U.S. Army – Identity and Access Management (IdAM) Reference Architecture (RA)

(Aligned to the DOD Enterprise)

Version 3.0 7 May 2014

Executive Summary

The Army Identity and Access Management (IdAM) Reference Architecture (RA) V3.0 is a collection of strategic-level architecture views with the purpose of guiding and constraining Army enterprise and component solutions. The architecture contained within this document is intended to provide a clear description of what the Army IdAM must be and how its elements should work together to deliver effective and efficient identity and access management guidance.

This IdAM RA is intended to complement the Army's existing identity management and protection capabilities, Common Access Card (CAC) and Public Key Infrastructure (PKI), which enable strong authentication of trusted entities prior to access authorization determination. This RA supports synchronized and responsive operations across the Joint Information Environment (JIE)[1] by ensuring person and non-person entities can securely access all authorized resources, anywhere, at any time.

In addition to IdAM alignment with mission partners, this RA shall support the Federal Identity, Credential, and Access Management (FICAM) segment architecture, guidance, and standards, which focus on ensuring interoperability with domestic and international mission partners and support applicable Executive and Federal guidance and mandates.[2]

Army IdAM RA v3.0 supersedes IdAM RA v2.0, and provides Army leadership and their supporting organizations expanded architectural guidance to support the design, development, deployment, transition to and operational management of a JIE IdAM service framework and infrastructure, while assuring IdAM services in all Army tactical operating environments.

LORENZO.GREGORY.ROBERT.1197874216

Digitally signed by LORENZO.GREGORY.ROBERT.1197874216
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=LORENZO.GREGORY.ROBERT.1197874216
Date: 2014.05.07 14:27:54 -04'00'

Gregory R. Lorenzo
Acting Director, Army Architecture Integration Center
Chief Information Officer/G-6

[1] The JIE, as approved by the Joint Chiefs of Staff on 6 August 2012, is defined as a secure joint information environment, comprised of shared IT infrastructure, enterprise services, and single security architecture to achieve full-spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies.
[2] Presidential Executive Order 13587, Homeland Security Presidential Directive – 12 (HSPD-12), FICAM Roadmap and Implementation Guidance Version 2.0

Table of Contents

Tables

Figures

1 Introduction

Identity management is the combination of technical systems, policies, and processes that create, define, govern, and synchronize the ownership, utilization, and safeguarding of identity information. The primary goal of identity management is to establish a trustworthy process for assigning attributes to a digital identity and to connect that identity to an individual.[3] To ensure the security of our facilities and information, we must be able to confirm the true identities of all of the human and non-human components involved. These include people (e.g., Soldiers, Commanders and any/all Department of Defense (DOD) information consumers), computing/communications devices, networks, information systems, applications and data, as well as DOD and Service Component (SC) assets and other selected SC materiel (e.g., weapons systems, aircraft, ordnance). The use of automation and the ability to network computers, devices and the capabilities they provide has transformed how we fight. As a result, the Army's warfighting capability and ability to conduct the fight must be better, faster and, in many ways, safer, even as new cybersecurity risks arise and increase in number.

Historically, DOD, the Army and the other SCs have developed and deployed Identity and Access Management (IdAM) services in a stovepipe manner, where access to information or facilities was handled by the asset owner. Even with the use of the DOD Common Access Card (CAC) for user authentication via Public Key Infrastructure (PKI) technology, inconsistencies remain between how authenticated information requesters or consumers are identified and what they should or should not have access to (resource authorization). DOD and the SCs have not previously had the ability to control authorization granularly to the extent required to make resources available on a need-to-know basis, or to rapidly manage changes in elements describing both requesters and resources.

These capability gaps apply to both the tactical and non-tactical environments. In tactical environments, where networks that allow enterprise authoritative data sources and services to be used for IdAM are often unavailable, a secure and accurate disconnected IdAM capability is required. IdAM must also be dynamic in order to accommodate rapidly changing identity attributes, personas, roles and access accounts as battlefield environments change. Further, as Soldiers move from a sustaining base and are deployed in theater, they need continuous information access and other access types to follow them with completeness, accuracy and minimal risk. This requirement applies to all stages within SC generational and rotational cycles (e.g., throughout the Army Force Generation (ARFORGEN) cycle). A DOD enterprise-level, rules-based IdAM Reference Architecture (RA) that meets the needs of Joint, SC, coalition and

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

external partners will address the operational, capability and security gaps that currently exist.

1.1 Background

In addition to complex cyber and physical security threats, the Army faces significant challenges in being able to carry out its mission activities in a manner that fulfills the needs of its business partners and appropriately leverages current information technology capabilities to enable electronic service delivery. The IdAM challenge to the modern force is having the capability to provide full spectrum services during all operational phases to all organizations. Subsequently DOD adopted a strategy consisting of CAC or secure token for user "authentication" via Public Key Infrastructure (PKI) technology capability filling in gaps between how authenticated information "subscribers" or "consumers" are identified by IdAM providers and offer services to the resources (i.e., data, facilities, networks, equipment).

At the present time, DOD has reached a crossroads where it must assess the best way to provide IdAM services to all its personnel, regardless of the environment. The envisioned end state should enable any Soldier or authorized entity to access information or facilities at any time, based on identity and context, irrespective of physical location.

1.2 Direction

As DOD moves toward a Joint operations strategy, it must begin to transition to an enterprise IdAM services environment while allowing distributed tactical operations. This transition will enhance coalition and non-DOD-partner secure access, as well as internal DOD operations. An enterprise IdAM services environment presents many challenges, both technically and in terms of ensuring that overall resource security is preserved while providing more extensive IdAM capabilities. Well-planned and executed access policy management will be the key to achieving these objectives and is a major focus of this RA.

The purpose of IdAM RA v.1 and 2 was to establish an inventory of authoritative sources. These versions provided a list of specifications describing IdAM principles and rules. IdAM RA does not receive benefits from Enterprise Architecture (EA) authoritative sources, scalable repository, access to cross-reference and audit functions. Therefore, regardless of intentions, manually created and updated documentation systems are prone to errors and omissions. The intention of IdAM RA v.3 is to integrate the following vital components of RA structure:

- **Capabilities -The mission achievements of IdAM**
- **Life cycle – IdAM on-going activities and processes**
- **Framework - Structure of dependencies among IdAM processes and facilities**

1.3 Document Purpose and Scope

The purpose of this document is to provide guidance for improving the Army's IdAM architecture. As required, the architectural rules within this document will be further described by a technical or operational position statement and a high-level implementation pattern to ensure the intent of the rule is understood, achievable and measurable. This document addresses Army IdAM requirements, and is written from the perspective of the Army as a consumer of DOD-provided enterprise IdAM services[4]. It also deals with environments where these enterprise services are not always available (i.e., when adequate network connectivity to the enterprise services does not exist). Therefore, an attempt has been made to make this document as generic as possible from a DOD perspective while concentrating on Army and the way that it operates on posts/camps/stations (P/C/S) and in forward-area tactical environments across both its generating and operating forces.

This document provides an authoritative source of information for Army IdAM requirements and guides and constrains the instantiations of multiple architectures and the solutions built upon them by serving as a framework for operational and Business components of the architecture. Army IdAM RA does not replace the policies that guide access determination and decisions. Rather, it attempts to improve the implementation and consistency of these decisions through more efficient information technology-enabled means. Ultimately, resource owners are still responsible for determining access rights based on existing law, policy and established agreements. The primary audience for the document is Army IdAM implementers at all stages of program planning, design and implementation; however, the document may also be used as a resource for systems integrators, end users and commercial business partners seeking interoperability or compatibility with Army programs. While the document serves to outline a common framework for IdAM in the Army, it is understood that components are at different stages in the implementation of their IdAM architectures and programs. As a result, they will need to approach alignment with IdAM from varying perspectives.

This RA has three primary objectives:

1. **Ensure that Army personnel and non-person entities can securely access all authorized Army resources from any location and at any time.**
   Personnel and non-person entities will possess an established, trusted digital identity that will enable authentication and authorization to Army resources. Army's access control will facilitate system owners' ability to make authentication and authorization decisions based on a single identity solution that is effectively distributed and consumable.

2. **Halt the development and deployment of stovepiped IdAM infrastructure for DOD/Joint enterprise and tactical environments.**
   Within the current DOD environment, authentication and authorization services have been designed differently and are too often focused on supporting a single

[4] https://intellipedia.intelink.gov/wiki/DoD_Identity_and_Access_Management_(IdAM)

application or application type. Implementations are sometimes commercial off the shelf (COTS), government off the shelf (GOTS) or integrated COTS and GOTS. The Architectural Rules in this RA are meant to stop this practice by promoting a more standardized and federated approach to IdAM infrastructure.

3. **Optimize the use of existing and future DOD enterprise IdAM services and infrastructure**.
   The Army must first attempt to leverage all of the available deployed, operational and enterprise IdAM service offerings; their service capabilities and their supporting network infrastructures in any solution architecture. This strategy applies to both logical and physical access controls.

1.4 Document Structure

This document provides information, guidance and direction that is applicable across the Army. This RA applies a rules-based methodology and presents the information in accordance with the DOD guidance for Component-level RA documents. Information, guidance and direction are provided in the following sections:

Section 3- IdAM Life Cycle – details the IdAM implementation life cycle and capability overview.

Section 4 – IdAM Army Principles and Rules - identifies goals and objectives of the Army IdAM and Architecture and details rules with high level foundational concepts that guide and constrain how IdAM will perform and be implemented.

Section 5 - Technical Positions and Implementation Patterns – provides generalized architecture representations that further clarify the rules with which the IdAM architecture must conform as well as details a minimal set of technical guidance and standards required to conform to a given rule.

1.5 Capability Drivers

Capability drivers consist of the following:

- **Regulatory compliance** - Create auditing, logging and monitoring capabilities while providing secured authentication and authorization
- **Security** - Reduce threat of individual and organized attackers
- **Convenience** - Provide Single Sign-On solution for ease of login capabilities for various types of users
- **Cost** - Reduce maintenance of multiple user accounts, optimize performance and create a single view for customers
- **Single access point** - Provide security, authentication and authorization across multiple channels from a single access point.

1.6 Capability Benefits

Capability benefits include the following:

- Increased cybersecurity capabilities
- Reduced user management cost and risk through automated provisioning and access management
- Reduced costs of serving users by moving secure transactions from physical offices to ones online
- Protect user privacy and identity through practical means
- Provide convenience, control and safely to consumers over virtual channels.

1.7 IdAM Challenges

The IdAM roadmap evolves organically and structurally. Infrastructure dependencies from network to the Global Information Grid (GIG) require solving challenges and achieving maturity across the enterprise. Specific concerns are related to following areas:

- The traditional identity management suites were built for yesterday's technology.
- The first challenge must be solved: automated provisioning and directory synchronization.
- New challenges are presented as the cloud, social media and mobile offerings disrupted the identity machine.
- New opportunity: bridge the gap between identity system and integration system (Service Oriented Architecture (SOA)/Enterprise Service Bus (ESB).

1.8 Current and Objective State

The Army IdAM vision defines a personnel entity as a human being with a single digital identity. Personnel entities include members of the Army and mission partners, such as members of government agencies, non-governmental organizations, industry and the general public. It is recognized that while a person may have one digital identity, they may have multiple personas (more information and guidance on persona management can be found in Section 4.5 of this document). A non-person entity is an entity with a digital identity that is not a person. A non-person entity that is an information system (device or application) may also function as both an entity seeking access and a resource. A digital identity is the unique set of enterprise attributes by which an entity can be distinguished from any other entity. The Army IdAM data set consists of all data required to support or make access control decisions to Army resources. Army IdAM data includes, but is not limited to, an entity's digital identity attributes and other distinguishing attributes (e.g., personnel data, contact data, location, role, etc.), entity credentials, resource attributes, access authorization policies and environmental attributes (e.g., security posture, time, location, etc.).

Through a structured and institutionalized governance/configuration management process, digital identities will be used to organize IdAM data to support authentication

and authorization decisions to Army resources, as illustrated by the Army IdAM operational view (Figure 1: Army IdAM Operational View, below).

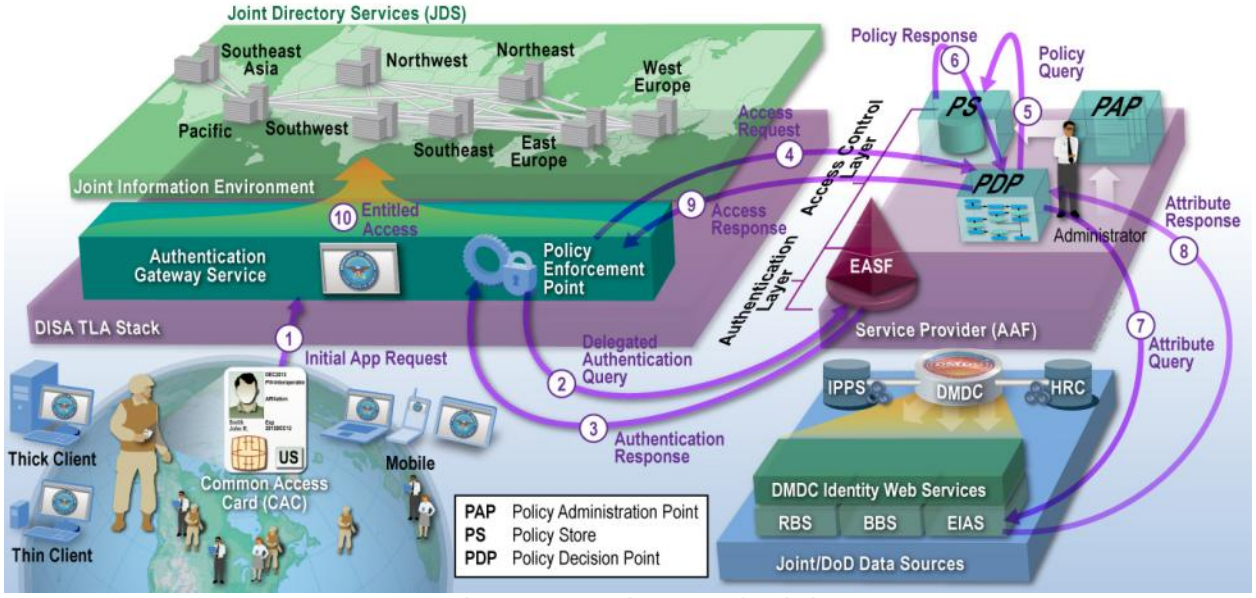


Figure 1: Army IdAM Operational View

Authentication includes verifying the identity of an entity against an issued DOD or other recognized credential (e.g., Personal Identity Verification [PIV]) and after verification/validation of the credential, mapping the identity on the credential to available IdAM data. The successful authentication of an entity allows for the next step of determining authorized access to an Army resource. Authorization is the manual or automated step, governed by the resource owner, where the access control decision is based on the entity's IdAM data and relevant access policies associated with the Army resource. Local environmental conditions may also influence the authorization decision. Army IdAM supports access accountability by binding an entity's identity to authentication and authorization decisions associated with a resource. Army IdAM ensures completely trustworthy and accurate IdAM data is readily accessible to resource owners to support access control decisions. A second-order effect of IdAM is the ability to synchronize and make available accurate enterprise-wide contact data so entities can easily look up entities' contact data.

Army IdAM supports access to Army resources for unclassified and classified networks up to the SECRET level. This includes enabling access from Army and non-Army end-user devices on external networks (e.g., mission partner networks or commercial enclaves). Army IdAM also may support Personnel Entities Physical Access Control Systems (PACS) that use information systems to support physical resource access management.

1.8.1 Key Authoritative Guidance

The IdAM objectives describe key focus areas that align Army activities and resources to DOD and Army guidance. Each objective has complementary performance indicators that specify how the Department will assess the successful implementation of the DOD IdAM strategy. DOD has published several enterprise-level architectures and strategies to provide a common foundation to support the transformation to net-centric operations. DOD has mandated that lower-level architectures align to higher-level strategies and guidance. The DOD Information Enterprise Architecture (DOD IEA) comprises the necessary information, information resources, assets and processes required to achieve an information advantage and to share information across the Department and with mission partners.

This IdAM RA is principally aligned to and guided by the following key roadmaps/strategies:

- DOD Information Enterprise Architecture (DOD IEA) v2.0, July 2012
- The Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0, 2 December 2011. Document referenced to identify Federal Identity Management framework and intersection with Army and DOD policies.
- The DOD Information Technology (IT) Enterprise Strategy and Implementation Roadmap (ESR) Initial Implementation Plan, Version 1.0, September 2011. Document referenced to ensure alignment and reusability of DOD IdAM solutions.

While the following documents are still in draft form, they were consulted to ensure alignment with mission partners:

- The draft DOD Identity and Access Management Strategy (IdAM) v0.8, November 14, 2013. Document referenced to ensure alignment with DOD end-state objectives for DoD IdAM across the department.
- The draft DOD IdAM RA V0.7, October 31, 2013. Document referenced to ensure alignment and reusability of DOD IdAM solutions.

1.9 IdAM Service Delivery Overview

The business value of IdAM- related services can be measured by coverage and ease of use of the supporting infrastructure. The identity infrastructure must provision identities in all identity repositories within the Army so soldiers can progress through their career and have their identity automatically move with them. Figure 2 demonstrates the relationship of an organization’s IdAM infrastructure and the expected business value that can be achieved.

