DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design

Version 1.0
June 2020

Prepared by Department of Defense, Office of the Chief Information Officer (DoD CIO)

Document Approvals

Prepared By:

LAM.NGOAN.THOMAS.1229438960

Digitally signed by LAM.NGOAN.THOMAS.1229438960
Date: 2020.07.16 11:22:39 -04'00'

N. Thomas Lam

IE/Architecture and Engineering

Department of Defense, Office of the Chief Information Officer (DoD CIO)

CLANCY.THOMAS.JEROME.JR.1022639923

Digitally signed by CLANCY.THOMAS.JEROME.JR.1022639923
Date: 2020.07.16 11:29:55 -04'00'

Thomas J Clancy, COL US Army

CS/Architecture and Capability Oversight, DoD ICAM Lead

Department of Defense, Office of the Chief Information Officer (DoD CIO)

Approved By:

RANKS.PETER.THOMAS.1284616665

Digitally signed by RANKS.PETER.THOMAS.1284616665
Date: 2020.07.16 17:25:42 -04'00'

Peter T. Ranks

Deputy Chief Information Officer for Information Enterprise (DCIO IE)

Department of Defense, Office of the Chief Information Officer (DoD CIO)

Digitally signed by WILMER.JOHN.W.III.1267975430
Date: 2020.07.17 11:07:35 -04'00'

John (Jack) W. Wilmer III

Deputy Chief Information Officer for Cyber Security (DCIO CS)

Department of Defense, Office of the Chief Information Officer (DoD CIO)

Version History

Version	Date	Approved By	Summary of Changes
1.0	TBD	TBD	Renames and replaces the IdAM Portfolio Description dated August 2015 and the IdAM Reference Architecture dated April 2014. (Existing IdAM SDs and TADs will remain valid until updated versions are established.) • Updates name from Identity and Access Management (IdAM) to Identity, Credential, and Access Management (ICAM) to align with Federal government terminology • Removes and cancels the list of formal ICAM related requirements • Restructures document for clarity • Updates ICAM Taxonomy to better conform to Federal ICAM Architecture • Updates descriptions and data flows of ICAM capabilities • Summarizes current DoD enterprise ICAM services • Defines ICAM roles and responsibilities

Executive Summary

The purpose of this Identity, Credential, and Access Management (ICAM) Reference Design (RD) is to provide a high-level description of ICAM from a capability perspective, including transformational goals for ICAM in accordance with the Department of Defense (DoD) Digital Modernization Strategy. As described in Goal 3, Objective 2 of the DoD Digital Modernization Strategy, ICAM "creates a secure and trusted environment where any user can access all authorized resources (including [services, information systems], and data) to have a successful mission, while also letting the Department of Defense (DoD) know who is on the network at any given time." This objective focuses on managing access to DoD resources while balancing the responsibility to share with the need to protect. ICAM is not a single process or technology, but is a complex set of systems and services that operate under varying policies and organizations.

There are significant advantages to the DoD in providing ICAM services at the DoD enterprise level, including consistency in how services are implemented, improved security, cost savings, and attribution by having a discrete defined digital identity for a single entity. ICAM is also fundamental for the transformation to a modern data-centric identity-based access management architecture that is required in a future-state Zero Trust (ZT) Architecture. To gain these advantages, DoD enterprise ICAM services must support functionality for both the DoD internal community and DoD mission partners, must provide interfaces that are usable by Component information systems, and must minimize or eliminate gaps in supporting ICAM capabilities.

The ICAM RD promotes centralization of identity and credential management, including attribute management and credential issuance and revocation. The ICAM RD also establishes standardized processes and protocols for authentication and authorization. Access decisions must be fundamentally managed by local administrators who understand the context and mission relevance for person entities and Non-Person Entities (NPE) who require access to resources.

The RD defines an ICAM taxonomy that is based on the core elements of the Federal ICAM (FICAM) Architecture, and describes data flow patterns for each of the capabilities defined in the ICAM taxonomy. Systems and services shown in these data flows may be operated at the DoD enterprise, DoD Component, Community of Interest (COI), or local level. In addition to generic data flow patterns, the RD provides a set of implementation patterns and their related use cases for ICAM capabilities. These patterns are intended to demonstrate how capabilities may be implemented to meet a broad set of mission and other needs. They are not intended to be prescriptive for how a given information system consumes ICAM capabilities, nor are they intended to describe all possible ICAM use cases. Finally, the RD describes existing and planned DoD Enterprise ICAM services, and roles and responsibilities for ICAM service providers and for DoD Components in deploying ICAM.

This document is not intended to mandate specific technologies, processes, or procedures. Instead, it is intended to:

- Aid mission owners in understanding ICAM requirements and describing current and planned DoD enterprise ICAM services to enable them to make decisions ICAM implementation so that it meets the needs of the mission, including enabling authorized access by mission partners.
- Support the owners and operators of DoD enterprise ICAM services so that these services can effectively interface with each other to support ICAM capabilities.

- Support DoD Components in understanding how to consume DoD enterprise ICAM services and how to operate DoD Component, COI, or local level ICAM services when DoD enterprise services do not meet mission needs.

Each mission owner is responsible for ensuring ICAM is implemented in a secure manner consistent with mission requirements. Conducting operational, threat representative cybersecurity testing as part of ICAM implementation efforts is a mechanism that needs to be used to check secure implementation.

Contents

Figures

Tables

Identity, Credential, and Access Management (ICAM) Reference Design (RD)

1. Introduction

As described in Goal 3 Objective 2 of the Department of Defense (DoD) Digital Modernization Strategy, Identity, Credential, and Access Management (ICAM) "creates a secure and trusted environment where any user can access all authorized resources (including [services, information systems], and data) to have a successful mission, while also letting DoD know who is on the network at any given time." To realize this objective, the DoD must support capabilities that:

- Provide identity, credential and access management services to protect DoD information systems and DoD electronic Physical Access Control Systems (PACS) resources Provide access accountability
- Enable entities to look up contact data for person entities and Non-Person Entities (NPE)

ICAM is not new to the DoD. ICAM capabilities are already pervasive throughout the DoD because Information Technology (IT) devices, systems, applications and services are in use throughout the DoD. All of this DoD IT has some form of ICAM capability implemented to protect the full range of DoD information systems and DoD PACS resources, from the least restricted and public to the most restricted and protected. In addition, current ICAM capabilities enable DoD personnel to find and contact each other and enable accountability of user behavior when accessing DoD resources.

Even though DoD ICAM capabilities already exist, these ICAM capabilities need to evolve, and additional ICAM systems and services need to be implemented to meet the DoD ICAM objective and to better align the DoD with the Federal ICAM (FICAM) Architecture. Additionally, DoD ICAM is evolving to support new operating environments such as cloud and the transformation to a modern identity-based access management architecture that is required in a future-state Zero Trust (ZT) Architecture.

DoD ICAM is not a single process or technology but is a complex set of systems and services that operate under various policies and organizations.

The ICAM RD promotes centralization of identity and credential management, including attribute management and credential issuance and revocation. The ICAM RD also establishes standardized processes and protocols for authentication and authorization. Access decisions must be fundamentally managed by local administrators who understand the context and mission relevance for person entities and Non-Person Entities (NPE) who require access to resources.

ICAM capabilities address Risk Management Framework (RMF) security controls designed to mitigate risk and protect resources. The Access Control (AC) and Identity and Authentication (IA) controls are addressed through ICAM, but other RMF controls may also be fully or partially addressed through proper ICAM implementation. Although a complete comparison between ICAM and the RMF security controls is out of scope for this document, a mapping of security controls to related ICAM Reference Design text is provided as Attachment B.

This document summarizes the designs for DoD ICAM:

- **Section 1** provides the purpose and scope for this document along with an overview of the DoD enterprise, including the user community and computing environment

- **Section 2** describes the DoD ICAM vision, presents the ICAM capability taxonomy, and provides an overview description of each of the ICAM capabilities
- **Section 3** provides data flow diagrams describing how ICAM services can work together to achieve ICAM capabilities
- **Section 4** identifies a set of use cases for implementing ICAM capabilities for various types of users
- **Section 5** identifies operational and planned DoD enterprise level ICAM systems and services that enable ICAM capabilities
- **Section 6** provides DoD Component roles and responsibilities for the implementation of ICAM
- **Section 7** summarizes gaps in current DoD enterprise ICAM capabilities

Details for design and implementation of DoD enterprise ICAM systems and services as well as interfaces for interacting with ICAM services are found in their respective system documentation.

1.1. Purpose

The purpose of this ICAM Reference Design (RD) is two-fold. First, as an architecture document, it supports the owners and operators of DoD enterprise ICAM services so that these services can effectively interface with each other to support ICAM capabilities, and supports developers so they can implement ICAM using consistent, standards-based methodologies. Second, as a descriptive document, it supports DoD Components in understanding how to consume DoD enterprise ICAM services and how to operate DoD Component, Community of Interest (COI), or local level ICAM services when DoD enterprise services do not meet mission needs. For this document, a COI is a community of people, information systems, and resources that share a common requirement for ICAM that is not at the DoD enterprise level or specific information system level. COIs may be part of other COIs.

There are significant advantages to the DoD to provide ICAM services at the DoD enterprise level, including cost savings from managing software licenses, economies of scale in deploying services, consistency in how services are implemented, improved security, and attribution by having a discrete defined digital identity for a single entity. However, to gain these advantages, DoD enterprise ICAM services must support functionality for both the DoD internal community and DoD mission partners, provide interfaces that are usable by Component information systems and resources, and minimize or eliminate gaps in supporting ICAM capabilities. By describing needed ICAM capabilities and documenting how DoD enterprise services are supporting these capabilities, this RD can promote adoption and use of these services.

Each mission is responsible for ensuring ICAM is implemented in a secure manner consistent with its unique mission requirements. This document is intended to aid mission owners in understanding ICAM capabilities and describing current and planned DoD enterprise ICAM services to enable mission owners to make decisions for how to implement ICAM so that it meets the needs of the mission. The intent of this document is not to mandate specific technologies, processes, or procedures, but to aid mission owners and implementers in evaluating the security and maintainability of their information systems and resources.

Some of the considerations this document will assist mission owners and implementers in assessing include:

- **Data Sources:** provide information about available DoD enterprise sources, attributes available from those sources, requirements for obtaining those attributes, and security considerations for using these services
- **Identity Synchronization:** enumerate common protocols, common procedures, and common technologies for obtaining and using identifiers to support synchronizing identity data between environments
- **Federation:** processes and procedures for leveraging identity data and credentials that are managed outside of the DoD to support authentication and authorization of DoD mission partner entities
- **Assurance Levels:** understanding identity assurance levels (IAL), authenticator assurance levels (AAL), and federation assurance levels (FAL) and their impact to assist mission owners in evaluating the right types of credentials to support in their missions
- **Authentication:** authentication processes, procedures, leading practices, and common pitfalls for person entities and NPEs
- **Authorization:** authorization processes, procedures, leading practices, and common pitfalls for person entities and NPEs
- **ICAM Technology:** key ICAM technical concepts, implementation patterns, and security considerations
- **Audit:** auditing and logging considerations to support accountability

1.2. Applicability

The contents of this document are applicable to all of the following.

- The Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the DoD Office of the Inspector General (OIG), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively as the "DoD Components").
- All DoD unclassified, secret, top secret, and United States (US) owned releasable networks and information systems under the authority of the Secretary of Defense (e.g., Non-classified Internet Protocol Router Network [NIPRNet], Secret Internet Protocol Router Network [SIPRNet], Defense Research and Engineering Network [DREN], Secret Defense Research and Engineering Network [SDREN], SIPRNet Releasable [SIPR REL] De-Militarized Zone (DMZ), United States Battlefield Information Collection and Exploitation System [USBICES], and DoD Mission Partner Environment [MPE]). Information systems include those that are owned and operated by or on behalf of the DoD, including systems hosted at DoD data centers, Platform Information Technology (PIT) systems including weapon systems and control systems, contractor operated systems, cloud hosted systems, and systems hosted on closed operational networks with no connection to the DoD Information Networks (DoDIN).
- All DoD and non-DoD person entity and NPE users (referred to as "entities") accessing DoD unclassified, secret, or top secret networks and resources under the authority of the Secretary of Defense, including DoD mission partners and DoD beneficiaries.

- All DoD ICAM capabilities, functions, systems, elements and services implemented at any and all locations, from well-connected Continental United States (CONUS) and Outside Continental United States (OCONUS) environments, to tactical environments, including the most challenging and restricted Denied, Degraded, Intermittent, or Limited bandwidth (DDIL) environments.

The ICAM taxonomy and ICAM data flows in this document apply regardless of whether systems are connected to the DoDIN and regardless of operational considerations. The use of DoD enterprise ICAM services may not be applicable for some mission environments. When DoD enterprise ICAM services are not used, the mission owner is responsible for implementing ICAM capabilities including identity proofing, credential issuance and revocation, attribute management, entitlement provisioning, and logging in accordance with this document.

The designs, requirements, and roles and responsibilities for ICAM capabilities, functions, systems, elements and services implemented by the Intelligence Community (IC) and on the Joint Worldwide Intelligence Communications System (JWICS) are the responsibility of the Director of National Intelligence (DNI) to determine. As a result, this ICAM design does not specifically apply to the following. However, ICAM capabilities should support interoperability to support information sharing between these environments and the DoDIN.

- Sensitive Compartmented Information (SCI) and information systems operated within the DoD that fall under the authority provided in Intelligence Community Directive 503
- Top Secret collateral systems
- Special Access Programs[1]

1.3. DoD Community

DoD provides resources to a broad community of users to support its core mission, provide services to beneficiaries, and to address non-traditional missions. ICAM capabilities must be flexible enough to meet the needs of information systems supporting these communities while providing sufficient security to prevent unauthorized access.

1.3.1. DoD Internal Community

The DoD internal community includes all people who are eligible for fully provisioned network accounts on NIPRNet or SIPRNet as a requirement of performing their job function, and NPEs that are fully managed by the DoD. Identity information for the DoD internal community person entities is managed through DoD enterprise services such as the Person Data Repository (PDR), and these entities are issued credentials for the NIPRNet on Common Access Cards (CAC) or Alternate Logon Tokens (ALT) by the DoD Public Key Infrastructure (PKI). On the SIPRNet, these entities are issued credentials by the DoD portion of the National Security System (NSS) PKI. These entities may also be issued additional credentials based on their primary credential for use in specialized environments such as mobile computing and non-traditional systems that do not support the CAC form factor. Identity information for DoD internal NPEs

[1] Note that the DoD Special Access Program (SAP) community operates under a separate but similar ICAM strategy and is implementing its own program with guidance from the DoD and the National Security Agency (NSA). Because of the highly sensitive nature of special access programs and their materials, they must be managed independently and fall under the purview of the DOD SAP Chief Information Officer (CIO) office. For additional details regarding SAP ICAM strategy and implementation, please contact the DOD SAP CIO office.

may be managed through DoD enterprise services or may be managed by the appropriate DoD Component. The DoD internal community includes:

- DoD military service members including active duty, reserve, and national guard
- DoD civilian employees
- Eligible non-US persons who work on DoD computers at DoD facilities
- Contractors who work on DoD computers at DoD facilities
- Eligible contractors who do not work at DoD facilities
- Roles managed by the DoD where the nature of the role requires establishment of a separate digital identity – role identities must be tightly bound to the people who perform them
- NPEs that are fully managed by the DoD including
    - Physical devices such as physical servers, workstations, mobile devices, or routers
    - Virtual machines including servers and workstations
    - Information systems, services, and processes with a long-term existence
    - Information systems, services, and processes with a limited duration and targeted purpose
    - Non-traditional systems such as weapons systems and control systems

1.3.2. External Mission Partner Community

DoD interacts with a broad community of mission partners who are not eligible for DoD enterprise credentials. The DoD mission partner community includes:

- Federal Department and Agency Employees and Provisioned Contractors
- Contractors who do not work on DoD computer at DoD facilities and are not otherwise eligible members of the DoD internal community
- Non-US persons, including allied and coalition partners
- Other Government, including state, local, and tribal government employees
- Non-Governmental Organizations (NGO)
- External NPEs including those operated by cloud service providers

Some mission partner entities have credentials issued by external providers that are approved for use by DoD information systems, such as Federal Agency Personal Identity Verification (PIV) smart cards, Defense Industrial Base (DIB) commercial PIV-Interoperable (PIV-I) smart cards, or non-US sovereign nation supported credentials. Some mission partner entities may interact with DoD in closed environments where they are issued credentials that are only trusted within that environment. In order to interact with these mission partner entities, authentication services must be able to consume mission partner credentials by leveraging a persistent, unique identifier provided by the mission partner entity. DoD services may map the identifier contained in the mission partner credential to a persistent, unique identifier assigned by the DoD either at an DoD enterprise, COI, or local level in order to provide an enterprise view of authentication.

1.3.3. Beneficiaries

DoD provides services to people who are eligible for benefits as a result of their relationship to the DoD. Identity information for DoD beneficiaries is managed through the PDR, and these entities are eligible to obtain credentials through DoD Self-service (DS) Logon. The DoD beneficiary community includes:

- DoD military service members including active duty, reserve, and national guard
- Military retirees

- Military spouses and other dependents
- Some overseas DoD civilian employees
- Designees who to represent a beneficiary, either by the beneficiary themselves or through a legal process such as dependency or power of attorney

1.3.4. Other Entities

Some DoD information systems interact with external entities for a limited duration or purpose. Identity information for these entities is generally not managed at the DoD enterprise level, and these entities may require locally issued credentials. Other entities include:

- Vendors
- Non-traditional mission non-government organizations
- Military accession applicants who are not yet registered in the PDR

1.4. DoD Computing Environment

The DoD environment is a complex computing environment with a multitude of programs, stakeholders, and other complexities. ICAM is a fundamental building block that must span the environment and cannot be implemented in a one-size-fits-all manner.

ICAM must support missions operating at all security levels, including unclassified, secret, and top secret. It is recognized that a mission operating in a high bandwidth unclassified environment will perform ICAM functions differently than a mission operating in a secret level DDIL environment. The complexity of the types of environments, degree of sensitivity of resources, and devices supported are contributing factors to the difficulty of operating in the DoD environment.

Resources may be hosted in different environments, including:

- DoD enterprise owned and managed data centers
- DoD Component owned and managed data centers
- Mission partner data centers
- Private, public, or hybrid clouds including government clouds
- Information systems deployed with tactical units

Person entities and NPEs accessing these resources operate from endpoint devices that include laptops and desktops, mobile phones or tablets, and virtual machines. These devices may be owned and managed by the DoD, owned and managed by DoD mission partners, or may be personally owned by person entities. These operations may also take place from within short-lived services or containers.

Information systems and endpoint devices operate in various network environments, including DoD protected high bandwidth, DDIL, closed COI enclaves, and external enclaves with varying degrees of trust such as mission partner networks, private networks, and the public internet.

1.5. References

This RD incorporates and cancels the following documents:

- Identity and Access Management Reference Architecture, Version 1.0, April 2014
- Identity and Access Management Portfolio Description, Version 2.0, August 2015

- Joint Information Environment (JIE) Executive Committee (EXCOM) approved Identity and Access Management (IdAM) Service Descriptions (SD) and Technical Architecture Descriptions (TAD) remain valid until updated versions are established

This RD also references the following documents:

- Committee on National Security Systems (CNSS) Instruction 4009, Committee on National Security Systems (CNSS) Glossary, 6 April 2015
  https://www.cnss.gov/CNSS/issuances/Instructions.cfm

- Department of Defense Naming Convention for People within DoD Identity, Credential, and Access Management, February 2020

- DoD Digital Modernization Strategy, 12 July 2019
  https://media.defense.gov/2019/jul/12/2002156622/-1/-1/1/dod-digital-modernization-strategy-2019.pdf

- DoD Cyber Security Reference Architecture (CSRA)

- DoD Identity, Credential, and Access Management Strategy (DRAFT), March 2020

- DoD Instruction 8520.03, Identity Authentication for Information Systems, Change 1, 27 July 2017
  https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/852003p.pdf

- Federal Identity, Credential, and Access Management (FICAM) Architecture
  https://arch.idmanagement.gov/

- Homeland Security Presidential Directive (HSPD) 12, Policies for a Common Identification Standard for Federal Employees and Contractors, 27 August 2004
  https://www.dhs.gov/homeland-security-presidential-directive-12

- Intelligence Community Directive (ICD) 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation, 15 September 2008
  https://www.dni.gov/files/documents/ICD/ICD_503.pdf

- National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) Glossary
  https://csrc.nist.gov/glossary

- NIST Federal Information Processing Standard (FIPS) 201-2, Person Identity Verification (PIV) of Federal Employees and Contractors, August 2013
  https://csrc.nist.gov/publications/detail/fips/201/2/final

- NIST Special Publication (SP) 800-53-4, Security and Privacy Controls for Federal Information Systems and Organizations
  https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

- NIST Special Publication (SP) 800-63-3, Digital Identity Guidelines, 22 June 2017
  SP 800-63A, Enrollment and Identity Proofing
  SP 800-63B, Authentication and Lifecycle Management
  SP 800-63C, Federation and Assertions
  https://pages.nist.gov/800-63-3

- NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations
  https://csrc.nist.gov/publications/detail/sp/800-162/final
- NIST SP 800-205, Attribute Considerations for Access Control Systems
  https://csrc.nist.gov/publications/detail/sp/800-205/final
- NISTIR 8112, Attribute Metadata: A Proposed Schema for Evaluating Federated Attributes
  https://csrc.nist.gov/publications/detail/nistir/8112/final
- Office of Management and Budget (OMB) Memo M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management, 21 May 2019
  https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

2. ICAM Capability Overview

This section provides the high-level ICAM capability perspective and includes the transformational vision (DoD Architecture Framework [DoDAF] Capability Viewpoint [CV]-1), a description of ICAM goals and objectives, and the capability taxonomy (DoDAF CV-2).

This DoD ICAM vision is depicted in Figure 1. ICAM capabilities improve mission effectiveness by providing core ICAM (which includes identity management, credential management, and access management), access accountability, and contact data capabilities to achieve ICAM results. These three ICAM operational capabilities define the complete scope of DoD ICAM.

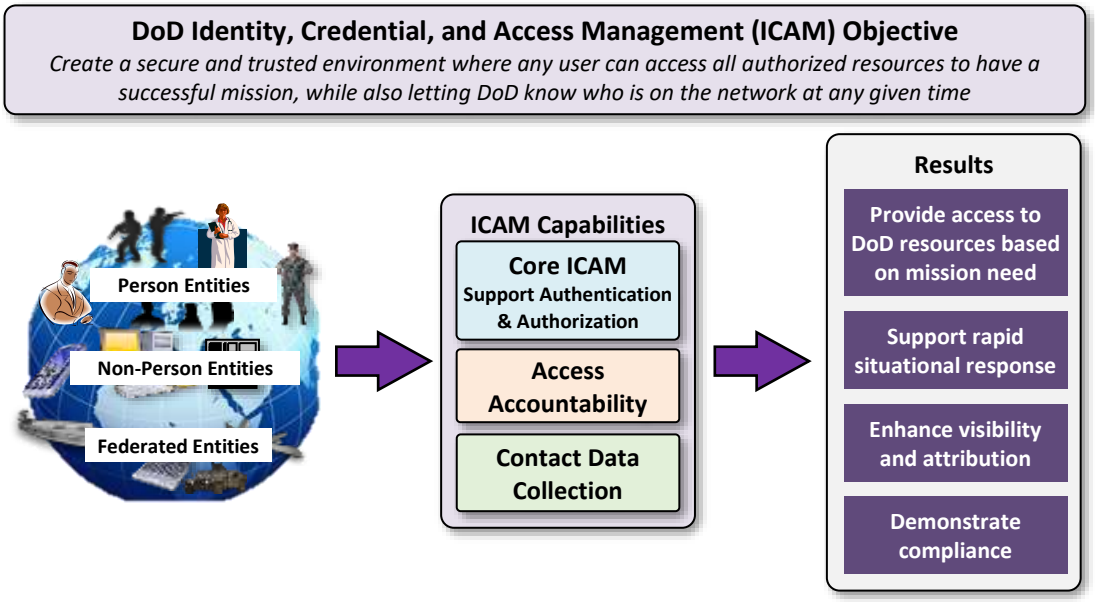


Figure 1 – DoD ICAM Vision Capability Viewpoint (CV-1)

The high-level operational concept for ICAM is shown in Figure 2. This diagram serves as the DoDAF Operational Viewpoint (OV) 1 and as an organizing construct for ICAM enablers, capabilities, business functions and services. It identifies the classes of entities: DoD person entities, DoD NPEs (such as servers and web applications), and federated mission partner entities. The three classes of entities have different processes for identity proofing and credentialing, as discussed in Sections 3.1.1 and 3.1.2. Once credentialed and authenticated, access decisions for entities follow a common process. Access to protected resources is based on the entity and their attributes (including roles), the access labels on a resource, and the access policy that compares the entity and resource attributes and evaluates to make a grant or deny decision.

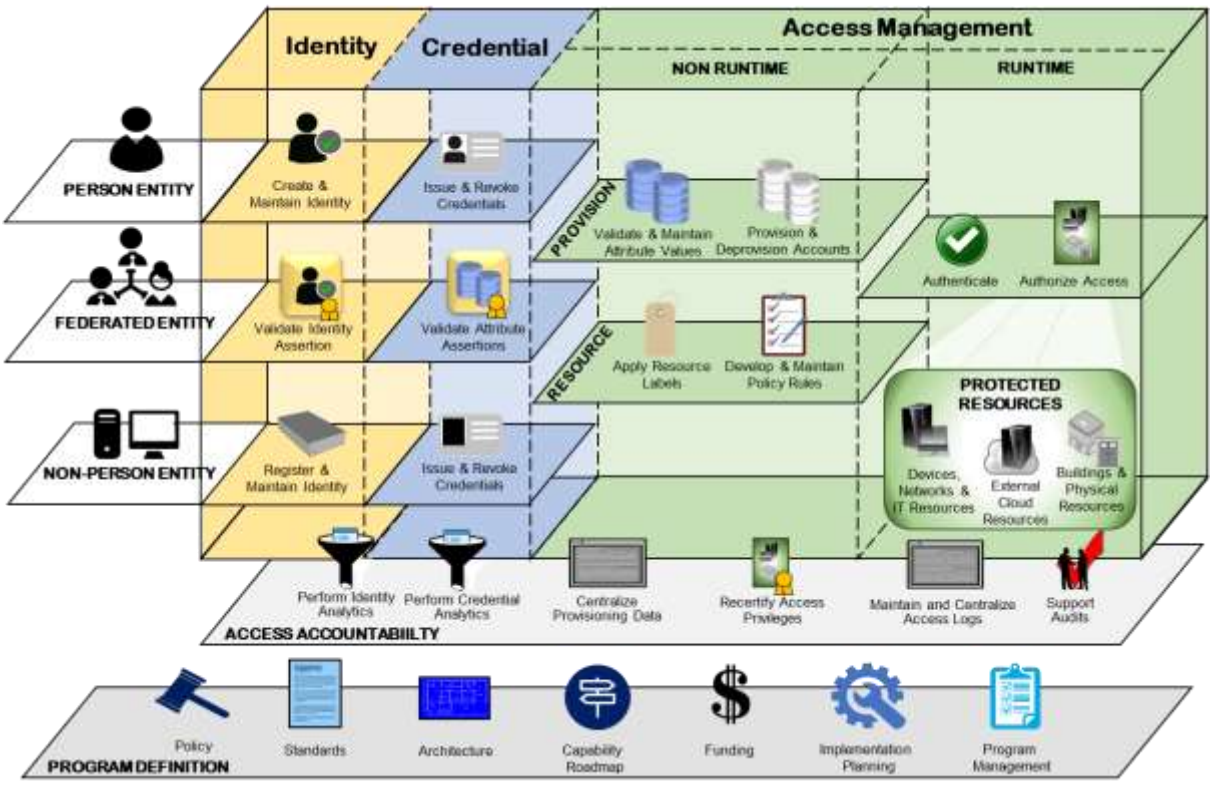


Figure 2 – Core ICAM High-Level Operational Concept Graphic (OV-1)

Implementing effective ICAM requires data management in accordance with data management principles, wherever ICAM data is originated or hosted. ICAM data includes identifiers and credentials to support authentication; authorization and environment attributes along with digital policy rules to support authorization; identity attributes to support contact data lookup; and access logs and provisioned entitlements to support attribution. While all data management principles are important, critical DoD Data Strategy goals include making ICAM data visible and accessible to information systems or other entities that require the data and ensuring that ICAM data has sufficient quality that it can be trusted by information systems in making access decisions.

2.1. Transformational Goals

The DoD Digital Modernization Strategy identifies eleven strategy elements in Goal 3, Objective 2, which is to "Deploy an End-to-End Identity, Credential, and Access Management (ICAM) Infrastructure." These strategy elements are designed to focus DoD resources towards building and deploying ICAM solutions. The resulting capabilities will facilitate information sharing across the DoD and with mission partners, while managing risks and protecting information against unauthorized access. The strategy elements are listed in Table 1.

Table 1 – ICAM Strategy Goals and Objectives

Element #	Strategy Element
1	Expand Public Key Enablement Capabilities to Support ICAM
2	Implement Automated Account Provisioning
3	Implement Support for Approved Multi-Factor Authentication Capabilities

Element #	Strategy Element
4	Enhance Enterprise Identity Attribute Service (EIAS)
5	Expand the Use of Derived Credentials
6	Implement a Data Centric Approach to Collect, Verify, Maintain, and Share identity and Other Attributes
7	Improve and Enable Authentication to DoD Networks and Resources through Common Standards, Shared Services, and Federation
8	Deploy Shared Services Promoting the Implementation of Enterprise ICAM
9	Enable Consistent Monitoring and Logging to Support Identity Analytics for Detecting Insider Threats and External Attacks
10	Enhance the Governance Structure Promoting the Development and Adoption of Enterprise ICAM Solutions
11	Create DoD Policies and Standards Clearly Defining Requirements for Identification, Credentialing, Authentication and Authorization Lifecycle Management

2.2. ICAM Capability Taxonomy Overview (DoDAF CV-2)

The DoD ICAM Capability taxonomy is shown in Figure 3. It consists of three high-level parent capabilities: core ICAM, access accountability, and contact data, and their second level child capabilities. These capabilities collectively provide the DoD with the ability to enable the right person entity or NPE to access the right resource at the right time for the right reason, and support knowing who is on the network at what time and for what reason. The CV-2 is based on the core elements of the FICAM Architecture. Attachment A contains a mapping of this taxonomy to the services defined in the FICAM Architecture.

This section provides an operational description of each of the ICAM capabilities identified in Figure 3. The intent of this section is to enumerate and describe these capabilities that must be part of DoD ICAM, but not to dictate exact implementations. ICAM capabilities may be performed at the DoD enterprise, DoD Component, COI, or local level. Some capabilities, such as identity management for mission partner entities, may also be performed externally to the DoD. Information systems may also consume capabilities from services operated at multiple levels depending on operational needs.

