analysis</b>	Process which includes examining and analyzing the policy definition outputs and findings to help design access control policies which can be implemented. During this phase, the risks, rules, and inputs discovered will be analyzed to determine the authentication token type, the access control model, the relevant authorization model, and the tools used to enforce access.	<ul style="list-style-type: none"> <li>• Determine the access control model required (agency-level)</li> <li>• Determine level of assurance based on industry standards and guidelines (e.g., SP 800-63)</li> <li>• Determine access control authorization model by analyzing policy definition access</li> <li>• Determine the access control techniques, standards, and technologies required to enforce the access control policy</li> <li>• Develop metrics to measure effectiveness and performance of access control policies implemented</li> <li>• Conduct testing to assess effectiveness and performance of access control policies</li> </ul>
<b>Policy Creation</b>	Process of expressing access control policies using access control mechanisms and technology platforms.	<ul style="list-style-type: none"> <li>• Build access control policies on physical or logical systems based on the access control policies, rules, and designs developed</li> <li>• Develop test use cases which can be used during the access control policy evaluation phase</li> </ul>
<b>Policy Evaluation</b>	Process of testing the policy or policies designed and developed on test assets or resources.	<ul style="list-style-type: none"> <li>• Independently test the access control policy using the test use cases developed</li> <li>• Provide test feedback to improve access control policy created and ensure metrics defined are met</li> </ul>
<b>Policy Implementation &amp; Enforcement</b>	Process of implementing the newly created or revised access control policy on a production physical or logical asset or resource, and granting or denying access requests based upon policy-based authorization decisions.	<ul style="list-style-type: none"> <li>• Implement the newly created or revised access control policy on a production physical or logical asset or resource</li> <li>• Test the access control policy to ensure effectiveness</li> </ul>

<sup>197</sup> Additional information about policy management can be obtained in [Enterprise Security Management](#), A Context Overview, DoD, March 2009.

<sup>198</sup> [SP 800-63](#), Electronic Authentication Guideline, Version 1.0.2, NIST, December 2008. [SP 800-63]

Life Cycle Phase	Description	Common Activities
<b>Policy Review &amp; Revision</b>	Process which includes measuring the effectiveness of the access control policy implemented, determining whether the access control policy should be retired, or deciding if the access control policy should be revised.	<ul style="list-style-type: none"> <li>• Attestation certifying the effectiveness of the access control policy in production</li> <li>• Recommendations to asset or resource stakeholders when access control policy metrics are not met</li> </ul>

**Figure 96: Policy Management Lifecycle**

Modernized PACS and LACS solutions, as discussed in Chapters 10 and 11, respectively are capable of offering policy management services at an enterprise level. Enterprise level policy management services provide the ability to administer access control policies at a local resource level using authoritative data, common attributes, and job/role definitions through a centralized construct. The target state ICAM segment architecture does not require the use of centralized policy management services; however, certain efficiencies can be achieved by leveraging this capability. Those include:

- **Reduced administrative burden.** Local resource owners/administrators develop access control policies to suit their specific needs; however the administrative burden associated with storing policies occurs within the access control solution.
- **Consistency and improved transparency of policies across agency resources.** Utilizing policy management services provided by a common access control solution ensures that access control policies across an agency enterprise are developed using consistent guidelines and tools, which reduces redundancy and enables reuse of commonly used policies.
- **Ability to detect and address conflict.** Coordinated management across agency policies ensures that policy privileges are not conflicting or inconsistent across the enterprise and are resolved before new policies are implemented.

## 9.4. Auditing and Reporting

This chapter has discussed the lifecycle management processes that support performing access control for physical and logical resources within a federal agency. Conducting automated access transactions will result in the logging of transaction event information, which can be used for auditing and reporting. Auditing and reporting, as defined within the ICAM Services Framework addresses the review and examination of records and activities to assess the adequacy of system controls and the presentation of logged data in a meaningful context.

This section discusses the enhanced enterprise auditing and reporting capabilities that are associated with the target state ICAM segment architecture. Additionally, this section seeks to provide answers to several common auditing and reporting questions, including:

- How will auditing and reporting differ in the ICAM target state?
- How can ICAM solutions support security compliance and performance reporting, as required by the ICAM target state?
- What types of reports should I consider when designing my ICAM solution?

Across the Federal Government, information systems, including PACS solutions, are designed and built to comply with specific accountability requirements, which mandate the capability to review and report on various access events within individual applications. Each application

administrator (or his/her designee) is responsible for tracking and reviewing access control events within their applications, and investigating anomalous entries. The processes for completing this task vary widely across agencies, business units, and individual resources. Typically, in order to provide contextual audit information in a meaningful manner, resource owners/administrators have to manually correlate transaction event data from multiple sources that may be paper-based and/or technology-based. Auditing and reporting capabilities are highly dependent on technological constraints such as: network limitations, application setup, application age, network infrastructure, etc. In addition, to the audit and reporting requirements for all IT resources, PACS solutions must be capable of providing additional reporting services for physical access events within the organization, as defined in the ISC's Use of Physical Security Performance Measures.<sup>199</sup>

The target state ICAM segment architecture does not specify particular requirements for auditing and reporting capabilities; however, many of the modernization efforts that agencies will be performing on their physical and logical access control systems present an opportunity to improve and automate their existing capabilities. For PACS, the transition to enterprise level services increases the visibility into logged access event data and increases the ability to correlate that data across individual site PACS, resulting in improved auditing and reporting capabilities. For logical access, many of the commercially available solutions that can be used to provide enterprise LACS services, as discussed in Chapter 11, include native auditing and reporting tools that can be configured to meet a variety of agency requirements. Agencies that choose not to deploy enterprise level access control services may still be able to perform centralized auditing and reporting; however, the consolidation processes required to do so are complex and time consuming. NIST SP 800-92, Guide to Computer Security Log Management,<sup>200</sup> provides a detailed discussion of the processes that are required to consolidate logs from various sources.

ROI	Implementing an enterprise reporting and auditing capability in a centralized fashion allows agencies to achieve transparency across a wider array of resources, detect and resolve inappropriate access, and rapidly detect patterns of unauthorized access attempts across the organization in a manner not currently possible.	
-----	---	---

Figure 97 describes several types of access control reports that could be provided by an agency's automated auditing and reporting services.

Report Type	Description
User Access by Resource	Provides an up-to-date account of successful user access attempts to both physical and logical resources, allowing the administrator/reviewer to select which resource they are primarily concerned about. This type of report may contain a large amount of data and its production could degrade solution performance. Agencies should consider when this type of report is necessary and determine when it could be produced with a minimum level of service interruption.
Unsuccessful Access Attempts	Provides an account of all unsuccessful access attempts to any resource within the organization. Allows administrators to determine if individual users have a disproportionate number of unsuccessful access attempts across a wide range of resources.

<sup>199</sup> Use of Physical Security Performance Measures, The Interagency Security Committee, 2009.

<sup>200</sup> [SP 800-92](#), Guide to Computer Security Log Management, NIST , September 2006. [SP 800-92]

Report Type	Description
Daily/Weekly/Monthly Activity	Provides an account of all access activity for a particular resource within a set time period; typically daily, weekly, or monthly.
Individual User Audit Log Report	Provides an audit log for all activities (successful and unsuccessful) attempted by an individual user.

**Figure 97: Common Access Control Reports**

The auditing and reporting improvements discussed in this section offer agencies significant benefits and ROI for many of the modernization expenditures that are already required in order to align with the target state ICAM segment architecture. These benefits include:

- **Ease of compliance with existing audit and accountability requirements.** Agencies are currently required to meet a myriad of auditing and accountability requirements associated with program efficiency (OMB Circular A-123)<sup>201</sup> and access control. For IT systems, these requirements are part of the FISMA reporting process and are outlined in the Audit and Accountability (AU) control family detailed in SP 800-53.<sup>202</sup> For PACS solutions, the ISC defines program efficiency measures to evaluate long-term achievement of strategic security program goals.<sup>203</sup> Additionally, enterprise access control solutions can support compliance with the continuous monitoring requirements outlined in SP 800-37.<sup>204</sup>
- **Ability to meet security control enhancements for high impact systems.** SP 800-53 specifies additional AU measures for high impact information systems as a means of ensuring increased levels of security on these highly sensitive resources. For example, AU-3 and AU-6<sup>205</sup> specify centralized management of audit records and the ability to correlate audit records across IT and physical security domains, respectively. The enhanced audit and reporting capabilities provided by modernized access control systems offer the ability to meet these security enhancements without placing an additional burden on individual resources and administrators.
- **Ability to provide security information in new meaningful contexts, not currently available.** Access control systems, built in accordance with the target state ICAM segment architecture, offer the ability to correlate and present large amounts of information from resources across an agency enterprise in a near real-time fashion. As part of reporting progress against the ICAM segment architecture, agencies are required to produce performance metrics and reports in accordance with the ICAM Performance Layer, as discussed in Section 3.2.1. Currently, this requires significant manual correlation and aggregation of information from an array of sources, whereas modernized access control solutions are capable of performing this task in an automated, streamlined manner.

<sup>201</sup> [OMB Circular A-123](#)

<sup>202</sup> [SP 800-53](#)

<sup>203</sup> Use of Physical Security Performance Measures, The Interagency Security Committee, 2009.

<sup>204</sup> [SP 800-37](#)

<sup>205</sup> [Audit and Accountability](#); AU-3: Content of Audit Records and AU-6: Audit Monitoring, Analysis and Reporting.

**Privacy Tip**

When seeking to enhance its auditing and reporting capabilities, an agency should ensure that appropriate security measures (e.g., data encryption, robust access control mechanisms, etc.) and policies are established to secure and limit access to and use of sensitive audit data.



- **Increased efficiency with auditing and reporting.** Agency resources have historically provided their own auditing and reporting capabilities, requiring resource owners design and build their resources with these capabilities in mind. Building auditing and reporting capabilities into each resource requires additional investment money and results in a significant time commitment to manage at a local level. Providing these capabilities at an enterprise level allows investment money to be reallocated to other mission critical areas and frees resource owners/administrators to focus on other priority activities.

This page is intentionally left blank.

## 10. Initiative 7: Modernize PACS Infrastructure

Initiative 7, as introduced in Section 5.2.2, is an agency-level ICAM implementation initiative that includes activities associated with upgrading PACS for routine access for PIV cardholders and standardized visitor access for individuals with other acceptable credentials. As defined in the ICAM segment architecture, a PACS is an automated system that manages the passage of people or assets through an opening(s) in a secure perimeter(s) based on successful authentication and associated authorization rules. The target state calls for a modernized PACS, which includes the following characteristics:

- Electronically authenticates PIV cards and accepts multi-factor authentication as defined in NIST SP 800-116;<sup>206</sup>
- Supports an agency-wide approach to managing physical access services that links individual PACS via an enterprise level network wherever possible and appropriate, while maintaining local control over authorization decisions;
- Interfaces with authoritative Identity Providers and data source(s) to supply user attributes and credential information for automated provisioning and de-provisioning; and
- Incorporates technologies that support secure, automated processes for requesting and provisioning visitor access.

The guidance provided in this chapter is intended to help agencies achieve the target state presented in the ICAM segment architecture Use Case 8, Grant Physical Access, and the associated transition activities listed in Section 5.2.2.3.

This chapter is organized into the following five sections:

- **Physical Access Implementation Planning.** This section discusses the activities and processes that are necessary to properly plan for a modernized PACS implementation within an agency. It includes existing standards and guidance, PACS program governance, facility risk assessments, program funding, and schedule planning considerations that are necessary to properly plan for a physical access deployment within an agency.
- **Physical Access Architecture and Design.** This section describes the architecture, components, and key design characteristics common to a modernized PACS solution.
- **Physical Access Technical Implementation.** This section covers common technical considerations for deploying PACS solutions within federal agencies, including automated provisioning and physical access scenarios.
- **Local Facility Access.** This section presents guidance concerning populations that need long-term local access but are ineligible (i.e., individuals other than federal employees and contractors) for a PIV card.
- **Visitor Access.** This section discusses common requirements of a Visitor Management System (VMS) and other visitor access considerations.

---

<sup>206</sup> [SP 800-116](#), A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), NIST, November 2008. [SP 800-116]

## 10.1. Physical Access Implementation Planning

Providing reliable, robust physical security for its facilities and buildings is an important responsibility for each agency. Additionally, physical security systems and procedures affect a variety of users accessing federally-controlled facilities every day. As such, implementations of modernized PACS solutions should be planned carefully to ensure success and prevent disruptions to operations. Typically, decisions related to the selection and implementation of PACS have been determined at the individual site level. As agencies move towards achieving the target state, planning for a modernized PACS at the enterprise level offers many benefits, including cost savings achieved from enterprise software licenses, decreases in redundant collection and management of user identity data, and improved security through increased consistency. Additional advantages are discussed throughout the rest of this chapter.

This section is targeted largely at those individuals responsible for setting the direction for and planning an agency's PACS modernization effort. It will explore key aspects of implementation planning, including: program governance, facility risk assessments, program funding, and schedule planning. The OMB memorandum released on May 23, 2008<sup>207</sup> provides agencies with additional guidelines for consideration when planning or updating plans for the use of the PIV card in their PACS, a central aspect of the ICAM target state. In addition, the ICAM Reporting Template provides a detailed list of activities associated with implementing the ICAM segment architecture.

### FAQ

#### Does Physical Access Control System (PACS) infrastructure modernization require the use of an electronic PACS at every facility?

No. Selection of security countermeasures, including PACS, should be based on the risk assessment of a facility. Other access control approaches, such as lock and key, might provide adequate security and be more cost effective for an exceptionally low risk facility. As agencies develop their implementation plans in accordance with ICAM, they should first focus on the highest-risk facilities for PACS modernization. Over time, this should expand to lower-risk facilities in order to leverage the PIV credential wherever possible.



The information and guidance presented in this section is intended to assist agencies in providing answers to several common questions related to physical access implementation planning, including:

- How can my agency coordinate management of its PACS modernization efforts?
- How can my agency perform risk assessments on its facilities?
- What should my agency consider when funding its PACS implementation?
- What are the necessary steps required when planning and executing a PACS implementation?

### 10.1.1. Program Governance

Chapter 6 provides guidance concerning overarching ICAM governance at the agency level. This section is intended to supplement that guidance and highlight specific areas that agency governance bodies should seek to address at an enterprise or component/bureau level to enable

<sup>207</sup> [Guidance for Homeland Security Presidential Directive 12 \(HSPD-12\) Implementation](#), OMB, May 23, 2008. [HSPD-12]

successful PACS modernization efforts. For example, as part of the planning for a PACS implementation, an agency should leverage its ICAM governance structure to coordinate the PACS-related activities and investments across the bureaus/components and foster effective communication and cooperation with other efforts, such as logical access and information technology. Formalizing program governance for an agency's PACS effort within the ICAM governance structure can ensure that change is managed properly, communications are delivered effectively, and that policy is created or refined to support the target state.

### Implementation Tip

To increase effectiveness, PACS governance should be made up of decision makers from each bureau/component. For example, the Change Control Board (CCB) for USDA's enterprise PACS implementation, ePACS, includes representatives from each of its sub-agencies who are educated on PACS policies and help ensure activities and efforts at their sub-agencies meet USDA policies and common requirements.



The transition to a modernized PACS needs to incorporate an appropriate change management approach to ensure that stakeholders embrace the changes associated with the implementation. An agency should take advantage of the many tools associated with effective change management, including following a project plan, developing communication tools, and conducting training. The approach should also include steps to reinforce change such as monitoring effectiveness, building stakeholder buy-in, and celebrating successes.

Communication is important throughout the change management process and also plays a key role in the other transition activities associated with modernizing a PACS. Because physical security and access to buildings affects all government employees, contractors, and visitors, communication with and education of the end-user population can significantly impact the success of the implementation. For example, the PACS governance team should plan for and communicate any revised policy and new procedures that are created early and often. Additionally, as new ICAM services are deployed, an agency should communicate key changes to its user populations well in advance to avoid disruptions. The communication options and delivery media presented in Section 6.1.3.1 of this document can be leveraged by PACS governance to ensure appropriate and effective messages are delivered at the right time.

### Lesson Learned

Some of the simplest communication tools can also be the most effective. For example, posting signs at entry points displaying important information regarding the modernization can help individuals prepare for upcoming changes. One agency learned that employees planned to arrive early on the first day PIV cards would be used at the entrance of the building because they had read the signs and were expecting delays.



#### **10.1.1.1. Existing Policy and Requirements**

The first priority of physical security is life safety, protecting the people who occupy federal buildings. In support of this paramount responsibility, there are standards, codes, and policies that individuals in the physical security field are required to follow. The PACS is one of many parts of the overarching physical security mission. Implementers must address additional standards and guidance, such as the following:

- **Interagency Security Committee (ISC)<sup>208</sup> Compendium of Standards.** The ISC was created to enhance the quality and effectiveness of physical security in, and the protection of, federal facilities in the U.S. These authoritative standards are designed to help federal security professionals implement effective security policies. Of particular relevance:
  - **Facility Security Level (FSL) Determinations for Federal Facilities.** Defines the criteria and process to be used in determining the FSL of a federal facility, a categorization which then serves as the basis for implementing protective measures under other ISC standards.
  - **Physical Security Criteria for Federal Facilities.** Establishes a baseline set of physical security criteria that provide a framework for the customization of security measures to address unique risks at a facility.
  - **Interim Design-Basis Threat Report.** A stand-alone threat analysis to be used in conjunction with the physical security criteria. It establishes a profile of the type, composition, and capabilities of adversaries.
- **National Fire Protection Agency (NFPA) codes.<sup>209</sup>** The NFPA is the authority on fire, electrical, and building safety and its mission is to reduce the burden of fire and other hazards on the quality of life by providing and advocating consensus codes and standards, research, training, and education. NFPA develops, publishes, and disseminates consensus codes and standards intended to minimize the possibility and effects of fire and other risks. Of specific note:
  - **NFPA 101.** The Code addresses those construction, protection, and occupancy features necessary to minimize danger to life from the effects of fire, including smoke, heat, and toxic gasses created during a fire.
  - **NFPA 72.** Covers the application, installation, location, performance, inspection, testing, and maintenance of fire alarm systems, supervising station alarm systems, public emergency alarm reporting systems, fire warning equipment and emergency communications systems, and their components.
- **Underwriters Laboratories (UL).** An independent product safety certification organization that tests products and writes standards for safety in an effort to promote safe living and working environments, support the production and use of products which are physically and environmentally safe and to prevent or reduce loss of life and property. UL is the trusted resource across the physical security industry for product safety certification and compliance. Standards of particular relevance:
  - **UL 294.** Specifies requirements for the construction, performance, and operation of systems intended to regulate or control entry into an area or access to or the use of a device(s) by electrical, electronic or mechanical means. These requirements apply to computer equipment that, when used in conjunction with the main control, is necessary for proper operation of the access control system.

---

<sup>208</sup> A description of the ISC and its ICAM authority can be found in Section 2.3.1.

<sup>209</sup> [National Fire Protection Agency \(NFPA\)](#)

- **UL 1076.** Specifies requirements for the construction, performance and operation of equipment intended for use in proprietary burglar alarm units and systems used to protect against burglary.
- **UL 2050.** Specifies requirements for the monitoring, signal processing, investigation, servicing and operation of alarm systems.
- **Federal Information Security Management Act (FISMA).** This act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for IT systems. As covered under FISMA, PACS implementers must meet all requirements associated with the RMF as defined in SP 800-37<sup>210</sup> and implement the appropriate security controls outlined in SP 800-53.<sup>211</sup> They must also comply with FISMA reporting guidelines.<sup>212</sup>
- **Open, Systems Integration and Performance Standards (OSIPS).** A family of standards developed by the Security Industry Association (SIA), an American National Standards Institute (ANSI) accredited standards organization. These standards are intended to promote interoperability between components in traditional access control systems by providing a common interface and creating levels of performance. OSIPS references architecture information for all parts of an integrated electronic security system, including the PACS, and addresses how to use the standards within a compliant ICAM implementation. Of particular note:
  - **OSIPS-ACR-200x.** Describes identity authentication and factors that are presented in a transaction seeking access to an Accessible Component Collection.
  - **OSIPS-APC-200x.** Describes the credentials presented to field devices at the access point controller.
  - **OSIPS-IDM-200x.** Describes claims of identity that are authenticated by comparing reference authentication factors with presented credentials.

In addition to these existing standards and regulations, the next section introduces recommended agency governance efforts that may be used to support PACS modernization. It is important to note that the recommendations in this document are not intended to replace or supersede existing life safety or physical security standards and regulations.

#### **10.1.1.2. Agency Governance Efforts**

Policy is a key enabler of success during a PACS modernization. As part of implementation planning, PACS governance should review existing agency policies to determine if they align with the ICAM segment architecture, as well as relevant laws, government-wide policies, and standards. As appropriate, the planning should address any policy gaps that are identified with revisions to existing or the creation of new policies. This section is intended to supplement the guidance around program governance found in Chapter 6 and highlight specific areas that agency governance bodies should seek to address to enable successful PACS modernization efforts.

---

<sup>210</sup> [SP 800-37](#)

<sup>211</sup> [SP 800-53](#)

<sup>212</sup> [M-10-15](#)

PACS-specific policies will vary based on an agency's size, mission and business requirements, as well as the maturity of its physical access policies relative to the ICAM target state. Per M-11-11,<sup>213</sup> agencies must develop and issue agency implementation policy requiring the use of the PIV credential for access to the agency's facilities, networks, and information systems and alignment with the ICAM segment architecture. There are also a number of other common topics that should be incorporated in an agency's governance efforts to support the modernized PACS implementation. Figure 98 includes a list of common governance efforts and describes how agencies might consider utilizing them as a means to promote compliance and overcome implementation challenges. Many of the governance efforts listed below are expected to apply to logical access, discussed in Chapter 11, and may be combined at some agencies.

Governance Effort	Description
Issue Policy Memorandum: Continued Implementation of HSPD-12	<ul style="list-style-type: none"> <li>• Agency-level policy, as required by M-11-11, that includes provisions for several items related to PACS modernization, including:</li> <li>• Enforcing use of the PIV card for physical access and the movement away from separate (often bureau/component-specific) ID cards.</li> <li>• Procurement of services and products for PACS in accordance with M-06-18<sup>214</sup> and the Federal Acquisition Regulation (FAR).<sup>215</sup></li> <li>• Acceptance of PIV credentials issued by other federal agencies for physical access.</li> <li>• Alignment with the ICAM segment architecture, including completion of an agency transition plan that includes information regarding the agency's PACS modernization.</li> </ul>
Issue Policy/Guidance Addressing Common Physical Access Scenarios	<ul style="list-style-type: none"> <li>• Policy or procedural guidance reflecting formal agency-level decisions for handling common physical access problem scenarios such as a lost/forgotten PIV card.</li> </ul>
Issue Policy/Guidance Addressing Standardization of Local Facility Access Cards	<ul style="list-style-type: none"> <li>• Policy or procedural guidance for establishing a standard local facility access card and providing guidance around when and how they are issued. This topic is discussed further in Section 10.4.</li> </ul>
Issue Policy/Guidance Addressing Visitor Management	<ul style="list-style-type: none"> <li>• Procedural guidance for establishing what types of credentials are considered acceptable for granting physical access to visitors. Direction should address additional procedures for handling individuals who are not PIV card holders (e.g., escort procedures). This topic is discussed further in Section 10.5.</li> </ul>
Define Baseline User Privileges for Physical Access	<ul style="list-style-type: none"> <li>• Effort to determine a set of baseline user privileges for physical access that can be linked into the agency's automated provisioning capability to grant new users privileges to multiple access points automatically.</li> </ul>
Bureaus/Component Modernization Plans	<ul style="list-style-type: none"> <li>• Effort by agency leadership and management to review and provide guidance related to bureau/subcomponent implementation plans for modernizing PACS. The review should take into consideration whether the proposed approach meets relevant requirements and is the most cost effective (e.g., upgrading an existing PACS rather than purchasing a new system).</li> </ul>
Incorporate the PIV Card Implementation Maturity Model (PIMM)	<ul style="list-style-type: none"> <li>• Effort to incorporate the PIMM into PACS project performance measurement. The PIMM describes various levels of PIV card use to help agency leadership and PACS implementers determine the maturity of the PACS program and make decisions accordingly.</li> </ul>

**Figure 98: Sample PACS Governance Efforts**

<sup>213</sup> [M-11-11](#)

<sup>214</sup> [M-06-18](#)

<sup>215</sup> [FAR Subpart 4.13](#)

An important aspect of governance is the ability to measure project performance and maturity; however, measuring the progress of a modernized PACS implementation can be complex due to variations in the requirements, facility size, and amount of existing electronic PACS. SP 800-116 presents the PIV card Implementation Maturity Model (PIMM),<sup>216</sup> which should be used by agencies to measure progress while working towards achieving the target state. The levels are progressive and range from, —Ad Hoc PIV card Verification,|| to —Access to Exclusion, Limited, or Controlled Areas by PIV card or Exception Only.|| The lowest level describes a site that has the ability to authenticate PIV cards by performing required authentication mechanisms on an ad hoc basis. The most mature level describes a site in which only the PIV card is an acceptable credential for federal employees and contractors covered under HSPD-12. The PIMM can be integrated into agency's ICAM performance management reviews to determine the success of the modernized PACS implementation effort and set completion goals.

### **10.1.2. Facility Risk Assessments**

Government facilities are a part of the nation's critical infrastructure, and as such, have certain protection requirements. The following mandates and requirements underscore an agency's responsibility for protecting federal facilities:

- **HSPD-7 Critical Infrastructure Protection Mandates.** Establishes a national policy for federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them from terrorist attack. HSPD-7 identifies 17 sectors that require protective actions to prepare for, protect, or mitigate against a terrorist attack or other hazards.
- **National Infrastructure Protection Plan (NIPP).** Outlines the parameters for infrastructure protection. The use of the NIPP risk management framework is a part of the overall effort to ensure the protection and resiliency of our Nation's Critical Infrastructure/Key Resources. The NIPP includes the Government Facilities Sector Plan, which provides an approach to enhancing protection of government facilities.

Facilities and access points should be protected based on risk. The ISC Compendium of Standards, discussed in Section 10.1.1.1, provides agencies with guidance on how to perform facility risk assessments, define the appropriate FSL, and analyze the required level of protection to determine and implement the appropriate security countermeasures. As described in M-11-11,<sup>217</sup> the Department of Homeland Security (DHS) has also partnered with the GSA Public Building Service (PBS) to ensure that risk assessments and implementation of physical access measures for buildings under PBS' purview are executed in accordance with the ISC and NIST guidelines. There are a variety of risk assessment processes available for agency use. Figure 99 provides a summary of the main steps that are commonly conducted as part of a facility risk assessment, as defined in the ISC guidance and based upon industry best practices.

---

<sup>216</sup> [SP 800-116](#)

<sup>217</sup> [M-11-11](#)

Process Integration Step	Description	Key Considerations
<b>Step 1: Set Security Goals</b>	Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture or baseline.	<ul style="list-style-type: none"> <li>• Agency's security control posture and risk tolerance.</li> <li>• Security requirements, including FICAM security targets for PACS.</li> </ul>
<b>Step 2: Identify</b>	Develop an inventory of the assets, systems, and access points that exist within a facility.	<ul style="list-style-type: none"> <li>• Range of systems and assets within a given facility.</li> <li>• Calculated value of assets within a given facility.</li> </ul>
<b>Step 3: Assess</b>	Determine risk by identifying potential consequences of vulnerabilities.	<ul style="list-style-type: none"> <li>• Likelihood of occurrence.</li> <li>• Impact if vulnerabilities are exploited.</li> <li>• Local conditions and the area surrounding a facility.</li> </ul>
<b>Step 4: Analyze</b>	Categorize and analyze risk assessment results to develop a comprehensive picture of facility risk.	<ul style="list-style-type: none"> <li>• Relevant legislation, policies, and standards.</li> <li>• Protection priorities and adequate countermeasures.</li> </ul>

**Figure 99: Common Risk Management Steps**

The end result of the risk assessment is a complete risk profile of the facility. This information helps physical security implementers make decisions regarding appropriate security countermeasures to employ, including electronic (e.g., video surveillance, intrusion detection, PACS, etc.), physical (e.g., bollards, gates), and guard force. The scope of this guidance is limited to authentication-based access control and thus focuses on the electronic PACS as a countermeasure;<sup>218</sup> however, agencies can find additional guidance on selecting a full range of alternative countermeasures in the ISC's Compendium of Standards.<sup>219</sup>

When applying the results of the facility risk assessment to the design of its PACS, an agency needs to determine the risk level of a particular facility and individual areas within the facility that will be protected by a controlled access point. The agency should then determine the appropriate authentication mechanism(s) that should be deployed at each access point, as defined in SP 800-116. SP 800-116 uses the restricted area concept of—Controlled, Limited, Exclusion areas to address individual areas nested within a facility that may have specific security requirements. They are defined as follows:

- **Exclusion Area.** An Exclusion area is a restricted area containing a security interest or other matter of such nature that access to the area, or proximity resulting from access to the area, constitutes access to the security interest or matter.
- **Limited Area.** A Limited area is a restricted area containing a security interest or other matter of such nature that uncontrolled movement will permit access to the security interest or matter. Access in Limited areas may be controlled by requiring escorts or by other internal restrictions and controls.

<sup>218</sup> For more information on the security controls that can be implemented by a PACS, see Federated Physical Access Control System (PACS) Guidance, Federal CIO Council.

<sup>219</sup> Government users with a need to know may access the ISC standards that are For Official Use Only (FOUO) by requesting access at [ISC@DHS.gov](mailto:ISC@DHS.gov).

- **Controlled Area.** A Controlled area is that portion of a restricted area usually near or surrounding an Exclusion or Limited area. Entry to the controlled area is restricted to authorized personnel.

### Lesson Learned

It can be difficult to analyze a site for its risks and know how to apply the appropriate guidance while keeping cost savings in mind. An agency might find value in assembling a small team of cross functional resources (including physical security, IT, etc.) from its ICAM program to help bureaus/components or individual sites conduct facility risk assessments and make decisions regarding the best way to achieve a compliant, modernized PACS.



Once an agency has determined the appropriate authentication mechanisms based on a facility's risk, it should make decisions around the best PACS solution and how to fund its implementation. The following section provides additional considerations and guidance on these topics.

### Implementation Tip

Focus on what you can control. Agencies frequently occupy leased space where the landlord controls the exterior physical security. If the existing system cannot process the PIV card for physical access, establish an access point at the entry to the agency-controlled space. This arrangement allows the agency to meet its requirements for PIV card authentication while still adhering to the leasing agreement.



### 10.1.3. Program Funding

A key aspect of physical access implementation planning is making decisions around the funding and acquisition of a modernized PACS solution. This includes estimating solution costs, determining the proper funding method, and planning for and completing acquisition of the required products and services. This section discusses key considerations for estimating program funding needs and potential funding models for an agency's PACS modernization. Additional information on acquisition planning and the budget request process can be found in Section 6.1.3.3.

### ROI

One large agency was able to save tens of thousands of dollars per site on costs associated with server hosting, hardware and software, and executing IT security requirements when their individual PACS were rolled into the enterprise service offering.



Selecting an appropriate PACS modernization approach and corresponding technology solution is one of the first steps in determining how a PACS program will be funded. Agencies should choose a solution that aligns with the ICAM segment architecture, supports their access control processes and requirements, leverages existing infrastructure wherever possible, and provides the best value for their investment. Once a solution has been determined, an agency should evaluate a number of factors in order to estimate the costs that will be incurred. The items provided in Figure 100 are examples of common factors and considerations that agencies should examine not only to determine costs, but also determine the potential cost savings that various PACS solutions are capable of providing.

Evaluation Factor	Description
Facility Size	The number of users requiring access to a facility significantly impacts the level of administrative effort required to provision user accounts and manage access privileges. In addition, there may be potential cost breaks for certain
Level of PACS Services Provided	Agencies should determine at which level PACS services should be provided. There are cost savings and efficiencies that can be achieved by providing services at the enterprise-level. For example, an agency hosting a server for the bureaus/components.
Analysis of Population	Organizations should examine populations (employees, contractors, short term, etc.) and facility tenants (federal, non-federal) to determine the types of groups requiring access. Complex user populations should be considered when making a decision on the type of PACS solution to implement. In addition, there should be capability to handle increased capacity as the modernization progresses and the amount/type of users change over time.
Number of PACS	The number of PACS within an agency often dictates implementation time and can significantly affect implementation cost, depending on the resources' connection requirements.
Type of PACS	The type of PACS varies based on the vendors, platforms, operating systems, products, databases, etc. that are in use across the organization. These variances impact the complexity of integrating resources with the PACS infrastructure and require different integration processes.
Existing PACS Investments	Agencies may have existing investments in place that are capable of providing physical access services in a manner consistent with the target state ICAM segment architecture. These investments should be leveraged wherever possible and offer the potential to achieve a modernized PACS state without requiring significant investment from the organization.
Credentials Supported	Agencies should examine the types of credentials that the PACS must support (including PIV-I) and incorporate any costs associated with validating acceptable credentials.
Protection Areas <sup>220</sup>	Agencies should consider the number or combination of protection areas (Limited, Exclusion, Controlled) when determining program costs. For example, a high number of exclusion protection areas may increase costs due to the added level of access control required to protect those areas.

**Figure 100: Common PACS Acquisition Considerations**

Once a solution has been identified and the potential costs and cost savings have been estimated, agencies should make decisions around how to fund the PACS solution. Typically, PACS have been selected and funded at the site level. As agencies look to move towards an enterprise model, this can introduce challenges for funding and implementing enterprise PACS services, where equipment and services will likely be purchased centrally. To date, agencies have taken several different approaches to funding their PACS modernization efforts. These include:

- **Incorporate Costs into Existing Investment.** Rather than having a separate PACS investment, costs for PACS modernization can be included in an existing business case.
- **Investment Business Case.** A new investment request to fund PACS modernization at the enterprise level. The business case includes details of how the proposed investment would support the agency's mission.
- **Working Capital Fund.** A fund that is able to provide financing to agencies without annual appropriation by Congress for operations that generate receipts. This funding method works well for an agency that is providing the enterprise PACS as a centralized service and has a fee structure for the users across the bureaus/components.

<sup>220</sup> More detailed information can be found in Section 10.1.1.2.

### Implementation Tip

The products implementing and executing the cryptographic processes with the PIV card must comply with FIPS 140 and be approved by NIST validated laboratory. Agencies should procure products and services from manufacturers who provide architectures that minimize the cost of FIPS 140 by producing components in very high volume, or by amortizing the cost into common components, such as a multi-door controller.



In addition to determining funding needs and obtaining funding, a key aspect of PACS implementation planning is outlining the life cycle activities associated with the modernization effort and determining the project schedule. This is addressed further in the following section.

#### 10.1.4. Schedule Planning

Modernizing PACS projects requires close coordination across multiple workstreams within an agency and may, in some cases, represent a multi-year effort. During this period, it is critical to develop a transition plan that keeps the current PACS and physical security infrastructure in place while reducing security system downtime. Because of this complexity, program/project managers should consider following a system development life cycle (SDLC) that addresses key activities and timing considerations. There are a variety of SDLCs that are commonly accepted and used within the Federal Government. Each agency should have a defined and repeatable SDLC that meets the agency's business needs and supports IT investments; these same concepts can be applied to physical security investments. While individual agency SDLCs may be more granular in detail and contain additional steps/phases, the activities and considerations presented in this section can be adapted into any SDLC model.

### Implementation Tip

An important aspect of developing a phased implementation approach is accurately documenting the activities that must occur during each phase and defining measurable exit criteria. This ensures that the implementation proceeds along a predictable path, which can help mitigate many common implementation risks.



The guidance presented in this document has been organized into a traditional, sequential five-phase SDLC (waterfall) process, as it is the simplest and most commonly used model. The phases discussed have been abstracted from a variety of individual agency SDLC models to suit the needs of this document and create an appropriate basis for discussion. The five phases are: Planning, Requirements and Design, Build, Implement, and Operate and Maintain. This section examines each of the SDLC phases in greater detail and discusses the PACS-specific events that should occur as part of each phase.

### Implementation Tip

One large agency created a working group to gather information around its deployed PACS infrastructure, such as vendor product, version and architecture. Collecting this data can help agency leadership determine how to leverage existing investments when planning and designing its target state PACS solution.



#### 10.1.4.1. Planning Phase

Section 10.1 of this chapter discusses the overall planning considerations when implementing a modernized PACS. This section describes planning as the first phase of the structured SDLC

process commonly used when executing complex solutions. Completing the Planning Phase is critical for modernizing PACS solutions, as many of the common problems encountered can be avoided through careful planning.

Lesson Learned	
<p>Investing in and installing multi-technology PIV card readers gives program implementers access control during the transition from agency-specific proximity cards to PIV cards. It also allows proximity cards to be issued to resolve temporary physical access challenges such as lost, stolen, or damaged PIV cards.</p>	

Figure 101 provides a list of common activities that should occur during the Planning Phase and notes estimated completion times for each; however, activities may occur in parallel, and actual times can vary widely based on organizational size and project complexity.

Activity	Description	Completion Time
Develop Communications Plan	Develop the approach and plan to communicate (using a variety of mediums) the changes that a PACS modernization effort will bring to internal users, resource owners, and stakeholders. It should include some form of agency cultural education plan if changes will be significant.	2 – 4 weeks
Conduct Gap Analysis	Determine the desired operation and use cases for the target state system and then compare against capabilities of the current equipment. This should be followed by an objective assessment of capabilities of the current PACS to determine what solution is required to achieve the desired target state.	2 – 4 weeks
Conduct Cost/Benefit Analysis	Evaluate organizational factors and conduct a cost/benefit analysis to determine an appropriate PACS solution.	3 – 6 weeks
Develop PACS Modernization Business Plan	Develop a business plan to support modernization of the existing PACS infrastructure or a new infrastructure. This should lay out the selected approach, timeline, resource requirements, and estimated costs.	4 – 6 weeks
Develop Implementation Plan/Schedule	Develop a phased implementation approach and schedule based on available information using standardized agency resources.	2 – 4 weeks
Categorize the PACS	Conduct Step 1 of the Risk Management Framework (RMF): <sup>221</sup> Categorize Information Systems based on mission/business objectives. Register the PACS in the IT system inventory.	4 – 12 weeks
Develop Risk Management Plan	Utilize existing risk management sources to develop a Risk Management Plan, as discussed in Chapter 6, for handling risks related to modernizing the PACS infrastructure.	2 – 4 weeks
Begin Field Prioritization	Begin examining agency PACS and developing field assessment criteria in order to prioritize/organize deployment of modernized PACS services to agency facilities.	1 – 2 weeks
Develop Field Integration Guide	Develop a Field Integration Guide, a formal document used to outline the process that an agency's physical security resources will go through to become integrated with the PACS solution.	6 – 8 weeks
Develop PACS Migration Plan	Develop a migration plan that outlines how the agency plans to transition its physical resources to use the modernized access control system.	1 – 3 weeks
Develop Pilot Implementation Plan	Develop a plan and schedule for piloting the modernized PACS solution on a small subset of the user population with well-defined resource requirements.	4 – 12 weeks

**Figure 101: Planning Phase Sample Activities**

<sup>221</sup> A more detailed discussion of the Risk Management Framework can be found in Section 6.2.4.1.

#### 10.1.4.2. Requirements and Design Phase

The Requirements and Design Phase follows the Planning Phase in the SDLC. In this phase, an agency thoroughly documents the requirements for the PACS solution and defines how the solution should operate within the existing infrastructure. Figure 102 provides a list of common activities that should occur during the Requirements and Design Phase and notes estimated completion times for each; however, activities may occur in parallel, and actual times can vary widely based on organizational size and project complexity.

Activity	Description	Completion Time
Gather PACS Solution Requirements	Conduct a requirements gathering exercise with stakeholders and impacted parties at all organizational levels to document requirements of the PACS solution. These requirements are critical as they will be used to drive the design, build, and configuration of the PACS capability.	4 – 6 weeks
Validate PACS Solution Requirements	Validate the documented requirements with the appropriate stakeholders in order to ensure that the PACS solution is properly designed and configured to meet the agency's needs.	1 – 2 weeks
Secure Funding Sources	Utilize the PACS business plan to secure funding sources for the modernization effort. This should include determining if existing investments exist and how to leverage them.	6 – 10 weeks
Select Security Controls	Conduct Step 2 of the Risk Management Framework (RMF): Select Security Controls by choosing the appropriate security controls and documenting the selected controls in the security plan. <sup>222</sup>	2 – 4 weeks
Document System Design	Draft an initial system design document that clearly states how the system should function within the agency's environment. The design document and associated requirements are then used during the build phase as a reference for how the PACS system should operate.	2 – 4 weeks
Define and Configure Provisioning Workflows	Define provisioning workflows, which are used to determine how users are granted rights to access points and what approvals or additional steps are required. This process often involves configuring automated workflows based on existing manual processes.	2 – 4 weeks
Develop Solution Architecture	Develop an initial solution architecture for the PACS implementation. This architecture defines the solution components and describes their interactions.	2 – 4 weeks
Conduct Resource Acquisition	With funding sources secured, conduct the process of purchasing any required hardware or software and services.	4 – 12 weeks

Figure 102: Requirements and Design Phase Sample Activities

#### Implementation Tip

Be sure to include ICAM requirements for modernized PACS in facility arrangements, negotiations, and the procurement process for leased space. When these requirements are introduced during the Requirements and Design Phase, an agency can more easily ensure the proper requirements are incorporated into lease agreements.



#### 10.1.4.3. Build Phase

Following the Design Phase, agencies enter the Build Phase, where the majority of the technical solution development, configuration, and testing occurs. Figure 103 provides a list of common

<sup>222</sup> For more information on the security controls that can be implemented by a PACS, see Federated Physical Access Control System (PACS) Guidance, Federal CIO Council.

activities that should occur during the Build Phase and notes estimated completion times for each; however, activities may occur in parallel, and actual times can vary widely based on organizational size and project complexity.

Activity	Description	Completion Time
Stand Up Development and Test Environments	Establish development and testing environments so that PACS developers and testers can conduct build activities in an environment that does not impact the agency's production systems.	4 – 6 weeks
Build/Configure Servers	Build and/or configure servers to properly operate the PACS solution, as needed based upon the chosen implementation path.	1 – 2 weeks
Install Supporting Software	Install supporting software (i.e., Commercial Off-The-Shelf [COTS] Identity Access Management [IAM] Suite) on PACS servers, as needed based upon the chosen implementation path.	1 – 2 weeks
Configure Supporting Software	Configure PACS software to specifically meet the agency's unique needs and/or perform certain functions, as needed based upon the chosen implementation path.	1 – 2 weeks
Implement and Assess Security Controls	Conduct Steps 3 and 4 of the Risk Management Framework (RMF) by applying the controls identified in the requirements and design phase and by assessing the adequacy and effectiveness of the security controls and documenting the findings in an assessment report.	12 – 20 weeks
Conduct Testing on Initial Build	Perform testing on the PACS solution in a development and/or test environment to ensure that system errors are found and corrected before the solution is deployed on the agency's network.	2 – 4 weeks
Conduct Pilot Implementation Deployment	Conduct a pilot implementation to expose a small subset of the agency's user base to the PACS solution for the purpose of evaluating the solution's operations against real-world requirements.	Varies on size of deployment (number of facilities and access points)

**Figure 103: Build Phase Sample Activities**

#### **10.1.4.4. Implement Phase**

Once an agency has configured its PACS solution and tested to ensure that it meets agency and government-wide requirements and performs appropriately, the program enters the Implementation Phase. This phase consists of activities for migration of the PACS solution from a development and test environment into the agency's production infrastructure. There may be an overlap in access control services provided by the old and new PACS for a period of time until the cardholder population is fully transitioned to the new PACS. Figure 104 provides a list of common activities that should occur during the Implement Phase and notes estimated completion times for each; however, activities may occur in parallel, and actual times can vary widely based on organizational size and project complexity.