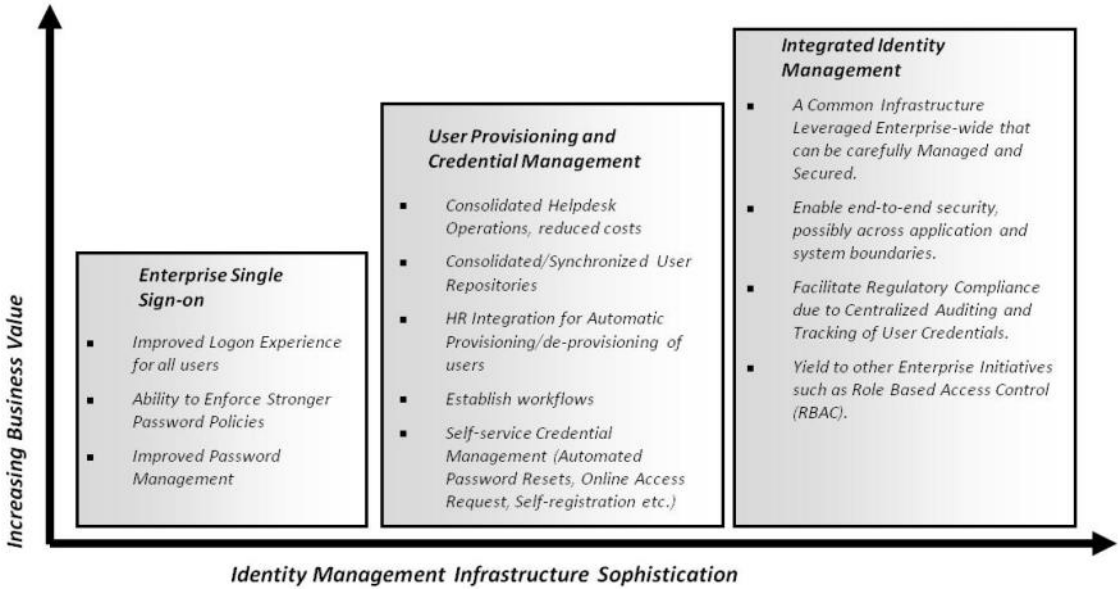
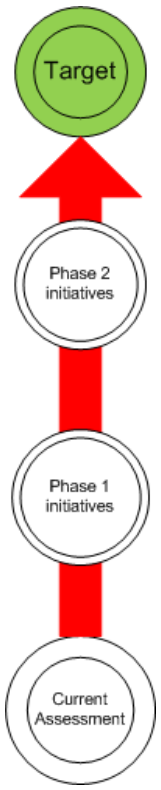


Figure 2: Increasing Business Value

The roadmap to higher levels of IdAM sophistication provides increasing business value by enhanced security and reduced user credential-management costs.

1.10 Current Army IdAM Maturity

Figure 3 depicts (at a high-level) IdAM business capabilities relative to an overall IdAM maturity. Currently, Army IdAM is operating at maturity level 1 with multiple ongoing initiatives that will deliver capabilities within levels 2-4.



MATURITY LEVELS	BUSINESS CAPABILITIES
5	▪ Security controls are established around business processes ▪ Trust & Federated Relationships are established with External Partners
4	▪ Centralized Authentication Mechanism ▪ Capability to Integrate with other business solutions ▪ Utilize workflow to automate identity management processes ▪ Security controls are established around business processes
3	▪ Rationalize Multiple Passwords ▪ Enterprise Level Processes and Mechanisms Established for non-US export controls, information subject to International Traffic in Arms Regulations (ITAR)/Export Administration Regulations (EAR), and information not-export control related
2	▪ Applications share user & group repositories ▪ User repositories are synchronized ▪ Users can access multiple LOB applications ▪ Consistent practice and infrastructure for access control
1	▪ Multiple user repositories and access control policies ▪ Security between applications is ad hoc ▪ Users sign on to individual applications ▪ Minimal infrastructure to facilitate security monitoring and auditing ▪ Accounts are created on a system-by-system basis

Figure 3: IdAM Maturity Levels

1.11 Current State

An Authentication and Authorization Framework (AAF), coupled with a Directory Service (DS) and an Account Provisioning Service (APS), are currently provided by the COTS products used to support DOD enterprise and network and information resource infrastructures. DOD and the Army have also built infrastructure components based on GOTS technology. Maturity level 1 of Figure 3 represents the current state of the IdAM program (shown in Figure 4).

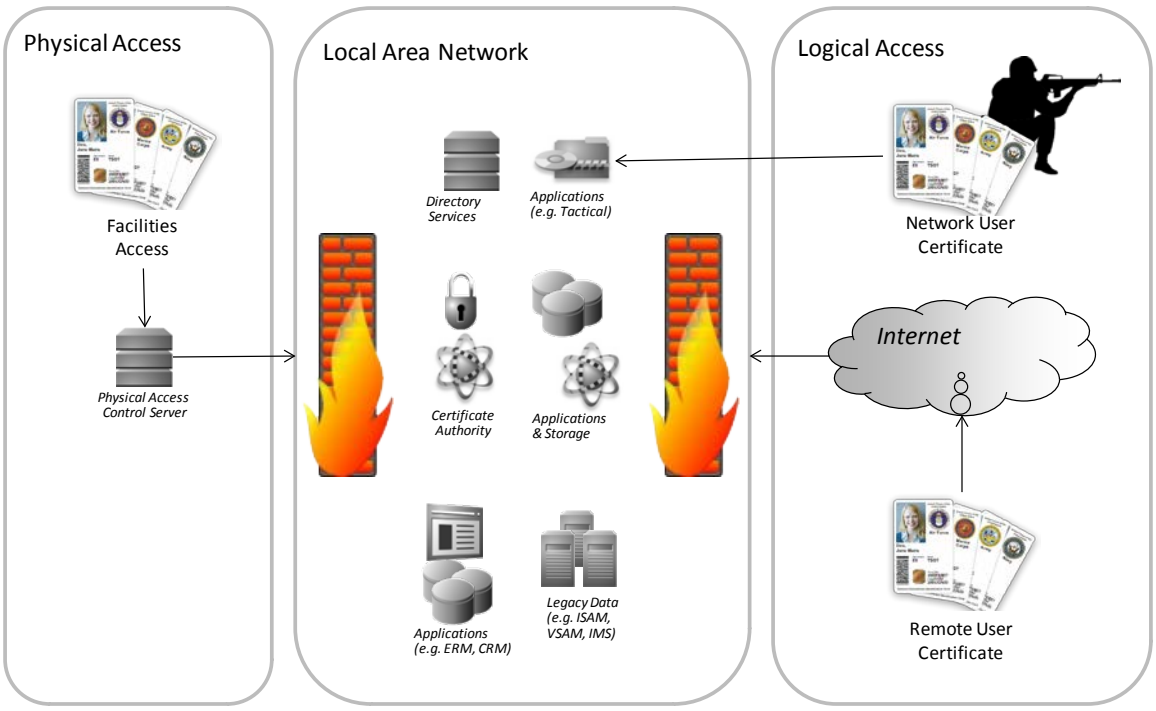


Figure 4: Digital Identity, Physical and Logical Access (Current State)

Army IdAM current-state capability gaps include the following:

- Authentication and Authorization are not holistically exercised across the enterprise.
- Single-sign-on (SSO) to Army applications are dependent on Army Knowledge Online (AKO) directory services for user authentication and/or authorization. Applications that use the Army SSO must transition away from SSO prior to consolidation /migration to enterprise data centers.
- Distributed directory data is unable to support central management of workstations, applications and network access.

1.12 Objective State

The objective IdAM state includes business capabilities identified by maturity level 5 with IdAM services and operations that consist of:

- Distributed authentication and authorization operations from a centrally controlled credential and credential support operation
- A federated infrastructure that makes the IdAM services look and operate like a single IdAM services implementation
- A single IdAM implementation and life-cycle management model.

The dependencies of IdAM construct reflect maturity and sophistication of Army IdAM architecture.

1.13 Army IdAM Objective State Goals

The following are the Army Objective State Goals:

- Leverage a single digital identity across the enterprise
- Migrate applications that are dependent on Army Knowledge Online (AKO) directory (SSO) to an enterprise capability (direct PKI)
- De-couple applications from reliance on directories for Authentication and Authorization
- Use CAC PKI to the maximum extent practicable, with 2-factor authentication as a back-up alternative
- Maximize the use of DMDC Authorization Attributes
- Ensure consistent use of PKI certificates (email or DoD).

Figure 5 is a high-level depiction of the Army IdAM Architecture Objective State.

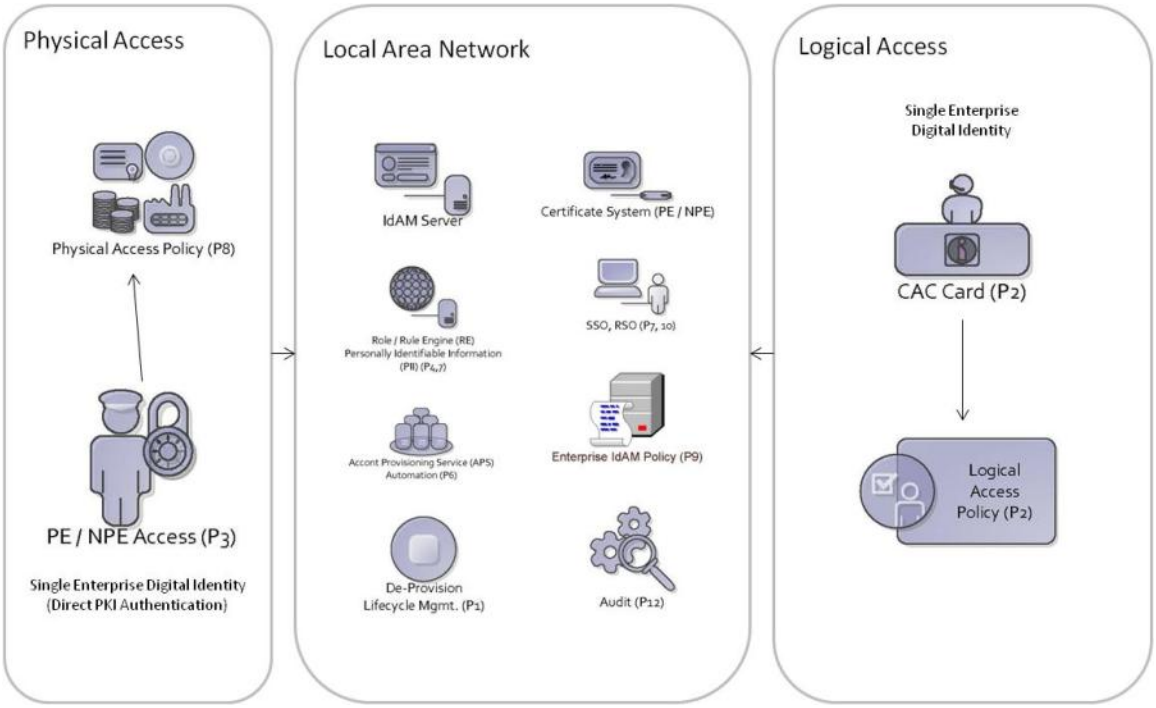


Figure 5: Army IdAM Objective State

1.14 Transitional Assumptions

There are several overarching assumptions that the Army must take into account in the transition to a comprehensive IdAM capability and infrastructure. These are noted in Table 1 – Army IdAM Transitional Assumptions.

	Transitional Assumption
Assumptions	The Army IdAM approach focuses on Army resources, but supports access to non-Army resources, assuming mission partner agreements are in place.
	There is a pre-built trust association between nodes in the network and not within the scope of this RA.
	The Army IdAM is intended to support and align with the DOD IdAM RA v 0.7.
	Credentialing, although defined as a key service area, is considered in this Army RA only from a service consumer perspective, the RA does not intend to conflict with DOD's purview to set and maintain standards.
	The Defense Manpower Data Center (DMDC) will be the Authoritative Data Provider for Person Entity (PE) and will define Personnel for the Army.
	DOD will provide enterprise account provisioning services to manage Army identity life cycles and to populate directories. This service will be accomplished through the current Enterprise Directory Services (EDS) initiative.
	All services, applications and networks will be required to enforce authorized access to information or devices according to specified access control rules and requirements for all individuals, organizations, Communities of Interest (COIs), automated services and devices.
	The Army Enterprise Identity Service for PE and NPE will include support for the tactical edge.
	Army applications will migrate from legacy infrastructures for authentication and authorization to the Enterprise Authentication Gateway and Access Management framework once instantiated
	Army IdAM does not govern access to physical resources, but may support electronic physical access control systems (ePACS).

Table 1 – Army IdAM Transitional Assumptions

2 IdAM Life Cycle

IdAM life-cycle management should consist of the following phases, illustrated in Figure 6:

- Change Request
- Identity Creation/Validation
- Identity Provisioning
- Mover/Leaver Process
- De-provision

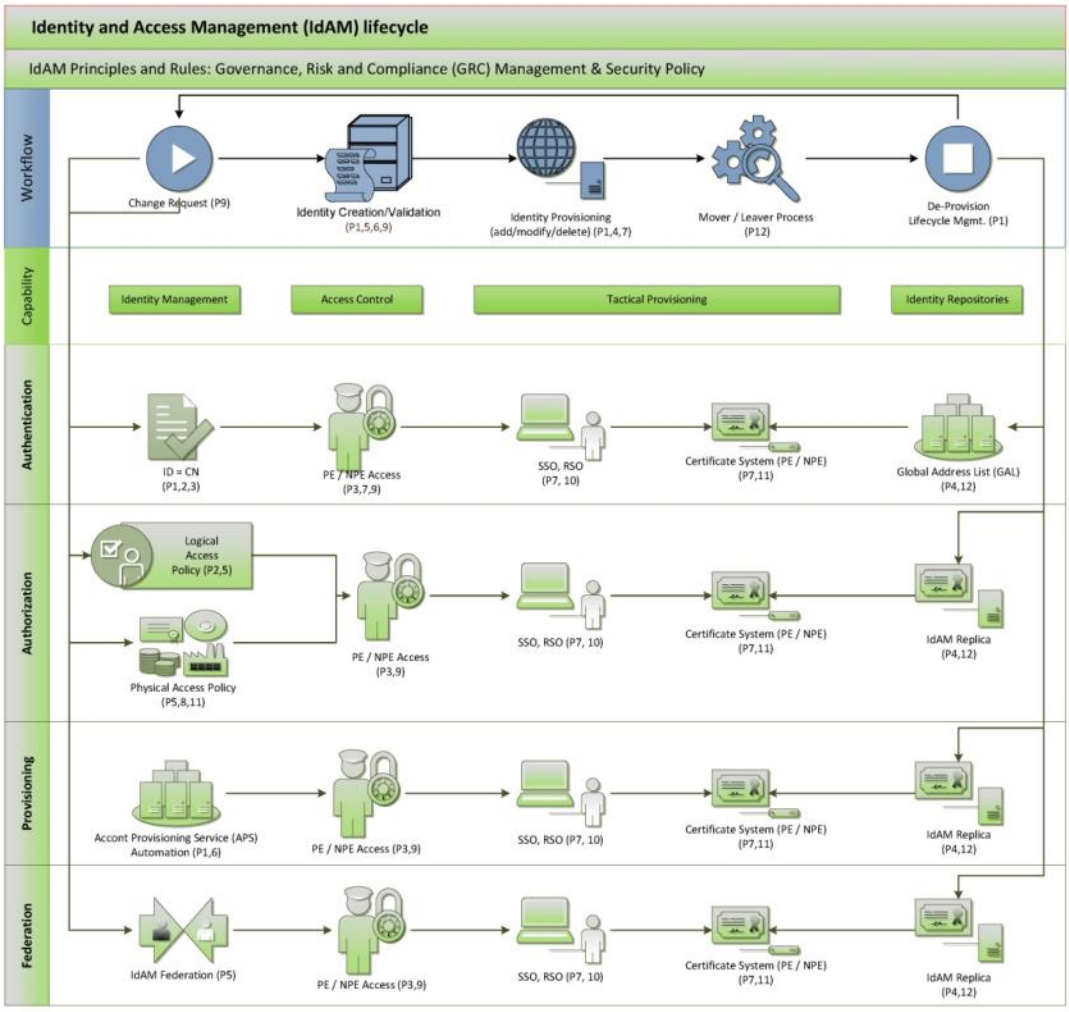


Figure 6: IdAM Life Cycle (Mapping IdAM Principles 1-12)

The workflow contains only major milestones starting with Change Requests, ending with De-Provision. The IdAM Life Cycle is mapped against all current capabilities:

- **Identity Management** provides users with the capability to register their identities and manage their passwords and profiles. Identity Management can

also delegate user administration to third-party business partners or different business units within the enterprise.

- **Access Control** provides user identification, authentication, secure session management, and authorization services to applications and resources within the enterprise. Access Control provides single or simplified sign-on to applications and helps reduce the number of usernames and passwords. A second order effect of IdAM is the ability to synchronize auditing records from diverse systems to find malicious behavior because the same identity is used on each system.

- **Provisioning** automates the creation and administration of user accounts, and access to systems, applications and resources. Security is enhanced by quickly implementing changes to access rights while administrative costs are reduced due to automation. Integrated workflow ensures that all required changes could be routed for approval where appropriate.