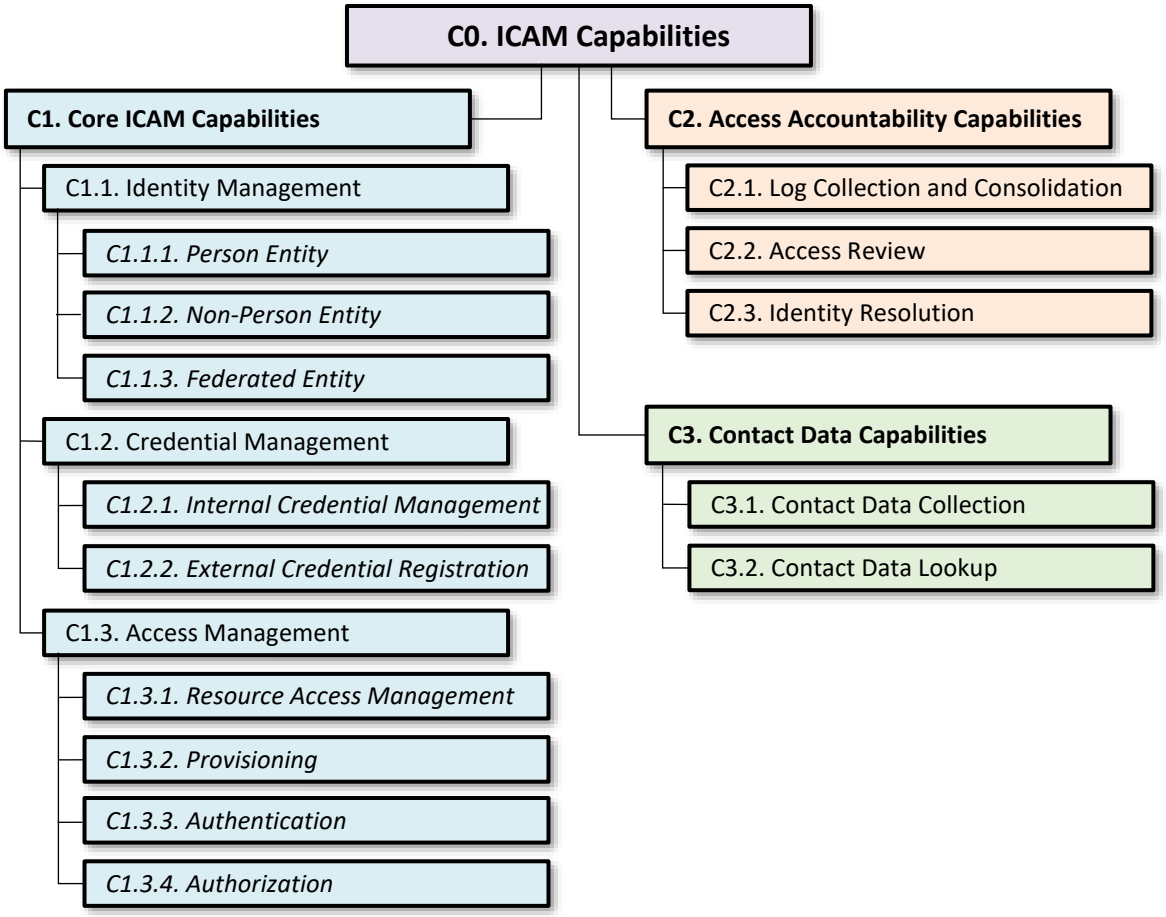


Figure 3 – ICAM Capability Taxonomy (CV-2)

2.2.1. Core ICAM Capabilities

As defined by the FICAM Architecture, ICAM is "the set of security disciplines that allows an organization to enable the right [entity] to access the right resource at the right time for the right reason." The FICAM architecture defines five lower level capabilities as:

- **Identity Management** allows an organization to construct a trusted digital identity based on an entity's defining attributes
- **Credential Management** allows an organization to associate a digital identity with authoritative proof of that claimed identity
- **Access Management** allows an organization to leverage trusted identities and authoritative credentials to ensure only permitted entities are granted access to protected resources
- **Governance** enables organizations to make programmatic decisions, manage enterprise policies, and promote program efficiency.
- **Federation** allows an organization to accept ICAM information and decisions across organizational boundaries based on an established trust**.**

This document focuses on the first three areas of identity management, credential management, and access management. Governance is addressed in Section 6, ICAM Implementation Responsibilities.

Federation is addressed within the three core areas. Core ICAM capabilities are shown inside the box in Figure 2, labeled Identity, Credential, and Access Management.

For DoD mission partner entities, ICAM capabilities can be performed internally by the DoD at the DoD enterprise, DoD Component, COI, or local level, or can be performed by federated service providers. These external services may onboard and manage mission partner entity identity and authorization attributes, issue and maintain credentials, and even perform authentication and generate assertions as an Identity Provider (IdP). Because DoD does not operate or oversee the operations of these external services, DoD must make a determination whether the service is operated in a fashion that is appropriate for DoD parties to rely on artifacts produced by the service. This determination requires that the service provider operates in accordance with an agreed upon set of minimum requirements. Approval may be implemented through a Memorandum of Agreement (MOA) or other formal mechanism.

Users who require a broad set of entitlements to perform their job function, or who require entitlements that allow them to manage the operations of information systems, network components, or resources are known as privileged users. Privileged users may require separate identifiers and credentials as well as additional auditing or monitoring to verify privileged user accounts are not being accessed by unauthorized users and privileged users themselves are acting within their job responsibilities. Provisioning entitlements for privileged users may leverage physical or virtual network segregation and specialized provisioning and authentication tools. However, the patterns for identity, credential, and access management for privileged users are the same as for non-privileged users. Examples of privileged users include:

- IT privileged users who have roles that allow read, write, or change access to manage IT systems including system, network, or database administrators; and security analysts who manage audit logs – IT privileged user roles are generic to all IT infrastructure, including transport, hosting environments, cybersecurity, and application deployment
- Developers and users with access to test tools
- Functional privileged users who have approval authorities within workflows – functional privileged user roles are specific to a mission area, such as human resources or finance

2.2.1.1 Identity Management

The baseline requirement for ICAM services is identity management. Entities must be assigned a persistent unique identifier. Attributes can then be bound to the identifier to define a digital identity. A single entity may be assigned different identifiers in different contexts. If these different contexts interconnect, it may be necessary to map identifiers from one context to another. While attributes associated with a digital identity change and evolve over time, digital identities never truly expire. Instead, a digital identity may be deactivated.

Attributes may be categorized into different types, such as identity, contact, and authorization, depending on how they are managed and used. Person entity identity attributes are generally managed as part of a human resources function, and may include name, rank, and organizational affiliation. Contact attributes are used to find and contact other entities, such as physical location, telephone number, and email address. Authorization attributes are used to support provisioning and access control decisions, such as clearance, training completion, and COI membership. Entitlements are an example of authorization attributes that are used to determine which information systems or resources within systems that an entity is authorized to access. Each attribute should be managed at a single source and distributed as needed.

Different authorization attributes for a single entity may be managed by different attribute services, depending on where the authoritative information for that attribute value is managed in the organization. Management and orchestration details for this distribution must be governed and controlled to ensure consistent data accuracy and to prevent collisions. It is important to note that a single attribute may be used for multiple purposes. For example, an organizational affiliation attribute may be managed as a human resource data element as an identity attribute but can also be used by a contact data lookup service as a filter or used by an information system to determine authorization to access a requested resource.

Attribute values may also have different degrees of validation. Identity attributes may be verified through background investigations or by obtaining attribute values from a trusted source. Contact attributes may be self-asserted without requiring validation. Attributes whose values are self-asserted and not verified should not be used for authentication or authorization.

Because of security and privacy considerations, it is important that the extent of the distribution of attributes be limited to what is required for specific ICAM operational capabilities. For example, if a digital policy rule only uses a specific subset of attributes to make an access decision for a resource, then only that subset should be provided. Another example is if an information system is accessed only by a subset of DoD entities, then generally only attributes for this subset of entities should be distributed to that information system. An exception might be a service that supports Contact Data capabilities, which may require distributing a subset of contact attributes for entities to that information system. Other considerations for determining the extent attributes should be distributed include privacy and legal considerations, operations security, and system performance, particularly when bandwidth is limited.

Identity management may be performed at the DoD enterprise, DoD Component, COI, or local level. Identity management for mission partner entities may also be performed externally to the DoD.

2.2.1.1.1 Person Entity

Person entities must be assigned an identifier that is persistent and unique within the context where it is used, which might be DoD enterprise, DoD Component, COI, or local. If a COI or local information system has a combination of users who are registered at the DoD enterprise level and users who are managed locally, digital identities for DoD enterprise registered users must be mapped to their DoD enterprise identifier to support access accountability.

Person entities include people, but person entities may also be roles. For most use cases, roles should be defined as attributes of the people authorized to hold those roles. When distinct identities for roles are required, such as for IT privileged user accounts and representation of organizational affiliation for systems that do not support multiple roles based on a single identity, the role identity must be tightly bound to the individual who is acting in that role to support attribution. Because attributes, credentials, and entitlements may be associated with roles, digital identities for roles must also be managed. A role may be linked to a specific individual, such as an organizational relationship or a privileged user identity. A role may also be shared by multiple person entities, either concurrently such as membership in a group or sequentially such as a watch officer station that is staffed by different people at different times.

For DoD internal community members and beneficiaries, identity information for person entities is managed at the DoD enterprise level by the Defense Manpower Data Center (DMDC). Person entities are assigned a unique ten digit number identifier by the Person Data Repository (PDR) when the person is first associated with the DoD, which is known as the Electronic Data Interchange Person Identifier (EDIPI). This number is permanently assigned and unchanging. In addition, person entities are assigned

an Enterprise Username (EUN), which is a declarative human readable identifier based on the person's name. The EUN is assigned when the person is first associated with the DoD. If the person changes their name, an additional EUN is assigned and it becomes the primary EUN. Because person entities may have multiple current and previous relationships with the DoD, and these relationships may have different authorizations to access DoD resources, DoD internal community person entities are also assigned one or more personas that identify the relationship of the person entity to the DoD. For example, a Military Service retiree may also be a DoD civilian employee, or a DoD contractor may also be serving in the National Guard. Personas are indicated by a Persona Type Code (PTC) that can be combined with either the EDIPI or the EUN to form a unique persona identifier. The set of PTCs is defined in the "Department of Defense Naming Convention for People within DoD Identity, Credential, and Access Management" document, and is also included as Attachment D. To support contact data lookup, the PDR also maintains a Persona Display Name (PDN), which is a human readable display name based on an individual persona.

2.2.1.1.2 Non-Person Entities (NPE)

NPEs include physical devices, systems, and processes that are assigned identifiers and may be issued credentials to support authentication and authorization. Accountability for the behavior of NPEs must be linked directly or through a chain of accountability to an individual or organization sponsor. The identity of the sponsor should be an attribute linked to the NPE. The following are examples of NPEs, note that a single NPE may fit in more than one of these categories.

- **Physical devices** including desktop and mobile endpoints, physical servers, and physical network infrastructure components such as firewalls and routers
- **Virtual machines** including virtual servers and virtual workstations
- **Information systems** hosted in data centers or in the cloud including applications and web servers with a long-term existence or with a short term existence (such as to support elasticity in the cloud)
- **Services** with a long-term or short-term existence including robotic process automation services and cloud-based services
- **Processes** spawned by information systems or services with a specific purpose that may have a limited lifespan, including artificial intelligence tools
- **Non-traditional systems** including weapons systems and control systems

Identifiers for NPEs must be managed. If an NPE will only need to be authenticated within a DoD Component or COI or be confined to a specific network layer, then the NPE must be assigned an identifier that will be unique within that community. NPEs that may interact across the DoD enterprise must be assigned an identifier that is unique across the DoD enterprise. ICAM data for these NPEs may be managed at the DoD, COI or local level. NPE attributes depend on the type of NPE, but may include organizational information, host name, Internet Protocol (IP) address, or fully qualified domain name.

Identity management for NPEs depends on the type of NPE. For devices, identity attributes should include linking the NPE to its supply chain and acquisition process, registration and configuration by an authorized person entity, and maintenance of the device from registration through decommissioning and destruction. For information systems and services, identity attributes should include the approval to operate and continued risk management framework status of the specific service or overall system it is a part of. For NPEs which are spawned by other information systems or services for a limited duration, identity attributes should include the identity of the creating information system or service and a unique identifier for each specific instance of the NPE. Because identities for processes are created by systems

or other processes, identity management of these processes must include the identity of the creating system.

2.2.1.1.3 Federated Entity

Identities for federated entities are managed external to the DoD enterprise. Where external entities are assigned identifiers by their own identity management system, these identifiers may be adopted and used by the DoD as part of the federation agreement if these identifiers are persistent and their construction means that there will be no chance of collision with DoD internal identifiers. If a persistent, unique identifier is not provided by a federated identity management system, a DoD enterprise, DoD Component, COI, or local identifier must be assigned and mapped to the external credential.

Identities managed in accordance with Federal standards including HSPD-12 and NIST FIPS 201 allow DoD to have a high level of confidence in these identities, credentials, and associated attributes.

For some federated entities, DoD may implement agreements to obtain identity attributes from the federated identity managers. Data exchange capabilities for these mission partners include:

- Identity registration management to obtain identifiers for mission partner entities and verify that those identifiers are persistent and will not cause collisions within the DoD enterprise, or to assign identifiers if the federated partner is not able to provide persistent unique identifiers
- Data exchange to provide attributes that can be cached by the DoD
- Sponsorship to identify whether specific person entities are approved by a DoD sponsor for having access to DoD resources
- Identity resolution to connect federated entities with DoD internally stored attributes such as Joint Personnel Adjudication System (JPAS)/Defense Information System for Security (DISS) background adjudication and clearance status

For some federated entities, the entity's own identity management service may be willing to provide attribute information. For other entities, the only attributes that will be available to DoD will be the identifier and the organization vouching for that entity. Attributes from federated entities should only be used during authentication and authorization decisions by DoD information systems if the DoD has evaluated the attribute provider as meeting DoD data quality requirements.

Authorization attributes may be provided by federated identity managers, or they may be provided by DoD authoritative attribute sources if the attribute is maintained internally to the DoD.

For some federated entities, identity and credential management will only be performed external to the DoD and individual users will not be registered or assigned DoD identifiers. Instead, the organization sponsoring these users will be registered and the relationship between the user and the registered organization will be asserted when access to a resource is requested. These users will only be able to access DoD resources that are releasable to the federated organization, such as a coalition partner country.

2.2.1.2 Credential Management

Credentials and their associated authenticators are the interface between real-world entities and digital identities. Credentials and authenticators are provided to entities and are then used by those entities to authenticate when requesting access to resources. Credentials are bound to one or more identifiers that

can be used by information systems or mapped to a COI or DoD enterprise identifier. Credentials that are issued in coordination with identity managers contain the identifier assigned to the digital identity.

The degree of confidence that relying parties have that the credential or authenticator is being presented by the real-world entity is known as the credential strength, and is based on three factors: the due diligence performed in identity proofing the identity of the real-world entity to create a binding between the real-world entity and the credential, the resistance of the credential itself to unauthorized access, and the operations of the credential issuance system.

Identity proofing is performed prior to issuing a credential to an entity. Generally, identity proofing occurs after the digital identity has been created (see Section 2.2.1.1) and is used to bind the credential to the digital identity. NIST SP 800-63A defines three IALs for person entities. IAL1 requires no validation of self-asserted claims made by the entity. IAL2 requires the collection of evidence that supports the real-world existence of the claimed identity and verifies the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing. IAL3 requires physical presence for identity proofing, presentation and verification of multiple high quality identity documents, and verification of identifying attributes performed by an authorized and trained representative of the Credential Service Provider (CSP). IAL2 is the minimum standard for access to DoD information systems unless IAL1 is specifically approved for access to a low sensitivity resource. IAL2 plus in-person identity proofing is required for credentials used to access highly sensitive information.

For NPEs, identity proofing and initial credential issuance are performed when the digital identity for the NPE is first created. Issuance of subsequent credentials to NPEs either relies on the NPE authenticating itself using an existing non-expired credential or the NPE's sponsor vouching for the identity of the NPE. Note that an existing credential can be used as proof of identity for additional credentials that have different form factors or are of different types.

Credential resistance to unauthorized use is directly related to the technology used for the credential. NIST SP 800-63B defines three AALs for credentials. AAL1 is a single factor such as username and password. AAL2 is multifactor where one factor may be username/password. AAL2 also includes software certificates issued by a PKI. AAL3 requires cryptographic authenticators with the private keys stored on hardware tokens. The AAL required for authentication depends on the level of sensitivity of the resource being accessed.

- **Username/Password Authentication** uses a single factor credential, the static password bound to the username. These AAL1 credentials are commonly used because they are relatively inexpensive to manage. However, users must maintain separate passwords for each independent system that requires their use, resulting in complex password management requirements. Password based authentication is also considered insecure because of various mechanisms that an attacker can use to obtain the username/password pair.
- **Multi-Factor Authentication (MFA)** is a characteristic of an authentication system or an authenticator that requires more than one distinct authentication factor for successful authentication. Additional authenticators may include authenticating the device in addition to the user, requiring that the user enter a one-time password obtained from a device or mobile application, providing a code sent out-of-band to the user, or verifying a cryptographic token possessed by the user. An MFA can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors.

Different MFA technologies have different authenticator assurance levels, depending on the factors selected.

- **Certificate-Based Authentication** relies on the cryptographic properties of public key cryptography where the use of the private key to encrypt can be verified by the use of the public key to decrypt, and where determining the private key is computationally infeasible even when the public key is known. Public key certificates are issued by a PKI that binds the public key to one or more identifiers. Private keys are protected in cryptographic modules that are under the control of the entity named in the certificate. Private keys may be generated and protected in software cryptographic modules that permit copying the private key, and are considered AAL2. For AAL3, private keys are generated and protected in hardware cryptographic modules that offer significantly stronger protection of the private key against attack. Private keys may also be generated and stored using hybrid approaches where the key is generated in a software cryptographic module but then moved to a hardware module and the copy in software is deleted. This hardware backed approach is not fully AAL3 compliant but is significantly stronger than AAL2 software PKI. Public key cryptography must use cryptographic algorithms that meet current NIST, CNSS, and DoD standards.

In addition to IAL and AAL, credential strength is also dependent on protections implemented by the CSP to prevent the unauthorized issuance of credentials. These protections include physical and logical controls around accessing the CSP, cryptographic protection of any keys used by the CSP to generate credentials, and checks and balances for personnel who either administer the system or are authorized to approve the issuance of credentials. Review of these controls is part of the approval to operate for DoD managed CSPs, and is included in the approval review for external CSPs.

2.2.1.2.1 Internal Credential Management

CSPs must support the following lifecycle management activities when issuing credentials to entities.

- **Sponsorship** – establishing that the entity is eligible to obtain the credential. Establishment of the digital identity is part of identity management. Sponsorship may occur as part of identity management or may be performed independently as part of credential management
- **Identity Proofing** – verifying that the entity requesting the credential is the enrolled entity
- **Issuance** – creation and registration of the credential and providing the authenticator to the entity
- **Maintenance** – performing any maintenance tasks related to the credential type
- **Revocation or Expiration** – making the credential invalid – some credentials, such as PKI digital certificates, may contain expiration dates within the credential while others remain valid until the CSP revokes them
- **Validation** – providing information to relying parties regarding the validity of the credential

Credentials may be issued based on the validation of an existing credential to support a different form factor or different use cases. These credentials, known as derived credentials, maintain the same IAL as the credential used to request them, and may have the same or lower AAL depending on the form factor of the new credential.

2.2.1.2.2 External Credential Registration

Many DoD mission partners perform identity management within their own enterprises and issue credentials to their entities. When these services are operated at a sufficient level of assurance, these credentials may be authenticated by DoD relying parties instead of issuing new credentials to these

entities from DoD operated credential providers. Although DoD may rely on these credentials, DoD does not have any control over what identifiers they contain. In order to support attributes about these entities that are managed within the DoD, and to provide attribution for the actions of these external entities, external mission partner entities must have an identifier that is unique within DoD enterprise, DoD Component, COI, or local level, as appropriate. When mission partner credentials have a unique identifier, such as the full distinguished name from a PKI-based digital certificate, this identifier may be used. If necessary, mission partner credentials may be mapped to an internally assigned unique identifier.

2.2.1.3 Access Management

As defined in the FICAM Architecture, access management is "the set of practices that enables only those permitted the ability to perform an action on a particular resource." As shown in Figure 2 – Core ICAM High-Level Operational Concept Graphic (OV-1) in Section 2, implementing access management includes resource management and provisioning that are performed prior to runtime, and authentication and authorization that are performed at runtime. Authentication is supported by identity management and credential management. Authorization is supported by resource management and provisioning. Attribute-Based Access Control (ABAC), a specific type of access authorization, is supported by identity management as it relies on real-time access to valid authorization attributes. Verifying entity identity and authorization to access resources is a foundational element of ZT, and must be performed within the context of the resource being accessed.

2.2.1.3.1 Resource Access Management

Resource management and data tagging are not in scope for the ICAM Reference Design, but resource access management, including the ability to properly relate a resource to an ICAM process, is a critical dependency for proper access determination. The DoD is developing a Data Reference Architecture to address data resources, but for ICAM, the term resource is broader than data. A resource is anything to which an entity can request access. Resources may be:

- Sets of information such as structured data in a database or unstructured data in a document
- Services such as e-mail or word processing
- NPEs
- Facilities, buildings, or protected areas within buildings
- Conference rooms or shared work spaces

Resources may be hosted at DoD sites, by DoD mission partners, or in private, public, or hybrid clouds. Although attribution of who accessed what resource is always important, some resources also require maintaining an accurate number of authorized users for licensing purposes or require a record of who is pre-authorized to access the resource to support audits. Understanding these constraints is important when defining access rules for resources, and when determining if access to the resource is a candidate for dynamic provisioning or dynamic access. See Section 2.2.1.3.2 for more information on dynamic provisioning and Section 2.2.1.3.4 for more information on dynamic access.

Access to resources may be managed through rules applied by the information system that hosts the resource, or the resource itself may be tagged with attributes that link its access to a specific rule. Resources may also be tagged with additional attributes that may be used by a content data lookup service. In all cases, rules must be developed by the resource owner that specify how access to that resource is to be granted, and these rules must be codified into digital policy rules. Management of these digital policy rules can be performed at a DoD enterprise or DoD Component level for some

resources, but may be delegated to a COI or local information system owner where more local rules need to be enforced.

Access to resources may be dependent on environmental factors such as time of day, date, external event occurrence, physical location of entity making the request, or threat level. These environmental attributes are data elements that are not specifically about the entity or the resource, but about the current environment at the time of the transaction itself. Another way of viewing environmental attributes is that they describe the *situation*. For example, "John Smith is attempting to access this resource from the Internet at 3am on a Sunday."

Digital policy rules must be stored in an isolated policy store with controlled interfaces to the access control mechanisms of information systems hosting the resource. Digital policy rules that control access to resources at an information system level may be hosted in a policy store or may be hosted by the information system itself (e.g., digital rights management).

2.2.1.3.2 Provisioning

Provisioning is the process of granting and revoking authorizations to entities for specific access rights to resources, known as entitlements. Provisioning entitlement processes must verify that the entity meets the requirements defined in the digital policy rule defined for the resource. Provisioning entitlements may be either manual or dynamic or a hybrid of both. This section specifically addresses provisioning for Role Based Access Control (RBAC). Provisioning and de-provisioning of attributes used for ABAC is discussed in Section 2.2.1.1.

Manual provisioning of entitlements requires a person entity to participate in the provisioning process by validating that the entity meets the digital policy rule requirements. Manual provisioning is performed when dynamic provisioning is not available, when one or more attribute values needed to satisfy the digital policy rule are not available on-line, or when digital policy rules do not support dynamic provisioning. For example, if the digital policy rule for a resource includes a requirement for manager approval, then the entitlement cannot be fully automated. Manual provisioning cannot be performed real-time. An entity can request access to a resource but will not be granted the entitlement to access that resource until the manual process is completed. When manual provisioning is required, digital policy rules should be documented to support consistent provisioning and to support future dynamic provisioning processes.

Dynamic provisioning of entitlements can be performed entirely without human intervention and can be implemented when the digital policy rules for access to the resource can be resolved by verifying that attribute values for the entity meet the requirements in the policy rule. Dynamic provisioning can happen at defined periodic intervals, in response to a request from an entity or a manager, or it can be triggered by an information system itself when an unanticipated user requests access to a resource.

De-provisioning of entitlements should occur when an entity no longer requires access to a resource to perform its job function, or when an entity is no longer eligible to be provisioned access to the resource as a result of changes in either the entity's attributes or the digital policy rules governing access to the resource. De-provisioning actions should be triggered when a user changes roles within an organization, when a user leaves an organization, at the end of a pre-determined period of time, or when other attribute values change that impact authorization. Manually provisioned entitlements may require manual de-provisioning when no longer valid unless they can be linked to dynamic triggers such as a the end of a contract. Where dynamic provisioning is used, de-provisioning must be implemented using the same dynamic processes. For some resources, a periodic access review must also be performed to verify

that all provisioned entitlements are still valid, and entitlements must be de-provisioned if no longer valid.

2.2.1.3.3 Authentication

Authentication is the process by which a claimed identity is confirmed, generally through the use of a credential. Credentials are validated by the CSP, either directly, or through artifacts generated or published by the CSP. Credentials may contain the identifier for the digital identity, or, for federated credentials, may contain an identifier that must be mapped to the internal identifier. As described in Section 2.2.1.1 and Section 2.2.1.2, different types of credentials have different assurance levels and are appropriate for authentication to resources at different levels of sensitivity as described in DoD Instruction 8520.03, *Identity Authentication for Information Systems*.

Entities must be authenticated prior to providing access to resources, except for resources that have been approved as publicly releasable. In addition, authentication should only be valid for a limited duration, and entities should be required to re-authenticate, especially after a period of inactivity. Appropriate duration is dependent on the information system and type of resource being accessed.

Information systems can directly authenticate entities. For direct authentication, the information system must be able to perform the following:

- Request and accept the authenticator provided by the entity
- Validate the credential by interfacing with the CSP or consuming validation artifacts produced by the CSP to determine that:
    - The CSP is trusted
    - The identity proofing of the entity was of sufficient strength (e.g., IAL)
    - The credential presented by the entity is of sufficient strength (e.g., AAL)
    - The credential has not expired or been revoked
- For MFA credentials, ensure each factor has been validated
- Map the identifier contained in the credential to the appropriate DoD enterprise, DoD Component, COI, or local identifier

While performing direct authentication maintains security by relying only on validation via the CSP, implementing direct authentication, especially in a federated environment where mission partner entities have credentials issued by multiple external CSPs, has proven to be difficult, impractical, expensive, and in some cases technically infeasible.

As an alternative to performing direct authentication, one or more information systems can be hosted behind an in-line reverse proxy IdP. The reverse proxy IdP performs all of the authentication functions on behalf of the information systems, and then provides a customized authentication assertion to each information system using a format that can be consumed by the information system without requiring changes to the existing capabilities of the information systems. Reverse proxy IdPs can also be used to support authentication of the endpoint device and establish network connectivity prior to authenticating the entity.

Information systems can also be configured to consume standards-based assertions from IdPs. Assertions are digitally signed data artifacts that contain the identifier of the entity that has been authenticated by the IdP, the IAL and AAL of the original authentication, and can optionally contain other attributes about the entity. NIST SP 800-63C defines three federation assurance levels for authentication assertions. FAL1 requires the assertion to be digitally signed. FAL2 requires the data in the assertion to be encrypted as well as signed. FAL3 includes an additional step known as “holder of

key" where the assertion includes the public key associated with a private key held by the entity, and the relying party must verify that the entity does have access to that private key in addition to accepting the information contained in the assertion. When using an IdP, the information system redirects the entity to the IdP. The IdP performs the authentication steps and provides an assertion that includes the entity's identifier and potentially additional attributes that can be used to support authorization decisions. The IdP can either provide the assertion directly to the information system or provide it back to the entity who then presents the assertion to the information system.

IdPs may be operated within the DoD, or they may be operated externally to the DoD. Some mission partners support IdPs that authenticate credentials issued by that mission partner and provide authentication assertions to the DoD rather than requiring DoD information systems to directly authenticate their credentials. IdPs can also be used when authenticating DoD users to externally operated information systems such as cloud Software as a Service (SaaS) providers. In general, SaaS solutions do not support direct authentication and require authentication assertions.

Authentication assertions can also support a special case of authentication, where an NPE process is acting on behalf of a person entity or another NPE. Direct authentication only supports authentication of the NPE process itself. Assertions can contain all identifiers associated with the request, including the identifier of the requesting person entity or NPE. Assertions can also require holder of key verification for any combination of the asserted entities.

Although reconfiguration of authentication is needed to recognize and accept authentication assertions in lieu of direct authentication, authentication assertions offload all of the complexity of authentication to the IdP, simplifying the overall authentication process. However, reliance upon an IdP does introduce dependencies that may affect latency and system availability. Because information systems rely on IdPs, the IdP must be operated securely. Specific areas of concern for secure operations include:

- Protection of the private key it uses to digitally sign assertions
- Physical and logical protections to prevent unauthorized access
- Background checks and multi-person control for administration of the IdP

2.2.1.3.4 Authorization

Authorization is the process of determining if the entity can be provided access to the requested resource based on the digital policy rule the resource owner identified for the resource. Authorization takes place after the entity has been authenticated. Authorization requires either that the entity has been provisioned for access (see Section 2.2.1.3.2) or that access can be dynamically authorized through ABAC.

Authorization at the network level to the requested resource should follow the ZT Architecture principle, which dynamically evaluates the authorization policy rule using the user's identity, the endpoint's NPE identity, attributes about the user, the endpoint, and the context such as time of day and geo-location. If a grant decision is made, Software Defined Networking (SDN) dynamically creates a micro-segment network path to provide access. The authorization decision should also be logged.

Authorization to access resources that are tied to provisioned entitlements requires checking the entitlements, which are either cached locally by the information system or are maintained in the appropriate provisioning system. For legacy information systems that are accessed via a reverse proxy IdP, the reverse proxy may determine authorization and request the resource on behalf of the entity.

Access to resources that are likely to have unanticipated users and that do not require provisioning of entitlements (e.g., to manage licenses or to maintain a record of who is authorized access to support audits, which may require individual or role-based entitlement provisioning) should be implemented through dynamic access, also known as ABAC. Dynamic access does not require the use of a provisioning system or the provisioning of entitlements at the information system level. Instead, authorization is determined at the point in time the entity requests access to the resource based on the digital policy rule for the resource and authorization and environment attribute values. In addition to providing a mechanism for real-time access for unanticipated users, dynamic access eliminates the need to provision and de-provision entitlements, as the access decision is based on current digital policy rules and entity attribute values. Implementing dynamic access requires that attributes needed to resolve digital policy rules be available in a standardized format and be maintained such that the value of these authorization attributes is of sufficient quality and accuracy to rely on them for making access decisions. The following documents provide additional information in deploying ABAC.

- NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations
- NIST SP 800-205, Attribute Considerations for Access Control Systems
- NISTIR 8112, Attribute Metadata: A Proposed Schema for Evaluating Federated Attributes

2.2.2. Access Accountability Capabilities

Access accountability supports accountability of person entities and the owners of NPEs for the actions of these entities. It also provides forensics and support for detection of entities that are attempting unauthorized access to DoD resources or access that is not aligned to the entity's role or function. ICAM supports access accountability through three lower level capabilities:

- **Log Collection and Consolidation** creates and makes available event logs for ICAM events including credential issuance, credential revocation, authentication, and access decisions
- **Access Review** allows supervisors and other approving officials to view provisioned accesses for their employees and other sponsored entities to confirm that only those access rights needed to perform the entity's job function have been granted
- **Identity Resolution** is a DoD enterprise, DoD Component, or COI level service that reviews digital identities to determine if a single real-world entity has more than one digital identity, and supports consolidation of the multiple digital identities into a single digital identity

Access accountability capabilities are shown on the plane at the bottom of Figure 2.

Although audit is out of scope for ICAM, access accountability capabilities provide information that can be used to support audits. For example, ICAM logs can be used to support insider threat detection, and access review is an important compensating control for financial audits. ICAM logs can also be used to support development of risk scores for risk adaptive digital policy rules.

2.2.2.1 Log Collection and Consolidation

Access accountability is about holding people accountable for their actions when they access DoD resources, and for holding people or organizations accountable for the actions of NPEs that access DoD resources. It also provides forensics and support for detection of unauthorized attempts to access to DoD resources. ICAM supports access accountability in two ways: by creating and maintaining event logs recording ICAM related activity, and by enabling access to these activity records. Information systems and services performing authentication and authorization must log ICAM events. Creation of ICAM event

logs is local to an information system or ICAM service. However, the ability to access event logs and review activity across consolidated logs may be a DoD enterprise, DoD Component, or COI level service.

Monitoring is a separate capability that is the joint responsibility of the system owner and organizations such as the US Cyber Command (USCYBERCOM), law enforcement, IT service providers, and physical protective services. Monitoring capabilities may rely, in part, on ICAM activity records as a source of information. In turn, monitoring capabilities can provide analytical data to information systems to support risk scores associated to entity activity. Information system owners and ICAM service providers must be aware of the need to work with organizations that are responsible for monitoring, to provide event log data, as appropriate. As a result, although monitoring of entity activity is not a DoD ICAM capability, collection of ICAM event logs for a group of information systems in support of monitoring may be performed as part of ICAM.