Activity	Description	Completion Time
Authorize the PACS	Conduct Step 5 of the Risk Management Framework (RMF): <sup>223</sup> Authorize Information System by preparing and submitting the security authorization package to the authorizing official. The authorizing official chooses to accept the risk and authorize the	1 – 2 weeks

<sup>223</sup> A detailed discussion of the RMF can be found in Section 6.2.4.1.

Activity	Description	Completion Time
	system if the risk associated with operating the PACS is deemed acceptable.	
Conduct User Acceptance Testing	Conduct user acceptance testing to ensure that the PACS solution is acceptable to stakeholders and end users and performs the required functions in an appropriate manner.	2 – 4 weeks
Conduct User Training	Develop training materials and conduct user training prior to PACS deployment to ensure that users are capable of accessing their worksites without disruption.	2 – 4 weeks
Deploy PACS Solution to Live Production Environment	Deploy the PACS solution on the agency's network infrastructure and begin controlling access to facilities.	Varies according to deployment size (number of facilities and access points)
Perform Awareness and Outreach	Conduct awareness and outreach activities in accordance with the Communications Plan developed as part of the Planning Phase. This involves actively communicating to users that a new access control system is being deployed, the benefits and efficiencies that users can expect, and any steps necessary to begin using the new system.	This will occur as needed throughout the deployment process

Figure 104: Implement Phase Sample Activities

#### 10.1.4.5. Operate and Maintain Phase

After an agency has successfully deployed its modernized PACS solution to a live production level, the program enters the Operate and Maintain Phase. This phase lasts for the remainder of the time that the PACS solution is in use and consists of ongoing management and system maintenance activities such as: conducting training, operating the PACS solution, and protecting new resources as they come online.

##### Implementation Tip

Enterprise development often includes connection of multiple local PACS servers that may contain local user records. This process may involve removal of redundant accounts in instances where one person has access to multiple sites. Additionally, agencies should have a plan for handling duplicate user records.



Figure 105 provides a list of common activities that should occur during the Operate and Maintain Phase and notes estimated completion times for each; however, activities may occur in parallel, and actual times can vary widely based on organizational size and project complexity.

Activity	Description	Completion Time
Monitor Security Controls	Conduct Step 6 of the Risk Management Framework (RMF): Monitor Security Controls by monitoring changes to the information system and its environment of operation and conducting ongoing assessments of security controls in accordance with the monitoring strategy.	On-going
Ongoing User Training	Continue to update and modify user training curriculums as the PACS solution matures and new technology is implemented. Conduct additional training as necessary.	This will occur as needed throughout the deployment process
Modify Provisioning Workflows	Update provisioning workflows as business needs and access rules change over time. Changes may also be required as resource owners experience the benefits that can be provided by modernized PACS services and provisioning workflows can be streamlined.	2 – 4 weeks per occurrence

Activity	Description	Completion Time
Conduct Hardware/ Technology Refresh	Conduct periodic updates and/or upgrades to solution hardware and other technology over the lifespan of a PACS solution as a means of extending the usable life of the solution or adding new capabilities.	12 – 36 weeks
Software/Firmware Refresh	Update software and firmware to accommodate manufacturer improvements, bug fixes, or to remain compliant with the latest policies and standards.	15 minutes per device (reader or controller)

Figure 105: Operate and Maintain Phase Sample Activities

## 10.2. Physical Access Architecture and Design

In order to align with the ICAM segment architecture, agencies should design and implement an enterprise-level, modernized PACS. This approach presents agencies with an opportunity to increase efficiency, improve interoperability, and reduce costs. As an agency designs its modernized physical access architecture, it should address the capabilities included in the ICAM Services Framework (Section 3.2.4), as well as the existing PACS infrastructure. Furthermore, as part of this process, an agency should take steps to ensure that its design does not incorporate any elements that could impair its ability to authenticate other agencies' PIV cards, as described in Section 8.4.

This section provides a solution architecture diagram, discusses the components that comprise a modernized PACS, and introduces common characteristics that an agency should consider when designing its target state PACS. This section is targeted largely at enterprise and solution architects who are responsible for the design of an agency's upgrade efforts. The information and guidance provided in this section is intended to provide answers to several common PACS architecture and design questions, including:

- What does a modernized PACS infrastructure, compliant with the ICAM target state, look like?
- What are the components of a modernized PACS infrastructure, and how do they support achievement of the ICAM target state?
- What common characteristics should I consider when designing a PACS solution?

### 10.2.1. Solution Architecture

The ICAM segment architecture describes the PACS target state as agencies establishing an enterprise approach to managing physical access that links individual PACS via a federated network wherever possible. There are a number of ways to achieve this goal; however agencies should implement a configuration that is cost-effective and aligns with their needs and organizational environment. Additionally, physical security staff should collaborate with IT staff to gain consensus on an appropriate system design, since the Office of the Chief Information Officer (OCIO) has oversight responsibility for ensuring that all IT systems meet relevant requirements. This section provides a high-level example of a solution architecture that encompasses the necessary elements of a modernized PACS. These components represent generic products and are not aligned with a particular vendor or solution offering. Note that several of the items on the diagram, such as Certification Authority (CA) and Authoritative Sources, are common infrastructure components within an agency's overall ICAM infrastructure. Many of these components are also depicted in the solution architecture for the LACS in Section 11.2.1; however, they should not be viewed as separate and independent for the two systems but

rather as interconnecting. Figure 106 illustrates an enterprise PACS solution model that incorporates the concepts described in the target state.

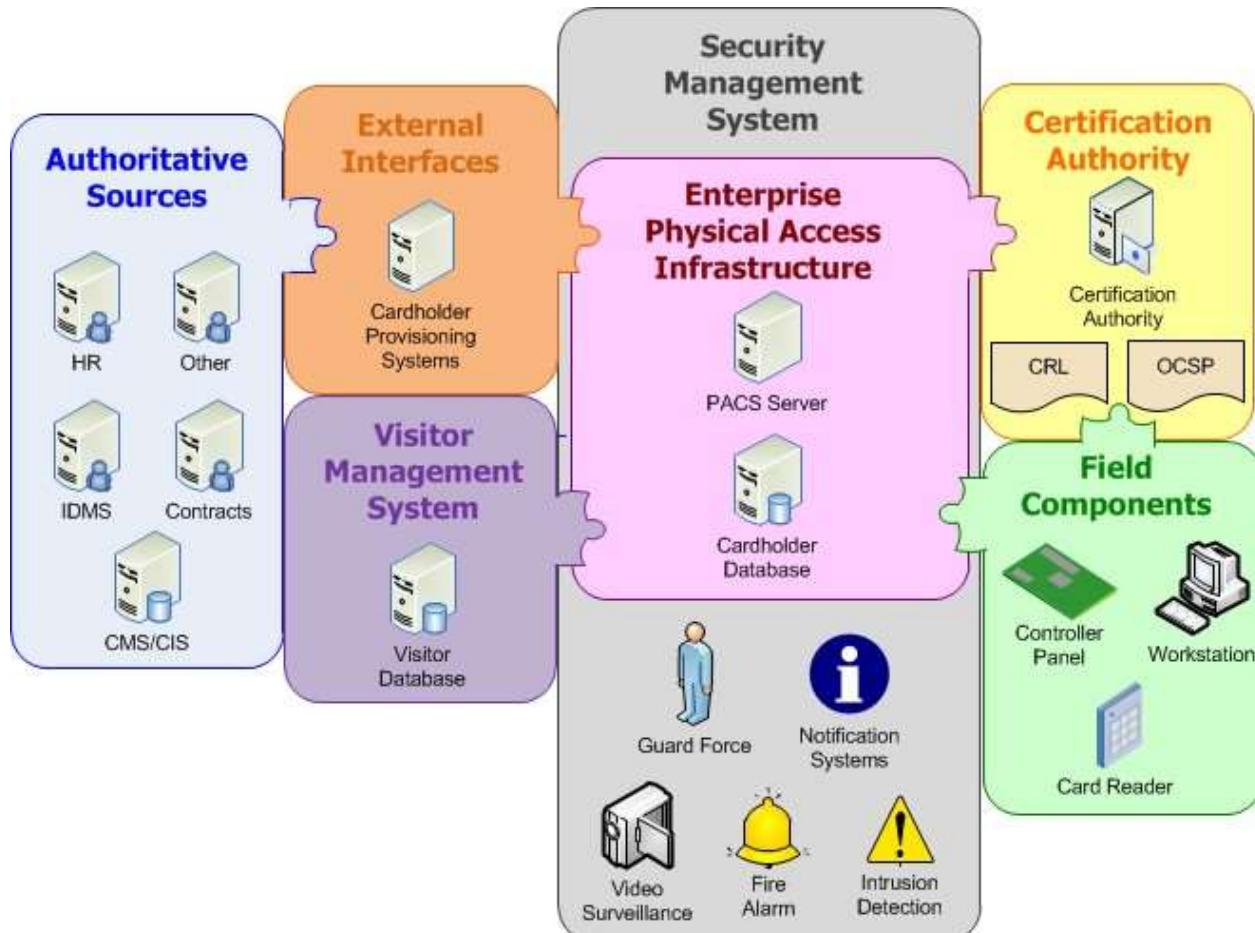


Figure 106: Physical Access Solution Architecture

The diagram represents the target state, in which the PACS is no longer a standalone system; rather it links into numerous components and provides enterprise physical access authentication and authorization services. The Enterprise Physical Access Infrastructure represents the main services of the PACS and includes critical services like central data storage, monitoring, and control over all of the other components of that system. The enterprise PACS is depicted as a piece of the larger Security Management System (SMS), which has interconnections with other physical security elements such as video surveillance systems, intrusion detection, and fire alarms. The Enterprise Physical Access Infrastructure relies on external interfaces to connect with the authoritative sources where relevant user and credential information is stored and maintained. The Enterprise Physical Access Infrastructure administers a variety of field components, which are distributed system components that directly control access at the local level. It is anticipated that many agencies will have numerous field components from multiple vendors. In the target state, these devices and subsystems do not necessarily need to be replaced with a single vendor product, but should be linked to an agency's PACS services at the enterprise level. The diagram depicts an electronic VMS that is integrated with the Enterprise Physical Access Infrastructure. The VMS is an optional element of the physical access solution architecture; however, incorporating an electronic VMS into the enterprise PACS solution may

enable additional automation and cost savings. Some agencies may implement a PACS solution in which visitor management is included as a part of the overall system or an agency may choose to develop an independent VMS.

## FAQ

### If the PACS server is hosted by the enterprise and not at my site, how do I know that it is secure?

When PACS services are provided at the enterprise-level, servers are hosted at high-security areas with redundant information back-ups, high network availability, and robust disaster recovery protocols. The Service Level Agreement (SLA) for hosting of the system details the security controls and procedures in place. The hosting facility is also subject to Federal Information Security Management Act (FISMA) requirements to ensure adherence with applicable security requirements.



## 10.2.2. Solution Components

Figure 106 illustrates the various components that comprise an enterprise PACS solution. This section identifies those individual solution components and describes the functionality of each. Section 10.2.2.1 discusses the components that make up the Enterprise Physical Access Infrastructure, Sections 10.2.2.2 through 10.2.2.4 make up the field components, Section 10.2.2.5 provides an example of a component commonly included in external interfaces.

### 10.2.2.1. PACS Server

The PACS server is an administrative tool used by the PACS operator to provision and de-provision access to a variety of physical resources, control and configure downstream access control and alarm devices in the system, journal all system activities, and execute security-related decisions. The PACS server is also typically the primary data source where a cardholder is enrolled or registered in the Cardholder Database (depicted separately in Figure 106). In the target state architecture, identity and credential data associated with the cardholder should be provisioned to the cardholder database from authoritative enterprise data sources. The server downloads cardholder record data and associated privileges to the relevant access control panel and serves as an access decision resource when a field panel is presented a PIV card that is not currently stored in the panel database.

In a modernized PACS, the server communicates with the federated PKI infrastructure to offer a high level of trust in the identity assertion made by the person presenting the PIV card to the system. Additionally, PACS servers in the target state become consumers of a user's authoritative digital identity and PIV card information, which is provisioned from the agency's authoritative data sources.

## Implementation Tip

PACS servers can be managed by the agency at the enterprise level or by a service provider using cloud computing approaches. This model, called Security-as-a-Service, involves a technology provider hosting the security management applications on behalf of the end user. This arrangement allows agencies to leverage the cost savings, flexibility, and ease-of-deployment and eliminate the server and storage infrastructure at each individual site.



#### **10.2.2.2. Workstation**

The workstation is subordinate to the PACS Server and provides administrative functions to manage the PACS. In an enterprise network with a network-centric PACS, a workstation can be placed where needed and connected to the network in order to operate in conjunction with the PACS Server. Some of the typical functions controlled at a workstation are adding or removing cardholders and credentials from the PACS, downloading cardholder data, and setting access levels and functions of the field components. They may leverage thin clients using browser interfaces only, or use thick clients that use locally installed software.

##### **Implementation Tip**

Close coordination with network administrators is required to successfully integrate workstations as part of the PACS solution. PACS implementers should coordinate with IT resources to help determine workstation location and set up network connectivity.



#### **10.2.2.3. Controller/Panel**

The controller/panel makes access control decisions by comparing cardholder data sent by the reader with the cardholder data stored locally. The controller/panel contains a number of cardholder records, usually one per cardholder, which typically consists of a cardholder record number, a cardholder photograph, a unique identifier (card number), a list of authorized access points, and a time when access is authorized. The decision to grant access is based upon successfully matching the cardholder data with an existing record and its associated access privileges.

In a modernized PACS, once the controller/panel determines that the data on the PIV card matches the information in the database, it authenticates<sup>224</sup> the cardholder using the various authentication mechanisms found on the PIV card (e.g., PKI certificates, biometrics). The decision result is sent to the access control server for display and archiving. When the controller/panel makes an access grant decision, it sends a signal to release the door locking mechanism and disarm associated alarm sensors, such as door position monitors. Access control data is stored locally so that the controller/panel can continue to operate during periods when panel-server communication is interrupted. Controller/panels also have battery backups for operation during times of power loss.

There are some PACS that operate without a controller/panel by connecting a variety of standard reader types directly to a network through Internet Protocol (IP) bridges. This type of architecture might typically be found in PACS architectures leveraging a Security-as-a-Service model.

#### **10.2.2.4. Card Reader**

A card reader is the device located at an access point to provide access control. A card reader may support communication with either the contact or contactless interface of the card, or in some cases support both. A target state card reader should support bi-directional communications with the system, processing the data and instructions from the card, sending the data to the

<sup>224</sup> Authentication may be performed in conjunction with other PACS components.

associated control panel, and receiving data and instructions back from the control panel within an acceptable time frame.

**Implementation Tip**

Ensure that environmental factors are taken into consideration when designing your agency's PACS, particularly when deciding what types of card readers to purchase. Environmental factors, such as exposure to weather conditions, can impact the successful use of a card reader through the contact mode. An agency may need to deploy additional equipment, such as a protective cover, in these scenarios.



In the target state, it is likely that a card reader will need to read and communicate various data from the card in order to support transactions that use multiple authentication modes, including Cardholder Unique Identifier (CHUID) and PKI authentication. There are a number of card readers that are approved by the FIPS 201 Evaluation Program<sup>225</sup> that can support various transaction types in the target state. As an agency selects card readers for purchase, it is important to ensure that the card reader chosen is capable of supporting the desired PIV card authentication mechanisms at a particular access point, as not all card readers support all authentication mechanisms.

**Implementation Tip**

When selecting to use an “edge reader” or “Internet Protocol (IP) reader,” it is suggested that agencies choose the two part variety. This ensures that the controller function and IP port are located on the secure side of the wall, opposite the reader.



#### **10.2.2.5. Cardholder Provisioning System**

A Cardholder Provisioning System is an example of an external interface that integrates between a PACS and an agency's authoritative identity source(s) for the purpose of provisioning user accounts and their associated card data to the PACS. The use of a Cardholder Provisioning System represents a shift in the target state, where the PACS is a consumer of identity and PIV credential information. As such, there are a number of approaches that an agency can take to provide this functionality within its PACS architecture. These are discussed in greater detail in Section 10.3.1.

#### **10.2.3. Common Design Characteristics**

In addition to identifying a solution architecture and the supporting components, agencies should have an understanding of the common design characteristics necessary to successfully implement a modernized PACS. Figure 107 describes, at a high level, the characteristics that agencies should consider when designing a PACS solution that meets the target state. It is important for agencies to make design decisions that are in line with their specific needs and relevant policy.

<sup>225</sup> For more information on the different types of card readers, refer to the [FIPS 201 Evaluation Program](#).

PACS Characteristic ID	PACS Solution Characteristics
<b>PACS 1</b>	Easily integrated into a centralized management and control system that combines access control with intrusion detection, event monitoring, and integrated video capabilities.
<b>PACS 2</b>	Supports access to its functionality through both a web-based native user interface and a programmatic application programming interface (API).
<b>PACS 3</b>	Capable of validating the PIV card in accordance with the authentication mechanisms defined in SP 800-116.
<b>PACS 4</b>	Supports validation of other credential types, as necessary, during migration stages to full PIV card implementation for physical access.
<b>PACS 5</b>	Provides middleware system(s) that seamlessly integrate the path validation of certificates required by FIPS 201.
<b>PACS 6</b>	Uses path validation to completely authenticate and validate the security relevant data objects within the PIV card and PIV-Interoperable (PIV-I) cards.
<b>PACS 7</b>	Provides system components that adhere to the Backend Attribute Exchange (BAE) Specification and are IPv6 addressable.
<b>PACS 8</b>	Provides a system controller that, with algorithms, will enforce all the rule checks prior to allowing access.
<b>PACS 9</b>	Adheres to the protocols and architecture recommended in Chapter 10 Initiative 7: Modernization of PACS, requirements.
<b>PACS 10</b>	Uses PKI certificates as a basis for system administration and visitor management between trusted organizations.
<b>PACS 11</b>	Included within the Federal Information Security Management Act (FISMA) Inventory of an organization.
<b>PACS 12</b>	Allows decision making logic to be local, rapid, located within the secure perimeter, and not dependent on a remote server.
<b>PACS 13</b>	Federated or synchronized with other identity stores that are used for logical access and other aspects of personnel management.
<b>PACS 14</b>	Consume and process credentials that were produced by authorities independent of the PACS, such as PIV, PIV-I, and facility access cards.
<b>PACS 15</b>	Read and extract the full Cardholder Unique Identifier (CHUID) from the PIV card, and recognize it within the controllers and server software.
<b>PACS 16</b>	Allows the PACS server authorization database to update access changes for affected user records in local PACS panels.
<b>PACS 17</b>	Provides a personal identification number (PIN) entry method to the PIV card.
<b>PACS 18</b>	Requests and receives the PIV Authentication Certificate from the card, sends data to external PKI infrastructure (Online Certificate Status Protocol [OCSP], Server-based Certificate Validation Protocol [SCVP], Certificate Revocation List [CRL]), and if valid, send to PACS server authorization database.
<b>PACS 19</b>	Allows the PACS authorization database to integrate to external PKI infrastructure and perform automatic validation of all registered PIV Authentication Certificates.
<b>PACS 20</b>	Continually checks and updates credential status after the cardholder's credentials are determined as valid and enrolled in a PACS.
<b>PACS 21</b>	Provides PACS server software and associated downstream hardware (controllers) that are web services-based in order to allow for more efficient customization to end-user requirements and integration into middleware and external systems components, including Logical Access Control Systems (LACS).
<b>PACS 22</b>	Provides a capability to automatically change access level requirements for doors and portals according to preset Threat Condition levels.

PACS Characteristic ID	PACS Solution Characteristics
<b>PACS 23</b>	Provides a capability to verify against an internal or integrated external watch list <sup>226</sup> database when a card is presented to a reader for access. Ideally, the watch list should be stored both in the PACS server and controller.
<b>PACS 24</b>	Provides a capability to compile reports with data from access records.

Figure 107: Common PACS Design Characteristics

### 10.3. Physical Access Technical Implementation

Implementing a modernized PACS in alignment with the ICAM segment architecture introduces several system changes to traditional PACS approaches and capabilities. This section discusses two areas that represent the biggest departure from the current state: automated provisioning and enabling the use of PIV card authentication mechanisms per SP 800-116. This section is targeted largely at those individuals responsible for implementing and overseeing the technical execution of an agency's PACS modernization efforts. The information presented in this section is intended to assist agencies in providing answers to several common questions related to the technical aspects of a PACS implementation, including:

- What automated provisioning approaches are available for use in a PACS?
- What are the benefits and limitations of the different PIV card authentication mechanism for PACS?

Lesson Learned	
Direct guidance and "how-to" information will help implementers and provide consistency throughout the agency's PACS modernization effort. For example, a large agency created a "field guide" to help its bureaus/components incorporate PIV-enabled solutions into their logical and physical access controls. It provides information on the tasks for preparation, the resources and tools that have been successfully used in implementation, and gives guidance on how the bureaus/components may best manage and execute the implementation.	

#### 10.3.1. Automated Provisioning to PACS

Automated provisioning to PACS has developed into an important aspect of consideration for those who manage and maintain those systems. Automated provisioning of an individual's digital identity into a PACS helps to address system resource management issues and several overarching security concerns including, but not limited to:

- Ensuring that an individual's user record is based on authoritative identity data;
- Providing system administrators the ability to better manage their PACS databases and keep records current; and
- Allowing for centralized and automatic de-provisioning when an individual separates from an agency.

Traditionally, the data elements needed to create an authorized cardholder within a PACS database have been entered manually. In addition, the procedures for determining how someone

<sup>226</sup> Watch list is a general term used within the physical security community to refer to a list of individuals to whom access should not be granted.

is granted access are disparate across the government and even within a single agency. This has led to the realization that a set of standard data elements within a digital identity should be available to the PACS for the creation of a cardholder profile. An agency will benefit from the standardization that results from having the PACS populated with an established digital identity from authoritative source(s). Additionally, the development and deployment of centralized automated provisioning capabilities support achievement of Transition Activity 7.4, as discussed in Section 5.2.2.3.

### Lesson Learned

Take your existing PACS infrastructure into account when selecting an automated provisioning approach. The Department of Health and Human Services (HHS) established the enterprise Credentialing Provisioning and Gateway System, which interconnects the HHS Smart Card Management System to the many stove-piped, proprietary PACS installed throughout HHS. HHS has been able to quickly realize the benefits of automated provisioning while reducing system development costs by leveraging their existing PACS to the maximum extent possible.



The target state of a modernized PACS is to realize a singular digital identity, which can be added to, modified, and deleted by one or more authoritative data source, as determined by each agency. The complexity of the digital identity is dependent upon the size of the agency, the facilities to be covered, and existing architecture in place to support the effort. The target state should be supportive of a single digital identity being created and maintained at the agency level for distributed cross-system use, a concept commonly referred to in the physical security community as —single enrollment, many uses.¶

Figure 108 compares commonly available automated provisioning approaches.

Approach	Description	Benefits	Limitations
<b>Integrated Provisioning Capability</b>	A fully automated provisioning capability that leverages a real time connector using open standards (i.e., eXtensible Markup Language [XML]) and enables two-way communication between the PACS and authoritative sources.	<ul style="list-style-type: none"> <li>• Significantly less level of effort for enrollment to PACS</li> <li>• Minimized development costs</li> <li>• Standardized naming conventions</li> <li>• Reporting capability</li> <li>• Works well if agency has a variety of vendors</li> <li>• More options for federation of PACS control into the enterprise</li> <li>• Security personnel have assurance that data integrity is maintained across the entire landscape of PACS</li> <li>• Provides the connected PACS with the most current cardholder account information, including access privileges</li> <li>• Provides a robust and flexible, oftentimes web-based, interface that can access data from the connected PACS in a seamless and intuitive fashion</li> <li>• Can function as a central point of revocation of cardholders' accounts, further increasing an</li> </ul>	<ul style="list-style-type: none"> <li>• Often reliant on software vendor after installation for maintenance</li> <li>• Must maintain connectivity through real-time connectors or system interfaces to update systems</li> <li>• Upgrading software can be costly</li> </ul>

Approach	Description	Benefits	Limitations
		efficient security posture of the organization <ul style="list-style-type: none"> <li>• Maintains connections on a near real-time basis using resource connectors or service interfaces</li> </ul>	
<b>Vendor Interfaces</b>	Leverages custom scripts written by a vendor using application programming interfaces (API) and software development kits (SDKs).	<ul style="list-style-type: none"> <li>• Allows data sharing between two systems on a long-term basis</li> <li>• Utilizes existing systems SDKs and vendor expertise</li> <li>• May be more open/flexible than batch processing</li> <li>• Pre-set schedules/time intervals for the transfer of new data/enrollments</li> <li>• Higher level of quality assurance with data integrity during data transfer than offered in the single-use option</li> <li>• Many current PACS and some legacy systems provide this option</li> <li>• Properly developed scripts are typically functional across a broad range of software versions</li> </ul>	<ul style="list-style-type: none"> <li>• Incomplete mapping of cardholder information</li> <li>• Real time operation depends on vendor</li> <li>• Depending on vendor may require heavy investment</li> <li>• Multiple systems would increase complexity in cross-system cardholder record integrity</li> <li>• May create inconsistency among systems which can negatively impact security</li> </ul>
<b>Batch Processes</b>	Leverages a single-use scripted data transfer.	<ul style="list-style-type: none"> <li>• Is easy to implement when transitioning from a legacy PACS to a new access control system</li> <li>• Can utilize existing custom infrastructure</li> <li>• Minimized effort through targeted scripts based on requirements</li> <li>• More flexible to meet particular agency requirements or unique existing infrastructure</li> </ul>	<ul style="list-style-type: none"> <li>• May not completely eliminate manual operations as part of provisioning process</li> <li>• Complexity may increase database management issues</li> <li>• Possible difficulty in validating data transfer</li> <li>• Generally used for one-time data transfer</li> <li>• No recurring data transfer as data changes in the authoritative source</li> <li>• Does not guarantee the quality and uniqueness of imported cardholder accounts</li> <li>• A scripted process is generally only functional within a small range of software versions</li> <li>• There can be disconnects between the individuals who build the data transfer script and those who are familiar with the PACS system itself</li> <li>• A significant time investment may be required to ensure cardholder accounts properly reflect the individuals they are</li> </ul>

**Figure 108: Comparison of Automated Provisioning Techniques**

### 10.3.2. Common Physical Access Scenarios

A primary focus of the PACS modernization implementation is the capability for agency PACS to electronically authenticate the PIV card in accordance with mechanisms specified in SP 800-116<sup>227</sup> and as determined based upon facility risk assessments.<sup>228</sup> Using the PIV card for physical access offers an agency the opportunity to align with the ICAM segment architecture and realize the enhanced security benefits of the authentication mechanisms on the PIV card. For example, agencies can achieve a level of trust in the claimed identity of the person presenting the PIV card as a result of authentication and validation processes.

This section introduces each of the allowable PIV card authentication mechanisms for PACS, discusses where it is appropriate to use each, and outlines the benefits and limitations associated with each. An agency PACS cannot be considered PIV-enabled if it is not leveraging the authentication mechanisms contained in this section in accordance with the guidance in SP 800-116.<sup>229</sup> Specifically, use of the PIV card with legacy technologies (e.g., proximity antennas, magnetic stripe, barcode, etc.) does not meet the intent of HSPD-12, the ICAM target state, and this guidance. As its PACS implementations mature, it is also recommended that an agency move towards the stronger authentication mechanisms, such as cryptographic authentication using the PIV Authentication Key as described in Section 10.3.2.3.

#### 10.3.2.1. CHUID Authentication

The CHUID is a mandatory data object on the PIV card, which includes the Federal Agency Smart Credential Number (FASC-N) element that uniquely identifies the card. The CHUID also contains a 16- or 128-bit binary field called the Global Unique Identifier (GUID) that stores the Universally Unique Identifier (UUID), which is leveraged to identify PIV-I cards. The CHUID is a free-read data object that is available on the contactless interface of the PIV card. Of the available PIV card authentication mechanisms, it is more closely aligned with legacy PACS operations, which read and compare a number from the card against the PACS user database; however, CHUID is the weakest of the PIV authentication mechanisms.

As indicated in SP 800-116, CHUID validation should minimally be based on reading and matching the complete FASC-N. It is important that a PACS be able to read at least the full FASC-N data subset to maintain uniqueness and prevent data collisions. The CHUID numbering scheme is standardized by FIPS 201 and can be counterfeited easily. CHUID validation based on a FASC-N read provides no protection against counterfeiting and should only be used in PACS that are in the initial stages of transitioning to the target state.

In the target state, use of the CHUID mechanism involves reading the full CHUID and validating the signed data object and the certificate used to sign the CHUID. This process allows the PACS to detect modifications or alterations to a CHUID, protecting against counterfeiting. Even using this approach, the PACS is still vulnerable to cloned CHUID data objects. For this reason, CHUID validation is considered a zero-factor authentication method when used alone. It should

---

<sup>227</sup> [SP 800-116](#)

<sup>228</sup> The process for conducting facility risk assessments is discussed further in Section 10.1.2.

<sup>229</sup> Per [M-10-15](#)

only be used in the target state for areas identified as having extremely low risk following a careful facility risk assessment.<sup>230</sup>

### Implementation Tip

Educate your users on proper PIV card storage and handling. Improper storage or handling can break the contactless interface on the PIV card, preventing use of certain authentication mechanisms, such as the Cardholder Unique Identifier (CHUID), in your PACS and driving up program costs for replacing damaged PIV cards. Failing to properly store the PIV card in its electromagnetically opaque holder when not in use can also increase security risks for the skimming of card data.



Based on the benefits and limitations listed in Figure 109 and the recommendations found in SP 800-116, agencies may use CHUID authentication at access points separating two areas at the same impact level, either Controlled or Limited. Agencies may also use the CHUID authentication mechanism, when paired with a visual (VIS) authentication mechanism, at access points between Unrestricted and Controlled areas.<sup>231</sup>

Benefits	Limitations
<ul style="list-style-type: none"> <li>If the CHUID signature verification is performed, the PACS can be sure the CHUID came from a valid issuer and it has not been altered.</li> <li>The partial CHUID read presents the simplest implementation alternative when migrating from legacy PACS.</li> <li>In comparison with other mechanisms, the CHUID offers the smallest data read on the PIV card.</li> </ul>	<ul style="list-style-type: none"> <li>The CHUID is a free read object on the PIV card; therefore it can be cloned.</li> <li>Because of the risk of CHUID counterfeiting or cloning, the CHUID authentication mechanism, used in isolation, provides a confidence level that is comparable to proximity cards in widespread use today.</li> <li>To achieve single-factor authentication with CHUID, the relying parties must validate the signature on the CHUID.</li> <li>Legacy technology cannot always accurately read the full CHUID, which can result in data collisions.</li> <li>The CHUID with signature validation authentication method can only be used to enter Controlled areas.</li> <li>There is no standard for checking revocation status of a CHUID.</li> <li>CHUID authentication can be vulnerable to electronic cloning, skimming, sniffing, and use of unreported lost or stolen PIV card (until card is revoked).</li> </ul>

Figure 109: Benefits and Limitations of CHUID Authentication in PACS

#### 10.3.2.2. CAK Authentication

CAK authentication involves verifying a claimed identity through validation of a digital certificate on the PIV card issued by a trusted CA.

The CAK method is characterized by the following:

- It may be used on either the contact or contactless interface, which is desirable in many PACS implementations;
- It does not require the entry of the PIN;

<sup>230</sup> Additionally, [SP 800-116](#) states that “it is strongly recommended that agencies use the PKI or asymmetric challenge/response methods instead of the CHUID.”

<sup>231</sup> A description of the area types mentioned in this section can be found in Section 10.1.2.

- It allows the PACS to determine the validity of certificates in real time or by pre-validating the certificates and storing the information in a cache;
- It leverages asymmetric key cryptography,<sup>232</sup> to perform certificate validation;
- It is an optional certificate,<sup>233</sup> and may not be present on all agency PIV cards, which could impact interoperability; and
- It provides single factor authentication, and thus is appropriate only for access to Controlled areas, unless used in combination with another authentication factor.

The CAK authentication of the PIV card represents a stronger alternative than standard CHUID-based authentication while meeting throughput expectations at facility access points. Furthermore, SP 800-116 recommends that the asymmetric CAK authentication mechanism be used instead of the CHUID authentication mechanism to the greatest extent practicable. Based on the benefits and limitations of CAK authentication, agencies may use this mechanism at access control points between Unrestricted and Controlled areas. When used in combination with attended biometric authentication, CAK authentication provides three-factor authentication and can be used at access control points between Limited and Exclusion areas.

Benefits	Limitations
<ul style="list-style-type: none"> <li>• CAK provides a higher assurance mechanism while still retaining the contactless capability.</li> <li>• Cached certificate validation can provide rapid authentication with an inherently stronger validation compared to a standard CHUID read.</li> <li>• Real-time certificate validation can provide strong authentication as it only relies upon the refresh rate of the published Certificate Revocation List (CRL).</li> <li>• A personal identification number (PIN) match to a system on the PACS may provide additional security to CAK authentication (Note: This is not equivalent to a PIN activation on the PIV card).</li> </ul>	<ul style="list-style-type: none"> <li>• Certificate validation technology can be marginally slower than a CHUID validation technology dependent on product selection.</li> <li>• Cached certificate results do not validate certificates in real-time, certificate status is based on PACS server to CRL refresh and server to panel refresh timeframes.</li> <li>• Real-time certificate validation technology can require a longer read time when compared to a standard CHUID or cached certificate read.</li> <li>• Not a native capability of many existing and available PACS systems, resulting in additional implementation costs and challenges.</li> <li>• The CAK authenticates the PIV card, not the individual; therefore it provides only some assurance in the identity of the individual.</li> <li>• CAK authentication can be vulnerable to social engineering and use of unreported lost or stolen PIV card (until card is revoked).</li> </ul>

Figure 110: Benefits and Limitation of CAK Authentication in PACS

#### 10.3.2.3. PKI Authentication

PKI authentication involves verifying a claimed identity through validation of a digital certificate on the PIV card issued by a trusted CA. For the PIV card, this may be accomplished using the PIV Authentication Key.

The PIV Authentication Key method is characterized by the following:

---

<sup>232</sup> While outside of the scope of this discussion, NIST does permit the CAK on a specific card to be symmetric. Agencies should note, however, that this approach is based upon use of a shared secret and is not considered an acceptable approach for using the CAK validation mechanism in the ICAM target state due to security, interoperability, and infrastructure cost concerns.

<sup>233</sup> Discussion is based upon current requirements found in [FIPS 201-1](#). It is anticipated that the CAK will be made mandatory in future revisions of the standard; however, PIV cards without the CAK will likely be in circulation following the anticipated revision.

- It provides two-factor authentication, since the cardholder must enter a PIN to unlock the card in order to successfully authenticate;
- It is a mandatory credential on the PIV card, and thus will be available on PIV cards of visitors from other agencies;
- Is accessible over the contact interface;
- It requires the PACS to determine the validity of certificates when an individual presents his card to a card reader;<sup>234</sup> and
- It may be used for authentication to areas up to and including Exclusion areas.

The PKI validation of the PIV card represents a stronger alternative than standard CHUID-based authentication while meeting throughput expectations at facility access points. As noted in the limitations below, PKI validation has traditionally posed challenges related to transaction speed and support within commercially-available vendor products; however, ongoing advances in technology and processes are making PKI authentication more viable within an operational PACS environment.

Based on the stronger LOA provided by PKI authentication, agencies may use this mechanism at access control points between Limited and Exclusion areas, the most sensitive access points. PKI authentication is the only PIV authentication mechanism allowed between these two areas that does not require an attended transaction. It is also an acceptable authentication mechanism at lower security areas.

Benefits	Limitations
<ul style="list-style-type: none"> <li>• Cached certificate validation can provide rapid authentication with an inherently stronger validation compared to a standard CHUID read.</li> <li>• Real-time certificate validation can provide strong authentication as it only relies upon the refresh rate of the published Certificate Revocation List (CRL).</li> </ul>	<ul style="list-style-type: none"> <li>• Certificate validation technology can be marginally slower than a CHUID validation technology dependent on product selection, real-time certificate validation technology can require a longer read time when compared to a standard CHUID or cached certificate read.</li> <li>• Cached certificate results do not validate certificates in real-time, certificate status is based on PACS server to CRL refresh and server to panel refresh timeframes.</li> <li>• Not a native capability of many existing and available PACS systems, resulting in additional implementation costs and challenges.</li> <li>• PKI authentication can be vulnerable to social engineering.</li> </ul>

Figure 111: Benefits and Limitations of PKI Authentication in PACS

#### 10.3.2.4. Biometric Authentication

Biometric authentication verifies an individual's identity by comparing the reference biometric template on the PIV card with the sample biometric template provided at the time of the transaction. This verification exchange occurs off-card, in the reader, or on a server. Every PIV card contains two fingerprint templates of the card holder in a standardized data format that is described in NIST SP 800-76.<sup>235</sup> Because these templates are standardized, they provide interoperability across a federated environment. As with several of the other objects on the card,

---

<sup>234</sup> Per [SP 800-116](#) and [FIPS 201](#), validation may be done on-line in real-time, or it may be implemented by pre-validating the certificates and caching the results.

<sup>235</sup> [SP 800-76](#), Biometric Data Specification for Personal Identity Verification, NIST, January 2007. [SP 800-76]

the biometric on the PIV card is signed by the issuer. It is recommended that the PACS verify the digital signature on the biometric template data object to verify the authenticity of the biometric.

PACS readers that incorporate biometric technology, supporting software, and hardware logic are commercially available and utilized across multiple federal agencies. As a general premise, biometric access points provide a higher level of authentication at the expense of a slight reduction in throughput due to the additional time required for an individual to provide a biometric sample for comparison in addition to reading the PIV card.

Based on the benefits and limitations listed below, an agency may use biometric authentication at access points between Controlled and Limited areas. When biometric authentication is performed in the presence of an attendant (Attended Biometric authentication [BIO-A]), it mitigates the risk that the user is presenting a fake card or fake or synthetic fingerprints that could falsely be accepted by the reader. For this reason, BIO-A may be used at access control points between Limited and Exclusion areas.

Benefits	Limitations
<ul style="list-style-type: none"> <li>• The biometric on the PIV card is signed by the issuer, so the authenticity of the biometric can be validated by the PACS.</li> <li>• Current biometric technology demonstrates low crossover error rates in NIST Minutia Exchange (MINEX) testing.</li> <li>• The 1:1 biometric match represents the closest cardholder to PIV card validation possible.</li> <li>• Provides mitigation against fraudulent authentication attempts with synthetic fingerprints when conducted in Attended Biometric authentication (BIO-A) mode.</li> </ul>	<ul style="list-style-type: none"> <li>• Biometric authentication cannot be used on the contactless interface.</li> <li>• This authentication mechanism by itself does not include authentication of the PIV card.</li> <li>• Slower transaction time due to requirement for use of contact interface and user PIN entry.</li> <li>• Biometric readers may not be viable at external access points, where environmental conditions can cause rapid equipment deterioration.</li> <li>• Biometric authentication can be vulnerable to biometric impersonation.</li> </ul>

**Figure 112: Benefits and Limitations of Biometric Authentication in PACS**

FIPS 201 requires the use of the contact interface and PIN entry to access the reference biometric fingerprint data stored on the PIV card.<sup>236</sup> This requirement presents a challenge in physical access environments where use of the contactless interface is necessary to support high throughput requirements (i.e., the time required to insert the PIV card into a card reader and enter the PIN would create a bottleneck at the access point). In these scenarios, there are two alternate approaches that an agency may consider in order to enable biometric authentication without requiring PIN entry.

- **Biometric template retention.** In this approach, the biometric template is retained in a site-based biometric system with a local database of biometric objects read from PIV cards. The biometric template can be obtained by reading it from the card the first time the card is used at the site, collecting it in a separate session, or provisioning the data from an authoritative data source that contains biometric samples. This approach is permissible because FIPS 201 does not restrict the length of time that an application may retain the biometric object from the PIV card; however, it is critical to note that the biometric object must be checked against the CHUID expiration date on the PIV card, per SP 800-116. When a PIV card is presented for biometric authentication, the CHUID is read from the PIV card, and the FASC-N from the CHUID is used to look up the

<sup>236</sup> Discussion is based upon current requirements found in [FIPS 201-1](#). It is anticipated that additional options for performing biometric authentication using the contactless interface will be incorporated as they become available and are deemed viable for ICAM implementation.

biometric object in the local database; the expiration date from the CHUID is then checked to make sure the biometric object is still valid. Following successful validation, the cardholder's live biometric sample is compared against the biometric object stored on the local database.

- **Biometric “match-on-card.”** In this approach, the fingerprint templates stored on the card are used for identity verification along with the optional on-card biometric comparison algorithm. The cardholder presents their card to a contactless biometric reader and their finger to the biometric scanner. The biometric data from the biometric scanner is sent to the PIV card for comparison by the ICC and an indication of success is sent to the card reader. This response includes information that allows the card reader to authenticate without the stored minutiae data ever leaving the card. Using the on-card comparison option to perform biometric authentication can be desirable in high throughput areas because it leverages a contactless interface and does not require PIN entry. However, this operation requires additional security measures to ensure the transaction data is encrypted and securely transmitted, which can impact performance. If an agency chooses to implement the match-on-card biometric comparison option, it must be implemented as defined in SP 800-73<sup>237</sup> and SP 800-76.<sup>238</sup>

Another potential challenge for using biometric authentication is environments where use of the fingerprint biometric modality is not feasible, such as instances where fingerprints are unavailable for a significant portion of the user population or environmental conditions at the access point do not allow for an acceptable fingerprint capture. In these cases, an agency may wish to implement an alternate biometric modality, such as iris. It is recommended that an agency only pursue this approach in the extremely rare case where authentication cannot be supported by another PIV authentication mechanism, as this approach incurs additional administration costs and effort to collect, manage, and protect additional biometric data. Because this approach requires locally-enrolled data to successfully complete the access transaction, it also significantly limits interoperability, which is a key objective of the ICAM segment architecture.