- **Federation** provides a trusted authority or digital identity across domains. Participating entities provide identity attributes that facilitate cross domain authentication to online resources thus streamlining access to digital assets while preserving security controls.

- **Identity Repositories and Directories** provide consolidated storage of user identities. Policies, audit log information, centralized repositories feed provisioning engines and provide the foundation for authentication and access control services.

2.1 IdAM Reference Framework

All activities related to IdAM RA are mapped to IdAM Reference Framework (RF). Business areas of identity and access management framework should comprise the following:

- Identity Life-Cycle Management
- Identity and Authentication Management
- Authorization and Permission Life-Cycle Management
- Authorization and Permission Management
- Identity Governance.

Figure 7 illustrates the Framework categories and attempts to organize the ontology of the subordinate capabilities.

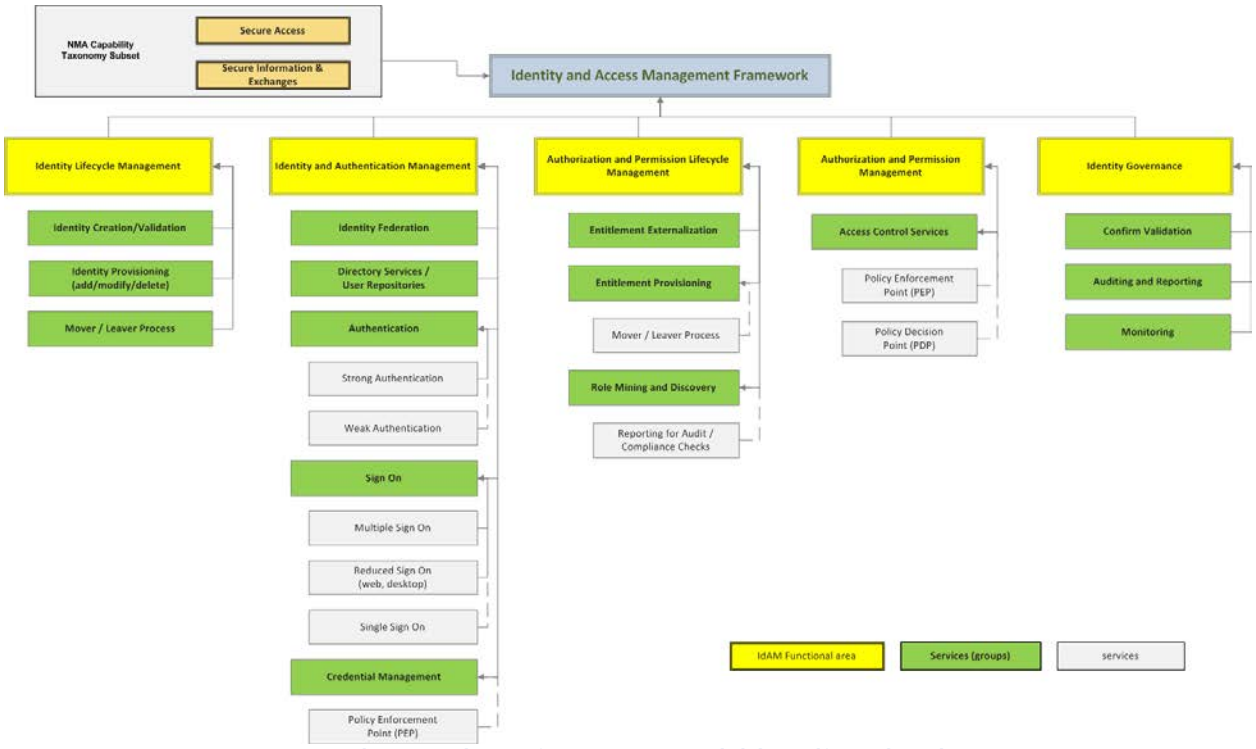


Figure 7: IdAM Reference Framework (IdAM Life Cycle RA)

Within the enterprise, an identity management system comprises a set of directories and access control mechanisms based on policies. It includes the maintenance of the system (additions, updates, deletions) and ideally offers single sign-on enabling the user to log in once to gain access to multiple resources.

2.2 IdAM Capability Overview

Identity and access management is the set of processes, people and technologies that control who has access to resources in the enterprise, and what actions can be taken. Every activity performed by IdAM is the result of a requirement that facilitated it. All supported capabilities hierarchy structures are organization specific as illustrated in Figure 8, Capability Taxonomy.

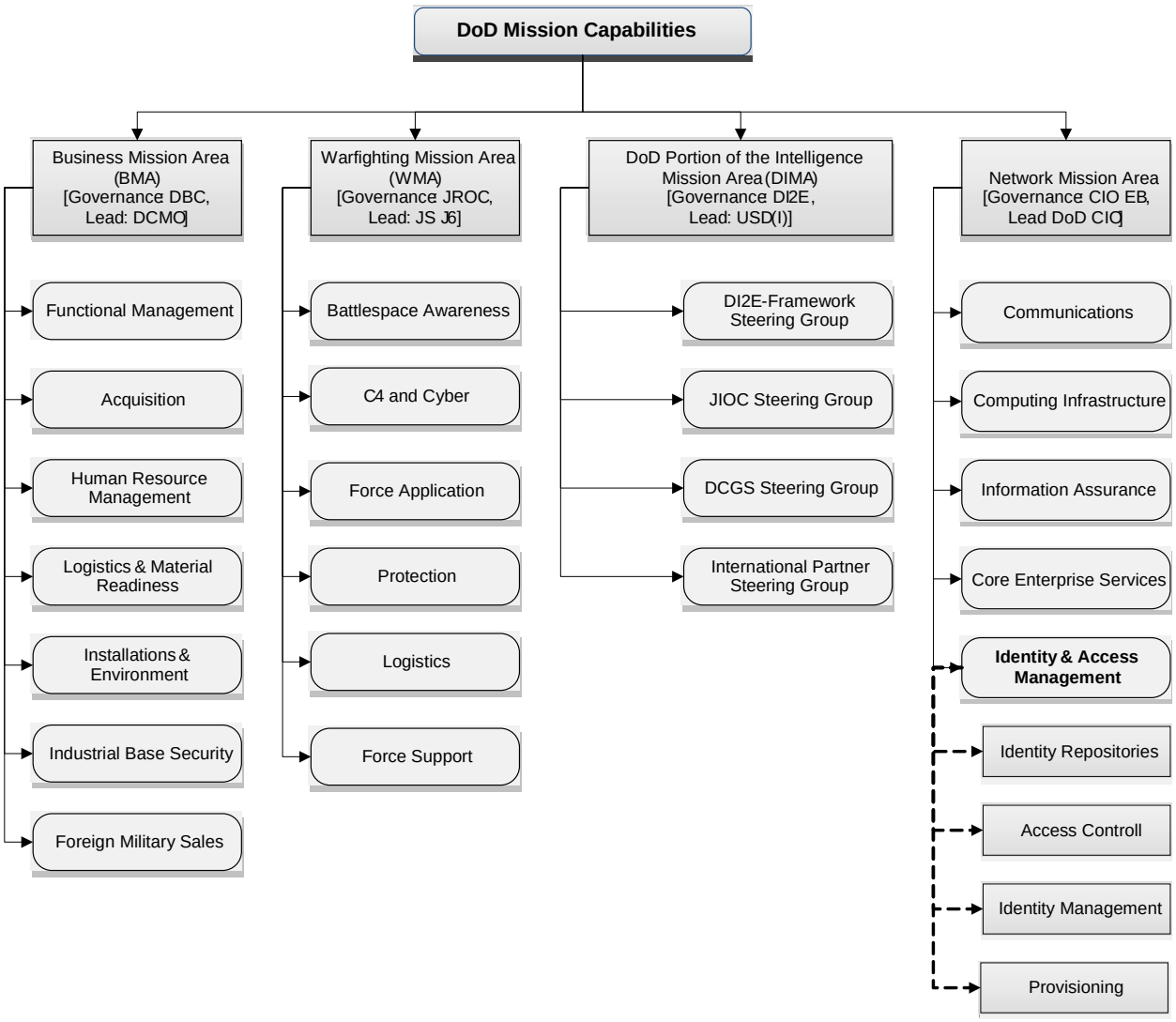


Figure 8: Capability Taxonomy

3 IdAM Army Principles and Rules (Synopsis)

The Army's IdAM principles are outlined in Sections 3.1 - 3.12, as well as Appendix E of this document.

3.1 Principle 1: Unique Identity and Credentials

Rule 1: Person Entity (PE) Unique Identifier
Rule 2: Allowed Identities
Rule 3: Personnel Life-Cycle Management
Rule 4: Identity Data Integrity
Rule 5: Person Entity (PE) - Identity Data Discoverability
Rule 6: Non-Person Entity (NPE) - Identity Data Discoverability
Rule 7: Identity Data Conformance
Rule 8: Authentication and Authorization Service Provisioning
Rule 9: Enterprise Identity Attribute Utilization
For more information, also see Appendix A, Section 4.5.1

3.2 Principle 2: Authoritative Identity Data Source

Rule 1: Authoritative Person Entity (PE) Identity Attribute Data
Rule 2: Authoritative Non-Person Entity (NPE) Identity Attribute Data
Rule 3: Common Access Card (CAC) Usage
Rule 4: Resource Account Provisioning Service (APS)
Rule 5: Adding Core Person Entity (PE) Identity Attributes
Rule 6: Adding Core Non-Person Entity (NPE) Identity Attributes
Rule 7: Non-Person Entity (NPE) Resource Data Federation
Rule 8: Directory Information Updates
For more information, also see Appendix A, Section 4.5.2

3.3 Principle 3: Person Entity (PE) and Non-Person Entity (NPE) Identification

Rule 1: Mobile/Edge Platforms/Devices
Rule 2: Mobile Device Binding
For more information, also see Appendix A, Section 4.5.3

3.4 Principle 4: Global Directory Services for Enterprise Services

Rule 1: Global Address List (GAL) Distribution
Rule 2: Global Address List (GAL) Views
Rule 3: Global Address List (GAL) Data Schema
Rule 4: Local Offline Address Book (OAB) Availability
Rule 5: Directory/Global Address List (GAL) Information Concurrency
For more information, also see Appendix A, Section 4.5.4

3.5 Principal 5: Authentication and Authorization

Rule 1: Authentication and Authorization Scope
Rule 2: Identity Service for Tactical Edge
Rule 3: Global Information Resource Access
Rule 4: Access and Policy Security
Rule 5: Availability of DOD Enterprise Authentication and Authorization Services
Rule 6: Availability of Army (Non-DOD Enterprise) Authentication and Authorization Services
For more information, also see Appendix A, Section 4.5.5

3.6 Principle 6: Dynamic Access Policy Management

Rule 1: Policy Management Service Scope
Rule 2: Standard Attribute Model
Rule 3: Standard Access Policies
Rule 4: Policy Change Management Responsibility
Rule 5: Policy Attribute Validation
For more information, also see Appendix A, Section 4.5.6

3.7 Principle 7: Access to Data, Services and Applications

Rule 1: Information Resource Types
Rule 2: Logical NPE Layered Logical Access Control
Rule 3: Public Key Infrastructure (PKI) Based Authentication
Rule 4: Data Resource Identification
Rule 5: Rules Engine (RE) Personally Identifiable Information (PII) Attribute Exposure
Rule 6: Data Tagging Development
Rule 7: Standardized Policy Languages
Rule 8: Access Policy Data Tagging Metadata Standards
For more information, also see Appendix A, Section 4.5.7

3.8 Principle 8: Physical Access

Rule 1: Non-Person Entity (NPE) Unique Identifier
Rule 2: Physical Access Control Policies
Rule 3: Non-Person Entity (NPE) Attribute Verification
Rule 4: Facilities Attributes Management
Rule 5: Common Access Card (CAC) Credential Mechanism
Rule 6: Common Access Card (CAC) Enrollment
Rule 7: Layered Physical Access Control for Subclass Type 1 Physical NPEs
Rule 8: Layered Physical Access Control for Subclass Type 2 Physical NPEs
Rule 9: Physical Access Control: Subclass Type 1 NPE Asset Naming
Rule 10: Physical Access Control: Subclass Type 2 NPE Asset Naming
For more information, also see Appendix A, Section 4.5.8

3.9 Principle 9: General IdAM Security Policy

Rule 1: Identity Attribute Data Validation
Rule 2: Authorization Service Scope
Rule 3: Enterprise Information Sharing
Rule 4: Information Resource Authentication Frequency
Rule 5: Cross-Domain Security
Rule 6: Information Resources Availability
Rule 7: Information/Data Resources Protection
Rule 8: DOD Enterprise Trust Management
Rule 9: Alternate Authentication Mechanisms (Non-CAC/Token)
Rule 10: Data Encryption
Rule 11: SHA-256: Secure Hashing Algorithm Migration
For more information, also see Appendix A, Section 4.5.9

3.10 Principle 10: Single Sign-On (SSO) and Reduced Sign-On (RSO)

Rule 1: SSO and RSO Directory Data Population
Rule 2: Electronic Data Interchange Personal Identifier (EDI-PI)
Rule 3: SSO and RSO Services Availability
For more information, also see Appendix A, Section 4.5.10

3.11 Principle 11: Network Access Controls

Rule 1: Authorization Policy Network Attributes
Rule 2: Network-Connected Device Authentication
Rule 3: Disconnected, Intermittent or Low-Bandwidth Authentication
Rule 4: Network Gateway Authentication and Authorization
For more information, also see Appendix A, Section 4.5.11

3.12 Principle 12: Monitoring and Reporting

Rule 1: Auditing Services
Rule 2: Identity and Access Management (IdAM) Infrastructure-Monitoring/Reporting
For more information, also see Appendix A, Section 4.5.12

4 Technical Positions and Implementation Patterns

4.1 Assurance Assessment Position

The following technical position is derived from the National Institute of Standards and Technology (NIST) Cybersecurity Framework and provides technical guidelines for implementing electronic authentication. It is not intended to constrain the development or use of standards outside of this purpose. The recommendation covers remote authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks. It defines technical requirements for each of four levels of assurance in the areas of identity proofing, registration, tokens, management processes, authentication protocols and related assertions. NIST published the table (see Table 2) in context of a number of publications where IdAM role is viewed from the perspective of Cybersecurity.

	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	1	2	3	4
Inconvenience, distress or damage to standing orders	Low	Med	Med	High
Financial loss or agency liability	Low	Med	Med	High
Harm to agency programs or public interests	N/A	Low	Med	High
Unauthorized release of sensitive information	N/A	Low	Med	High
Personal Safety	N/A	N/A	Low	Med High
Civil or criminal violations	N/A	Low	Med	High

Table 2 – Maximum Potential Impacts for Each Assurance Level[5]

In supporting IdAM assurance level impact, NIST E-Authentication Guidance (SP 800-63-2) provides the following recommendations:

- Required (if practical) by e-Sign, Paperwork Elimination and other laws
- Premature to take sides in web services wars
- Difficult: many technologies, apples and oranges comparisons

OMB guidance (SP 800-63-2):

- Level 1: Little or no confidence in asserted identity's validity
- Level 2: Some confidence in asserted identity's validity
- Level 3: High confidence in asserted identity's validity
- Level 4: Very high confidence in asserted identity's validity

4.1.1 Level 1 Assurance

Although there is no identity-proofing requirement at this level, the authentication mechanism provides some assurance that the same Claimant who participated in

[5] NIST E-Authentication Guidance, SP 800-63-2, August, 2013

previous transactions is accessing the protected transaction or data. It allows a wide range of available authentication technologies to be employed and permits the use of any of the token methods of Levels 2, 3, or 4. Successful authentication requires that the Claimant prove, through a secure authentication protocol, that he or she possesses and controls the token.

4.1.2 Level 2 Assurance

Level 2 provides single-factor remote network authentication. At Level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information. A wide range of available authentication technologies can be employed at Level 2. For single factor authentication, Memorized Secret Tokens, Pre-Registered Knowledge Tokens, Look-up Secret Tokens, Out of Band Tokens, and Single Factor One-Time Password (OTP) Devices are allowed at Level 2. Level 2 also permits any of the token methods of Levels 3 or 4. Successful authentication requires that the Claimant prove through a secure authentication protocol that he or she controls the token. Online guessing, replay, session hijacking and eavesdropping attacks are resisted. Protocols are also required to be at least weakly resistant to man-in-the middle (MitM) attacks.

4.1.3 Level 3 Assurance

Level 3 provides multi-factor (MF) remote network authentication. At least two authentication factors are required. At this level, identity-proofing procedures require verification of identifying materials and information. A level 3 authentication is based on proof of possession of the allowed types of tokens through a cryptographic protocol. MF Software Cryptographic Tokens are allowed at Level 3. Level 3 also permits any of the token methods of Level 4. Level 3 authentications require cryptographic strength mechanisms that protect the primary authentication token against compromise by the protocol threats for all threats at Level 2 as well as verifier impersonation attacks. Long-term shared authentication secrets, if used, shall never be revealed to any party except the Claimant and Credential Service Provider (CSP); however, session (temporary) shared secrets may be provided to Verifiers by the CSP, possibly via the Claimant. Approved cryptographic techniques shall be used for all operations including the transfer of session data. Level 3 assurance may be satisfied by client-authenticated TLS (implemented in all modern browsers) with Claimants who have public key certificates. Other protocols with similar properties may also be used. Level 3 authentication assurances may also be met by tunneling the output of a MF OTP Token, or the output of a SF OTP Token in combination with a Level 2 personal password, through a TLS session.