ICAM operational and data capabilities must be implemented such that they do the following:

- Link an entity's digital identity to their ICAM activity
- Record that entity's activity in ICAM event logs
- Record other ICAM activity not directly associated with entity activity (i.e., modification of an access policy)
- Enable authorized access to these ICAM event logs, as appropriate

For all ICAM events, DoD ICAM access accountability operational capabilities must:

- Create and maintain ICAM event logs
- Enable appropriate authorized access to these ICAM event logs

The requirement to create and maintain ICAM event logs should not be interpreted as a requirement to implement new or separate logging systems. ICAM event logging capabilities should generally be implemented as an integral part of the event logging capabilities already available in information systems. ICAM event logs and logging capabilities must have the following characteristics:

- **Auditable** – provisioning, authentication, authorization, and other ICAM related events can be formally tracked, whether successful or not successful
- **Traceable** – it is possible to determine where an event occurs in all tiers of ICAM systems
- **High integrity** – logs cannot be overwritten or tampered with by local or remote entities
- **High confidentiality** – logs are appropriately protected from unauthorized disclosure
- **Traceability** – entity identifiers are linked to entity activity

2.2.2.2 Access Review

Unlike log collection, consolidation, and review, which provide information about what resources an entity has actually attempted or succeeded in accessing, access review is a process used to verify that the set of resources that an entity is authorized to access is limited to what is needed to perform that entity's job function. Access reviews can be performed by the manager for a person entity or by the sponsor of an NPE, or may be performed by an information system owner to verify that all entities that have access have appropriate need to know. Access review may be required for some types of resources, such as financial systems. Access reviews may also be performed to mitigate the concern of a single entity collecting too many access rights over a long period of time when additional entitlements are granted when the entity changes job function, but entitlements needed to perform the previous job function are not removed.

Access reviews may also be referred to as access re-certification or access attestation.

2.2.2.3 Identity Resolution

Enterprise-wide identity management and credential registration services help to implement a single digital identity for a real-world entity across the DoD. However, manual processes and elevation of digital identities originally managed at a DoD Component, COI, or local level can result in a single real-world entity having more than one digital identity. Identity resolution is the process used to review digital identities and map distinct digital identities to a single digital identity if they represent a single real-world entity. Identity resolution is implemented using a combination of automated processes that monitor digital identity information and flag potential duplicates and manual review to determine if the potential duplicate should be consolidated to a single identity.

Where a single real-world entity has multiple roles and has been issued different credentials for use with different roles, each role may have its own identifier, but the roles should be linked in an identity management system to allow mapping the distinct identifiers to the single real-world entity. Examples of different identifiers for different roles include:

- A single person entity may have multiple personas when interacting with DoD relying parties – such as a contractor and a reservist, with different access rights depending on which persona the person entity is acting in
- A privileged user such as a network administrator may use a separate credential and identity when performing administrator duties
- An aide may be authorized to perform certain actions on behalf of an executive, and uses a credential that identifies the relationship with the executive when performing those actions

2.2.3. Contact Data Capabilities

Contact data provides the ability to obtain contact information about how to locate and communicate with person entities as well as relevant resources and NPEs. Examples of resources and NPEs that could be included in the contact data capability are: conference rooms, email lists, organizational calendars, and information systems. Attributes that may help distinguish a person entity include display name, name, rank, location, and organizational affiliations. Attributes for NPEs include URL, IP address, fully qualified domain name, and what resources are managed by the NPE. Attributes that may help contact an entity include telephone numbers, physical addresses, email addresses, encryption certificates, and contact preferences. These attributes are managed and made available using the same or similar systems as other ICAM services, which is why they are included in the scope of ICAM.[2] ICAM supports two lower level capabilities for contact data lookup:

- **Contact Data Collection** collects contact information for a COI into a single data store. Contact information may include mission partner entities as well as DoD internal community members
- **Contact Data Lookup** provides an interface for entities to access and search contact data across a COI using a defined interface.

[2] Note that contact data repositories are likely to be systems of record under the Privacy Act and may require a Privacy Impact Assessment (PIA) and other compliance measures.

2.2.3.1 Contact Data Collection

Contact data collection requires obtaining contact attributes from one or more repositories, including identity managers, entity data repositories, and attribute services. Contact data collection also requires normalization to guard the integrity and validity of the collection. Where available, contact attributes should be obtained from authoritative sources. However, contact attributes may be self-asserted and may be locally maintained if they are only of interest at a COI or local level.

2.2.3.2 Contact Data Lookup

Contact data lookup should be implemented primarily as robust, user-friendly search capabilities, but may also include the ability to browse through structured records. Contact data may include Personally Identifiable Information (PII), other Controlled Unclassified Information (CUI) or information with a restricted need to know. Contact data must have appropriate confidentiality and access control protections.

These capabilities should enable a person to search for entities in a variety of ways, including the following:

- Searchable by person entity attributes, with results presented by persona
- Searchable by organization attributes, with results presented by persona or organization
- Searchable by functions (such as job skills), with results presented by persona or organization

2.3. Using DoD Enterprise ICAM Services

This Reference Design provides architecture guidelines and requirements for ICAM services implemented at the DoD enterprise, DoD Component, COI, or local level. Information systems are encouraged to leverage DoD enterprise ICAM services. Centralization of identity and credential management with distributed execution of access management using consistent standards provides benefits both to the DoD and to information system owners.

2.3.1. DoD Enterprise Benefits from Use of DoD Enterprise ICAM Services

Deploying and using DoD enterprise ICAM services provides significant benefits to the DoD. The primary benefit is consistency. When entities are assigned an enterprise identifier that is linked to one or more approved credentials, attribute values and other information about that entity can be applied in a consistent fashion across the DoD and access decisions can be made based on this common data. Because systems implementing DoD enterprise ICAM services are dedicated to those functions, they can better focus on policy compliance, accuracy, and performance.

By centrally managing and implementing enterprise ICAM services, the DoD can minimize costs caused by duplication of effort for deployment and integration, as well as reducing redundant licensing costs for the same set of users.

Using DoD enterprise ICAM services also provides a better user experience, especially for person entities. Use of enterprise ICAM services results in fewer credentials to manage, and a consistent set of processes to follow to register and validate attribute values. Enterprise services can also provide a consistent process for requesting and obtaining access to resources.

Finally, adoption of DoD enterprise ICAM services provides enhanced cyber security. De-provisioning an entity who is no longer authorized access to DoD resources at the point of registration can immediately

result in denial of access to all resources that are relying on enterprise ICAM services. Monitoring activity across DoD information systems can also help to identify potential insider threat or external credential hijacking faster and more accurately.

2.3.2. Information System Benefits from Using DoD Enterprise ICAM Services

Integrating DoD enterprise ICAM services also provides benefits to information systems. Dedicated enterprise services can manage the complexity of performing ICAM actions, freeing system owners from local customization to address internal DoD community and mission partner users. Information system owners can build to specific interfaces supported by enterprise systems rather than maintaining compatibility with changing industry standards. Also, provisioning and de-provisioning entitlements can be simplified when linked to enterprise events such as revocation of a credential or change in attribute values.

2.3.3. Mitigating Challenges to Using DoD Enterprise ICAM Services

Using DoD enterprise ICAM services can also pose challenges for information system owners. Table 2 describes some of these challenges and identifies recommended actions for mitigating those challenges.

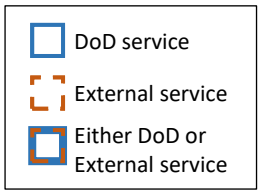
Table 2 – Mitigating Challenges with Use of Enterprise ICAM

Enterprise ICAM Service Challenge	Recommended Mitigations
System owner is dependent on functionality decisions made by others, which may not fully reflect specific system needs	• Leverage enterprise services to the maximum extent possible • Participate in requirements management process to incorporate additional features in future enterprise service updates
System customization may be required to integrate with interfaces supported by enterprise service	• Plan for and deploy required customization • Deploy or use existing reverse proxy service that can consume enterprise services and provide supported interface to information system
Interfaces for enterprise service are not supported by technology underlying information system	• Plan for integration with enterprise service aligned with planned information system modernization • Deploy or use existing reverse proxy service that can consume enterprise services and provide supported interface to information system
Execution of enterprise service processes to complete user authorization are difficult for users to implement or not timely	• Participate in requirements management process to address process issues in future enterprise service updates • Leverage enterprise services for identity, credentialing, and authentication and Implement local services for authorization
Resource owner is not willing to accept the risk of authorizing access based on enterprise provided attribute values	• Participate in requirements management process to identify data accuracy requirements for identity and authorization related attributes • Update DoD policy to address reliance on attributes and requirements for attribute accuracy and currency • Request documentation from enterprise services for their data accuracy and refresh frequency commitments • Use Component, COI, or local services to address gaps

Enterprise ICAM Service Challenge	Recommended Mitigations
Service availability and response time are not within acceptable tolerance for information system	• Participate in requirements management process to identify availability and response time needs • Determine if tolerance can be changed for information system • Use Component, COI, or local services to address gaps
Enterprise services do not fully support mission need	• Participate in requirements management process to identify needs not currently met by enterprise services • Use enterprise services for capabilities provided by those services • Use Component, COI, or local services to extend enterprise services and address gaps
Enterprise services do not support entire user community	• Participate in requirements management process to identify needs not currently met by enterprise services • Use enterprise services for covered users • Use Component, COI, or local services to extend enterprise services and address gaps

3. ICAM Data Flows

This section provides generic data flows for the ICAM capabilities described in Section 2. These flows represent OV-5b activity flows. The intent of these data flows is to provide patterns for how ICAM capabilities will function to promote interoperability across the DoD enterprise, COIs, and local implementations. The data flows indicate on possible path, but in some cases actions may be performed in a different order. For some capabilities, multiple data flow options are described. Information systems may use one or more of the data flow options, depending on specific mission needs. Systems and services shown in these data flows may be operated at the DoD enterprise, DoD Component, community, or local level. In addition, a single service may provide the capabilities of more than one system shown in the data flow diagram, especially for services operated at the COI or local level. Data flows apply both to DoDIN connected systems and to standalone or closed restricted networks. For disconnected or intermittently connected systems, the services shown would either be locally managed and operated or would use local services that periodically obtain and cache data from enterprise services.



As shown in the box to the left, entities and services operated internal to the DoD are shown in blue, entities and services operated externally to the DoD are shown in brown with a dashed line, and entities and services that may be either internal or external to the DoD are shown by a thick blue box with an internal brown dashed line.

Table 3 describes the entities and services that are used in the data flow diagrams. Examples of existing DoD enterprise ICAM services are listed in bold italic font in the "Name" column. Descriptions of these enterprise ICAM services as well as services that are currently in development are provided in Section 5.

Table 3 – ICAM Data Flow Entities and Services

Name	Description and Functionality
Entities	
Entity	• The entity whose identity is being managed and that will be requesting access to resources
Approver	• An entity who is authorized to approve the creation and maintenance of digital identities
Sponsor	• A person entity who is responsible for the operations and actions of another entity such as an NPE or a mission partner entity
Resource Owner	• A person entity or organization that is responsible for a resource
Requestor	• An entity requesting that another entity be authorized access to a resource. The requestor may be the entity that is requesting access or may be another person entity or NPE requesting the access on the entity's behalf
Manager	• A person entity who has supervisory authority over an entity
Reviewer	• A person entity or NPE responsible for reviewing ICAM related logs
Services	
Local Identity Manager	• A data repository where identity related attributes are on-boarded and managed for a set of entities • Verifies attribute value correctness and currency

Name	Description and Functionality
	• Provides updates to entity and attribute values to identity manager
Identity Manager ***PDR***	• A data repository where identity related attributes are collected and managed for a set of entities • Obtains entity and attribute values from local identity managers • Assigns unique identifiers to entities • Provides identifiers and identity information to CSPs and entity data repositories
Entity Data Repository (EDR)	• A data repository that holds identifiers, credential information, and other attributes for a set of entities • Obtains identifiers and attributes from identity managers • Generates identifiers for mission partner entities that are not contained in identity managers • Registers credentials for internal and federated entities • Provides identifiers to IdPs and information systems based on the credential used to authenticate • Provides attributes to information systems, provisioning systems, and other systems and services
Authoritative Attribute Source ***milConnect, TASS***	• A data repository where ICAM authorization attributes are on-boarded and managed for a set of entities • Verifies attribute value correctness and currency • Provides updates to entity and attribute values to attribute services
Attribute Service ***EIAS, IdSS***	• A data repository where ICAM authorization attributes are collected and managed for a set of entities • Obtains attribute information from authoritative attribute sources • Provides attribute values to provisioning systems, policy decision points, and other systems and services
Credential Service Provider (CSP) ***DoD PKI, RAPIDS, DS Logon***	• A system that issues, maintains, and revokes credentials • Obtains identifier and other information from identity managers • Generates and issues credentials to entities based on approval and identity proofing • Maintains credentials • Revoke credentials in response to authorized requests • Provides credential validation, either directly or through publication of revocation lists or other artifacts
Resource Policy Service	• A data repository where digital policy rules governing access to resources are stored • Accepts and maintains digital policy rules defined by resource owners • Provides digital policy rules to entitlement provisioning services and policy decision points
Entitlement Provisioning Service	• A data repository that stores entitlements for a set of entities and provides entitlements to information systems • Accepts information regarding entitlements from information systems

Name	Description and Functionality
	• Provides an interface for manual provisioning and de-provisioning actions by authorized users • Obtains digital policy rules from resource policy services for use in dynamic provisioning • Obtains attributes from entity data repositories and attribute services for use in dynamic provisioning • Makes dynamic provisioning and de-provisioning decisions based on digital policy rules and entity attributes • Provides entity entitlement information to information systems
Information System	• A system that hosts resources • Performs direct credential validation or processes authentication assertions from approved IdPs • Defines entitlements and provides them to entitlement provisioning services • Obtains entitlement information from entitlement provisioning services • (Optional) requests dynamic access authorization from a policy enforcement point • Provides resource access to authorized entities
Reverse Proxy Identity Provider (IdP)	• A system that performs direct authentication and optionally authorization on behalf of one or more information systems • Authenticates entities • Provides authentication information to information systems located in-line behind the reverse proxy using a format that can be consumed by each information system • (Optional) determines if entities are authorized to access resources hosted by each information system
Identity Provider (IdP) ***IdSS***	• A system that performs direct authentication of entities and provides an authentication assertions to the entity for use in authenticating • Authenticates entities • Obtains identifiers from entity data repositories for entities whose credentials do not directly contain the appropriate DoD identifier • Generates authentication assertions that include the DoD identifier, IAL and AAL of the authentication • Provides authentication assertion back to the entity or to the information system
Policy Enforcement Point (PEP)	• A system that responds to dynamic access requests from information systems • Receives access request • Provides information regarding the access, including the identifier of the requesting entity, the action, and resource or resources requested to a policy decision point • Receives authorization decision information from a policy decision point and provides it to the information system

Name	Description and Functionality
Policy Decision Point (PDP)	• A system that responds to dynamic access requests from policy enforcement points to make a real-time dynamic access decision for one or more resources • Obtains information regarding the access, including the identifier of the requesting entity, the resource or resources requested from a policy decision point, and the type of access requested • Obtains digital policy rules for requested resources from a resource policy service • Obtains entity attributes from the entity data repository and attribute services identified in the digital policy rules • Obtains environmental or other attributes identified in the digital policy rules • Makes an authorization decision by determining if the requirements of the digital policy rule have been satisfied • Provides the authorization decision to the policy enforcement point
Log Management System	• A data repository that hosts ICAM related event logs • Obtains ICAM related event logs from information systems, provisioning systems, reverse proxy IdPs, and other systems • Provides ICAM related event logs to monitoring services • Supports person entity or NPE review of logs to identify anomalous behavior
Master User Record (MUR)	• A data repository that hosts a record of entitlements entities have been granted • Obtains entitlements from entitlement provisioning services • Obtains organizational information from identity managers • Provides detailed entitlement reports for all entities that share a common manager
Contact Data Repository ***EDS, GDS***	• A data repository that hosts contact information for a set of person entities, resources, and NPEs • Obtains contact attributes from identity managers and attribute services • (Optional) provides an interface for entities to update contact attributes that are self-asserted • Provides a search capability for authorized users to obtain contact data

3.1. Core ICAM Capabilities

This section provides data flows for core ICAM capabilities including identity management, credential management, and access management. These core ICAM capabilities depict portions of the end-to-end flows for the lifecycle management of Identities and Credentials, and of the processes to manage and implement authentication and authorization. End-to-end flows will be tailored to specific technologies, mission partner integration, and mission needs.

3.1.1. Identity Management

This section addresses identity management for person entities, NPEs, and federated entities.

3.1.1.1 Person Entity

Digital Identity Creation

Figure 4 illustrates the services and steps for creation of a new digital identity. The role of the identity manager is to assign unique identifiers for all users and to store identity attribute data about each user. In a large distributed enterprise such as the DoD, identity information may be first entered into a local identity manager which then interfaces with the enterprise identity manager to obtain the unique identifier. The identity manager also registers the new digital identity by providing the identifier and appropriate attributes to the entity data repository. The role of the entity data repository is to support authentication and authorization events for the enterprise.

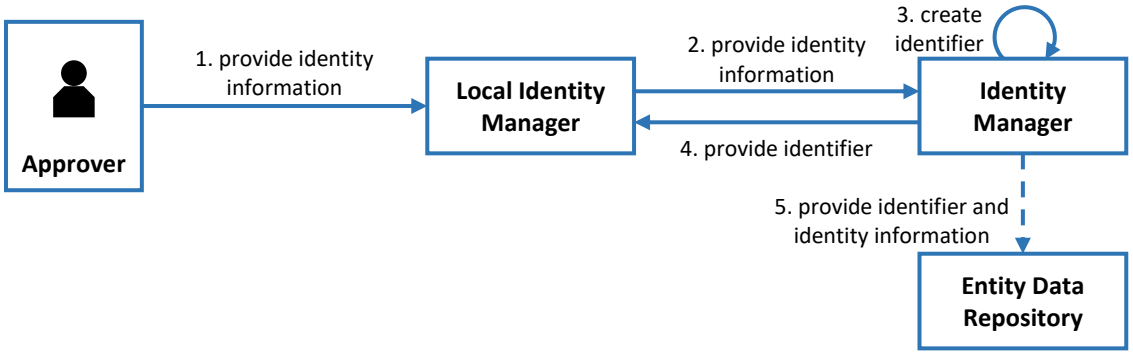


Figure 4 – Person Entity Identity Creation (C1.1.1)

Digital Identity Maintenance

Figure 5 illustrates the services and steps for updating identity attributes managed by the identity manager. Identity attributes should be updated directly to the same identity manager where the digital identity was first created and then provided to the enterprise identity manager. The enterprise identity manager then provides updated information to the entity data repository if the updated attributes are also stored in the entity data repository. For self-asserted contact attributes, the approver may be the person entity.

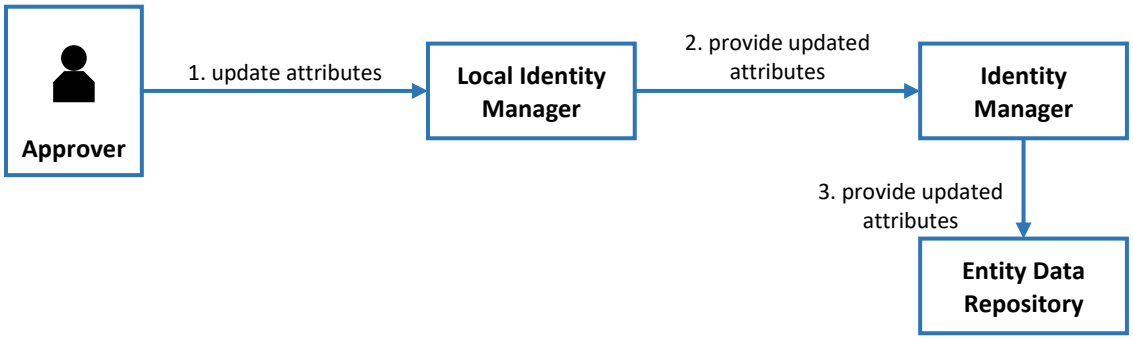


Figure 5 – Modify Identity Attributes (C1.1.1)

Attribute Maintenance

Not all attributes associated with a digital identity are managed at an enterprise level. Authorization attributes may be managed by separate authoritative attribute sources, depending on the entity and the attribute. Figure 6 illustrates the services and steps for updating these attributes.

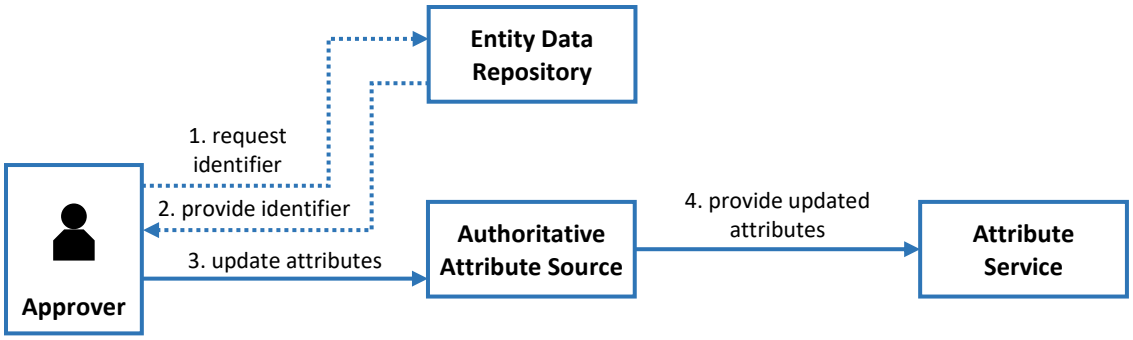


Figure 6 – Modify Attributes (C.1.1.1)

Attribute sources must include the unique identifier associated with the entity at the enterprise, DoD Component, COI, or local level. If the approver does not know the identifier, it may be obtained from an entity data repository. Attribute services combine attributes for a defined set of entities from one or more authoritative attribute sources and make those attributes available for use. For self-asserted contact attributes, the approver may be the person entity.

Digital Identity Deactivation

When a person is no longer affiliated with the DoD enterprise, DoD Component, COI, or local information system, the digital identity must be deactivated. Systems may retain the digital identity for audit purposes or in case the entity reestablishes a relationship with the DoD, but identity attributes must be updated to indicate that the digital identity is no longer active, and credentials must be revoked. Figure 7 shows the process of systems processing the deactivation notification to verify that the identity is deactivated in all systems connected to the identity.

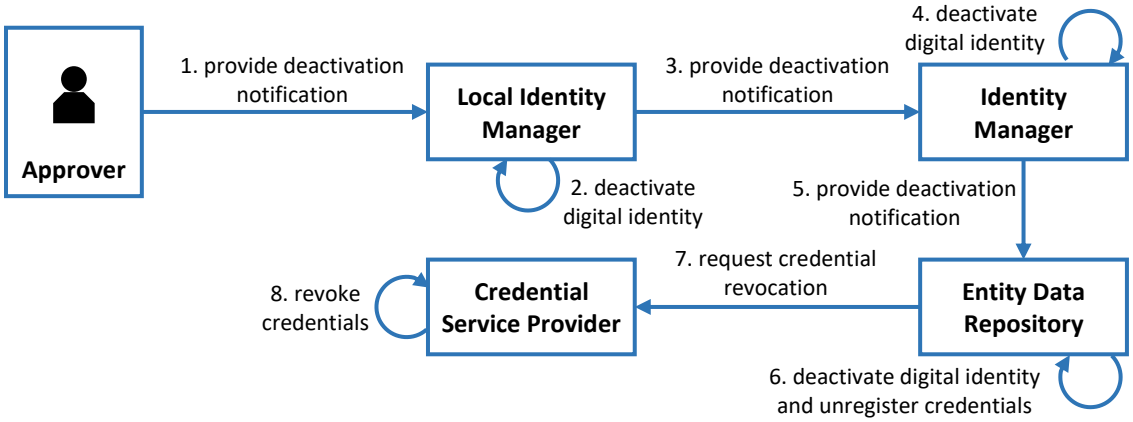


Figure 7 – Deactivate Identity (C1.1.1)

Deactivating a digital identity does not necessarily result in that identity being deactivated in authoritative attribute stores and attribute services. These systems are maintained independently of the identity management systems. However, because the person entity will no longer have valid credentials, that person entity will not be able to authenticate. Authoritative attributes stores should update attributes during their normal refresh cycles, or when notified that the status of a person entity has changed.

3.1.1.2 NPE

NPE Digital Identity Creation and Maintenance

The creation of a digital identity for an NPE is initiated by a sponsor, as shown in Figure 8. The sponsor may be a person entity or may itself be an NPE. Depending on the type of NPE, the NPE may have its own identifier, such as the serial number of a device, or it may be assigned an identifier by an enterprise, DoD Component, COI, or local level entity data repository. The entity is configured by its sponsor, and information about the NPE is entered into the entity data repository. If the configuration of the entity is modified such that attributes are modified, these attributes must be updated in the entity data repository.

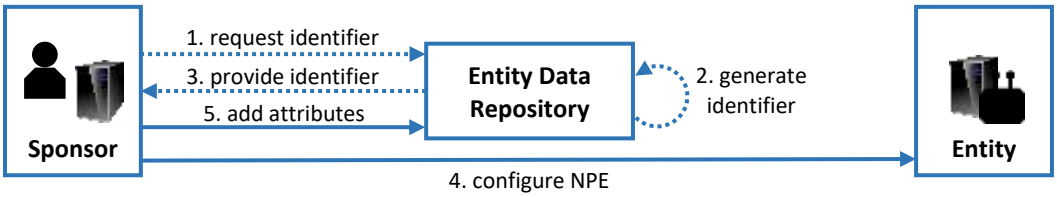


Figure 8 – Create and Maintain NPE Identity (C1.1.2)

NPE Digital Identity Decommissioning

Unlike person entities that are decommissioned but not deleted, digital identities for NPEs do not necessarily need to be maintained when the entity is decommissioned. When an NPE is decommissioned, the sponsor notifies the entity data repository, and the entity data repository requests revocation of any credentials registered to the entity. Once credentials are revoked, the entity data repository marks the entity as disabled. When the NPE is destroyed, the record can be updated to indicate it has been destroyed and the record can be archived. Keeping the record as disabled allows for processes including audits and inventory tracking while the NPE is unused but not yet destroyed.

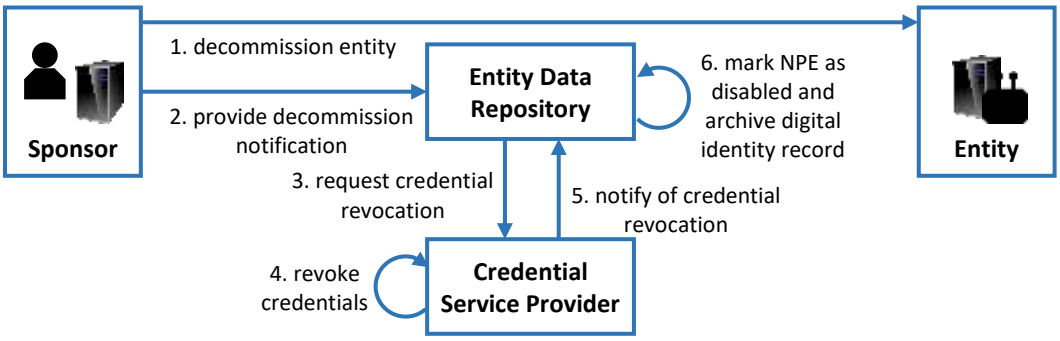


Figure 9 – Decommission NPE Identity (C1.1.2)

3.1.1.3 Federated Entity

Federated Digital Identity Creation

Digital identities for federated entities are created externally to the DoD. These federated digital identities and any associated credentials may be registered as described in Section 3.1.2.2.

Federated Digital Identity Maintenance

Digital identities for federated entities are managed externally to the DoD. However, for some external communities, the DoD may have an agreement to exchange and normalize one or more attributes.

Where such agreements exist, the external identity manager may provide updates to these attributes directly to the entity data repository as shown in Figure 10.

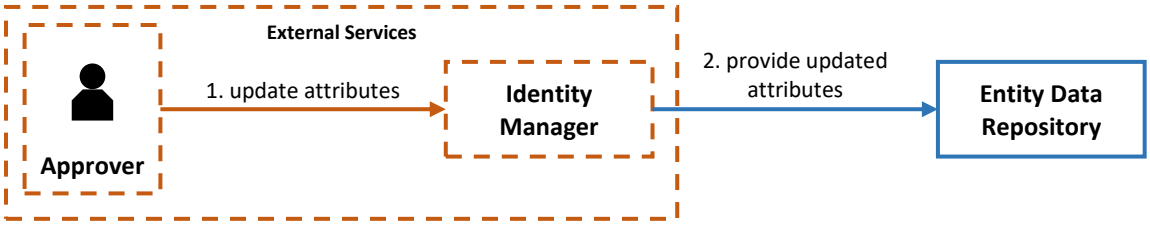


Figure 10 – Modify Federated Identity Attributes (C1.1.3)

Federated Digital Identity Deactivation

Digital identities for federated entities are deactivated externally to the DoD. Where attribute exchange agreements exist, the external identity manager will notify the entity data repository of the identity deactivation using the process shown in Figure 10. External identity managers should also require revocation of all credentials issued to that entity when a digital identity is deactivated.

Because management of digital identities and attributes for federated entities is not performed by the DoD, ICAM services that rely on information for federated entities should periodically refresh any stored information about these entities to verify that the digital identity is still valid.

3.1.2. Credential Management

This section addresses credential issuance, registration, maintenance, and revocation. Credentials that are issued internally are registered as a part of the credential issuance process. Entities that have credentials issued by approved external CSPs may register those credentials at the enterprise, DoD Component, community or interest, or local level in order to use those credentials to authenticate for access to DoD resources.

3.1.2.1 Internal Credential Management

Credential Issuance

Figure 11 illustrates the process for issuing a credential to a registered entity. This process assumes that the entity has prior approval to obtain the credential, see Figure 5 in Section 3.1.1.1 for information on how to register a person entity, and Figure 8 in Section 3.1.1.2 for information on how to register an NPE. Registration and credential issuance may take place at the same time or registration may happen before issuance. For example, an entity requesting a new credential because their current credential is about to expire may already be approved for the new credential. Alternatively, a workstation may obtain its credential as part of the process of initial configuration. The entity or its sponsor (for NPEs that are not able to request credentials directly) starts the process by submitting the request. The entity must provide information to prove its identity so that the CSP can verify that the entity is authorized to obtain the requested credential, and obtain the unique identifier for the digital identity associated with the entity. The CSP then creates a credential that includes the identifier and provides the credential or associated authenticator to the entity. The CSP also registers the credential with the entity data repository.

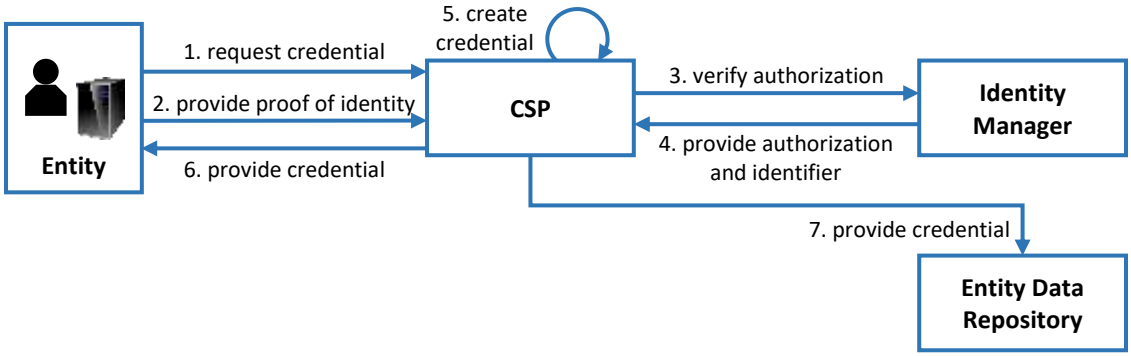


Figure 11 – Credential Issuance (C1.2.1)

Derived Credential Issuance

Derived credentials are credentials that are issued based on electronic authentication of an existing credential, and may have a different form factor than the original credential. Derived credentials have the same IAL as the credential used to authenticate, and may have the same or lower AAL depending on the type of credential. Revocation of the primary credential does not necessarily mean automatic revocation of the derived credential. For example, loss of the primary credential does not mean that a derived credential must be revoked. Because derived credentials are based on eligibility to hold the primary credential as part of the process to create the derived credential, if the entity is no longer eligible to hold the primary credential, the derived credential must also be revoked.

Figure 12 illustrates the process for issuing a derived credential. The entity starts the process by authenticating to the CSP that will issue the derived credential. The CSP must validate the credential, which may require requesting and obtaining validation from a different CSP if the CSP issuing the derived credential is different than the CSP that issued the original credential. The CSP then creates a credential based on the information contained in the original credential and provides the credential or associated authenticator to the entity. The CSP also registers the credential with the entity data repository.