#### **10.3.2.5. Multi-factor Authentication**

As noted in the ICAM segment architecture, multi-factor authentication involves a combination of 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 comparison with biometric data stored on the card. Several of the PIV card authentication mechanisms, including reading a signed object from the card or performing challenge/response authentication with the card, only provide validation of possession of the PIV card (i.e., something you have). Likewise, biometric authentication also only provides a single factor of authentication (i.e., something you are). To overcome the drawbacks and limitations of each individual factor of authentication, an agency may choose to combine two or more authentication mechanisms (e.g., PKI certificate and biometric) for the same transaction to meet facility area access requirements. As defined in SP 800-116, two-factor authentication is specified for access to Limited areas, and three-factor authentication is specified for access to

---

<sup>237</sup> [SP 800-73](#)

<sup>238</sup> [SP 800-76](#)

Exclusion areas. Multi-factor authentication mechanisms should be commonly leveraged in areas that require higher levels of access control.

## **10.4. Local Facility Access**

HSPD-12 requires the use of identification that meets federal standards (i.e., the PIV card) in order to gain physical access to federally controlled facilities; however, there are certain user populations that need physical access but for whom issuance of the PIV card is not required (e.g., individuals that require access for less than six months, non-federal building tenants, interns, and visiting scientists, etc.). These individuals for whom a PIV card is not required should be appropriately credentialed and validated in order to maintain adequate security for the facility.

To achieve alignment with the ICAM target state for populations that will not receive a PIV card, agencies should establish a common approach for issuing and accepting credentials for local facility access, where appropriate. It is recommended that an agency pursue an option that utilizes electronic authentication mechanisms and leverages the trust framework and PIV card infrastructure. Examples include accepting PIV-I cards from valid issuers or issuing individuals a card using approved card stock (ACS) with a trusted PKI certificate. Section 8.1.4.2 provides additional information on non-PIV credential types that could be applied for local facility access scenarios.

An agency may pursue an agency-specific approach if it is deemed the most cost effective based upon a cost/benefit analysis. Decisions around which user populations should receive a local facility access card may be made at the bureau/component or site level. In both of these instances, agencies are expected to move away from multiple, inconsistent credentials for these populations and leverage PIV infrastructure.

### **ROI**

Moving toward acceptance of PIV-I cards and local facility access cards that are interoperable with an agency's existing PIV infrastructure not only increases security for non-PIV populations, but also allows an agency to see a greater return on its PIV issuance and PACS modernization efforts. One large agency found that standardizing local facility access cards and visitor badges across its bureaus/components eliminated redundant credentialing and access control processes and yielded cost savings within their ICAM PACS implementation.



When determining agency policies for local facility access cardholders, access should be limited to the facility or specific areas within a facility that are appropriate for the individual. For example, a child care worker assigned to a child care facility might also have access to a facility's cafeteria or external restrooms, if necessary, but should not have unfettered access to other areas of the building not related to his work assignment. For more considerations around implementing a local facility access credentialing approach, see Section 8.1.4.3.

## **10.5. Visitor Access**

In addition to managing physical access for its employees and contractors using a PIV card or other affiliates using a local facility access card, agencies may also need to address physical access for a wide variety of visitors to federal facilities. While it is expected that there will continue to be a degree of variation in visitor processes and systems due to agency-specific policy and security requirements, the ICAM segment architecture defines several key aspects of

developing and operating a visitor management capability in the target state. The target state specifies that an agency move away from manual, paper-based methods for managing visitors and implement an electronic enterprise VMS capability, leveraging its existing PIV infrastructure (e.g., using visitor credentials that can be validated using the PIV-enabled PACS) and process automation wherever possible.

#### Privacy Tip

Privacy requirements should not be reduced or removed when technology is introduced to an agency's visitor management procedures. The same privacy protections for paper-based, manual processes should be applied to electronic, automated versions. For example, some electronic Visitor Management Systems (VMS) might offer the ability to scan an individual's driver's license to collect personal identifiers instead of having the individual handwrite his/her information. Agencies should ensure that only relevant and necessary information is obtained from the driver's license and is handled in accordance with their privacy policies.



Agencies must accept PIV cards from visitors from another agency and electronically authenticate them in accordance with applicable access control procedures. In addition, visitors with PIV cards from another agency should be provisioned into the hosting agency's PACS and electronically authenticated for the timeframe during which access is required. These efforts will reduce risk, enhance interoperability, improve efficiency, and positively impact customer service. Agencies should also seek to leverage their existing infrastructure and accept PIV-I cards from visitors when they are available.

#### Implementation Tip

Agencies should enable their security guard force with electronic authentication means wherever possible. This allows security guards to make access decisions based upon reliable, timely information. It also allows them to focus their time and attention on monitoring for other security threats, rather than performing visual authentication of credentials, which can help improve the overall security of the facility.



Agencies should consider a number of factors when designing their VMS capability and visitor management procedures, including:

- **Type of visitor.** The ICAM segment architecture defines a visitor as an individual external to an agency who requires access (often short-term or intermittent) to a facility or site controlled by the agency. This covers a wide variety of visitor types that an agency may encounter, including federal employees from other agencies, business partners, or members of the public. Agencies should analyze the visitor population(s) associated with its facilities, as it may impact system design.
- **Type of credential/identification used.** In most cases, the types of visitors an agency encounters dictates the type of credential that is available for performing authentication. For example, a visitor from another agency should have a PIV card, whereas, a member of the public would likely only have a lower assurance credential available. An agency's visitor management policy should specify what kinds of IDs are acceptable and the procedures that will be used to authenticate them. Per M-11-11,<sup>239</sup> an agency must accept and electronically verify PIV credentials issued by other federal agencies. Additionally,

<sup>239</sup> M-11-11

as part of the ICAM target state, agencies should be implementing the capability to accept PIV-I credentials from visitors, where an appropriate trust relationship exists.

- **Background vetting.** Different visitor types will have been subjected to varying levels of background vetting. For example, federal employees and contractors from another agency will meet the minimum PIV card investigation standards, whereas members of the public may not have any background vetting. An agency should consider the background vetting of its visitor populations when determining visitor procedures, such as the requirement for an escort.
- **Areas to which a visitor requires access.** Based on the facility risk assessment, an agency would likely adjust its visitor procedures if a visitor requires access to an Exclusion area, as opposed to a controlled area. Additionally, access points may need to be added to separate areas open to facility visitors from more restricted areas.
- **Visitor pre-registration.** The use case for visitor access in the ICAM segment architecture assumes that visitor access is substantiated by a sponsor, who validates the visitor's need to access the facility or area. Agencies should establish a pre-registration process to capture this sponsorship and provision visitor credential data, where applicable. Additionally, many agencies encounter visitors who arrive at reception with no pre-registration (e.g., members of the public visiting an open cafeteria or credit union). Agencies encountering this scenario should include it in process and VMS planning.

## FAQ

### When should I require an escort for visitors at my facility?

Escort requirements should be based on the risk associated with the facility or area which a visitor is accessing. It is recommended that agencies have a consistent approach to escort policies while maintaining flexibility for decisions at the local site level, as each facility may have varying levels of risk.



It is recommended that agencies implement a standard, enterprise-wide approach to address visitor types, levels of screening associated with these types, and standardized options for visitor credentials. This approach should incorporate considerations for interoperability, improving efficiencies in handling large volumes of visitors, and reuse of existing agency investments for physical access control. The business processes associated with providing credentials to visitors should also leverage efficiencies and best practices from the processes associated with established credentialing efforts, such as creation and issuance of PIV cards.

## ROI

Leveraging PIV and PIV-I cards from visitors within the Visitor Management System (VMS) and PACS allows an agency to better utilize its investment in PIV card and PACS modernization efforts to incorporate PIV card. Furthermore, an agency can see reduced costs associated with manual, time-consuming authentication procedures for other credential types, which are also typically less secure.



When developing their electronic VMS capabilities, agencies should incorporate the following common characteristics of a modernized, target state implementation:

Characteristic ID	Solution Characteristic
<b>VMS 1</b>	Supports validation of acceptable credentials of visitors, including PIV and PIV-I, using standard methods for each card type, including certificate checking.
<b>VMS 2</b>	Integrated into or interfaced with an electronic, modernized PACS, where possible.
<b>VMS 3</b>	Supports automatically provisioning and de-provisioning access rights for visitors based on length of stay.
<b>VMS 4</b>	Provides visitor pre-registration capability, where sponsors are able to enter biographic information for visitors, set up meeting times, and notify visitors.
<b>VMS 5</b>	Provides reporting and audit functions.
<b>VMS 6</b>	References the agency's Watch List <sup>240</sup> and denies access to those included on the list.
<b>VMS 7</b>	Allows security personnel to maintain their Watch List using a receptionist or administrator console.
<b>VMS 8</b>	Supports migration of select current data (or similar) from manual Watch List to VMS.
<b>VMS 9</b>	Supports automatic removal of visitor accounts after a specified period of inactivity.
<b>VMS 10</b>	Provides a central visitor database repository such that visitors do not have to repeat registration processes upon subsequent visits once their attributes have been captured.
<b>VMS 11</b>	Supports an additional level of security through advanced screening and background checks (if necessary).

**Figure 113: Common VMS Design Characteristics**

Lesson Learned
The value of the PIV card doesn't have to be limited to sites with an electronic PACS. USDA has created a web-based Card Confirmation Service that allows individuals at smaller field locations to input card data to check the validity of a visitor's PIV card against the authoritative security database.



<sup>240</sup>Watch list is a general term used within the physical security community to refer to a list of individuals to whom access should not be granted.

## 11. Initiative 8: Modernize LACS Infrastructure

Initiative 8 of the ICAM Transition Roadmap, as introduced in Section 5.2.2, is an agency-level initiative that includes activities associated with upgrading LACS to fully leverage the PIV card, make better use of cryptographic capabilities, and automate and streamline capabilities to increase efficiency and improve security. A LACS is an automated system that controls a user's ability to access one or more computer system resources such as a workstation, network, application, or database. A LACS validates an individual's identity through some mechanism such as a PIN, card, biometric, or other token. Based on the selected implementation path, it also grants or denies user access to resources based on pre-defined criteria, such as affiliation with the organization, role, or individual privileges granted to further the agency's mission. The target state calls for a modernized LACS, which includes the following characteristics:

- Provides high assurance of user identity while allowing streamlined access across multiple applications using a single credential;
- Reduces administrative burden on the part of resource owners and administrators by minimizing the need to manually manage user accounts and access privileges;
- Enables streamlined detection and remediation of conflicting access privileges within and across resources (e.g., segregation of duties);
- Provides a standardized, strong authentication mechanism for users accessing agency resources;
- Secures access through strong authentication for remote users accessing agency resources;
- Supports the use of encryption and digital signature services to encrypt and digitally sign data using the PIV card; and
- Enables strong authentication for remote users while leveraging the existing infrastructure.

The guidance provided in this chapter supports achievement of the target state Use Case 10, Grant Logical Access, and the associated transition activities listed in Section 5.2.2.4. This guidance primarily focuses on logical access control for federal employees and contractors authenticating with a FIPS 201 compliant PIV card<sup>241</sup> for all resources, regardless of assurance level.<sup>242</sup> The guidance addresses authentication using the cryptographic capabilities of the PIV card (Authentication X.509 certificate and user PIN); however, other authentication types (e.g., PIV biometric authentication) may be supported within an agency.

This chapter is organized into the following three primary sections:

- **Logical Access Implementation Planning.** This section discusses LACS program governance, investment planning, and schedule planning considerations that are necessary to properly plan for a logical access deployment within an agency.
- **Logical Access Architecture and Design.** This section describes the architecture, components, and key design requirements common to LACS solutions and provides reference architecture diagrams to illustrate how LACS solution components interact with each other.

---

<sup>241</sup> Logical access guidance for external users at all four assurance levels is addressed further in Chapter 12, Initiative 9: Implement Federated Identity Capability.

<sup>242</sup> As specified in [M-04-04](#) and [SP800-63](#).

- **Logical Access Technical Implementation.** This section covers common technical considerations for deploying LACS solutions and their supporting infrastructure within federal agencies, including workstations, servers, and networks.

## **11.1. Logical Access Implementation Planning**

Planning for a LACS implementation is similar, in many respects, to planning for any other large-scale IT program. The far reaching scope of LACS solutions, however, increases the importance of planning activities to overall implementation success. This section examines several specific areas that agencies should consider when initiating a LACS implementation effort, including organizational governance, program funding, and schedule planning. Section 11.2 introduces a high-level solution architecture for achievement of the target state ICAM segment architecture for LACS and discusses various solution components. This information may be helpful for understanding the concepts and activities discussed throughout the remainder of Section 11.1. The OMB memorandum released on May 23, 2008<sup>243</sup> provide agencies with additional guidelines for consideration when planning or updating plans for the use of the PIV card in their LACS, a central aspect of the ICAM target state. In addition, the ICAM Reporting Template provides a detailed list of activities associated with implementing the ICAM segment architecture.

The information and guidance provided in this section is intended to provide answers to several common LACS implementation planning questions, including:

- How can organizational governance support my LACS implementation effort?
- What factors within my agency's operational environment should I examine when determining what type(s) of LACS solution to acquire?
- What should I consider when building my LACS business plan?
- What activities should I be aware of when planning a LACS implementation?
- How can I secure program funding for my LACS modernization effort?

### **11.1.1. Program Governance**

For many agencies, modernization of their LACS infrastructure in accordance with the target state ICAM segment architecture may require changes to existing policies, processes, and technologies. Chapter 6 introduces a variety of techniques for governing an agency's ICAM program, including the modernization of LACS solutions. This section is intended to supplement that guidance and highlight specific areas that agency governance bodies should seek to address at an enterprise or component/bureau level to enable successful LACS modernization efforts.

Many federal agencies have existing policies that determine requirements, processes, and technologies for controlling access to internal IT resources. As part of the LACS modernization planning effort, agencies should evaluate their logical access policies and identify potential gaps where revisions, updates, and new policies and/or standards are needed to drive the process and underlying technology changes identified in the target state ICAM segment architecture gap analysis for logical access. As outlined in Section 6.1.1, agencies may need to consider establishing working groups and/or cross functional teams within the overall ICAM governance

---

<sup>243</sup> [HSPD-12](#)

structure to directly support LACS projects. This approach ensures that a responsible party is established to assess, manage, and maintain LACS policies and procedures over time.

Updates to existing policy or creation of new policy, where appropriate, can help agencies overcome many of the internal hurdles and challenges that most often hinder implementation efforts. These challenges are particularly prevalent with LACS modernization efforts as their success is heavily dependent on adoption and use at the user and resource level. Policy and governance structures are key enablers of ensuring enterprise adoption of LACS solutions, which is critical if they are to achieve their desired outcome.

While each agency is unique in the maturity of its logical access policies, relative to the ICAM target state, there are a number of common topics that should be incorporated to support LACS modernization. Figure 114 includes a list of the common governance efforts and describes how agencies might consider utilizing them as a means to support compliance and overcome implementation hurdles.

Governance Effort	Description
Issue Policy Memorandum: Continued Implementation of HSPD-12	<p>Agency-level policy, as required by M-11-11,<sup>244</sup> that includes provisions for several items related to LACS modernization, including:</p> <ul style="list-style-type: none"> <li>• Enforcing use of the PIV card for authentication to networks and applications.</li> <li>• Procurement of services and products for LACS in accordance with M-06-18<sup>245</sup> and the Federal Acquisition Regulation (FAR).<sup>246</sup></li> <li>• Acceptance of PIV credentials issued by other federal agencies for logical access.</li> <li>• Alignment with the ICAM segment architecture, including completion of an agency transition plan that includes information regarding the agency's LACS modernization.</li> </ul>
Common Logical Access Scenarios	Policy or procedural guidance reflecting formal agency-level decisions for handling common logical access problem scenarios, such as granting access when a user forgets/loses PIV card or forgets personal identification number (PIN), requires mobile/remote access and does not have access to a smart card reader, and hardware malfunction preventing use of PIV card.
Define Agency Level Security Benchmarks	Procedural guidance for agencies to implement additional security benchmarks, beyond federal standards and guidance, for internally owned and operated IT resources to require use of LACS services and authentication mechanisms.
Define Roles and Responsibilities for Cross Functional Working Groups	Effort to establish roles and responsibilities for cross functional working groups to facilitate collaboration and achievement of stated objectives between members from multiple groups, offices, and bureaus/components within the agency.
Define Enterprise Data and Attribute Format Standards	Effort to define standard data formats for identity and entitlement attributes to streamline provisioning and application integration processes. Agencies should leverage the guidance provided in Chapter 7 when completing this activity.

<sup>244</sup> [M-11-11](#)

<sup>245</sup> [M-06-18](#)

<sup>246</sup> [FAR Subpart 4.13](#)

Governance Effort	Description
Determine Trusted Authoritative Sources (e.g., HR, Personnel Security, Payroll, Contracts, Identity Management System [IDMS], or other systems)	Effort to define authoritative sources for identity and entitlement attributes to ensure access to accurate, reliable information. Agencies should leverage the guidance provided in Chapter 7 when completing this activity.
Determine Core User Identity Attributes	Effort to define a core set of attributes that are required to uniquely identify an individual at an enterprise level to ensure consistency between the authoritative sources, LACS infrastructure, and IT resources. Agencies should leverage the guidance provided in Chapter 7 when completing this activity.
Define Baseline User Privileges for IT Access	Effort to define a set of baseline user privileges for IT access can be accomplished at various levels within the enterprise and should be considered where significant efficiencies can be achieved. When linked to an automated provisioning capability new users can be granted access to a large number of applications automatically, based on a well-defined set of baseline needs.
Define a Stakeholder Messaging Strategy	Effort to develop a Stakeholder Messaging Strategy, which allows an agency to identify stakeholders and understand their individual motivations, and business drivers. Knowing these characteristics allows an agency to tailor multiple custom messages, which will improve adoption and overall buy-in. This strategy supports development of a Communications and Outreach Plan once the implementation begins.
Determine Staffing Strategy	Effort to develop a plan/strategy to rotate/reallocate staff members whose positions may be automated (i.e., electronic account creation) as part of the LACS modernization effort.
Define Agency-level Privacy Requirements	Effort to assess whether existing privacy and data protection requirements/guidelines are sufficient to address privacy concerns associated with LACS automation and data sharing or if additional privacy requirements are needed for specific LACS services.

**Figure 114: Sample LACS Governance Efforts**

### 11.1.2. Program Funding

Logical access control deployments require adequate planning and consideration to ensure that an agency achieves the best possible value for its investment. As noted throughout this chapter, LACS projects offer agencies the potential to realize significant ROI in the form of cost avoidance, reallocation of resources, productivity gains, and reduced administrative burden. In order to achieve these benefits, an agency should assess its organizational structure, identity stores/repositories, access control processes, and IT resources when planning new or modifying existing LACS investments. This section discusses these considerations in greater detail and examines the impact that these items may have on funding for the LACS implementation. Additionally, the considerations discussed below provide an agency with guidance for evaluating its own organizational factors to determine what LACS solution architecture best meets its needs.

In order to select an appropriate LACS solution that supports the agency mission and business goals, agencies should look beyond the up-front costs associated with LACS investments. There are additional factors that should be evaluated at an organizational and LACS project level when determining what type of LACS solution best meets the organization's needs. The items provided in Figure 115 are examples of common factors and considerations that agencies should examine not only to determine implementation cost, but also determine the potential benefits that various LACS solutions are capable of providing.

Evaluation Factor	Description
Organizational Size	The number and type of users requiring access to agency IT resources, as well as the frequency of turnover of users, significantly impacts the level of administrative effort required to provision user accounts and manage access privileges.
Cost Effectiveness	Agencies need to evaluate the return on investment (ROI) that their agency would gain compared with the upfront investment costs when planning for a LACS investment. Those agencies that would achieve low or negative ROI if implementing an enterprise-level LACS solution may opt for a variation on the architecture presented in Section 11.2.1.
Complexity of User Population	Organizations with complex user and role management requirements should consider LACS solutions that offer services in these areas. User management complexity represents an opportunity to streamline existing processes or, potentially, an area that could significantly increase implementation costs. Additionally, the availability (or lack thereof) of user repositories can impact implementation costs.
Number of IT Resources	The number of IT resources within an agency often dictates implementation time and can significantly affect implementation cost, depending on the resources' connection requirements.
Type of IT Resources	The type of IT resources varies based on the platforms, operating systems, products, databases, etc. that are in use across the organization. These variances impact the complexity of integrating resources with the LACS infrastructure and require different integration processes.
Complexity of Integrating with IT Resources	<p>Resource integration complexity is a combination of several factors, including: age of resource, underlying infrastructure, operating requirements, and user base. Combined, these factors among others indicate how complex it is to integrate particular resources into the modernized LACS infrastructure. Large numbers of complex resources (including mainframe applications) can rapidly increase overall implementation costs. At a high-level the complexity and cost associated with common application types can be grouped as follows:</p> <ul style="list-style-type: none"> <li>• Web Based Applications – Low to Moderate Complexity</li> <li>• Client/Server Applications – Moderate to High Complexity</li> <li>• Distributed Applications – Varied Complexity</li> <li>• Mainframe/Legacy Applications – High to Very High Complexity</li> </ul>
Business Goals/Drivers	Internal agency policies and business needs as well as required compliance with external federal policies and regulations drive organizational requirements for LACS solutions. Certain solutions, while inexpensive, may not always create long term cost savings and may prohibit the organization from meeting certain business goals.
Workflow Requirements	Agencies should examine the complexity of various manual and semi-manual workflows that are used to provision user accounts and access privileges to IT resources. The number and complexity of an agency's workflows impacts the schedule and labor costs associated with implementing some LACS solutions.
Organizational IT Infrastructure	Specific platforms and operating environments, particularly ones that leverage legacy products, may require additional support and/or custom configuration to achieve the maximum benefit from LACS solutions. This also includes potential costs associated with networking LACS components, high-availability components, etc. Additionally, environments that utilize non-standard Operating Systems may require additional investment to integrate to a modernized LACS infrastructure.
Vendor Product Compatibility and Interoperability with Existing Infrastructure	While it is not required for agencies to purchase a Commercial Off-The-Shelf (COTS) Identity Access Management (IAM) product suite, agencies considering this option for modernizing their LACS infrastructure should assess the integration approach of these products to ensure interoperability, and identify and determine a best fit for their current infrastructures, applications, and business needs. Additionally, the availability of enterprise software licenses should be investigated, as these can significantly lower acquisition costs and influence an agency's make or buy decision.

Evaluation Factor	Description
Existing LACS Investments	Agencies may have existing investments in place that are capable of providing logical access services in a manner consistent with the target state ICAM segment architecture. These investments should be leveraged wherever possible and offer the potential to achieve a modernized LACS state without requiring significant investment from the organization.
Bureau/Component Level Application Integration Needs	Many agencies contain multiple bureaus/components that perform an array of mission-specific services. Often, these bureaus house IT resources that are used throughout the organization. Agencies should evaluate their internal structure to determine how LACS services can be provided to bureau resources. This could be done at an enterprise level or de-centralized based upon agency-specific needs.
Prioritized Logical Access Services	When examining logical access needs, many agencies will recognize that large efficiencies and ROI can be achieved by prioritizing deployment of certain access control services. This will be dependent on the agency's infrastructure and existing LACS investments, but should be considered when determining how to modernize LACS across the enterprise.

**Figure 115: Common LACS Funding Considerations**

The factors discussed in Figure 115 provide a baseline for agencies when determining what type of LACS solution is best suited to meet the organization's unique needs. When making such a determination agencies should seek to strike a balance between the up-front investment costs, long-term potential cost savings, and ability to meet the organization's overall business objectives to arrive at a total cost of ownership. The total cost of ownership is used to realistically forecast LACS solution ownership costs in terms of 1-, 3-, and 5-, year cycles in order to provide an accurate assessment of the solution's impact and benefit. This can be accomplished through completion of a detailed cost/benefit analysis, which is generally conducted as part of an organization's business and investment planning process.

#### Lesson Learned

In order to drive adoption of its enterprise LACS and participation in pilot implementations, USDA offered to fund the initial LACS integration costs for a subset of agency applications that were candidates for early adoption. Doing so increased participation and enabled the Department to demonstrate technical using real world examples.



#### 11.1.2.1. Building a Business Plan for LACS Modernization

Using the factors discussed in Figure 115 along with others identified within the organization, agencies should complete a cost/benefit evaluation and develop a business plan to outline the selected LACS implementation approach, timeline, resource requirements, and estimated costs necessary to complete a modernization of their LACS infrastructure. Completion of a LACS business plan supports achievement of Transition Activity 8.4, as discussed in Section 5.2.2.4.

#### Implementation Tip

In order to justify the agency's investment in an enterprise LACS solution, the General Services Administration (GSA) developed a detailed business plan that outlined the current access management situation, upcoming regulatory requirements that define the need to modernize, and discussed the various implementation alternatives at the agency's disposal before arriving at a recommended implementation approach to best meet the agency's current and future access management needs.



Many federal agencies have existing tools and templates designed to support development of business plans for IT investments. The guidance presented in this document does not seek to influence basic business plan development processes; however, it does highlight several important factors and considerations, specific to LACS. The following list includes items and areas that should be closely assessed when constructing a business plan for a LACS modernization effort, and weighed by key decision makers.

- **Alternatives Evaluation.** There are a multitude of ways to modernize an organization's LACS infrastructure, including a variety of solution alternatives and implementation approaches. An effective business plan should thoroughly evaluate each potential solution and a variety of implementation approaches, which might include varying timelines, deployment scope, and deployment phasing. Such an evaluation ensures that the agency is investing in a solution that will best meet its needs.
- **Technology Solution Analysis.** There are a wide variety of technology solutions that can provide an agency with logical access services. An agency should analyze available COTS products, the ability to modify existing investments, and custom development options to determine which solution best suits the overall needs of the organization in the most cost effective manner.
- **Cost and ROI Forecasting.** The purpose of LACS modernization is to achieve higher levels of security while streamlining existing processes and promoting organizational efficiency. In order to achieve this, agencies should examine the total cost of solution ownership and maintenance for each potential alternative over a five year (at a minimum) period. This allows leadership to examine cost of ownership beyond the initial up-front investment cost, and accurately predict cost savings over a longer period of time.

ROI	
By implementing a modernized LACS solution, USDA anticipates being able to reduce its staff currently dedicated to managing user accounts and application access by approximately 70 full-time resources. These functions can now be automated and performed electronically. USDA will be able to eliminate numerous contractor positions and reallocate agency employees to support mission programs.	

- **Qualitative Benefits.** Typical business plans and cost/benefit analyses focus primarily on quantifiable cost savings. While this is important to LACS modernization efforts, planners must not overlook the qualitative benefits (process efficiencies, data privacy, information security, etc.) that can be gained through deployment of logical access services. Specific implementation alternatives and approaches yield differing levels of qualitative benefits based on each agency's unique needs. It is important that these qualitative factors be addressed in the business plan as they may represent a critical deciding factor between similar approaches.
- **Risk.** Similar to qualitative benefits, each potential LACS modernization alternative includes a certain level of risk. These risks could impact project cost, deployment schedule, organizational security, and user acceptance depending on the scope of LACS solutions. An agency must evaluate all alternatives and plan to manage risk appropriately, regardless of the solution option selected.

### 11.1.3. Schedule Planning

LACS modernizations are complex undertakings and therefore require significant up-front planning to ensure a successful deployment. Program/project managers should consider following a structured life cycle model to assist them with the planning process. Chapter 10 introduces a phased SDLC model that identifies key activities and timing considerations during a PACS modernization. The five phases are: Planning, Requirements and Design, Build, Implement, and Operate and Maintain. The SDLC model presented in Chapter 10 can be used by program/project managers to plan for LACS modernizations. This section examines each of the SDLC phases and discusses the LACS-specific events that should occur as part of each phase.

#### Privacy Tip

Agencies should involve representatives from their Privacy Office during the Requirements and Design and Build phases to ensure that solutions are designed in a manner that protects privacy. While many privacy activities typically occur during the Requirements and Design and Build phases, agencies should also consider data protection and privacy requirements throughout the entire LACS development life cycle and incorporate appropriate privacy measures. Privacy should not be overlooked when attempting to solve complex technical challenges, as the overarching goal of increased efficiency and security must be maintained.



#### 11.1.3.1. Planning Phase

The Planning Phase is the first step in beginning a LACS modernization effort within a federal agency. This phase includes many of the topics discussed in Chapter 6 and Section 11.1 of this chapter. Completing the Planning Phase is critical for modernizing LACS solutions, as many of the common problems encountered can be avoided through careful planning. Figure 116 provides a list of common activities that should occur during the Planning Phase and notes estimated completion times for each; however, activities may occur in parallel, and actual times can vary widely based on organizational size and project complexity.

Activity	Description	Completion Time
Conduct Cost/Benefit Analysis	Evaluate the factors discussed in Section 11.1.2 and conduct a cost/benefit analysis to determine an appropriate LACS solution.	3 – 6 weeks
Develop LACS Modernization Business Plan	Develop a business plan to support modernization of the existing LACS infrastructure. This should lay out the selected approach, timeline, resource requirements, and estimated costs, and supports Transition Activity 8.4.	4 – 6 weeks
Develop Implementation Plan/Schedule	Develop a phased implementation approach and schedule based on available information using standardized agency resources. This should include planning for future integration periods beyond the initial LACS deployment.	4 – 6 weeks
Categorize the LACS	Conduct Step 1 of the Risk Management Framework (RMF): Categorize Information Systems based on mission/business objectives. Register the LACS in the agency's IT system inventory.	4 – 12 weeks
Begin Application Prioritization	Examine IT resources and develop application assessment criteria in order to prioritize/organize deployment of modernized LACS services to agency IT resources.	4 – 6 weeks
Develop Risk Management Plan	Utilize existing risk management sources to develop a Risk Management Plan, as discussed in Chapter 6, for handling risks related to modernizing the LACS	2 – 4 weeks

Activity	Description	Completion Time
Develop Communications Plan	Develop the approach and plan to communicate (using a variety of media) the changes that a LACS modernization effort will bring to internal users, resource owners, and stakeholders.	2 – 4 weeks
Develop Application Integration Guide	Develop an Application Integration Guide, a formal document used to outline the process that an agency's IT resources will go through to become integrated with the LACS solution.	6 – 8 weeks
Develop LACS Migration Plan	Develop a migration plan that outlines how the agency plans to transition its logical resources to use the modernized access control system.	2 – 6 weeks
Develop Pilot Implementation Plan	Develop a plan and schedule for piloting the modernized LACS solution on a small subset of the user population with well-defined resource requirements.	4 – 12 weeks

Figure 116: Planning Phase Sample Activities

#### 11.1.3.2. Requirements and Design Phase

Once an organization has planned its LACS modernization effort it enters the Requirements and Design Phase. This phase is where the agency thoroughly documents the requirements for the LACS solution and defines how the solution should operate within the agency's infrastructure. Figure 117 provides a list of common activities that should occur during the Requirements and Design Phase and notes estimated completion times for each; however, activities may occur in parallel, and actual times can vary widely based on organizational size and project complexity.

Activity	Description	Completion Time
Finalize LACS Solution Requirements	Conduct a requirements gathering exercise with stakeholders and impacted parties at all organizational levels to document requirements of the LACS solution. These requirements are critical as they will be used to design, build, and configure the LACS capability.	4 – 8 weeks
Validate LACS Solution Requirements	Validate the documented requirements with the LACS stakeholders in order to ensure that the LACS solution is properly designed and configured to meet the agency's needs.	2 – 3 weeks
Identify and Secure Funding Sources	Utilize the LACS business plan to secure funding sources for the modernization effort. All information technology (IT) investments need to include funding as appropriate to support ICAM activities.	6 – 10 weeks
Select Security Controls	Conduct Step 2 of the Risk Management Framework (RMF): Select Security Controls by choosing the appropriate security controls and documenting the selected controls in the security plan.	2 – 4 weeks
Develop Solution Architecture	Develop an initial solution architecture for the LACS implementation, which defines the solution components and describes their interactions.	2 – 3 weeks
Identify Authoritative Stores	Identify the authoritative store(s) of user information that will be used with LACS solution to enable automated provisioning of user accounts.	4 – 8 weeks
Establish Common Rules, Roles, and Policies	Determine the common roles, rules, and policies that shall apply to all applications in the enterprise environment. These common rules serve as a base set of configurable items within a LACS solution, and added granularity can be provided on a per application basis.	4 – 6 weeks
Map Consolidated Rules, Roles, and Policies to Applications	Map the base set of rules, roles, and policies to those currently used by the target applications (e.g., the downstream IT resources being protected by the LACS infrastructure).	8 – 12 weeks (depending on scope and complexity)

Activity	Description	Completion Time
Document System Design	Draft an initial system design document that clearly states how the system should function within the agency's environment. The design document and associated requirements are then used during the build phase as a reference for how the LACS system should operate. The design document will also demonstrate how common roles, rules, and policies will be applied to enterprise LACS applications, and will further demonstrate how granular level policies, rules, and roles are supported to meet the LACS application owner needs.	10 – 12 weeks
Document LACS Use Cases	Document detailed LACS use cases, which the designed solution should address in the build phase. These models should seek to capture existing manual processes that will be automated, along with any exception workflows that are not part of the primary workflow.	4 – 6 weeks
Define and Configure Provisioning Workflows	Define provisioning workflows, which are used to determine how users are granted access to logical resources and what approvals or additional steps are required. This process often involves configuring automated workflows based on existing manual processes. Provisioning workflows are based on a solid understanding of the enterprise approach to common rules, roles, and policies which are applied consistently across managed end-point applications.	2 – 4 weeks
Develop Demo Application	Consider development of a demo application that can be used for training business/resource owners on the LACS capabilities that the agency is implementing. Having such a capability provides LACS program management with the ability to showcase all the capabilities and streamline integration processes.	6 – 8 weeks
Determine Physical Deployed Architecture	Outline the physical elements that need to reside in data centers, and allow for advanced coordination of the end state solution that will need to be located/hosted there. Best practice dictates that the agency should include the production environment, pre-production testing environment, user acceptance testing environment, and the development testing environment. These four environments will need to be maintained throughout a solution life cycle to allow for proper testing, regression testing, and solution integration over time.	4 – 6 weeks
Conduct Detailed Application Assessments	As part of the application prioritization and integration process, conduct application assessments as a means of gaining information about resource configuration and existing workflows.	12 – 14 weeks
Conduct Privacy Assessment	Review the LACS design and solution requirements against established privacy guidelines and agency policies to ensure compliance.	4 – 6 weeks
Conduct Resource Acquisition	With funding sources secured, conduct the process of purchasing any required hardware, software, or labor support that will be needed.	4 – 12 weeks

**Figure 117: Requirements and Design Phase Sample Activities**

#### 11.1.3.3. Build Phase

Following the Design Phase, agencies enter the Build Phase, where the majority of the technical solution development, configuration, and testing occurs. Figure 118 provides a list of common activities that should occur during the Build Phase and notes estimated completion times for each; however, activities may occur in parallel, and actual times can vary widely based on organizational size and project complexity.

Activity	Description	Completion Time
Stand Up Development and Test Environments	Establish development and testing environments so that LACS developers and testers can conduct build activities in an environment that does not impact the agency's production systems.	4 – 6 weeks
Build/Configure Servers	Build and/or configure servers to properly operate the LACS solution, as needed based upon the chosen implementation path. Agencies should align with acquisition activities (if applicable) to ensure that hardware is on-hand in an appropriate timeframe.	4 – 6 weeks
Install Supporting Software	Install supporting software (i.e., Commercial Off-The-Shelf [COTS] Identity Access Management [IAM] Suite) on LACS servers, as needed based upon the chosen implementation path.	8 – 10 weeks
Configure Supporting Software	Configure LACS software to specifically meet the agency's unique needs and/or perform certain functions, as needed based upon the chosen implementation path	8 – 10 weeks
Implement and Assess Security Controls	Conduct Steps 3 and 4 of the Risk Management Framework (RMF) by applying the controls identified in the requirements and design phase and by assessing the adequacy and effectiveness of the security controls and documenting the findings in an assessment report.	12 – 20 weeks
Build Resource Adapters, Service Interfaces, and Network Connectors	Build and configure network connectors, service interfaces, and resource adapters in order to deploy the LACS solution onto the agency's network and integrate with IT resources.	2 – 4 weeks per resource
Develop a Test Plan and Test Scripts	Define a test plan and test scripts to organize the testing process and identify the key capabilities that must occur successfully to ensure that the LACS solution performs as it was designed and operates securely and efficiently.	2 – 3 weeks
Conduct Testing on Initial Build	Perform testing (including failover <sup>247</sup> and regression testing, interoperability testing with other infrastructure components, and performance testing) on the LACS solution in a development and/or test environment to ensure that system errors are found and corrected before the solution is deployed on the agency's network.	4 – 8 weeks <sup>248</sup>
Conduct Pilot Implementation Deployment	Conduct a pilot implementation to expose a small subset of the agency's user base to the LACS solution for the purpose of evaluating the solution's operations against real-world requirements.	4 – 6 weeks

**Figure 118: Build Phase Sample Activities**

#### **11.1.3.4. Implement Phase**

Once an agency has configured its LACS solution and tested to ensure that it meets agency requirements and performs appropriately, the project enters the Implement Phase. This phase consists of activities for migrating the LACS solution from a development and test environment into the agency's production infrastructure. Figure 119 provides a list of common activities that should occur during the Implement Phase and notes estimated completion times for each; however, activities may occur in parallel, and actual times can vary widely based on organizational size and project complexity.

<sup>247</sup> Described in [SP800-53](#).

<sup>248</sup> Estimated time includes testing and remediation of findings.

Activity	Description	Completion Time
Authorize the LACS	Conduct Step 5 of the Risk Management Framework (RMF): <sup>249</sup> Authorize Information System by preparing and submitting the security authorization package to the authorizing official. The authorizing official chooses to accept the risk and authorize the system if the risk associated with operating the LACS is deemed acceptable.	1 – 2 weeks
Conduct User Acceptance Testing	Conduct user acceptance testing to ensure that the LACS solution is acceptable to stakeholders and end users and performs the required functions in an appropriate manner.	4 – 6 weeks <sup>250</sup>
Deploy LACS Solution to Live Production Environment	Deploy the LACS solution on the agency's network infrastructure and begin controlling access to protected resources.	4 – 6 weeks
Conduct User Training	Develop training materials and conduct user training prior to LACS deployment to ensure that users are capable of accessing their worksites without disruption.	3 – 4 weeks
Perform Awareness and Outreach	Conduct awareness and outreach activities in accordance with the Communications Plan developed as part of the Planning Phase. This involves actively communicating to users that a new access control system is being deployed, the benefits and efficiencies that users can expect, and any steps necessary to begin using the new system.	This will occur as needed throughout the deployment process.

**Figure 119: Implement Phase Sample Activities**

#### **11.1.3.5. Operate and Maintain Phase**

After an agency has successfully deployed its modernized LACS solution to a live production level, the project enters the Operate and Maintain Phase. This phase lasts for the remainder of the time that the LACS solution is in use and consists of ongoing management and system maintenance activities such as: conducting training, operating the LACS solution, and protecting new resources as they are integrated with the enterprise solution. Figure 120 provides a list of common activities that should occur during the Operate and Maintain Phase and notes estimated completion times for each; however, activities may occur in parallel, and actual times can vary widely based on organizational size and project complexity.

Activity	Description	Completion Time
Monitor Security Controls	Conduct Step 6 of the Risk Management Framework (RMF): Monitor Security Controls by monitoring changes to the information system and its environment of operation and conducting ongoing assessments of security controls in accordance with the monitoring strategy.	On-going
Ongoing User Training	Continue to update and modify user training curriculums as the LACS solution matures, new resources are protected, and new users are added. Conduct additional training as necessary.	This will occur as needed throughout the deployment
Execute Change Control Board (CCB)	Conduct activities with the CCB to evaluate potential changes to the LACS solution and provide a governance structure for determining which solution changes should be implemented.	Occurs throughout the life cycle, as changes are proposed

<sup>249</sup> A detailed discussion of the RMF can be found in Section 6.2.4.1.

<sup>250</sup> Estimated time includes testing and remediation of findings.

Activity	Description	Completion Time
Build/Configure Resource Adapters and Service Interfaces	Build/configure additional resource adapters and service interfaces to properly connect and manage authentication to new applications as they are integrated into the LACS infrastructure.	2 – 4 weeks per resource
Modify Provisioning Workflows	Update provisioning workflows as business needs and access rules change over time. Changes may also be required as resource owners experience the benefits that can be provided by modernized LACS services and provisioning workflows can be streamlined.	3 – 4 weeks planning 5 – 8 weeks for development and integration
Conduct Hardware/Technology Refresh	Conduct periodic updates and/or upgrades to solution hardware and other technology over the lifespan of a LACS solution as a means of extending the usable life of the solution or adding new capabilities.	12 – 36 weeks, depending on scope and system size
Remove Sunsetted Resources	Ultimately, IT resources are replaced, upgraded, or consolidated over time as mission and business needs change. Accordingly, as applications become sunsetted, user privileges will need to be de-provisioned and the resource itself can be disconnected from the LACS solution.	1 – 2 weeks

**Figure 120: Operate and Maintain Phase Sample Activities**

#### **11.1.3.6. Application Integration Planning**

LACS solutions achieve their value primarily through integration with an agency’s IT resources (applications). Once integrated, the agency’s applications utilize the LACS infrastructure to perform PIV-based PKI certificate authentication, and consume additional access control services (i.e., authorization, policy management, audit and reporting, etc.), if provided. Successfully integrating applications requires detailed planning as certain types of applications (e.g., legacy, custom built) are more complex to integrate and require additional time and resources. For this reason, agencies should gather and assess information about their applications in an effort to categorize and prioritize them for integration. Completion of this planning activity aligns with the activities titled, —Begin Prioritizing Applications,|| and —Conduct Detailed Application Assessments,|| in Figure 116 and Figure 117, respectively. Several factors should be evaluated to successfully prioritize an agency’s applications for integration with the LACS infrastructure, including:

- **Risk Profile.** Risk profiles for applications consist of an evaluation of the application’s compliance requirements, data sensitivity needs, data privacy requirements, and other artifacts of the FISMA and RMF processes. It is wise to choose low impact applications for inclusion in early integration activities, such as a pilot implementation, to avoid disruptions to sensitive applications during deployment. Once the full enterprise LACS capability has been established, an agency will likely prioritize its highest impact applications for integration first.
- **Inclusion.** In order to achieve widely accepted value across the enterprise, the agency should integrate applications from a representative set of business and mission areas as soon as possible.
- **Technical Readiness.** As noted previously, applications vary widely in their use of technology, platforms, operating systems, etc., and vary in maturity and usage. These factors, along with the complexity of the application’s interfaces and availability of application connectors and service interfaces, contribute to the technical readiness of

applications for integration. Agencies should seek to prioritize the applications that are the most technically ready as they are generally faster and easier to integrate.

- **Operational Readiness.** Many agencies operate applications that support mission-specific functions, which may dictate certain time periods where operational readiness is of paramount concern. Agencies should seek to integrate applications during the most appropriate timeframe and take into consideration when the resource could tolerate integration efforts.
- **Application Life Cycle Phase.** An agency should prioritize integration of applications that are under development such that they can be linked to the enterprise LACS solution as they are deployed. Applications that are currently operational should be prioritized based on the other factors relevant to the application, such as technical readiness. An agency should identify any applications that are planned to be phased out, as these applications do not need to be integrated with the LACS solution.