4.1.4 Level 4 Assurance

Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 authentications are based on proof of possession of a key through a cryptographic protocol. At this level, in-person identity proofing is required. Level 4 is similar to Level 3 except that only “hard” cryptographic tokens are allowed. The token is required to be a hardware cryptographic module validated at Federal Information Processing Standard (FIPS) 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security. Level 4 token requirements can be met by using the PIV

authentication key of a FIPS 201 compliant Personal Identity Verification (PIV) Card. Long-term shared authentication secrets, if used, shall never be revealed to any party except the Claimant and CSP; however session (temporary) shared secrets may be provided to Verifiers or Relying Parties (RPs) by the CSP. Strong, Approved cryptographic techniques shall be used for all operations including the transfer of session data. All sensitive data transfers shall be cryptographically authenticated using keys that are derived from the authentication process in such a way that MitM attacks are strongly resisted. Level 4 assurance may be satisfied by client-authenticated TLS (implemented in all modern browsers), with Claimants who have public key MF Hardware Cryptographic Tokens. Other protocols with similar properties can also be used.

4.2 Direct PKI Migration Process Pattern

Certification Authority (CA) migration is described as the process of moving an existing CA to a new environment while preserving CA functionality and certain CA-specific attributes. These attributes can include configuration settings required to support existing applications, historical and pending transactions, and the CA signing certificate and keys. Characteristics that are not specific to the CA (such as computer name) and CA properties (such as stand-alone versus enterprise CA type) may be changed in some migrations. Certificate Service (CS) technology recognizes the following components of the process:

- Active Directory Certificate Services. The server role provides the certificate infrastructure to enable scenarios such as secure wireless networks, Internet Protocol security (IPsec), and Network Access Protection (NAP), Encrypting File System (EFS), and smart card logon.

- Certification authority (CA). The AD CS role service that is used to issue and manage certificates. A PKI can include multiple CAs.

- CA Web enrollment. The AD CS role service that provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.

- Online Responder. The AD CS role service that implements the Online Certificate Status Protocol (OCSP) in Windows Server 2008.

- Network Device Enrollment Service. The AD CS role service that implements the Simple Certificate Enrollment Protocol (SCEP).

- Upgrade process. The process of changing the underlying Windows version of an existing CA computer to a newer release. Usually, configuration settings are preserved during an upgrade and can be changed as part of normal configuration change management after the upgrade.

The chronological steps of the process are illustrated in Figure 9: Direct PKI Migration Process.

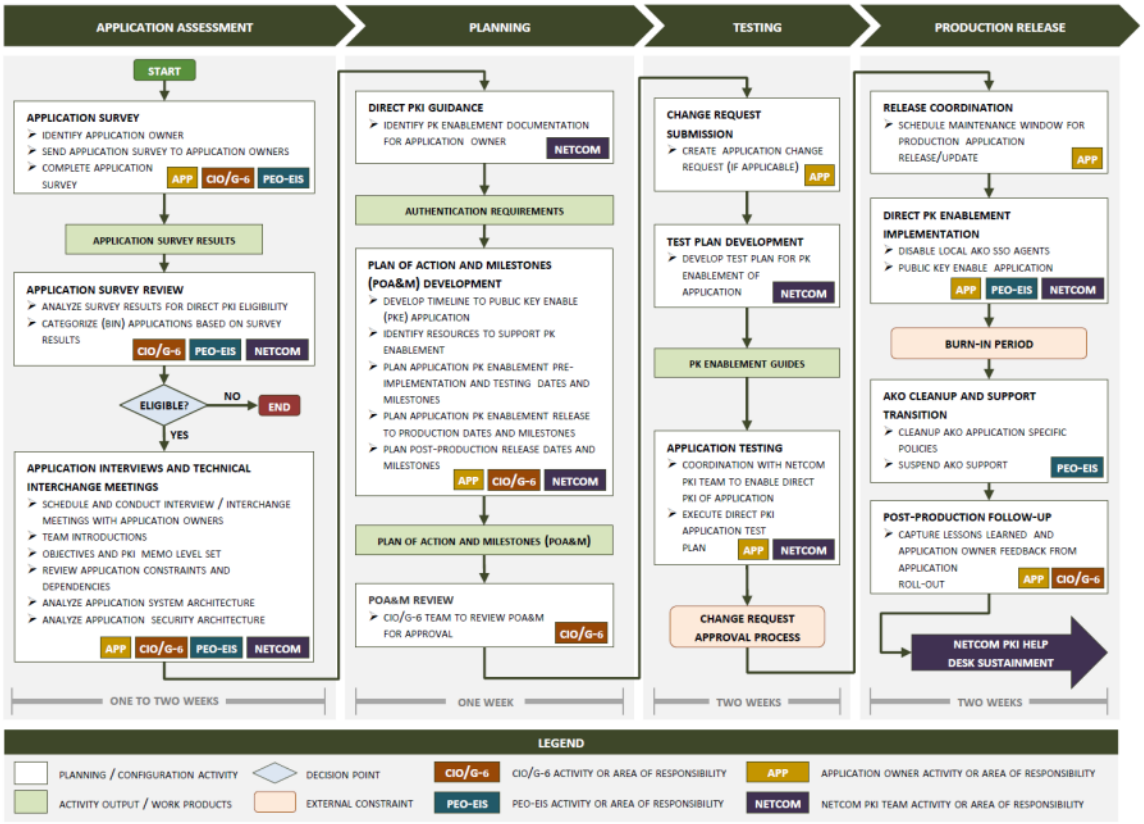


Figure 9: Direct PKI Migration Process

4.3 Network Characteristics Pattern

Figure 10 provides a framework for further analysis and decision support when deciding how IdAM-related services are deployed beyond the tactical edge of the enterprise environment. In this context, patterns and frameworks describe future and theoretical capabilities orchestrated for planned tactical capabilities realignment. The description or constraint (minimal, moderate or severe) is in relation to the environmental characteristics typically represented within the enterprise environment. This figure represents a section of DOD infrastructure limited to DOD compatible branches.

Navy Echelon				Large Ship and Support Ship		
Army Echelon			Theater	BGD and BN	CO	PLT and below
USMC Echelon			MEF, DIV, REG	BN	CO	PLT and below
Tactical Edge Constraints			Tactical Fixed Center	Tactical Mobile Center	Mobile Platform	Dismounted User
Network	Bandwidth	SATCOM	Army/Navy: nearly unlimited Marine: <8/20Mbps	Army: <3/4 Mbps (2013) 0.5/4 Mbps (now) Navy: 128/256/512Kbps/ 4Mbps (2013) Marine: <4 Mbps	Army: 0.3Kbps(now), 128Kbps(2013) Marine: <2.6/19/120Kbps /8Mbps	Army: 0.3Kbps(now), 9.6Kbps(2013) Marine: <2.6/60Kbps
		WAN	Army/Navy: nearly unlimited Marine: <16Mbps	Army: 2Mbps(now), 10Mbps(2013) Navy: None Marine: <16Mbps	Army: 128-256Kbps(now), 0.6-2Mbps(2013) Marine: <2.6/16/486Kbps	Army: 9.6-64Kbps(now), 0.6Mbps(2013) Marine: <2.4/16Kbps
	Connectivity	LAN	>85%	>85%	25-84%	5-24%
		WAN	>99%	85-99%	25-84%	<5%
	Latency	LAN	<250ms	<250ms	>250ms	>250ms
		WAN	<250ms	250-1000ms	250-1000ms	>1000ms
	Reliability	LAN	>90%	>90%	>90%	>90%
		WAN	>90%	>75%	<75%	<75%
System	User Interface		desktop-laptop	desktop-laptop	laptop-tablet-handheld	laptop-tablet-handheld
	Processing Power		nearly unlimited	300-900 spec int	<300 spec int	<30 spec int
	Storage		nearly unlimited	~10-50TB	~500GB	~160GB
	Weight		100s lbs	100s lbs	10-100 lbs	< 10 lbs
	Power		grid, macro generator	generator - batteries	generator -batteries	batteries
Operational	Decision Time		minutes - weeks	minutes - days	seconds -minutes	seconds - minutes
	Content		complex	complex	intermediate	simplified
	Mobility		fixed	occasional move	frequent move	frequent move

minimal to no constraints moderate constraints severe constraints

Figure 10: Network Characteristics

4.4 Tactical Token Issuance Pattern

IdAM services need to authenticate clients in a heterogeneous environment. Additional controls such as authorization and authentication can be implemented. An organization can use an authentication broker to provide a common access control infrastructure for a group of applications. The authentication broker negotiates trust between client applications and Web services; this removes the need for a direct relationship. The authentication broker should issue signed security tokens that can be used for authentication as shown in Figure 11, Tactical PKI Token Issuance.

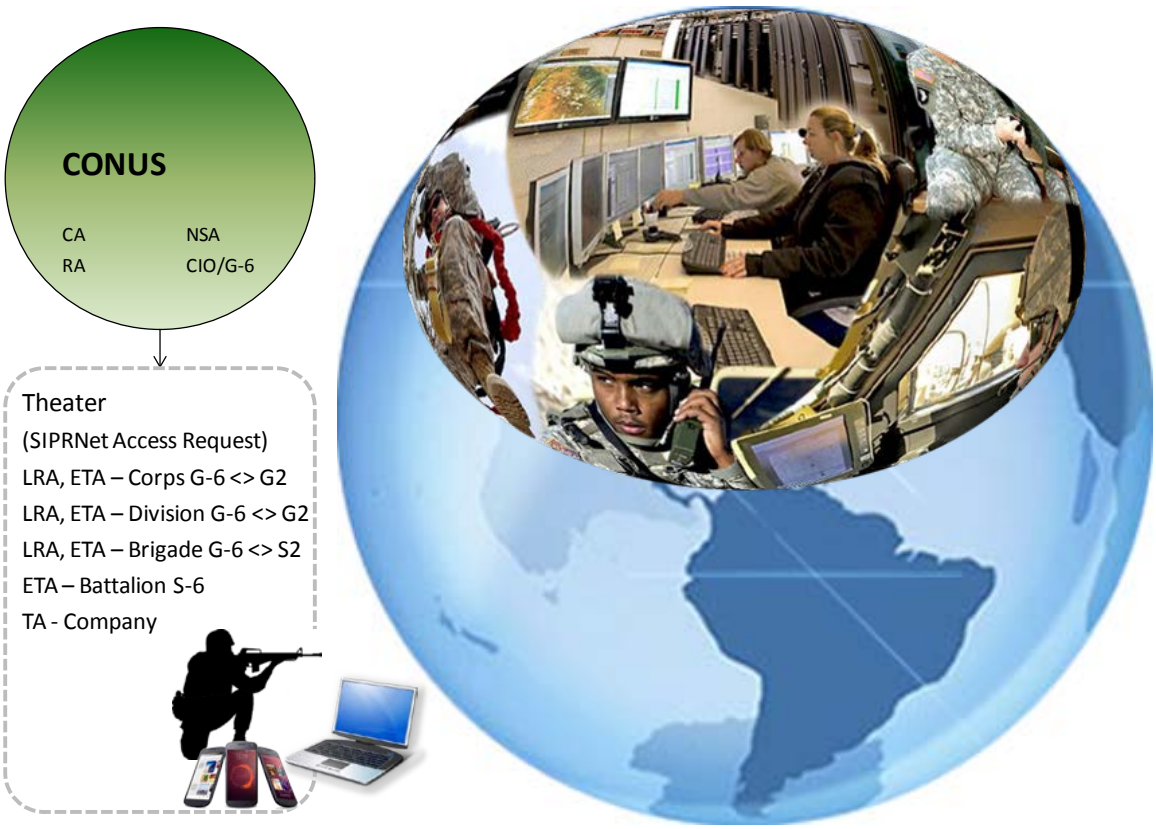


Figure 11: Tactical PKI Token Issuance

PKI Roles:

- CA Certificate Authority
- RA Registration Authority
- LRA Local Registration Authority
- ETA Enhanced Trusted Agent
- TA Trusted Agent

Appendix A - IdAM RA Principles and Rules

The section was originally a part of IdAM RA v.2 and continues to expand the present version of RA. Eventually, all listed principles will map to IdAM capabilities, life cycle and framework. This is an ongoing attempt to provide an even more holistic list of Army IdAM principles and rules supporting tactical and non-tactical environments.

4.5 Specifications

4.5.1 (P1) Principle 1 – Unique Identity and Credentials

Principle	Description
All authorized person entities and non-person entities will have one identity that is recognized by all producers of information and services.	Persons seeking access resources within the Joint Information Environment (JIE) will be required to have a unique set of identifiers and credentials that can be used across the enterprise. Physical devices must be identifiable and portable in a similar manner.

Table 3 – Unique Identity and Credentials

4.5.1.1 (P1/R1) Business Rule 1 – Person Entity (PE) Unique Identifier

Business Rule	Description
The Army will use an established identifier, provided by DOD as the digital identity indexer for all Army personnel with Common Access Cards (CAC) or an interim equivalent.	An Electronic Data Interchange Personal Identifier (EDI-PI) is a unique number assigned to a record in the Defense Enrollment and Eligibility Reporting System (DEERS) database, which is the authoritative source for EDI-PI. A record in the DEERS database is a person linked to a personnel type or category (e.g., contractor, reservist, civilian, active duty, etc.). The CAC, issued by DOD through DEERS, and any other similar interim mechanism (e.g., SIPRNET Hard Token) are required to support user authentication. Currently, a person with more than one personnel category is issued a CAC for each persona.

Table 4 – Person Entity (PE) Unique Identifier

(P1/R1) Assumptions

- EDI-PI is unique to a person, not to a persona or role.
- EDI-PIs can be associated with one or more persona per PE.
- The Army and the other SCs use the Personal Category Codes (PCC) as a key identity attribute.
- Authoritative Data Sources will synchronize Identity data.

(P1/R1) Constraints

- There may be multiple authoritative sources containing different sets of data about any PE, but all must be associated with only one EDI-PI.
- EDI-PIs must be reconciled on a regular basis to ensure that there are neither redundant identifiers nor the same PE with different identifiers.
- The CAC must not be used as a credential to authenticate users on a classified network.

(P1/R1) Risk

- Constantly shifting personnel strength and responsibilities will increase the level of difficulty associated with creating, modifying and deleting PE personas and linking them with the right EDI-PI.
- Personas associated with any EDI-PI may be accidentally inherited when a PE is re-enrolled if they are not purged every time a CAC is revoked or expires.

(P1/R1) Technical Positions and Patterns (Reference Appendix B – Pattern View)

(P1/R1) Technical Standards Profiles:

- ***Technical Profile:*** Common Access Card (CAC)

(P1/R1) Policy/Regulation Profiles:

- Army IdAM RA to Army Regulation (AR) 25-2 Mapping

4.5.1.2 (P1/R2) Business Rule 2 – Allowed Identities

Business Rule	Description
The Army will require that all person entity and non-person entity digital identities be authenticated.	DOD and SC personnel and equipment residing on any SC or DOD network, of any information classification level, must have registered identities and identifiers assigned to them. This includes infrastructure components (e.g., routers, switches, bridges) and information resources (e.g., servers, storage, data brokers). None of these entities will be allowed to authenticate to, access or transport information within the JIE without first establishing their identities.

Table 5 – Allowed Identities

(P1/R2) Assumptions

- All PEs and NPEs can be assigned unique identifiers that will allow X.509 certificates to be assigned to and removed from association with them.
- Globally Unique Identifiers (GUIDs) for NPE would be in addition to use of PKI/X.509 certificates.

(P1/R2) Constraints

- A GUID must be assigned to every NPE.
- Once established, the EDI-PI must remain associated with a unique PE.
- Once established, the GUID must remain associated with a unique NPE.

(P1/R2) Risk

- If an EDI-PI or GUID is assigned to the wrong PE or NPE, invalid authorization may occur.
- Unless identity data are regularly audited to assure that it is uniquely associated with a PE or NPE, it is possible that an unauthorized entity could be allowed access.

(P1/R2) Technical Positions and Patterns

P1/R2 Technical Standards Profile

- ***Technical Profile:*** Identity Proofing

P1/R2 Policy/Regulation Profile

- ***Technical Profile:*** Policy in Authentication

4.5.1.3 (P1/R3) Business Rule 3 – Persona Life-Cycle Management

Business Rule	Description
The Army will use digital identity in the form of personas to determine suitability/fitness for access to resources, and as a basis for digital identity life-cycle management.	Identities are comprised of hierarchical layers of associated attributes. In addition to a unique identifier (i.e., EDI-PI), one or more personas can define a PE or NPE. The next level would be one or more personas that describe what functions a persona engages in at any point in time. A PE's or NPE's identity life-cycle management will be based on these elements, which can serve as major components of access policies across the JIE. The problem with the CAC today is that it is not tied to a persona but to the individual person so that each CAC has the same values on it. For example, a Civil Service CAC and a reservist CAC for the same person have the same values; thus, systems/applications cannot differentiate between the Civil Service personas versus the reservist person. An objective of this rule is to migrate to a more comprehensive set of identity attributes to accommodate multiple personas via a single credential mechanism.