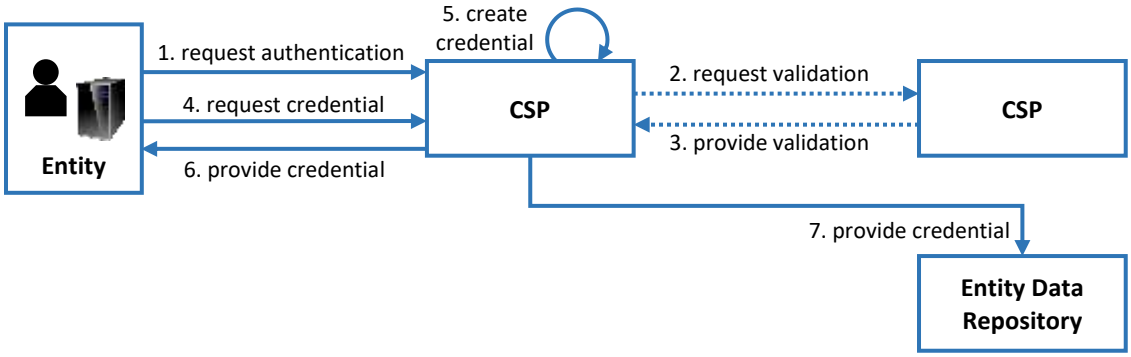


Figure 12 – Derived Credential Issuance (C1.2.1)

Credential Maintenance

It is the responsibility of the CSP to document credential maintenance support and data flows.

Credential Revocation

Figure 13 shows the process for revoking credentials. The approver may be the entity holding the credential, or may be another authorized entity. Once the CSP has verified that the approver is authorized, the CSP revokes the credential and notifies any connected entity data repositories that the credential has been revoked and should no longer be bound to the entity. CSPs are also responsible for providing revocation information to any requesting system, either through publication of a list of revoked credentials or though providing validity information upon request.

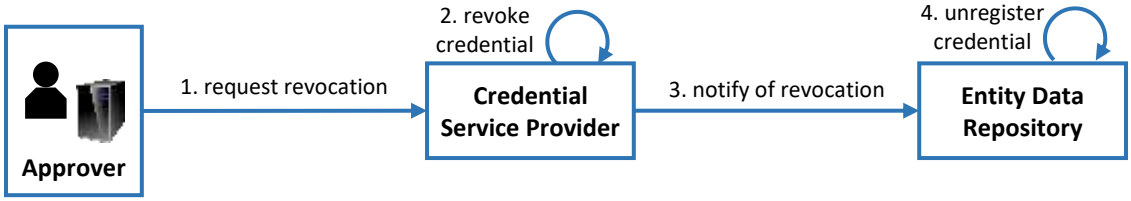


Figure 13 – Credential Revocation (C1.2.1)

3.1.2.2 External Credential Registration

Entities whose identity is managed outside of the DoD and who are issued credentials by external approved credential providers may be registered in an entity data repository in order to use their external credentials to authenticate for access to DoD resources that require provisioned access, or when DoD managed attributes are associated with the entity that are needed for resolving dynamic access policy rules. Credential registration is not required when all attributes needed for making dynamic access decisions are either contained within the credential or are provided by the federated mission partner at the time of access request through an assertion.

Registration may happen at an enterprise, DoD Component, COI, or local level, and may be performed prior to the access request or dynamically at runtime by an information system the first time access is requested. As shown in Figure 14, the entity data repository must validate that the credential presented by the entity was issued by an approved credential provider and that the credential is valid. If agreements for exchanging identity attributes exist between the external entity's identity manager and the entity data repository, the entity data repository may obtain and cache additional attributes about the entity at the time of registration. The attributes must be received as a normalized collection, or normalized internally, before acceptance and storage. The entity data repository must determine if the entity has already been registered and assigned an identifier, by checking internal to the entity data repository and by querying the identity manager to determine if a record of the entity exists there. If the entity has already been registered, then the entity data repository must map the new credential to the existing digital identity and identifier. If the entity has not been previously registered, the entity data repository must create a new digital identity and assign a new identifier. Identifiers assigned by the external identity manager should be used instead of assigning a new DoD only identifier when externally managed identifiers are persistent and will not create possible collisions.

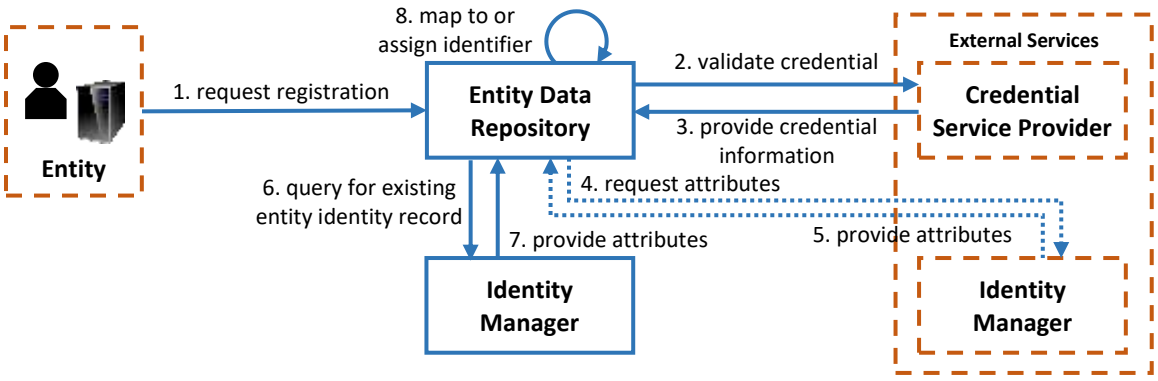


Figure 14 – Credential Registration (C1.2.2)

3.1.3. Access Management

This section addresses access management patterns, including establishing access rules for resources, provisioning entities with entitlements, authentication, and authorization. Different patterns may be implemented by different information systems and resources depending on the environment, capabilities, and needs of the information system hosting the resource. The services described in these patterns may be operated independently, or the capabilities may be combined. For example, a COI may operate a single service that acts as an entity data repository, IdP, and entitlement provisioning service.

3.1.3.1 Resource Access Management

Resource Access Management via Hosting Information System

Figure 15 shows the process for managing access to resources when access to resources is managed by an information system hosting the resource. The resource owner must identify the digital policy rule for accessing the resource and encode this rule in a digital-readable form in a resource policy service. When the resource is hosted by an information system, the policy rule is bound to an entitlement that is defined in the information system that meets the digital policy rule. If a new entitlement is defined, this new entitlement is uploaded to the entitlement provisioning service used by the information system. If the resource is only hosted by a single information system, the information system may act as the resource policy service.

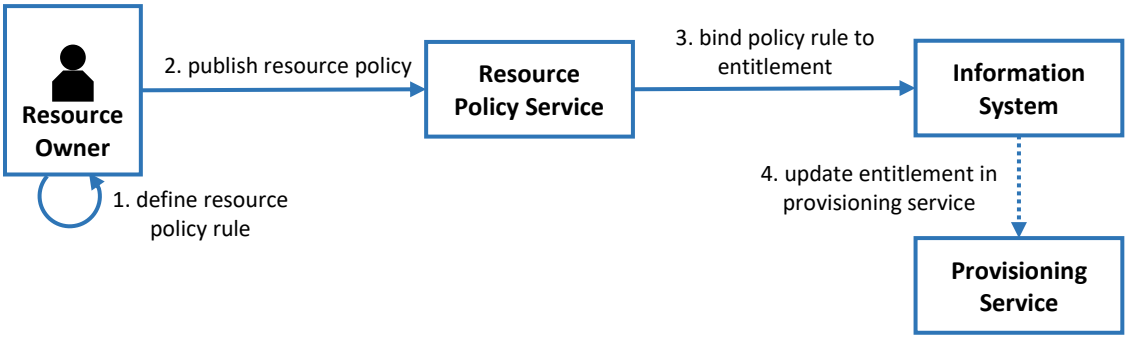


Figure 15 – Resource Access Management via Hosting Information System (C1.3.1)

Resource Access Management via Data Tagging

Figure 16 shows the process for managing resource access when the access policy is bound to the resource itself through data tagging. The resource owner must identify the digital policy rule for

accessing the resource and encode this rule in a digital-readable form in a resource policy service. The resource owner then binds the digital policy rule to the resource itself.

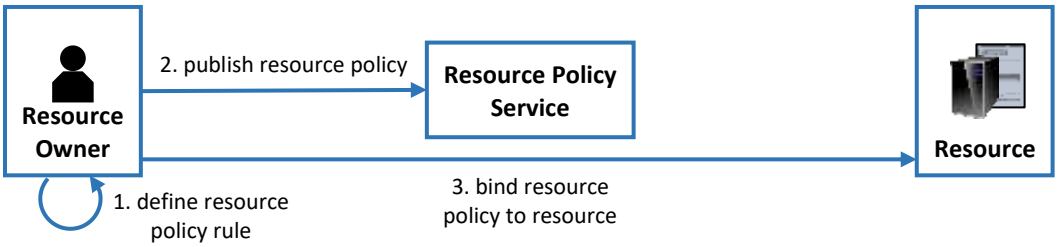


Figure 16 – Resource Access Management via Data Tagging (C1.3.1)

3.1.3.2 Provisioning

Manual Entitlement Provisioning

As shown in Figure 17, manual entitlement provisioning via Access Control Lists (ACL) or Role Based Access Control (RBAC) requires an approver to determine if the entity is authorized to access the resource. Entitlements may be requested by the entity or the hosting information system, or entitlements may be pre-approved by the approver without a specific request being made. The approver may be acting on a request to add the entitlement, or may be following an on-boarding or other process. If the entitlement is authorized, the approver adds the appropriate entitlement for the entity to the entitlement provisioning service to reflect the authorization. The entitlement provisioning service may then update the information system's local access control system to add the entitlement to the entity if the information system uses locally hosted entitlements and does not refer to the entitlement provisioning service at runtime. The entitlement provisioning service may also provide an updated attribute value to an attribute service that reflects the entitlement. For locally managed provisioning, the entitlement provisioning service may be the information system itself.

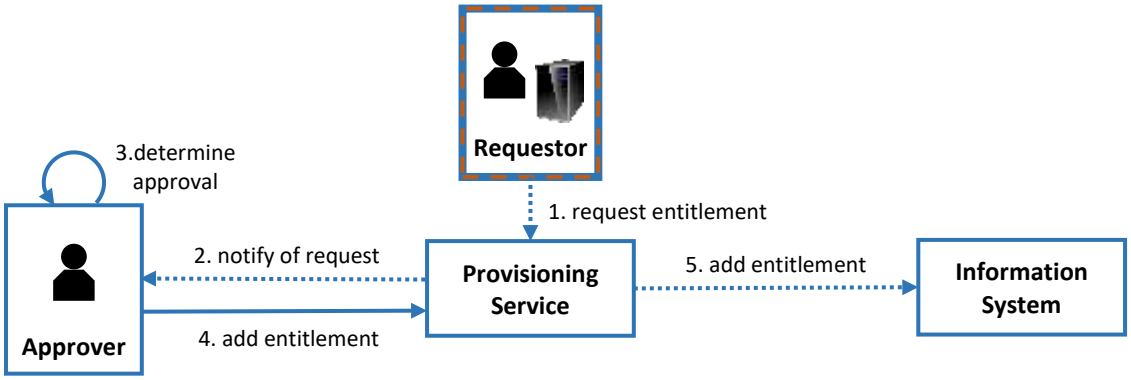


Figure 17 – Manual Provisioning (C1.3.2)

Manual entitlement provisioning is commonly used, but is labor intensive, especially for resources that have a large number of potential users. Manual entitlement provisioning can also result in inconsistent application of policy rules for access to resources, as these rules may not be formally defined or may only be understood by a single person.

Dynamic Entitlement Provisioning

Dynamic entitlement provisioning allows an entity or other requestor to be provisioned for access to a resource based on the digital policy rules governing access without requiring a manual approval,

provided that the entitlement provisioning service can determine that the entity possesses the appropriate attribute values as defined in the digital policy rule. As shown in Figure 18, the requestor asks for the entitlement. Note that for information systems leveraging ABAC, the requestor may be the information system itself. The entitlement provisioning service then obtains the appropriate digital policy rule for the resource, and obtains information about the entity from authorized sources, which may include the entity data repository and one or more attribute services. If the entitlement provisioning service is able to verify that the digital policy rule has been satisfied, then the entitlement provisioning service adds the entitlement for the requestor and may forward the entitlement update to the information system.

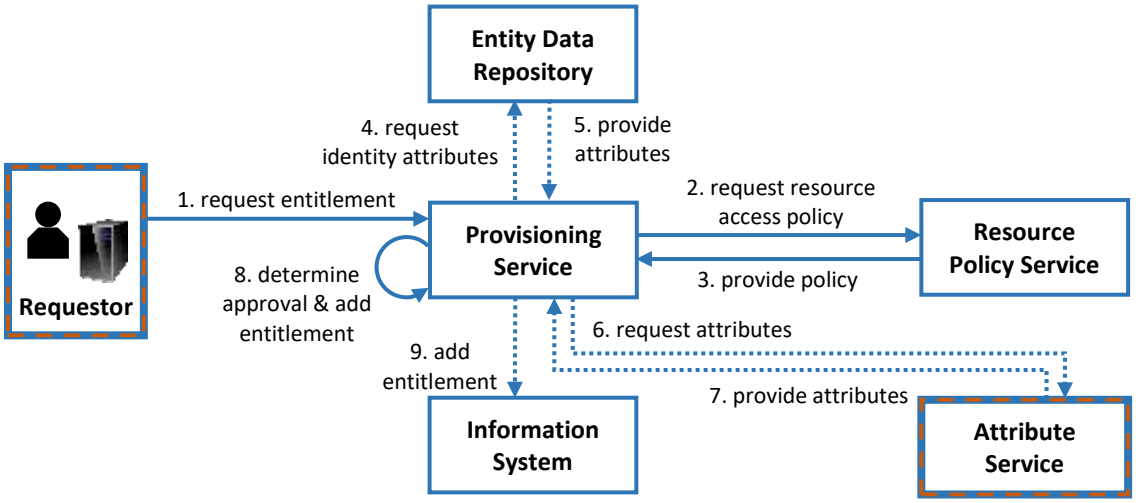


Figure 18 – Dynamic Provisioning (C1.3.2)

Dynamic entitlement provisioning can greatly reduce the time required to provision entitlements to users, especially for unanticipated users. However, dynamic de-provisioning must also be implemented so that users who no longer qualify for an entitlement are de-provisioned within an acceptable timeframe and do not maintain entitlements that they no longer need.

Hybrid Entitlement Provisioning

Hybrid entitlement provisioning uses a combination of dynamic attribute provisioning to partially determine if the entitlement can be granted but also requires manual approval steps in the workflow to fully determine if the entitlement should be provisioned.

Entitlement De-Provisioning

De-provisioning uses the same data flows as manual and dynamic provisioning (see Figure 17 and Figure 18) to remove entitlements from entities. When dynamic provisioning is used, the entitlement provisioning service should either run a periodic process to check for changes in attribute values that result in removing entitlements from entities, or the entitlement provisioning service should receive regular updates from attribute services, entity data repositories, and resource policy services and determine if any changes result in the need to de-provision entitlements.

3.1.3.3 Authentication

Direct Authentication

In direct authentication, as shown in Figure 19, the entity presents its authenticator to the information system. The information system validates that the authenticator was issued by the CSP, verifies the identifier in the credential, and determines that the credential has not expired or been revoked. If the credential does not contain a persistent unique identifier, the information system requests the identifier linked to the credential from the entity data repository. If the credential has been registered, the entity data repository provides the identifier. If the credential has not previously been registered, the entity data repository generates a new identifier and links it to the credential identifier. If the credential was issued by an internal CSP and the identifier is present in the credential, the information system does not need to query the entity data repository for the identifier.

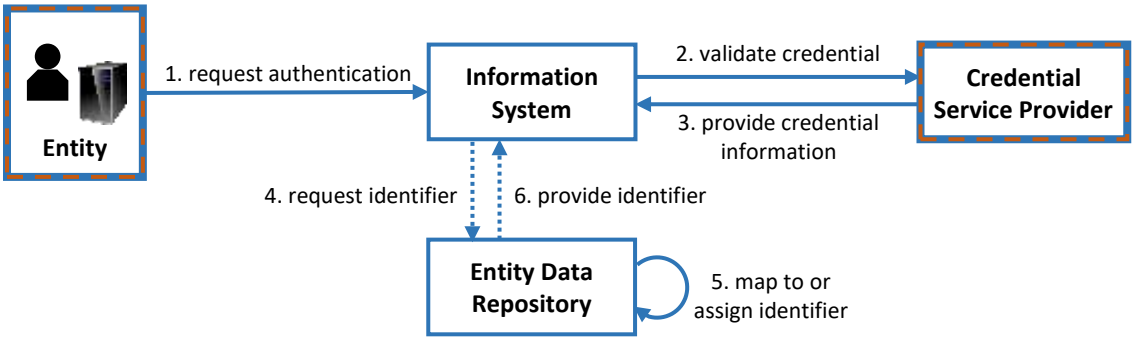


Figure 19 – Direct Authentication (C1.3.3)

Direct authentication provides the greatest resistance to attacks because the information system obtains credential validation information directly from the CSP. For PKI based authentication, validation is performed using artifacts that are digitally signed by the same Certificate Authority (CA) that issued the entity a credential. However, direct authentication is not practical in all cases. For example, direct authentication is only practical for non-PKI based authenticators if the information system locally issued the credential. Some information systems do not have interfaces that support direct authentication of PKI based credentials. Where approved authenticators include PKI based credentials from a number of different PKIs, or where multiple authenticators will be used, information systems may not correctly implement the complexity of performing direct authentication.

Direct authentication methods may be complicated if there is a need to inspect the contents of encrypted sessions. In those cases, the break and inspect process represents a reverse proxy IdP authentication where the intermediary system performing the inspection acts as the reverse proxy IdP.

Reverse Proxy IdP Authentication

Figure 20 shows authentication using a reverse proxy IdP. In this model, the reverse proxy IdP performs the authentication on behalf of the information system by validating that the authenticator was issued by the CSP, verifying the identifier in the credential, and determining that the credential has not expired or been revoked. If required, the IdP obtains the identifier from the entity data repository. The reverse proxy IdP then provides an assertion to the information system regarding the identity of the requesting entity, or the assertion may represent the reverse proxy IdP's own identity provided that the reverse proxy IdP maintains a log of the identifier of the authenticated entity. Assertions provided by reverse proxy IdPs may be configured using whatever format is needed by the information system, provided that the information system can only be accessed via the IdP.

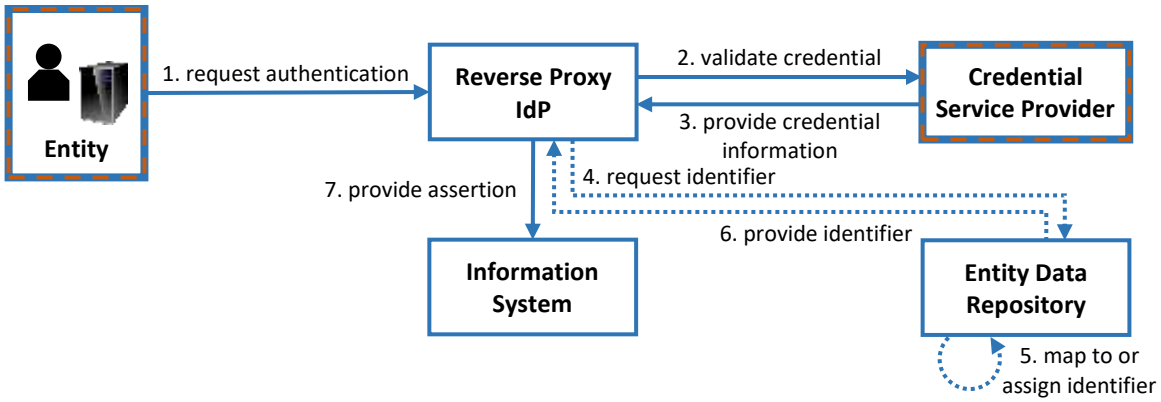


Figure 20 – Authentication using a Reverse Proxy IdP (C1.3.3)

Authentication using a reverse proxy IdP can be used to support a wide variety of mission needs. One primary use is to enable legacy systems built to outdated standards to meet modern authentication and authorization requirements. These IdPs must be configured to support whatever authentication and authorization is supported by the legacy system. Other uses of reverse proxy IdPs include enabling simplified sign-on to a group of systems that support a similar mission objective, or to support micro-segmentation in a ZT environment. When used to support needs other than legacy system support, reverse proxy IdPs must support standards based assertion formats.

Reverse proxy IdP authentication moves the complexity of performing authentication away from the information system to a dedicated service. The reverse proxy IdP adds an additional element to the authentication process because assertions are sent directly from the reverse proxy IdP to the information system. Because the information system only authenticates users via the IdP, this pattern is significantly more secure than authentication using a general purpose IdP. Use of a reverse proxy IdP can result in more consistent level of user access, less configuration maintenance, and fewer implementation errors.

IdP Authentication

Figure 20 shows authentication using an IdP. In this model, the information system initiates the request for authentication. The IdP performs the authentication on behalf of the information system by validating that the authenticator was issued by the CSP, verifying the identifier in the credential, and determining that the credential has not expired or been revoked. If required, the IdP obtains the identifier from the entity data repository. The external IdP then either provides the assertion directly to the entity, or provides a one-time artifact back to the entity that the entity provides to the information system which then requests the assertion from the IdP.

The assertion must contain the appropriate identifier for the entity, as well as the IAL and AAL for the authentication performed by the IdP which allows the information system to make its own determination regarding whether the authentication represents sufficient assurance in the identity of the entity. The assertion may also contain additional attributes which can be used by the information system in making access decisions.

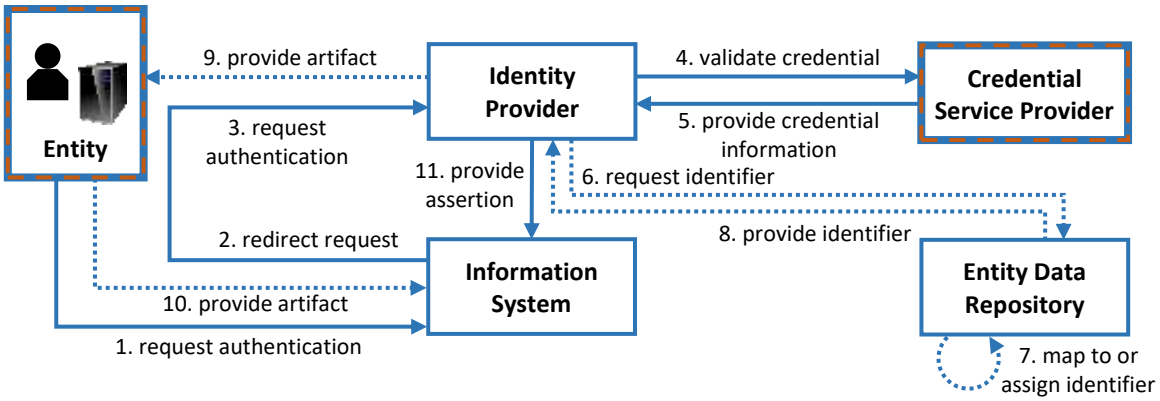


Figure 21 – Authentication using an IdP (C1.3.3)

When using IdP authentication, it is important to protect against replay attacks where an attacker hijacks the assertion and either replays it to the intended information system or presents it to a different information system to gain unauthorized access. Requiring holder of key validation in the assertion is the most secure mitigation approach, but may not be practical or supported by technology for all use cases. Other protections include timestamping the assertion, designating the intended recipient in the assertion, and encrypting the assertion with the intended recipient's public key. Providing the assertion directly to the information system as shown in this pattern also protects against replay attacks.

External IdP Authentication

Figure 22 shows the use of an external IdP. In this model, the entity authenticates to the external IdP, which validates the credential with the external CSP and obtains any relevant information. The external IdP then provides a one-time artifact back to the entity, passing the assertion by reference. The entity provides the artifact to the internal relying party, which uses the artifact to request the assertion from the external IdP. In the figure, the internal relying party is a reverse proxy IdP, but it could be an internal IdP or even a specific information system. Because the assertion is provided by an external IdP, the relying party may need to map the identifier contained in the assertion to the entity's internal identifier through the entity data repository.

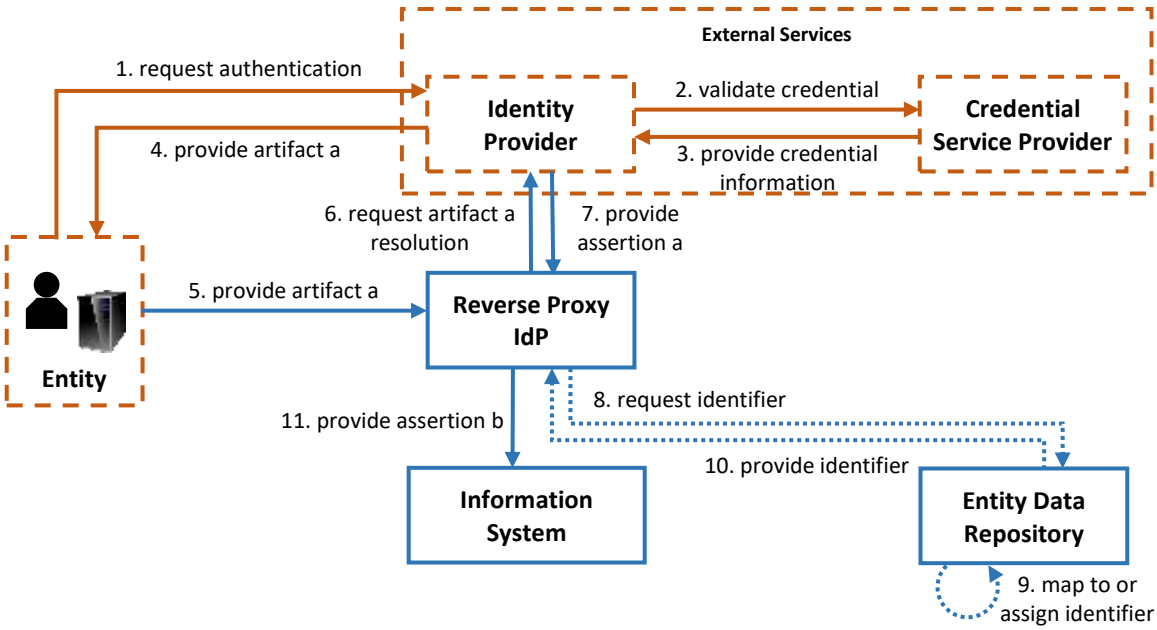


Figure 22 – Authentication of an External Entity using an External IdP (C1.3.3)

External IdP authentication presents similar security concerns to IdP authentication. The use of pass by reference results in the external IdP providing the assertion directly to the internal reverse proxy IdP via a secure channel instead of providing it through the entity, which mitigates assertion hijacking attacks.

3.1.3.4 Authorization

Direct Authorization

For provisioned access, once the information system has authenticated the requesting entity, the information system looks at provisioned entitlements to determine if the entity is entitled to access the resource as shown in Figure 23. The information system may host entitlements locally or may reach out to an entitlement provisioning service. If the entity is entitled to access the resource, the information system provides access to the resource.

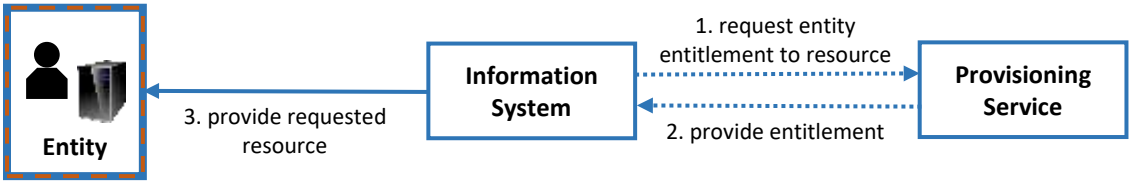


Figure 23 – Direct Authorization (C1.3.4)

Direct authorization, especially when entitlements are cached locally, provides the fastest response time for users who have already been provisioned with appropriate entitlements. Unanticipated users can only be accommodated by either providing the user with the information needed to be manually provisioned for access, or by requesting dynamic provisioning where that service is available.

Reverse Proxy IdP Authorization

Generally, information systems manage authorization decisions directly. However, reverse proxy IdPs may perform authorization decisions on behalf of information systems hosted behind the reverse proxy IdP. In this model, as shown in Figure 24, the reverse proxy IdP determines if the entity is authorized to

access the resource. If so, the reverse proxy IdP requests the resource and provides access to the resource to the entity.

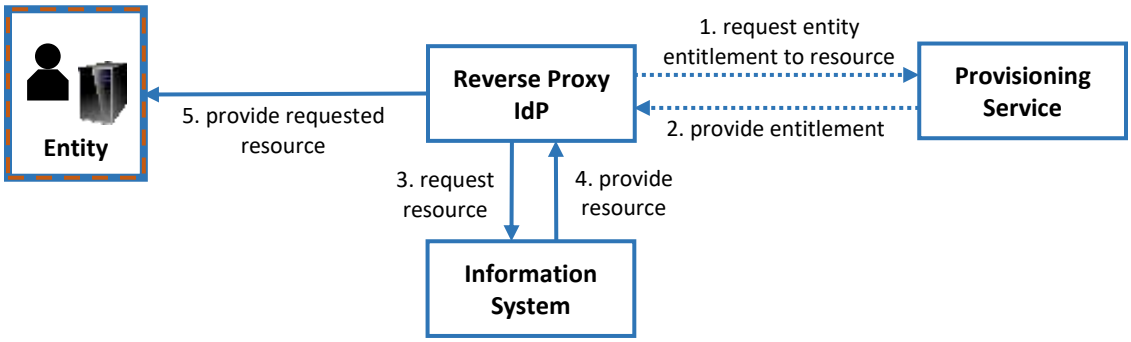


Figure 24 – Authorization using Reverse Proxy IdP (C1.3.4)

Reverse proxy IdP authorization is recommended where information systems lack the ability to support local direct authorization, or where authorization information is centrally managed for a group of information systems.

Dynamic Access

Access to some resources is provided through dynamic access instead of provisioned access. This model is also called ABAC. In the dynamic access model, shown in Figure 25, users are not provisioned for access. Instead, each time an entity requests access to a resource the information system refers the identifier of the authenticated entity to a policy enforcement point. Alternatively, the policy enforcement point may initiate the request. The policy enforcement point leverages a policy decision point. The policy decision point first identifies the digital policy rule governing access to the resource, then requests attributes from the entity data repository and one or more attribute services. The policy decision point compares the attribute values to the policy requirements to determine if the entity is authorized to access the resource. If the policy decision point is not able to identify attribute values or if the attribute values do not meet the policy rule, then access is not granted. The policy decision point provides the authorization decision to the policy enforcement point, which forwards it to the information system. The information system then provides access to the resource if authorized, or provides the resource to the policy enforcement point which then provides it to the entity.

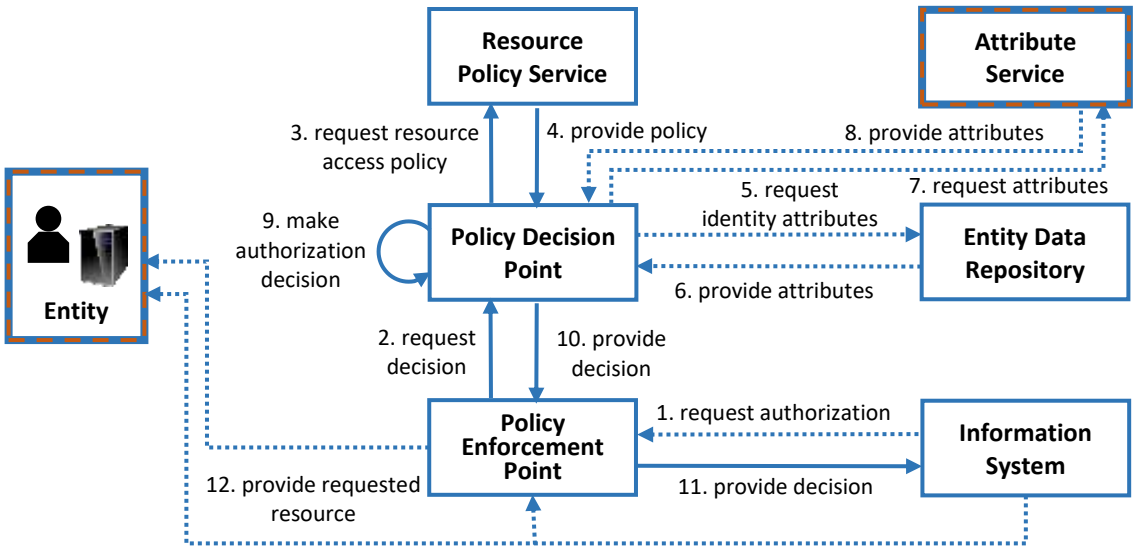


Figure 25 – Dynamic Access using ABAC (C1.3.4)

Dynamic access is well suited for environments with a large number of users, especially when accessing information resources. Because access is always determined real-time, there is no requirement for provisioning or de-provisioning. However, dynamic access can introduce delays in the authorization process if network connectivity is insufficient to support all of the data collection and data exchange steps. Dynamic access is also not recommended for access to resources that require managing licensing, or for resources that require the ability to audit who can access the resource, not just who has accessed the resource.