Each of the factors introduced above should be examined in greater detail against an agency's mission needs and operational business requirements in order to determine an appropriate weighting mechanism for evaluating the agency's applications. Once the factors are weighted, each application should be evaluated and scored. This type of evaluation results in a score for each application, which can then be used to determine integration priority.

#### Implementation Tip

When modernizing your agency's logical access infrastructure, be sure to factor in support for emerging technologies. With the growing push to take advantage of the benefits offered by cloud-based computing,<sup>251</sup> agency LACS should be designed and built in such a way that they are capable of appropriately securing an agency's applications and services in the cloud. For example, GSA is in the process of migrating to a cloud-based e-mail system, which will be protected by the agency's LACS.



Obtaining the information necessary to complete a comprehensive evaluation of an agency's applications as part of the prioritization process can be achieved through a variety of mechanisms. As discussed in Section 9.1, there are a variety of application information sources available within an organization. Much of the information necessary to perform an application evaluation can be obtained by reviewing the information available through these sources. However, it may be necessary to gather additional information from application owners and administrators. Agencies may evaluate and prioritize applications manually, which could be advantageous when very similar or few applications exist. However, tools exist that utilize technology to analyze and score applications in a semi-automated fashion, which significantly reduces evaluation time in agencies with many applications.

#### Implementation Tip

The Department of Agriculture (USDA) utilizes Decision Lens to analyze, evaluate, and prioritize their applications for integration with the agency's LACS infrastructure. This tool evaluates each application's business continuity, operational risk, multi-agency applicability, and OMB Circular A-123 compliance factors, and automatically ranks them for integration based on a configurable weighting scale.



<sup>251</sup> [M-10-19](#) directs agencies to evaluate the potential to adopt cloud computing solutions by analyzing computing alternatives for IT investments in FY 2012. [The Federal Cloud Computing Strategy](#) released on February 8, 2011 also emphasizes the capability of cloud computing to reduce inefficiencies and improve government service delivery.

Part of prioritizing applications for integration is identifying a small subset of applications that are relatively simple to integrate, are used by a well-defined group, and are receptive to new technologies. This subset should be targeted for integration with the LACS pilot implementation. The next section discusses the establishment of pilot implementations and the benefits that they provide.

#### **11.1.3.7. Pilot Implementation Development**

Pilot implementations are used to test newly developed solutions in a real-world environment on a small, well-defined group of users within a small number of easily integrated applications. This approach allows an organization to measure the effectiveness and user acceptance of the LACS solution in an environment that offers relatively low risk, while finely tuning the solution to ensure that it meets the organization's needs.

<b>Privacy Tip</b>	
While pilot implementations are often small in size and scope, agencies should keep in mind that legal and regulatory requirements for privacy and data protection apply equally to pilot implementations. Agencies should involve appropriate personnel from privacy and security offices to ensure that adequate safeguards are in place prior to implementing pilot activities.	

When establishing a LACS pilot implementation, agencies should consider several specific factors, which influence not only the success of the pilot but may also impact the agency's ability to predict the success of wide-scale deployment. These factors include:

- **Define scope of pilot.** Start small with limited number of willing and informed users, using agency PIV cards to access the agency's domain. Given the potential risk of delays or inability for users to log on to their computers, agencies should consider excluding personnel who require IT access with minimal disruption. Agencies should develop use cases that fall within the scope of the pilot and identify exceptional use cases that can be addressed based on the success of the initial pilot and lessons learned.
- **Identify potential privacy impacts of pilot.** Agencies should evaluate the potential privacy impact associated with the planned pilot implementation. This should include an evaluation of the type of data that is being used and/or exchanged within the pilot to determine if live production data containing any PII will be included. Agencies should consider using alternative data sources, if available, or ensure that the live production data is properly protected and disposed of in accordance with the agency's privacy and data protection policies.
- **Identify metrics for success and determine how evaluation data will be collected.** Defining a concrete set of objectives and measures up-front ensures clarity of purpose and ensures that the results can be accurately assessed. Collecting evaluation data consists of evaluating the performance of the LACS solution in terms of the number of authentication attempts (successful and unsuccessful), application downtime as a result of solution usage, as well as measuring the acceptance and use of the solution by the pilot participants.
- **Ensure coordination and communication.** Pilot implementations require coordination between LACS program management, resource owners and administrators, and program stakeholders. The pilot project manager should be responsible for managing the overall

schedule and ensuring that updates, concerns, and lessons learned are communicated to the pilot participants in a timely manner.

- **Identify pilot participants.** Pilot participants are generally identified as part of the application integration and prioritization effort, when specific applications are targeted for involvement in pilot implementations. However, agencies should seek to involve participants who will provide a broad representation of users' familiarity with using smart cards, office, position, physical location, and hardware used. Additionally agencies should consider the users' willingness to accept the risk associated with use of the new technology and who may be easily helped if they experience problems.
- **Formally evaluate the success of the pilot implementation.** When planning for a LACS pilot implementation agencies should plan on holding a formal evaluation of the criteria for success immediately following the program's conclusion. This allows the agency to identify and correct any deficiencies with the LACS solution before wide-scale deployment occurs.

### Lesson Learned

The General Services Administration (GSA) recognized that a LACS deployment relies on "quick wins" to demonstrate success and build support throughout the organization for continuing along the LACS maturity curve. "Quick wins" can be achieved through thoughtful application prioritization and pilot integration – select applications with well-defined user groups where user satisfaction and process streamlining can be easily evaluated.



## 11.2. Logical Access Architecture and Design

Designing a LACS solution requires agencies to consider the capabilities presented in the ICAM target state, existing LACS investments, and the agency's overall IT infrastructure. The objective of this effort is to determine how modernized LACS solutions will integrate with the agency's IT infrastructure and provide logical access services, as defined in the ICAM Services Framework (Section 3.2.4), to the agency's applications. Furthermore, as part of this process, an agency should take steps to ensure that its design does not incorporate any elements that could impair its ability to authenticate other agencies' PIV cards, as described in Section 8.4.

This section provides a solution architecture diagram, discusses the components that comprise a modernized LACS, and introduces common characteristics that an agency should consider when designing its target state LACS. The information and guidance provided in this section is intended to provide answers to several common LACS architecture and design questions, including:

- What does a modernized LACS infrastructure, compliant with the ICAM target state, look like?
- What are the components of a modernized LACS infrastructure, and how do they support achievement of the ICAM target state?
- What common characteristics should I consider when designing a LACS solution?

### 11.2.1. Solution Architecture

The ICAM Segment Architecture presented in Part A describes the LACS target state and introduces logical access services as part of the ICAM Services Framework. One of the key characteristics of the target state is moving toward providing common logical access services

(privilege management, authentication, and authorization) at an enterprise level. Many agencies within the Federal Government are moving toward this model and the purpose of this section is to illustrate how those services are aligned within a LACS solution. The solution architecture outlined in Figure 121 is intended to illustrate the concept of leveraging shared agency resources to provide a common set of logical access services across an agency's enterprise. The box at the center of the diagram depicts the LACS infrastructure with a variety of common components capable of supporting LACS services, as outlined in the ICAM Services Framework. These components represent generic products and are not aligned with a particular vendor or solution offering.

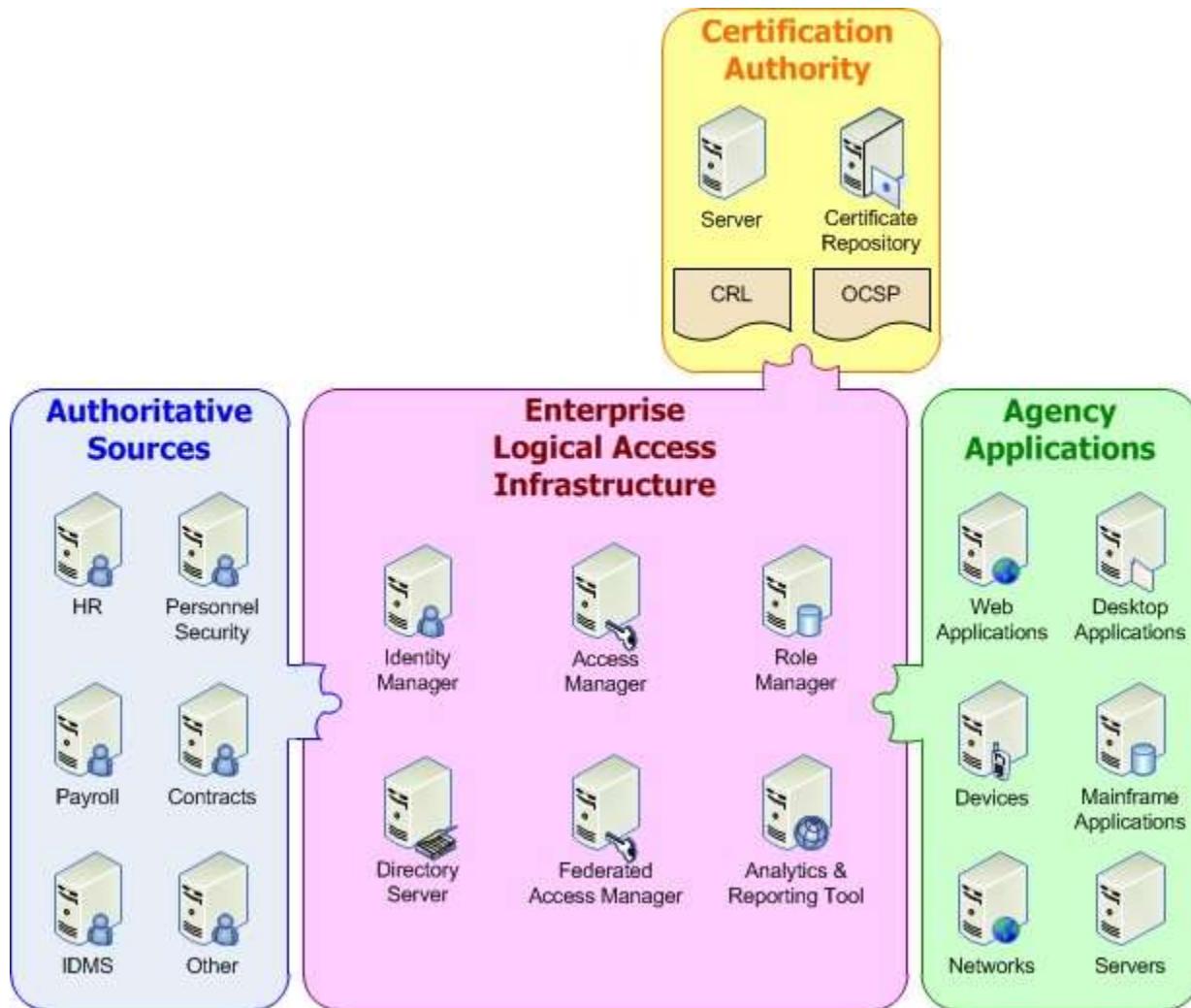


Figure 121: Logical Access Solution Architecture

The diagram above is intended to serve as a high-level depiction of the target state for LACS, and is representative of the many solution variations/designs that agencies may choose to implement. The solution components within the Enterprise Logical Access Infrastructure are represented generically and could be implemented using a variety of COTS and purpose-built products. This type of solution architecture provides both authentication and authorization services at an enterprise level for all protected resources, and is the recommended means of achieving the ICAM target state. The enterprise authentication and authorization solution is

discussed further in Section 11.2.1.1. While it is expected that enterprise LACS services, as represented in Figure 121, will be the predominant solution model in the target state, this approach may not be appropriate for all agencies or for all applications within a particular agency. Situations may exist where it is either not feasible to deploy such a solution, or not practical or cost effective to integrate particular applications if such a solution exists. In support of these situations, sections 11.2.1.2, 11.2.1.3, and 11.2.1.4 discuss several of the most common variations on the enterprise LACS services solution architecture presented above and provide examples of where it may be advantageous to pursue an alternate approach.

#### **11.2.1.1. Enterprise Authentication and Authorization**

In the enterprise authentication and authorization architecture outlined in Figure 121, an agency's IT resources are integrated with one or more central LACS solutions that provide both user authentication and authorization services for the integrated resources. This model allows resource owners to leverage authoritative identity data, centralized authentication, and enterprise access control enforcement to streamline the management of users and privileges for their resource. This approach is recommended for a wide variety of departments and agencies, particularly large independent agencies, agencies that are geographically centralized, or agencies with a large number of standardized web applications. Figure 122 highlights some of the potential benefits and limitations associated with the enterprise authentication and authorization solution.

Benefits	Limitations
<ul style="list-style-type: none"> <li>• Agency aligns with the preferred model for achievement of the ICAM target state for LACS</li> <li>• Agency needs can be supported by a number of widely available Commercial Off-The-Shelf (COTS) products/suites</li> <li>• Applications gain added security through use of a standardized authentication mechanism</li> <li>• Users may be able to experience single sign-on (SSO) capabilities across multiple applications</li> <li>• User authorization decisions are based on authoritative entitlement attributes and access privileges</li> <li>• Applications receive fine grained authorization decisions based on up-to-date user entitlements</li> <li>• Agencies realize an enhanced ability to manage user access across the user life cycle</li> <li>• Agencies and resource owners gain an enhanced ability to detect and remediate compliance issues within resources (i.e., segregation of duties [SOD]) and across one or more applications</li> <li>• Agencies have the ability to employ role-based access control based on user attributes</li> </ul>	<ul style="list-style-type: none"> <li>• Agencies may require an up-front investment to build, configure, and deploy a LACS solution</li> <li>• Agencies may experience difficult and time consuming deployment across the enterprise due to the complexity of the organization</li> <li>• Legacy applications may not easily integrate with an enterprise solution</li> <li>• Enterprise solutions may not be financially feasible for all agencies, based on size and scope of deployment</li> </ul>

**Figure 122: Benefits and Limitations of Enterprise Authentication and Authorization**

#### **11.2.1.2. Enterprise Authentication and Decentralized Authorization**

Some organizations may require a hybrid approach to providing LACS services whereby authentication is performed via enterprise authentication services, while authorization decisions are performed natively by the resource. For example, many web access management products, which could make up a part of an agency's enterprise authentication services, create and send an

identity assertion to each protected application when the user attempts to gain access.<sup>252</sup> The application itself accepts the assertion and relies on locally maintained access privileges to make a user authorization decision. Additional system components within the authentication services address other resource types, such as mainframe applications.

Terminology	
<b>Assertion</b> – a statement from an entity that verifies a user's identity, such as an enterprise authentication service, to a relying party that contains identity information about a user. Assertions may also contain verified attributes. Assertions may be digitally signed objects or they may be obtained from a trusted source by a secure protocol (e.g., Security Assertions Markup Language [SAML], Kerberos).	

Agencies may choose this type of approach for legacy applications or in situations where it makes sense for a local resource to maintain control over user authorization. For example, certain legacy applications may be incapable of processing more granular authorization decisions (e.g., role- or attribute-based) or the application does not require robust or granular authorization capability (e.g., applications with a single user role). Figure 123 highlights some of the potential benefits and limitations associated with decentralized authorization approaches.

Benefits	Limitations
<ul style="list-style-type: none"> <li>Applications benefit from the added security of a standardized authentication mechanism</li> <li>Users may be able to experience single sign-on (SSO) capabilities across multiple applications</li> <li>Applications maintain local control over authorization decisions</li> </ul>	<ul style="list-style-type: none"> <li>Authorization decisions remain highly dependent on locally managed access privileges</li> <li>Changes to the security model of the application require local code changes</li> <li>Reduced ability to detect and remediate compliance issues within resources (i.e., segregation of duties[SOD])</li> <li>Authorization may be managed inconsistently across the organization</li> <li>Reduced ability to manage users across the user life cycle</li> <li>Resource owners must continue to maintain native reporting and auditing capability</li> </ul>

Figure 123: Benefits and Limitations of Decentralized Authorization Approaches

#### 11.2.1.3. Decentralized Authentication and Enterprise Authorization

Agencies may opt for an additional hybrid solution architecture, which utilizes a decentralized approach for user authentication while leveraging an enterprise authorization service. In this model, authentication occurs at a local level as applications are configured to accept and validate user PKI certificates. Authorization occurs via an enterprise role and entitlement management service provided by one or more centrally managed authorization products. This type of approach is generally applied in agencies with very diverse or complex applications that require custom connectors or service interfaces to accept authentication decisions, or for high-risk (LOA 4)<sup>253</sup> applications that require a direct link between certificate-based authentication and the user's session. Figure 124 highlights some of the potential benefits and limitations associated with decentralized authorization approaches.

<sup>252</sup> Examples of identity assertion-based authentication technologies that extend network login to applications while maintaining local authorization decisions include Kerberos and Secure Assertion Markup Language (SAML).

<sup>253</sup> As defined in SP 800-63.

Benefits	Limitations
<ul style="list-style-type: none"> <li>Authorization decisions are based on authoritative user entitlement attributes and access privileges</li> <li>Applications receive fine grained authorization decisions based on up-to-date user entitlements</li> <li>Enhanced ability to manage user access across the user life cycle</li> <li>Enhanced ability to detect and remediate compliance issues within resources (i.e., segregation of duties [SOD]) across one or more applications</li> <li>Ability to employ role-based access control based on user attributes</li> </ul>	<ul style="list-style-type: none"> <li>Less support for enhanced enterprise level services (i.e., enterprise event auditing, single sign-on [SSO], etc.)</li> <li>Resource owners must continue to maintain native reporting and auditing capability</li> <li>Reduced ability to provision users in an automated fashion</li> <li>Authentication may be managed inconsistently across the organization</li> <li>Solution viable only at an operating system level; cannot be easily scaled for multiple web applications</li> <li>Highly complex and onerous change management processes</li> </ul>

Figure 124: Benefits and Limitations of Decentralized Authentication Approaches

#### 11.2.1.4. Decentralized Authentication and Authorization

A decentralized LACS model relies on the native authentication and authorization capabilities within each application to validate users and manage user privileges. When using the PIV credential, this approach is most often achieved by enabling applications to accept and validate PKI certificates to perform user authentication, and then performing authorization against locally maintained access privileges. In the target state, it is expected that this type of approach will be used in organizations with a relatively small number of applications where implementing a centralized LACS infrastructure is not cost effective. An agency might also choose this approach if its applications are based on proprietary technology and cannot be easily integrated with enterprise services. Typically these organizations perform a cost/benefit analysis, as described in Section 11.1.2, and discover that the cost of deploying an enterprise services solution outweighs the benefits that could be achieved. Figure 125 highlights some of the potential benefits and limitations associated with decentralized LACS approaches.

Benefits	Limitations
<ul style="list-style-type: none"> <li>Lower up-front investment required to enable LACS</li> <li>Implementation is generally faster than enterprise solutions</li> <li>Resource owners maintain control over user authentication and authorization decisions</li> <li>Low learning curve for managers and administrators</li> </ul>	<ul style="list-style-type: none"> <li>Inability to provide enhanced enterprise level services (i.e., enterprise event auditing, single sign-on [SSO], etc.)</li> <li>Resource owners must continue to maintain application specific user account and privilege data</li> <li>Authorization decisions remain highly dependent on locally managed access control lists (ACLS)</li> <li>Reduced ability to provision users in an automated fashion</li> <li>Authentication and authorization may be managed inconsistently across the organization</li> <li>Reduced ability to detect and remediate compliance issues within resources (i.e., segregation of duties [SOD])</li> <li>No visibility into whether appropriate application access on a per application basis creates policy violations when paired with other application access</li> <li>Inability to manage users across the user</li> </ul>

Figure 125: Benefits and Limitations of Decentralized Authentication and Authorization Approaches

## 11.2.2. Solution Components

LACS infrastructures consist of a variety of components, as shown in Figure 121, including shared agency resources that make up the main Enterprise Logical Access Infrastructure, authoritative identity stores, agency applications, and common components to support PIV card authentication. This section examines the individual solution components that comprise the Enterprise Logical Access Infrastructure. Each of these components can be provided by a variety of Commercial Off-The-Shelf (COTS) software products, in-house agency resources, and custom built tools. Many of the components discussed may be referred to differently by different product vendors; the component names used throughout this section are generic representations meant to be descriptive of the functionality provided by the component. In some cases more than one product or solution may be required to achieve the level of functionality described below. This varies based on each agency's selected implementation approach, infrastructure, business, and operational requirements. Agencies should examine the primary capabilities of each component discussed in this section when designing LACS solutions in order to ensure that software capabilities are consistent with the ICAM Services Framework, regardless of technology and terminology differences.

### Privacy Tip

When customizing and configuring a Commercial Off-The-Shelf (COTS) solution component or developing a purpose-built tool to address the capabilities discussed in Section 11.2.2 and its subsections, agencies must consider existing privacy requirements and regulations. Involving appropriate security and privacy personnel can help ensure that solution components are properly configured and capable of meeting data protection, transmission, storage, and disposal requirements.



### 11.2.2.1. Identity Manager

The Identity Manager is primarily designed to correlate identity attributes from a variety of authoritative sources for the purpose of provisioning user accounts to agency resources. When integrating with legacy applications, this may include integrating with the application's native user stores (locally maintained user information for administering access control) or providing service interfaces as a means of correlating existing user data with authoritative sources. The Identity Manager automates the provisioning process (i.e., creating, updating, deleting, enabling, and disabling user accounts in applications and/or directories used by enterprise access management solutions).

The Identity Manager manages an array of automated workflows that leverage technology to eliminate manual paper-driven provisioning processes.<sup>254</sup> These workflows include self-service, approval, escalation, manual tracking of approvals, ticketing requests, etc. The Identity Manager eliminates redundant collection of user identity data at the local resource level and prevents violations of segregation of duty (SOD) policies by not allowing accounts and entitlements to be provisioned if they violate a policy. A variety of COTS and purpose-built products are available to serve as the Identity Manager within a LACS infrastructure. Deployment of an Identity Manager that provides automated provisioning capabilities supports achievement of Transition Activity 8.2, as identified in Section 5.2.2.4.

<sup>254</sup> Provisioning processes, workflows, technologies, and characteristics of an automated provisioning capability are discussed in detail in Section 9.2.3.

### 11.2.2.2. Access Manager

The Access Manager provides runtime authentication and authorization decisions; enforcement services for protected applications, networks, and operating systems; and can provide an interface for managing access privileges and policies. Within the target state LACS solution architecture presented in Figure 121, the Access Manager complements the Identity Manager by integrating with the directories provisioned by the Identity Manager. Typical products that provide Access Manager functionality offer flexibility and the ability to customize the way that they are integrated into the LACS infrastructure and in the services that are provided at an enterprise level.

The Access Manager performs session management, which enables a single sign-on (SSO) experience from the user perspective, wherein a user only authenticates with the PIV credential once and can access protected applications, provided session and application policy allows it. This eliminates the need for users to authenticate multiple times, thereby streamlining the access process and creating efficiencies for end users. The authentication process occurs between the Access Manager and the individual application in a manner that is transparent to the user.

#### Terminology

**Single Sign-On (SSO)** – a mechanism by which a single act of user authentication and log on enables access to multiple independent resources.



In practice, many organizations achieve a variation called reduced sign-on, whereby a user experiences SSO for a set of resources but is required to independently authenticate to a small set other resources due to resource-specific security requirements or technical constraints.

The Access Manager can also serve as a standalone component, without the need to integrate with a dedicated Identity Manager. This is most often the case where an agency chooses to integrate its Access Manager with an existing directory (e.g., Active Directory). This model uses the agency's directory as its user store and relies on the Access Manager to manage policies and privileges in addition to making runtime authentication and authorization decisions. While this is a valid approach, the guidance presented in this chapter aligns with the preferred solution architecture outlined in Section 11.2.1.1 and assumes that the Access Manager is integrated with an Identity Manager component, unless otherwise indicated.

#### Lesson Learned

LACS architectures that use a standalone Access Manager (i.e., not integrated with an Identity Manager) may not be a viable solution for agencies that do not have a single authoritative user store, as there is no way to ensure uniqueness of users across the enterprise. A large federal agency attempted to implement a standalone Access Manager solution with disparate data sources and quickly discovered this problem. By implementing an Identity Manager, the agency was able to create unique digital identities and successfully complete their LACS modernization effort.



A number of COTS and purpose-built products are available as an Access Manager and often include a variety of pre-built or custom resource agents and service interfaces, which are used to integrate with the application and provide enterprise authorization services through policy decision making and enforcement. These agents and services allow the application to intercept unauthenticated and/or unauthorized access attempts to ensure that applications are properly protected. When designing a LACS solution agencies should consider the types of web

applications that exist within their IT infrastructure and select an Access Manager that most closely aligns with the agency’s existing investments and infrastructure requirements; this topic is discussed further in Sections 11.1.2 and 11.3.2.

#### **11.2.2.3. Role Manager**

The Role Manager integrates with the Identity Manager and supports the process of engineering roles that can be consumed by the Identity Manager and utilized in the provisioning process. Role engineering can be performed in either a top-down (step-wise definition of roles based on organizational characteristics) or bottom-up (mining existing entitlements from applications) fashion or some combination of the two. By assembling individual entitlements into logical groups the Role Manager supports business friendly RBAC.<sup>255</sup>

The Role Manager supports SOD policies by preventing the creation of roles that include access entitlements in violation of established policy. The Role Manager allows business owners, resource owners, and resource administrators to revise existing or create new access control rules/policies as business and operational requirements change over time. A variety of COTS and purpose-built products exist to perform Role Manager functions. Many of these products are designed around role-based access control with the emergence of more granular models, as described in Section 9.3, as many commercial vendors offer tools which provide greater support. When designing a LACS solution agencies should closely examine the Role Manager’s ability to interact and interface with other LACS components (both existing and new).

#### **11.2.2.4. Directory Server**

The Directory Server manages user identity data in a directory format and supports the identity attribute correlation capabilities provided by Identity Manager. This is an optional component within the LACS infrastructure and is typically used when integrating with or consolidating data from one or more directory services, such as Microsoft Active Directory or Radiant Logic Virtual Directory Server.

#### **11.2.2.5. Federated Access Manager**

The Federated Access Manager integrates with the Access Manager and Identity Manager to provide access for users that do not have identity records within the LACS (i.e., users from outside of the organization). In cases where an agency operates multiple LACS (e.g., a large agency with multiple independent bureaus/components), the Federated Access Manager may be used to enable access for users from another bureau/component within the agency by obtaining the necessary identity information from the other bureau/component’s LACS. Within the ICAM target state, it is also expected that the Federated Access Manager could support transactions across the Government-to-Government (G2G), Government-to-Business (G2B), and Government-to-Citizen (G2C) domains for users with other credential types. In these cases, the Federated Access Manager obtains the necessary identity information for these users from an appropriate Identity Provider, as discussed in Section 12.3.

In addition to enabling access for users outside of the organization, the Federated Access Manager can also extend the SSO experience for an agency’s internal users by passing the

---

<sup>255</sup> The definition of user roles and access control policies within an organization along with a discussion of access control models is provided in Section 9.3.

necessary identity information to external partner applications. This can enhance privacy by providing more granular control over what information is shared and with whom.

Considerations for deploying a federated identity management capability are discussed further in Chapter 12.

#### **11.2.2.6. Analytics and Reporting Tool**

The Analytics and Reporting Tool provides the ability to collect and correlate logged data from the other solution components discussed in this section into relevant information. Typically the Analytics and Reporting Tool is used to create a variety of reports that can be presented on a dashboard for various managers and administrators within the organization. The Analytics and Reporting Tool offers the ability to tailor reports and dashboard information based upon the user's role and management privileges. For example, a resource administrator may be allowed to view information about his/her resource, but not that of another resource. The tool also provides the capability to correlate information across multiple resources. This enables an enhanced ability to identify duplicative or orphaned accounts, detect and resolve segregation of duties (SOD) violations, and periodically re-certify a user's access need for certain resources or roles. Enhanced privilege management is discussed further in Section 9.2.2. The Analytics and Reporting Tool supports SOD by identifying where a user has been given access privileges on systems that are in conflict with established SOD policies. Additionally, the tool provides an array of enhanced management capabilities, including the ability to enable continuous monitoring and detect patterns of unauthorized access across multiple resources.

The Analytics and Reporting Tool provides resource owners with access to audit, compliance, and reporting data while reducing the administrative burden inherent with maintaining such a capability natively within the application. The Analytics and Reporting Tool is an optional component within the LACS infrastructure and while its absence does not degrade access control functionality, agencies should consider implementing it in order to achieve the enhanced capabilities that are offered.

#### **11.2.3. Common Design Characteristics**

In order to successfully build and deploy a modernized LACS solution, as defined in the target state ICAM segment architecture, it is necessary to understand the common characteristics that the solution should include in order to meet the objectives of the ICAM target state. These common characteristics are identified in Figure 126; however it is also important for agencies to consider their specific needs when designing a LACS solution.

LACS Characteristic ID	LACS Solution Characteristics
<b>LACS 1</b>	Provides a mechanism to support enterprise level provisioning of user identities.
<b>LACS 2</b>	Provides a workflow engine for executing business logic.
<b>LACS 3</b>	Provides a set of common enterprise workflows with the flexibility to handle various approval and escalation steps.
<b>LACS 4</b>	Provides support for identity management industry standards.
<b>LACS 5</b>	Provides system interfaces that are flexible and scalable in order to support provisioning requests to existing in scope platforms.
<b>LACS 6</b>	Provides automated tools for existing account discovery and correlation with individual users to the target applications.
<b>LACS 7</b>	Provides a framework to determine that the identity profiles created within the

LACS Characteristic ID	LACS Solution Characteristics
	Identity Management System (IDMS) have required integrity.
<b>LACS 8</b>	Supports deployment of connectors and service interfaces to provision identity profiles within an agency-defined timeframe (as defined in Service Level Agreements [SLA]) of receiving the identity/triggering event from sources based on entitlement policies.
<b>LACS 9</b>	Provides a management console for defining provisioning rules and policies.
<b>LACS 10</b>	Provides a provisioning repository for storage of workflow policy rules, in scope application and system attributes, access controls, and logs.
<b>LACS 11</b>	Provides interfaces to identity repositories that store identities, attributes, entitlements, roles, credentials, and other profile information.
<b>LACS 12</b>	Provides a secure self-service component for access by users over the intranet.
<b>LACS 13</b>	Allows schema extensions to accommodate custom agency data.
<b>LACS 14</b>	Provides the ability to define and enforce rules that are specific to an identity and its relationship to the agency.
<b>LACS 15</b>	Provides bi-directional communications to receive and report changes to local resources.
<b>LACS 16</b>	Provides the ability to setup, schedule, monitor and review logs for automated jobs/events.
<b>LACS 17</b>	Minimizes the use of customized code, significant schema changes and other application customization.
<b>LACS 18</b>	Provides an authentication framework that can be used across the enterprise.
<b>LACS 19</b>	Provides easy to use and customer focused authentication methods that utilize the PIV-based PKI certificates for authentication.
<b>LACS 20</b>	Provides additional identity proofing that can be used to further an authentication attempt, if necessary.
<b>LACS 21</b>	Provides an interface for native and Commercial Of-The-Shelf (COTS) application to turn over authentication decisions to the LACS components.
<b>LACS 22</b>	Provides an authorization management framework that includes entitlement administration, enforcement and audit.
<b>LACS 23</b>	Provides policy administration and authoritative policy store, a policy decision – making system and policy enforcement. This system should be aligned with the authorization management framework.
<b>LACS 24</b>	Provides policy creation tools that are designed for users and business owners.
<b>LACS 25</b>	Provides a role management framework that works in conjunction and integrates with other authorization systems in use.
<b>LACS 26</b>	Provides an authorization management framework that supports/interoperates with structured data, unstructured data, services and devices.
<b>LACS 27</b>	Provides an interface for native and COTS application to turn over authorization decisions to the LACS components.
<b>LACS 28</b>	Supports authentication and authorization of remote users using the PIV card.
<b>LACS 29</b>	Provides a requirement for the LACS system that it can differentiate between PKI policy Object Identifiers (OIDs).
<b>LACS 30</b>	Provides capability to secure IT resources provided by cloud services.

Figure 126: Common LACS Design Characteristics

### 11.3. Logical Access Technical Implementation

Implementing a LACS solution requires a well-defined solution design backed by measurable requirements that dictate how the solution should function when it is complete. While there are many potential implementation paths that an agency could choose to follow, there are several common areas that can affect the overall success and use of LACS solutions. This section

discusses these areas and provides guidance intended to streamline the implementation and integration processes. The information and guidance provided in this section is intended to provide answers to several common LACS technical implementation questions, including:

- What should I consider when configuring my agency’s workstations, networks, and servers?
- Are there any important considerations that I should be aware of when deploying the components of my LACS solution and integrating agency applications?
- What are the most common types of use scenarios that the LACS solution will need to support?

### 11.3.1. System Configuration

When implementing a LACS solution, one of the most important steps is configuring the agency’s LACS and infrastructure components to work together to support access based on cryptographic authentication of the PIV card. This section discusses configuration changes, including both hardware and software changes, to an agency’s IT infrastructure (e.g., workstations, networks, and servers) based on the type of LACS solution that is being implemented.

#### 11.3.1.1. Workstation (Desktop/Laptop) Configuration

In order to achieve the ICAM target state and utilize modernized LACS services, as defined in the ICAM Services Framework, agency workstations may require additional components in order to utilize smart cards. These additional components include:

- **Smart card readers.** Includes internal or external hardware components and associated device drivers necessary to access PKI certificate data stored on the smart card.
- **Middleware.** A software component that is required to allow communication between the smart card, smart card reader, and workstation.
- **Third party plug-ins.** A software component that may be required for workstations that run an operating system that does not support certain protocols.

To allow users to authenticate using a PIV card, agency workstations must incorporate smart card readers. Readers may be either internal (built-in) or external (add-on) components, which can be connected to workstations using existing universal serial bus (USB) connections (for external readers). Many systems today provide built-in readers, and operating system software that supports PIV card usage without middleware. Some older versions of operating systems will require middleware to support PIV credential use, and agencies may also want to provide middleware to support advanced card management features. Multiple middleware products, from a variety of approved vendors are available through the GSA FIPS 201 Evaluation Program Approved Products List.<sup>256</sup>

A third party plug-in may be necessary if the workstation OS does not natively support certain protocols. An example would be the inability of an OS to create Online Certificate Status Protocol (OSCP) requests or Server-Based Certificate Validation Protocol (SCVP) requests in support of certificate validation. If the OS does not support OSCP or SCVP, then a third party

---

<sup>256</sup>[APL](#)

plug-in can be acquired and implemented to perform these capabilities. Windows XP does not natively support OSCP or SCVP.

#### **11.3.1.2. Network Configuration**

Performing PIV-based cryptographic logon to an agency's network(s) requires the setup and configuration of many different components, all of which must be available and configured properly for PIV card logon to occur successfully. Configuring an agency's network to support PIV card logon offers a number of benefits, one such benefit is that the client strongly authenticates to the domain controller. This is accomplished through the establishment of trust and issuance of PKI device certificates to the domain controller. Unless an agency's domain controllers are already performing secure communication, it is unlikely they have a PKI device certificate issued to them.

Within the Federal Government, all PKI certificates issued to individuals to assert identity must conform to the Federal PKI Common Policy Framework<sup>257</sup> (COMMON), as discussed in Section 4.5. This is not the case for non-person entities (NPEs), particularly those that are internal facing only. The guidance presented in this section assumes that the agency is enabling a Microsoft Windows Server 2003 SP1 or later version. Agencies should consider the following:

- **Install PKI certificates.** All domain controllers require PKI certificates that have the Enhanced Key Use of Client Authentication and Server Authentication. This is relatively easy to do by installing a Microsoft CA, which comes with predesigned templates for domain controller certificates.
- **Establish mechanism to validate certificate status.** Agencies should determine where Certificate Revocation Lists (CRLs) will be published and how they will be accessible on the network and/or determine how to connect with an OCSP service.
- **Establish trust with the CA.** As part of network configuration, an agency may need to deal with distributing multiple trust chains. This situation occurs when an agency uses PIV card certificates from one provider and receives device certificates from their own Microsoft CA or a different PKI provider.
- **Map Windows user account setting to certificate.** Certificate mapping provides a more secure method for user authentication. With certificate mapping, a specific certificate is linked to the Windows account of a user. A server application can then use public key technology to authenticate the user by means of this certificate.

#### **Implementation Tip**

Mapping Windows user account settings to a specific public key is preferred over the approach of mapping to the User Principal Name (UPN) present in the user's certificate. Mapping to a specific public key mitigates the risk of someone creating a digital certificate under Common Policy that contains the same UPN, which could create a situation where unauthorized access can occur.



- **Ensure high network availability.** The network providing access to the CRLs, OCSP services, and path validation services must be highly available. Authentication of PIV cards will fail, if the certificate status or trust chain for the certificate is not available.

<sup>257</sup> COMMON

LACS components are considered high value, and should be segmented from the rest of the network. A compromise of the LACS system provides an attacker with further access to all connected resources. Components should be positioned within network segments based on a least privilege approach. CRLs, OCSP, and SCVP responders are considered public and should be in the demilitarized zone (DMZ), access management agents and proxies should be collocated with the protected agency applications, whether on the enterprise Local Area Network (LAN), or in the DMZ. Primary LACS components, Identity Manager, Access Manager, Role Manager, Directory Server, Federated Access Manager, and Analytics & Reporting Tool, should be configured in a protected subnet with access limited to only essential personnel at a network level. Additionally, networks supporting LACS components must meet NIST<sup>258</sup> standards for fail-over/redundancy capabilities to ensure high availability.

#### **11.3.1.3. Server Configuration**

Servers within a LACS infrastructure either host solution components or agency applications. All agency servers should be hardened to federally recommended or required standards, with access limited to only essential personnel. Configuring an agency's servers to support PIV card logon requires that the servers be capable of validating PKI authentication certificates presented by users. Each of the various types and models of servers deployed across the Federal Government requires a different level of configuration to support PKI authentication and PIV-based logon as the native capabilities can vary widely based on age, manufacturer, and supporting software. Agencies should work with their server manufacturers and IT personnel to determine what specific configuration steps are necessary to support the LACS implementation effort. Web-based applications utilizing the PIV credential for authentication must perform certificate status validation using CRLs or OSCP requests to ensure the validity of the authentication certificate and possibly SCVP to validate the certificate chain.

#### **FAQ**

##### **What level of support do some of the common server platforms provide for certificate status validation?**

Internet Information Services (IIS) 6.0 with Windows Server 2003 performs CRL checks, but not OCSP or Server-based Certificate Validation Protocol (SCVP) requests. Microsoft Internet Information Services (IIS) 7.0 with Windows Server 2008 and IIS 7.5 with Windows Server 2008 R2 can perform both CRL checks and OCSP requests. In all current Windows Server implementations, if the server chain is not locally available then a third party plug-in is required to perform SCVP validation.



#### **11.3.2. LACS Enterprise Solution Integration**

Integrating and deploying a LACS solution into the agency's infrastructure involves evaluation of a number of different factors. This section examines several topics that agencies should consider as part of the integration and deployment process, including:

- **Component Design.** An agency should determine which solution components are required to fulfill its logical access control requirements. As noted in Section 11.2.2, several of the components described in the solution architecture are optional. Additionally, an agency may be able to fulfill some of the functionality of the enterprise

<sup>258</sup> Specific requirements are contained in [SP 800-53](#).

logical access services with existing infrastructure or capabilities. Existing EA also needs to be revisited and possibly re-designed in order to best leverage the LACS solution. An agency should also consider and plan for adequate performance capabilities of the system to ensure that the appropriate capacity is available to operate the system and there are response provisions for server or data failures.

- **Integration Approach.** The process and technology used to integrate agency applications with the LACS infrastructure can differ for each type of application. Most major directories, databases, operating systems, and web applications can be integrated using commercially available standards-based plug-in solutions or service interfaces for provisioning and managing user accounts and access. Some legacy applications may require custom application programming interfaces (APIs) or web service calls to provide the necessary capabilities to support enterprise LACS services.
- **Security and Risk.** Agencies should consider the integrity, confidentiality, and availability considerations associated with deploying a LACS solution. This includes properly securing the digital identity data that is transmitted between LACS solution components, authoritative identity sources, and agency applications. Additionally, agencies should establish appropriate recourse and reconstitution measures, should a LACS component fail, as a means of ensuring that agency applications remain secure.

The following subsections discuss considerations for the deployment of Enterprise Logical Access Infrastructure components and integration of those components with the agency's infrastructure.

#### **11.3.2.1. Component Deployment**

The first step in deploying a modernized LACS is the installation and configuration of the main LACS components. Each LACS solution component has different considerations which must be evaluated as part of the deployment process. Figure 127 contains a list of sample considerations that agencies should assess when planning to deploy LACS solution components.

Solution Component	Deployment Considerations
<b>Identity Manager</b>	<ul style="list-style-type: none"> <li>• <b>Availability of authoritative source(s).</b> An agency should determine what source(s) are authoritative for digital identity data for its users. Integration with these sources will impact how the Identity Manager is deployed.</li> <li>• <b>Identity data cleansing and normalization.</b> Identity data within authoritative source(s) must be properly formatted (in accordance with defined standards) and reviewed for consistency and quality prior to integration with the Identity Manager.</li> <li>• <b>Ability to reconcile data changes within authoritative source(s).</b> An agency should consider how often and how quickly the Identity Manager should detect changes in the authoritative source(s) data. Changes could happen immediately through real-time messaging or in scheduled increments through either flat file reconciliation or Lightweight Directory Access Protocol (LDAP)/database queries.</li> <li>• <b>Define a unique identifier.</b> An agency should define a unique identifier for its users. The Identity Manager will key off of this identifier to reconcile and synchronize digital identity data with authoritative source(s) and when provisioning to resources.</li> <li>• <b>Provisioning.</b> An agency should determine which applications, directories, or Access Managers to provision accounts and digital identity data. Provisioning may lead to increased data integrity as well as improved access control.</li> </ul>
<b>Access Manager</b>	<ul style="list-style-type: none"> <li>• <b>Availability of out-of-the-box capabilities.</b> Many commercially available products offer a number of out-of-the-box service interfaces, web/application server plug-ins, or resource agents that are capable of supporting integration with most standards-based applications. An agency should determine which of these capabilities should</li> </ul>

Solution Component	Deployment Considerations
	<p>be deployed based on its requirements.</p> <ul style="list-style-type: none"> <li><b>Customization requirements.</b> An agency should consider the level of effort required to perform modifications and integrate with resources, even when using out-of-the-box tools, to accept information via headers or assertions when identities are asserted or mapped during run-time authentication.</li> <li><b>Application modification.</b> Applications will likely require modification to support integration with an Access Manager. Modifications usually include changing the application's login module to automatically authenticate the account of the userid passed in the Hypertext Transfer Protocol (HTTP) request header.</li> <li><b>Performance requirements.</b> In order to prevent performance issues when externalizing authorization decisions to an Access Manager, it is important to consider how the system will handle multiple queries to the Policy Decision Point (PDP), as well as a PDP's ability to handle complex queries.</li> </ul>
<b>Role Manager</b>	<ul style="list-style-type: none"> <li><b>Degree of integration.</b> The Role Manager can be integrated with the Identity Manager and Access Manager. Because the degree of integration dictates the Role Manager's capabilities to administer roles and handle segregation of duties (SOD), an agency should consider the appropriate level of integration for this</li> </ul>
<b>Directory Server</b>	<ul style="list-style-type: none"> <li><b>Performance requirements.</b> The Directory Server is a LACS' identity store and sometimes, the authentication source. The infrastructure should be appropriately scaled to handle the volume of authentication and authorization requests.</li> <li><b>Reuse of existing infrastructure.</b> Most agencies typically have an agency-wide directory. An agency should consider leveraging this existing directory or migrating the directory to one that will serve as the LACS' identity store. This will prevent duplication of digital identity data and likely reduce the risk of data discrepancies across the identity stores.</li> <li><b>Consolidation of directories.</b> In situations where multiple, fragmented directories exist, agencies should consider consolidating into a single agency directory to streamline the integration process and minimize the risk of having duplicative,</li> </ul>
<b>Federated Access Manager</b>	<ul style="list-style-type: none"> <li><b>Intra-agency federation.</b> As previously discussed, organizations (e.g., components/bureaus) within an agency may already have LACS solutions in place. To capitalize on the resources committed and investments made, leveraging a federated access management model to enable user access across the agency enterprise should be considered. Regardless of which organization within the agency is the Identity Provider or service provider, a key consideration is the identification and synchronization of digital identity data between the organizations. The agency should strive to enforce a capability that uniquely identifies individuals across the agency's enterprise in order to more easily federate across existing systems.<sup>259</sup></li> <li><b>Inter-agency federation.</b> An agency should perform a cost/benefit analysis to determine whether federating across agency boundaries is more cost-effective than requiring each agency to simply provision/manage an account as if the user belonged to that agency. Currently, the number of external users who need to access an agency's applications may not be at a critical mass; however, an agency should consider potential future business needs and externally-facing services as part of this analysis.</li> <li><b>Leveraging standards.</b> An agency should select a Federated Access Manager that leverages common industry standards for the exchange of identity information, such as Security Assertion Markup Language (SAML) and Kerberos. This will help enable interoperability with other federated access management systems and</li> </ul>
<b>Analytics and Reporting Tool</b>	<ul style="list-style-type: none"> <li><b>Existing reporting requirements.</b> An agency should examine its existing reporting requirements and model the reporting capabilities of the Analytics and Reporting Tool to meet its needs.</li> <li><b>Relevance of log data.</b> An agency should determine what access event log data is</li> </ul>

<sup>259</sup> Additional information and guidance on uniquely identifying an individual is provided in Section 7.1.3.