Table 6 – Persona Life-Cycle Management

(P1/R3) Assumptions

- PE personas and their associated persona definitions will be the basis for need-to-know access rules.
- PE and NPE personas will be manageable to accommodate changes in mission, function and/or location for Army and DOD personnel.
- Personas will be portable across the JIE.

(P1/R3) Constraints

- Personas must be based on a standard set of identity attributes that are captured during the initial credentialing process.
- Identity attributes must be able to support multiple personas on a single credential mechanism.
- Persona accuracy must be maintained throughout the life cycle of all digital identities.

(P1/R3) Risk

- Failure to do regular due-diligence on persona assignments may result in "hijacking" of authorization privileges and unauthorized access to information and/or facilities.
- Failure to perform regular due diligence on persona definitions and assignments may result in loss of information or required physical access.

(P1/R3) Technical Positions and Patterns

P1/R3 Technical Standards ProfileTechnical Profile: Identity Proofing

- ***Technical Profile:*** Identity Management

P1/R3 Policy/Regulation Profile

- ***Technical Profile:*** Policy in Authentication

4.5.1.4 (P1/R4) Business Rule 4 – Identity Data Integrity

Business Rule	Description
The consistency and integrity of identity data must be enforced through policies, processes and tools established by DOD and the Army.	The reliability of identity data is foundational to trust and the ability to access and consume information from service/agency and multinational environments. Adherence to a standard digital identity "language" format will allow the required access policies to be created and executed in a non-ambiguous manner.

Table 7 – Identity Data Integrity

(P1/R4) Assumptions

- Both PE and NPE DOD identity data standards exist and are applied consistently across the JIE.
- Identity data attributes will have a consistent set of possible values, meanings and context at any one point in time.

(P1/R4) Constraints

- Human intervention and governance of identity data policies and management processes must be required.
- Tools required for management of identity data integrity must consistently apply the required rules and policies, and be able to validate each identity attribute associated with each PE and NPE.
- Identity data (i.e., Personally Identifiable Information (PII)) must have limited exposure to all access management components.

(P1/R4) Risk

- Unless identity data integrity is maintained for all non-U.S. or non-DOD entities that require access to information, it will be impossible to maintain consistent policies and practices that constrain access appropriately.
- Accidental exposure and/or storage of PII could result in violation of federal laws and/or DOD and Army regulations.

(P1/R4) Technical Positions and Patterns

P1/R4 Technical Standards Profile

- ***Technical Profile:*** Digital Certificate (PKI)
- ***Technical Profile:*** Common Access Card (CAC)

P1/R4 Policy/Regulation Profile

- Army IdAM RA to Army Regulation (AR) 25-2 Mapping

4.5.1.5 (P1/R5) Business Rule 5 – Person Entity (PE) - Identity Data Discoverability

Business Rule	Description
Identity data must be available independent of person entity location, and the attribute data must be discoverable by authorized access policy and controls and infrastructure components.	The ability to post and access identity data relies upon a known, visible, authoritative Attributes Data Repository (i.e., EIADRSS) that is supported by a virtual infrastructure and provides the ability for a rules engine to access and utilize it in the authentication and authorization processes.

Table 8 – Person Entity (PE) - Identity Data Discoverability

(P1/R5) Assumptions

- Attribute data will be organized so that access by any consumer will be non-ambiguous and reliable.
- There is consistency and concurrency between attribute data in an ADR and the access policies that they are applied to.

(P1/R5) Constraints

- The utilization of local ADRs must be minimized or eliminated, with emphasis on use mainly in tactical environments with DIL.
- Avoidance of unnecessary or accidental exposure and/or storage of PII and other sensitive identity attribute data must be assured.
- Requester attribute data must not be disseminated beyond the PDP to any other authorization services.

(P1/R5) Risk

- Unavailability of selective attribute data may prevent proper authentication of a PE requesting access.
- Unavailability of selective attribute data may restrict or prevent proper authorization of a PE to resources controlled by attribute-based policies.

(P1/R5) Technical Positions and Patterns

P1/R5 Technical Standards Profile

- ***Technical Profile:*** Identity Proofing

P1/R5 Policy/Regulation Profile

- Army IdAM RA to Army Regulation (AR) 25-2 Mapping

4.5.1.6 (P1/R6) Business Rule 6 – Non-Person Entity (NPE) - Identity Data Discoverability

Business Rule	Description
Identity data must be available independent of non-person entity location, and the attribute data must be discoverable by authorized access policy and controls and infrastructure components.	The ability to post and access identity data relies upon a known, visible, authoritative Attributes Data Repository (i.e., EIADRSS) and the ability of a rules engine to access and utilize it in authentication and authorization.

Table 9 – Non-Person Entity (NPE) - Identity Data Discoverability

(P1/R6) Assumptions

- Attribute data will be organized so that access by any consumer will be non-ambiguous and reliable.
- There is consistency and concurrency between attribute data in an ADR and the access policies to which they are applied.

(P1/R6) Constraints

- All forms of logical NPE must be supported.
- Both types of physical NPEs must be supported.

(P1/R6) Risk

- Unavailability of selective "entitlement" attribute data may restrict or prevent proper authorization of a NPE to resources controlled by attribute-based policies.
- Outdated, retired, invalid or NPE resource attribute data that fails to federate to the enterprise level will result in failed authorizations and possibly orphaned access policies.

(P1/R6) Technical Positions and Patterns

P1/R6 Technical Standards Profile

- ***Technical Profile:*** Credential Management

P1/R6 Policy/Regulation Profile

- Army IdAM RA to Army Regulation (AR) 25-2 Mapping

4.5.1.7 (P1/R7) Business Rule 7 – Identity Data Conformance

Business Rule	Description
Army digital identity data will conform to relevant schema and business rules established by DOD.	Army IdAM services will follow a business process life cycle for both enterprise and local services. All processes are dependent on having a common data schema that supports interoperable attribute exchange across the JIE.

Table 10 – Identity Data Conformance

(P1/R7) Assumptions

- A standard data schema is maintained at the DOD enterprise level for all identity data.
- All access policies will be based on the standard identity attribute data schema.
- Both PE and NPE digital identity data will consist of informational attributes, access control attributes and functional attributes.

(P1/R7) Constraints

- Digital identity data must be comprised of only the essential attribute data that are required to specify any PE or NPE and any corresponding persona.
- Identity data schema must continually be synchronized across the JIE.

(P1/R7) Risk

- Continued use of stovepiped data schema will prevent synchronization of data and limit or prevent proper identity interoperability and portability.
- Without an enterprise view and the ability to manage identity data schema, attribute data management will be extremely difficult, and consistent enterprise resource access cannot be assured.

(P1/R7) Technical Positions and Patterns

P1/R7 Technical Standards Profile

- ***Technical Profile***: Credential Management

P1/R7 Policy/Regulation Profile

- Army IdAM RA to Army Regulation (AR) 25-2 Mapping

4.5.1.8 (P1/R8) Business Rule 8 – Authentication and Authorization Service Provisioning

Business Rule	Description
All authentication and authorization services must be supported by an account provisioning service.	Any logical and physical resource will require use of an authorization service. The component realization of this would be in the form of an AAF or standalone infrastructure that supports account-based authorization. Therefore, AAF access policies must be aligned to a set of approved requesters whose accounts are provisioned using an APS.

Table 11 – Authentication and Authorization Service Provisioning

(P1/R8) Assumptions

- Tactical operating units (Brigade Combat Team, Regiment, Division, Corps, Army, Fleet, and Air Wing) can be supported by their own independent T-AAFs and T-APSs.

(P1/R8) Constraints

- The number of DOD and SC AAFs will be minimized while optimizing support for Joint warfighting operations.
- Provisioning of all AAFs will utilize a single primary enterprise identity attribute data repository.
- The Army and the other SCs must not create any new individual system- or applications-level directory services if the DOD enterprise directory service is readily network-available.
- Any APS must support all forms of access account provisioning (e.g., network domains, systems, applications, data, facilities, any physical or NPE assets).

(P1/R8) Risk

- The inability to update identity attribute data accurately and/or in a timely manner in the EIADRSS (from authoritative data sources) will impact the accuracy and overall capability of an APS.
- The inability to provision network domains and resource accounts in an accurate and timely manner will impact the effectiveness of any AAF.

(P1/R8) Technical Positions and Patterns (Reference Appendix B – Pattern View)

P1/R8 Technical Standards Profile

- ***Technical Profile:*** Attribute Management Services
- ***Technical profile:*** Authoritative Attribute Exchange Service

P1/R8 Policy/Regulation Profile

- ***Technical Profile:*** Policy in Credentialing

4.5.1.9 (P1/R9) Business Rule 9 – Enterprise Identity Attribute Utilization

Business Rule	Description
The Army will utilize DOD-established authoritative identity attributes for authentication, based solely on DOD authoritative data sources.	The Army and the other SCs' continued propagation of stovepiped identity data repositories is inefficient and does not either promote or optimize JIE interoperability. Identities must be initiated by authoritative data sources, then collected and distributed to all consuming IdAM services across the JIE. With the exception of certain tactical operational environments, no additional identity data repositories at the SC level will be allowed. This rule is intended to prevent developers' from creating new repositories for the purpose of authenticating and authorizing users/requesters without direct dependence on the Enterprise Identity Attribute Data Repository and Synchronization Service (EIADRSS).

Table 12 – Enterprise Identity Attribute Utilization

(P1/R9) Assumptions

- All or most legacy JIE non-tactical information resources can be transitioned to an enterprise-level ADR (i.e., EIADRSS) to support enterprise authentication services.
- The EIADRSS will assure that non-ambiguous identity data are maintained for use across the JIE.

(P1/R9) Constraints

- Non-tactical legacy information resources and systems-of-systems that cannot easily be transitioned to use an ADR must be either subsumed or sunsetted.

(P1/R9) Risk

- If an ADR does not fully and consistently support both the legacy and current attribute data requirements, potential impacts on authentication and authorization services may affect both the non-tactical and tactical environments and their corresponding operations.
- If an ADR's attribute data concurrency cannot be maintained at the tactical level with minimal latency in accuracy, invalid authentications may occur.
- Army tactical operations will have to accept some level of latency between PE enrollment and revocation at the DOD enterprise level.

(P1/R9) Technical Positions and Patterns

P1/R9 Technical Standards Profile

- ***Technical Profile:*** Attribute Management Services
- ***Technical profile:*** Authoritative Attribute Exchange Service

P1/R9 Policy/Regulation Profile

- Technical Profile: Policy in Authentication
- Army IdAM RA to Army Regulation (AR) 25-2 Mapping

4.5.2 (P2) Principle 2 – Authoritative Identity Data Source

Principle	Description
Identities must be tied to universal portable credentials (i.e., enterprise digital identities) that are maintained by authoritative data sources.	Identities established by a centralized authoritative data source will be portable and reusable across the JIE. The appropriate ADR can collect and distribute authoritative credential data, and synchronize it with one or more ADRs and/or AAFs.

Table 13 – Authoritative Identity Data Source

4.5.2.1 (P2/R1) Business Rule 1 – Authoritative Person Entity (PE) Identity Attribute Data

Business Rule	Description
The Army must utilize authoritative identity data sources as the primary broker to define and maintain person-entity personas.	DMDC maintains the largest archive of personnel, manpower, training and financial data in DOD, and is the most qualified source for authoritative personal identity information. It will be used to establish and maintain the authoritative PE attribute data set. All authoritative attribute data to support all DOD/Joint operations are brokered by DMDC, as shown in Figure 1. PEs can have one or more personas that define role(s) and/or function(s) for any requester. All identity attribute data that comprise a PE persona must reside within or under the control of the DMDC.

Table 14 – Authoritative Person Entity (PE) Identity Attribute Data

(P2/R1) Assumptions

- DMDC maintains reliable and accurate authoritative identity data from DOD personnel management systems and data sources.
- The authoritative data maintained in an authoritative data source is at a minimum near-real-time accurate according to established DISA Service-Level Agreements.

(P2/R1) Constraints

- All PE identity data consumed by Army IdAM services and components sourced from DMDC must be indexed by an EDI-PI.
- DMDC-based identity data cannot be directly modified; changes must not occur in the originating systems and data sources without first being instantiated in the appropriate ADR.

(P2/R1) Risk

- Data value errors in an authoritative data source will propagate across ADRs and AAFs, and could impact the accuracy and effectiveness all IdAM components.
- If the DMDC>EIADRSS>DS data propagation is not near real-time, unauthorized access to information resources may be granted.
- When a T-DS is Disconnected, Intermittent or Low-Bandwidth (DIL) WANWAN connectivity, unauthorized access to information and physical resources may be granted.
- All IdAM service consumers who do not define their acceptable risk levels, based on assessments of the range of possible data propagation latencies, may experience both unexpected and negative operational and security impacts.

(P2/R1) Technical Positions and Patterns

P2/R1 Technical Standards Profile

- ***Technical Profile:*** Identity Management

4.5.2.2 (P2/R2) Business Rule 2 – Authoritative Non-Person Entity (NPE) Identity Attribute Data

Business Rule	Description
The Army will utilize authoritative identity data sources as the primary broker to define and maintain non-person entity personas.	DMDC maintains the largest archive of personnel, manpower, training and financial data in DOD, and is the most qualified source for authoritative personal identity information. All authoritative attribute data to support all DOD/Joint operations are brokered by DMDC, as shown in Figure 1. Once established by the DOD for the JIE, all NPE identity attribute data and NPE persona would reside within or at least under the control of the DMDC. NPEs may have one or more personas that define the function and purpose as a form of NPE requester (e.g., device, service) or as an NPE resource (e.g., system, application, or facility).

Table 15 – Authoritative Non-Person Entity (NPE) Identity Attribute Data

(P2/R2) Assumptions

- (Same as for P2/R1)

(P2/R2) Constraints

- All NPE identity data consumed by Army IdAM services and components sourced from DMDC must be indexed by a GUID.
- DMDC-based identity data cannot be directly modified; changes must not occur in the originating systems and data sources without first being instantiated in the EIADRSS.

(P2/R2) Risk

- (Same as for P2/R1)

(P2/R2) Technical Positions and Patterns

P2/R2 Policy/Regulation Profile

- ***Technical Profile:*** Policy in Credentialing

4.5.2.3 (P2/R3) Business Rule 3 – Common Access Card (CAC) Usage

Business Rule	Description
The Army will use a DOD-issued personal identity verification (PIV) mechanism for Public Key Infrastructure certificates and other key person entity identity data.	CAC – PIV v2.0-compliant cards will be used as the preferred authoritative credential mechanism to support any Public Key Infrastructure-based access within DOD. However, the DoD-issued CAC is an official identification mechanism that is currently used to support authentication and access control to unclassified DOD networks and

	information resources. Due to information spillage restrictions, the CAC cannot be and is not currently used to support digital identity data for access to classified information systems. This is due to security restrictions that prohibit a physical mechanism containing classified information, including the digital identity data related to classified access that would have to be resident on a CAC, from being physically connected to a classified system/user device. Therefore, a separate PIV mechanism (e.g., smartcard, SIPRNET token) must be issued.

Table 16 – Common Access Card (CAC) Usage

(P2/R3) Assumptions

- CAC provisioning is accurate at the time the CAC is issued.
- The CAC Personal Identification Number (PIN) is uniquely bound to every CAC. Classified logical and physical resource access must be supported by a smart card or other separate digital identity mechanism.

(P2/R3) Constraints

- The CAC will be the primary form of PIV for any PE.
- This business rule applies only to DOD CAC-holders who require access to logical NPE and both types of physical NPE resources.
- If a CAC is lost, damaged or destroyed, an alternate non-CAC authentication methodology must be available.

(P2/R3) Risk

- Mobile or portable computing devices with network access may not always be able to interface physically with CAC readers.
- Tactical environment access (logical and physical) to unclassified resources may not be capable of being supported by CAC-based authentication.
- Tactical environment access (logical and physical) to classified resources may not be capable of being supported by smart cards alone.

(P2/R3) Technical Positions and Patterns

P2/R3 Technical Standards Profile

- ***Technical Profile:*** Common Access Card (CAC)
- ***Technical Profile:*** Digital Certificate (PKI)

4.5.2.4 (P2/R4) Business Rule 4 – Resource Account Provisioning Service (APS)

Business Rule	Description
Network domain, application and data resource accounts must be enabled by an enterprise directory service that supports all account provisioning as part of the access life-cycle management of all Army logical and physical resources.	DOD and SC directory, authentication, authorization and account management services are all currently provided within Microsoft Active Directory Forests and Domains and their supporting infrastructure, via a set of management services for : • User accounts • Domain relationships • Lightweight Directory Access Protocol (LDAP) configuration • Authentication • Policies (User and Group) An APS can support these existing Microsoft AD services generically as a set of IdAM components: ADR, DS and ASF/AAF. These IdAM components can exist in both non-tactical and tactical operations. In any case, as defined by this RA, an APS will be required. All PE and NPE access accounts will be created and managed by leveraging some or

	all of the PE and NPE identity attributes made available by the appropriate ADR.

Table 17 – Resource Account Provisioning Service (APS)

(P2/R4) Assumptions

- The current DOD, Army and other SC Microsoft AD Forest/Domain infrastructures are being reconfigured.
- The APS will eliminate the need to use external systems (e.g., currently Army EDS-Lite) to maintain ADR, DS and ASF/AAF identity data in each account.
- Use of an enterprise/centralized provisioning service is an option for existing and future DOD, Army and other SC ADR, DS and ASF/AAF, but they must derive authorization policies only from the authoritative enterprise attribute data schema.