3.2. Access Accountability Capabilities

This section addresses access accountability capabilities including log collection and consolidation, access review, and identity resolution.

3.2.1. Log Collection and Consolidation

As shown in Figure 26, each information system or ICAM service creates ICAM event logs. These logs are then consolidated by a log management system and compared against provisioned entitlements or resource access policies for each entity. This consolidated log information can then be reviewed by an authorized reviewer for anomalous activity or provided to an authorized monitoring service.

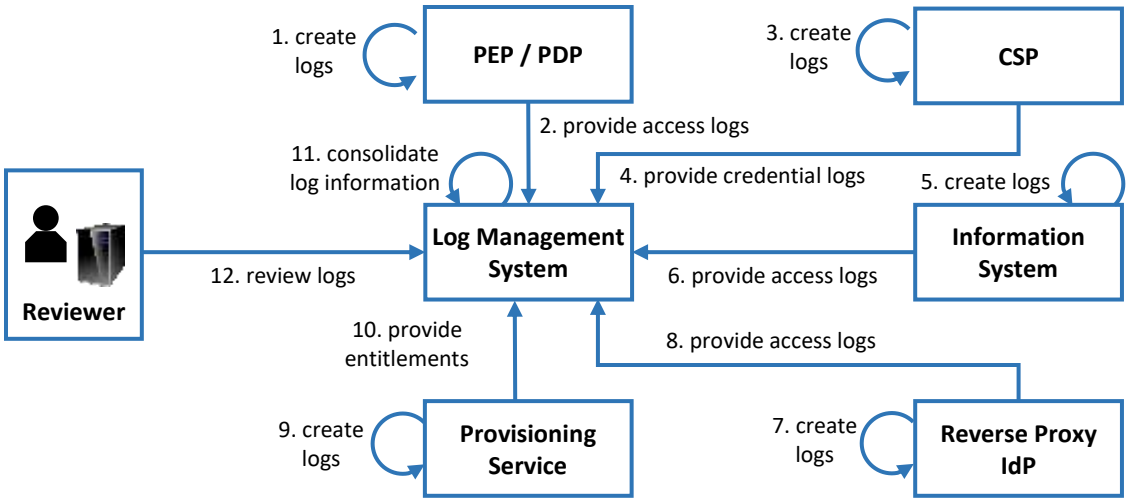


Figure 26 – Log Collection and Consolidation (C2.1)

3.2.2. Access Review

Person Entity Centric Access Review

The steps required to perform an access review as shown in Figure 27 can be grouped into four primary phases. The first phase requires identifying who is responsible for performing the access review for each entity (step 1). This phase should be performed using organization information contained in identity managers for both person entities and NPEs. The second phase requires collecting all information about each entity's access rights into a single location (steps 3-6). Access rights may be hosted in entitlement provisioning services or may be based on digital policy rules that rely on attributes hosted by attribute services. Access rights may also be hosted in information systems that are performing provisioning locally. In this case, the information system is acting as an entitlement provisioning service. Access information may also be collected from other systems such as User and Entity Based Analytics (UEBA) tools. Once information has been collected into a master user record, a report is generated for each manager or sponsor (step 7). Finally, the manager or sponsor reviews the entitlements listed in the report. If any entitlements or attributes are incorrect, the manager must use the processes described in Sections 3.1.1.1 and 3.1.3.2 to update provisioned entitlements and attributes as appropriate. At the COI level, if a single entitlement provisioning service is used to manage entitlements for all information systems within the COI, a separate master user record service is not required, as the entitlement provisioning service can provide all information required to perform access reviews, including connectivity to attribute services used to support provisioning.

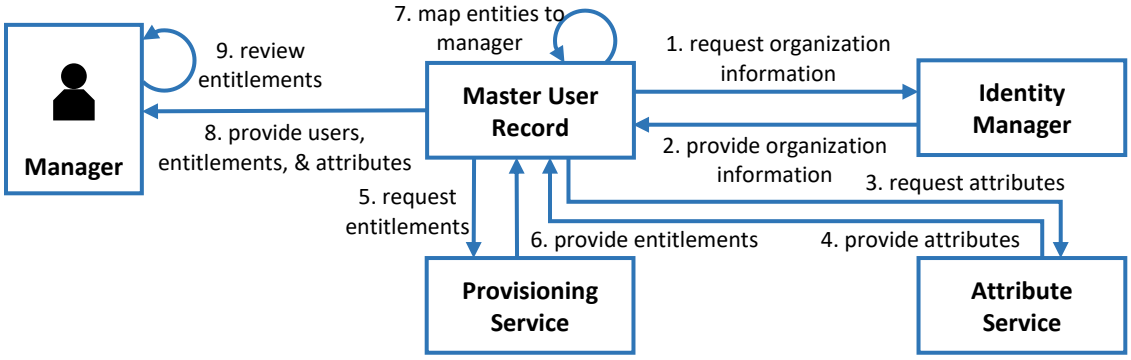


Figure 27 – Person Entity Centric Access Review (C2.2)

Full access reviews are not practical at the DoD enterprise level, as there will be locally stored attributes and entitlements. For COIs where access review is needed, the COI must implement processes to ensure that all attributes are reported to the appropriate master user record.

Resource Centric Access Review

Access reviews may also be performed at an information system level. The reviewer obtains the list of users and entitlements from the information system, and should also retrieve the list of users and entitlements from any provisioning system used to provision entitlements for the information system. As part of the access review, these two lists are first reconciled. Then the reviewer verifies entitlements, with specific focus on IT privileged user and functional privileged user access. . If any entitlements or attributes are incorrect, the reviewer must use the processes described in Sections 3.1.1.1 and 3.1.3.2 to update provisioned entitlements and attributes as appropriate.

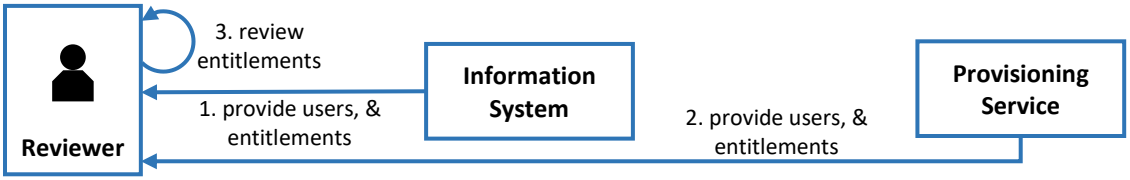


Figure 28 – Resource Centric Access Review

NPE Centric Access Review

Many NPEs authenticate to other NPEs in order to perform their functions. These access privileges should also be reviewed to ensure that NPEs do not have access to information systems they no longer need access to. In addition, when an NPE is decommissioned, any entitlements provisioned to that NPE must also be removed. Similar to person entity access reviews, the NPE sponsor obtains information about the NPE from the entity data repository where it is registered, and from the master user record which contains information regarding what entitlements are provisioned to the NPE. The sponsor reviews the attributes and provisioned entitlements and updates any information using the processes described in Sections 3.1.1.2 and 3.1.3.2.

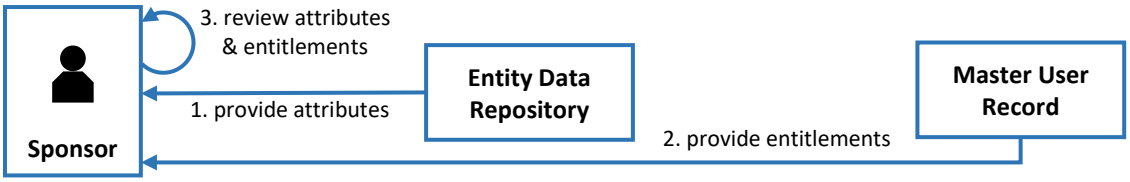


Figure 29 – NPE Centric Access Review

3.2.3. Identity Resolution

Figure 30 shows the process of performing identity resolution. Entity data repositories and attribute services should periodically review registered digital identities and flag those that cross a pre-determined threshold for similarities. For example, if two different digital identities have registered credentials with the same or very similar names, and share other identity attributes, there is a possibility that those two digital identities map to the same real-world entity. These services should alert a reviewer who can analyze the two records and determine if they do map to the same real-world entity. If so, the reviewer will update the entity data repository to map the two digital identifiers to each other to create a single digital identity. This process may also be used to evaluate digital identities from more

than one entity data repository, such as if a COI level data repository is being elevated to an enterprise level.

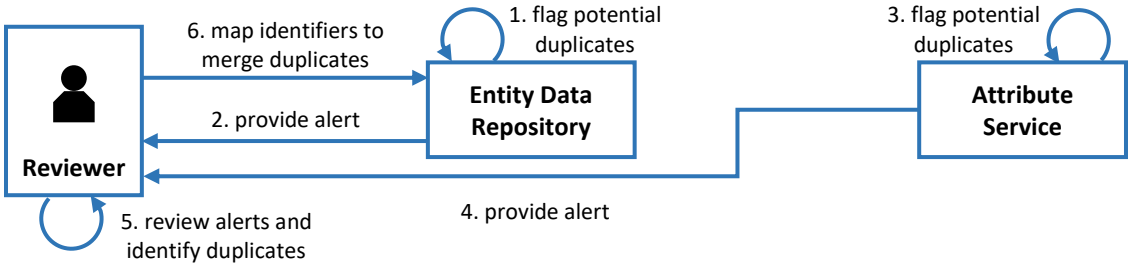


Figure 30 – Identity Resolution (C2.3)

3.3. Contact Data Capabilities

Supporting contact data lookup requires the collection of contact data into a single repository or virtual repository and providing search capabilities for entities to obtain contact data from that repository. The contact data repository may contain all of the necessary information (i.e., is may have been previously populated) or may need to dynamically request the information from the identity manager, attribute service or entity data repository. Figure 31 illustrates the steps for collecting contact data into a searchable repository (steps 1-7) and the process for requesting contact data (steps 8-9). The repository must collate contact data from one or more data sources for each entity that is included. The repository may support lookup information for a DoD Component, for a COI, or for the entire enterprise of DoD internal users. Data sources for contact data may themselves be internal to the DoD, or the repository may have agreements and technical interconnections in place to host contact data provided by external services. Generally, contact data attributes will be found in identity managers, but additional attributes may be collected from the entity data repository or from one or more attribute services. Attributes are linked by a common identifier for each entity.

When an entity requests contact data, that entity may not know the common identifier, so Contact Data Capabilities should provide a search interface that allows for searching on multiple attributes, such as name or organizational affiliation.

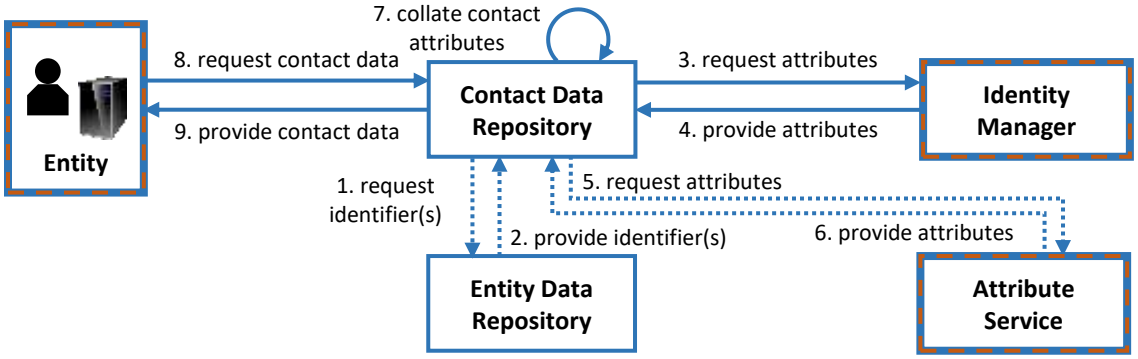


Figure 31 – Contact Data Collection and Lookup (C3.1, C3.2)

Because many contact data elements are considered PII, access to contact data must therefore be protected. Contact data repositories must have appropriate agreements in place with data sources for the collection and intended dissemination of the data. In addition, entities requesting access to contact data must be authenticated and authorized to obtain contact data from the repository.

4. ICAM Patterns and Associated Use Cases

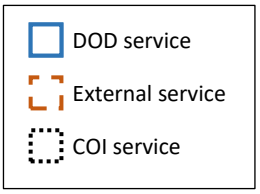
This section describes patterns for ICAM capabilities. These patterns represent Service View (SvcV)-2 resource flow descriptions. These patterns and their related use cases are intended to demonstrate how capabilities may be implemented to meet a broad set of mission and other needs. They are not intended to be prescriptive for how a given information system consumes ICAM capabilities, nor are they intended to describe all possible ICAM use cases.

Use cases have been organized around four capability areas. Identity management and credential management are combined, as these actions are generally performed together for entities who are registered prior to requesting access to resources. Access management use cases focus on the real-time activities of an entity requesting a resource, and include use cases for pre-registered entities as well as dynamic access for unanticipated entities. Use cases for access accountability and for contact data are also included.

4.1. Identity and Credential Patterns

These use cases describe patterns for registering users in advance. User registration is needed if attributes specific to the user will be managed by DoD or if entitlements need to be provisioned specific to the user. User registration for mission partner entities may not be required if attributes used in access decisions for the user will be provided via assertions from the user's IdP.

Depending on the type of user and the use case, identity management may be performed by the DoD or by a DoD mission partner prior to the issuance of a credential. In other use cases, entities may be issued credentials based on minimal or no prior identity management activities. Additional attributes for registered users may also be managed with the DoD or by DoD mission partners.



As shown in the box to the left, services operated internal to the DoD are shown in blue, services operated externally to the DoD are shown in brown with a dashed line, and services operated by a COI are shown in black with a dotted line.

4.1.1. Unclassified Enterprise DoD Internal Initial Registration

Pattern:

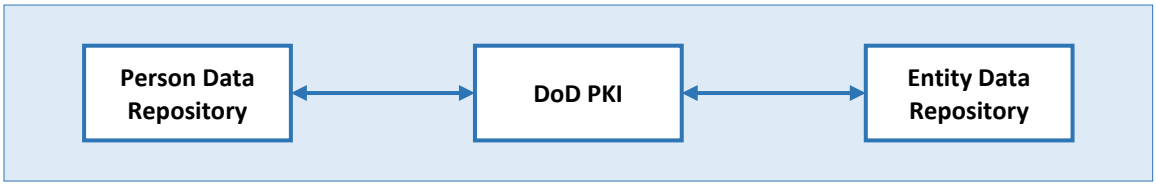


Figure 32 – Unclassified DoD Internal Initial Registration

Registration of internal entities includes collecting and verifying identity information about the entity, creating a digital identity for that entity, and issuing credentials to the entity. The pattern includes the following four steps:

- New entities must be sponsored. For new military and civilian employees, the sponsorship is through the Component that is initiating the employment. For contractors, the sponsorship is through the contracting organization. For NPEs, sponsorship is the person or organization that is responsible for the NPE. The sponsor initiates the on-boarding pattern and facilitates completion of on-boarding steps.

- Once an entity is sponsored, information about the entity must be verified and entered into appropriate identity management systems. For person entities, the verification pattern includes appropriate background investigation activities. Creation of the new digital identity also involves assigning an identifier to that identity. For person entities, the identifier is usually the EDIPI along with the appropriate PTC. If the new user already had an EDIPI assigned, the existing EDIPI will be used. Otherwise, a new EDIPI will be assigned by the PDR. Person entities are also assigned a PDN, which is a human readable name used to support contact data lookup capabilities.
- The third step in onboarding is the issuance of one or more credentials to the entity. Person entities provide proof of their identity and are issued a CAC which contains digital certificates issued by the DoD PKI. NPEs are issued one or more digital certificates by the DoD PKI based on identity verification of their sponsor.
- Finally, the entity must be provisioned for appropriate physical and logical access by linking authorization attributes to the entity based on its identifier, and by provisioning entitlements to the entity.

Use Cases:

4.1.1(a) A new DoD internal person entity reports for duty, and is Identity proofed, credentialed, and registered.

4.1.1(b) A new NPE with an intended long term existence that requires an identity valid across the DoD enterprise (such as a web server hosted in a traditional data center) is brought online.

4.1.1(c) A new NPE with an intended limited duration that requires and identity valid across the DoD enterprise (such as a cloud-based web server) is brought online.

Gaps:

For person entities, basic identity management and credentialing processes are mature, leveraging Component on-boarding of identity information, assignment of an EDIPI and EDIPI+PTC through the PDR, assignment of an Enterprise Name and Enterprise Name+PTC, and the issuance of a CAC with digital certificates from the DoD PKI that contain the Enterprise Name and Enterprise Name+PTC. However, processes to provision attributes and entitlements beyond core identity attributes are decentralized and manual, and the attributes and values are not normalized across the Components.

As DoD adopts SaaS, provisioning person entities to those SaaS is becoming a critical gap.

For NPEs, manual processes exist to issue credentials from the DoD PKI. However, enterprise registration and naming capabilities are lacking. Fully automated processes for NPEs are also lacking.

The Entity Data Repository (EDR) does not currently exist.

4.1.2. Unclassified Enterprise Mission Partner Entity Registration

Pattern:

Figure 33 – Unclassified Mission Partner Entity Registration

For this pattern, mission partner entity identities are created and managed externally to the DoD, and the mission partner entity is provided with a credential from a DoD approved external credential provider. For some mission partners, such as Federal Agencies and some Defense Industrial Base (DIB) companies, limited attributes for the use may be made available to the DoD through an attribute exchange process. Other attributes for registered mission partner entities may be managed internally by the DoD enterprise or by DoD COI attribute stores. To support attribute and entitlement management, these entities must be assigned a persistent DoD identifier which can be linked to their credential and accessed by DoD relying parties. The pattern includes the following three steps:

- Prior to accepting externally issued credentials, the DoD must establish a trust relationship with the external credential provider or identity manager. As part of this relationship, the DoD and the external provider define the type(s) of credentials that will be accepted, what identifiers are used in those credentials, what, if any, additional attributes will be made available, and what the process is for requesting and obtaining additional attributes. As part of the trust establishment process, the external provider may pre-register existing users with the DoD to facilitate these users obtaining access to DoD resources.
- When a mission partner entity with an approved credential requests registration, the DoD validates the presented credential and determines if the credential has been pre-registered. If not, the DoD assigns a persistent identifier to the user and links the credential to the identifier. For some users, such as Federal Agency mission partner entities whose certificates contain a federally recognized unique identifier, the DoD may assign the identifier contained in the credential as that user's DoD identifier. If there is no globally unique identifier contained in the credential, the DoD will generate a new identifier and link it to the credential.
- Once an entity has been registered, the entity may be provisioned for appropriate physical and logical access by linking authorization attributes to the entity based on its identifier, and by provisioning entitlements to the entity.

Use Cases:

4.1.2(a) One or more DoD relying parties have identified a requirement to interact with entities from one or more Federal Agencies. These entities have been issued PIV cards by their agency.

4.1.2(b) An individual from a Federal Agency who has been provisioned with a PIV card by their agency has identified a need to access a DoD resource.

4.1.2(c) One or more DoD relying parties have identified a requirement to interact with entities from a DIB partner that issues DoD approved credentials to its employees and affiliates.

4.1.2(d) A DoD mission partner entity with a DoD approved credential has identified a need to access a DoD resource.

Gaps:

The DoD does not have an enterprise registration capability for mission partner entities that have DoD approved external credentials. Some relying party information systems support local registration of mission partner entities. Others do not support registration of mission partner entity credentials and deny mission partner entities access or require mission partner person entities to obtain CACs in order to gain access.

Some DoD resources use the DoD issued EDIPI as the durable unique identifier for person entities. Because mission partner entities with externally issued credentials, including other Federal agencies and the DIB, do not have EDIPIs associated with their external identities, they are unable to access these resources.

4.1.3. Community of Interest User Registration

Pattern:

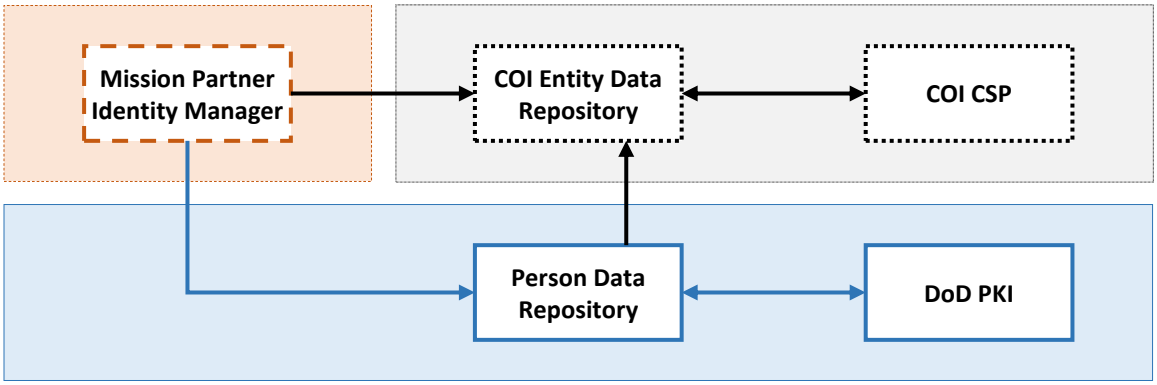


Figure 34 – COI User Registration

Supporting all users in this environment requires the implementation of a COI IdP to support all relying parties within the COI that supports four types of users:

- DoD Internal users with DoD issued PKI certificate use these certificates with the EDIPI identifiers contained in their certificates within the COI. The COI data repository obtains information about these users from the DoD enterprise Person Data Repository. Certificate status is verified either by periodically obtaining and caching Certificate Revocation Lists (CRL) from the DoD PKI, by using the real time certificate validation service using Online Certificate Status Protocol (OCSP) service from the DoD PKI, or by using a COI operated OCSP service that provides certificate revocation status information for the DoD PKI.
- Mission partner entities with certificates from DoD approved external PKIs who have been registered at the DoD enterprise level use their certificates and the DoD enterprise identifiers that have been assigned at registration. The COI data repository obtains information about these users from the DoD enterprise Person Data Repository. Certificate status is verified either by periodically obtaining and caching CRLs from the external PKI, using an external PKI OCSP service, or by using a COI operated OCSP service that provides certificate revocation status information for the DoD approved external PKIs.

- Unanticipated mission partner entities with certificates from DoD approved external PKIs who have not been registered at the DoD enterprise level use their certificates. These users are registered upon their first authentication by the COI data repository. The full distinguished name in the certificate can be used as a COI identifier. Relevant attributes from the PKI certificates are persisted with the registration. Certificate status is verified either by periodically obtaining and caching CRLs from the external PKI, using an external PKI OCSP service, or by using a COI operated OCSP service that provides certificate revocation status information for the DoD approved external PKIs.
- Mission partner entities without certificates issued by DoD approved external PKIs or COI participants whose identity information is not available as a result of lack of network connectivity are provided credentials by a COI CSP. These credentials are limited for use within the COI. The authorizing official for the COI must approve the identity proofing processes and credential authenticators used and how those authenticators will be validated, based on the sensitivity of resources available to the network and the operational needs of the COI environment.

Use Cases:

4.1.3(a) The DoD is operating an unclassified network to support a coalition exercise. DoD members of the coalition have CACs with digital certificates issued by the DoD PKI. Some coalition partners also have hardware based PKI credentials issued by DoD approved external PKIs. Other coalition partners do not have credentials they can use within the coalition and must be issued new credentials. The coalition network has limited connectivity to the DoDIN.

4.1.3(b) A DoD unit is operating at the tactical edge with intermittent or limited connectivity to the DoDIN. DoD enterprise ICAM information for person entities can be periodically downloaded to the tactical environment, but local credentials must be supported for local NPEs and for users who join the community while connectivity to the DoD enterprise is not available.

Gaps:

This use case does not depend solely on DoD enterprise ICAM services. DoD enterprise ICAM services for identity management and credential issuance to DoD internal users are mature, see 4.1.1. Some COIs have implemented the capability to issue local credentials, but may not be following consistent standards for identity lifecycle management. Acceptance of mission partner credentials by COIs is limited.

Closed Restricted Networks and Standalone Systems/Networks offer significant challenges because there is (by design) no access to enterprise capabilities.

4.1.4. Community of Interest Person Entity Identity Provider Registration

Pattern:

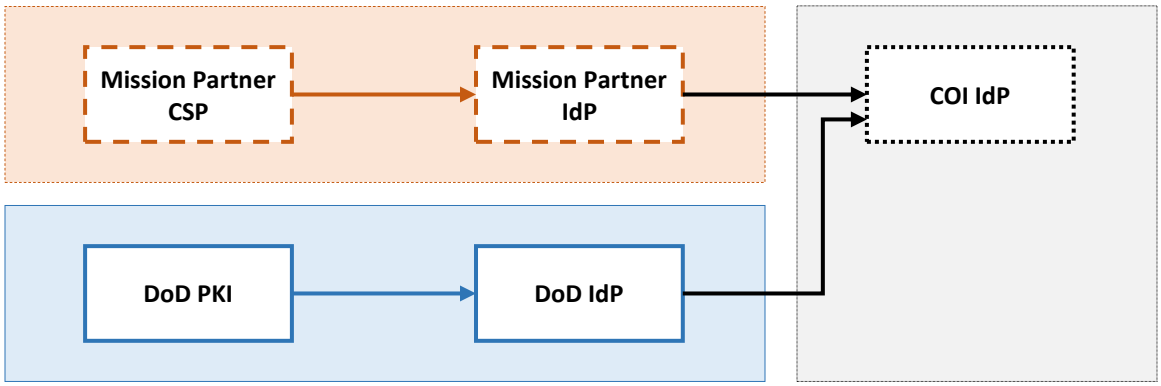


Figure 35 – COI IdP Registration

The previous use cases all involve registration of the end entity users. For this use case, users are registered within their own network, but are not registered with the COI. Instead, the public keys for each IdP operated by each mission partner participating in the information exchange are registered using an out-of-band mechanism such as manual in-person transfer. Once the COI registers the IdPs, relying parties within the COI can validate assertions from the IdPs and leverage information contained in the assertions to make access decisions. Although not shown in the figure, assertions provided by the mission partner or DoD IdPs can also include additional attributes needed by the COI.

Use Cases:

4.1.4(a) A Secret//Releasable COI is formed to share information among the DoD and coalition mission partners. All resources within the COI are labeled for releasability by country and possibly additional attributes such as mission name or user role, but not specifically by user.

4.1.4(b) Digital policy rules for access to resources are established such that access is governed based on the organization requesting the resource, such as a Federal Agency or DIB partner.

4.1.4(c) Digital policy rules for access to resources are established such that access is governed based on the organization requesting the resource and the value of attributes asserted by the user's organization.

Gaps:

Currently, the DoD does not provide an enterprise IdP capability. Some mission partners have implemented IdPs, but others do not support this capability. As a result, the COI would need to implement a COI IdP for validating credentials for DoD and mission partner entities that do not yet operate an IdP that allows users to authenticate at their home organization. A COI operated IdP can provide organization information based on the credentials being validated, but the COI IdP would not be able to provide user attributes beyond those asserted in the user credentials.

Many relying party information systems are not configured to securely process authentication assertions in lieu of performing direct credential validation. Addressing the gaps in this use case requires modifying relying party authentication behavior in addition to registration capabilities.

4.1.5. Secret Enterprise Registration for DoD and Federal Agencies

Pattern:

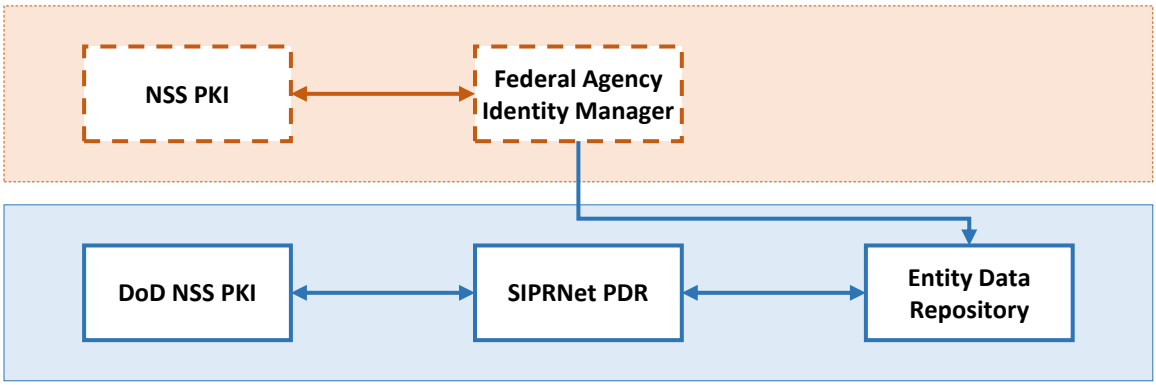


Figure 36 – Secret Network Initial Registration

Identity data for most DoD person entities is managed in the NIPRNet PDR and then a subset of that data is uploaded to the SIPRNet PDR. Users with SIPRNet accounts can obtain credentials from the DoD portion of the NSS PKI. NPEs can also obtain credentials from the DoD NSS PKI.

The NSS PKI also supports the issuance of certificates to Federal Agency mission partner entities. All certificates issued by the NSS PKI contain unique full distinguished names which can be used as identifiers by DoD relying parties. Most of these Federal Agencies obtain their credentials from the Common Service Provider operated by the DoD. Identity management for these users is performed internal to their agencies.

Contractors and other person entities who are provisioned accounts on US Secret Networks can obtain credentials from the NSS PKI but must be sponsored by a Federal Agency.

Use Cases:

4.1.5(a) A DoD internal person entity requires access to resources hosted on SIPRNet

4.1.5(b) A new NPE with an intended long term existence that requires an identity valid across the DoD enterprise (such as a web server hosted in a traditional data center) is brought online on the SIPRNet

4.1.5(c) A new NPE with an intended limited duration that requires and identity valid across the DoD enterprise (such as a cloud-based web server) is brought online on the SIPRNet

4.1.5(d) A Federal Agency person entity or NPE requires access to DoD resources on the SIPRNet. The entity has already been provided with a certificate issued by the NSS PKI.

Gaps:

For person entities, basic identity management and credentialing processes are mature, leveraging a data transfer for person entities registered in the NIPRNet PDR to maintain the same identifier in the SIPRNet PDR and their DoD NSS PKI credentials. Manual processes are available for registering DoD internal users who are not in the NIPRNet PDR but require credentials on SIPRNet. However, processes to provision attributes and entitlements beyond core identity attributes are decentralized and often manual.

For NPEs, manual processes exist to issue credentials from the DoD NSS PKI. However, enterprise registration and naming capabilities are lacking. Fully automated processes for NPEs are also lacking.

For Federal Agency partners, processes are in place to provision them with certificates from the NSS PKI. Because the NSS PKI is a single infrastructure with a single Root CA, validation of certificates can be performed, and all certificates contain a unique full distinguished name which can be used as a unique identifier. However, the DoD does not have an enterprise ICAM service for registering non-DoD users. Also, many DoD relying parties have chosen to use the EDIPI as the identifier, which results in a lack of interoperability with non-DoD Federal Agency users as the EDIPI is only used within the DoD internal community. Processes for sharing attributes beyond those asserted in NSS PKI certificates are also lacking.