Solution Component	Deployment Considerations
	applicable and to whom. The Analytics and Reporting tool should be configured to present this information as well as notifications and alerts.

Figure 127: LACS Solution Component Deployment Considerations

### 11.3.2.2. Application Integration

Once the primary LACS solution components have been deployed, the next step is integrating the agency’s applications and resources with the solution. A modernized LACS solution integration provides enterprise automated provisioning, authentication, authorization, analytics, and reporting and auditing services for the agency’s resources. Utilizing a modernized LACS solution to manage access to IT resources supports achievement of Transition Activity 8.1, as discussed in Section 5.2.2.4. An agency should consider the following when integrating applications to deploy these capabilities:

- **Automated Provisioning.**<sup>260</sup> The Identity Manager utilizes a number of out-of-the-box plug-ins and services interfaces to connect to agency resources. It works in conjunction with the Role Manager component to determine which target applications to provision or de-provision based on attributes like employee status, geographic location, or title change. The Identity Manager should be integrated to perform all tasks of the user life cycle, including transfers, role changes, approval workflow and delegation, and notifications. It should also be integrated to handle outlier scenarios involving user accounts on the target systems, such as addressing orphaned or questionable accounts.

FAQ	What is the difference between “push” and “pull” provisioning architectures?	?
	In “push” provisioning architectures, LACS components initiate the transmission of identity data (attributes, roles, privileges, etc.) through data feeds at predetermined time intervals or based on events, such as when the data is updated. In “pull” provisioning architectures, however, relying parties initiate the transmission of identity data from LACS components by request, when needed. Agencies should examine the viability of both “push” and “pull” architectures based on their unique business needs and technical requirements.	?

- **Authentication.** Authentication responsibility is assigned to the Access Manager. Applications should be integrated with the Access Manager to manage specific user access to web applications across the enterprise. Integration for authentication tools must not be limited to just web services, but should also have a set of (APIs) available for tighter integration. The use of digital certificates or shared secrets between the Access Manager and other LACS solution components for authentication services ensures that integrated applications can trust the authentication decisions.
- **Authorization.** Authorization responsibility belongs to the Access Manager component. The goal is to externalize the Policy Decision Point (PDP). There should also be considerations on how the Policy Enforcement Point (PEP) will capture requests to data. The requests will come either through a Uniform Resource Locator (URL) or a tight integration with the application. Considerations should be made around how tightly

<sup>260</sup> Development and deployment of a centralized automated provisioning capability supports achievement of Transition Activities 8.2, 8.3, and 8.5, as discussed in Section 5.2.2.4.

coupled (or de-coupled) a PDP and PEP are, and if/how policies for these components are stored, administered, and extracted. Additionally, an agency should consider whether to allow applications to externalize their authorization model and require the Access Manager component to perform fine-grained authorization.

- **Reporting/Auditing.** The reporting and auditing functionality of a LACS solution is very important to the integrity of all the systems. Therefore, it is important to first understand the auditing requirements and reporting requirements and benchmarking the reports based on each organization’s requirements. Reporting tools should be flexible and able to generate reports based on any number of scenarios. For example, the report tool should handle the generation of reports based on any attributes stored within an identity manager component. It should also be able to generate report activity based on a particular role from the role manager component.

#### Implementation Tip

When integrating agency IT resources with an enterprise LACS solution, an agency should analyze existing provisioning (and de-provisioning) workflows and ensure that these workflows are accurately replicated within the automated provisioning capability. This ensures that existing decision points and approval processes are maintained, while achieving the benefits afforded by leveraging technology to streamline paper-based provisioning processes.



### 11.3.3. Common Logical Access Scenarios

When implementing a LACS solution for PIV-based access across an enterprise, there are a number of common scenarios that the solution must be capable of supporting. This section identifies and discusses two of these common scenarios, network logon and client authentication to servers. Each subsection explains how these scenarios are accomplished, and introduces specific considerations that agencies should be aware of when configuring and deploying their LACS solution.

#### Implementation Tip

While transitioning an agency’s networks and applications to support PIV card logon as part of a LACS modernization effort agencies should consider implementing short term transitional solutions to help mitigate the risk of inadvertently causing users to lose access to IT resources. An example of such a solution is acceptance of multiple credentials (e.g., username/password, PIV card, token, etc.) during the transitional period. This ensures that users can continue to logon using the legacy authentication process while preparing for and transitioning to the target state PIV credential authentication process.



#### 11.3.3.1. Network Logon

Network logon is the process through which agency users utilize their PIV cards to access an agency’s computer networks and shared information systems. Successfully logging onto an agency’s network using a PIV card is reliant on proper configuration of agency infrastructure and LACS solution components, as discussed in Sections 11.3.1 and 11.3.2, respectively. The process involved in logging onto an agency network involves the user presenting a PIV-based authentication certificate to the network’s domain controller, validation of the certificate through CRL, OCSP, and SCVP processes, and matching of the user’s identity to one recognized and

accepted by the network's identity repository. When implementing network logon capabilities agencies should consider the following challenges:

- **Extracting and matching User Principal Name (UPN).** The UPN must be extracted from the user authentication certificate and matched to an identity stored in the network's identity repository (e.g., Microsoft Active Directory, Radian Logic Virtual Directory Service). This process ensures that the identity repository does not store the certificate information, but possesses the key attribute required for certificate mapping. Alternatively, the certificate could be stored within the identity repository and compared with the live authentication certificate presented. If the UPN cannot be extracted from the certificate or matched with an existing identity, then the authentication attempt will fail.
- **Achieving SSO.** It is possible to achieve SSO through network logon by passing identity assertions in the form of cookies, Kerberos tickets, or encrypted Hypertext Transfer Protocol (HTTP) headers to applications, or through agent-based authentication (i.e., through use of an Access Manager). The application handles the identity assertion and need not process the user's authentication certificate.

ROI	Enabling remote access servers and virtual private network (VPN) clients to accept the PIV card not only satisfies relevant security requirements related to remote access, <sup>261</sup> but also offers significant benefits over separate tokens or devices. Use of the PIV card eliminates the costs and administrative burden of operating a separate token infrastructure and enables an agency's users to take advantage of the digital signature and encryption capabilities of the PIV card when working remotely.	\$

#### **11.3.3.2. Client Authentication to Servers**

Client authentication to servers is the process through which users utilize their PIV cards to access an agency's IT resources that reside on web or application servers. Successfully accessing an agency's IT resources through a web or application server using a PIV card is reliant on proper configuration of agency infrastructure and LACS solution components, as discussed in Sections 11.3.1 and 11.3.2, respectively. The process through which the authentication occurs is very similar to the process for logging on to an agency's network, presented in Section 11.3.3.1, whereby the user's authentication certificate is validated by the server, and the user's identity matched to an existing identity within the identity repository.

When implementing a LACS solution agencies should consider enabling two-way Transport Layer Security (TLS) to support client authentication. Also known as mutual TLS authentication, this allows a TLS client to confirm the identity of the TLS server, and vice versa as a means of supporting cross-certificate trust. The TLS client communicates the identity of the user via the authentication certificate to the application or web server.

<sup>261</sup> As described in [M-06-16](#), agencies must allow remote access with only two-factor authentication. Per [M-11-11](#), an agency must require the use of the PIV credential as the means for authentication to access its networks and information systems.

This page is intentionally left blank.

## 12. Initiative 9: Implement Federated Identity Capability

Initiative 9 of the ICAM Transition Roadmap, as discussed in Section 5.2.2, is an agency-level ICAM implementation initiative that includes activities to support streamlined access across organizational boundaries and reduce redundancy in ICAM programs by leveraging a government-wide trust framework. The ICAM segment architecture seeks to achieve greater levels of cross-organizational efficiency by leveraging third-party credentials<sup>262</sup> (i.e., a credential issued by industry Identity Providers to assert portable identity for a user). This initiative has been further emphasized with the release of the National Strategy for Trusted Identities in Cyberspace, which encourages the use and acceptance of trusted third-party credentials for access to Federal Government services.

While previous chapters have focused exclusively on an agency's internal ICAM initiatives and interagency federation<sup>263</sup> using the PIV card, Chapter 12 addresses federation that occurs with entities and organizations external to the Federal Government. This includes an array of different user, credential, and transaction types that span the Government-to-Government (G2G), Government-to-Business (G2B), and Government-to-Citizen (G2C) environments, as introduced in Section 3.2.2.1, at all levels of assurance.<sup>264</sup> Given that these transactions occur across the Internet and involve non-federal users, data protection and privacy are of paramount importance.

This chapter is organized into the following four sections:

- **Federation Overview.** This section introduces the common need for agencies to provide access for non-federal users, discusses why an agency should consider federation, and introduces the most common trust topologies that are used to describe an agency's relationship with external parties.
- **Federal Trust Framework.** This section provides an overview of the mechanisms that exist to support acceptance of externally-issued credentials, based on the credential type, and explains how these elements support cross-organizational trust.
- **Provisioning External Users.** This section provides guidance on a number of different scenarios, processes, and mechanisms to enable agencies to provision accounts for users external to the Federal Government.
- **Federated Access Using Third-Party Credentials.** This section provides guidance for leveraging third-party credentials; including determining acceptable credentials, working with Identity Providers, and implementing a capability to accept credentials issued outside of the agency.

### 12.1. Federation Overview

Identity federation, commonly referred to simply as federation, is a term used to describe the technology, standards, policies, and processes that allow an organization to trust digital identities, identity attributes, and credentials created and issued by another organization. A core element of the Authentication Services<sup>265</sup> component of the ICAM Services Framework,

<sup>262</sup> Third-party credentials are also referred to as externally-issued credentials. These terms are used interchangeably in this document.

<sup>263</sup> See Chapter 8 for a discussion on interagency federation using the PIV card.

<sup>264</sup> [M-04-04](#)

<sup>265</sup> As introduced in the ICAM Services Framework, see Section 3.2.4.4.

federation enables an agency to provide modernized logical access control services for users, by trusting and accepting credentials that those users already have. This can allow non-federal users to access an agency's resources while minimizing and potentially eliminating the need to redundantly collect and manage identity information and credentials. Additional detail related to the process for providing logical access control services for external users can be found in Use Case 10, Grant Logical Access (Section 4.10).

Within the Federal Government, the business need to federate with a non-federal partner is driven primarily by each agency's mission. The largest consumers of federated identity data will likely be agencies with missions that involve significant collaboration with non-federal organizations (e.g., state and local governments) or provide a large number of citizen-focused services. Each agency should evaluate its citizen-focused and cross-organizational collaboration and information sharing needs to determine the need for implementing federation capabilities. The vast majority of federation transactions that occur within the Federal Government can be grouped into two categories, namely:

- **Interagency federation.** Includes federation that occurs between two or more federal agencies based upon authentication of the PIV card. Interagency federation may include the passing of identity assertions between agencies. This topic is discussed in greater detail in Chapter 8.
- **Federation with entities external to the Federal Government.** Includes federation that occurs between a federal agency and any other non-federal organization or entity (e.g., state, local, or tribal governments, commercial entities, and citizens); this type of federation is the primary focus of this chapter.

Federation is made possible through the establishment and use of common exchange protocols and agreed-upon open standards/specifications that allow an agency to authenticate a user from another organization or trust an authentication conducted outside of the agency. The use of these common rules enables an agency to place a level of trust in the federated identity and credential to which that identity is bound. Given the nature of federated transactions and the electronic exchange of identity data across organizational boundaries, there is an increased focus on security and privacy to ensure users' sensitive identity data is appropriately safeguarded.

In a federated environment, these transactions occur between trusted Identity Providers that have been approved through the Federal Trust Framework and relying parties. Identity Providers are service providers that create, maintain, and manage identity information and credentials for users, in accordance with one of the four levels of assurance.<sup>266</sup> Relying parties are entities that receive and consume identity and credential data from Identity Providers and make access control decisions based on that data, in accordance with the Federal Trust Framework and established federation governance. Section 12.2 provides a more detailed overview of the Federal Trust Framework, which exists to provide a foundational level of trust between relying parties and approved Identity Providers. Additionally, Section 12.4.2 provides guidance to help agencies select Identity Providers and credentials that have been approved through the Federal Trust Framework.

The information presented in this section is intended to assist agencies in providing answers to several common questions, including:

---

<sup>266</sup> [M-04-04](#) and [SP800-63](#).

- Why should my agency trust identity data and credentials that we did not create and issue?
- What benefits can my agency expect to see from trusting and accepting another organization's credentials?
- How can my agency connect with our external business partners and are there common approaches that can be used?

### 12.1.1. Why Federate?

The Federal Government has established a number of resources to provide a common basis for trust and interoperability and enable agencies to streamline the manner in which access is provided. In many cases, providing access for a non-federal user has often meant that an agency collects identity information about that individual and issues them a credential. The ICAM target state seeks to leverage trust mechanisms that exist under the Federal Trust Framework, discussed in Section 12.2, to enable agencies to reduce or eliminate the need to issue credentials to users that are external to the Federal Government and thus eliminate unnecessary data collection wherever possible. Agencies should leverage these mechanisms and move toward trusting and accepting third-party credentials that have been created and issued in accordance with the Federal Trust Framework. In doing so, an agency that has a mission or business need to federate with non-federal organizations and entities can achieve a number of benefits, including:

- **Cost savings.** An agency can achieve significant cost savings by leveraging digital identities that are created and managed by trusted third-parties and meet appropriate requirements for use within the Federal Trust Framework. Federation allows an agency to avoid incurring costs associated with identity proofing, credential issuance and management, and management of digital identity repositories for users outside of the organization because these services are being provided by a trusted third-party.
- **Enhanced privacy protections.** By trusting digital identities that are created and managed by trusted third-parties and complying with applicable privacy requirements, rooted in the FIPPs (see Section 6.3), an agency can significantly minimize the need to collect and manage identity information for those users, thereby reducing the likelihood of unintentional disclosure of PII.
- **Increased confidence in user identity.** In many cases, external Identity Providers have a closer relationship with remote users than is possible for most agencies. This increased proximity enables the third-party Identity Provider to issue stronger credentials by performing required in-person identity validation. These stronger credentials allow an agency's IT applications to use more robust authentication mechanisms.
- **Streamlined revocation of access.** The close relationship that external Identity Providers often have with their users means, in many cases, that they are aware of status changes within the user's record more quickly than a relying party. As such, the external Identity Provider has the ability to immediately revoke the user's credential upon the end of the relationship. Revocation of access through this process often allows an agency to more quickly and efficiently meet its obligation to remove an individual's access to an application when it is no longer required.
- **Increased security.** Federation reduces the number of accounts and credentials that an agency must manage and maintain, which could become the target for a potential attacker. When properly implemented, this can reduce instances of inappropriate access.

## 12.1.2. Federation Trust Topologies

In order to accommodate the wide range of mission and business reasons behind federation, there are a number of different information exchange approaches that an agency might choose. These approaches, referred to as topologies, differ based on the type of relationship that exists with the external parties involved and the level of trust required for the transaction and are driven by the organization's business model. Three common federation trust topologies are:

- **Point-to-Point.** Refers to a model in which an organization establishes a bi-lateral trust agreement with another organization directly and uses federation protocols to exchange data. An example of the Point-to-Point topology within the Federal Government is the Defense Support of Civil Authorities pilot program between DHS and DoD, which involved the exchange of data between the two agencies for the purpose of enabling DoD personnel to access DHS resources. Because the Defense Support of Civil Authorities pilot program involved only two organizations, the point-to-point model was deemed the most appropriate.
- **Hub-and-Spoke.** Refers to a model in which a single entity acts as a central point of communication and exchange for a number of relying parties. In this model, the relying parties do not communicate with each other; all communication and information exchange occurs through the central hub. An example of a Hub-and-Spoke topology is OMB's Max.gov knowledge sharing and collaboration portal. Max.gov acts as a central broker that each agency connects to in order to communicate and share data with other agencies. The hub-and-spoke model was selected due to the number of parties involved and the desire to consolidate data in a single location that could enforce strict access restrictions.
- **Networked.** Refers to a peer-to-peer model in which all entities are interconnected and can communicate and exchange data with all others. Entities in this model may be leveraging one or more approved Identity Providers. An example of a Networked topology is InCommon Federation, which provides a common framework for trustworthy shared management of access to online resources in support of education and research. InCommon uses the networked model because it provides a common trust and technology fabric that enables relying parties to quickly establish peer-to-peer connections as the need arises.

When establishing a new federation, it is likely that an agency will be able select a trust model to suit the specific needs of the involved parties. This decision is often affected by existing infrastructure availability, business requirements, privacy considerations, and granular attribute release needs. An agency's existing ICAM investments, such as modernized logical access control systems (LACS), may also provide additional capabilities that could impact the federation topology that best meets the agency's needs. These additional factors may drive an agency to adopt a hybrid approach that combines elements of multiple topologies, resulting in a model that closely represents the agency's needs. Regardless of the federation trust topology selected, there are a number of resources that have been established within the Federal Government to provide agencies with a foundational level of trust. When entering into an established federation; however, it is likely that the existing federation members have already chosen a trust topology. Therefore it is important than an agency examine the factors previously discussed to select a federation that most closely meets its needs.

## 12.2. Federal Trust Framework

A key facet of federation is the ability of an agency to reliably accept the identity of users from outside of the organization and ensure the trustworthiness of third-party credentials. To support this effort, the Federal ICAM Initiative has put significant work into creating a government-wide framework to enable trust in federated environments. This framework includes parallel efforts and mechanisms for establishing the trust necessary to support federation for the Federal Government based on the credential type, namely:

- **Federal PKI.** The Federal PKI (FPKI)<sup>267</sup> provides a common, government-wide infrastructure for the purpose of administering the issuance, management, and revocation of PKI certificates for the Federal Government.
- **Open Identity Initiative.** The Open Identity Initiative outlines processes, standards, and specifications that must be followed by credential issuers for credentials that are comparable to LOA 1, 2, and non-PKI 3. The two main mechanisms that comprise the Open Identity Initiative are:
  - The **Trust Framework Provider Adoption Process (TFPAP).**<sup>268</sup> A process for assessing the efficacy of industry-based trust frameworks to enable an agency to trust an externally-issued electronic identity credential at a known level of assurance comparable to the levels of assurance.<sup>269</sup> The scope of the TFPAP is limited to externally-issued credentials comparable to LOA 1, 2, and 3 (non-PKI).
  - The **Identity Scheme Adoption Process.**<sup>270</sup> A process for assessing the efficacy of schemes (i.e., specific subsets of identity management standards) to enable their use by an agency in a manner that is secure, technically interoperable, and reliable at a known level of assurance comparable to one of the four levels of assurance, as defined in SP 800-63.

Figure 128 provides an overview of the policies, standards, and technical specifications used to establish trust in Identity Providers within the FPKI and Open Identity Initiative. The sub-sections that follow provide an in-depth analysis of the mechanisms that exist within the Federal Trust Framework as they pertain to supporting trust and interoperability for PKI and non-PKI credential types.

---

<sup>267</sup> For more information, refer to the Federal PKI Infrastructure.

<sup>268</sup> For more information on the TFPAP, see [Trust Framework Provider Adoption Process \(TFPAP\) For Levels of Assurance 1, 2, and Non-PKI 3](#), Version 1.0.1, September 4, 2009.

<sup>269</sup> [M-04-04](#)

<sup>270</sup> For more information, refer to the [Identity Scheme Adoption Process](#), Version 1.0.0, July 8, 2009.

	<b>Federal PKI</b>	<b>Open Identity Initiative</b>
<b>Policies &amp; Processes</b>	<ul style="list-style-type: none"> <li><b>Federal PKI Policy Authority.</b> Working group under the ICAMSC that manages the FPKI Certification Policies and votes on whether to trust industry PKIs.</li> <li><b>Federal PKI Management Authority.</b> Operates the trust infrastructure and issues digital certificates to trusted PKIs as directed by the Policy Authority.</li> <li><b>Certificate Policy Working Group.</b> Working group which makes comparisons of industry certificate policies to federal certificate policies to see if the requirements can be mapped (policy mapping exercise). This group then provides a report to the Policy Authority for voting purposes.</li> <li><b>Independent Auditors.</b> Industry PKIs must have independent auditors assess their practices against the Certificate Policy.</li> <li><b>Federal PKI Certification Policies.<sup>271</sup></b> Certificate Policies managed by FPKI Policy Authority, COMMON, and the FBCA.</li> <li><b>Federal PKI Criteria Methodology.</b> A document which describes how industry PKIs are vetted.</li> </ul>	<ul style="list-style-type: none"> <li><b>Trust Framework Providers.</b> An organization that assesses individual Identity Providers for compliance with the policies, standards, and processes of the trust framework.</li> <li><b>Trust Framework Evaluation Team.</b> Group responsible for reviewing and evaluating Trust Framework Provider applications at a given level of assurance.</li> <li><b>Independent Auditors.</b> Leveraged by Trust Framework Providers (TFPs) as part of their assessment against Certification Policies.</li> <li><b>Trust Framework Adoption Process.</b> A process for assessing the efficacy of industry-based trust frameworks to enable an agency to trust an externally-issued electronic identity credential at a known level of assurance comparable to the levels of assurance, as described in SP 800-63.</li> </ul>
<b>Technology</b>	<ul style="list-style-type: none"> <li><b>Federal PKI Management Authority Trust Infrastructure.</b> Certificate Authorities which certify trusted issuers of certificates (i.e., certifies Certification Authorities).</li> <li><b>Federal PKI Certificate Profiles.</b> X.509 certificate profiles describe how digital certificates should look; these are analogous to SAML profiles.</li> <li><b>NIST Special Publications.</b> There are many PKI related specifications, such as NIST Special Publications which specify cryptographic algorithms used by the PKI such as SP 800-78<sup>272</sup> and SP 800-131.<sup>273</sup></li> <li><b>X.500 Standards.</b> x.509 is the standard for certificates and x.500 is the directory of protocols, these are an industry standard used at the technical level by the FPKI.</li> <li><b>RFC 5280.<sup>274</sup></b> An industry standard on how mesh PKIs work, this is the basis for the Federal PKI vision.</li> <li><b>Public Key Interoperability Test Suite (PKITS).<sup>275</sup></b> A test suite and tool that simulates a complex FPKI to facilitate product testing.</li> </ul>	<ul style="list-style-type: none"> <li><b>Federal ICAM Lab.</b> Provides testing and profiling support to determine the maturity of an identity scheme's interoperability.</li> <li><b>Identity Scheme Adoption Process.</b> Assesses the security, reliability, and technical interoperability of new identity schemes at a known level of assurance based on SP 800-63<sup>276</sup> and develops a "Scheme Profile" for use with the government.</li> <li><b>ICAM Scheme Profiles.</b> Specifies the subset of requirements and functionality within the identity scheme standard that is acceptable for government use at various LOAs based upon compliance with SP 800-63 and other security and privacy requirements.</li> <li><b>Federal PKI Management Authority E-Governance Trust Services.</b> Serves as the trust infrastructure for non-PKI federation and provides continuity with the Federal COMMON Policy for PKI.</li> </ul>

**Figure 128: Overview of Federal Trust Framework Components**

<sup>271</sup> For more information see the FPKI PA [website](#).

<sup>272</sup> [SP 800-78](#), Cryptographic Algorithms and Key Sizes for Personal Identity Verification (PIV), NIST, June 2008.

<sup>273</sup> [SP 800-131A](#)

<sup>274</sup> For more information on mesh PKI see the [Computer Security Division Computer Security Resource Center](#).

<sup>275</sup> For more information see NIST's PKI testing [website](#).

<sup>276</sup> [SP 800-63](#)

The information presented in this section is intended to assist agencies in providing answers to several common trust framework questions, including:

- What process must an organization go through to be able to certify the Identity Providers that will be offering services to my agency?
- How can my agency be sure that applications are secure when implementing identity management standards?
- How can my agency ensure that privacy is protected when interacting with external entities?

### 12.2.1. Federal PKI (FPKI)

A core component of the Federal Trust Framework, FPKI provides a common, government-wide infrastructure (e.g., policies, processes, server platforms, software, and workstations) for the purpose of administering digital certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.<sup>277</sup>

As introduced in Figure 128, the Federal PKI Policy Authority<sup>278</sup> (FPKIPA) and the Federal PKI Management Authority<sup>279</sup> (FPKIMA) are the Federal Trust Framework governance bodies for PKI credentials. The FPKIPA, an interagency body established under the CIO Council, determines that the appropriate levels of assurance are satisfied by the policies supported in the PKI domain and that the PKI domain fulfills its responsibilities under these policies. It enforces digital certificate standards for trusted identity authentication across and between federal agencies and non-federal organizations. The FPKIMA, governed under the FPKIPA, provides trust infrastructure services to support organizations in meeting their identity management and data security goals using PKI. Aligning with the technology layer of the ICAM segment architecture, the FPKIMA manages the PKI trust infrastructure, which supports the leveraging of IT investments and assets that are seen as government-wide opportunities.

The policies of the FPKIPA and services of the FPKIMA help to create an environment in which different organizations can trust each other's PKI credentials. As discussed in Sections 3.2.5 and 4.5 and illustrated in Figure 9,<sup>280</sup> creation and issuance of PKI credentials that can be trusted across the Federal Government is governed by two Federal PKI components:

- **Federal Bridge Certification Authority (FBCA).** The FBCA is an information system that facilitates acceptance of PKI certificates for transactions. The FBCA maintains peer-to-peer cross-certified relationships with Enterprise PKI implementations, including federal agency legacy PKIs and commercially-operated PKIs. Thus, both the FBCA and the entities/agencies it interacts with can maintain, issue and revoke public key certificates. This characteristic allows each entity/agency to be independent and have maximum control over their individual public key certificates. This is illustrated in Figure

---

<sup>277</sup> A complete definition can be found within the Glossary.

<sup>278</sup> For more information, refer to the [FPKIPA](#) website.

<sup>279</sup> For more information, refer to the [FPKIMA](#) website.

<sup>280</sup> Section 3.2.5 and 4.5 provide an in depth discussion of Federal PKI, as well as Figure 9 which illustrates the relationship of FBCA and FCPMA within the Federal PKI Architecture. These references can be found in Part A of the FICAM Roadmap and Implementation Guidance via [www.idmanagement.gov](#).

9, through the location of the FBCA in relation to the entities/agencies (as the FBCA is not the trust anchor),<sup>281</sup> as well as the bi-directional arrows.

- **Federal Common Policy Framework Certification Authority (FCPCA).** The FCPCA is the Federal PKI Trust Root, which acts as the top of a hierarchy. This framework, as illustrated in Figure 9, has one-way arrows from the FCPCA down to the entities/agencies in which it is maintaining, issuing or revoking digital certificates and public key certificates for. The entities/agencies in which FCPCA is interacting do not have revocation or issuance power, only the FCPCA does, thus allowing the FCPCA to have maximum control over all entities within the hierarchy. The FCPCA also includes a set of shared service providers from whom federal agencies can acquire PKI services that comply with policy requirements outlined in Federal PKI Common Policy Framework<sup>282</sup> (COMMON) and FBCA Certificate Policy.

As illustrated in Section 3.2.5, by leveraging PKI certificates issued under COMMON or issued by Certification Authorities cross-certified with the FBCA, an agency is provided with several benefits, including:

- **Streamlined compliance with federal requirements.** Agencies are to leverage the Federal PKI infrastructure to ensure that all digital certificates issued within the Federal Government are either issued under COMMON or by Certification Authorities that have been cross-certified with the FBCA.<sup>283</sup>
- **Enhanced ability to trust and leverage external PKI credentials.** PKI credentials created and issued in accordance with established Federal PKI policies and processes can be leveraged for authentication of external users. Leveraging these credentials, wherever possible, minimizes the need for agencies to issue redundant PKI credentials for external users.
- **Increased ability to leverage stronger forms of authentication.** PKI credentials are ubiquitous across the Federal Government, which means that most agencies generally have the ability to consume them without the need for significant technical or policy changes. Acceptance of PKI credentials issued by external to the Federal Government allows an agency to take advantage of strong, PKI-based authentication rather than lower assurance forms of authentication offered by non-PKI credentials.

### 12.2.2. Open Identity Initiative

The Open Identity Initiative provides a common, government-wide trust mechanism for other, non-PKI credentials types, which tend to be more prevalent with non-federal users. Non-PKI credentials come in a variety of form factors, including software and hardware-based one-time password tokens and traditional username/passwords, and can be issued at a known LOA that is comparable to 1, 2, and non-PKI 3. As part of the Open Identity Initiative, the Federal Government has established the TFPAP and Identity Scheme Adoption Process to provide a foundational level of trust in issuance processes and technical interoperability associated with

---

<sup>281</sup> A detailed discussion around a trust anchor can be found in Section 8.2.2.1.

<sup>282</sup> [COMMON](#)

<sup>283</sup> [M-05-05](#), Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services, OMB, December 20, 2004.

non-PKI credentials issued outside of the Federal Government. The following sections provide an in-depth analysis of these two mechanisms.

#### **12.2.2.1. Trust Framework Provider Adoption Process (TFPAP)**

In order for agencies to fully achieve the ICAM target state and implement a federated identity capability, they need to have confidence in the processes and policies used to provide external users with electronic identity credentials that will be used as the basis for granting access. This confidence is provided via the trust framework that governs the identity services provided to a relying party. A trust framework defines the appropriate technical and functional processes, standards, and technologies to support the operation of a federated relationship; the rules that govern the federated relationship; and the mechanisms to enforce those rules. An organization that assesses individual Identity Providers for compliance with the policies, standards, and processes of the trust framework is referred to as a Trust Framework Provider (TFP).

In order to allow the Federal Government to leverage existing industry TFPs, which assess and certify individual Identity Providers, the Open Identity Initiative created the TFPAP. The TFPAP consists of several key steps that are necessary to adopt a TFP. These steps are outlined in Figure 129.

Process Step	Description
<b>Step 1: Assessment Package Submission</b>	An Applicant TFP submits an Assessment Package that demonstrates that the Applicant's trust model and practices are comparable to federal standards at the desired level of assurance.
<b>Step 2: Value Determination</b>	The ICAMSC determines whether assessment of the Applicant would be valuable to Federal Agencies, based on several factors, including industry recognition, applicability to the Federal Government, etc.
<b>Step 3: Comparability Assessment</b>	The Trust Framework Evaluation Team assesses if the Applicant's trust framework criteria (e.g., auditing qualifications and processes, privacy criteria for member Identity Providers) are comparable to one or more specific LOAs.
<b>Step 4: Adoption Decision</b>	The ICAMSC reviews the Assessment Report and votes on whether to adopt the Applicant. Upon adoption, the Applicant is added to the Approved TFP List and posted on appropriate websites; agencies may be notified of the adoption; and the TFP can be used by the Federal Government.

**Figure 129: TFPAP Process Overview**

Once a TFP has been adopted, it then certifies industry-based Identity Providers against the requirements for LOA 1, 2, and/or non-PKI 3 based on SP 800-63.<sup>284</sup> The Identity Providers approved via this process are qualified to provide identity services to federal agencies and are placed on a —certified Identity Provider|| list.<sup>285</sup> Leveraging the TFPAP and using Identity Providers approved through the process offers an agency several benefits, including:

- **Ease of compliance with federal requirements.** As previously stated, the TFPAP allows agencies to interact with Identity Providers at a known level of assurance, meeting the requirements of M-04-04. Additionally, TFPs are assessed on their technical and policy comparability based upon the trust criteria in SP 800-63, simplifying an agency's compliance with the standard.

<sup>284</sup> [SP 800-63](#)

<sup>285</sup> An up-to-date list of approved TFPs and Identity Providers is available at [www.idmanagement.gov](#).

- **Value in supporting an agency's business.** A part of the TFPAP includes determining if the adoption of the TFP would be valuable to federal agencies. This decision is based on the TFP's industry recognition, direct applicability to the Federal Government, organizational maturity, and other factors as appropriate.
- **Assurance of privacy protections.** Due to the exchange of identity information, privacy is a significant and mandatory consideration when implementing a federated identity capability. The TFPAP includes rigorous privacy requirements, based on the FIPPs, which TFPs must ensure their member Identity Providers meet in order for their credentials to be accepted by an agency.

The TFPAP assesses how a TFP's privacy policies and practices compare to the established TFPAP Privacy Principles for non-PKI credentials, which are based on the Fair Information Practice Principles (see Section 6.3).

#### Privacy Tip

The Privacy Act of 1974<sup>286</sup> states that an agency shall not use or disclose information that was collected about an individual for any purpose other than the specified routine use in which it was originally collected. Future use of these records for other purposes requires prior written consent from the individual to whom the record pertains as well as revisions to the application's System of Records Notice (SORN) and PIA.



Figure 130 below describes the privacy principles that TFP applicants are measured against and how ICAM implementers can apply these within a federated environment.

TFPAP Privacy Principle	Description	ICAM Considerations
<b>Non-Compulsory</b>	As an alternative to 3rd-party Identity Providers, agencies should provide alternative access such that the disclosure of End User PII to commercial partners must not be a condition of access to any Federal service.	<ul style="list-style-type: none"> <li>Agencies will not require any user to disclose PII to a third party to obtain access to federal resources.</li> <li>At Level 1, agencies must provide an alternative means to access the equivalent online services.</li> <li>At Levels 2 and non-PKI 3, agencies must provide alternative means to access resources; such access may be provided offline.</li> <li>To the extent possible, federal resources should also be available on the website and accessible through an easy to use search engine.</li> </ul>
<b>Adequate Notice</b>	Identity Providers must provide End Users with adequate notice regarding federated authentication. Adequate Notice includes a general description of the authentication event, any transaction(s) with the Relying Party, the purpose of the transaction(s), and a description of any disclosure or transmission of PII to any party. Adequate Notice should be incorporated into the Opt In process.	<ul style="list-style-type: none"> <li>ICAM implementers must provide notice in accordance with the Privacy Act.</li> <li>In addition, ICAM implementers should provide in real time at the point of credential log-in, information about the user's alternatives to using a federated credential.</li> <li>ICAM implementers should consider what other information users may need for obtaining or employing a federated credential.</li> </ul>
<b>Opt In</b>	Identity Providers must obtain positive confirmation from the End User before any End User	<ul style="list-style-type: none"> <li>Identity Providers will enable the end-user to demonstrate his or her express consent to the transaction before any of the user's information is</li> </ul>

<sup>286</sup> 5 U.S.C. § 552a, Privacy Act of 1974

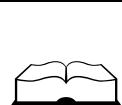
TFPAP Privacy Principle	Description	ICAM Considerations
	<p>information is transmitted to any government applications. The End User must be able to see each attribute that is to be transmitted as part of the Opt In process. Identity Provider should allow End Users to opt out of individual attributes for each transaction.</p>	<p>transmitted to the government website. This consent will be based on Adequate Notice (see above), which (1) will include identification of the specific attributes that will be transmitted from the Identity Provider to the government website and (2) could provide the opportunity to opt out of individual attributes.</p> <ul style="list-style-type: none"> <li>Users cannot opt-out of the transmission of specific attributes that are required for authentication or authorization by the ICAM implementer, although they can cancel the entire transaction and be returned to the government application.</li> <li>However, users should be given the opportunity to opt-out of attributes that the ICAM implementer would like to have transmitted, but does not need to have. For example, Identity Providers may have attributes like email addresses that could be used to pre-populate fields in the ICAM implementer's application as a convenience for the user.</li> <li>Therefore, to assist Identity Providers in providing appropriate choices to users about attribute transmissions, ICAM implementers should clearly distinguish which information is required for authentication or authorization and which information is optional for transmission.</li> <li>Doing so, will help ensure that users have meaningful notice and consent.</li> </ul>
<b>Activity Tracking</b>	<p>Commercial Identity Provider must not disclose information on End User activities with the government to any party, or use the information for any purpose other than federated authentication. Relying Party Application use of PII must be consistent with Relying Party PIA as required by the E-Government Act of 2002.</p>	<ul style="list-style-type: none"> <li>Identity Providers are prohibited from using authentication confirmations of users' credentials for any purpose other than to manage the authentication process.</li> <li>ICAM implementers must ensure that their use of information is in accordance with the ICAM implementer's PIA.</li> </ul>
<b>Minimalism</b>	<p>Identity Provider must transmit only those attributes that were explicitly requested by the Relying Party application or required by the Federal profile. Relying Party Application attribute requests must be consistent with the data contemplated in their Privacy Impact Assessment (PIA) as required by the E-Government Act of 2002.</p>	<ul style="list-style-type: none"> <li>Identity Providers may only transmit attributes that are explicitly requested by the ICAM implementer or required by the Federal profile. Therefore, ICAM implementers must ensure that they clearly specify what information Identity Providers may transmit in accordance with the ICAM implementer's PIA.</li> <li>ICAM implementers must have oversight mechanisms to ensure that Identity Providers are transmitting only what the ICAM implementer requested, including oversight of any contractors or third party software or cloud services acting as the application provider.</li> <li>Whenever possible, agencies should use validated assertions about an individual's identity or attributes in lieu of identifying data elements. For example, if an application has an age limitation, the program should ask for proof that the person meets the age requirement rather than the specific age or exact birth date.</li> </ul>

TFPAP Privacy Principle	Description	ICAM Considerations
<b>Termination</b>	In the event an Identity Provider ceases to provide this service, the Provider shall continue to protect any sensitive data including PII.	<ul style="list-style-type: none"> <li>ICAM implementers will continue to protect any PII collected from the user or linked to the user, even when its services are terminated.</li> <li>Retention of such PII will be subject to the National Archives Records Administration (NARA) retention schedules, but should be limited to that necessary for providing the service.</li> <li>Users may request to terminate their relationship with the agency at any time and request deletion of their information. Such deletion will be subject to the NARA schedule.</li> </ul>

Figure 130: TFPAP Privacy Principles

#### 12.2.2.2. Identity Scheme Adoption Process

Credentials issued by a TFP's Identity Provider, as described in the previous section, present identity assertions to applications through one or more identity schemes. Identity schemes are specific types of authentication tokens and associated protocols (e.g., OpenID, SAML assertion) that support the exchange of identity information between two parties. Identity schemes, like TFPs, need to be approved in such a way that the Federal Government has confidence implementing them within their applications. As such, the Identity Scheme Adoption Process was developed as a standard process for adopting and leveraging open standards, protocols, and technologies for government-wide implementation. The Identity Scheme Adoption Process assesses the security, reliability, and technical interoperability of new identity schemes at a known level of assurance based on SP 800-63 and develops a —Scheme Profile for use with government.

Terminology	
<b>Scheme Profile</b> – Specifies the subset of requirements and functionality within the identity scheme standard that is acceptable for government use at various LOAs based upon compliance with NIST SP 800-63 and other security and privacy requirements.	

The Identity Scheme Adoption Process consists of several key steps that are necessary to adopt a scheme. These steps are outlined in Figure 131.

Process Step	Description
<b>Step 1: Value Determination</b>	The ICAMSC determines whether adoption of a published identity scheme would be valuable to Federal Agencies. In doing so, the ICAMSC considers whether the identity scheme has (or is gaining) industry traction, uses proven technology, has (or is gaining) penetration in particular communities, has direct applicability to Federal activities, and addresses federal security and privacy considerations.
<b>Step 2: Standardization Review</b>	The ICAMSC Architecture Working Group (AWG) reviews the identity scheme to determine its viability based upon use of standards and scheme interoperability and maturity. If the assessment indicates the scheme is viable, the AWG creates a Scheme Profile. Upon conclusion of this step, the AWG delivers a report to the ICAMSC.

Process Step	Description
<b>Step 3: Adoption Decision</b>	The ICAMSC reviews the standardization report and votes on whether to adopt the identity scheme. Upon adoption, the scheme is added to the Adopted Identity Scheme List. Relying Parties and Identity Providers may be notified of the adoption as necessary, and the Scheme Profile can be used by the Federal Government.

**Figure 131: Overview of Identity Scheme Adoption Process Steps**

The following list<sup>287</sup> describes the identity schemes that have been adopted under the Identity Scheme Adoption Process:

- **ICAM OpenID 2.0.**<sup>288</sup> A standards-based protocol that facilitates exchange of messages (requests and/or responses) between endpoints for the purpose of exchanging an identity assertion that includes authentication and attribute information. In the ICAM Scheme Profile, the endpoints are typically the Relying Party and the Identity Provider.
- **ICAM Identity Metasystem Interoperability (IMI) 1.0.**<sup>289</sup> A protocol specification that facilitates portable identity through open standards such as Web Services Security (WS-Security), Web Services Trust (WS-Trust), and SOAP. IMI 1.0 can be used to conduct both low and higher-risk transactions with the Federal Government, based on factors, such as identity proofing and credential issuance.
- **ICAM Security Assertion Markup Language (SAML) 2.0 Web Browser SSO.**<sup>290</sup> An XML-based protocol for exchanging authentication and authorization data between endpoints, which uses security tokens containing assertions to pass information about an individual between an Identity Provider and a web service.