(P2/R4) Constraints

- Future DOD, Army and other SC ADRs and AAFs must derive authorization policies only from the authoritative enterprise attribute data schema.
- The EIADRSS must maintain synchronization of identity data across all existing ADR, DS and ASF/AAF infrastructures across the JIE.
- The EIADRSS must not identify attributes that are unique only to the Army or any one SC.

(P2/R4) Technical Positions and Patterns (Reference Appendix B – Pattern View)

P2/R4 Technical Standards Profile

- ***Technical Profile:*** *Digital Certificate (PKI)*

P2/R4 Policy/Regulation Profile

- ***Technical Profile:*** Policy in Authentication

4.5.2.5 (P2/R5) Business Rule 5 – Adding Core Person Entity (PE) Identity Attributes

Business Rule	Description
The Army must be able to propose or request supplements to the existing core enterprise person entity identity attributes repository, but all identity data attributes used must either already exist in an authoritative identity data source or be approved and added to these by DOD.	If additional identity attributes are required for any PE, two options are available: 1) Existing identity attributes available in the authoritative data sources can be identified, vetted and approved; or 2) New attributes can be proposed for inclusion in the core enterprise identity data schema provided by the EIARDSS.

Table 18 – Adding Core Person Entity (PE) Identity Attributes

(P2/R5) Assumptions

- The required PE identity attributes do not already exist in the EIADRSS.
- The required PE identity attributes may already exist in a DOD registered and approved authoritative data source.

(P2/R5) Constraints

- New attributes must never directly populate the EIADRSS.
- The EIADRSS component must never maintain any Army or SC-unique PE identity data.
- Proposed enterprise PE identity attributes for the Army must be submitted through a governance process that reviews and approves the request(s) prior to use by the Army or any SC within the JIE.

(P2/R5) Risk

- If proposed additional PE identity attributes are not vetted for non-ambiguity and re-usability by the Army and the other SCs, consistent and executable access policies cannot be inserted into the JIE.

(P2/R5) Technical Positions and Patterns (Reference Appendix B – Pattern View)

P2/R5 Technical Standards Profile

- ***Technical Profile:*** Attribute Management Services
- ***Technical profile:*** Authoritative Attribute Exchange Service

4.5.2.6 (P2/R6) Business Rule 6 – Adding Core Non-Person Entity (NPE) Identity Attributes

Business Rule	Description
DOD will have the ability to supplement the enterprise non-person entity identity attribute data repository identity data schema with additional or "extended" attributes as needed to provide more finely grained resource authorization policies or experience customizations as required.	Applications and information resources may require additional identity attributes to support the execution of required authorization policies. Management of these attributes, which are available within an ADR, to a Policy Decision Point (PDP) and Policy Enforcement Points (PEP) will be required to assure their consistency and accuracy, and to optimize their usability. The core identity attributes provided by an ADR are derived solely from an authoritative DOD data source, and will never be updated directly in an ADR by an SC. In addition to any automated resource attribute data federation process that may be in place, the Army or any other SC can submit a request to add attributes (ad hoc) that do not already exist in either a local or enterprise ADR schema.

Table 19 – Adding Core Non-Person Entity (NPE) Identity Attributes

(P2/R6) Assumptions

- The required "extended" NPE identity attributes do not already exist in the EIADRSS.
- Resource NPE attribute data can be federated to the DOD enterprise level by the Army and the other SCs, but would be initially treated only as candidates to be added to the EIADRSS.

(P2/R6) Constraints

- Any NPE identity attributes added to the JIE data set must be provided by the EIADRSS.
- Any "extended" NPE identity attributes and attribute data originate from a DOD authoritative data source.
- No Army or SC-unique identity attributes for NPE will be created, stored or distributed within the Army or the JIE.

(P2/R6) Risk

- A Dynamic Access Policy Management Service (DAPMS) capability leveraging the EIADRSS will not be possible if NPE resource attribute data cannot be fully and accurately maintained.

- If the Army or other SCs create and distribute local "extended" identity attributes that are not instantiated in the EIADRSS, full resource availability will be limited or possibly prevented across the JIE.

(P2/R6) Technical Positions and Patterns (Reference Appendix B – Pattern View)

P2/R6 Technical Standards Profile

- ***Technical Profile:*** Attribute Management Services
- ***Technical profile:*** Authoritative Attribute Exchange Service

4.5.2.7 (P2/R7) Business Rule 7 – Non-Person Entity (NPE) Resource Data Federation

Business Rule	Description
Non-person entity non-enterprise resource data must be federated to a DOD enterprise repository, either by automated processes or by periodic auditing and updates based on local Army authorization services and the resources they manage.	Resources will be identified by NPE resource names, GUIDs, and other NPE attribute data. This will not be "identity attribute data" in the same sense as for PE. Both logical and physical resources are created and deleted across DOD every day. Tracking and managing these changes as they occur is a monumental task. The need exists for an ongoing automated process where any DOD, Army or other SC can create a local resource in a local ADR that is then automatically discovered by DOD enterprise services. This can be supplemented by the process of proposing new DOD enterprise-level and/or Army resources that can be made available to the JIE immediately. DOD/DISA will have the ability to assess the resource discovery results and add any resource to a JIE entitlement list.

Table 20 – Non-Person Entity (NPE) Resource Data Federation

(P2/R7) Assumptions

- Local resources can exist at the Army or SC level that are not considered enterprise assets.
- New required resource data do not already exist in the EIADRSS.
- Resource data can be federated to the DOD enterprise level by the Army and the other SCs, but would be initially treated only as candidate entitlements to be added to the EIADRSS by DOD/DISA.

(P2/R7) Constraints

- Any NPE resource data added to the JIE data set must be provided by the EIADRSS.

(P2/R7) Risk

- A DAPMS service capability leveraging the EIADRSS will not be possible if resource data cannot be fully and accurately maintained.
- Critical resource availability across the JIE will be limited or possibly prevented if the Army or other SCs create and distribute themselves local resources that they do not report to DOD and that are not instantiated in the EIADRSS.

(P2/R7) Technical Positions and Patterns

P2/R7 Technical Standards Profile

- ***Technical profile:*** Authentication Management Services

4.5.2.8 (P2/R8) Business Rule 8 – Directory Information Updates

Business Rule	Description
DOD business systems, and DOD personnel, when necessary, must populate up-to-date organizational and contact information in DOD authoritative identity data sources.	The Defense Manpower Data Center (DMDC) serves, provides and utilizes personnel, manpower, training, financial and other data for DOD. These data catalogue the history of personnel in the military and their family for purposes of healthcare, retirement funding and other administrative needs. These data sources provide or are capable of providing the required attribute data to support comprehensive PE and NPE identities. However, these data will only be as current and as accurate as what is regularly entered and maintained in these systems.

Table 21 – Directory Information Updates

(P2/R8) Assumptions

- DOD/the Office of the Secretary of Defense (OSD) will provide retired military and civilian employees a uniform DOD identification card that can be easily recognized at any DOD base or facility within the United States and its territories or possessions.

(P2/R8) Constraints

- Access to DMDC (web site) requires a DOD certificate.

(P2/R8) Technical Positions and Patterns

P2/R8 Technical Standards Profile

- ***Technical profile:*** Authoritative Attribute Exchange Service

4.5.3 (P3) Principle 3 – Person Entity and Non-Person Entity Identification

Principle	Description
Identities must be provided for all authorized entities, to include DOD, the Intelligence Community and coalition partner personnel, as well as elements of the infrastructure, such as servers, unmanned aerial vehicles and handheld devices.	Identity data must be developed for all PE and NPE, to include both DOD and non-DOD entities and assets. In some cases, coalition partner personnel can be issued CACs, but in many cases identities will have to be trusted between the Army and other U.S. Government agencies, coalition and industry partners through the Federal Bridge or other secure identity gateway services.

Table 22 – Person Entity (PE) and Non-Person Entity (NPE) Identification

4.5.3.1 (P3/R1) Business Rule 1 – Mobile/Edge Platforms/Devices

Business Rule	Description
The Army will use the digital identity standards established by DOD to support mobile/edge platforms/devices.	Enterprise Identity Management must be consistent in terms of identity data and process workflow for all NPE, from the Business Mission Area to tactical deployed assets, to include all devices that reside in the mobile, platform or sensor computing environments.

Table 23 – Mobile/Edge Platforms/Devices

(P3/R1) Assumptions

- Mobile/edge platforms and devices will have the ability to be credentialed in the same manner as any other NPE.
- CAC or smartcard/token credentials will be the primary mechanism for user authentication for all Mobile/edge platforms and devices.
- Classified user authentication and authorization will use a read-only smartcard/token and not a CAC.
- Other forms of authentication will be available to authenticate and authorize users of Mobile/edge platforms and devices (e.g., explicit login, multiple PINs, test questions).

(P3/R1) Constraints

- Mobile/edge platforms and devices (such as NPEs) will each have a unique identifier and/or X.509 certificate(s).
- Mobile/edge platforms and devices must have the ability to allow authentication while they are operating Disconnected, Intermittent or Low-Bandwidth environments (e.g., classified, tactical).
- No identity data or attributes may be stored on non-volatile media on any mobile/edge platforms or devices.
- A mobile device's unique ID or GUID must be a hardware integrated component of the device that cannot be redefined by users.

(P3/R1) Risk

- Mobile/edge platforms/devices (portable) may not be able to easily interface with CAC readers.
- Resources can easily be compromised if portable computing/communications devices do not provide for at least two-factor authentication.

(P3/R1) Technical Positions and Patterns

P3/R1 Technical Standards Profile

- ***Technical Profile:*** Identity Management

P3/R1 Policy/Regulation Profile

4.5.3.2 (P3/R2) Business Rule 2 – Mobile Device Binding

Business Rule	Description
Authorized mobile devices connected to Army networks will be bound to one or more user groups, and linked to a unique non-person entity identifier and DOD-issued PKI certificate using a digital identity standard registration and binding service.	To optimize overall security and limit exposure to information and networking, all mobile devices will need to be bound to a single or selective set of users and linked to a unique device identifier.

Table 24 – Mobile Device Binding

(P3/R2) Assumptions

- Mobile devices are able to support an identity registration and binding service capability.
- Mobile devices (as NPE) will be identified by a unique ID or GUID in the same manner as any other NPE.

(P3/R2) Constraints

- The registration and binding service must not be made available until user(s) are fully authenticated to each device.
- A mobile device unique ID or GUID must be an integrated component of any device that cannot be redefined without major hardware and/or software modification.
- To better assure device and network/information resource security for mobile devices, a mechanism to unbind quickly and automatically a user(s) from a device must be in place.

(P3/R2) Risk

- A centralized enterprise registration and binding service could be a single major security point of failure for large numbers of mobile devices operating within the JIE.
- Registration and binding services may not operate reliably in mobile Disconnected, Intermittent or Low-Bandwidth environments (e.g., classified, tactical).

(P3/R2) Technical Positions and Patterns (Reference Appendix B – Pattern View)

P3/R2 Technical Standards Profile

- ***Technical Profile:*** **Identity Management**

4.5.4 (P4) Principle 4 – Global Directory Services for Enterprise Services

Principle	Description
A DOD enterprise directory service will allow users to find addresses and contact information for all DOD related personnel and organizations.	At any given time, depending on circumstances and roles, Soldiers, civilians and contractors serving the U.S. military may need to communicate with each other in a digitally safe environment via email and other JIE information and communications services.

Table 25 – Global Directory Services for Enterprise Services

(P4/R1) Business Rule 1 – Global Address List (GAL) Distribution

Business Rule	Description
The DOD enterprise global directory shall provide the ability to disseminate address lists to users of DOD and Army information and communications services.	The GAL is a directory service that contains information for users of Enterprise Email and other services, to include collaboration tools, instant messaging and Unified Capability services (i.e., integrated voice, data and video). JIE enterprise services users will utilize the Enterprise Directory GAL Service in multiple forms, to include but not be limited to: Voice over Internet working protocol (VoIP) lookups File/information resource-sharing user information Unclassified email service account identification Classified email service account identification (a separate GAL based on the Enterprise Directory Service) Peer-to-peer or broadcast video teleconferencing distribution

Table 26 – Global Address List (GAL) Distribution

(P4/R1) Assumptions

- DISA creates and manages the DOD GAL out of the NT-DS and T-DS data sourced from the EIADRSS.
- DOD component mail systems will have the ability to include both DOD hosted and deployed SC tactical mail systems.
- GAL addresses and contact information is federated from Army and other SC mail systems to the DOD enterprise GAL.
- Dissemination of the enterprise GAL for use by disparate mail systems is based on need-to-know access policies.

(P4/R1) Constraints

- Any federated SC GAL address and contact information must first be reviewed and approved at the DOD level before being added to an enterprise-level DS and GAL/GAL views.
- Access to the GAL to support email services must be network-specific, depending on information resource security classification.
- GAL service structure and content must be agnostic to the hardware and software that it supports.

(P4/R1) Risk

- Significant impact to operations and information security would occur in the event that GAL information and GAL updates were intercepted by unauthorized entities.

(P4/R1) Technical Positions and Patterns (Reference Appendix B – Pattern View)

P4/R1 Technical Standards Profile

- ***Technical Profile:*** **Digital Certificate (PKI)**

4.5.4.2 (P4/R2) Business Rule 2 – Global Address List (GAL) Views

Business Rule	Description
DOD's global address list must allow for segmented views by Army organization, location/facility and/or operating unit.	In addition to the DOD enterprise GAL, SCs and their operating units and agencies will require much smaller segmented views of the GAL. These can be provided as an enterprise service to all of the SCs via NT-DSs and T-DSs for DoD organizational views, and could also provide SC-specific GAL views. Distribution groups and views of any form of requester must also be supported. Similarly, resource views must also be provided as subsets of the resources identified in the DoD GAL.

Table 27 – Global Address List (GAL) Views

(P4/R2) Assumptions

- GAL views will be sourced from and synchronized with the DOD enterprise GAL.
- Views will be maintained in accordance with the information/network classification environments that they are intended to support.

(P4/R2) Constraints

- Organizations and operating units have access to GAL views only on a need-to-know basis.
- GAL view updates must be near real-time at a minimum, based on an appropriate Service-Level Agreement.

(P4/R2) Risk

- View-control spillages will allow sensitive user information to appear to unauthorized information/network classification environments.
- Loss of DOD enterprise GAL and DOD GAL view synchronization will result in access gaps among users of JIE enterprise services.
- Loss of the DOD enterprise GAL and SC GAL view synchronization will result in access gaps within and among the SCs.

(P4/R2) Technical Positions and Patterns

P4/R2 Technical Standards Profile

- ***Technical Profile:*** **Global Directory Services for Enterprise Services**

4.5.4.3 (P4/R3) Business Rule 2 – Global Address List (GAL) Data Schema

Business Rule	Description
The Army will utilize the DOD directory service that provides a common data schema to support a global address list, as well as segmented views of it, where its data schema is a subset of the total DOD enterprise identity attribute data schema.	The directory service data schema must be agnostic to the device and applications utilizing the GAL or GAL views, regardless of the information being delivered to the end user. NT-DS and T-DS GAL data schemas will be characterized by a common data schema, which is a selective set of attributes sourced from the enterprise attribute repository (i.e., EIADRSS).

Table 28 – Global Address List (GAL) Data Schema

(P4/R3) Assumptions

- The software and hardware used to access the GAL and GAL views comply with DISA Security Technical Implementation Guides (STIGs).
- EIADRSS will provide NT-DS and T-DS attribute data using either scheduled or triggered web service data calls.
- The directory service data schema is agnostic to the device and applications utilizing the GAL or GAL views, regardless of the information being delivered to the end user.

(P4/R3) Constraints

- Applications that use the NT-DS, T-DSs, GAL and GAL views and search services must have a Certification of Networthiness (CoN).
- Web services used by GAL/GAL view services must utilize a standard web service data protocol.
- The NT-DS and T-DS GAL data schemas must be based on a common data schema, which is a selective set of attributes sourced from the enterprise attribute repository (i.e., EIADRSS).

(P4/R3) Risk

- Changes to the NT-DS and T-DS data schema may impact the accuracy and effectiveness of all GAL services used by applications.
- Application software updates may create security vulnerabilities or introduce interoperability problems within applications that utilize GAL services.

(P4/R3) Technical Positions and Patterns

P4/R3 Technical Standards Profile

- ***Technical Profile:*** Global Directory Services for Enterprise Services

4.5.4.4 (P4/R4) Business Rule 4 – Local Offline Address Book (OAB) Availability

Business Rule	Description
Army personnel will have access to a local directory address book that is	There are times when Army email and other enterprise services users will not have network access, but still require

available when network connectivity is not available, and that is synchronized with a DOD directory service when network connectivity is available.	access to a GAL and GAL views. An offline service will allow users to properly identify the correct resources that can be accessed. Because this service is subject to regular change, including removal of authorized requesters and resources, it must be regularly synchronized with EDSs when network connectivity is sufficiently available. The Army must determine the acceptable time lapse between sync points, and be willing to assume any consequential security and/or operational risks involved.