4.1.6. Secret Enterprise Registration for Non-Federal Agency Mission Partner Entities

Pattern:

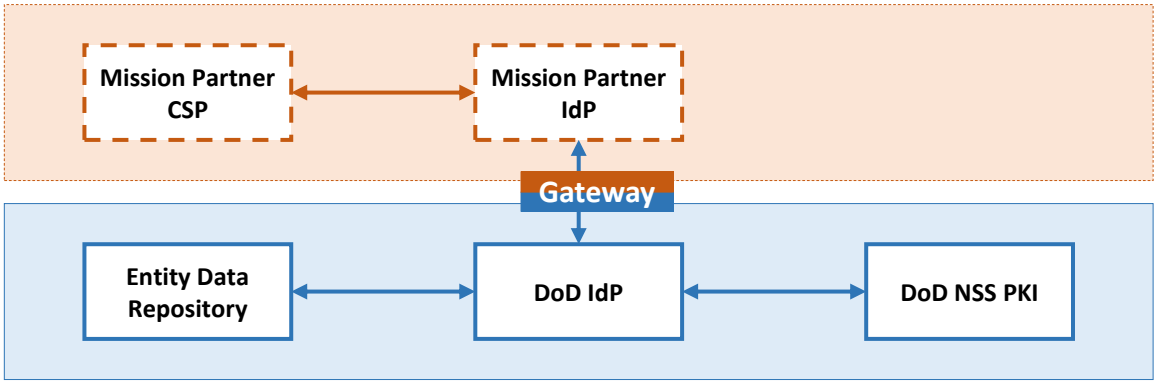


Figure 37 – Secret Registration for Mission Partners

This pattern requires that person entities and NPEs are registered within their own network. Entities may or may not be registered within the DoD Secret network.

The public keys for each IdP operated by each mission partner participating in the information exchange are registered with the Mission Partner Gateway using an out-of-band mechanism such as manual in-person transfer. These public keys are needed to be able to validate assertions provided by the IdPs. In addition, each IdP asserts identifiers for users that it validates that are unique both within the mission partner's network and with the DoD network. Format of these identifiers must be defined as part of the agreement established between the mission partner and the DoD for information exchange.

The gateway verifies the signature on the assertion, and then passes the information in the assertion through the gateway so that it can be re-signed using a private key associated with a digital certificate issued by the DoD NSS PKI or another DoD approved PKI on the DoD side of the gateway. For users who only require access to resources that are authorized based on the country of origin attribute or other attributes that are included in the assertion, no additional attributes are required.

Users who require access to resources that are authorized based on additional attribute information hosted by the DoD must be registered using their identifier with the DoD Entity Data Repository. Attributes may also be included in assertions from the Mission Partner IdP through Gateways and cross domain devices, constrained by trust agreements. Additional attributes or entitlements can then be provisioned to that user.

Use Cases:

4.1.6(a) A DoD Combined Communication Electronics Board (CCEB) mission partner person entity or NPE requires access to resources hosted on a DoD Secret network. The CCEB mission partner entity has been identity proofed by the mission partner and has been issued a credential that is valid on the mission partner's Secret network. The mission partner network has connectivity to the DoD Secret network through an approved Mission Partner Gateway.

4.1.6(b) An IC mission partner person entity or NPE requires access to resources hosted on a DoD Secret network. The IC mission partner entity has been identity proofed and issued a credential on the JWICS network. JWICS has connectivity to the DoD Secret network through an approved Cross Domain Solution (CDS) gateway.

4.1.6(c) A Combatant Command mission partner person entity or NPE requires access to resources hosted on a Combatant Command mission partner Secret Releasable network. The Combatant Command mission partner entity has been identity proofed and issued a credential on their national Secret Releasable mission partner network. The mission partner national Secret Releasable network has connectivity to the Combatant Command Secret Releasable network through an approved Mission Partner Gateway.

Gaps:

Currently, the DoD does not provide an enterprise ICAM capability for an IdP. Some mission partners have implemented IdPs, but others do not support this capability.

Gateway functionality is also limited and may not support the verification of assertions, recreation of the assertion, or digital signing of the recreated assertion.

Because many relying party information systems are not configured to securely process authentication assertions in lieu of performing direct credential validation, ICAM services have been deployed that create a new PKI digital certificate for the mission partner entity that can be presented to the relying party. Migrating to assertion based authentication can eliminate the need for operating CAs at the boundary while still maintaining attribution of who requested the resource and supporting the need to inspect information as it crosses the boundary.

4.1.7. Short-Lived NPE Registration

Pattern:

Figure 38 – Cloud Elasticity Registration

Generally, registration of an entity occurs where there is a need for a long-term recognition of that entity. This pattern is for when one or more short lived entities need to be credentialed in a short period of time and then only exist for a limited time period. The pattern depicted here takes place after the requirements in section 3.1.1.2 have been met.

A requesting service generates key pairs and certificate requests and submits the requests to the CSP. The CSP issues certificates and returns them to the requesting service in a fully automated fashion with little to no time delay. The requesting service then deploys the private keys and certificates to the new short-lived entities for use. When the new entities reach end of life, the requesting service notifies the CSP to revoke the credentials. The CSP can also limit the validity period of the certificates to reduce CRL size. The requesting service must submit a new request prior to the expiration date of the current certificates.

Use Cases:

4.1.7(a) A cloud based application needs to stand up 10,000 instances to process data in response to a real-world event. Each instance requires 5 PKI key-pairs including signed certificates. After 3 days of operations, the processing is complete, these instances are all decommissioned.

4.1.7(b) An information system needs to stand up an automated process to perform a specific function on its behalf. Once the function is complete, the automated process is decommissioned.

Gaps:

The interface to the DoD Issuing Certification Authority for securely connecting to and for automating the submission and retrieval of certificate signing requests does not currently exist.

For the use of "Only Locally Trusted (OLT)" solutions that may be used for certificates that are only used internally (e.g., behind a load balancer), the Azure Application Service Certificates and Azure Key Vault capabilities do not currently have DoD Provisional Authorizations and are not currently approved as required by DoD Instruction 8520.02.

Processes and capabilities for short lived NPEs do not exist, including identity vetting/provenance, issuance and validation of short term credentials, and provisioning entitlements.

4.1.8. DoD Beneficiary Registration

Pattern:

Figure 39 – DoD Beneficiary Registration

These use cases all require the issuance of non-PKI credentials to beneficiaries. Beneficiary identity is managed by the PDR, and beneficiaries are assigned an EDIPI. Beneficiaries may be issued a credential by DS Logon that contains their EDIPI, or they may use a commercially issued credential that must be registered to connect it to their beneficiary identity. Accessing information on behalf of another user also requires that the relationship be managed, either at the time of initial identity on-boarding (e.g., for a dependent), or through a formal process where the beneficiary delegates authorization to another individual.

Use Cases:

4.1.8(a) A DoD retiree desires to interact electronically with the DoD to manage their own health or other benefits.

4.1.8(b) A DoD military service member desires to interact electronically with the DoD using their personally owned device to manage health benefits or review their own financial information.

4.1.8(c) An individual desires to interact electronically with the DoD to manage health, financial, or other beneficiary information on behalf of a DoD beneficiary. The beneficiary is either a dependent of the individual or has specifically authorized the individual to act on their behalf.

4.1.8(d) A DoD beneficiary desires to interact electronically with the DoD related to low sensitivity non-Protected Health Information (PHI) such as scheduling an appointment at a DoD owned recreational facility.

Gaps:

Registering and managing beneficiary information through the PDR is a mature set of processes. DS Logon supports the issuance of password based credentials that are linked to the EDIPI. Migration to an MFA credential is in process.

Registering externally issued and managed credentials to a specific beneficiary is not supported today.

Registering a relationship to allow an individual to act on behalf of a beneficiary is not generally supported today, although beneficiaries may act on behalf of their dependent beneficiaries as a result of the dependency relationship.

4.1.9. DoD Applicant Registration

Pattern:

Figure 40 – Applicant Registration

These use cases require the registration of users to support consistent interaction with that user, but it may not be possible or desirable to collect and verify identity attributes. As a result, participants register and self-assert required attributes and are provided with a local identifier.

At the conclusion of a limited duration event, or if an applicant or recruit is not hired, all information, including identifiers, is archived as required by data retention policies and removed from active systems. If an applicant is hired or a recruit joins the military service, then information about that user is verified and used in registering the user as a member of the DoD internal community (see section 4.1.1).

Use Cases:

4.1.9(a) An individual applies for a job with the DoD.

4.1.9(b) An individual is recruited for military service and is completing initial accession activities.

4.1.9(c) A DoD relying party needs to register users for a limited duration event that will only require sharing low sensitivity non-PHI information such as registration for a conference or training class.

4.1.9(c) A tactical unit establishes a short term limited scope network that is not specifically NIPRNet or SIPRNet and does not support the connectivity requirements needed for the pattern described in Section 4.1.3.

Gaps:

These use cases are implemented locally when required. There are no DoD enterprise ICAM gaps.

4.2. Access Management Patterns

These use cases describe processes for accessing resources real time. Entities requesting access may be registered in advance, or may be unanticipated. Depending on the access requirements and digital policy rules for the resource being requested, unanticipated entities may be able to obtain access in near real time, or may be required to complete registration steps prior to access being granted.

These use cases assume that the entity is able to present an appropriate credential that is DoD approved for accessing the type of resource being requested and do not distinguish between credentials that are issued by a DoD enterprise ICAM capability, a COI or local DoD ICAM capability, or a DoD mission partner.

4.2.1. Access to DoD Managed Resources

Pattern:

The access pattern consists of three steps – authenticating the entity, determining if the entity is authorized to access the resource, and providing access to the resource if the entity is authorized.

Authentication requires that the entity present a credential claiming a digital identity, verifying that the credential was issued by a DoD approved credential provider, verifying that the credential is valid at the time of the request, and determining the identifier associated with that credential. Entities may be authenticated directly by the relying party information system that the entity is requesting access to, or entities may be authenticated by an IdP that then forwards the entity's identity information in a digitally signed assertion, which must be validated by the information system, to ensure that the assertion originates from a trusted source and that the contents of the assertion have not been modified. Identifiers may be present within the credential, or the credential may be registered with an entity data repository that maps the credential to an identifier. Entities that have not been provisioned to the specific relying party information system may already be registered with an entity data repository, or may be registered and linked to an identifier at the time of access request.

Authorization requires determining what the access policy rule is for the resource being requested, either through resource labeling and linking to a resource policy rule store, or locally through identifying entitlements such as group membership that are necessary for access to the resource. Once the policy rule has been identified, the relying party must determine if necessary attribute values are available about the resource and the entity to determine if access can be granted. If the entity is provisioned with entitlements to access the resource, no further action is necessary. If the entity is not provisioned, the relying party may seek to perform dynamic provisioning through attributes available in the credential, provided in an authentication assertion, or linked to the entity's identifier using one or more attribute services. If dynamic provisioning is not available, or if required attribute information cannot be obtained, the entity cannot be granted access to the resource.

If the entity is authorized, then access to the resource is granted. Otherwise, access is not granted. The relying party may provide information to the user regarding what steps will be needed to obtain access.

Use Cases:

4.2.1(a) An entity who has been registered and provisioned requests access to a DoD resource hosted by a DoD managed information system.

4.2.1(b) An entity who has not been provisioned requests access to a DoD resource hosted by a DoD managed information system that requires user registration.

Gaps:

The registration gap for mission partner entities after authenticating is the inability to link to the attributes needed for access. As a result, mission partner entities are unable to access many resources that they should be authorized for.

The DoD does not have an enterprise IdP service that accommodates DoD internal and mission partner entities.

DoD relying party information systems lack the ability to process assertions in lieu of direct authentication, limiting their ability to consume capabilities from DoD enterprise ICAM services.

The DoD has only limited enterprise services for attribute services. While some Components and COIs maintain attribute values for a limited population, the lack of availability of authorization attributes limits the implementation of dynamic provisioning and ABAC. Also, both attributes and their allowed value lists are not normalized across the Components, making ABAC decisions difficult to consistently evaluate.

DoD does not have an enterprise entitlement provisioning service. As a result, provisioning entitlements must be done for systems through COI portals or locally. These manual provisioning processes require significant processing time, delaying access to required resources.

Resource labeling is only performed by limited COIs, and the development and implementation of digital policy rules for access to resources is even more limited. The lack of defined digital policy rules is a primary deterrent to the expanded implementation of dynamic access.

Enterprise standards and policies for NPEs are lacking, resulting in limited ability for NPEs to access resources.

Enterprise standards, policies and ICAM services for NPEs are lacking, resulting in limited ability for NPEs to access resources.

4.2.2. Access for Unanticipated Entities

Pattern:

Access to many resources, especially information resources, should be supported through dynamic access which does not require registration of entities but instead allows a real-time access decision to be made at the time of the request based on information which can be made available the resource or PDP making the access control decision.

This access pattern still requires the three steps of authenticating the entity, determining if the entity is authorized to access the resource, and providing access to the resource if the entity is authorized.

Authentication may be performed by a DoD information system, DoD IdP, or approved external IdP, and requires that the entity present a credential claiming a digital identity, verifying that the credential was

issued by a DoD approved credential provider, verifying that the credential is valid at the time of the request, and determining the identifier associated with that credential. For unregistered entities who are authenticated by an external IdP, a DoD identifier may not be established or needed. Instead, the identifier will consist of the IdP's own identity combined with the identifier used by the IdP for that entity such as a full distinguished name from a PKI certificate.

Authorization requires determining what the access policy rule is for the resource being requested, through resource labeling and linking to a resource policy rule store. Once the policy rule has been identified, the relying party must determine if sufficient attributes are available about the entity to grant access. The entity is not required to be registered or provisioned. Instead, the relying party uses attributes available in the credential, provided in an authentication assertion, or linked to the entity's identifier using one or more attribute services. If required attribute information cannot be obtained, the entity cannot be granted access to the resource.

If the entity is authorized, then access to the resource is granted. Otherwise, access is not granted. The relying party may provide information to the entity regarding what steps will be needed to obtain access.

Use Cases:

4.2.2(a) An entity requests access to a DoD resource that is managed through a fully ABAC model that does not provision entities.

4.2.2(b) An entity requests access to a DoD resource that does not provision users and all attributes required for satisfying the digital policy rule for access to that resource are included in the entity's credential or the assertion presented to the information system hosting the resource.

4.2.2(c) A person entity or NPE supporting a member of a coalition requests access to a resource where access is limited by member nation, not by individual entity.

4.2.2(d) An NPE is created in response to a user request which then requests access to a resource on behalf of the originating user. The NPE is provided with an assertion that includes the identity of the NPE that created it and the identity of the user making the request (the user may be a person entity or NPE). Access decisions by relying parties should be made taking into account both the requesting NPE and the rights of the requesting user.

4.2.2(e) An entity in a DDIL environment requests access to a resource that is in the same DDIL environment. If attributes needed for satisfying the digital policy rule for access to that resource have been cached in the environment, the entity is able to dynamically obtain access to the resource. However, if required attributes have not been cached within the environment, the resource owner will need to use a manual provisioning process for that user. Manual provisioning of required entitlements may be temporary pending the opportunity to request and cache needed attributes for that user when connectivity to attribute stores becomes available.

Gaps:

There is no DoD enterprise IdP service available. IdPs that have been implemented by Components or COIs do not always support authentication of DoD mission partner entities.

Because there is no DoD enterprise service for registering mission partner entities, mapping attributes to mission partner entities is lacking or only performed at a local level.

Relying party information systems are not generally configured to process assertions in lieu of performing direct authentication. As a result, many of these systems do not support access by mission partner entities because of the complexity of authenticating mission partner credentials.

Labeling resources and aligning them to digital policy rules for access is lacking across the DoDIN, with some exceptions in coalition environments where resources are tagged with country releasability. The lack of defined digital policy rules is a primary deterrent to the expanded implementation of dynamic access.

Enterprise standards, policies and ICAM services for NPEs are lacking, resulting in limited ability for NPEs to access resources.

4.2.3. Privileged User Access

Pattern:

The access pattern consists of three steps – authenticating the user, determining if the user is authorized to access the resource, and providing access to the resource if the user is authorized. This pattern is similar to the pattern described in Section 4.2.1. However, additional monitoring and oversight should be implemented to address the additional risks presented by users with elevated access rights, including:

- Required use of separate credentials to perform privileged functions from those used for non-privileged access
- Workstation and network connectivity limitations for accessing privileged functions
- Allow access to privileged user accounts only through Privileged Account Management (PAM) tools that control access to privileged user accounts, monitor behavior, and log activity

PAM tools provide an enhanced capability for the discovery, management, and enforcement of business rules that define which users can perform which actions against which resources.

Use Cases:

4.2.3(a) An IT privileged user requests access to a DoD resource to perform privileged functions.

4.2.3(b) A functional privileged user such as an approver requests access to a DoD resource to perform privileged functions.

Gaps:

The DoD PKI supports the issuance of segregated credentials to privileged users. Minimum requirements for specific types of privileged users are not defined across the DoD enterprise.

Capabilities for privileged user monitoring are currently implemented at the Component or COI level, no enterprise services exist.

Although PAM tools currently in the market provide integrations with many market leading applications and SaaS providers, there are many relying party information systems currently in use within the DoD that are not supported by PAM tools.

Workflows within the relying party information systems must be configured to require dual-approval of changes for privileged actions where appropriate. Not all relying parties support such configuration.

Workflows within functional management tools must be configured to require dual-approvals for privileged actions where appropriate. This configuration is typically performed locally and is impractical to automate at the enterprise level.

Individual accountability can be limited in tactical DDIL environments since many systems implement group authentication without traceability back to enterprise defined identities.

4.2.4. Zero Trust

Pattern:

ICAM is a fundamental pillar of a Zero Trust (ZT) environment. As ZT becomes better defined within the DoD, ICAM support for ZT will be critical. The access pattern in a ZT environment includes multiple steps:

- User and end user device both authenticate to network
- Network decision point dynamically provisions default connectivity based on identity, state, and environmental conditions
- User requests access to a resource
- Access to the requested resource is evaluated; if the user and the user's endpoint device are granted access to that resource, the network dynamically provisions a connection for the duration of that session
- Access to the requested resource for the specific action is evaluated and the grant/deny decision is enforced
- At end of session, connection is de-provisioned
- Everything is logged

Use Cases:

4.2.4(a) An entity requests access to a DoD resource that is managed in a ZT environment.

Gaps:

Prerequisite capabilities to enable enterprise-level ZT are not yet in place across the DoD, including:

- Enterprise ICAM, including a robust set of user attributes and values for both person entities and NPEs
- Resource labeling with associated defined digital policy rules for access
- Access policy management, decision, and enforcement points, with applications refactored to externalize access decisions
- Software Defined Networking to enable dynamic provisioning and de-provisioning of network connections
- Existing resources often rely upon access control decisions made elsewhere instead of each resource performing an access control decision.

4.2.5. Access to Software as a Service (SaaS) Cloud Managed System

Pattern:

The access pattern consists of three steps: authenticating the user, determining if the user is authorized to access the resource, and providing access to the resource if the user is authorized. This pattern is similar to the pattern described in Section 4.2.1. However, there are differences in the way that Software as a Service (SaaS) vendors support authentication and authorization.

For authentication, while some SaaS vendors support direct PKI based authentication, most require the presentation of an assertion from an IdP.

For authorization, cloud SaaS providers generally follow one of these five processes.

- The SaaS vendor requires pre-provisioning of all entity accounts and entitlements to its local access control engine and performs authentication of the entity using credentials issued and managed by the SaaS vendor (e.g., does not support federated authentication). The authentication of the entity to the SaaS must be proxied by the DoD IdP. Entity accounts are provisioned to the SaaS. The internal identifier and authentication factors (e.g., password) are stored in the SaaS internal IdP, and in the DoD IdP with a mapping to the DoD entity identity. When an entity requests access to the SaaS resource, the entity authenticates directly to the DoD IdP, which then presents the identifier and authentication factors that the SaaS is expecting on the entity's behalf. This process does not support entities who have not been pre-registered and provisioned.
- The SaaS vendor requires pre-provisioning of all entity accounts and entitlements to its local access control engine and supports authentication through presentation of assertions from an external IdP. Authorized entities must be pre-provisioned to the SaaS vendor using the vendor provided interface. Changes to access rights must be uploaded to the SaaS vendor when the change is made. After the entity authenticates to a DoD IdP, the IdP provides an assertion to the SaaS vendor containing the user's identifier. This process does not support entities who have not been pre-registered and provisioned.
- The SaaS vendor requires pre-provisioning of all entity accounts and inclusion of attributes needed for authorization in the assertion. The use of assertions requires that the vendor and the DoD IdP set up a trust agreement that defines the attributes to be used and the schema for the attributes. Entity accounts must be managed through the interface provided by the SaaS vendor. After the entity authenticates to a DoD IdP, the IdP determines appropriate attribute values and includes them in an assertion to the SaaS vendor containing the user's identifier. This process does not support entities who have not been pre-registered, but does support entities whose authorization attributes have changed.
- The SaaS vendor does not pre-provision entity accounts but requires inclusion of identity and attributes needed for authorization in the assertion. The use of assertions requires that the vendor and the DoD IdP set up a trust agreement that defines the attributes to be used and the schema for the attributes. After the entity authenticates to a DoD IdP, the IdP determines appropriate attribute values and includes them in an assertion to the SaaS vendor containing the entity's identifier.
- The SaaS vendor does not manage access. After the entity authenticates to a DoD IdP, the IdP determines whether the entity is authorized, and only forwards a request to the SaaS vendor for an authorized entity. this pattern requires the IdP to be:
    - Provisioned with entitlements for the entity accessing the specific resource (or use a service that provides them), or
    - Obtain a policy for determining access to the resource from somewhere AND obtain information about the resource from the SaaS (or an attribute service) to be able to use the policy to make a decision.

Use Cases:

4.2.5(a) An entity who has been registered and provisioned requests access to a DoD resource hosted by a cloud SaaS provider.

4.2.5(b) An entity who has not been provisioned requests access to a DoD resource hosted by a cloud SaaS provider.

Gaps:

There is no DoD enterprise IdP service available. IdPs that have been implemented by Components or COIs do not always support authentication of DoD mission partner entities.

Because there is no DoD enterprise service for registering mission partner entities, mapping attributes to mission partner entities is lacking or only performed at a local level.

Most mission partners do not have IdPs implemented that can generate assertions, and DoD relying parties are not configured to consume IdPs from external mission partners. These assertions could potentially include attributes in addition to identity information that could support authorization decisions.

Resource labeling is only performed by limited COIs, and the development and implementation of digital policy rules for access to resources is even more limited. The lack of defined digital policy rules is a primary deterrent to the expanded implementation of dynamic access. The lack of consistent up to date data tagging is a larger issue than the perceived lack of digital policy.

The DoD has only limited enterprise services for attribute services. While some Components and COIs maintain attribute values for a limited population, the lack of availability of authorization attributes limits the implementation of dynamic provisioning and ABAC. Also, both attributes and their allowed value lists are not normalized across the Components, making ABAC decisions difficult to consistently evaluate

Enterprise standards, policies and ICAM services for NPEs are lacking, resulting in limited ability for NPEs to access resources.

4.3. Access Accountability Patterns

4.3.1. Logging and Monitoring

Pattern:

The pattern for log collection is described in Section 3.2.1.

Use Cases:

4.3.1(a) A person entity is suspected of engaging in unauthorized behavior, and the investigator requires information regarding all resources the user has accessed within the past six months.

4.3.1(b) A DoD Security Operations Center (SOC) or Cybersecurity Service Provider (CSSP) monitors access behavior across the DoD enterprise and flags anomalous behavior for review by human analysts to identify potential insider threats.

4.3.1(c) An NPE might be compromised and there is a need to analyze traffic and resource accesses related to it.

4.3.1(d) Evidence exists that a DoD resource was leaked/compromised and investigation requires a list of all person entities and NPEs who accessed it over a given timeframe.

Gaps:

Standards and processes for collecting and correlating ICAM related logs have not been deployed at the DoD enterprise level.

4.3.2. Access Review

Pattern:

The patterns for access review is described in Section 3.2.2.

Use Cases:

4.3.2(a) The DoD financial audit requires a review of entitlements for users of in-scope financial information systems to verify that users only have accesses they required to perform their job functions, and that no user's accesses violate separation of duty rules either within a single information system or across multiple information systems.

4.3.2(b) A security auditor reviews access rights for IT privileged users to verify that users only have accesses they require to perform their job functions, and that all required privileged user accounts are managed through PAM tools.

4.3.2(c) A person entity with attributes that grant access to certain systems in the organization leaves that organization. An individual with supervisory responsibilities reviews all attributes and provisioned entitlements for that person entity and requests changes as warranted in line with the person entity's role change.

4.3.2(d) A system owner reviews access rights for all entities with provisioned entitlements on the system to verify that entities only have those accesses need to perform their job functions.

4.3.2(e) A sponsoring organization reviews access rights for long-life NPEs to verify that the NPEs only have accesses they require to perform their job functions.

4.3.2(f) An NPE is being decommissioned. The NPE sponsoring organization reviews all access rights for the NPE and notifies any systems or services that the NPE is being decommissioned so that credentials, attributes, and provisioned entitlements can be revoked or changed.

Gaps:

Consolidation of entitlement information is not available as a DoD enterprise ICAM capability, resulting in a lack of ability to perform access reviews except at the relying party information system level.

DoD lacks the ability to review dynamic access.

Access reviews are not performed when person entity roles changed. Failure to accurately maintain attribute values is a significant challenge/gap that will grow over time as more dynamic decisions are implemented.

Access review should be performed for both person entities and NPEs. As more and more automation occurs, NPEs can face the same problems as person entities, and are often reviewed even less frequently.

4.3.3. Identity Resolution

Pattern:

The pattern for identity resolution is described in Section 3.2.3.

Use Cases:

4.3.3(a) DoD registers and issues locally valid credentials to community care providers and other first responders within a DDIL network established in response to an emergency. When the local network establishes connectivity with the DoDIN, the DoD must determine if any of the locally registered person entities already have identifiers issued by the PDR.

4.3.3(b) Department of Homeland Security (DHS) registers and issues PIV cards to its employees. DHS engages with DoD on a joint short term activity and provides identity information about users who will be participating in the activity to the DoD COI. The DoD and DHS later decide that the activity will continue indefinitely and the COI decides to upload the registered DHS users to the DoD enterprise PDR. DoD must determine if any of the DHS managed users also have existing DoD identifiers, such as former DoD dependents, contractors supporting both DoD and DHS, or DoD reservists who are employees of DHS.

4.3.3(c) An individual who has been banned from DoD networks as a result of engaging in unauthorized activity gets a job working for a DIB mission partner.

4.3.3(d) A local identity is established and a credential is issued to a person entity on a closed restricted network that is derived from presentation of an enterprise credential such as a CAC. Because the closed restricted network may be connected to the DoD enterprise at a later date, the local identity records the enterprise identifier to support identity resolution.

Gaps:

Identity resolution is performed for DoD internal community members both at the time of initial registration and periodically. However, identity resolution capabilities for mission partner entities is not generally performed.

Local identities are often established without ever attempting to link the identities to DoD identities. Even if a DoD-wide authenticator is checked at the time of registration (e.g., vet a person's identity using a CAC), the local system uses a different way of identifying the person (e.g., first initial, last name for the user name); creating a new digital identity without linking it to the existing DoD enterprise identity.

4.4. Contact Data Lookup

Pattern:

The pattern for contact data lookup is described in Section 3.3.

Use Cases:

4.4(a) A DoD internal community member needs to identify the email address of another DoD internal community member.

4.4(b) A coalition member needs to identify the email address of another coalition member.

4.4(c) A DoD internal community member needs to identify the email address of a Federal Agency mission partner person entity.

4.4(d) An NPE needs to look up contact data for a person entity in order to send an alert.

4.4(e) A management NPE needs to discover all of the NPEs it has oversight of so it can send out an update or get status (e.g., managing all of the radios in the network).

Gaps:

Contact data lookup for DoD internal person entities is supported through the Enterprise Directory Service (EDS). Contact data collection and lookup for NPEs and mission partner entities is limited.

5. DoD Enterprise ICAM Services

This section identifies and describes existing and planned DoD Enterprise ICAM services. The context of the collection of ICAM services is shown in Figure 41. These services are organized according to the capabilities that were identified in Section 2 that they implement. The broad interface categories and data flows are also depicted, wherein data from authoritative sources are used within the ICAM processes to enable access decisions and to enable a robust audit trail. Initial gap analysis has identified several ICAM services that do not currently exist and are not currently planned. Authoritative sources are intended to be representational and do not represent all possible source systems.

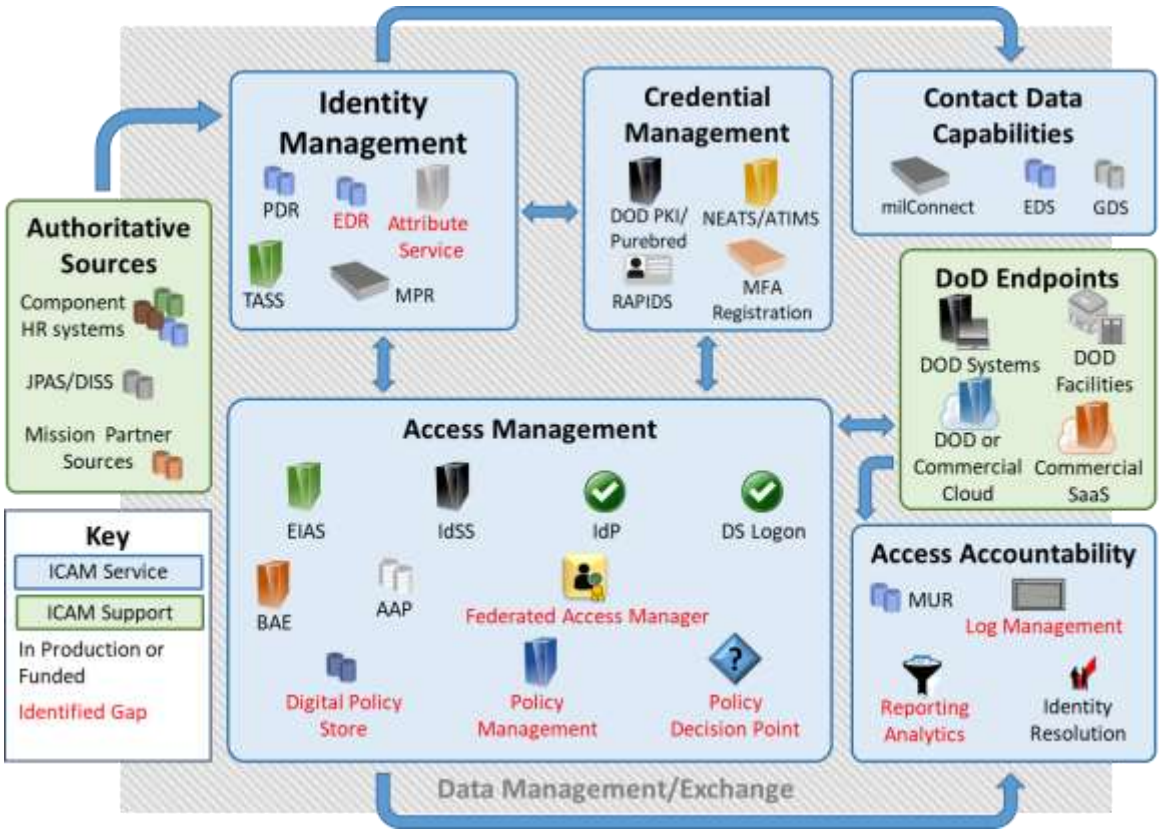


Figure 41 – ICAM Service View (SvcV-1)

Some DoD enterprise ICAM services, especially identity management and access accountability services, are dependent on receiving accurate and timely information from DoD Component or COI level ICAM services. DoD Components must coordinate with DoD enterprise ICAM service providers to ensure common standards and interoperability between enterprise and DoD Component and COI level ICAM services.

5.1. DoD ICAM Enterprise Services Summary

Table 4 provides a summary of DoD ICAM Enterprise Services that are either in production today or are planned and budgeted. Each service is described in this section, including what the service does, who operates it, what entities the service supports, and what the service interfaces with. The Capabilities column aligns with the capability taxonomy in Section 2.2, Figure 3. For more detailed information about availability, capabilities, and interfaces, relying parties can contact their customer service representative at the service provider listed, either the Defense Information Systems Agency (DISA) or DMDC.