### **12.3. Provisioning Users External to the Federal Government**

In order to accurately and reliably grant access to users of government systems who are external to the Federal Government, an agency must be able to associate the identity and credential information of the individual provided by an Identity Provider to entitlement attribute information managed within the agency. This is accomplished through the process of provisioning, which is introduced in Use Case 7, Provision and De-provision User Account for an Application (Section 4.7). Provisioning, as defined in the ICAM Services Framework (Section 3.2.4.3), is the process of creating user access accounts and assigning privileges or entitlements (as defined in Section 9.2.1) within the scope of a defined process or interaction. For internal agency users, provisioning is closely intertwined with other business processes related to employee management (e.g., on-boarding, establishing employee records, etc.). The key outcome in the ICAM target state for internal users is the requirement for establishing an automated provisioning capability to streamline provisioning of user accounts, as discussed in Section 9.2.3.

Performing provisioning for external users, however, presents a number of additional challenges. In a federated environment, an agency's provisioning capability must be able to expect and process external users from other domains, which may result in name collisions or the same

<sup>287</sup> This list is up-to-date as of publication of the FICAM Roadmap and Implementation Guidance Version 2.0. For a current list, visit [www.idmanagement.gov](http://www.idmanagement.gov).

<sup>288</sup> [OpenID 2.0 Profile](#), Version 1.0.1, November 18, 2009.

<sup>289</sup> [ICAM IMI Profile](#), Version 1.0, November 18, 2009.

<sup>290</sup> [Security Assertion Markup Language \(SAML\) 2.0 Web Browser Single Sign-on \(SSO\) Profile](#), Version 1.0, September 27, 2010.

person using multiple credentials (e.g., a citizen who has and uses multiple credentials at the same federal agency web site). An agency must also be able to obtain sufficient information about the individual, typically not natively collected and stored by the agency, to associate the identity with the agency resource and support relying party authorization decisions. Once an individual has been provisioned, an agency must also associate the user's account with a credential deemed acceptable through the Federal Trust Framework.

## FAQ

### How does the provisioning process for external users differ from the process used for internal agency users?

Provisioning for external users involves obtaining user information from a trusted third party (e.g., through an authentication assertion or data exchange), as opposed to sharing information collected and managed within the agency, the approach typically used for internal users. The specific process and technology used to obtain this information from an Identity Provider is driven by the underlying business relationship and type of access.<sup>291</sup>



The guidance presented in this section seeks to address this challenge and provide answers to several common questions regarding provisioning for external users, including:

- What are the most common scenarios in which my agency may need to provision accounts for users that are external to the Federal Government?
- How can my agency collect the information about these non-federal users that is needed to establish user accounts and manage access?
- What are the most common implementation approaches to provisioning user accounts for external users?
- What potential issues should my agency consider when provisioning accounts for external users?

#### 12.3.1. Provisioning Scenarios

There are a variety of different approaches available that enable an agency to obtain information about and provision users whose affiliation is external to the Federal Government. Determining whether or not provisioning is necessary, and if so, selecting an appropriate approach is often dependent on the type of relationship that the agency has with the user and/or the user's organization, as well as the amount of information about those users that is available to the agency prior to the initial access attempt. This section provides an overview of the most common scenarios through which an agency might provision non-federal users. These scenarios are intended to provide a high-level context through which the remainder of the guidance related to provisioning non-federal users can be framed. The scenarios discussed below are not intended to represent all of the possible permutations for provisioning users that are external to the Federal Government; an agency should determine which scenario most closely represents its environment and leverage the associated guidance as best as possible.

<sup>291</sup> See Section 12.3.1 and 12.3.2 for a detailed discussion of the most common scenarios for provisioning non-federal users and techniques for obtaining user information from an Identity Provider, respectively.

#### **12.3.1.1. Business-Entity Relationship with Known User Base**

In this scenario, an agency has an established business relationship with a non-federal entity and knows which users within that organization will need access to the agency's resources. Based on the type of relationship and the nature of the required access, an agency may need to establish accounts or roles for these users in order to support relevant business transactions. Because the target user base is known, the agency has the choice of provisioning the user account in advance or waiting until the first time that the user attempts to access the application.

When provisioning in advance, an agency establishes user accounts using information provided by the business entity or the user prior to the first access attempt to the application. This approach allows a user to access the resource at the time of first attempt because his/her account has already been established. Alternatively, an agency may choose to provision an account when the user first attempts to access the application. This approach may result in delayed access to the resource but can prevent creation of unnecessary accounts which may never be used.

A common example of a business entity relationship with a known user base includes providing access to a SharePoint or similar knowledge sharing repository to known users that are performing work in accordance with a contract or agreement, such as state government employees collaborating with an agency on a research effort. In this example, the agency has an established business-entity relationship with the state and knows which employees require access to the SharePoint site. The agency has enough information from the state government and automatically establishes user accounts for the state employees and enables access using their state identity credentials.

#### **12.3.1.2. Business-Entity Relationship with Indeterminate User Base**

In this scenario, an agency has an established business relationship with a non-federal entity, but the agency does not know which individuals will need access to the agency's resources. This is commonly the case where an agency has a relationship with an organization (e.g., an educational institution), but frequent changes in the user population (e.g., students taking classes or doing research) make it difficult to predict who will need access at a given point in time. Because the target user base is unknown, an agency cannot establish user accounts prior to the initial access attempt.

Prior to the access attempt, an agency may choose to establish a common role for all users from that organization based on the type of access indicated in the business relationship. When the user first attempts access, the agency can then establish a user account using information provided by the user, the authentication mechanism, or another backend process. This may result in a delay of access, as additional approval workflows may apply to ensure that user access is provisioned appropriately.

An example of such a scenario includes providing access to the PubMed National Library of Medicine research tool or a similar subscription service. PubMed provides access to medical literature, journals, etc. for an array of users based on an organizational affiliation, such as students and teachers from an institution or educational program. In this example, the agency does not know who, specifically, from the non-federal organization will need access, but is able to provide it upon request by verifying an individual's affiliation with the non-federal entity with whom the business-entity relationship exists. In this example, a university medical student

attempts to access PubMed using his university credentials. He is prompted to enter some basic information in order to create a user account and is then able to enter the research tool.

#### **12.3.1.3. Relationship with an Individual, Known User**

In this scenario, an agency has an established relationship with a known individual based on a need to conduct business with or provide services directly to the individual. An agency may choose to establish an account or role for this individual prior to or at the time when the user first attempts to access the application. In these cases, an agency may create the user account using information provided directly by the individual or by a trusted Identity Provider, depending on the risk associated with the type of access.

An example of such a scenario includes a research study for the Centers for Disease Control and Prevention (CDC) with defined list of volunteer participants. In this example, each participant needs to access a CDC system to enter study-related information on a weekly basis. Prior to the start of the study, CDC sends an invitation request to each participant to create a user account on the research application. The user is prompted by the CDC application to enter a minimal amount of identity information to create a user account and access the application.

#### **12.3.1.4. Relationship with an Individual, Unknown User**

In this scenario, an agency has an established business or service relationship with a group of individuals that meet specified criteria, but does not know which individuals will need access to the resource at the time that the business or service is established. This scenario is common to citizen-focused government services where a user account may be necessary and access is initiated by the user based on a desire to take advantage of the service offered. Because the target user base is unknown, an agency cannot establish user accounts prior to the initial access attempt. In these cases, an agency may create the user account using information provided directly by the individual or by a trusted Identity Provider, depending on the risk associated with the type of access.

An example of such a scenario is the grants.gov web application, which is used by non-federal users to apply for and manage awarded grants. In this example, individual researchers use the application to apply for grants as they become available; however, prior to initiating the grant application process these users are unknown to the grants.gov application. In this example, the unknown user creates a user account on grants.gov and then is able to access and apply for active grants in the system.

#### **12.3.1.5. Temporary Access Session**

This scenario is not strictly a provisioning use case because no persistent user account is created within the agency resource. However, this scenario represents a number of common interactions in which a previously unknown user, external to the Federal Government, requires temporary access to an agency resource or information that is not publicly available. In order to protect the agency resource or information, the agency requests and receives information about the user that is then used to permit or deny access to the relevant resources or data. In this scenario access and identity information do not persist once a user's session has ended.

An example of such a scenario may include a Department of Education survey of public university students to determine satisfaction with financial aid services. In this example, a public university student accesses the survey using his university credential. The survey application

verifies his affiliation with a public education institution and establishes an anonymous survey session. Upon completion of the survey, the session ends and transactional details are logged in accordance with applicable FISMA requirements and NARA records retention schedules; however, the student's identity data is not retained.

### **12.3.2. Provisioning Process for External Users**

The process for provisioning users that are external to the Federal Government is very similar to the process used for internal agency users, which is well defined in Sections 4.7 and 9.2.3. However, when provisioning non-federal users, the agency must obtain identity and credential information from trusted third-party Identity Providers. This information is then used to uniquely identify the individual, verify that an account does not already exist for that user, and, if necessary, establish a user account. Due to the exchange of information, it is important to address potential security- and privacy-related issues throughout the provisioning process.

Within the provisioning process, there are two key steps that must be performed in order to accurately and reliably establish user accounts, including:

- **Disambiguation.** The process of determining whether the authenticated user is already known by a relying party application. Occurring after a user has been successfully authenticated, disambiguation begins with an attempt to map the user to an existing user account and/or entitlement privileges. This step in the provisioning process is critical to eliminating redundant user accounts for a single user. In some cases it may also be necessary to resolve name collisions (e.g., multiple Tom Smith's) during the disambiguation process. This could be accomplished through the use and exchange of unique person identifiers or multi-attribute keys that serve to uniquely identify an individual, as discussed in Section 7.1.2.
- **Account Creation.** The process of establishing a unique account specific to a single user (or possibly a user/credential combination). Account creation occurs if disambiguation determines that the user is not known and cannot be mapped to existing credential and privilege information. Access to a relying party application and any associated data or resources is determined by the roles and privileges specified for the user. Account creation typically occurs just once per user (or possibly user/credential combination). The account creation process may include the definition of user roles and access privileges, though this may occur at any time, as determined by the relying party application. It should be noted that account creation can occur in either real-time (fully automated) or can be delayed to allow for one or more offline administrator approval processes, as deemed appropriate by the relying party application.

As part of the account creation step described above, an agency may need to obtain additional information about the user to associate the identity with credential and privilege information. There are a number of ways that the agency can obtain this information from the Identity Provider, however, the specific provisioning scenario and type of additional information needed often dictates the information gathering approach that is taken. The sub-sections below provide an overview of the four main methods of gathering information about users that are external to the Federal Government, including automatic collection, prompted collection, deferred collection, and a hybrid collection approach. In each of these methods an existing trust relationship has already been established between the parties exchanging information.

### Privacy Tip

An agency should only collect the information that is considered to be minimally necessary to complete the provisioning process. As stated in M-07-16,<sup>292</sup> by collecting only the information necessary, an agency is able to reduce the volume of sensitive information they possess, which reduces the amount of PII that the agency is responsible for protecting.



#### 12.3.2.1. Automatic Information Collection

Automatic information collection involves the use of pre-existing, automated technical solutions to gather additional information about an external user at the point at which access is requested, without requiring additional human intervention. There are two main ways that automatic information collection is performed:

- **Front-Channel Automatic Collection.** This approach leverages information available directly and immediately from the authentication mechanism (e.g., contained within the SAML assertion) to obtain information needed to correctly and uniquely identify/distinguish the user and set up the user account, if necessary. Each authentication mechanism provides information in accordance with its corresponding Scheme Profile.<sup>293</sup>
- **Back-Channel Automatic Collection.** This approach uses the Backend Attribute Exchange (BAE) to obtain, in real-time, additional information needed to correctly and uniquely identify/distinguish the user and to set up the user account, if necessary.

While automatic information collection is the fastest way to obtain additional information about an external user, there are a number of benefits and limitations associated with each of the approaches described above, as discussed in Figure 132.

	Benefits	Limitations
Front-Channel	<ul style="list-style-type: none"> <li>• Information gathered in a real-time manner directly from the authentication mechanism</li> <li>• Information from the authentication mechanism is typically secured during transmission, so information integrity is protected</li> <li>• Approach requires little or additional information exchange capability between Relying Party and Identity Provider (to support provisioning)</li> </ul>	<ul style="list-style-type: none"> <li>• Information limited to what the authentication mechanism provides</li> <li>• Inclusion of additional, optional information requires negotiation between Relying Party and Identity Provider prior to authentication</li> </ul>
Back-Channel	<ul style="list-style-type: none"> <li>• Backend Attribute Exchange (BAE) provides the largest potential set of information about a user</li> <li>• Information collection request sent through BAE occurs in real-time at the point in which access request occurs</li> <li>• Information exchanged through BAE is typically secured during transmission, so information integrity is protected</li> </ul>	<ul style="list-style-type: none"> <li>• Relying Party may need to know, in advance, all of the authoritative sources that contain information about the user</li> <li>• BAE is dependent on accessing Identity Provider servers to obtain user information</li> <li>• User and Relying Party may see a delay in access processing due to reliance on external servers</li> </ul>

Figure 132: Benefits and Limitations of Automatic Information Collection

<sup>292</sup> [M-07-16](#)

<sup>293</sup> For additional information regarding Scheme Profiles refer to [www.idmanagement.gov](http://www.idmanagement.gov).

Regardless of whether front-channel or back-channel exchanges are employed, an agency should consider several important characteristics associated with automatic information collection, including:

- As necessary, a relying party application must be able to maintain and subsequently use uniquely identifying information from the authentication;
- There must be a high degree of confidence that a relying party's information about users is accurate and current; and
- A relying party must use policies and techniques capable of correctly matching the identity of the end user in its list of users, using only the information from the authentication.

Automatic information collection can be applied in a wide range of provisioning scenarios, based on the information needed to complete the provisioning process and the identity data available either through the authentication mechanism or the back-channel mechanism. Given the automated nature, however, this information collection approach is especially well-suited to support the temporary access session scenario, described in Section 12.3.1.5. In these cases, the information that is immediately available to a relying party application via the authentication transaction or back-channel mechanism is gathered and used to create custom sessions for the user, without the need for more manual time-consuming information collection methods.

#### **12.3.2.2. Prompted Information Collection**

Prompted information collection involves a real-time interaction with the user that is requesting access to the agency resource. This interaction typically includes a question/response request to the user for additional information needed to correctly and uniquely identify/distinguish the user and establish a user account, if necessary. Prompted information collection offers agencies a means of rapidly obtaining additional information about an external user; however, the information that is obtained is not being provided by an authoritative data source. There are a number of additional benefits and limitations associated with this approach that are discussed in Figure 133.

Benefits	Limitations
<ul style="list-style-type: none"> <li>• If all questions are answered by the user, then all necessary information is likely to be obtained</li> <li>• For attributes that do not require verification, information provided by the user is often the most accurate</li> </ul>	<ul style="list-style-type: none"> <li>• Access process is visually delayed, which may seem inconvenient to the user</li> <li>• User may be reluctant to provide data when unexpectedly prompted for identity information</li> <li>• Prompted user information requires careful consideration of security for data exchange and handling to prevent interception by an attacker</li> <li>• Potential for data interception may allow an attacker</li> </ul>

**Figure 133: Benefits and Limitations of Prompted Information Collection**

In addition to the benefits and limitations discussed above, an agency should consider several important characteristics associated with prompted information collection, including:

- A relying party should determine whether validation of prompted information is necessary, and if so, what validation strategy should be used. For example, the relying party may employ an external knowledge-based service provider to assist in the activation process. Determining an appropriate strategy should factor in such things as

the Risk Assessment, required level of assurance, and validation mechanisms available (e.g., BAE, cloud-based identity management services, etc.).

- As necessary, a relying party must be able to maintain and subsequently use uniquely identifying information from the authentication;
- There must be a high degree of confidence that a relying party's information about users is accurate and current; and
- A relying party must use policies and techniques capable of correctly matching the identity of the end user in its list of users, using the information from the authentication in conjunction with additional information obtained by the relying party prompting the end user.

Prompted information collection is typically used in scenarios where a business-entity or individual relationship exists, but the users are unknown to the relying party, such as in the scenarios described in Sections 12.3.1.2 and 12.3.1.4. In these cases, it is common for prompted information collection to be built into an application's workflow to collect information that was not available before the user attempted access (e.g., websites that require registration upon first visit).

#### **12.3.2.3. Deferred Information Collection**

Deferred information collection involves use of manual, out-of-band processing (e.g., offline communications with the Identity Provider, in-person information gathering, etc.) to obtain additional information needed to correctly and uniquely identify/distinguish the user and establish a user account, if necessary. This approach does not occur in real-time and may cause substantial delays in processing access requests from external users that are not known. There are a number of additional benefits and limitations associated with this approach that are discussed in Figure 134.

Benefits	Limitations
<ul style="list-style-type: none"> <li>• Manual intervention may be useful in obtaining specific information that is difficult to find or process in an automated fashion</li> <li>• Enhanced ability to verify obtained information through manual intervention</li> <li>• Greater ability to grant final provisioning approval in high security environments</li> </ul>	<ul style="list-style-type: none"> <li>• Slow approach to obtaining additional user information</li> <li>• May cause significant delays in processing external user access requests</li> <li>• Relying Party required to make risk-based determination if immediate (perhaps limited) access can be granted based on authentication data</li> <li>• Manual nature of approach may be vulnerable to errors or further delays</li> </ul>

**Figure 134: Benefits and Limitations of Deferred Information Collection**

In addition to the benefits and limitations discussed above, an agency should consider several important characteristics associated with deferred information collection, including:

- As necessary, a relying party must be able to maintain and subsequently use uniquely identifying information from the authentication;
- A relying party does not have suitable online, real-time matching policies or techniques available; and
- The organization itself (e.g., federal agency) has a suitable mechanism for contacting the end user to confirm the user's identity.

Deferred information collection can be applied across many of the scenarios described in Section 12.3.1, where the information needed to complete the provisioning process is unavailable

through the authentication mechanism or other electronic means. In situations where it would be necessary to use deferred information collection for a large number of resources or users, an agency should consider establishing an automated process to request and receive the desired data in a more streamlined and cost-effective manner.

#### **12.3.2.4. Hybrid Information Collection**

In some cases there may not be a single information collection approach that is sufficient to gather and verify the information needed to uniquely identify/distinguish the user and establish a user account, if necessary. Therefore, it may be necessary to combine elements of two or more of the methods previously discussed (e.g., a combination of front-channel automatic and prompted collection) to obtain the necessary user information. Each instance of a hybrid approach is unique and should be based on an agency or relying party application's specific business needs and security requirements; however, there are a number of common benefits and limitations associated with this type of approach, as depicted in Figure 135.

Benefits	Limitations
<ul style="list-style-type: none"> <li>• Approach is custom-tailored to meet the specific business needs and security requirements of an individual relying party application</li> <li>• Approach may be well-suited for high security or mission specific applications</li> <li>• Custom nature makes it very likely that all required additional information can be gathered and verified as accurate</li> </ul>	<ul style="list-style-type: none"> <li>• Approach may be highly complex, costly to implement, and require custom development of corresponding exchange capabilities</li> <li>• May be time consuming and cause delays in processing external user access requests, particularly where deferred collection is involved</li> </ul>

**Figure 135: Benefits and Limitations of Hybrid Information Collection Approaches**

Hybrid information collection is an extremely flexible approach that can be applied in nearly all provisioning scenarios because it is custom tailored to meet the specific needs of each relying party application. For example, combining elements of automatic and prompted information collection approaches can be used to provide users with a baseline level of access using the information available in the authentication mechanism while allowing the user to provide additional information in order to achieve a higher level of access.

#### **12.3.3. Provisioning Implementation Patterns**

When provisioning users that are external to the Federal Government, it is likely that an agency will encounter several common implementation patterns, which can create an additional challenge during the disambiguation process. For any implementation pattern, the level of difficulty associated with disambiguating a user depends upon how much information is stored in the relying party application user accounts and what information is available when the user attempts to access the relying party application. Figure 136 provides an overview of the more common patterns that an agency may encounter and provides guidance and considerations to help an agency resolve the additional challenge.

Implementation Pattern	Description	Guidance / Considerations
<b>New Account with one Credential Type</b>	Simplest of the implementation patterns, a relying party application accepts only one credential type and therefore creates one account per user.	<ul style="list-style-type: none"> <li>Relying party application should identify a unique person identifier to ensure easy and successful disambiguation</li> <li>Unique person identifier (if used) should still work if/when a relying party application migrates to a multiple credential environment</li> <li>Lack of a unique person identifier (see Section 7.1.3.1) to aid in disambiguation could cause a relying party application to have to create a new user account each time the user attempts to access the application</li> <li>Pattern is well-suited to front-channel automatic collection approach</li> </ul>
<b>Migration of User Accounts from one Credential Type to Another</b>	In this pattern, a relying party application is changing from one form of credential acceptance to another. For example, a relying party application has account information based upon userID and password, but is moving towards accepting only Identity Provider assertions. As end users access a relying party application with the new credential type, disambiguation must map the user with the new credential type to an account with the old credential type. This is potentially the most complex pattern, depending upon what information is stored in the original user accounts and what information is available from the new credential type.	<ul style="list-style-type: none"> <li>Account migration should occur as a one-time event (performed upon first presentation of the new credential type)</li> <li>Additional information collection (discussed in Section 12.3.2) may be required to disambiguate and map a user account to the new credential type</li> <li>A relying party should implement a policy for handling old accounts that do not get migrated after some period of time (e.g., criteria for deleting old accounts)</li> </ul>
<b>One Account per User / Credential Combination</b>	In this pattern, a relying party application creates a separate account for each user/credential combination. This results in a multiple, unique accounts for each user holding multiple credentials.	<ul style="list-style-type: none"> <li>Only the account associated with the presented credential (used for authentication) can be accessed at any one time</li> <li>Pattern may require additional relying party system resources if many multi account users exist</li> <li>Approach may be well-suited for users that hold multiple roles within a single application</li> </ul>
<b>One Account per User Regardless of the Number of Credentials</b>	In this pattern, a relying party application creates one account for each user, regardless of the number of different credentials the end user presents.	<ul style="list-style-type: none"> <li>Pattern requires slightly fewer relying party system resources than the one account per user / credential approach</li> <li>Relying party application should be careful to ensure that each credential associated with a user account has all of the necessary information for successful disambiguation</li> <li>Relying party application should ensure that all credentials used by a single individual meet applicable level of assurance requirements</li> <li>Approach may be well-suited for users with a single role that hold multiple credentials (e.g., contractors)</li> </ul>

Implementation Pattern	Description	Guidance / Considerations
<b>Role-Based Accounts</b>	In this pattern, a relying party provisions access privileges on a per role basis, where each role requires a separate credential. For example, a user accesses a relying party application as an Administrator using one credential, but accesses the relying party application as a non-Administrator using another credential.	<ul style="list-style-type: none"> <li>• Pattern supports multiple credentials of the same type or different types for a single user</li> <li>• Pattern capable of supporting account creation on both the user/credential basis or per user bases</li> <li>• A relying party application should ensure that the account uniquely identifies the user and any (or all) associated credentials</li> <li>• Segregation of duties should be enforced such that aggregated privileges across multiple role-based accounts does not violate established policies</li> </ul>

**Figure 136: Overview of Provisioning Implementation Patterns**

Other implementation patterns may exist, which require different implementation approaches. An agency should evaluate which implementation scenarios apply within its organization to determine how best to leverage the guidance and considerations provided.

#### 12.3.4. Considerations for Provisioning Non-Federal Users

Regardless of the implementation pattern and information collection approach selected, there are a number of common considerations that agencies should be aware of when implementing provisioning solutions for non-federal users, including:

- **Selecting an appropriate provisioning strategy.** Selecting the most appropriate provisioning strategy depends upon several factors, including but not limited to the authentication mechanism used (i.e., the information available from the authentication mechanism – standard and optional), the impact of allowing access to a relying party application with a less than certain knowledge of the user; and privacy requirements. Therefore, a relying party should engage in the following steps to determine the most appropriate provisioning strategy:
  - Verify what attributes are provided in the authentication response from various Identity Providers;
  - Take into consideration relevant risks from the IT risk assessment;<sup>294</sup>
  - Assess privacy policies and requirements; and
  - Assess capabilities and costs associated with implementing each strategy (or hybrid).
- **Protecting personal privacy.** In order to maintain public confidence in the Federal ICAM initiative, agencies and Relying Party applications must make privacy a paramount concern. An agency should engage its Privacy Office to understand and comply with the FIPPs and applicable privacy laws and regulations, such as the Privacy Act of 1974,<sup>295</sup> OMB M-03-22,<sup>296</sup> and M-07-16.<sup>297</sup>

<sup>294</sup> [SP 800-37](#)

<sup>295</sup> [Privacy Act of 1974](#)

<sup>296</sup> [M-03-22](#), OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, OMB, September 23, 2006.

- **Utilize common, standards-based exchange protocols.** In order to facilitate trust and enhance interoperability, agencies, relying party applications, and Identity Providers should utilize common, standards based exchange protocols (e.g., LDAP/S, DSML, SAML, SPML)<sup>298</sup> when exchanging user information/attributes.
- **Providing support for multiple credentials.** In a federated environment, a user may have multiple credentials that are acceptable at a given assurance level. In fact, in the open government scenario, it is very likely that citizens will have multiple credentials. Therefore, a relying party must determine a strategy for handling the same end user that presents different credentials at different times. A key question a relying party should answer is whether all of the user/credential pairs should be (and can be) linked to the same end user (i.e., one account for the user no matter how many credentials are used by the user over time). If the answer is no, a relying party must provision users on a user/credential basis (i.e., one account per user/credential pair). In making this decision, the relying party should analyze and assess the impacts of each approach, specifically determining whether or not all of the credentials held by a single individual meet the level of assurance requirement of the relying party application. The various implementation patterns that are appropriate for dealing with multiple credential scenarios are discussed in greater detail in 12.3.3.
- **Handling provisioning failure.** Should provisioning not succeed for any reason, a relying party should analyze the cause of the provisioning failure to determine the best response. Provisioning failure could occur due to the inability to definitively identify a user, which could result from the relying party being unable to retrieve identity information from the Identity Provider. The following are some strategies for handling a provisioning failure:
  - Implement a secondary (backup) provisioning strategy. For example, a relying party normally uses just automated provisioning. However, if on occasion the automatic approach does not suffice, the relying party application uses the prompted approach to obtain any remaining information. Of course, if the backup approach is used frequently, that likely indicates that a hybrid strategy should be the primary strategy.
  - For any failure situation that cannot be rectified, if possible, a relying party application may want to place the user on a —landing page<sup>299</sup> where the end user is provided with an explanation of the failed provisioning, and information on next steps (e.g., how to contact the appropriate Help Desk).
- **De-provisioning access when it is no longer needed.** A relying party should determine whether it needs a process and mechanism to end its relationship with a user.<sup>300</sup> Doing so may be important for a number of reasons, including but not limited to security, privacy, and management of internal resources. De-provisioning likely requires deactivation of all accounts associated with the user, precluding any further access to the relying party

---

<sup>297</sup> [M-07-16](#)

<sup>298</sup> See Section 7.3.1.1 for additional information about common protocols for exchanging user data.

<sup>299</sup> A —landing page is a URL where a user may be directed based on specific criteria (e.g., certain error conditions, user has completed processing and needs to be brought to a page for guidance as to what actions to take next, etc.).

<sup>300</sup> In cases where an account does not need to be completely removed but access privileges have been changed, detailed information can be found in Section 9.2.1.

system. However, a determination must be made as to whether a single de-provisioning trigger requires deactivation of a specific user/credential pair, or indeed all accounts associated with the user regardless of credential. The latter may be difficult to do, depending upon how a relying party has implemented its user account system. In order to accurately determine de-provisioning requirements, a relying party application should seek to answer five essential questions:

- What triggers de-provisioning?
- When should the actual de-provisioning take place?
- What data needs to be retained, and what record retention schedules apply?
- Should the user be notified of the de-provisioning, if so, how?
- What redress, if any, should be available to users that believe they have been de-provisioned in error?

#### Implementation Tip

An agency should take steps to establish a policy that addresses how user accounts and corresponding user data are handled and appropriately protected or destroyed during de-provisioning of external users.<sup>301</sup> The specific requirements for account deactivation or deletion should be based upon the type of federation transactions that the agency employs, the types of users involved, and the access held by those users. For example, an agency may choose account deactivation in cases where the user is likely to return or where specific account information must be maintained for audit and reporting purposes.



- **Re-provisioning access that has been lost or changed.** User information may change over time (e.g., a user's last name may change due to marriage). A relying party should determine whether it needs revised user information to ensure the effectiveness of its user account system (e.g., to continue to definitively and uniquely identify users). If revised information is deemed necessary, a relying party should then determine the processes and mechanisms to obtain the revised information. In many cases, the Identity Provider also requires a mechanism to notify a relying party that the information it uses for provisioning has changed and to convey the revised information, either through direct communication or an out of band process. In cases where information is obtained from the user (e.g., prompted information collection) a relying party should implement some mechanism, such as a user profile update feature that the user invokes to capture the changes, however, this requires the user to proactively volunteer revised information.

#### 12.4. Federated Access Using Third-Party Credentials

The ICAM segment architecture includes a transition activity<sup>302</sup> for agencies to enable their externally facing applications to accept third-party credentials, as defined in Section 4.12, in order to reduce or eliminate the need to issue and manage redundant credentials for external users. The guidance presented in this section seeks to provide answers to several common questions regarding acceptance of third-party credentials, including:

<sup>301</sup> Additional information regarding records retention and appropriate storage methods is available in the [NARA General Records Schedules](#).

<sup>302</sup> ICAM Transition Activity 9.4, as discussed in Section 5.2.2.5.

- How do I determine which third-party credentials are acceptable for accessing my application?
- What should I know about external Identity Providers and what should I consider when working with them?
- What should I consider when planning to accept third-party credentials from my application's external users?

#### 12.4.1. Determining Acceptable Credentials

One of the first steps that an agency should take to enable the use of trusted third-party credentials is determining what types of credentials are acceptable for access. This is a multi-step process that involves careful consideration of a number of factors associated with both the application, including business, security, and infrastructure requirements, and the target user population. Figure 137 provides a high-level description of this process that agencies should seek to leverage and adapt to suit their specific mission and business needs.

Process Step	Description	Key Considerations
<b>Step 1: Determine LOA and Security &amp; Privacy Requirements</b>	Review the application's level of assurance and analyze the specific security and technology requirements and infrastructure limitations.	<ul style="list-style-type: none"> <li>• Each application's level of assurance is defined in accordance with M-04-04<sup>303</sup></li> <li>• GSA provides the eAuthentication Risk and Requirements Assessment<sup>304</sup> (e-RA) to assist in determining level of assurance</li> <li>• Application-specific security and privacy requirements should be documented in the system security plan</li> </ul>
<b>Step 2: Identify Credential Requirements</b>	Based on the application's level of assurance, review the list of approved credential schemes that meet the security, privacy, and technology requirements.	<ul style="list-style-type: none"> <li>• The application's level of assurance dictates minimally acceptable credential types<sup>305</sup></li> <li>• Additional, enhanced security controls may impact credential selection</li> <li>• Agencies should refer to guidance posted on the Federal Government's Identity Management homepage<sup>306</sup> for a current list of approved credentials</li> </ul>
<b>Step 3: Analyze User Population</b>	Analyze the target user population to determine what credentials are available or can easily be obtained that meet the requirements identified in Steps 1 and 2.	<ul style="list-style-type: none"> <li>• Determine what external credentials the target user population already has</li> <li>• Determine if additional credential types could be easily obtained</li> <li>• Determine need to support additional credential types in the future</li> <li>• Analyze potential shifts in the target user population that could affect credential types</li> </ul>
<b>Step 4: Select Acceptable Credentials</b>	Select acceptable credentials that meet the criteria established in Steps 1 and 2 and are appropriate based on the user population analysis conducted in Step 3.	<ul style="list-style-type: none"> <li>• An agency should select acceptable credentials that meet level of assurance, security, and privacy requirements and are available to the target user population</li> </ul>

Figure 137: Common Steps for Determining Acceptable Third-Party Credentials

<sup>303</sup> [M-04-04](#)

<sup>304</sup> [GSA eAuthentication Risk and Requirements Assessment](#) (e-RA).

<sup>305</sup> See [SP 800-63](#) for more information around levels of assurance.

<sup>306</sup> [www.idmanagement.gov](#)

As noted in Steps 1 and 2 of Figure 137, one of the key requirements that an agency should look to when determining which third-party credentials to accept is the application's level of assurance. The work performed by the Identity Scheme Adoption Process and the requirements contained in NIST SP 800-63 dictate which identity schemes and associated credentials are acceptable based on the application's level of assurance. Additionally, the Federal PKI Common Policy Framework<sup>307</sup> (COMMON) and the Federal Bridge Certification Authority (FBCA) Certificate Policy govern the PKI certificate types and their associated level of assurance. Figure 138 provides a summary of the schemes adopted through the Identity Scheme Adoption Process as well as the PKI certificate policies and maps them to the corresponding level of assurance for each. Figure 138 is not intended to be comprehensive; an agency should refer to idmanagement.gov for additional information and an up-to-date list of adopted schemes.

Identity Scheme <sup>308</sup>	Level of Assurance (LOA)			
	1	2	3	4
<b>Security Assertion Markup Language (SAML) 2.0 Web Browser SSO</b>	✓	✓	✓	
<b>ICAM OpenID 2.0</b>	✓			
<b>ICAM Identity Metasystem Interoperability (IMI) 1.0</b>	✓	✓	✓	
<b>Public Key Infrastructure (PKI)<sup>309</sup></b>  • PIV-Interoperable • COMMON PIV Authentication Certificate • COMMON Software Certificate • COMMON Hardware Certificate • COMMON High • Citizen and Commerce Class <sup>310</sup> • Basic • Medium • Medium Hardware • High	✓	✓	✓	✓
	✓	✓	✓	✓
	✓	✓	✓	
	✓	✓	✓	
	✓	✓	✓	✓
	✓	✓	✓	
	✓	✓		
	✓	✓	✓	
	✓	✓	✓	✓
	✓	✓	✓	

**Figure 138: Adopted Schemes and E-Authentication Levels of Assurance**

In addition to identifying what credentials meet the application's level of assurance, an agency should determine what credentials are appropriate for the target user population. An agency can determine this by performing an analysis of the target user population, as introduced in Step 3 of Figure 137. This analysis provides an agency with sufficient information about its external users to narrow down the list of minimally acceptable credentials to those that are feasible for

<sup>307</sup> [COMMON](#)

<sup>308</sup> Agencies should refer to the Federal Government's ICAM website, [www.idmanagement.gov](http://www.idmanagement.gov), for an up-to-date list of adopted schemes.

<sup>309</sup> [SP 800-63](#)

<sup>310</sup> These policies are not asserted in the user certificates, but equivalence is established through policy mapping at the Federal Bridge Certificate Authority (FBCA).

implementation. When conducting a user population analysis, an agency should consider the following:

- **Credentials that users external to the Federal Government already have.** Leveraging a credential type that is already commonly possessed by an application’s user population enables an agency to reduce redundant issuance of credentials while requiring the lowest level of effort on the part of the user. An agency should take steps to determine which trusted credentials are available for the user population, based on the application’s security and level of assurance requirements.
- **Total number of external users.** An agency should determine how many non-federal users its application has. The total population size could affect the total complexity and cost of integrating a potential credential type.
- **User information requirements.** As discussed in Section 12.3, it is often necessary to collect additional information beyond what is provided as part of the authentication transaction in order to provision user accounts. The availability of this information could vary depending on the type of credential used; however, an agency should seek to collect only the information that is minimally necessary to complete the provisioning process.
- **Ability of user to complete credential enrollment/issuance steps.** Some types of credentials require an in-person enrollment and/or issuance interaction between the user and Identity Provider. An agency should consider the ability of its user population to participate in this type of interaction when determining the feasibility of implementing a particular credential type.

#### Lesson Learned

In order to provide users (researchers, students, etc.) from higher education institutions with access to its biomedical data and research tools, NIH chose to partner with InCommon Federation and its affiliated Identity Providers (colleges, universities, etc.). Selecting InCommon enabled the NIH iTrust program to provide federated access to its target population by leveraging the trusted identities and credentials that those users already possessed.



#### 12.4.2. Identity Providers

Once an agency has selected appropriate credential(s), it then needs to establish a relationship with one or more Identity Providers capable of supporting the selected credential type(s). Identity providers that have been certified by approved TFPs, as described in Section 12.2.1, have demonstrated to have policies and practices comparable to ICAM trust requirements established for one or more adopted Scheme Profiles.<sup>311</sup> This certification and approval process helps ensure trust and interoperability for an agency relying party. If the certification process is successful, then the Identity Provider is added to a list of approved providers. Approved Identity Providers must continue to meet the requirements in order to maintain their certification.

When selecting one or more Identity Providers with which to interact, an agency should consider the following:

- **The list of approved identity providers offers protection.** The list of approved Identity Providers can be found on idmanagement.gov and is meant to be exclusive but not static.

<sup>311</sup> As introduced in the [Trust Framework Provider Adoption Process](#) for LOA 1, 2, and non-PKI 3, September 2009.

New Identity Providers may seek to be added to the approved providers list by working through an approved TFP. The list is intended to provide a layer of protection for federal agencies against potential variations in credentials that may put agencies and their applications at risk.

- **Periodically review your selected Identity Providers.** As previously mentioned, Identity Providers must consistently meet the requirements for specific credential types in order to maintain their certification. An agency should periodically review the list of approved Identity Providers to ensure that their selected provider(s) remain on the approved list and be informed as new Identity Providers become approved for use. This step minimizes risk to a relying party application and may increase the availability of the application to its external user population.
- **Determine need for additional credential and profile types.** Application owners seeking to use a credential type that has not been assessed or for which a credential profile has not been created, the Federal ICAM Initiative can create a scheme profile and begin assessing Identity Providers against the profile.
- **Consider all Identity Providers for a particular credential type.** An agency should consider all Identity Providers that may be viable for their target user population, as different Identity Providers may be more suitable for specific groups or individuals within the user population. It is unnecessary to integrate with all applicable Identity Providers in cases where it would create undue burden; however, enabling multiple Identity Providers provides a greater selection for customers.

As previously discussed, external Identity Providers are assessed and certified by the approved TFPs. The following is a list of approved Identity Providers; however, agencies should refer to the Federal Government's ICAM website<sup>312</sup> for an up-to-date list:

- Google (OpenID Foundation)
- PayPal (OpenID Foundation, InfoCard Foundation)
- Equifax (InfoCard Foundation)
- VeriSign (OpenID Foundation)
- Wave

Given the non-compulsory nature of the TFPAP, it is likely that in some cases, an agency may need to serve as the Identity Provider for external users to the Federal Government that require access to the agency's applications or services. This is particularly likely when users do not have (or choose not to obtain) credentials from an external provider or for legacy applications that cannot support certain identity schemes. In these cases, an agency must follow applicable policies and guidance when establishing the identity of an individual and binding that identity to a credential.<sup>313</sup> An agency should be aware that these requirements and the associated guidance vary based on the LOA.

---

<sup>312</sup> See [www.idmanagement.gov](http://www.idmanagement.gov) for a current list of approved Identity Providers, as the list referenced is up-to-date as of publication of this document.

<sup>313</sup> As specified in [M-04-04](#) and [SP800-63](#).

### 12.4.3. Federation Governance

As discussed throughout this chapter, trust is a key enabler of federation. The components of the Federal Trust Framework, described in Section 12.2, provide the foundation for establishing trust with parties that are external to the Federal Government and help ensure that trusted third-party credentials meet minimal acceptance and interoperability criteria. However, agencies engaging in federation outside of the Federal Government should evaluate the need for additional governance to solidify the foundational level of trust, provided by the Federal Trust Framework, and establish accountability and liability with the third parties involved.

#### Lesson Learned

The Defense Manpower Data Center (DMDC) has entered into an agreement, called a Memorandum of Understanding, with the Federation for Identity and Cross Credentialing Systems (FiXs), a not-for-profit organization which provides an identity management model and governance structure for industry and government entities. Together, DMDC and FiXs have established a secure and interoperable network that is able to authenticate identity credentials between the DoD and FiXs industry partners. With this governance structure in place, DoD is able to trust identity credentials from FiXs that meet TFPAP approval.



In the context of federation, governance between Identity Providers and relying parties provides an additional layer of detail, necessary to clearly define the roles and responsibilities and technical regulations, formally establish trust, ensure data quality, and establish guidelines for accountability. There are several governance mechanisms available to agencies that help achieve this, the most common being federation agreements. Federation agreements are enacted to help ensure that a relying party application receives the information necessary to make reliable access control decisions and that that information is appropriately secured while in transit and at rest. While federation agreements will vary based on agency requirements, laws, and policies, the ICAMSC has developed a Federation Agreement Checklist<sup>314</sup> to serve as a starting point for agencies to use when developing federation agreements for information/attribute sharing. This section provides considerations that an agency should take into account when developing federation governance, including:

- **Member responsibilities.** Federation governance should detail the procedural process participants must follow in order to become and remain members in the federation. Some examples of what should be covered in regards to membership responsibilities include the application and approval process, how suspensions and revocations are handled, the fees and costs for being a federation member, how disputes will be resolved, and proactively taking steps to raise risks as they appear.
- **Governance board.** Federation governance should define the membership and roles and responsibilities of the Governance Board. This is the executive-level body with representation from primary stakeholders that guides the federation and is the final body to make decisions for the federation. This group is typically responsible for approval of any modifications and/or recommendations to guidelines, standards, or documents of the federation, as well as management and resolution of risks.

<sup>314</sup> Guidance for developing federation agreements has been developed by the ICAM Sub-committee's Architecture Working Group and is available on the [OMB Max.gov](#) website.

- **Federation management.** Federation governance should define the membership and roles and responsibilities of the Federation Management. This body manages the day-to-day operations of the federation. Some responsibilities may include developing policies and guidelines, implementing approval processes, reviewing membership conformance, ensuring validity of the documents of the federation (e.g., legal agreements/contracts), facilitating the roles, relationships and mutual obligations of all parties operating in the federation, and providing administrative support for the Governance Board.
- **Identity providers.** Federation governance should define the membership and roles and responsibilities of the Identity Providers. Identity Providers create, maintain, and manage accurate, reliable and current identity information for end users in accordance with their published procedures. Some responsibilities may include performing end user authentication and supplying the authenticated user information to relying parties, maintaining a direct relationship with end users, and communicating and implementing relevant federation rules into their agreements with end users.
- **Relying parties.** Federation governance should define the membership and roles and responsibilities of the relying parties. Relying parties supply electronic information services to users signed up with an Identity Providers.
- **Server requirements.** Federation governance should describe the technical requirements related to how the servers are configured, on-boarded, audited, and checked for quality.
- **Security and Privacy.<sup>315</sup>** Federation governance should describe the technical requirements for how security will be maintained within the federation, such as the protections for personally identifiable data collected and maintained by the federation, personnel security processes for federation administrative staff, physical security for sites hosting federation services, and processes and tools to be used to detect failures and intrusion attempts and to mediate and recover from intrusions.
- **Integration and testing.** Federation governance should describe the requirements for integrating and testing the technology that impacts the federation, such as identity management provisioning systems, authentication servers, user logon client software, commercial products, schemes or protocols, applications that consume credentials, and auditing, alerting and logging infrastructure.