Table 29 – Local Offline Address Book (OAB) Availability

(P4/R4) Assumptions

- Both the JIE and the user's organizational or operating unit address book are accessible offline.
- An OAB will support access to address information both internal and external to the user's organization or operating unit.
- The local OAB synchronizes with a DOD directory service when network connectivity outages occur, and re-synchronized when connectivity is re-established.

(P4/R4) Constraints

- OAB information at rest and in transit must be protected by encryption, and must be distributed in a secure manner.
- OABs must not be made available to offline users who are not locally authenticated.

(P4/R4) Risk

- Mobile hardware devices that have downloaded an address book could be lost or stolen.
- Digital artifacts of a downloaded address book may remain on decommissioned or reassigned hardware, potentially providing unauthorized users access to DOD personnel information.

(P4/R4) Technical Positions and Patterns (Reference Appendix B – Pattern View)

P4/R4 Technical Standards Profile

- ***Technical Profile:*** Global Directory Services for Enterprise Services

4.5.4.5 (P4/R5) Business Rule 5 – Directory/Global Address List (GAL) Information Concurrency

Business Rule	Description
Army users must be able to obtain address information on all current and valid JIE enterprise services users from anywhere, at any time and from any authorized device, via the global address list and/or views.	Fixed and mobile devices, regardless of hardware/OS type, provide DOD authorized users a capability to access enterprise services from any authorized device, thus enhancing the portable communications ability of all Army personnel.

Table 30 – Directory/Global Address List (GAL) Information Concurrency

(P4/R5) Assumptions

- An email user can be authenticated from any device.
- The device being used to access DOD email is capable of assuring reliable and secure authentication mechanisms (i.e., tokens).

(P4/R5) Constraints

- User authentication must be tied to information/network classification.

(P4/R5) Risk

- Users sometimes lose mobile devices.
- Users may mistakenly transmit sensitive information on the DOD network.
- Hardware used to access information may be operational in unsecured areas.

(P4/R5) Technical Positions and Patterns (Reference Appendix B – Pattern View)

P4/R5 Technical Standards Profile

- ***Technical Profile:*** Global Directory Services for Enterprise Services

4.5.5 (P5) Principal 5 – Authentication and Authorization

Principle	Description
Army requesters of logical and physical DOD and Army resources will be granted specific access based on who they are, where they are and their assigned mission (i.e., mission roles, operational functions, operating area/location).	Access decisions will require dynamic analysis of PE and NPE identity attributes used by access policy components. Persona, roles or functions for any requester of information or physical access are expected to be constantly updated through their authoritative data source(s). These updates must be made readily available to maintain the accuracy of the policy decision and enforcement actions.

Table 31 – Authentication and Authorization

4.5.5.1 (P5/R1) Business Rule 1 – Authentication and Authorization Scope

Business Rule	Description
All Army information services and applications must uniquely identify and authenticate users and devices using a common DOD authentication service model, regardless of the logical or physical resources to which access is being requested.	The foundation of any access control architecture includes an authentication service to affirm and re-affirm at regular intervals or via unscheduled audits that any PE or NPE is who/what they claim to be and possesses a certain persona. The effectiveness of any authorization service can be impacted by not performing this due diligence. This function can be provided by the current and collapsing DOD Microsoft AD infrastructure and other components, such as the EASF and the AAF.

Table 32 – Authentication and Authorization Scope

(P5/R1) Technical Positions and Patterns

P5/R1 Technical Standards Profile

- ***Technical Profile:*** Identity Based Access Control (IBAC)
- ***Technical Profile:*** Identity Management
- ***Technical Profile:*** Credential Management
- ***Technical Profile:*** Secure Shell
- ***Technical Profile:*** Digital Certificate (PKI)

4.5.5.2 (P5/R2) Business Rule 2 – Identity Service For Tactical Edge

Business Rule	Description
The Army will utilize persona and role definitions for both person entities and non-person entities at the tactical edge, and will maintain concurrency with all similar DOD enterprise identity management services when network connectivity is available.	DOD mission operations will require requester and resource identity service across all of the SCs to support all Joint and coalition force PE and NPE at the tactical edge. This service will be initially sourced from an ADR as an enterprise digital identity service, and further supported by an enterprise DS and by NT-DSs at CONUS (continental United States) base/post/camp/station or T-DSs in OCONUS (outside the continental United States) locations. All other non-tactical, tactical, JIE and other SC IdAM components will be dependent on the receipt and consumption of these data, which applies to PE and NPE requester identities as well as NPE resource identity attribute data.

Table 33 – Identity Service for Tactical Edge

(P5/R2) Assumptions

- Internal DOD SCs and Joint PE and NPE will have established identities based on DOD-provisioned and -managed credentials (i.e., X.509 Certificates).
- External non-DOD and coalition PE and NPE will have pre-established trusted credentials to the appropriate internal DOD PE and NPE.
- Coalition PE and NPE will not be issued DOD CACs.

(P5/R2) Constraints

- Digital identities at the tactical edge must be portable and reusable during all phases of the ARFORGEN cycle.
- Non-DOD and coalition partner trusted credentials must assure a high degree of non-repudiation.

(P5/R2) Risk

- The limited ability to establish the preferred and optimally reliable non-DOD and coalition partner credentialing mechanism (i.e., X.509 Certificates) for authentication will create a greater possibility of unauthorized access to DOD information and physical resources.
- Theater personas required to support tactical operations may change often enough that they must be maintained in real time or near-real time to assure that authorization is adequately accurate and reliable.

(P5/R2) Technical Positions and Patterns (Reference Appendix B – Pattern View)

P5/R2 Technical Standards Profile

- ***Technical Profile:*** Identity Based Access Control (IBAC)

4.5.5.3 (P5/R3) Business Rule 3 – Global Information Resource Access

Business Rule	Description
The DOD authentication service will support global access to Army systems, applications, files and data by requesters anywhere, using any type of device, when connectivity to the DOD Global Information Grid is available.	The Army must be able to operate within the JIE such that it is able to access information and resources from any device belonging to any Computing Environment. This requires that devices and their users be vetted for authentication and then authorized to connect to any appropriate requested information resource from any location.

Table 34 – Global Information Resource Access

(P5/R3) Assumptions

- The Authentication Service is Computing Environment/device agnostic.
- Mobile devices will use the same authentication service mechanisms and protocols as fixed or non-mobile clients.

(P5/R3) Constraints

- Requester re-authentication is required when a Disconnected and/or Network-Disadvantaged Disconnected, Intermittent or Low-Bandwidth (e.g., classified, tactical environments) device is reconnected to any network or network-based resource.

(P5/R3) Technical Positions and Patterns (Reference Appendix B – Pattern View)

P5/R3 Technical Standards Profile

- ***Technical Profile***: Secure Shell

P5/R3 Policy/Regulation Profile

- Army IdAM RA to Army Regulation (AR) 25-2 Mapping

4.5.5.4 P5/R4) Business Rule 4 – Access and Policy Security

Business Rule	Description
Army access policies shall be protected in the same manner as DoD policies allowing read-only capability to access control services and the components that utilize them.	Limiting the transport, replication and remote storage of identity attribute data will minimize possibilities for compromise.

Table 35 – Access and Policy Security

(P5/R4) Assumptions

- An administrative interface is available to the PS to accommodate additional, modified or updated policies.

(P5/R4) Constraints

- Army access policies shall allow read-only capability to access control services and the components that utilize them.
- Authorization components in any IdAM architecture must minimize the exposure of identity attribute data.
- All authentication and authorization services and their supporting infrastructures must assure minimal exposure of sensitive identity data, at rest or in transit (e.g., PII, persona attribute data).
- RE components shall have read-only access to identity ADRs.

(P5/R4) Technical Positions and Patterns

P5/R4 Technical Standards Profile

- ***Technical Profile***: Identity Based Access Control (IBAC)
- ***Technical profile:*** Authentication Management Services
- ***Technical Profile:*** Secure Shell

4.5.5.5 (P5/R5) Business Rule 5 – Availability of DoD Enterprise Authentication and Authorization Services

Business Rule	Description
When connectivity to the DOD GIG is available, the Army will utilize DOD enterprise-level authentication and authorization services to allow access to both local Army and JIE information resources.	Perpetuation across the JIE of stovepiped mechanisms to permit a requester of information to access one or more resources using a single access request must be discontinued. The SSOS and RSOS will address this limitation and provide the capability to both non-tactical and tactical JIE resources. Immediately, the Army's *Google Docs* services will be supported by this capability.

Table 36 – Availability of DoD Enterprise Authentication and Authorization Services

(P5/R5) Assumptions

- The current AKO SSO and RSO services will be replaced.
- Any SSOS and RSOS will support either public or private cloud services, hosted by either a commercial service provider (e.g., Google Apps, Microsoft Azure) or DOD/DISA.
- Future Web Apps that are not PKI-ready will be supported by DOD Enterprise Authentication and Authorization services.

(P5/R5) Technical Positions and Patterns

P5/R5 Technical Standards Profile

- ***Technical Profile:*** Secure Shell

P5/R5 Policy/Regulation Profile

- Army IdAM RA to Army Regulation (AR) 25-2 Mapping

4.5.5.6 (P5/R6) Business Rule 6 – Availability of Army (Non-DOD Enterprise) Authentication and Authorization Services

Business Rule	Description
When connectivity to the DOD GIG is not available, the Army will utilize local Army authentication and authorization services to allow access to only local Army information resources.	All authentication and authorization services and their supporting infrastructures must leverage DOD enterprise services when they are available. In tactical operating environments, this is not always possible. Therefore, a T-ASF or T-AAF must be available when no or poor network connectivity exists, but it must follow all of the business rules established in this RA for both authentication and authorization services.

Table 37 – Availability of Army (Non-DoD Enterprise) Authentication and Authorization Services

(P5/R6) Assumptions

- An administrative interface is available to the PS to accommodate additional, modified or updated policies.

(P5/R6) Constraints

- All authentication and authorization services and their supporting infrastructures must leverage DOD enterprise services when they are available.
- In tactical operating environments, a T-ASF or T-AAF must be available in all DIL environments.
- T-ASFs and T-AFFs must follow all of the business rules established in this RA for both authentication and authorization services.

(P5/R6) Technical Positions and Patterns

P5/R6 Technical Standards Profile

- ***Technical profile:*** Authentication Management Services
- ***Technical profile:*** Authoritative Attribute Exchange Service

4.5.6 (P6) Principle 6 – Dynamic Access Policy Management

Principle	Description
Access decisions must be dynamically configurable to support changing mission needs, attack response and level of information service and network resource availability.	The Dynamic Access Policy Management Service (DAPMS) will provide a flexible and robust decision and enforcement mechanism to accommodate changes in user privileges and policy related to resource access decisions. This allows the selection of attributes based on various PE or NPE identity factors to define persona, as well as unique characteristics of the requested resource. General DOD IA policy and the threat environment at the time of the transaction influence the need to have a dynamic access-control and management capability.

Table 38 – Dynamic Access Policy Management

4.5.6.1 (P6/R1) Business Rule 1 – Policy Management Service Scope

Business Rule	Description
Army identity management services must include a policy management service with a policy repository that can be created and/or modified to accommodate changes in identity attributes, persona, person entity roles, resource entitlements and/or operating location.	To provide secure, timely control and access to all resources, accurate, reliable and timely information about resources, users and devices is required. Pairing this information results in the creation of rules/policies that define which attributes a requester must have in order to access a particular resource**.** A Policy Decision Point (PDP) identifies the relevant access policies, and provides direction based on those policies to a Policy Enforcement Point (PEP), where an authorization protocol is executed either to permit or deny an access request.

Table 39 – Policy Management Service Scope

(P6/R1) Assumptions

- The authentication service will be based on identity attributes that are made available by ADR.
- The authentication service will be the major control gate that allows the access policies to be retrieved and executed.
- A common DOD resource directory is available through an AAF resource data federation service.
- The single authentication service will support both PE and NPE authentication.
- The PEP protocol is capable of authorizing access at either the network domain or information resource levels.

(P6/R1) Technical Positions and Patterns (Reference Appendix B – Pattern View)

4.5.6.2 (P6/R2) Business Rule 2 – Standard Attribute Model

Business Rule	Description
The Army will utilize a DOD standard attribute model to enable dynamic access policy management for all Army personnel, services and assets.	The standard attribute model includes a common set of agreed upon attributes as defined by Communities of Interest, and establishes and publishes a standardized format for each agreed upon attribute. These formats must be interoperable across the Army Generating and Operational forces, and able to be verified, updated or deleted, as required, when adequate network connectivity is available.

Table 40 – Standard Attribute Model

(P6/R2) Technical Positions and Patterns

Core Standards and Pattern View (Ref: Appendix B)

4.5.6.3 (P6/R3) Business Rule 3 – Standard Access Policies

Business Rule	Description
The JIE and the Army must utilize established DOD access policies, and be able to create new policies that can be utilized at the Army and DOD enterprise levels as part of a dynamic policy management service capability.	Access policies will be maintained in a PS that will be a consumer of both PE and NPE requester attribute data, as well as of NPE or information resource data. The PS will ensure proper DOD access rights are granted to the correct users, and that they utilize a DOD enterprise Authentication and Authorization Framework to access DOD and/or SC resources (networks, information & facilities). The Rules Engine (RE) is responsible for managing user access permissions and consists of three sub-services: 1) Policy Enforcement Point (PEP); 2) Policy Decision Point (PDP); and 3) PS. The PDP permits or denies a user's request for access, based on the information it receives from the PEP. The PEP receives the requester's credentials from the PDP, and extracts the requester's PII attribute data from the EIADRSS and delivers it to the PS.

Table 41 – Standard Access Policies

(P6/R3) Assumptions

- An authentication service will support DAPMS for both non-tactical and physical access control.
- A PS can be limited to a set of standard policy templates that can utilize current identity attribute data in order to execute in real time or near–real time.
- A PS can be a set of complete policies, including all of the imbedded pertinent identity attribute data.

(P6/R3) Constraints

- The RE components that reside in the DOD IdAM Enterprise Service's DAPMS must use common syntax.
- A RE will function normally, optimally and securely if and only if real-time or near-real-time attribute data are available to the policy templates.
- When the DAPMS is not available, users must not be authorized to access DOD networks and information resources.

(P6/R3) Risk

- Non-virtual DOD IdAM DAPMS infrastructure can be a single point of failure for all users of DOD information resources.

4.5.6.4 (P6/R4) Business Rule 4 – Policy Change Management Responsibility

Business Rule	Description
The responsible owner of any access-controlled logical or physical resource will have the ability to request new and/or modified Army resource access policies.	Resource owners are responsible for identifying and tagging their information resources (all levels) as a major enabler of DAPMS policies. For this BR, a resource is defined in further detail as a digital object, an information service or repository, a facility or other NPE that is made accessible to any requester.

Table 42 – Policy Change Management Responsibility

(P6/R4) Assumptions

- A common DOD information resource portal service will use all resource access policies that have been created and are being maintained for them.

(P6/R4) Constraints

- Access Policy changes to JIE-available Army resources must not be solely managed by the Army.
- Policy template, structures and syntax must be identical across the JIE.
- All access policies must be in compliance with federal laws and DOD guidance, as well as SC regulations.

(P6/R4) Risk

- If access policy management cannot be automated and governed rapidly and reliably, the process for implementing new or modifying existing access policies may be lengthy, thus causing possible operational capability functional gaps and delays.

(P6/R4) Technical Positions and Patterns (Reference Appendix B – Pattern View)

4.5.6.5 (P6/R5) Business Rule 5 – Policy Attribute Validation

Business Rule	Description
The policy decision process shall return an appropriate trusted token to the requesting authorization service to allow access, only if the concurrency and validity of all identity requester and resource attribute data used in the policies being executed can be verified with a high degree of confidence.	Only when both PE and NPE Requester attribute data can be validated or used with a high degree of confidence, can the appropriate secure tokens be created and passed to the proper authorization or policy enforcement (i.e., connection) service.

Table 43 – Policy Attribute Validation

(P6/R5) Assumptions

- An alternative form of trusted credentials for non-DOD and coalition PE and NPE has been issued.
- External non-DOD and coalition PE and NPE credentials are trusted by the appropriate internal DOD NPE.
- Policy decisions are based on current and executable policies.

(P6/R5) Constraints

- Coalition PE must not be issued DOD CACs
- DOD access control components must accept alternative credentials.
- Non-DOD and coalition partner trusted credentials must assure a high degree of non-repudiation.
- Non-DOD and coalition partner trusted credentials must be capable of supporting two-factor authentication.
- Before an access policy is fully executed and authorization controls are applied, attributes utilized in the policy's execution must be affirmed, as well as the basic structure, taxonomy and language of the policies themselves.

(P7) Principle 7 – Access to Data, Services and Applications

Principle	Description
All authenticated and authorized entities using approved devices will have timely access to applications and services, and the ability to share critical data across the Army and the DOD.	Information resource access can only be made available to computing/communications devices used within the JIE through a flexible authentication and authorization capability. Data and applications resources will need to be made available at many different levels, each of which requires proper access management through both authentication and authorization services.

Table 44 – Access to Data, Services and Applications

4.5.7.1 (P7/R1) Business Rule 1 – Information Resource Types

Business Rule	Description
DOD and the Army must provide services that can enable access to any DOD and Army logical resource, such as information systems, databases, applications/services, files, data queries and granular data elements.	Both PE and NPE will require access to information/data provided by multiple resource types, including systems that support one or more applications, databases, files and data; individual applications, software and networking service instances; and standalone instances of files and granular data elements. IdAM and its enabling services will assure that the right requesters will be granted access to all of the resources they require.