Table 4 – ICAM Enterprise Services

Service	Provider	Status	Network	Capabilities
Identity Management				
Person Data Repository (PDR)	DMDC	Production	• NIPRNet • SIPRNet	• Person Entity
Trusted Associate Sponsorship System (TASS)	DMDC	Production	• NIPRNet	• Person Entity
Mission Partner Registration (MPR)	DMDC	Planned	• NIPRNet	• Federated Entity
Multi-Factor Authentication (MFA) Registration Service	DMDC	Planned	• NIPRNet	• Federated Entity
Credential Management				
DoD Public Key Infrastructure (PKI)	DISA	Production	• NIPRNet • SIPRNet	• Internal Credential Management
Real-Time Automated Personnel Identification System (RAPIDS)	DMDC	Production	• NIPRNet	• Internal Credential Management
NIPRNet Enterprise Alternate Token System (NEATS) / Alternate Token Issuance and Management System (ATIMS)	DMDC	Production	• NIPRNet	• Internal Credential Management
Purebred	DISA	Production	• NIPRNet	• Internal Credential Management
MPR	DMDC	Planned	• NIPRNet	• External Credential Registration
MFA Registration Service	DMDC	Planned	• NIPRNet	• External Credential Registration
DoD Self-service (DS) Logon	DMDC	Production	• NIPRNet	• Internal Credential Management
DS Logon (Enhanced)	DMDC	Planned	• NIPRNet	• Internal Credential Management
Identity Provider (IdP)	DISA	Planned	• NIPRNet	• Internal Credential Management • External Credential Registration
Access Management				
Enterprise Identity Attribute Service (EIAS)	DMDC	Production	• NIPRNet • SIPRNet	• Authorization
EIAS (Enhanced)	DMDC	Planned	• NIPRNet	• Authorization

Service	Provider	Status	Network	Capabilities
			• SIPRNet	
Backend Attribute Exchange (BAE)	DMDC	Planned	• NIPRNet	• Authorization
Identity Synchronization Service (IdSS)	DISA	Production	• NIPRNet • SIPRNet	• Authentication • Authorization
Enterprise Directory Services (EDS)	DISA / DMDC	Production	• NIPRNet	• Authentication
IdP	DISA	Planned	• NIPRNet	• Authentication • Authorization
MFA Registration Service	DMDC	Planned	• NIPRNet	• Authentication
MPR	DMDC	Planned	• NIPRNet	• Authorization
Automated Account Provisioning (AAP)	DISA	Planned	• NIPRNet	• Provisioning
DS Logon	DMDC	Production	• NIPRNet	• Authentication • Authorization
Access Accountability				
Master User Record (MUR)	DISA	Planned	• NIPRNet	• Access Review
Identity Resolution Service	DMDC	Production	• NIPRNet	• Identity Resolution
Contact Data				
EDS	DISA / DMDC	Production	• NIPRNet	• Contact Data Lookup
milConnect	DMDC	Production	• NIPRNet	• Contact Data Collection
IdSS	DISA	Production	• NIPRNet	• Contact Data Collection
Global Directory Service (GDS)	DISA	Production	• NIPRNet • SIPRNet	• Contact Data Lookup

5.2. Production DoD ICAM Enterprise Services

This section provides a high level description of DoD ICAM enterprise services that are currently in production. Descriptions include a high level purpose statement for the service, who operates the service, what interfaces the service supports, and which data flows the service provides.

5.2.1. Person Data Repository (PDR)

The Person Data Repository (PDR), operated by DMDC, is the DoD human resource authoritative source for person, personnel, and identity attributes. The PDR supports DoD internal community and beneficiary members. The PDR provides DoD person entity Data Management capabilities including: Extract, Transform, and Load (ETL) and data attribute normalization. The PDR operates on both NIPRNet and SIPRNet.

The PDR aggregates information provided by DoD component human resource databases and TASS as well as data regarding CACs from RAPIDS, and provides information to EIAS.

The PDR is an identity management service. It provides digital identity creation, maintenance, and deactivation for person entities that are part of the DoD internal community and beneficiaries.

5.2.2. Identity Resolution Service

The Identity Resolution Service, operated by DMDC, is performed on the PDR on a daily basis to verify that there are no duplicate digital identities for a single person entity. The identity resolution service supports DoD internal community and beneficiary members. The identity resolution service operates on the NIPRNet.

The Identity Resolution Service operates in support of the PDR.

The Identity Resolution Service provides identity resolution as part of access accountability.

5.2.3. Trusted Associate Sponsorship System (TASS)

Trusted Associate Sponsorship System (TASS), operated by DMDC, is the authorized personnel source for DoD contractors. TASS supports contractors who are being enrolled as part of the DoD internal community. TASS operates on the NIPRNet.

TASS is the authoritative data source for contractor information. Once a contractor is enrolled in TASS, their information is forwarded to the PDR.

TASS is an identity management service. It provides digital identity creation, maintenance, and deactivation for contractors that are part of the DoD internal community.

5.2.4. DoD Public Key Infrastructure (PKI)

The DoD PKI, operated jointly by DISA and the NSA, is a framework established to issue, maintain, and revoke public key certificates for person entities and NPEs. The DoD PKI operates on both NIPRNet and SIPRNet.

The DoD PKI interfaces with certificate issuance systems including RAPIDS/CAC, NEATS, and Purebred, as well as supporting manual requests from Registration Authorities and other authorized users for certificate issuance and revocation. The DoD PKI publishes CRL and provides real-time responses to requests for certificate validation to any user. The DoD PKI also supports interoperability with DoD External Certificate Authorities (ECA), other Federal Agency PKIs, selected commercial PKIs, and selected CCEB PKIs as approved by the DoD CIO.

The DoD PKI is a credential management service. It provides internal credential issuance, credential maintenance, and credential revocation for entities that are part of the DoD internal community. It also supports external federation through the issuance and maintenance of cross certificates to external PKIs.

5.2.5. Real-Time Automated Personnel Identification System (RAPIDS)

Real-Time Automated Personnel Identification System (RAPIDS), operated by DMDC, provides the capability for the DoD's identity card issuance service that supports credential lifecycle management, including Common Access Cards (CAC) used for physical and logical access and other physical DoD identity cards that are used for physical access only. RAPIDS supports DoD internal community members and beneficiaries. RAPIDS operates on the NIPRNet.

RAPIDS interfaces with the PDR to obtain identity information used to generate CACs and DoD identity cards and to verify that the person requesting the card has been authorized to obtain one. RAPIDS also generates public/private key pairs and interfaces with the DoD PKI to request the issuance of PKI based digital certificates. RAPIDS writes the key pairs and respective certificates onto CACs.

RAPIDS is a credential management service. It provides internal credential issuance, credential maintenance, and credential revocation for entities that are part of the DoD internal community and beneficiaries.

5.2.6. NIPRNet Enterprise Alternate Token System (NEATS) / Alternate Token Issuance and Management System (ATIMS)

NIPRNet Enterprise Alternate Token System (NEATS) / Alternate Token Issuance and Management System (ATIMS), operated by DMDC, supports the issuance of hardware PKI tokens to people who are not eligible for CACs and to users who require an additional hardware PKI token to support privileged user, group and role, and code signing uses. NEATS/ATIMS operates on the NIPRNet.

NEATS/ATIMS interfaces with the PDR to obtain identity information. NEATS/ATIMS also interfaces with the DoD PKI to request the issuance of PKI based digital certificates.

NEATS/ATIMS is a credential management service. It provides internal credential issuance, credential maintenance, and credential revocation for entities that are part of the DoD internal community and limited mission partner entities who are not part of the DoD internal community but who require DoD PKI issued hardware credentials.

5.2.7. Purebred

Purebred, operated by DISA, supports the issuance of PKI based digital certificates to person entities and NPEs for use with internal DoD user assigned mobile devices with hardware backed key stores or security tokens. Purebred operates on the NIPRNet.[3]

Purebred interfaces with the DoD PKI to request the issuance of PKI based digital certificates.

Purebred is a credential management service. It provides credential issuance, credential maintenance, and credential revocation for entities that are part of the DoD internal community who have approved mobile devices.

5.2.8. DoD Self-service (DS) Logon

DoD Self-service (DS) Logon, operated by DMDC, issues and manages credentials and associated attributes for beneficiaries. DS Logon also supports access to information systems that provide self-service information and information technology resources for DS Logon participants. DS Logon operates on the NIPRNet.

DS Logon interfaces with the PDR for identity information. DS Logon also interfaces with information systems to provide authentication assertions when users have authenticated to DS Logon.

DS Logon is a credential and access service. It provides internal credential issuance, credential maintenance, and credential revocation for beneficiaries. It also acts as an identity provider to support authentication.

[3] More information regarding Purebred may be found at https://cyber.mil/pki-pke/purebred/.

5.2.9. Enterprise Identity Attribute Service (EIAS)

Enterprise Identity Attribute Service (EIAS), operated by DMDC, distributes DoD person, persona, and personnel attributes to applications and services in a controlled, consistent, and secure manner. EIAS operates on the NIPRNet and SIPRNet.

EIAS interfaces with the PDR to obtain attribute information. Because attributes supported by EIAS contain PII, appropriate Privacy Impact Assessments (PIA) or System of Records Notices (SORN) must be in place prior to providing identity and identity attribute information. EIAS interfaces with other DoD enterprise ICAM services and DoD components to provide attribute information.

EIAS is an access management service. It is an attribute service that provides identity attribute information about person entities that are part of the DoD internal community to support dynamic and hybrid entitlement provisioning and authorization using dynamic access.

5.2.10. Identity Synchronization Service (IdSS)

Identity Synchronization Service (IdSS) controls all account creation, deletion, and updates into DISA's EASF and downstream directory system supporting DoD internal community members that require access to DISA hosted DoD enterprise services. IdSS operates on the NIPRNet and SIPRNet.

IdSS interfaces with EIAS to obtain identity attribute and credential information and with GDS to obtain email encryption certificates. IdSS also interfaces with DISA hosted information systems to provide authentication assertions and other attributes as needed. IdSS can also provide authentication assertions to cloud-based or DoD operated information systems.

IdSS is an access management service. It is an authentication service that acts as an identity provider to support authentication, and it is an authorization service that provides identity attribute information about person entities that are part of the DoD internal community to support dynamic and hybrid entitlement provisioning and authorization using dynamic access.

5.2.11. milConnect

milConnect, operated by DMDC, allows DoD internal community members to access and update their personal and personnel information. milConnect operates on the NIPRNet[4].

milConnect interfaces with the PDR to update contact data attributes.

milConnect is a contact data service that supports contact data collection.

5.2.12. Enterprise Directory Services (EDS)

Enterprise Directory Service (EDS), jointly operated by DISA and DMDC, is a suite of services that provide authoritative DoD enterprise identity and contact attributes. EDS operates on the NIPRNet. EDS includes the following services:

- Real-time Broker Service (RBS), operated by DMDC, synchronous web service that provides DoD identity and contact data
- Batch Broker Service (BBS), operated by DMDC, asynchronous web service that provides DoD identity and contact data
- IDSS Machine Interface (IDMI), operated by DISA, supports local directory provisioning and updating by providing DoD identity and contact data

[4] milConnect is scheduled to be fully decommissioned by the end of fiscal year 2021.

- Enterprise Directory Query Service (EDQS), operated by DISA, provides a Lightweight Directory Access Protocol LDAP interface to query IdSS data

EDS interfaces with PDR and IdSS to obtain identity and contact data information. EDS interfaces with component directories to provide identity and contact data information.

EDS is an access management service. It is an attribute service that provides identity attribute information about person entities that are part of the DoD internal community to support dynamic and hybrid entitlement provisioning and authorization using dynamic access. EDS is also a contact data collection service that provides contact data to local directories.

5.2.13. Global Directory Service (GDS)

Global Directory Service (GDS), operated by DISA, is a directory service that supports the DoD PKI program. GDS is the distribution point for DoD PKI CA certificates, CRLs, and email encryption certificates. GDS operates on NIPRNet and SIPRNet.

GDS interfaces with the DoD PKI to obtain certificate information. GDS also provides a search capability for users to obtain email addresses and email encryption certificates for DoD internal community members.

GDS is a contact data lookup service for email addresses and email encryption certificates.

5.3. Planned DoD ICAM Enterprise Services

This section provides a high level description of DoD ICAM enterprise services that are in the planning or development stage. Descriptions include a high level purpose statement for the service, who operates the service, what interfaces the service supports, and which data flows the service provides. Implementation timelines for planned services are in development, capabilities are expected to be operational in fiscal year 2021.

5.3.1. Mission Partner Registration (MPR)

The Mission Partner Registration (MPR), in development by DMDC, will allow DoD government personnel to sponsor DoD mission partner identities and register their identifiers so that identity can be shared across the DoD ICAM architecture in a similar fashion to DoD personnel.

The MPR will interface with external mission partner identity and credentialing systems to obtain identity attributes and register credentials. The MPR will also interface with information systems to provide identifier and attribute information.

The MPR is an identity management service that supports creation, maintenance, and deactivation of federated entity identities. It is also a credential management service that performs external credential registration.

5.3.2. Identity Provider (IdP)

The Identity Provider (IdP), in development by DISA, will be a centralized authentication service for applications for both DoD issued and mission partner credentials, including username and password management, MFA credential authentication enablement and management, PKI certificate validation, and a token provider.

The IdP will interface with PDR and MPR to obtain identity attribute information for DoD internal community members and registered mission partner entities. The IdP will also interface with external

approved IdPs and credential service providers to validate mission partner credentials and assertions. The IdP will provide assertions to DoD information systems once users have been authenticated.

The IdP is an access management service. It is an authentication service that acts as an identity provider to support authentication.

5.3.3. Multi-Factor Authentication (MFA) Registration Service

The Multi-Factor Authentication (MFA) Registration Service, in development by DMDC, will aggregate and combine DoD issued credentials for DoD internal community members and external credentials for mission partner entities into a single repository that supports the IdP for user authentication. The MFA Registration Service will register approved external credentials, perform validation of external credentials, and connect mission partner entities to other identity attributes to support use for DoD information system relying parties.

The MFA Registration Service will interface with the PDR and the MPR to obtain identity information, and with external credential service providers to validate mission partner credentials. It will also interface with the IdP to validate external credentials and provide identity information.

The MFA Registration Service is an identity management service that supports creation, maintenance, and deactivation of federated entity identities. It is also a credential management service that performs external credential registration. It is also an access management service that supports authentication as well as authorization by providing identity attribute information.

5.3.4. EIAS (Enhanced)

See Section 5.2.9 for a description of EIAS. Planned enhancements to EIAS include implementing processes to enhance data quality for attributes provided, and to modernize standards supported in providing attribute information to information systems.

5.3.5. Backend Attribute Exchange (BAE)

Backend Attribute Exchange (BAE), in development by DMDC, will allow DoD to exchange identity and credential information about person entities seeking access or transferring from one agency to another with other participating Federal Agency mission partners.

BAE will interface with the PDR and MPR to maintain information about registered Federal Agency mission partner entities. BAE will also interface with Federal Agency mission partner identity and credential management systems to obtain this information.

BAE is an access management system. It is an attribute service that provides identity attribute information about Federal Agency mission partner person entities to support dynamic and hybrid entitlement provisioning and authorization using dynamic access.

5.3.6. DS Logon (Enhanced)

See section 5.2.8 for a description of DS Logon. Planned enhancements to DS Logon include modernizing the architecture, support for MFA credentials, and support for federated credentials.

5.3.7. Automated Account Provisioning (AAP)

Automated Account Provisioning (AAP), in development by DISA, will provide identity governance services such as user entitlement management, business role auditing and enforcement, and account

provisioning and de-provisioning based on identity data produced during DoD people-centric activities such as on and off-boarding, continuous vetting, talent management, and readiness training.

AAP will interface with the PDR, EIAS, and other attribute services to obtain attribute information to support automated provisioning. AAP will also interface with information systems to provision and de-provision entitlements.

AAP is an access management system. It supports manual, dynamic, and hybrid entitlement provisioning and de-provisioning.

5.3.8. Master User Record (MUR)

Master User Record (MUR), in development by DISA, will enable DoD-wide knowledge, audit, and data rollup reporting of who has access to what system or applications. MUR will support identification of insider and external threats, and will enable financial management segregation of duties auditability across DoD Component organizations.

MUR will interface with the PDR, as well as DoD Component ICAM services and information systems to collect and correlate attribute and entitlement information for person entities that have access to DoD resources.

MUR is an access accountability system that supports access review.

6. ICAM Implementation Responsibilities

This section highlights responsibilities for implementing the ICAM program across the DoD. Responsibilities are divided between DoD enterprise ICAM service providers and DoD Components who consume DoD enterprise ICAM services and operate COI and local ICAM services. This section also identifies responsibilities related to accepting services provided by external federated ICAM service providers. These roles and responsibilities are aligned with ICAM policy defined in OMB Memo M-19-17.

6.1. DoD ICAM Joint Program Integration Office (JPIO) Responsibilities

The JPIO provides integration responsibility for the DoD ICAM enterprise capabilities. The JPIO is led by DISA, and NSA and DMDC both provide a Senior Executive-level individual to serve as deputy leads and to coordinate their agencies' ICAM efforts. The DoD ICAM JPIO develops and maintains an implementation plan for DoD enterprise ICAM services.

6.2. DoD Enterprise ICAM Service Provider Responsibilities

DoD enterprise ICAM service providers provide one or more services that support ICAM capabilities. A service is defined as DoD enterprise if it can be used by anyone across the DoD, and, for externally facing federation services, by any DoD mission partner. DoD enterprise ICAM services may be hosted by DISA or DMDC, or may be hosted by another DoD Component. DoD enterprise ICAM service providers must:

- Provide DoD enterprise ICAM services meeting defined availability targets
- Support cybersecurity and interoperability testing of DoD enterprise ICAM services
- Develop and publish interface specifications describing the capabilities provided by the enterprise service, the entities the service provides information for, and the interfaces the service supports
- Implement a process for collecting and prioritizing requirements for functionality enhancements to the service
- Monitor and identify enhancements needed to ensure resilience and adaptability to changes in the threat environment

6.3. DoD Component Responsibilities

DoD Components rely on ICAM services to perform their missions. DoD Components support DoD enterprise ICAM services such as providing verified identity and attribute data and providing trained personnel to verify identity and issue credentials. Where ICAM enterprise services do not meet the needs of Component use cases, Components are also responsible for operating COI and local ICAM services that comply with DoD enterprise technical and process standards.

6.3.1. Establish DoD Component Level ICAM Governance

DoD Components must establish DoD Component level governance to implement ICAM, to include:

- Developing and maintaining DoD Component level ICAM policies and procedures
- Maintaining visibility into DoD Component level budgets for ICAM capabilities

- Identifying DoD Component level organizations responsible for coordinating and providing ICAM services and executing organizational structures for effective ICAM service coordination and implementation

6.3.2. Support DoD Enterprise ICAM Services

DoD Components must support DoD enterprise ICAM services, to include:

- Identifying requirements for enterprise ICAM services to support DoD Component ICAM implementation and provide requirements to the JPIO
- Defining and implementing processes for the accurate collection and management of enterprise attributes for DoD Component entities and provide this information to DoD enterprise attribute services in a timely fashion
- Performing identity proofing and suitability determination for the issuance of DoD enterprise credentials
- Coordinating with enterprise ICAM service providers to ensure common standards and interoperability between enterprise and DoD Component and COI level ICAM services.

6.3.3. Use DoD Enterprise ICAM Services

DoD Components must implement ICAM for DoD Component employees, contractors, mission partner entities, information systems, and resources to include:

- Leveraging DoD enterprise ICAM services where available and appropriate for the mission
- Supporting interoperability testing of DoD enterprise ICAM services
- Using standards-based interfaces to perform ICAM activities including the acceptance of authentication assertions. Where legacy information systems do not support ICAM standards, implement proxies to support ICAM standards where operationally feasible
- Leveraging DoD enterprise ICAM services where available to support ICAM for NPEs, including naming, identity management, credentialing, and provisioning
- Developing and implementing policy rules for access to resources. Where appropriate, publish resource policy rules to DoD enterprise policy stores
- Aligning resources to policy rules through data tagging or within information systems that host the resources
- Performing authentication and authorization to access all DoD Component managed resources, including physical and logical access, unless the resource has been approved for public release
- Logging ICAM events and make ICAM logs available to DoD enterprise log collection services

6.3.4. Operate COI and Local ICAM Services

Although DoD Components are encouraged to use DoD enterprise ICAM services, there may be circumstances where enterprise services are not available or do not meet the needs of the mission. For example, a coalition network may have only minimal or no connectivity to the NIPRNet and must register and provide credentials to local nationals who require access to resources on the coalition network. When operating COI or local ICAM services, DoD Components must:

- Ensure that the ICAM services use standards-based interfaces and are operated in accordance with DoD policy
- Address the full lifecycle of the ICAM service. For example, if the DoD Component is operating a CSP, the DoD Component must address all aspects of credential issuance, including identity proofing, credential management, credential validation, and credential revocation

6.4. Responsibilities Related to External Federated ICAM Service Providers

DoD relying parties may use ICAM services providers that are owned and operated externally to the DoD. Examples of these external service providers include:

- Federal agencies that issue PIV cards to their employees and contractors and manage identity and other attributes about these people
- Commercial and non-US mission partners that issue PKI certificate based credentials to their users
- External IdPs that authenticate external credentials including PKI certificate based, MFA based, and username/password based and generate assertions that are passed to the DoD
- Cloud-based SaaS vendors who consume assertions from DoD IdPs and manage authentication and authorization decisions inside the cloud

Prior to relying on external providers, DoD must ensure the following:

- The service provider has been approved.
    - For enterprise ICAM service providers, the DoD CIO manages the approval
    - For component, COI, and local external service providers, approval may be managed by the DoD CIO or by the component depending on the type of service being provided and the overall risk to the DoD enterprise
    - Approval may be implemented through a specific Memorandum of Approval, by leveraging an existing agreement, or as part of a contractual arrangement with the service provider
    - Approval will generally be based on the service provider meeting an agreed upon set of minimum standards – which may be verified by an independent testing capability or self-asserted
- The service provider uses standards-based interfaces that do not place an undue burden on DoD relying parties to accept
- The service provider's own operations are performed using appropriate security measures depending on the level of sensitivity of the DoD resources that will be accessed leveraging capabilities from the service provider

7. Summary of ICAM Service Gaps

Table 5 provides a summary of identified ICAM capability gaps in currently available DoD ICAM enterprise services.

Table 5 – Summary of DoD ICAM Enterprise Capability Gaps

Capability	Gaps
General Gaps	
General	• Processes for ensuring resiliency and dynamic adaptability are not defined.
General	• Enterprise ICAM services are not available on the various Combatant Command and MPCO-managed Secret Releasable environments.
C1. Core ICAM Capabilities	
C1.1. Identity Management	
C1.1.1. Person Entity	• Processes to provision attributes and entitlements beyond core identity attributes are decentralized and manual. • Attributes and values for commonly used attributes are not normalized across the DoD enterprise. • The DoD has only limited enterprise services for attribute services. • Minimum requirements for specific types of privileged users are not defined across the DoD Enterprise. • Managing attributes to support authorization at the scale needed is not well supported for enterprise deployments of SaaS cloud solutions. • Capabilities and standards for managing identities across classification domains are not well defined.
C1.1.2. Non-Person Entity	• Enterprise registration and naming capabilities for NPEs are lacking. • Enterprise attributes for NPEs are not defined or normalized across the DoD enterprise. • No plans to develop an Enterprise Data Repository that can manage person entities and NPEs. • Identity vetting and provenance processes and capabilities do not exist for short lived NPEs.
C1.1.3. Federated Entity	• The DoD does not have an enterprise ICAM service for registering mission partner entities. • Because there is no DoD enterprise service for registering mission partner entities, mapping attributes to mission partner entities is lacking or only performed at a local level.
C1.2. Credential Management	
C1.2.1. Internal Credential Management	• Fully automated processes for issuing and managing credentials for NPEs are lacking. • DS Logon does not support MFA credentials.

Capability	Gaps
	• Processes and capabilities for issuance and validation of short term credentials for short lived NPEs do not exist.
C1.2.2. External Credential Registration	• DoD does not have an enterprise registration capability for mission partner entities that have DoD approved external credentials. • DS Logon does not support registering externally issued and managed credentials for beneficiaries.
C1.3. Access Management	
C1.3.1. Resource Access Management	• Resource labeling is only performed by a limited number of COIs, and the development and implementation of digital policy rules for access to resources is even more limited. • The lack of defined digital policy rules is a primary deterrent to the expanded implementation of dynamic access. • No plans to develop enterprise services for developing and managing digital policies. • No plans to develop an enterprise digital policy store.
C1.3.2. Provisioning	• DoD does not have an enterprise service to support entitlement provisioning and de-provisioning. • Manual provisioning and de-provisioning processes require significant processing time, delaying access to required resources. • DoD lacks a consistent standards-based approach for provisioning and de-provisioning entities to SaaS information systems. • The lack of availability of authorization attributes limits the implementation of dynamic provisioning. • Linking mission partner digital identities and attributes to their federated credentials results in an inability for mission partner entities to access many resources that they should be authorized for. • Software defined networking to enable dynamic provisioning and de-provisioning of network connections to support ZT architectures is lacking. • Processes and capabilities for provisioning entitlements for short lived NPEs do not exist.
C1.3.3. Authentication	• DoD resources that require a DoD issued EDIPI as the unique identifier for person entities are unable to authenticate mission partner entities with externally issued credentials that do not have EDIPIs as their identifiers. • DoD does not provide an enterprise IdP capability that accommodates DoD internal and mission partners entities with approved external credentials. • IdPs that have been implemented by Components or COIs do not always support authentication of DoD mission partner entities. • Relying party information systems are not configured to accept and process authentication assertions in lieu of performing direct credential

Capability	Gaps
	validation, limiting their ability to consume capabilities from DoD enterprise ICAM services and limiting the ability to authenticate mission partner entities because of the complexity of authenticating mission partner credentials. • Because many relying party information systems are not configured to securely process authentication assertions in lieu of performing direct credential validation, ICAM services have been deployed that create a new PKI digital certificate for the mission partner entity that can be presented to the relying party. Migrating to assertion based authentication can eliminate the need for operating CAs at the boundary while still maintaining attribution of who requested the resource and supporting the need to inspect information as it crosses the boundary. • Enclave gateway and CDS functionality is limited and may not support the verification of assertions, recreation of the assertion, and digital signature of the recreated assertion. • Information systems currently in use across the DoD are not configured to support PAM tools for IT privilege user authentication.
C1.3.4. Authorization	• Processes for sharing attributes beyond those asserted in credentials certificates are lacking. • Enterprise standards and policies for NPEs are lacking, resulting in limited ability for NPEs to access resources. • Access policy management, decision, and enforcement points are not deployed as enterprise ICAM services. • Relying party information systems are not configured to externalize access decisions. • The lack of availability of authorization attributes limits the implementation of dynamic provisioning and ABAC. • Implementing dynamic access will require resource labeling, but the DoD lacks an actionable strategy for implementing data tagging that fully supports ICAM. • No plans to develop an enterprise PDP. • No plans to support federated access management for mission partner entities. • Workflows within the relying party information systems must be configured to require dual-approval of changes for privileged actions where appropriate. Not all relying parties support such configuration. • Workflows within functional management tools must be configured to require dual-approvals for privileged actions where appropriate. This configuration is typically performed locally and is impractical to automate at the enterprise level. • Most mission partners do not have IdPs implemented that can generate assertions, and DoD relying parties are not configured to consume IdP assertions from external mission partners. These assertions could

Capability	Gaps
	potentially include attributes in addition to identity information that could support authorization decisions. • Registering a relationship to allow an individual to act on behalf of a beneficiary is not generally supported today, although beneficiaries may act on behalf of their dependent beneficiaries as a result of the dependency relationship.
C2. Access Accountability	
C2.1. Log Collection and Consolidation	• Standards and processes for collecting and correlating ICAM related logs have not been deployed at the DoD enterprise level. • Capabilities for privileged user monitoring are currently implemented at the Component or COI level, no enterprise services exist. • No plans to develop an enterprise service for log management, collection, and consolidation service.
C2.2. Access Review	• Consolidation of entitlement information is not available as a DoD enterprise ICAM capability, resulting in a lack of ability to perform access reviews except at the relying party information system level. • No plans to develop an enterprise service to support reporting and analysis. • Access reviews are not performed when person entity roles change. • Access reviews are not consistently performed for both person entities and NPEs.
C2.3. Identity Resolution	• Identity resolution capabilities for mission partner entities are not implemented at the DoD enterprise level. • Local identities are not linked to existing DoD identities. • Individual accountability can be limited in tactical DDIL environments since many systems implement group authentication without traceability back to enterprise managed identities.
C3. Contact Data	
C3.1. Contact Data Collection	• Contact data collection for NPEs and mission partner entities is limited.
C3.2. Contact Data Lookup	• Contact data lookup for NPEs and mission partner entities is limited.

Attachment A. Mapping ICAM Capabilities to the FICAM Architecture

Table 6 maps the services defined in the FICAM Architecture to the ICAM capability taxonomy. Access accountability capabilities and Contact Data Capabilities are not in scope for the FICAM Architecture.

Table 6 – Mapping of ICAM Capabilities to FICAM Architecture Services

FICAM Architecture Service		ICAM Capability
Identity Management	**The set of practices that allow an organization to establish, maintain, and terminate identities.**	**C1.1 Identity Management**
Identity Proofing	Verifying information to establish the identity of a person or entity	C1.2.1 Internal Credential Management
Creation	Establishing a digital identity composed of attributes that define a person or entity	C1.1.1 Person Entity C1.1.2 NPE
Maintenance	Maintaining accurate and current attributes within an identity record over its life cycle	C1.1.1 Person Entity C1.1.2 NPE
Identity Resolution	Finding and connecting disparate identity records for the same person or entity	C2.3 Identity Resolution
Deactivation	Deactivating or removing an identity record	C1.1.1 Person Entity C1.1.2 NPE
Credential Management	**The set of practices that an organization uses to issue, track, update, and revoke credentials for identities within their context.**	**C1.2 Credential Management**
Sponsorship	Formally establishing that a person or entity requires a credential	C1.2.1 Internal Credential Management
Registration	Collecting the information needed from a person or entity to issue them a credential	C1.1.1 Person Entity C1.1.2 NPE
Issuance	Transferring a credential to a person or entity	C1.2.1 Internal Credential Management
Maintenance	Maintaining a credential over its life cycle	C1.2.1 Internal Credential Management
Revocation	Withdrawing a credential from a person or entity	C1.2.1 Internal Credential Management
Access Management	**The set of practices that enables only those permitted the ability to perform an action on a particular resource.**	**C1.3 Access Management**
Policy Administration	Creating and maintaining the rule sets that govern access to protected resources	C1.3.1 Resource Management
Entitlement Management	Establishing and maintaining the authoritative access permissions for a person or entity	C1.3.2 Provisioning
Provisioning	Linking and unlinking access permissions for a person or entity to a protected resource	C1.3.2 Provisioning

	FICAM Architecture Service	ICAM Capability
Authentication	Verifying that a claimed identity is genuine based on valid credentials	C1.3.3 Authentication
Authorization	Granting or denying access requests to protected resources based on a policy determination	C1.3.4 Authorization
Federation	**The ability of one organization to accept another organization's work**	**C1.1.3 Federated Entity** **C1.2.2 External Credential Registration** **C1.3 Access Management**
Attribute Exchange	Discovering and sharing identity attributes between different systems to promote interoperability and simplify the process for establishing an identity	C1.1.3 Federated Entity
Credential Bridging	Transforming a token or credential into an alternative format, potentially containing claims about the client, for acceptance at a relying party	C1.3.3.Authentication
Credential Translation	Establishing a cross-certified, affiliated relationship to trust credentials at a level of assurance asserted by those credentials	C1.3.3 Authentication
Policy Alignment	Establishing a mutual relationship between parties by deliberately establishing common standards and principles	C1.1.3 Federated Entity C1.2.2 External Credential Registration
Governance	**The set of practices that allow organizations to administer and support the successful execution of the core ICAM services and functions**	**N/A**
Enterprise Governance	Developing and implementing the policies, rules, and procedures to manage and improve an ICAM program	Section 6
Auditing and Reporting	Monitoring, reviewing, and reporting on an ICAM program's conformance with rules, policies, and requirements	C2 Access Accountability for general auditing and reporting N/A for ICAM services as this is a system specific requirement
Redress	Fixing problems and vulnerabilities that occur during standard operation of an ICAM program	N/A – System specific requirement
Recovery	Preparing the procedures and assets that would be needed to recover from a security or privacy breach and ensure continuity of service	N/A – System specific requirement

Attachment B. ICAM and the Risk Management Framework

Table 7– Mapping NIST SP 800-53 Controls to ICAMTable 7 maps ICAM to security controls defined in NIST SP 800-53.