#### 12.4.4. Federated Access Implementation Considerations

Enabling an agency’s externally facing applications to trust external identity information and third-party credentials is an undertaking that requires planning, support, and coordination from various groups within an agency and with the agency’s external partners. Specific planning and coordination considerations include the following:

- **Define access control requirements.** An agency should define specific access control requirements related to granting access to users external to the Federal Government by determining what levels of access are needed and employing robust access control models<sup>316</sup> to provide a more granular level of control over user access privileges. Verifying the user’s access need occurs in addition to the identity proofing process performed by the Identity Provider.

---

<sup>315</sup> Where Federal Government information is processed through the federation, this data is subject to all FISMA regulations.

<sup>316</sup> Access control models (e.g., role-based access control, attribute-based access control, etc.) are discussed in-depth in Chapter 9.3.1.

- **Determine an identity lifecycle management process for non-federal users.** In order to establish a user account for a non-federal user, an identity record will need to be created for them as part of the provisioning process (see Section 12.3.2). As discussed in Section 7.1, an agency has existing digital identity life cycle management processes in place for its internal users; however, this process may need to be expanded or modified to include a non-federal user population. Records for non-federal users may contain a different set of identity attributes, but they must be managed in a way that is consistent with existing agency requirements and processes.
- **Protect privacy of personal data.** When granting users external to the Federal Government access to an agency’s resources in a federated environment, an agency should involve representatives from their Privacy Office to ensure that all applicable privacy policies and regulations are enforced. These policies and regulations help ensure the privacy of personal information exchanged between a relying party application and Identity Provider as well as data contained within the relying party application. See Section 12.2.2.1 for a discussion on applying the TFPAP privacy principles in a federated environment.
- **Work with application owners to understand additional needs.** In addition to leveraging the existing government-wide frameworks and standards provided through the TFPAP and Identity Scheme Adoption Process, an agency should work with its application and system owners to determine if additional profiles and schemes are required to support specific mission or business needs and communicate those needs through the appropriate review and approval channels.
- **Focus on the user experience.** One of the core drivers behind accepting external users’ third-party credentials for access to agency applications is improving the user experience. An agency should keep this driver in mind when planning such a program and focus on elements that will make the access process easier or better for non-federal users, such as selecting credentials that users already have or can easily be obtained, provided security requirements are met.
- **Communicate changes to stakeholders and users.** Accepting externally issued credentials for access to government resources signals a paradigm shift for agencies and users that have traditionally relied on federally-issued credentials. The process and technology changes required to support this transition must be communicated to a relying party application’s stakeholders as well as the target user population.
- **Determine requirements for availability and incident response.**<sup>317</sup> In the event that an Identity Provider becomes unavailable due to a service outage or intrusion, the agency application may require back-up support. Each application should determine these needs independently as low availability applications can often sustain extended periods of down time while high-availability applications have little or no tolerance for service outages.

---

<sup>317</sup> More information around contingency planning can be found in [SP 800-34](#), Contingency Planning Guide for Federal Information Systems, NIST, May 2010.

More information around incident handling and response can be found in [SP 800-61](#), Computer Security Incident Handling Guide, NIST, March 2008; [SP 800-83](#), Guide to Malware Incident Prevention and Handling, NIST, November 2005; and [SP 800-86](#), Guide to Integrating Forensic Techniques into Incident Response, NIST, August 2006.

- **Incorporate into the IT change management process.**<sup>318</sup> Accepting trusted non-federally issued credentials may require changes to an agency's IT application. When planning to enable an application to federate with external parties an agency should evaluate any necessary procedural or technical changes through their established change management processes.

By enabling externally-facing applications to accept third-party credentials for users external to the Federal Government, an agency is not only able to meet objectives of the ICAM target state, but also achieve a number of benefits, including:

- **Cost savings.** Agencies that are able to leverage third-party credentials will recognize cost savings by reducing or eliminating the need to provide life cycle maintenance support on credentials for their external user population. This could include significant savings in cases where agencies are currently purchasing and distributing physical credentials, such as one-time password tokens.
- **Improved user experience.** Reducing the number of credentials that a user must manage by allowing the reuse of existing credentials provides an improved user experience, reduces the amount of personal information that the user must provide to the agency, and makes the process of accessing agency systems and services less burdensome.
- **Improved collaboration with business partners.** Agencies may be able to improve business relationships and foster enhanced collaboration through acceptance of trusted third-party credentials. This minimizes both the burden on agencies to issue and manage credentials and allows business partners to more easily obtain access to agency resources, when appropriate.

ROI	
By accepting trusted third-party credentials, the NIH iTrust program has been able to eliminate the need to issue and manage separate credentials for over approximately 100,000 non-federal users and provide these users with streamlined access to approximately 100 federated applications.	

<sup>318</sup> Additional information around configuration management can be found in [SP 800-128](#), DRAFT Guide for Security Configuration Management of Information Systems, NIST, March 18, 2010.

This page is intentionally left blank.

## Appendix A Acronym List

Acronym	Description
1:n	One-to-many
AAES	Authoritative Attribute Exchange Service
ABAC	Attribute-Based Access Control
AC	Access Control (this acronym is used when referencing the Access Control control family)
ACL	Access Control List
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
APL	Approved Products List
AU	Audit and Accountability (this acronym is used when referencing the Audit and Accountability control family)
AWG	Architecture Working Group
BAE	Backend Attribute Exchange
BIO (-A)	PIV Biometrics (-Attended)
CA	Certification Authority
CA	Security Assessment and Authorization (this acronym is used when referencing the Security Assessment and Authorization control family)
CAC	Common Access Card
CAK	Card Authentication Key
CCB	Change Control Board
CDC	Centers for Disease Control and Prevention
CHUID	Cardholder Unique Identifier
CIO	Chief Information Officer
CNSS	Committee of National Security Systems
COFG	Citizen Outreach Focus Group
COMMON	Federal PKI Common Policy Framework
COTS	Commercial Off-The-Shelf
CPIC	Capital Planning and Investment Control
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CUI	Controlled Unclassified Information
CVS	Central Verification System
DHS	Department of Homeland Security
DME	Development, Modernization, and Enhancement
DMZ	Demilitarized Zone
DNS	Domain Name Service
DOB	Date of Birth
DoD	Department of Defense
DSA	Digital Signature Algorithm
EA	Enterprise Architecture

Acronym	Description
EASR	Enterprise Architecture Segment Report
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
E.O.	Executive Order
e-QIP	Electronic Questionnaires for Investigations Processing
e-RA	E-authentication Risk and Requirements Assessment
ESC	Executive Steering Committee
ESIGN	Electronic Signatures In Global and National
ESSF	Enterprise Services Security Framework
F/ERO	Federal/Emergency Response Official
FAR	Federal Acquisition Regulation
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
FBI IAFIS	Federal Bureau of Investigation Integrated Automated Fingerprint Identification System
FCPCA	Federal Common Policy Certification Authority
FDCC	Federal Desktop Core Configuration
FEA	Federal Enterprise Architecture
FEMA	Federal Emergency Management Agency
FICAM	Federal Identity, Credential, and Access Management
FICC	Federal Identity Credentialing Committee
FIPPS	Fair Information Practice Principles
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FIWG	Federation Interoperability Working Group
FiXs	Federation for Identity and Cross Credentialing Systems
FPKI	Federal PKI
FPKIMA	Federal PKI Management Authority
FPKIPA	Federal PKI Policy Authority
FRAC	First Responder Access Card
FRCA	Federal Root Certification Authority
FSL	Facility Security Level
FSAM	Federal Segment Architecture Methodology
G2B	Government-to-Business
G2C	Government-to-Citizen
G2G	Government-to-Government
GAO	Government Accountability Office
GFIPM	Global Federated Identity and Privilege Management
GPEA	Government Paperwork Elimination Act
GSA	General Services Administration

Acronym	Description
GUID	Global Unique Identifier
HHS	Health and Human Services
HR	Human Resources
HSC	Homeland Security Council
HSPD-12	Homeland Security Presidential Directive 12
HTTP	Hypertext Transfer Protocol
IA	Identification and Authentication (this acronym is used when referencing the Identification and Authentication control family)
IAFIS	Integrated Automated Fingerprint Identification System
IAM	Identity Access Management
ICAM	Identity, Credential & Access Management
ICAMSC	Identity, Credential and Access Management Subcommittee
ICC	Integrated-Circuit Chip
ICF	Information Card Foundation
ICI-IPC	Information and Communications Infrastructure Interagency Policy Committee
ID	Identification
IDMS	Identity Management System
IdP	Identity Provider
IEE	Internal Effectiveness & Efficiency
IEC	International Electrotechnical Commission
IG	Inspector General
IIS	Internet Information Services
IMI	Identity Metasystem Interoperability
IP	Internet Protocol
IPC	Interagency Policy Committee
IPSec	Internet Protocol Security
IRC	Information Resources Catalog
IRS	Internal Revenue Service
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISE	Information Sharing Environment
ISC	Interagency Security Committee
ISO	International Organization for Standardization
ISIMC	Information Security and Identity Management Committee
IT	Information Technology
JPAS	Joint Personnel Adjudication System
KRA	Key Recovery Agent
LACS	Logical Access Control Systems
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LOA	Level of Assurance
LRA	Local Registration Agent
MAC	Media Access Control

Acronym	Description
MAS	Multiple Award Schedule
MINEX	Minutia Exchange
NAC	National Agency Check
NACI	National Agency Check with Written Inquiries
NARA	National Archives Records Administration
NASA	National Aeronautics and Space Administration
NCES	Net-Centric Enterprise Services
NCIC	National Crime Information Center
NFPA	National Fire Protection Agency
NFI	Non-Federal Issuers
NIEM	National Information Exchange Model
NIPP	National Infrastructure Protection Plan
NISC	Network and Infrastructure Security Sub Committee
NIST	National Institute of Standards and Technology
NIST-ITL	National Institute of Standards and Technology Information Technology Lab
NPE	Non-Person Entity
NSC	National Security Council
NSS	National Security Staff
NSTC	National Science and Technology Council
O&M	Operations and Maintenance
OASIS	Organization for the Advancement of Structured Information Standards
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OCISO	Office of the Chief Information Security Officer
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSIPS	Open, Systems Integration and Performance Standards
PACS	Physical Access Control Systems
PBAC	Policy-Based Access Control
PBS	Public Building Service
PCI	PIV Card Issuers
PDP	Policy Decision Point
PDVAL	Path Discovery and Validation
PE	Physical and Environmental Protection (this acronym is used when referencing the Physical and Environmental Protection control family)
PEP	Policy Enforcement Point
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIMM	PIV Card Implementation Maturity Model

Acronym	Description
PIN	Personal Identification Number
PIPS	Personnel Investigations Processing System
PIV	Personal Identity Verification
PIV-AUTH	PIV Authentication Key
PIV-I	Personal identity Verification Interoperable
PKI	Public Key Infrastructure
PKITS	Public Key Interoperability Test Suite
PMO	Program Management Office
PRM	Performance Reference Model
PRQP	PKI Resource Query Protocol
RA	Registration Authority
RA	Risk Assessment (this acronym is used when referencing the Risk Assessment control family)
RAdAC	Risk-Adaptable Access Control
RBAC	Role-Based Access Control
RDT	Roadmap Development Team
REBCA	Research & Education Bridge Certification Authority
RMF	Risk Management Framework
ROI	Return on Investment
RSA	Rivest, Shamir and Adleman
SAML	Security Assertion Markup Language
SASC	Security Acquisitions Sub Committee
SCVP	Server-based Certificate Validation Protocol
SDK	Software Development Kit
SDLC	System Development Life Cycle
SF	Standard Form
SHA	Secure Hash Algorithm
SIA	Security Industry Association
SIN	Special Item Number
SIP	Shared Infrastructure Provider
SLA	Service Level Agreement
SMS	Security Management System
SMTP	Simple Mail Transfer Protocol
SPMSC	Security Program Management Subcommittee
SOAP	Simple Object Access Protocol
SOD	Segregation of Duties
SORN	System of Records Notice
SP	Special Publication
SRM	Service Component Reference Model
SSA	Social Security Administration
SSL	Secure Socket Layer
SSN	Social Security Number

Acronym	Description
SSO	Single Sign-on
SSP	Shared Service Provider
TAMP	Trust Anchor Management Protocol
TFPAP	Trust Framework Provider Adoption Process
TFP	Trust Framework Provider
TIC	Trusted Internet Connection
TLS	Transport Layer Security
TrUID	Treasury Unique Identifier
TSCP	Transglobal Secure Collaboration Program
UCore	Universal Core
UL	Underwriters Laboratories
UPN	User Principal Name
URL	Uniform Resource Locator
USB	Universal Serial Bus
USDA	United States Department of Agriculture
UUID	Universally Unique Identifier
VIS	Visual Authentication Mechanism
VMS	Visitor Management System
VPN	Virtual Private Network
WS	Web Service
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

## Appendix B Glossary

Please note, the FICAM Roadmap and Implementation Guidance is a compilation of relevant terms and definitions from various sources. Many of the terms presented below are specific to the FICAM Roadmap and Implementation Guidance as discussed within the Use Cases or have been tailored to best suit this document.

Term	Definition
Access Control	The process of granting or denying specific requests: 1. for obtaining and using information and related information processing services; and 2. to enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances). <sup>319</sup>
Access Control List (ACL)	1. A list of permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object. 2. A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity. <sup>320</sup>
Access Management	The management and control of the ways in which entities are granted or denied access to the resources of an organization and are authorized to perform a specific action(s) within a given resource.
Account Management	ICAM Services Framework service component within the Privilege Management service type. The processes of requesting, establishing, issuing, and closing user accounts; tracking users and their respective access authorizations; and managing these functions. <sup>321</sup>
Adjudication	ICAM Services Framework service component within the Digital Identity service type. 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: <ul style="list-style-type: none"><li>• suitable for Government employment;</li><li>• eligible for logical and physical access;</li><li>• eligible for access to classified information;</li><li>• eligible to hold a sensitive position; or</li><li>• fit to perform work for or on behalf of the Government as a contractor employee.</li></ul> <sup>322</sup>
Adjudicator	Individual who 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.
Applicant	Individual who requests 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 individual responsible for the maintenance and implementation of access control rights. Application Administrators should not be the approvers due to separation of duties.

<sup>319</sup> As defined in [FIPS 201](#), Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006. [FIPS 201]

<sup>320</sup> As defined in [RFC 4949 Internet Security Glossary](#), Version 2, August 2007.

<sup>321</sup> As defined in [SP 800-12](#), An Introduction to Computer Security: The NIST Handbook, NIST, October 1995. [SP 800-12]

<sup>322</sup> As defined in the [Executive Order 13467](#), Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, The White House, June 30, 2008. [E.O. 13467]

Term	Definition
Assertion	A statement from which an entity verifies a user's identity, such as an enterprise authentication service, to a relying party that contains identity information about a user. Assertions may also contain verified attributes. Assertions may be digitally signed objects or they may be obtained from a trusted source by a secure protocol <sup>323</sup> (e.g., Security Assertions Markup Language ((SAML), Kerberos).
Assurance	Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. <sup>324</sup>
Attribute	A claim of a named quality or characteristic inherent in or ascribed to someone or something. <sup>325</sup>
Attribute Authority	An entity recognized as having the authority to verify the association of attributes to an identity. <sup>326</sup>
Attribute Based Access Control (ABAC)	Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place. <sup>327</sup>
Attribute Contract	A document that extensively describes the agreement on the set of, and syntax of, attributes that members of a federation have to abide by on the "payload."
Attribute Management	The act of dynamically creating, maintaining, disseminating, and revoking attributes (e.g., clearances, citizenship, location, biometrics, group memberships, and work roles), which are assigned and bound to subjects. <sup>328</sup>
Audit Trail	ICAM Services Framework service component within the Auditing and Reporting service type. A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result. <sup>329</sup>
Auditing and Reporting	ICAM Services Framework service type made up of service components. 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.
Authentication	The process of verifying that a claimed identity is genuine and based on valid credentials. <sup>330</sup>
Authoritative Attribute Exchange Service (AAES)	ICAM Services Framework service component within the Digital Identity service type. Service that performs discovery and mapping of attributes from authoritative source repositories and enables sharing of these attributes.
Authoritative Data Source	The repository or system that contains attributes about an individual and is considered to be the primary or reliable source for this information. The data in the authoritative data source is used in situations where two or more systems that house an individual's identity data have mismatched or conflicting information.

<sup>323</sup> Adapted from [SP 800-63](#).

<sup>324</sup>Please see [M-04-04](#).

<sup>325</sup> As defined in the ICAM Lexicon. The ICAM Lexicon is a comprehensive list of ICAM related definitions currently being used throughout multiple organizations within the Federal Government; identifies any divergence in terminology; and selects a preferred term and definition for continued usage within the Committee on National Security Systems. It was compiled using the FICAM Roadmap as the baseline.

<sup>326</sup> Adapted from [SP 800-32](#), Introduction to Public Key Technology and the Federal PKI Infrastructure, February 26, 2001 and [X.509 Certificate Policy For The Federal PKI Common Policy Framework](#). [SP 800-32]

<sup>327</sup> As defined in [CNSS 4009](#), Committee on National Security Instructions.

<sup>328</sup> As defined in the ICAM Lexicon.

<sup>329</sup> As defined in the [Federal Enterprise Architecture \(FEA\) Practice Guidance](#), November 2007. [FEA]

<sup>330</sup> As defined in the ICAM Lexicon.

Term	Definition
Authorization	The processes of granting or denying specific requests for obtaining and using information processing services or data and to enter specific physical facilities.
Authorization and Access	ICAM Services Framework service type made up of service components. 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 approval purposes, enforcing security policies that govern access throughout the enterprise.
Authorizer	Individual that approves or denies access to applications or facilities based on business rules.
Backend Attribute Exchange (BAE)	A standards-based architecture and interface specification to securely obtain attributes of subjects (e.g., PIV card holders, federation members) from authoritative sources to make access control decisions and/or to do provisioning.
Backend Attribute Retrieval	ICAM Services Framework service component within the Authorization and Access service type. Service acquires additional information not found in the authenticated credential that is required by a relying party to make an access based decision.
Bind/Unbind	ICAM Services Framework service component within the Privilege Management service type. Building or removing a relationship between an entity's identity and further attribute information on the entity (e.g., properties, status, or credentials). <sup>331</sup>
Biometric Validation	Services Framework service component within the Authentication services type. Services to support capturing, extracting, comparing and matching a measurable, physical characteristic or personal behavior 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. <sup>332</sup>
Biometrics	A measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition. <sup>333</sup> 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. <sup>334</sup>
Cardholder/Credential Holder	An individual possessing an issued token, PKI certificate, PIV Card or other authentication device. <sup>335</sup>
Central 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. <sup>336</sup>
Certificate	A data object containing a subject identified, a public key, and other information that is digitally signed by a Certification Authority. Certificates convey trust in the relationship of the subject identifier to the public key. <sup>337</sup>

<sup>331</sup> Adapted from the [COMMON](#).

<sup>332</sup> Adapted from [FIPS 201](#).

<sup>333</sup> Adapted from the [Identity Management Task Force Report 2008](#).

<sup>334</sup> Adapted from [FIPS 201](#).

<sup>335</sup> Adapted from [FIPS 201](#).

<sup>336</sup> Please see the [Office of Personnel Management \(OPM\)](#) website.

<sup>337</sup> As defined in the ICAM Lexicon.

Term	Definition
Certificate Revocation List (CRL)	A signed artifact composed of all revoked or otherwise suspended certificates issued from a CA that can be used to verify the current status of a PKI certificate. <sup>338</sup>
Certificate Status Servers	The counterpart to the Certification Authority that passes revocation and expiration status to relying parties in real time. <sup>339</sup>
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs. <sup>340</sup>
Continuous Monitoring	One of six steps in the Risk Management Framework (RMF) described in NIST SP 800-37. The objective of a continuous monitoring program is to determine if the complete set of planned, required, and deployed security controls within an information system or inherited by the system continue to be effective over time in light of the inevitable changes that occur. <sup>341</sup>
Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by an entity. <sup>342</sup>
Credential Lifecycle Management	ICAM Services Framework service component within the Credentialing service type. Refers to maintenance of a credential and associated support over the lifecycle; common processes include renewal, reissuance, suspension, blocking and unblocking, revocation, etc. Life cycle support activities vary depending on the credential type, and may include a Self Service Component. <sup>343</sup>
Credential Service Provider	A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The Credential Service Provider may encompass Registration Authorities and verifiers that it operates. A Credential Service Provider may be an independent third party, or may issue credentials for its own use. <sup>344</sup>
Credential Validation	Services Framework service component within the Authentication service type. 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/TSL, the validation of digital signatures, or other non-biometric and non-cryptographic mechanisms.
Credentialing	ICAM Services Framework service type made up of service components. 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.
Credentialing Determination	Determination of whether or not an individual is eligible to receive a PIV credential as either a Federal employee or contractor. <sup>345</sup>

<sup>338</sup> Adapted from [FIPS 201](#).

<sup>339</sup> Adapted from the [COMMON](#).

<sup>340</sup> Adapted from the [COMMON](#).

<sup>341</sup> Adapted from [NIST SP 800-37](#).

<sup>342</sup> As defined in [NIST SP 800-63](#).

<sup>343</sup> Adapted from the [National Security Agency \(NSA\) Enterprise Security Management \(ESM\)](#).

<sup>344</sup> As defined in [SP 800-63](#).

<sup>345</sup> Adapted from [OMB Memorandum, Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12](#), July 21, 2008.

Term	Definition
Cryptography	ICAM Services framework service type made up of service components. 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. <sup>346</sup>
Data Administrator	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.
Decryption	ICAM Services Framework service component within the Cryptography service type. A transformation that restores encrypted data to its original form. <sup>347</sup>
Digital Identity	ICAM Services Framework service type made up of service components. <sup>348</sup> The representation of Identity in a digital environment.
Digital Identity Life Cycle Management	ICAM Services Framework service component within the Digital Identity services type. 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.
Digital Signature	ICAM Services Framework service component within the Cryptography service type. An asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection. <sup>349</sup>
Domain Controller	The server(s) that manages passwords and authentication requests for a set of applications.
Elliptic Curve Cryptography (ECC)	An approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. This algorithm technology can provide exponentially stronger security with a smaller bit size than current algorithms in use (e.g., SHA-256).
Encryption	ICAM Services Framework service component within the Cryptography service type. Cryptographic transformation of data (called "plain text") into a different form (called "cipher text") that conceals the data's original meaning and prevents the original form from being used. <sup>350</sup>
Enhanced Electronic Questionnaires for Investigations Processing (e-QIP)	Web-based automated system designed to facilitate the processing of standard investigative forms used when conducting background investigations. <sup>351</sup>
Enrollment Official	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. <sup>352</sup>

<sup>346</sup> Adapted from [SP 800-12](#).

<sup>347</sup> As defined in [RFC 4949](#).

<sup>348</sup> As defined in the [Identity Management Task Force Report 2008](#).

<sup>349</sup> As defined in [SP 800-63](#).

<sup>350</sup> As defined in [RFC 4949](#).

<sup>351</sup> Please see the Office of Personnel Management (OPM) website.

<sup>352</sup> As defined in [FIPS 201](#). Within the Part A of the FICAM Roadmap and Implementation Guidance, this term is used in conjunction with Registrar, as they can be used interchangeably.

Term	Definition
Enrollment/Registration	ICAM Services Framework within the Credentialing service type. 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. <sup>353</sup>
Enterprise	Within the Implementation Guidance, “enterprise” is used to refer to a discrete agency/department. “Enterprise level” is used interchangeably with “agency level.” Activities that are described as Enterprise level indicate capabilities, services, technologies, etc. that are expected to be implemented at the agency/department level.
Enterprise Architecture	A management practice for aligning resources to improve business performance and help agencies better execute their core missions. An EA describes the current and future state of the agency, and lays out a plan for transitioning from the current state to the desired future state. <sup>354</sup>
Enterprise Services	Common or shared IT services that support core mission areas and business services. <sup>355</sup>
Entitlement Attributes	Also referred to as privilege attributes. Features of an individual that are used as the basis for determining access decisions to both physical and logical resources <sup>356</sup> .
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 <sup>357</sup>
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.
Federal Enterprise Architecture (FEA)	A business-based framework for government-wide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the Federal Government to one that is citizen-centered, results-oriented, and market-based. <sup>358</sup>
Federal Emergency Response Official (F/ERO)	A federal employee or contractor who is responsible for the execution of the National Response Framework (NRF), National Infrastructure Protection Plan (NIPP), National Continuity Policy Implementation Plan (NCPIP), and/or National Incident Management System (NIMS). These Emergency Responders are those employees who are designated to restore and/or maintain continuity of operations after a disaster. The requirements and restrictions for Emergency Responders are typically included in agency continuity plans and this designation is indicated on the individual's PIV card by a red stripe at the bottom front of the card.

<sup>353</sup> Adapted from the [FEA](#).

<sup>354</sup> As defined in the [FEA](#).

<sup>355</sup> As defined in the [FEA](#).

<sup>356</sup> Adapted from the [Identity Management Task Force Report 2008](#).

<sup>357</sup> Please see [The Department of Homeland Security \(DHS\) website](#).

<sup>358</sup> As defined in [SP 800-53](#), Recommended Security Controls for Federal Information Systems and Organizations, August 2009.

Term	Definition
Federal ICAM Initiative	The government-wide effort to provide policy and programmatic support for identity, credential, and access management business functions within the Federal Government. It is governed by the ICAMSC within the Federal CIO Council and managed operationally by the GSA Office of Governmentwide Policy. It addresses the convergence of HSPD-12 and the Federal PIV infrastructure, Federal PKI Management and Policy Authorities and FICAM governance/guidance.
Federation	<p>Services Framework service component within the Authentication service type. A trust relationship between discrete digital Identity Providers that enables a relying party to accept credentials for 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.<sup>359</sup></p> <p>In implementation, federation includes the technology, standards, policies, and processes that allow an organization to trust digital identities, identity attributes, and credentials created and issued by another organization.</p>
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. <sup>360</sup>
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. <sup>361</sup>
Identifier	A data object-often, a printable, non-blank character string- that definitively represents a specific identity of a system entity, distinguishing that identity from all others. <sup>362</sup>
Identity	The set of attribute values (i.e., characteristics) by which entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity. <sup>363</sup>
Identity Attribute Discovery	<p>ICAM Services Framework service component within the Digital Identity service component.</p> <p>Process of mapping pathways and creating indexes or directories that allows identification of authoritative data sources of identity data.</p>
Identity Management (IdM)	The combination of technical systems, policies and processes that create, define, govern and synchronize the ownership, utilization and safeguarding of identity information. <sup>364</sup>
Identity Management System (IDMS)	An automated system comprised of one or more systems or applications that provides the workflow management of identity functions.
Identity Proofing	ICAM Services Framework service component within the Digital Identity service type. A process that vets and verifies the information (e.g., identity history, credentials, documents) that is used to establish the identity of a system entity. <sup>365</sup>

<sup>359</sup> Adapted from [NIST SP 800-95](#), Guide to Secure Web Services, August 2007. [SP 800-95]

<sup>360</sup> Please see the [Office of Personnel Management \(OPM\)](#) website.

<sup>361</sup> Please see [The Department of Justice, Justice Information Sharing](#) website.

<sup>362</sup> As defined in [RFC 4949](#).

<sup>363</sup> As defined in [Identity Management Task Force Report 2008](#) and the ICAM Lexicon.

<sup>364</sup> As defined in the ICAM Lexicon.

<sup>365</sup> Adapted from [FIPS 201](#).

Term	Definition
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. <sup>366</sup>
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. <sup>367</sup>
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. <sup>368</sup>
Initiative	See "project" for definition.
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. <sup>369</sup>
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.
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.
Investigative Service Provider	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.
Issuance	ICAM Services Framework service component within the Credentialing service type. Process by which possession of a credential is passed to an entity. Service characteristics vary by credential type. <sup>370</sup>
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. <sup>371</sup>

<sup>366</sup> As defined in [SP 800-63](#).

<sup>367</sup> As defined in [SP 800-18](#), Guide for Developing Security Plans for Federal Information Systems, February 2006.

<sup>368</sup> As defined in the ICAM Lexicon.

<sup>369</sup> As defined on the Federal Bureau of Investigations (FBI) website.

<sup>370</sup> This definition is adopted from [FIPS 201](#).

<sup>371</sup> Please see the [Defense Security Service](#).

Term	Definition
Key Management	ICAM Services Framework service component within the Cryptography service type. The activities involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and <sup>372</sup>
Level of Assurance (LOA)	Also referred to as Assurance Level. A measure of trust or confidence in an authentication mechanism in terms of four levels: Level 1: LITTLE OR NO confidence Level 2: SOME confidence Level 3: HIGH confidence Level 4: VERY HIGH confidence <sup>373</sup>
Linking/Association	ICAM Services Framework service component within the Digital Identity service type. 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. <sup>374</sup>
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.
Metadata	Structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource.
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. <sup>375</sup>
Non-Person Entity (NPE)	Any type of non-human device (e.g., routers, servers, switches, firewalls, sensors) or software object. <sup>376</sup>
Orphaned Account	An account belonging to a user that has left the organization or no longer requires access to the resource. Orphaned accounts are most often the result of ineffective de-provisioning processes wherein user access privileges are not removed immediately upon a user leaving the organization. These accounts create security vulnerabilities, which may be exploited by individuals seeking to do harm.
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. <sup>377</sup>
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. <sup>378</sup>

<sup>372</sup> As defined in [FIPS Publication 140](#), Security Requirements for Cryptographic Modules, January 1, 1994.

<sup>373</sup> As defined in [M-04-04](#).

<sup>374</sup> Adapted from the [FEA Consolidated Reference Model Document](#), Version 2.3.

<sup>375</sup> Please see the [National Crime Information Center-FBI](#).

<sup>376</sup> As defined in the ICAM Lexicon.

<sup>377</sup> Adapted from [NIST SP 800-63](#).

<sup>378</sup> Adapted from [SP 800-116](#).

Term	Definition
PIV Card	A physical artifact (e.g., identity card, “smart” card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). <sup>379</sup>
PIV Interoperable Card	An identity card that meets the technical standards to work with PIV infrastructure elements such as card readers, and is issued in a manner that allows federal relying parties to trust the cards. <sup>380</sup>
Policy Administration	Services Framework service component within the Authorization and Access service type. The process of creating, disseminating, modifying, managing, and maintaining hierarchical rule sets to control digital resource management, utilization, and protection in a standard policy exchange format.
Policy Based Access Control (PBAC)	A form of access control that uses authorization policy that is flexible in the types of evaluated parameters (e.g., identity, role, clearance, operational need, risk, heuristics). <sup>381</sup>
Policy Decision	ICAM Services Framework service component within the Authorization and Access Service type. Serves as an access control authorization authority for evaluating access control policies based on a variety of inputs
Policy Enforcement	ICAM Services Framework service component within the Authorization and Access Service type. Restricts access to specific systems or content in accordance with policy decisions that are made
Private Key	The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data. <sup>382</sup>
Privilege Administration	ICAM Services Framework service component within the Privilege Management service type. 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.
Privilege Management	ICAM Services Framework service type made up of service components. A set of processes for establishing and maintaining the entitlement or privilege attributes that comprise an individual’s access profile. These attributes are features of an individual that can be used as the basis for determining access decisions to both physical and logical resources.
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.
Program	A group of related projects managed in a coordinated way. All of the projects which support alignment with the business functions defined in the ICAM segment architecture are considered to comprise an agency’s ICAM program. An agency may administer its ICAM program through one or multiple management structures or offices.

<sup>379</sup> As defined in [FIPS 201](#).

<sup>380</sup> As defined in [Personal Identity Verification Interoperability for Non-Federal Issuers](#), May 2009.

<sup>381</sup> As defined in [CNSS 4009](#).

<sup>382</sup> As defined in [SP 800-63](#).

Term	Definition
Project	An endeavor undertaken to create a unique product, service, or result. Within this document, the term “project” is used to refer to a discrete effort to implement a particular functionality or requirement as a part of the agency’s overall ICAM program, such as the modernization of physical access control systems. Also referred to as an “initiative.”
Provisioning	Services Framework service component within the Privilege Management service type. 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 maybe available in an environment, may include the creation, modification, deletion, suspension, or restoration of a defined set of privileges. <sup>383</sup>
Public Key	The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data. <sup>384</sup>
Public Key Infrastructure	The framework and services that provide for generation, production, distribution, control, accounting and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates. <sup>385</sup>
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. <sup>386</sup>
Registration Authority	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). <sup>387</sup>
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 Identity Provider, 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 Identity Provider’s or Trusted Broker’s assertions. <sup>388</sup>
Reports Management	Services Framework service component within the Auditing and Reporting service type. Collection of detailed information about system entities, usage activity, and identity audit events and presented in a meaningful way.

<sup>383</sup> Adapted from the [Identity Management Task Force Report 2008](#).

<sup>384</sup> Adapted from [FIPS 201](#).

<sup>385</sup> As defined in the ICAM Lexicon.

<sup>386</sup> Adapted from [FIPS 201](#).

<sup>387</sup> As defined in the [COMMON](#).

<sup>388</sup> Adapted from [SP 800-63](#).

Term	Definition
Resource Attribute/Metadata Management	<p>Services framework service component within the Privilege Management service type.</p> <p>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.</p>
Risk Adaptable Access Control (RadAC)	<p>A form of access control that uses an authorization policy that takes into account operational need, risk, and heuristics.<sup>389</sup></p>
Risk Assessment	<p>The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated, potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF).<sup>390</sup></p>
Risk Management	<p>The process of identifying, measuring, and controlling (i.e., mitigating) risks in information systems so as to reduce the risks to a level commensurate with the value of the assets protected.<sup>391</sup></p>
Role Based Access Control (RBAC)	<p>A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.<sup>392</sup></p>
Security Clearance Determination	<p>Determination of whether or not an individual is eligible for access to sensitive or classified information.<sup>393</sup></p>
Self-Service	<p>ICAM Services Framework service component within the Credentialing service type. 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.</p>
Session Management	<p>ICAM Services Framework service component within the Authentication service type. 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.</p>
Scheme Profile	<p>The subset of requirements and functionality within the identity scheme standard that is acceptable for government use at various LOAs based upon compliance with NIST SP 800-63 and other security and privacy requirements.</p>
Single Sign-On	<p>A mechanism by which a single act of user authentication and log on enables access to multiple independent resources.</p>
Situational Access Control	<p>An approach for adopting access control decisions for a resource to support the current operational environment. In this approach, the attributes about a user or resource typically do not change; however, their relevance to the situation impacts the access control decisions. For example, an individual may be granted access to a location that he/she does not routinely have access to during an emergency situation based on his/her designation as an Emergency Response Official.</p>

<sup>389</sup> As defined in [CNSS 4009](#).

<sup>390</sup> As defined in the ICAM Lexicon.

<sup>391</sup> As defined in [RFC 4949](#).

<sup>392</sup> As defined in [AASC](#), Authorization and Attributes Glossary Unclassified (Found within NIST IR 7657).

<sup>393</sup> Please see the [Office of Personnel Management \(OPM\) website](#).

Term	Definition
Sponsor	The party that verify that applicants have a need for a credential and initiate the credential enrollment and issuance process, especially for PKI and PIV credentials. <sup>394</sup>
Sponsorship	ICAM Services Framework service component within the Credentialing service type. Process for establishing the need for a card/credential by an authorized official; this step is critical for NPE credential request and issuance. <sup>395</sup>
Suitability Determination	A decision by OPM or an agency to determine an individual's suitability for employment in a position in the competitive service, a position in the excepted service where the incumbent can be noncompetitively converted to the competitive service, and a career appointment to a position in the Senior Executive Service. <sup>396</sup>
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.
Unique Person Identifier	An alphanumeric string attribute that identifies or selects exactly one individual from a defined community (e.g., the current and former employees of an Executive Branch agency or department) in order to distinguish his/her enterprise digital identity from others, even in cases where the underlying identity attributes may be the same (e.g., two employees with the same name).
User	An individual that is utilizing services provided by an agency and interacting with an information or business process. 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. <sup>397</sup>
Vetting	ICAM Services Framework service component within the Digital Identity service type. Process of examination and evaluation, including background check activities; results in establishing verified credentials and attributes. <sup>398</sup>
Visitor	An external user that is requesting short term access to an agency facility.

<sup>394</sup> Adapted from [FIPS 201](#).

<sup>395</sup> Adapted from [FIPS 201](#).

<sup>396</sup> Please see the [Office of Personnel Management \(OPM\)](#) website.

<sup>397</sup> Adapted from [SP 800-63](#).

<sup>398</sup> Adapted from [FIPS 201](#).

This page is intentionally left blank.

## Appendix C Policy List

GROUP	DOCUMENT NAME	DESCRIPTION
Joint Security and Suitability Reform Team	<a href="#">Federal Investigative Standards:</a> Investigative Standards for Background Investigations for Access to Classified Information	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.
The Office of Management and Budget (OMB)	<a href="#">M-00-10: OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act</a>	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	Streamlining Authentication and Identity Management within the Federal Government (July 3, 2003)	This document provides agency Chief Information Officers (CIOs) with guidance regarding next steps for the E-Authentication Initiative and specific actions that agencies should undertake to support that plan by coordinating and consolidating investments related to authentication and identity management.
OMB	<a href="#">M-04-04: E-Authentication Guidance for Federal Agencies</a>	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	<a href="#">M-05-05: Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services</a>	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	<a href="#">M-05-22: Transition Planning for Internet Protocol Version 6 (IPv6)</a>	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).

GROUP	DOCUMENT NAME	DESCRIPTION
OMB	<a href="#">M-05-24: Implementation of Homeland Security Presidential Directive (HSPD) 12- Policy for a Common Identification Standard for Federal Employees and Contractors</a>	This memorandum provides implementing instructions for Homeland Security Presidential Directive 12 (HSPD-12) and FIPS 201.
OMB	<a href="#">M-06-06: Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12</a>	This memorandum includes sample Privacy Act Systems of Records Notices, Privacy Act statements, and a privacy impact assessment developed by a working group of privacy experts.
OMB	<a href="#">M-06-16: Protection of Sensitive Agency Information</a>	The memorandum directs all Federal Agencies and departments to "encrypt all sensitive data on their mobile computers/devices."
OMB	<a href="#">M-06-18: Acquisition of Products and Services for Implementation of HSPD-12</a>	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	<a href="#">M-07-06: Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials</a>	This memorandum discusses validation and monitoring agency issuance of Personal Identity Verification (PIV) compliant identity credentials.
OMB	<a href="#">M-07-16 (esp. Attachment 1): Safeguarding Against and Responding to the Breach of Personally Identifiable Information</a>	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	<a href="#">M-07-20: FY 2007 E-Government Act Reporting Instructions</a>	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	<a href="#">M-08-01: Update of Statistical Area Definitions and Guidance on Their Uses</a>	This memorandum serves as a reminder for agencies to complete background investigations and issue credentials as required for the implementation of HSPD-12.

GROUP	DOCUMENT NAME	DESCRIPTION
OMB	Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation (May 23, 2008)	This document provides guidelines to agencies around planning for the use of Personal Identity Verification (PIV) credentials with physical and logical access control systems. The guideline is to be used to assist in the planning efforts and status of these activities and the HSPD-12 plans that should be available to the OMB, Government Accountability Office (GAO), and the agency's Inspector General (IG).
OMB	<a href="#">M-11-11: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12- Policy for a Common Identification Standard for Federal Employees and Contractors</a>	Policy for the continued implementation of HSPD-12; requires agencies to designate a lead official and issue an implementation policy.
Presidential Directive	<a href="#">HSPD-5: Management of Domestic Incidents</a>	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.
Presidential Directive	<a href="#">HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection</a>	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	<a href="#">HSPD-8: National Preparedness</a>	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	<a href="#">HSPD-12: Homeland Security Presidential 12: Policy for a Common Identification Standard for Federal Employees and Contractors</a>	HSPD-12 calls for a mandatory, government-wide standard for secure and reliable forms of identification (ID) issued by the Federal Government to its employees and employees of federal contractors for access to federally-controlled facilities and networks.
Presidential Directive	<a href="#">HSPD-24: Biometrics for Identification and Screening to Enhance National Security</a>	"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	<a href="#">The Privacy Act of 1974</a>	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 [SSN]).

GROUP	DOCUMENT NAME	DESCRIPTION
DHS	<a href="#">REAL ID Act of 2005</a>	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	<a href="#">Final Credentialing Standards</a>	Formally titled <i>Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12</i> , 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.
N/A	<a href="#">Health Insurance Portability and Accountability Act of 1996 (HIPAA)</a>	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	<a href="#">Government Paperwork Elimination Act of 1998 (GPEA)</a>	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	<a href="#">E-Government Act of 2002</a>	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 (OMB), and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes.
N/A	<a href="#">Electronic Signatures In Global and National (ESIGN) Commerce Act of 2000</a>	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	<a href="#">Federal Information Security Management Act (FISMA) of 2002</a>	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	<a href="#">Federal Government Intelligence Reform and Terrorism Prevention Act of 2004</a>	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	<a href="#">Public Law No: 110-53, The Implementing the 9/11 Commission Recommendations Act of 2007</a>	This law provides for the implementation of the recommendations of the National Commission on Terrorist Attacks Upon the United States.
N/A	<a href="#">Executive Order (E.O.) 12958: Classified National Security Information</a>	Established to have a uniform system for classifying, safeguarding, and declassifying national security information. Changes to the national security threats provide greater opportunity to emphasize the commitment to open Government.
N/A	<a href="#">E.O.12977: Access to Classified Information</a>	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.

GROUP	DOCUMENT NAME	DESCRIPTION
N/A	<a href="#"><u>E.O.13467: Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information</u></a>	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.					Risk List
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	Identity Provider Liability	Commercial entities may be unwilling to serve as an Identity Provider 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 [SSNs], 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 Identity Provider trusted (directly and indirectly) by the	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 Identity Providers, 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 life cycle, 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., Security Assertion Markup Language [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 139, provided in the FEA Practice Guidance document,<sup>399</sup> depicts the hierarchical relationships between enterprise, segment, and solution architectures.

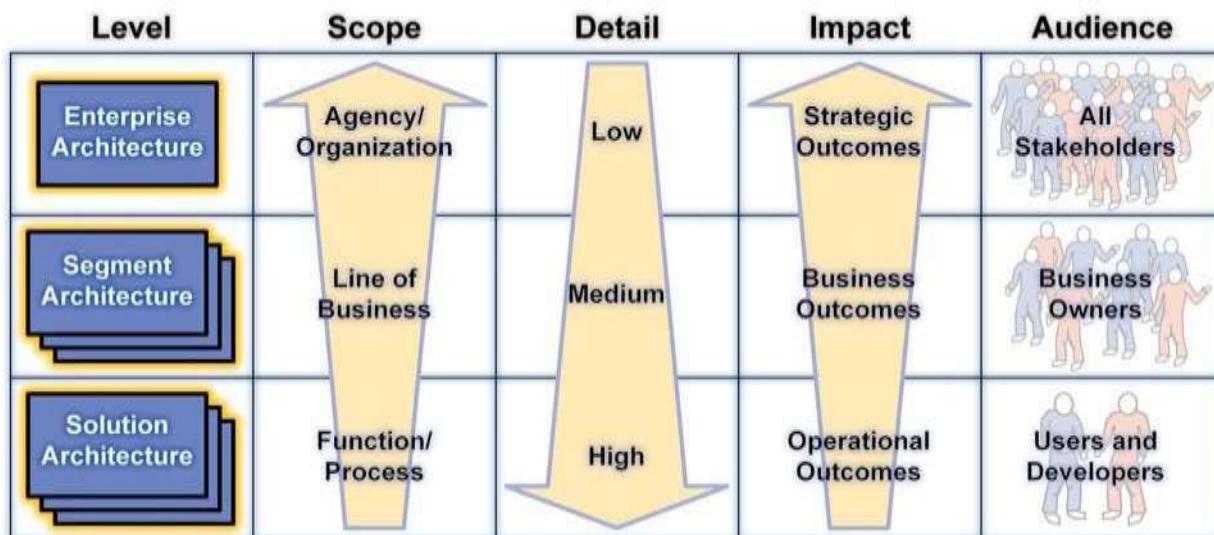


Figure 139: Levels of Architecture

A segment architecture defines a simple roadmap for a primary 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 (RDT), coordinating activities with the Lead Architect and supporting working groups, and reporting to the ICAMSC on the progress of the initiative.

<sup>399</sup> [FEA Practice Guidance](#), Federal Enterprise Architecture Program Management Office, OMB, November 2007.

- Roadmap Development Team (RDT). Representatives from all Federal Chief Information Officer Council organizations with experience in ICAM projects. The RDT 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 EA inputs from practitioners at their respective agencies.
- Lead Architect. Senior EA 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 RDT, 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 RDT 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 RDT 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.<sup>400</sup> 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?

---

<sup>400</sup> 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.

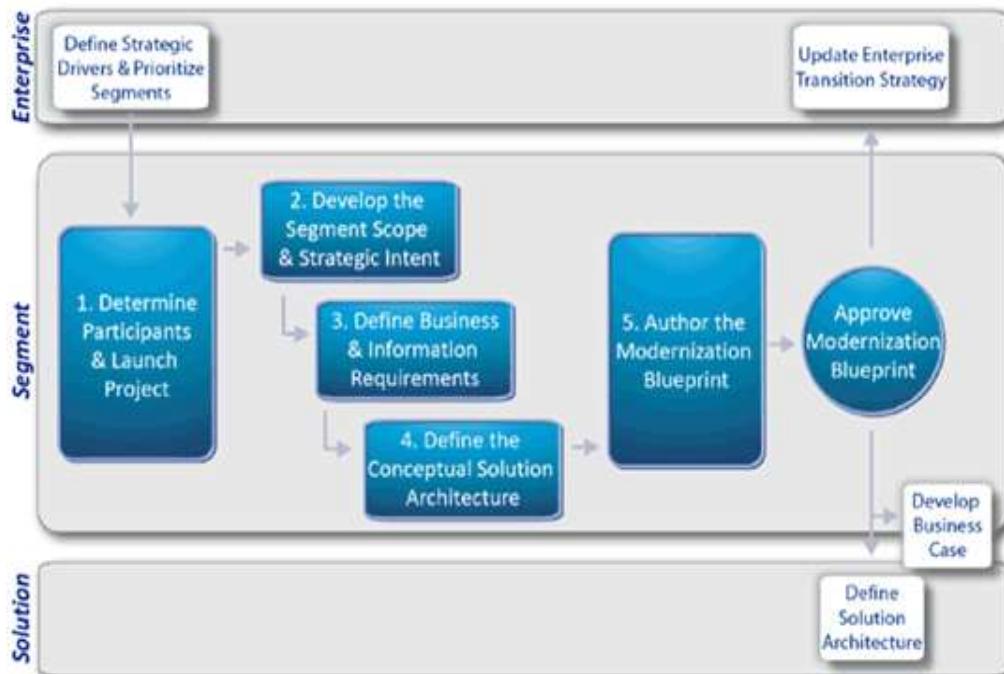


Figure 140: FSAM Implementation Steps

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.

	<b>Step 1: Determine Participants and Launch Project</b>	<b>Step 2: Define the Segment Scope and Strategic Intent</b>	<b>Step 3: Define Business and Information Requirements</b>	<b>Step 4: Define the Conceptual Solution Architecture</b>	<b>Step 5: Author the Modernization Blueprint</b>
<b>Activities</b>	<ul style="list-style-type: none"> <li>Determine the executive sponsor</li> <li>Develop the purpose statement for the segment</li> <li>Solicit Core Team members</li> <li>Create Core Team charter and project plan</li> <li>Establish the communications strategy</li> </ul>	<ul style="list-style-type: none"> <li>Establish segment scope and context</li> <li>Identify and prioritize strategic improvement opportunities</li> <li>Define segment strategic intent</li> <li>Validate and communicate the scope and strategic intent</li> </ul>	<ul style="list-style-type: none"> <li>Determine current business and information environment associated with strategic improvement opportunities</li> <li>Determine business and information improvement opportunities</li> <li>Define target business and data architectures</li> <li>Validate and communicate target business and data architectures</li> </ul>	<ul style="list-style-type: none"> <li>Assess systems and technology environment for alignment with performance, business, and information requirements</li> <li>Define the target conceptual solution architecture</li> <li>Identify and analyze system and service transition dependencies</li> <li>Validate and communicate the conceptual solution architecture</li> </ul>	<ul style="list-style-type: none"> <li>Perform cost/value/risk analysis to develop implementation recommendations</li> <li>Develop draft blueprint and sequencing plan</li> <li>Review and finalize the blueprint and sequencing plan</li> <li>Brief Core Team and obtain approval</li> </ul>
<b>Outputs</b>	<ul style="list-style-type: none"> <li>Segment Architecture Purpose Statement</li> <li>Core Team Roster</li> <li>Roles &amp; Responsibilities</li> <li>Project Plan</li> </ul>	<ul style="list-style-type: none"> <li>Stakeholder List</li> <li>Policy Map</li> <li>Risk Registry</li> <li>Business Challenges Analysis</li> <li>Business Drivers, Goals, &amp; Objectives</li> <li>Performance Metrics</li> </ul>	<ul style="list-style-type: none"> <li>Business Value Chain Analysis</li> <li>As-is Use Cases</li> <li>Inventory of authoritative data sources &amp; Data Elements</li> <li>Target Use Cases</li> <li>Target Information Flow Diagram</li> </ul>	<ul style="list-style-type: none"> <li>As-is System Interface Diagram</li> <li>Target System Interface Diagram</li> <li>Services Framework</li> </ul>	<ul style="list-style-type: none"> <li>Recommendation Implementation Overview</li> <li>Implementation Sequencing Plan</li> <li>Transition Plan Milestones</li> <li>Comments Matrix</li> </ul>

**Figure 141: Tailored FSAM Outputs for the Federal ICAM Segment**

The outputs shown in Figure 141 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	<a href="#">HSPD-12 Shared Component Infrastructure Interface Specification Common Elements</a>	This document provides Extensible Markup Language (XML) elements common to [Agency-SIP] and [ESP-SIP].
AWG	<a href="#">HSPD-12 Shared Component Infrastructure Metadata Management</a>	This document describes SCI metadata management. It captures assumptions the AWG has made about the full life cycle of SCI metadata (definition, distribution, configuration, use, and maintenance).
AWG	<a href="#">Finalization Service Provider to System Infrastructure Provider Interface</a>	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	<a href="#">System Infrastructure Provider and Production Service Provider Interface Specification</a>	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	<a href="#">System infrastructure Provider to Federal PKI Shared Service Provider Interface Specification</a>	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].
NIST	<a href="#">SP 800-73: Interfaces for Personal Identity Verification</a>	This document specifies the PIV data model, command interface, client application programming interface (API) and references to transitional interface specifications.
NIST	<a href="#">SP 800-73: Part 1: End Point PIV Card Application Namespace, Data Model &amp; Representation, 2: PIV Card Application Card Common Interface, 3: PIV Client Application Programming Interface, and 4: The PIV Transitional Interfaces &amp; Data Model Specification</a>	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	<a href="#">SP 800-76: Biometric Data Specification for Personal Identity Verification</a>	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	<a href="#">SP 800-79: Guidelines for the Accreditation of Personal Identity Verification Card Issuers</a>	This document provides guidelines for accrediting the reliability of issuers of Personal Identity Verification (PIV) cards that are established to collect, store, and disseminate personal identity credentials and issue smart cards, based on the standards published in response to HSPD-12.
NIST	<a href="#">SP 800-87: Codes for Identification of Federal and Federally-Assisted Organizations</a>	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	<a href="#">SP 800-103: An Ontology of Identity Credentials, Part 1: Background and Formulation</a>	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	<a href="#">SP 800-104: A Scheme for PIV Visual Card Topography</a>	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	<a href="#">SP 800-122: Guide for Protecting the Confidentiality of Personally Identifiable Information (PII)</a>	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	<a href="#">FIPS 199: Standards for Security Categorization of Federal Information and Information Systems</a>	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 (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.
NIST	<a href="#">FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors</a>	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.
IAB	<a href="#">Technical Implementation Guidance Smart Card Enabled Physical Access Control Systems</a>	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	<a href="#">UCore</a>	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	<a href="#">NIEM</a>	NIEM, the National Information Exchange Model, is a partnership of the Department of Justice and the Department of Homeland Security (DHS). 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	<a href="#">American National Standards Institute (ANSI)/National Institute of Standards and Technology Information Technology Lab (NIST-ITL) 1-2000, and 2006</a>	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 Federal Bureau of Investigation Integrated Automated Fingerprint Identification System (FBI IAFIS). Will be updated to reflect changes in ANSI/NIST-ITL 1-2006 and renamed to EBTS: Electronic Biometric Transmission Specification.
International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC)	<a href="#">ISO/IEC 24727</a> Identification Cards	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 life cycle 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	<a href="#">Open, Systems Integration, and Performance Standards (OSIPS)-01: 2008, Framework</a>	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	<a href="#">OSIPS-ACR-200x</a>	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	<a href="#">OSIPS-APC:200x</a>	This document describes the access point and credentials presented to field devices at the access point controller.
ANSI/SIA	Standards	<a href="#">OSIPS-IDM:200x</a>	This document describes identities and carrier claims of identity that are authenticated by comparing reference authentication factors with presented credentials.
AWG	Guidance	<a href="#">HSPD-12 Shared Component Infrastructure Trust Model</a>	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	<a href="#">HSPD-12 Shared Component Architecture</a>	This document describes the Smart Card Alliance 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	<a href="#">HSPD-12 Shared Component Infrastructure Technical Interoperability Model</a>	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	<a href="#">Agency to System Infrastructure Provider Interface Specification</a>	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	<a href="#">Enrollment Service Provider to System Infrastructure Provider Interface Specification</a>	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	<a href="#">HSPD-12 Fingerprint Process Considerations &amp; Research</a>	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	<a href="#">Backend Attribute Exchange Architecture and Interface Specification</a>	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	<a href="#">HSPD-12 Implementation Architecture Working Group Concept Overview</a>	This document briefly covers concepts that are critical to understanding the shared component architecture.
NIST	Guidelines	<a href="#">SP 800-53 (parts): Recommended Security Controls for Federal Information Systems and Organizations</a>	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	<a href="#">SP 800-63: Electronic Authentication Guideline</a>	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	<a href="#">SP 800-67: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher</a>	This publication specifies the Triple Data Encryption Algorithm , including its primary component cryptographic engine, the Data Encryption Algorithm. When implemented in an SP 800-38 series-compliant mode of operation and in a FIPS 140 compliant cryptographic module, Triple Data Encryption Algorithm 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 Triple Data Encryption Algorithm and to subsequently process such protected data. The Triple Data Encryption Algorithm 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	<a href="#">SP 800-73: Part 1: End Point PIV Card Application Namespace, Data Model &amp; Representation, 2: PIV Card Application Card Common Interface, 3: PIV Client Application Programming Interface, and 4: The PIV Transitional Interfaces &amp; Data Model Specification</a>	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	<a href="#">SP 800-76: Biometric Data Specification for Personal Identity Verification</a>	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	<a href="#">SP 800-78: Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV)</a>	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 [SP 800-73], and SP 800-76, Biometric Data Specification for Personal Identity Verification [SP 800-76], that rely on cryptographic functions.
NIST	Guidelines	<a href="#">SP 800-85 A-2: PIV Card Application and Middleware Interface Test Guidelines (SP 800-73 Compliance)</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	<a href="#">SP 800-85 B: PIV Card Application and Middleware Interface Test Guidelines</a>	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 FIPS 201, SP 800-73, SP 800-76, and SP 800-78.

GROUP	TYPE	NAME	DESCRIPTION
NIST	Guidelines	<a href="#">SP 800-96: PIV Card to Reader Interoperability Guidelines</a>	<p>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.</p> <p>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.</p>
NIST	Guidelines	<a href="#">SP 800-116: A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)</a>	<p>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.</p>
NIST	Federal Standards	<a href="#">FIPS 140: Security Requirements for Cryptographic Modules</a>	<p>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.</p>
NIST	Federal Standards	<a href="#">FIPS 180: Secure Hash Standard</a>	<p>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 &lt; 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.</p>
NIST	Federal Standards	<a href="#">FIPS 186: Digital Signature Standard (DSS)</a>	<p>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.</p>

GROUP	TYPE	NAME	DESCRIPTION
NIST	Federal Standards	<a href="#">FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors</a>	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 (PIV) 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	<a href="#">Personal Identity Verification Interoperability for Non-Federal Issuers</a>	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 (PIV-I) specifications meet the minimum vetting requirements at E-authentication level 4 as indicated in NIST SP 800-63. PIV-I credentials are not intended for individuals to whom HSPD-12 applies per OMB M-05-24.
FPKIMA	Guidance	<a href="#">Bridge-Enabling Web Servers</a>	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).
FPKIMA	Guidance	<a href="#">Functional Requirements for Path Validation Systems</a>	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	<a href="#">Product/Services Category List</a>	This document contains a FIPS 201 products list, and a description of each
FIPS 201 Evaluation Program	Guidance	<a href="#">Card to Reader Interoperability Requirement Guideline</a>	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.

GROUP	TYPE	NAME	DESCRIPTION
FIPS 201 Evaluation Program	Guidance	<a href="#">Configuration Management Plan</a>	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	<a href="#">Test Procedures - Card Printer Station</a>	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	<a href="#">Test Procedures - Electromagnetically Opaque Sleeve</a>	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	<a href="#">Test Procedures - Electronic Personalization</a>	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	<a href="#">Test Procedures - Facial Image Capturing Camera</a>	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.
FIPS 201 Evaluation Program	Guidance	<a href="#">Test Procedures - Facial Image Capturing Middleware</a>	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	<a href="#">Test Procedures - Graphical Personalization</a>	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	<a href="#">Test Procedures - PIV Card</a>	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	<a href="#">Test Procedures - PIV Card Reader - Authentication Key</a>	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	<a href="#">Test Procedures - PIV Card Reader - Biometric</a>	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	<a href="#">Test Procedures - PIV Card Reader - CHUID Authentication (Contact)</a>	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.

GROUP	TYPE	NAME	DESCRIPTION
FIPS 201 Evaluation Program	Guidance	<a href="#">Test Procedures - PIV Card Reader - CHUID Authentication (Contactless)</a>	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	<a href="#">Test Procedures - PIV Card Reader - CHUID (Contact)</a>	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	<a href="#">Test Procedures - PIV Card Reader - CHUID (Contactless)</a>	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	<a href="#">Test Procedures - PIV Card Reader - Transparent</a>	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	<a href="#">Test Procedures - Template Generator</a>	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.
N/A	Standard	<a href="#">Security Assertion Markup Language (SAML)</a>	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	<a href="#">Extensible Markup Language (XML)</a>	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	<a href="#">Lightweight Directory Access Protocol (LDAP)</a>	The Lightweight Directory Access Protocol (LDAP) is an Internet Protocol (IP) for accessing distributed directory services that act in accordance with X.500 data and service models.
N/A	Standard	<a href="#">Simple Object Access Protocol (SOAP)</a>	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	<a href="#">Hypertext Transfer Protocol (HTTP)</a>	Combines Hypertext Transfer Protocol and a cryptographic protocol

GROUP	TYPE	NAME	DESCRIPTION
NIST	Standard	<a href="#">FIPS 197: Advanced Encryption Standard (AES)</a>	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	<a href="#">Online Certificate Status Protocol (OCSP)</a>	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	<a href="#">Extensible Access Control Markup Language (XACML)</a>	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.
N/A	Standard	<a href="#">Simple Mail Transfer Protocol (SMTP)</a>	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	<a href="#">Secure Socket Layer (SSL)</a>	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	<a href="#">Secure Hash Algorithms (SHA)</a>	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.].
International Organization for Standardization (ISO)	Standard	<a href="#">ISO/IEC 7810 (card physical structure)</a>	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	<a href="#">ISO/IEC 18033-3:2005</a>	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	<a href="#">Elliptic Curve Digital Signature Algorithm (ECDSA)</a>	The ECDSA 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.

## Appendix H Decision Trees for Component Migration Decisions

As part of the planning phase for PACS modernization discussed in Section 10.1.4.1, an agency determines its approach for migrating to a modernized PACS. Because PACS impacts all employees entering federal facilities, adequate migration planning is critical during the implementation of a modernized PACS. A successful migration plan allows the integration of the new solution to have a low impact on existing infrastructure and operations. In addition, migration plans evaluate existing hardware and infrastructure to determine to what extent they can be reused. The figures in this appendix address the criteria an agency is to use when determining if existing PACS components can be reused in the target state modernized PACS solution.

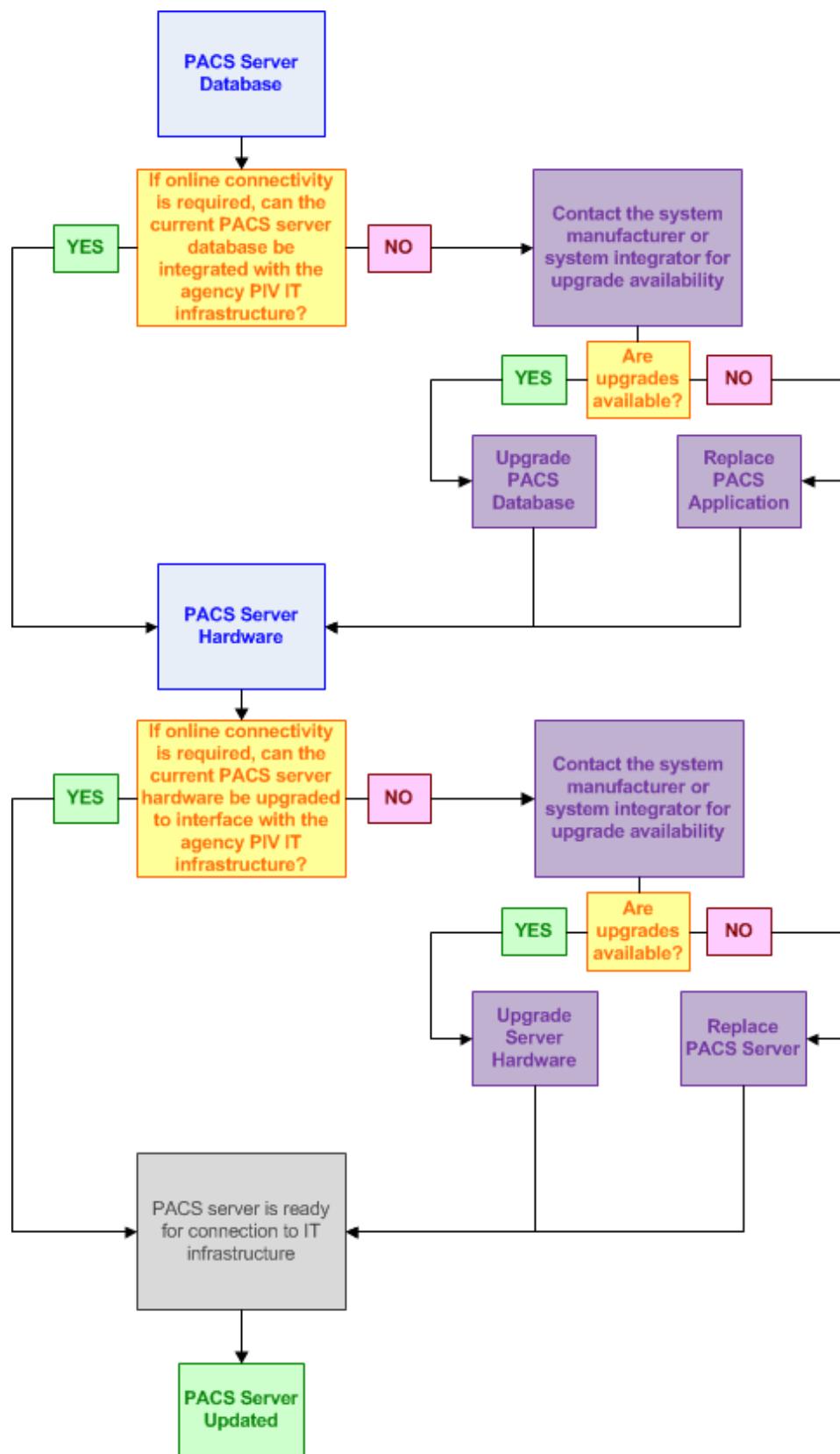


Figure 142: PACS Server Migration

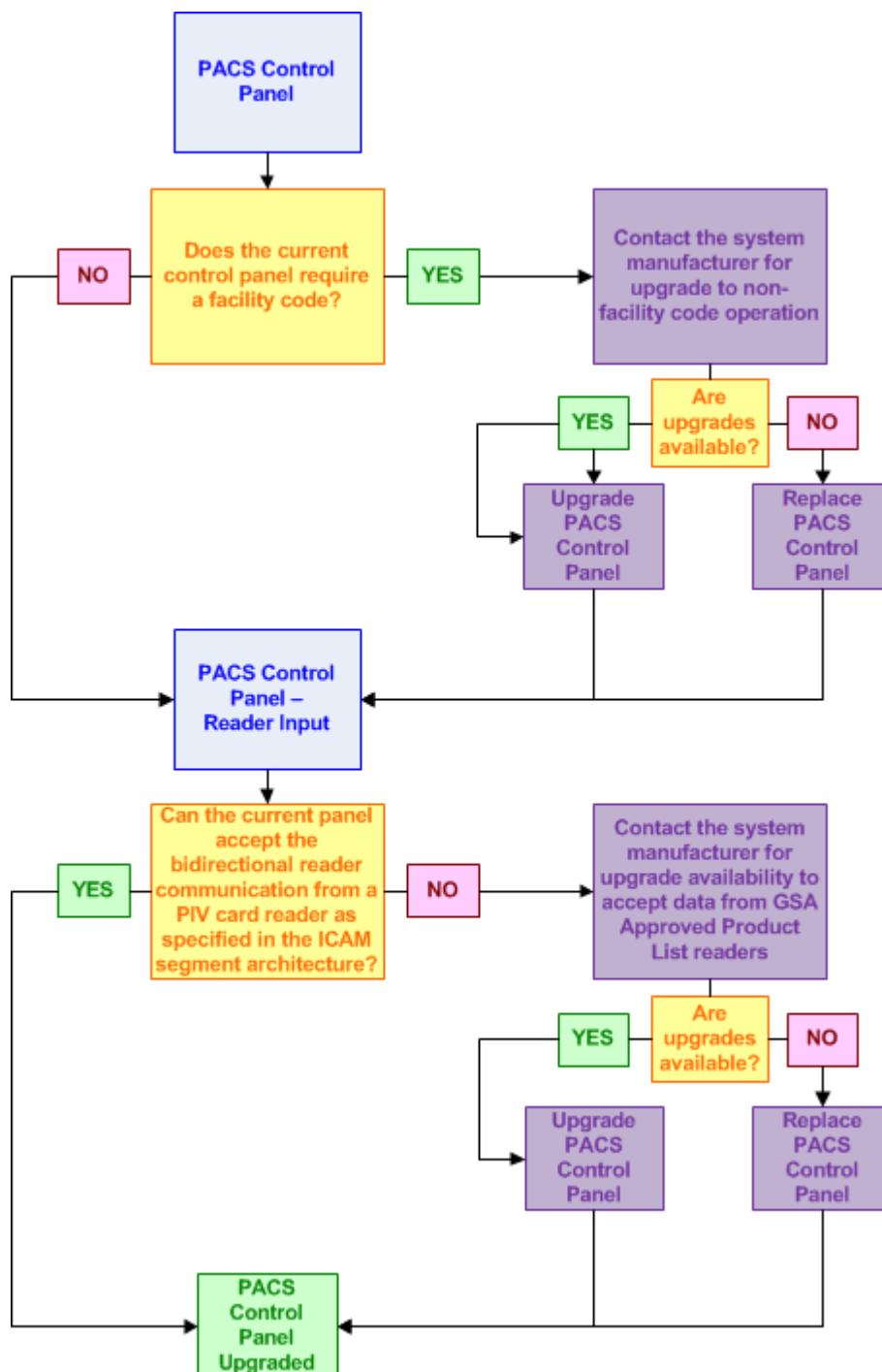


Figure 143: PACS Control Panel Migration

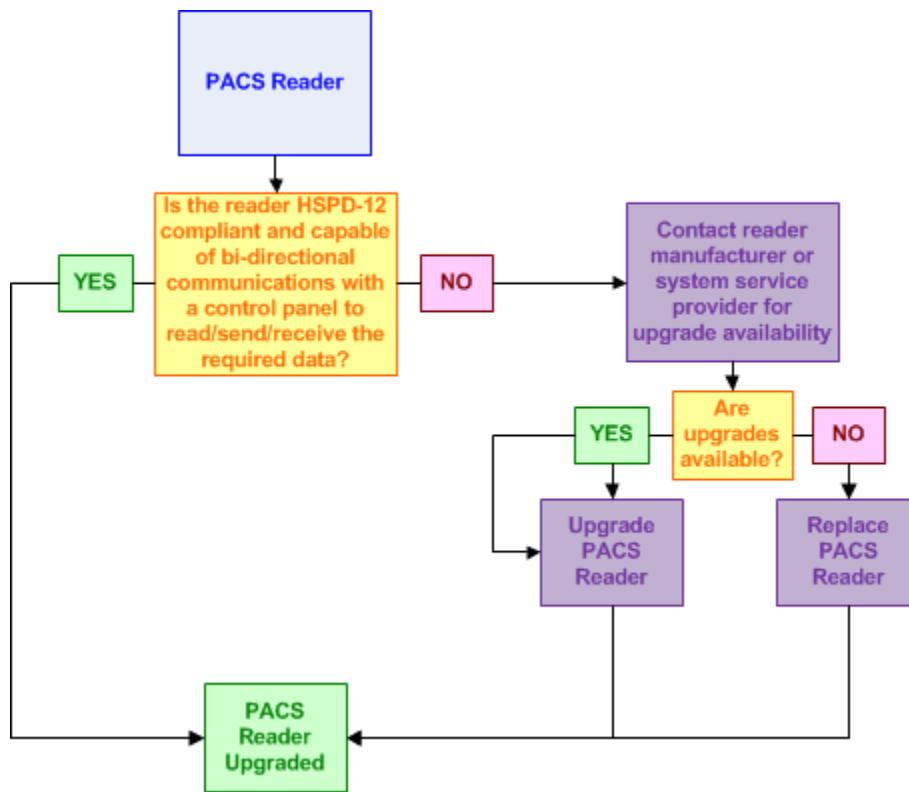


Figure 144: PACS Reader Migration

## Appendix I Existing Identity Exchange Models

This section provides additional background information and lessons learned from the three existing identity attribute exchange models introduced in Section 7.3.6, including: the Backend Attribute Exchange, National Information Exchange Model, and Global Federated Identity and Privilege Management model. As noted previously, each of these programs was designed to address the needs of a specific mission or business area; however, there are a number of common practices and lessons that an agency should seek to leverage as it implements its own agency-level information sharing and exchange capability, such as an Authoritative Attribute Exchange Service (AAES).

### **Backend Attribute Exchange (BAE)**

The Backend Attribute Exchange (BAE) is a standards based architecture and interface specification to securely obtain attributes of subjects (e.g., PIV card holders, federation members), from authoritative sources, to make access control decisions and/or to conduct provisioning.<sup>401</sup> The BAE is designed to support any community-defined attribute contract; as such, an agency could use this approach to exchange a wide variety of identity attributes in support of improved identity life cycle management. Since development of the specification in May 2008, it has been employed and developed further as part of a pilot program between the Department of Defense (DoD) and the Department of Homeland Security (DHS) to support the secure exchange of identity attributes during emergency response events. The need for such a capability was identified following the events of Hurricane Katrina in 2005, in which no adequate means existed to pre-provision external user accounts, primarily military or reserve military personnel that were mobilized to serve as first responders. This inability kept external users from being able to access the necessary information, information systems, sites, and restricted areas to effectively respond to the crisis. Therefore the BAE pilot was established to enable DHS and DoD to retrieve certain backend attributes from the other agency to enable dynamic provisioning of user accounts in situations where pre-provisioning is not possible. In this exchange, a relationship is established between the Attribute Authority, the individual's home agency, and a relying party, the agency requesting backend attributes for account provisioning.

#### **FAQ**

##### **What elements are considered backend attributes?**

Backend attributes include a number of entitlement or privilege attributes that are used to support authorization decisions but are not available on the PIV card, including: the PIV cardholder's security clearance level and PIV cardholder emergency responder capabilities.



The BAE employs two standards-based models to enable agencies to securely and electronically exchange backend attributes, including:

- **Single PIV Cardholder Model.** The Single PIV Cardholder Model utilizes Security Assertion Markup Language (SAML) to enable the exchange of information for a single PIV cardholder per request, in which a relying party (requestor) makes a digitally-signed request and the Attribute Authority responds with an encrypted message containing the

<sup>401</sup> A detailed discussion of attributes used to make access control decisions can be found in Section 9.2.1.

requested attributes (SAML assertion). This process happens in real-time, transparent to the user, and allows a relying party to make an authorization decision based on up-to-date authoritative identity attributes.

- **Batch Processing Model.** The Batch Processing Model utilizes Security Provisioning Markup Language (SPML) to enable the exchange of backend attributes for multiple individuals requesting access privileges at the same time. This model allows a relying party to digitally sign a group of requests (e.g., —Provide the attribute for each of the FASC-Ns in this list.) and the Attribute Authority to respond with an encrypted SPML message containing the requested information. The Batch Processing Model affords the enhanced security enabled through BAE usage with the convenience of being able to rapidly obtain attributes for a large number of users.

Both of these models can use pull-based architecture, where the needed attributes are requested from the Attribute Authority when the need for access is identified or requested. SPML can also use push-base architecture, which may be used to pre-provision or share attributes before the need for access is identified or requested. The individual is authenticated and an account is created with no roles, rights, or privileges. A request is generated for the necessary attributes and when there is positive confirmation the needed attributes are retrieved from the external sources to implement the access control policy and grant access to resources.

### Lesson Learned

Within large distributed agencies and in federated operating environments, it is increasingly likely that the user population will be comprised of primarily unknown and unanticipated users. The BAE determined that a pull-based architecture is better suited to this type of environment, offering greater flexibility while requiring a less intrusive infrastructure.



As was previously noted, the BAE pilot program was developed to address a specific mission need for DoD and DHS; however, as agencies begin to design and develop their own AAES capabilities there are a number of important lessons that can be learned from the BAE pilot program, including:

- **Make data quality and authoritativeness a top priority.** Before an agency can reliably use an AAES capability to support user authorization it must focus on ensuring the authoritativeness and validity of its source systems. The attributes that are used for authorization are only as reliable as the data housed in the agency's authoritative sources; invalid data can lead to inappropriate access based upon incorrect data.
- **Educate data owners.** Data owners and managers of authoritative data sources must be made aware that their data is being used in an AAES solution to support enterprise-wide authentication and authorization decisions and informed of the potential risks of invalid data management practices. Data owners should be encouraged to institute practices and processes to ensure data quality and authoritativeness.
- **Define and standardize entitlement attributes.** As part of establishing an enterprise digital identity exchange capability, agencies have the opportunity to extend their core identity model with a set of common entitlement attributes that can be used to support a broader variety of authorization decisions within an enterprise. Agencies should look to their systems with the largest user bases as a starting point for defining these entitlement attributes (discussed further in Section 9.2.1).

- **Consider implementing a virtual directory to avoid creating a new authoritative source.** The BAE implemented a virtual directory as the backend for BAE in order to enable read-only access to the various authoritative data sources. This allowed the BAE to correlate data without the need to store it, thereby avoiding the problem of creating, maintaining, and protecting a new authoritative repository. Agencies should consider this model when designing an AAES capability within their own agency, based on existing infrastructure and business requirements.
- **Do not overlook data privacy.** As it becomes easier for agencies to exchange identity data within external business partners it is critical that solution designers and implementers place an increased focus on data privacy to ensure that identity data is not exposed unnecessarily or in a manner that hampers security. Data should only be shared for the uses specified in the system of records notice (SORN).

#### Privacy Tip

When implementing an attribute sharing capability, an agency should seek to take advantage of technologies that are capable of enhancing the control over the means by which, and to whom identity attributes are released. For example, a selective attribute release mechanism, such as an Extensible Markup Language (XML) security gateway serving as a policy enforcement point, offers more granular control in the enforcement of existing access control policies.



### **National Information Exchange Model**

The National Information Exchange Model (NIEM) initially began as a Global Justice Initiative, stemming from many of the laws and regulations that were passed following the September 11, 2001 terrorist attacks on the United States. The Federal Government was seeking an enhanced means of sharing information with state, local, and tribal governments and began an inter-agency initiative supported by the Department of Justice (DOJ), Department of Homeland Security (DHS), and Department of Health and Human Services (HHS). This initiative was designed to reduce costs, decrease ambiguity, and leverage existing information sources by providing a national data standards framework, capable of supporting day-to-day business operations as well as mission critical emergency and disaster management capabilities.

NIEM expanded on the foundation provided by the Global Justice XML Data Model (GJXDM) by defining and using sets of common, approved Extensible Markup Language (XML) data elements. These elements comprise a data layer standard that provides a common vocabulary to foster collaboration and consistency across multiple organizations. The NIEM data model is organized into communities of interest, called domains, which share similar information in support of common mission-based objectives. Data elements contained within the NIEM data model are organized into two categories:

- **NIEM Core.** Consists of data elements that are commonly understood and used across all domains.
- **NIEM Domains.** Consists of mission specific data that is organized and managed within the specific domain.

The common language that exists within the NIEM domains is developed using a repeatable, reusable process that results in creation of XML Information Exchange Packages (IEPs). Once developed, these IEPs can be reused within other domains should a similar information need

exist. This use of this common vocabulary creates a structured way to exchange information between multiple organizations without the need to enforce strict technology requirements.

While NIEM was developed and is being used to address a number of mission-specific information sharing needs that go beyond the need to share identity data, there are a number of important lessons learned from this effort that agencies can apply to their own AAES implementations, including:

- **Define a common data model.** In order to achieve the ICAM target state for digital identities, agencies will need to define an enterprise digital identity comprised of a core set of identity attributes. As with NIEM, this model provides a common vocabulary for digital identity across the agency enterprise that can be used to streamline the implementation of other ICAM programs.
- **Consider additional models for entitlement attributes.** Agencies may find that certain groups of applications make authorization decisions using common sets of entitlement attributes in addition to those included in the enterprise digital identity. In order to accommodate this, agencies should consider making additional attributes available through their AAES capability.
- **Drive enterprise adoption by targeting large operational elements.** In order to achieve enterprise-wide adoption of the agency's AAES capability, implementers should begin by targeting groups with large user populations that can be used to demonstrate solution value.
- **Incorporate AAES usage into SDLC, SOA, change management, and acquisition processes.** Agencies should consider building requirements to use an AAES into existing business processes for new IT investments, such as SDLC, SOA, change management, and acquisition reviews. Taking this step ensures that newly built or upgraded IT systems are required to use an agency's AAES capability.

#### Lesson Learned

In order to drive agency-wide adoption and usage of the National Information Exchange Model (NIEM) data model, the Department of Homeland Security built checkpoints into their software development life cycle, service oriented architecture, and acquisition processes requiring that new IT investments align with the NIEM data model.



### Global Federated Identity and Privilege Management

The Global Federated Identity and Privilege Management (GFIPM) program is a federated access model that is jointly led and funded by the Department of Justice (DOJ) and DHS to support information sharing between federal, state, and local law enforcement agencies under the direction of the Global Justice Information Sharing Initiative.<sup>402</sup> The main goal of the GFIPM program was to enable streamlined federated access to law enforcement applications by provisioning local user accounts through trusted attribute sharing. The initial GFIPM pilot program ran from 2005 to 2007 and has existed as an operational model since 2007 under the name National Information Exchange Federation (NIEF).

<sup>402</sup> <http://gfipm.net/about.html> was leveraged in for the content of this section.

In order to create a feasible solution for the target community, GFIPM employed a bottom-up approach in which adoption and usage of the federated access model was driven primarily by the attractiveness of the solution rather than through a top-down mandate. This approach avoided many of the traditional barriers to adoption, such as the initial stand-up costs and the requirement to implement a high-security model. GFIPM accomplished this by providing centralized federation governance with a decentralized federation architecture. In this model, operational trust is anchored through a central governance body comprised of representatives from each participating agency, which is responsible for defining GFIPM's federation policies. This framework provides a central point of trust through which communications and standards-based data exchange occurs on a peer-to-peer basis, without the need for a central trust broker. Participants are governed by the agreed upon federation rules but granted the flexibility to establish additional layered agreements with other participants and within communities of interest. Rather than requiring all participants to adopt a high-security model, GFIPM requires that all participants disclose local security policies. This approach allows the various participants to make a risk-based decision to determine with whom they want to interact. This lightweight, standards-based governance and federation structure provides GFIPM with the ability to adapt as the community's needs change.

The standards-based federation framework provided by GFIPM allows for two primary types peer-to-peer interactions, including:

- **Dynamic Provisioning.** Dynamic provisioning involves the exchange of identity attributes between two GFIPM participants for the purpose of establishing local user accounts at the point in which an access request is made. This approach is well suited for external or unanticipated users for which an account would not already exist. GFIPM relies on a lightweight version of the NIEM person data model to standardize the exchange of attributes between participants.
- **Federated Authorization.** Once a user account has been established through dynamic provisioning, the GFIPM framework supports attribute-based access control decisions based on entitlement attributes obtained through secure attribute sharing. This capability enables participants to make reliable authorization decisions in a federated environment and can be achieved without the need for intervention from a local security administrator. This concept is further discussed in Chapter 12.

While GFIPM and its successor, NIEF, were developed and are being used to address the specific information sharing and federated access needs of the federal, state, and local law enforcement community, there are a number of important lessons learned from this effort that agencies can apply to their own AAES implementations, including:

- **Clearly define a set of core identity attributes.** Defining a set of core identity attributes, as discussed in Section 7.1.1, aligns with the ICAM vision for enterprise digital identity and provides a common standardized model for defining a person within an organization. From this starting point, agencies can expand into entitlement attributes to provide baseline user access across the enterprise.
- **Analyze the needs of the agency's largest attribute consumers.** As agencies begin to design and implement AAES capabilities within their organization, they should consider the needs of the largest consumers of attributes first and foremost. Most often, the largest consumers of attributes have the widest reach within an organization and adoption by these users can provide immediate operational value and return on investment.

- **Create operational value.** In order to drive enterprise-wide adoption and usage of an AAES capability it is necessary for the agency to create and demonstrate operational value through achievement of return on investment, such as through the streamlining and automation of existing manual processes, reallocation of support staff, and elimination of tedious and onerous tasks from system administrators. This is especially true in agencies where a top-down approach is either not feasible or practical and adoption must be driven from the bottom up.

**Implementation Tip**

Agencies should consider demonstrating value by implementing pilot programs in controlled environments with well-defined user populations. By demonstrating the ability to achieve federated access at a lower cost while enhancing the user experience, the Global Federated Identity and Privilege Management pilot program was transitioned into an operational phase as the National Information Exchange Federation.



## Acknowledgements

This document was prepared by the Identity, Credential, and Access Management Subcommittee (ICAMSC) under the auspices of the CIO Council. Part A comprises a segment architecture for ICAM that was developed at the request of the Federal Enterprise Architect. Part B comprises implementation guidance to provide agencies with information and tools to realize the goals of ICAM. The ICAMSC wishes to thank their colleagues who reviewed drafts of this document and contributed to its development:

- Tim Baldridge, National Aeronautics and Space Administration (NASA)
- Carol Bales, Executive Office of the President (EOP)
- Duane Blackburn, EOP
- Amanda Boxer, Social Security Administration (SSA)
- Debbie Bucci, National Institute of Health (NIH)
- Ken Clark, Office of the Director of National Intelligence (ODNI)
- Michael Cockrell, Treasury Department
- Kellie Cosgrove Riley, Federal Trade Commission (FTC)
- Mike DeFrancisco, Department of Agriculture (USDA)
- Debra Diener, Department of Homeland Security (DHS)
- Bill Erwin, GSA
- Hildegarde Ferraiolo, National Institute of Science and Technology (NIST)
- Salvatore Francomacaro, NIST
- Arthur Friedman, National Security Agency (NSA)
- Tim Gaines, Department of Energy (DOE)
- Deb Gallagher, GSA
- Paul Grant, Department of Defense (DoD)
- Steve Gregory, State Department
- John Hannan, Government Printing Office (GPO)
- Mary Heard, USDA
- Thomas Henry, SSA
- Johnna Hoban, Department of Justice (DOJ)
- Bernard Holt, DHS
- Corinne Irwin, NASA
- Anil John, DHS Science and Technology
- Steve Kerr, ODNI
- Naomi Lefkowitz, National Security Staff (NSS)
- Richard Lewis, Department of Labor (DOL)
- William MacGregor, NIST
- Ron Martin, Department of Health and Human Services (HHS)
- Brandi Meighan, DOJ
- Keith Minard, DoD
- Eric Mitchell, SSA
- Rachel Murdock, GSA
- Robert Myers, State Department
- Elaine Newton, NIST
- Kshemendra Paul, EOP
- Tammy Paul, Office of Personnel Management (OPM)
- Sheron Randolph, DoD
- Gina Reyes, Treasury Department
- Jonathan Rich, GSA
- Scott Rissmiller, DHS
- Phillip Rodman, Environmental Protection Agency (EPA)
- Allison Scogin, Defense Information Systems Agency
- Teresa Schwarzhoff, NIST
- Larry Slaughter, Department of Transportation (DOT)
- Amber Smith, Internal Revenue Service (IRS)
- James Smith, Government Printing Office (GPO)
- Judith Snoich, Department of the Interior (DOI)

- Judith Spencer, GSA
- Mike Sulak, State Department
- David Temoshok, GSA
- Owen Unangst, USDA
- Jeremy Warren, DOJ
- George White, DOJ
- David Wilson, Securities and Exchange Commission