Table 7– Mapping NIST SP 800-53 Controls to ICAM

Security Control	Section	ICAM Reference Design Related Text
Family: Access Control (AC)		
AC-1 - Access Control	6.3	Components are also responsible for operating COI and local ICAM services that comply with DoD enterprise technical and process standards
AC-2 - Account Management	4.2.3	Allow access to privileged user accounts only through Privileged Account Management (PAM) tools that control access to privileged user accounts, monitor behavior, and log activity
AC-3 - Access Enforcement	4.1.1	Finally, the entity must be provisioned for appropriate physical and logical access by linking authorization attributes to the entity based on its identifier, and by provisioning entitlements to the entity.
AC-4 - Information Flow Enforcement	3.1.2.2	Entities whose identity is managed outside of the DoD and who are issued credentials by external approved credential providers may be registered in an entity data repository in order to use their external credentials to authenticate for access to DoD resources that require provisioned access, or when DoD managed attributes are associated with the entity that are needed for resolving dynamic access policy rules.
AC-5 - Separation of Duties	4.3.2	The DoD financial audit requires a review of entitlements for users of in-scope financial information systems to verify that users only have accesses they required to perform their job functions, and that no user's accesses violate separation of duty rules either within a single information system or across multiple information systems.
AC-6 - Least Privilege	Attach-ment B	Because of the prevalence of CAC based authentication and authorization, people who have been issued CACs have access to a broad range of DoD resources, many of which are not required for DoD or mission partner person entities to perform their job function. This broad access violates the principle of least privilege and presents a security risk.
AC-12 -Session Termination	4.2.4	At end of session, connection is de-provisioned
AC-14 - Permitted Actions Without Identification or Authentication	4.3.3	Local identities are often established without ever attempting to link the identities to DoD identities. Even if a DoD-wide authenticator is checked at the time of registration (e.g., vet a person's identity using a CAC), the local system uses a different way of identifying the person (e.g., first initial, last name for the user name); creating a new "person" without linking it to the existing DoD identity.

Security Control	Section	ICAM Reference Design Related Text
AC-16 - Security and Privacy Attributes	2.2.1.1 and throughout	Throughout the document
AC-17 - Remote Access	2.2.1.2	IAL2 introduces the need for either remote or physically-present identity proofing.
AC-19 - Access Control for Mobile Devices	5.2.7	Purebred, operated by DISA, supports the issuance of PKI based digital certificates to person entities and NPEs for use with internal DoD user assigned mobile devices with hardware backed key stores or security tokens. Purebred operates on the NIPRNet.
AC-20 - Use of External Systems	1.3.4	Some DoD information systems interact with external entities for a limited duration or purpose. Identity information for these entities is generally not managed at the DoD enterprise level, and these entities may require locally issued credentials.
AC-21 - Information Sharing	2.1	The resulting capabilities will facilitate information sharing across the DoD and with mission partners, while managing risks and protecting information against unauthorized access.
AC-24 - Access Control Decisions	2.2.2.1.3	Attributes from federated entities should only be used during authentication and authorization decisions by DoD information systems if the DoD has evaluated the attribute provider as meeting DoD data quality requirements.
Family: Awareness and Training (AT)		
AT-2 – Security Awareness Training	5.3.7	Automated Account Provisioning (AAP), in development by DISA, will provide identity governance services such as user entitlement management, business role auditing and enforcement, and account provisioning and de-provisioning based on identity data produced during DoD person-centric activities such as on and off-boarding, continuous vetting, talent management, and readiness training.
Family: Audit and Accountability		
AU-2 - Event Logging	2.2.2.1	Entire section
AU-6 - Audit Record Review, Analysis, and Reporting	3.2.1	These logs are then consolidated by a log management system and compared against provisioned entitlements or resource access policies for each entity. This consolidated log information can then be reviewed by an authorized reviewer for anomalous activity or provided to an authorized monitoring service.
AU-8 - Time Stamps	3.1.3.3	Other protections include timestamping the assertion, designating the intended recipient in the assertion, and encrypting the assertion with the intended recipient's public key.
AU-9 - Protection of Audit Information	3.1.3.3	Other protections include timestamping the assertion, designating the intended recipient in the assertion, and encrypting the assertion with the intended recipient's public key.

Security Control	Section	ICAM Reference Design Related Text
AU-13 - Monitoring for Information Disclosure	2.2.2.1	High confidentiality – logs are appropriately protected from unauthorized disclosure
Family: Security Assessment and Authorization		
CA-3 - Information Exchange	4.1.6	The public keys for each IdP operated by each mission partner participating in the information exchange are registered with the Mission Partner Gateway using an out-of-band mechanism such as manual in-person transfer. / Format of these identifiers must be defined as part of the agreement established between the mission partner and the DoD for information exchange.
Family: Configuration Management		
CM-7 - Least Functionality	6.2	Implement a process for collecting and prioritizing requirements for functionality enhancements to the service
CM-12 - Information Location	1.2	All DoD ICAM capabilities, functions, systems, elements and services implemented at any and all locations, from well-connected Continental United States (CONUS) and Outside Continental United States (OCONUS) environments, to tactical environments, including the most challenging and restricted denied, degraded, intermittent, or limited bandwidth (DDIL) environments.
Family: Identification and Authentication		
IA-2 - Identification and Authentication (Organizational User)	3.1.3.3	If the credential does not contain a persistent unique identifier, the information system requests the identifier linked to the credential from the entity data repository.
IA-3 - Device Identification and Authentication	2.2.1.1.2	For devices, identity attributes should include linking the NPE to its supply chain and acquisition process, registration and configuration by an authorized person entity, and maintenance of the device from registration through decommissioning and destruction.
IA-5 - Authenticator Management	2.2.1.2	Entire section
IA-7 - Cryptographic Module Authentication	2.2.1.2	Private keys may also be generated and stored using hybrid approaches where the key is generated in a software cryptographic module but then moved to a hardware module and the copy in software is deleted.
IA-8 - Identification and Authentication (Non-Organizational Users)	2.2.1.2.2	Entire section

Security Control	Section	ICAM Reference Design Related Text
IA-9 - Service Identification and Authentication	3.1.1.2	Entire section
IA-11 - Re-authentication	2.2.1.3.3	In addition, authentication should only be valid for a limited duration, and entities should be required to re-authenticate, especially after a period of inactivity. Appropriate duration is dependent on the information system and type of resource being accessed.
IA-12 - Identity Proofing	2.2.1.2	Identity proofing is performed prior to issuing a credential to an entity. Generally, identity proofing occurs after the digital identity has been created (see Section 2.2.1.1) and is used to bind the credential to the digital identity. NIST SP 800-63A defines three IALs for person entities.
Family: Physical and Environmental Protection Policy and Procedures		
PE-2 - Physical Access Authorizations	1	Provide access to and protection for DoD information systems and DoD electronic Physical Access Control Systems (PACS) resources
Family: Program Management		
PM-12 - Insider Threat Program	2.2.2	Although audit is out of scope for ICAM, access accountability capabilities provide information that can be used to support audits. For example, ICAM logs can be used to support insider threat detection, and access review is an important compensating control for financial audits.
PM-20 - Dissemination of Privacy Program Information	2.2.1.1	Because of security and privacy considerations, it is very important that the extent of the distribution of attributes be limited to what is required for specific ICAM operational capabilities. / Other considerations for determining the extent attributes should be distributed include privacy and legal considerations, operations security, and system performance, particularly when bandwidth is limited.
Family: Personnel Security		
PS-3	Multiple	Sections 2.2.1.2, 5.2.1, 5.2.3, 5.2.5, 5.2.9, and 5.3.1
PS-4 - Personnel Termination	3.1.1.1	When a person is no longer affiliated with the DoD enterprise, DoD Component, COI, or local information system, the digital identity must be deactivated
PS-7 - External Personnel Security	3.1.1.3	Where attribute exchange agreements exist, the external identity manager will notify the entity data repository of the identity deactivation using the process shown in Figure 10. External identity managers should also require revocation of all credentials issued to that entity when a digital identity is deactivated.

Security Control	Section	ICAM Reference Design Related Text
Family: Risk Assessment		
RA-3 - Risk Assessment	2.2.2.1	However, monitoring capabilities may rely, in part, on ICAM activity records as a source of information. In turn, monitoring capabilities can provide analytical data to information systems to support risk scores associated to entity activity.
RA-5 - Vulnerability Monitoring and Scanning	2.2.2.1	Although monitoring of entity activity is not a DoD ICAM capability, collection of ICAM event logs for a group of information systems in support of monitoring may be performed as part of ICAM
RA-9 - Criticality Analysis	2.2.1.3.1	Resource management and data tagging are not in scope for the ICAM Reference Design, but resource access management, including the ability to properly relate a resource to an ICAM process, is a critical dependency for proper access determination. The DoD is developing a Data Reference Architecture to address data resources, but for ICAM, the term resource is broader than data. A resource is anything to which an entity can request access.
Family: System and Services Acquisition		
SA-4 - Acquisition Process	2.2.1.1.2	Identity management for NPEs depends on the type of NPE. For devices, identity attributes should include linking the NPE to its supply chain and acquisition process, registration and configuration by an authorized person entity, and maintenance of the device from registration through decommissioning and destruction.
SA-9 External System Services	2.2.1	Because DoD does not operate or oversee the operations of these external services, DoD must make a determination whether the service is operated in a fashion that is appropriate for DoD relying parties to trust artifacts produced by the service. This determination requires that the service provider operates in accordance with an agreed upon set of minimum requirements.
SA-11 - Developer Testing and Evaluation	5.3.2	The Identity Provider (IdP), in development by DISA, will be a centralized authentication service for applications for both DoD issued and mission partner credentials, including username and password management, MFA credential authentication enablement and management, PKI certificate validation, and a token provider.
SA-15 - Development Process, Standards, and Tools	5.3.3	The Multi-Factor Authentication (MFA) Registration Service, in development by DMDC, will aggregate and combine DoD issued credentials for DoD internal community members and external credentials for mission partner entities into a single repository that supports the IdP for user authentication.
SA-23 - Specialization	2.2.2.1	ICAM operational and data capabilities must be implemented such that they do the following: • Link an entity's digital identity to their ICAM activity • Record that entity ICAM activity in ICAM event logs • Record other ICAM activity not directly associated with entity activity (i.e., modification of an access policy)

Security Control	Section	ICAM Reference Design Related Text
		• Enable authorized access to these ICAM event logs, as appropriate
Family: System and Communications Protection		
SC-2 - Separation of System and User Functionality	4.3.2	The DoD financial audit requires a review of entitlements for users of in-scope financial information systems to verify that users only have accesses they required to perform their job functions, and that no user's accesses violate separation of duty rules either within a single information system or across multiple information systems.
SC-4 - Information in Shared System Resources	5.3.1	The Mission Partner Registration (MPR), in development by DMDC, will allow DoD government personnel to sponsor DoD mission partner identities and register their identifiers so that identity can be shared across the DoD ICAM architecture in a similar fashion to DoD personnel.
SC-7 - Boundary Protection	4.1.6	(Gap) (Acknowledged) Migrating to assertion based authentication can eliminate the need for operating CAs at the boundary while still maintaining attribution of who requested the resource and supporting the need to inspect information as it crosses the boundary.
SC-10	3	For disconnected or intermittently connected systems, the services shown would either be locally managed and operated or would use local services that periodically obtain and cache data from enterprise services.
SC-12 Cryptographic Key Establishment and Management	4.1.6	The public keys for each IdP operated by each mission partner participating in the information exchange are registered with the Mission Partner Gateway using an out-of-band mechanism such as manual in-person transfer. These public keys are needed to be able to validate assertions provided by the IdPs.
SC-13 - Cryptographic Protection	2.2.1.2	Private keys are protected in cryptographic modules that are under the control of the entity named in the certificate. Private keys may be generated and protected in software cryptographic modules that permit copying the private key, and are considered AAL2.
SC-37 - Out-of-Band Channels	4.1.6	The public keys for each IdP operated by each mission partner participating in the information exchange are registered with the Mission Partner Gateway using an out-of-band mechanism such as manual in-person transfer. These public keys are needed to be able to validate assertions provided by the IdPs
Family: System and Information Security		
SI-4 – Information System Monitoring	Table 5	(Gap) (Acknowledged) Capabilities for privileged user monitoring are currently implemented at the Component or COI level, no enterprise services exist.

Security Control	Section	ICAM Reference Design Related Text
Family: Supply Chain Risk Management		
SR-4 - Provenance	4.1.7	(Gap) (Acknowledged) Processes and capabilities for short lived NPEs do not exist, including identity vetting/provenance, issuance and validation of short term credentials, and provisioning entitlements.

Attachment C. Case Study: Moving Beyond CAC Authentication and Authorization

Information systems across the DoD have implemented access based on the user presenting a PKI certificate from a CAC. For many of these systems, the ability to authenticate via the CAC also serves as the only authorization needed to access resources hosted on those systems. Users with a CAC have access, and users without a CAC cannot gain access to these systems. Implementing CAC based authentication and authorization was seen as a straightforward mechanism for meeting DoD mandates to use PKI for authentication. However, this migration to CAC based authentication and authorization has resulted in some significant issues for the DoD.

- Mission partner person entities are authorized to obtain CACs simply because they need to access one or more DoD managed information systems, even if these users do not need regular physical access to DoD facilities and are not provisioned for DoD network accounts. Managing identities and issuing credentials for these users has a significant cost, both in terms of personnel time and in terms of licensing and card purchasing.
- Because of the prevalence of CAC based authentication and authorization, people who have been issued CACs have access to a broad range of DoD resources, many of which are not required for DoD or mission partner person entities to perform their job function. This broad access violates the principle of least privilege and presents a security risk.
- People who do not use a DoD issued workstation to perform their regular duties must manage the CAC as well as their corporate credentials when accessing DoD. Although not a significant challenge, this requirement does degrade the user experience, especially for users who already have smart-card based PKI credentials for their corporate credentials.
- Mission partner person entities who are unable to obtain CACs are not able to access DoD resources that they require to perform their job function and would otherwise be authorized to access.

Adoption of CAC based authentication and authorization may be based on the overall ease of implementation, but the CAC also performs a number of functions that may be needed in making an access decision, either directly or indirectly. Moving away from CAC based authentication and authorization will require deploying DoD enterprise ICAM services that can perform these same functions for federated mission partner credentials. These functions include:

- Knowledge that the authentication is based on a high assurance (AAL3) credential
- Knowledge that the authentication is based on high assurance (IAL2) identity proofing
- Presentation of a unique identifier, either the full DN or the EDIPI (note that some systems are using email address; however CACs issued after August of 2020 will only allow use of the authentication certificate which does not contain an email address)
- Indication that the user has a successfully adjudicated background investigation
- Proof of a current relationship with the DoD
- Real time credential validation
- No cost to the information system owner for issuing or managing the CAC (costs are incurred at the DoD Component level)

- No requirement for managing an access control list

Migration from CAC based authentication and authorization will require the deployment of planned DoD enterprise ICAM services, but it will also require information systems owners to modify their approach authentication and authorization. Table 8 provides a listing of enterprise service capabilities and sample information system modifications to leverage these enterprise services to support authentication and authorization for CAC holders and mission partner entities.

Table 8 – Sample Modifications to Support Mission Partner Entity Access

Action	Enterprise Service Support	Information System Modifications
Authentication		
Authentication	• IdP either directly validates mission partner credential by interfacing with the appropriate credential service provider or validates an assertion from the mission partner's IdP • IdP generates an assertion that contains the mission partner entity's identifier and the IAL and AAL used for the initial authentication	• Information system receives and validates assertion from the IdP for authentication
Authorization		
Local Authorization	• MPR registers mission partner entity	• Information system implements local authorization and registers mission partner entity access request • Information system manually verifies DoD sponsorship or other attributes needed
Enterprise Supported Authorization	• AAP provides an interface for requesting and approving access to application • MPR registers mission partner entity and provides a mechanism for linking mission partner identifier to attributes from mission partner's identity manager and from DoD systems such as JPAS/DISS • AAP automates access approval where attributes are available, and supports manual approval where needed	• Information system redirects access request to AAP if user is not already authorized for access • Information system receives access entitlement from AAP

Action	Enterprise Service Support	Information System Modifications
	• AAP pushes entitlement to information system	
Dynamic Access using ABAC	• MPR registers mission partner entity and provides a mechanism for linking mission partner identifier to attributes from mission partner's identity manager and from DoD systems such as JPAS/DISS • EIAS provides additional attributes that may be required • Digital policy service hosts digital policy required for access to resource • PDP obtains digital policy and attributes needed to resolve access request • PDP provides access approval or denial to information system to the PEP	• Information system owner develops digital policy rules for access to resources • Information system owner updates the system to accept and validate the assertion from the PDP • Information system owner labels resources to connect them to digital policy rules • Information system either implements a PEP or connects system to a COI PEP • Information system redirects all access requests to the PEP • PEP redirects all access requests to the PDP

Attachment D. DoD Internal Community Persona Type Codes

Table 9 provides the list of PTCs assigned to personas by the PDR as defined in the DoD Naming Convention for People within DoD Identity, Credential, and Access Management.

Table 9 – Persona Type Codes

Personnel Type Definition	Type Code
Active Duty member	MIL
Academy student (USAFA, USCGA, USMA, USMMA, USNA)	MIL
ROTC (under contract)	MIL
National Guard member (on active duty)	MIL
National Guard member (SEL RES)	MIL
National Guard member (IRR)	MIL
Reserve member (on active duty)	MIL
Reserve member (SEL RES)	MIL
Reserve member (RES RET)	MIL
Reserve member (IRR)	MIL
Presidential Appointee (any Federal Agency)	CIV
DoD/Uniformed Service Civil Service employee	CIV
Non-DoD Civil Service employee (other federal agency)	CIV
Non-federal civilian associates (State employees of NGB)	NFG
Non-federal civilian associates (Red Cross)	NGO
Non-federal civilian associates (USO)	USO
DoD or Uniformed Service Contract employee	CTR
Non-DoD Contract employee (other federal agency)	CTR
DoD OCONUS hires (local national DoD employee)	LN
Foreign Military	FM
Foreign Civilian	FN
Non-Appropriated fund DoD/Uniformed Service employee	NAF
Former/Retired Military Member (receiving retired pay)	RET
Former Military Member discharged under honorable conditions and not retired	VET
Civilian Retiree	CVR
Non-federal civilian affiliate (volunteer)	VOL
Medal of Honor Recipient	MOH
Current Beneficiary (sponsor level)	BEN
Current family member	BEN
No known current association with the DoD	NCA

Attachment E. Non-Person Entity Type Codes

Reserved for future version

Attachment F. Core Authorization Attributes

Reserved for future version

Attachment G. Glossary of Terms

The terms used in this DoD ICAM RD remain consistent with ICAM-related language in other documents and architectures, particularly FICAM architecture. Table 10 provides a glossary of terms used within this document.

Table 10 – Glossary

Term	Description
Access Management	The set of practices that enables only those permitted the ability to perform an action on a particular resource. *--FICAM Architecture*
Access Review	Review of the appropriateness of user access privileges to address audit requirements and reduce risks.
Approver	An entity who is authorized to approve the creation and maintenance of digital identities and attributes associated with those identities.
Assertion	A digitally signed data artifact that contains the identifier of the entity that has been authenticated by the IdP, the IAL and AAL of the original authentication, and can optionally contain other attributes about the entity.
Assurance Level	The grounds for confidence that the set of intended security are effective in their application. *-- CNSSI 4009*
Attribute	A quality or characteristic ascribed to someone or something. *-- NIST SP 800-63*
Attribute Based Access Control (ABAC)	An access control paradigm whereby access rights are granted to users through the use of policies which combine attributes together. The policies can use any type of attributes. (Also see Role Based Access Control) *-- NIST CSRC Glossary*
Attribute Service	A data repository where authorization attributes are collected and managed for a set of entities that is recognized as having the authority to verify the association of attributes to an identity, accessible only through a service that both provisions and serves up authorization attributes.
Authentication	The process by which a claimed identity is confirmed, generally through the use of a credential. --FICAM Architecture
Authenticator	Something that the Claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the Claimant's identity *-- NIST SP 800-63*
Authenticator Assurance Level (AAL)	A category describing the strength of the authentication process. *-- NIST SP 800-63*

Term	Description
Authoritative Attribute Source	A data repository where authorization attributes are on-boarded and managed for a set of entities.
Authorization	The process by which a request to perform an action on a resource is decided, typically based on a policy. (Also see Access Management) *-- FICAM Architecture*
Authorization Attribute	An attribute used in authorization decisions.
Beneficiary	Any person eligible for benefits under the provisions of chapter 55 of Title 10, United States Code, which will generally include active duty Service members, retirees, certain reserve and national guard members, and eligible dependents and survivors. *-- DoD Manual 6025.13*
Certificate	See public key certificate
Cloud Service Provider	An organization that provides cloud services. *-- NIST CSRC Glossary*
Community of Interest (COI)	A collaborative group of users who exchange information in pursuit of their shared goals, interests, missions, or business processes. *-- NIST CSRC Glossary*
Contact Attribute	An attribute used by contact data lookup services to provide information about an entity.
Contact Data Repository	A data repository that hosts contact information for a set of person entities, resources, and NPEs.
Credential	An object or data structure that authoritatively binds an identity - via an identifier or identifiers - and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber. While common usage often assumes that the subscriber maintains the credential, these guidelines also use the term to refer to electronic records maintained by the CSP that establish binding between the subscriber's authenticator(s) and identity. *-- NIST SP 800-63*
Credential Management	The set of practices that an organization uses to issue, track, update, and revoke credentials for identities within their context. *--FICAM Architecture*
Credential Service Provider (CSP)	A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. *-- NIST SP 800-63*
Denied Degraded Intermittent or Limited (DDIL) Bandwidth Environment	Any environment where high bandwidth high availability connectivity to the DoDIN is not consistently available.

Term	Description
Derived Credential	Credentials that are issued based on electronic authentication of an existing credential, and may have a different form factor than the original credential.
Digital Certificate	See Public Key Certificate
Digital Identity	The digital representation of an identity including an identifier and a set of attribute values about the identity.
Digital Policy Rule	A rule that defines the combination of attributes under which an access may take place *-- CNSSI 4009 ABAC*
DoD Internal Community	All people who are eligible for fully provisioned network accounts on NIPRNet or SIPRNet as a requirement of performing their job function, and NPEs (NPE) that are fully managed by the DoD.
DoDIN	The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. *-- CNSSI 4009*
Entitlement	Authorization to access one or more resources within an information system
Entitlement Provisioning Service	A data repository that stores entitlements for a set of entities, provides an interface for managing those entitlements, and provides entitlements to information systems. This repository is accessible only through the service that both provisions and serves up entitlements.
Entity	A person, role, organization, device, or process that requests access to and uses resources.
Entity Data Repository (PDR)	A data repository that holds identifiers, credential information, and other attributes for a set of entities.
Federated Entity	An entity whose identity is managed external to the DoD enterprise but who possesses a credential and potentially attributes managed external to the DoD that are approved for use within the DoD.
Federation	The ability of one organization to accept another organization's work. Federation is based on inter-organizational trust. The trusting organization has to be comfortable that the trusted organization has similar policies, and that those policies are being followed. *-- FICAM Architecture*
Federation Assurance Level (FAL)	A category describing the assertion protocol used by a federation to communicate authentication and attribute information (if applicable) to a relying party.

Term	Description
	-- *NIST SP 800-63*
Functional Privileged User	A user who has approval authorities within workflows. Functional privileged user roles are specific to a mission area, such as Human Resources or Finance. (Also see Privileged User)
Identifier	Unique attribute that can be used to locate a specific identity within its context *--FICAM Architecture*
Identity	The set of characteristics (also called "attributes") that describe an entity within a given context. (Also see Digital Identity) *--FICAM Architecture*
Identity Assurance Level (IAL)	The degree of confidence that the applicant's claimed identity is their real identity. -- *NIST SP 800-63*
Identity Attribute	An attribute containing identity information, (Also see Attribute)
Identity Credential and Access Management (ICAM)	The set of security disciplines that allows an organization to enable the right entity to access the right resource at the right time for the right reason. It is the tools, policies, and systems that allow an organization to manage, monitor, and secure access to protected resources. These resources may be electronic files, computer systems, or physical resources such as server rooms and buildings. *--FICAM Architecture*
Identity Management	The set of practices that allow an organization to establish, maintain, and terminate identities. *--FICAM Architecture*
Identity Manager	A data repository where identity related attributes are collected and managed for a set of entities
Identity Proofing	The process by which a CSP collects, validates, and verifies information about a person. -- *NIST SP 800-63*
Identity Provider (IdP)	A system that performs direct authentication of entities based on their credentials and issues assertions derived from those credentials. Assertions may contain attribute information in addition to identity information.
Identity Resolution	Finding and connecting disparate identity records for the same person or entity. *--FICAM Architecture*
Information System	An IT system that hosts one or more resources.
IT Privileged User	A user who has roles that allow read, write, or change access to manage IT systems including system, network, or database administrators; and security analysts who manage audit logs. IT privileged user roles are generic

Term	Description
	to all IT infrastructure, including transport, hosting environments, cybersecurity, and application deployment. (Also see Privileged User)
Local Identity Manager	A data repository where identity related attributes are on-boarded and managed for a set of entities.
Log Management System	A data repository that hosts ICAM related event logs.
Manager	A person entity who has supervisory authority over an entity.
Master User Record (MUR)	A data repository that hosts a record of all entitlements entities have been granted.
Mission Partner	An organization with which the DoD cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; State and local governments; allies, coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector
Mission Partner Entity	A person entity or NPE who is a member of a DoD mission partner
Multi-Factor Authentication (MFA)	A characteristic of an authentication system or an authenticator that requires more than one distinct authentication factor for successful authentication. MFA can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors. *-- NIST SP 800-63*
Non-Person Entity (NPE)	A physical device, virtual machine, system, service, or process that is assigned an identifier and may be issued credentials to support authentication and authorization.
Person Entity	An individual acting as themselves or in the capacity of a role that is assigned an identifier, assigned attributes, issued credentials, and provided with entitlements to support authentication and authorization.
Persona	An electronic identity that can be unambiguously associated with a single person or non-person entity (NPE). A single person or NPE may have multiple personas, with each persona being managed by the same or different organizations *-- NIST CSRC Glossary*
Policy Decision Point (PDP)	Mechanism that examines requests to access resources, and compares them to the policy that applies to all requests for accessing that resource to determine whether specific access should be granted to the particular requester who issued the request under consideration. *-- NIST CSRC Glossary*
Policy Enforcement Point (PEP)	A system entity that requests and subsequently enforces authorization decisions.

Term	Description
	-- *NIST CSRC Glossary*
Privileged User	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. (Also see IT Privileged User, Functional Privileged User) – *NIST CSRC Glossary*
Provisioning	Linking and unlinking access permissions for a person or entity to a protected resource. -- *FICAM Architecture*
Public Key Certificate	A digital document issued and digitally signed by the private key of a certificate authority that binds an identifier to a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key. -- *NIST SP 800-63*
Public Key Infrastructure (PKI)	A set of 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, and revoke public key certificates. -- *NIST SP 800-63*
Registration	Creation of a new digital identity for an entity including and assigning one or more credentials to that entity or of a link between an existing digital identity from a federated context to a potentially different identifier within the DoD enterprise, COI, or local context.
Relying Party	An entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system. (Also see Information System) – *NIST SP 800-63*
Requestor	An entity requesting that another entity be authorized access to a resource. The requestor may be the entity that is requesting access or may be another person or NPE requesting the access on the entity's behalf.
Resource Attribute	Attribute applied to a resource rather than to an entity.
Resource Owner	A person entity or organization that is responsible for a resource.
Resource Policy Service	A data repository where digital policy rules governing access to resources are stored.
Reverse Proxy Identity Provider (IdP)	A system that performs direct authentication and optionally authorization on behalf of one or more information systems.
Reviewer	A person or NPE responsible for reviewing ICAM related logs.
Role	A job function or employment position to which person entities or other system entities may be assigned in a system. -- *NIST CSRC Glossary*

Term	Description
Role Based Access Control (RBAC)	A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities. (Also see Attribute Based Access Control) -- *NIST CSRC Glossary*
Sponsor	A person entity who is responsible for the operations and actions of an NPE or other person entity.
Transaction	A discrete event between user and systems that supports a business or programmatic purpose.
Zero Trust (ZT)	Zero Trust is an IT security model that requires strict identity verification for every person and device trying to access resources on a network, regardless of whether they are accessing from within or outside of the network perimeter.

Attachment H. Acronyms

AAL	Authenticator Assurance Level
AAP	Automated Account Provisioning
ABAC	Attribute-Based Access Control]
AC	Access Control
ACL	Access Control List
ALT	Alternative Login Token
ATIMS	Alternate Token Issuance and Management System
BAE	Backend Attribute Exchange
BBS	Batch Broker Service
CA	Certification Authority
CAC	Common Access Card
CCEB	Combined Communications Electronic Board
CDS	Cross Domain Solution
CJCS	Chairman of the Joint Chiefs of Staff
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
COI	Community of Interest
CONUS	Continental United States
CRL	Certificate Revocation List
CSP	Credential Service Provider
CSRC	Computer Security Resource Center
CSSP	Cybersecurity Service Provider
CUI	Controlled Unclassified Information
CV	Capability Viewpoint
DDIL	Denied, Degraded, Intermittent, or Limited Bandwidth
DISA	Defense Information Systems Agency
DISS	Defense Information System for Security
DNI	Director of National Intelligence
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DMDC	Defense Manpower Data Center
DMZ	De-Militarized Zone
DoD	Department of Defense
DoDAF	DoD Architecture Framework

DoDIN	DoD Information Networks
DREN	Defense Research and Engineering Network
DS	DoD Self-service
ECA	External Certification Authority
EDIPI	Electronic Data Interchange Person Identifier
EDQS	Enterprise Directory Query Service
EDR	Entity Data Repository
EDS	Enterprise Directory Services
EIAS	Enterprise Identity Attribute Service
ETL	Extract, Transform, and Load
EUN	Enterprise Username
EXCOM	Executive Committee
FAL	Federation Assurance Level
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standard
GDS	Global Directory Service
HSPD	Homeland Security Presidential Directive
IA	Identity and Authentication
IAL	Identity Assurance Level
IC	Intelligence Community
ICAM	Identity, Credential, and Access Management
ICD	Intelligence Community Directive
IdAM	Identity and Access Management (term replaced by ICAM)
IDMI	IdSS Machine Interface
IdSS	Identity Synchronization Service
IdP	Identity Provider
IP	Internet Protocol
IT	Information Technology
JIE	Joint Information Environment
JPAS	Joint Personnel Adjudication System
JPIO	Joint Program Integration Office
JWICS	Joint Worldwide Intelligence Communications System
LDAP	Lightweight Directory Access Protocol
MFA	Multi-Factor Authentication
MOA	Memorandum of Agreement

MPE	Mission Partner Environment
MPR	Mission Partner Registration
MUR	Master User Record
NEATS	NIPRNet Enterprise Alternate Token System
NGO	Non-Governmental Organiztion
NIPRNet	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
NSA	National Security Agency
NSS	National Security System
OCONUS	Outside the Continental United States
OCSP	Online Certificate Status Protocol
OIG	Office of the Inspector General
OLT	Only Locally Trusted
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
OV	Operational Viewpoint
PACS	Physical Access Control System
PAM	Privilege Access Management
PDP	Policy Decision Point
PDN	Persona Display Name
PDR	Person Data Repository
PEP	Policy Enforcement Point
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIT	Platform Information Technology
PIV	Person Identity Verification
PIV-I	PIV Interoperable
PKI	Public Key Infrastructure
PTC	Person Type Code
RAPIDS	Real-time Automated Personnel Identification System
RBAC	Role Based Access Control
RBS	Real-time Broker Service
RD	Reference Design

RMF	Risk Management Framework
SaaS	Software as a Service
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SvcV	Service View
SD	Service Description
SDN	Software Defined Network
SDREN	Secret Defense Research and Engineering Network
SIPRNet	Secret Internet Protocol Router Network
SIPR REL	SIPRNet Releasable
SOC	Security Operations Center
SORN	System of Records Notice
SP	Special Publication
TAD	Technical Architecture Description
TASS	Trusted Associate Sponsorship System
US	United States
USBICES	US Battlefield Information Collection and Exploitation System
USCYBERCOM	US Cyber Command
ZT	Zero Trust