Table 45 – Information Resource Types

(P7/R1) Assumptions

- All information systems and data resources are classified as NPE.
- A set of identity attributes exists for each information resource type and data element.

(P7/R1) Constraints

- Every information system/device (as an NPE) must have a valid and unique credential (i.e., PKI certificate).
- Every information system/device will have a unique permanent NPE identifier, and any PE will have an EDI-PI (e.g., mobile device Electronic Serial Number).
- Access to information resources must be dictated by a managed and automated set of security policies.

(P7/R1) Risk

- Changes in information resource attributes that are not conveyed either in real time or near-real time to RE mechanisms may impact authorization requests.
- Portability of information JIE-available resources requires careful management and distribution of their identity attributes and associated access polices across the entire JIE.

4.5.7.2 (P7/R2) Business Rule 2 – Logical NPE Layered Logical Access Control

Business Rule	Description
Access to logical non-person entities, including groups, systems, applications, data, devices and all other forms of Army assets, regardless of security classification level, must be granted based on a separate authentication and authorization process at each logical boundary/layer.	If physical access authorization cannot be provided adequately for a given environment (e.g., for multiple access control points), then a second level of validation will be required. Typically, for a PE, this will be a visual inspection by a security officer at a DOD facility. If and only if CAC-based access control cannot be provided, a separate but similar access control card can be used as an interim solution, until such time as the CAC capability is made available.

Table 46 – Logical NPE Layered Logical Access Control

(P7/R2) Assumptions

- Logical NPE is characterized by groups, distribution lists, systems, software/applications, data and other Army intellectual or informational assets.

(P7/R2) Technical Positions and Patterns

P7/R2 Technical Standards Profile

- ***Technical Profile:*** Standardized Policy Languages

4.5.7.3 (P7/R3) Business Rule 3 – Public Key Infrastructure (PKI) Based Authentication

Business Rule	Description
Access to all Army and DOD systems, databases, applications/services, files, data queries and granular data elements must be supported by a Public Key Infrastructure-based authentication service.	Verifiable PKI-based credentials issued by DOD in the form of CACs and other hard tokens (e.g., SIPRNET token smart cards) must be made available to every PE who requests data and/or services from any DOD resource. The electronic certificates, encryption and password controls provided as components of PKI-based services will be applied to authenticate all access requesters before any information resource is made available. All PKI CAC or token resident information will be encrypted both locally and for any secure transport token information that transits a DOD network.

Table 47– Public Key Infrastructure (PKI) Based Authentication

(P7/R3) Assumptions

- An X.509 certificate management service will be available at all times, unless there is a loss of infrastructure and/or local or wide-area network connectivity failure impacting it. In such cases, any Army authentication and/or access authorization service will limit access to one or more local devices only.

(P7/R3) Constraints

- PKI transactions will be transported across network boundaries encapsulated in Security Assertion Markup Language (SAML) tokens for Web Service (WS) or WS-protocols
- Kerberos, Simple Sockets Application Programming Interface (SSAPI) and Secure Socket Layer (SSL)/Transport Layer Security (TLS) protocols and their secure transport will be used when SAML/WS cannot.

(P7/R3) Risk

- An unauthorized user or malicious hacker may attempt to hijack a SAML token and replay it to gain illicit access to DOD information resources (i.e., a replay attack).

(P7/R3) Technical Positions and Patterns

P7/R3 Policy/Regulation Profile

- Army IdAM RA to Army Regulation (AR) 25-2 Mapping

4.5.7.4 (P7/R4) Business Rule 4 – Data Resource Identification

Business Rule	Description
Data owners must identify and classify all data resources to more effectively create and maintain access control policies for all Army resources that reside on the Global Information Grid.	The Army and DOD must migrate to tagging all applications or standalone data at rest. Army applications/software development and COTS procurement organizations must begin building their information services and programs of record using a standardized XML-based resource/data tagging methodology and taxonomy. Legacy information resources must be analyzed to see whether this migration can be executed or whether their data and services should be consolidated to an environment where data tagging can be accomplished. System, application and/or data asset owners will be responsible for tagging their own data in accordance with this rule. At a minimum, the tag values and resource linkage relationships must be known to and stored in the Attributes Data Repository and/or the Policy Store.

Table 48 – Data Resource Identification

(P7/R4) Assumptions

- Data tagging is standardized for all JIE information resources.
- Data tagging is XML based and conforms to a standard metadata schema.

(P7/R4) Constraints

- Data tagging must conform to approved DOD standards (i.e., DOD IT Standards Registry).
- The DOD enterprise DAPMS must confirm that a data tag has been applied to all data resources to which authorization policy can be applied.
- Data tags must be maintained and synchronized in all attribute data that identify information resources (e.g., in a DAPMS PS with NPE resource attribute data provided by the EIADRSS).

(P7/R4) Risk

- Without regular auditing to ensure the consistency of data tags at both the JIE and SC levels, resources will not be correctly identified and authorization policies cannot be executed correctly.
- Failure to synchronize data tags in all ADRs may prevent authorized resource access or allow unauthorized resource access.

4.5.7.5 (P7/R5) Business Rule 5 – Rules Engine (RE) Personally Identifiable Information (PII) Attribute Exposure

Business Rule	Description
Rules Engines components will not store or retain Personally Identifiable Information attribute data if the supporting attribute data repository and any related policy decision and/or enforcement service are not collocated and integrated components within a common local infrastructure.	When the Policy Store is not a collocated component of an RE, it would only need to be a source of basic policy templates that are made available to the PDP. The PDP requires both requester and resource identity attributes, sourced from an ADR, to make a policy decisions. It is critical to protect PII exposure to the greatest extent possible. Identity attribute data must be accessed and deleted internal to the PDP after it has rendered its access decision and either refused the access request or passed its approval to the PEP. Once this has occurred, the PDP no longer requires these data. This eliminates one additional possible point of PII exposure and compromise across DOD networks.

Table 49 – Rules Engine (RE) Personally Identifiable Information (PII) Attribute Exposure

(P7/R5) Assumptions

- If the PS is not collocated with the other sub-components of RE, requester PII data will be required to transit a network in order to be consumed by an RE.
- The PDP will render decisions based on the same PII attribute data that are used by the DOD enterprise AAF and SSOS.

(P7/R5) Constraints

- PS will not be collocated with PII when adequate networking capability is available.
- All PII attribute data in transit and temporarily at rest must be encrypted.
- The PDP must internally and automatically delete all PII attribute data after it has rendered its access decision.
- PE identity attribute data must be accessed, utilized and deleted by the RE sub-services (i.e., PDP and PS).
- The EIADRSS must provide all PII attribute data to the RE.
- The PDP must retrieve all PII attribute data that are required to render an access decision via the DOD enterprise AAF, SSOS and RSOS, which are sourced from the EIADRSS.
- If not collocated with the RE, the PS must internally and automatically delete all PII attribute data after it has completed providing services to the PDP.
- The PEP must never receive any PII attribute data.

(P7/R5) Risk

- Any failure to deliver authoritative and accurate PII attribute data to the RE will result in an authorization failure and allow access to unauthorized resources.
- Separation and duplication of ADR sources and PSs to support the RE over a network increase the possibility of PII compromise.

(P7/R5) Technical Positions and Patterns (Reference Appendix B – Pattern View)

4.5.7.6 (P7/R6) Business Rule 6 – Data Tagging Development

Business Rule	Description
Identity attribute data, to include data tagging and other metadata at rest and in transit across the Global Information Grid (GIG) and any Army network, must conform to quotas to reduce storage requirements, and implement quality-of-service management to reduce network transport payloads.	System, application and/or data asset owners will be responsible for tagging their own data in accordance with this rule. This requires efficient use of data tagging structure, level of information and standardized metadata schema to minimize network overhead. At a minimum, the tag values and resource linkage relationships must be known to and stored in the identity Attribute Data Repository and/or the Policy Store. Data tagging guidelines must be developed to establish limits regarding what data at what level must be tagged in order to reduce network transport requirements and the complexity of information resource storage and management.

Table 50 – Data Tagging Development

(P7/R6) Assumptions

- Data tagging is standardized, at a minimum, within the individual SC information resources.
- Data tagging is XML-based, and conforms to a standard metadata schema.

(P7/R6) Constraints

- Data tagging must conform to approved DOD (i.e., DISR) standards.
- A DOD enterprise RE must constantly re-confirm that a data tag has been applied to all application and data resources to which authorization policy can be applied.
- Data tags will be maintained and synchronized in a DAPMS PS with those utilized by the EIADRSS.
- All Service Components will use a common SDK.
- All SCs must use the same standards schema and syntax.

(P7/R6) Risk

- Without regular auditing to ensure the consistency of data tags at both the JIE and SC levels, resources will not be correctly identified and authorization policies cannot be executed correctly.
- Failure to synchronize data tags in all ADRs may prevent authorized resource access or allow unauthorized resource access.
- Unless data tagging is protected on the information resource side as well as at the RE, a flaw in XML encryption can leave web services carrying tag metadata vulnerable to attacks and “hijacking”.

(P7/R6) Technical Positions and Patterns

P7/R6 Technical Standards Profile

- ***Technical Profile:*** Standardized Policy Languages

P7/R3 Policy/Regulation Profile

- **Army IdAM RA to Army Regulation (AR) 25-2 Mapping**

4.5.7.7 (P7/R7) Business Rule 7 – Standardized Policy Languages

Business Rule	Description
Systems, applications and/or data asset owners must create and maintain access policies using XACML, WS policy and other industry standard markup languages.	XACML is a current standard access policy rules markup language, and should be used for all new DOD systems/applications access policies. If current DOD authorization services, such as those within Microsoft AD, are not supported by XACML, then a migration plan must be put in place to make this transition where possible. Only approved versions of XACML will be allowed, and backward compatibility will be required to ensure interoperability with legacy information resources.

Table 51 – Standardized Policy Languages

(P7/R7) Assumptions

- DoD and the SCs will create, concur on and collectively maintain XACML-based access policies using the same SDK for all authorization services that can be supported by XACML.

(P7/R7) Constraints

- Existing legacy systems must create and implement a migration plan if they are not currently compliant.

(P7/R7) Technical Positions and Patterns

P7/R7 Technical Standards Profile

- ***Technical Profile:*** Standardized Policy Languages

4.5.7.8 (P7/R8) Business Rule 8 – Access Policy Data Tagging Metadata Standards

Business Rule	Description
Systems, applications and/or data asset owners will be responsible for creating and maintaining XACML-based policies using standardized data tagging metadata structures.	XACML-based access policies must be supported by metadata structures, such as DDMS and TDF. Some backward compatibility will be required to ensure interoperability with metadata structures used by legacy information resources.

Table 52 – Access Policy Data Tagging Metadata Standards

(P7/R8) Technical Positions and Patterns

P7/R8 Technical Standards Profile

- ***Technical Profile:*** Policy in Credentialing

P7/R8 Policy/Regulation Profile

- Army IdAM RA to Army Regulation (AR) 25-2 Mapping

4.5.7 (P8) Principle 8 – Physical Access

Principle	Description
All authorized Army entities will have timely access to physical facilities and assets anywhere within any DOD and Army operating environment or location.	All PEs will require access to DOD installations and facilities, ranging from post/camp/station to deployed tactical environments, to perform their mission functions. Access policies must control who gains access to what, and be able to revoke this access as required.

Table 53 – Physical Access

4.5.8.1 (P8/R1) Business Rule 1 – Non-Person Entity (NPE) Unique Identifier

Business Rule	Description
Every non-person entity physical resource must be assigned an enduring unique identifier or index for each set of attributes that define it.	A unique identifier will be required to identify all NPE, and established in the EIADRSS, will support authentication and authorization services and will be used as a basis for granting or denying access to any Resource. This establishes an enduring index for all other attributes related to any resource. The standards for NPE identifiers and attributes are still under development at the DOD level.

Table 54 – Non-Person Entity (NPE) Unique Identifier

(P8/R1) Technical Positions and Patterns

P8/R1 Technical Standards Profile

Technical profile: Authoritative Attribute Exchange Service

4.5.8.2 (P8/R2) Business Rule 2 – Physical Access Control Policies

Business Rule	Description
Physical access to DOD and Army facilities and other non-person entity assets will be enforced by access control policies.	Similar to access policies related to information resources, access policies that define who gains access to which facility, equipment or any other physical NPE will be required.

Table 55 – Physical Access Control Policies

(P8/R2) Technical Positions and Patterns

P8/R2 Technical Standards Profile

- ***Technical Profile:*** Cryptography Algorithms
- ***Technical Profile:*** Attribute Management Services

4.5.8.3 (P8/R3) Business Rule 3 – Non-Person Entity (NPE) Attribute Verification

Business Rule	Description
The Army must implement processes to continuously verify and maintain attributes related to physical assets/non-person entities.	In the same manner as for PEs, NPE attribute data must be maintained and kept as accurate and as current as possible. This is a key factor in maintaining access to facilities, weapons systems, ordnance and other physical DOD assets.

Table 56 – Person Entity (NPE) Attribute Verification

(P8/R3) Assumptions

- Subclass 1 logical NPEs are things such as buildings, installations, rooms, areas and other locations and facilities.
- Subclass 2 logical NPEs can include groups of information resources/data, distribution lists printers and other physical assets.

(P8/R3) Technical Positions and Patterns

P8/R3 Technical Standards Profile

- ***Technical Profile:*** Attribute Management Services

4.5.8.4 (P8/R4) Business Rule 4 – Facilities Attributes Management

Business Rule	Description
Owners of Army facilities and physical assets will be responsible for defining the required resource identity attributes and attribute data using a standard structure and taxonomy, and making them available to supplement DOD enterprise-level identity attributes.	The responsibility of correctly identifying all NPE will belong to the NPE owner, who must be required to follow standards for structure and content to present the access policy criteria and/or create the access policies themselves.

Table 57 – Facilities Attributes Management

(P8/R4) Technical Positions and Patterns

P8/R4 Technical Standards Profile

- ***Technical Profile:*** Attribute Management Services
- ***Technical profile: Authoritative*** Attribute Exchange Service

4.5.8.5 (P8/R5) Business Rule 5 – Common Access Card (CAC) Credential Mechanism

Business Rule	Description
The principal credential mechanism for identity authentication to allow access to any facility or physical asset will be the Common Access Card -DOD PIV credential.	The DOD CAC, with integrated smart card technology, bar code and magnetic strip storage mechanisms, is one form of DOD credential mechanism standard that should be used by both PE and NPE. It can support multiple physical access systems, but the desired environment is CAC-based PKI, the same as for access control to all logical resources. Access to classified and/or tactical resources currently requires use of a separate token smart card.

Table 58 – Common Access Card (CAC) Credential Mechanism

(P8/R5) Technical Positions and Patterns

P8/R5 Technical Standards Profile

- ***Technical Profile:*** Common Access Card (CAC)

4.5.8.6 (P8/R6) Business Rule 6 – Common Access Card (CAC) Enrollment

Business Rule	Description
For all forms of physical access, Army credential validation must be supported by visual inspection of a CAC, enrolling the CAC in a local access control system and/or issuance of a separate card associated with a local physical access system.	Typically, for a PE, visual inspection by a security officer at a DOD facility will be the initial process for access authorization. This may be the only process available if and only if CAC-based access control cannot be provided. A separate but similar access control card (i.e., non-CAC) may have to be used as an interim solution, until such time as a CAC, or other form of facility-specific credentials become available.

Table 59 – Common Access Card (CAC) Enrollment

(P8/R6) Technical Positions and Patterns

P8/R6 Technical Standards Profile

- ***Technical Profile:*** Common Access Card (CAC)

4.5.8.7 (P8/R7) Business Rule 7 – Layered Physical Access Control for Subclass Type 1 Physical NPEs

Business Rule	Description
Physical access to non-person entities, including Army bases, buildings, rooms, areas and all other forms of Army real property, regardless of security classification level, must be granted based on a separate authentication and authorization action at each physical boundary/layer.	If physical access authorization cannot be adequately provided for given environments (e.g., for multiple access control points), then a second level of validation will be required.

Table 60 – Layered Physical Access Control for Subclass Type 1 Physical NPEs

(P8/R7) Assumptions

- Subclass 1 physical NPEs are characterized by locations/areas, bases, installations, facilities, buildings, rooms and other Army real property assets.

(P8/R7) Technical Positions and Patterns

P8/R7 Technical Standards Profile

- ***Technical profile:*** Authentication Management Services
- ***Technical profile: Authoritative*** Attribute Exchange Service

4.5.8.8 (P8/R8) Business Rule 8 – Layered Physical Access Control for Subclass Type 2 Physical NPEs

Business Rule	Description
Physical access to non-person entities, including hardware, devices and all other forms of Army assets, regardless of security classification level, must be granted based on a separate authentication and authorization action at each physical boundary/layer.	If physical access authorization cannot be adequately provided for given environments (e.g., for multiple access control points), then a second level of validation will be required.

Table 61 – Layered Physical Access Control for Subclass Type 2 Physical NPEs

(P8/R8) Assumptions

- Subclass 2 physical NPEs include hardware, devices and other Army assets.

(P8/R8) Technical Positions and Patterns

P8/R8 Technical Standards Profile

- ***Technical profile:*** Authentication Management Services
- ***Technical profile:*** Authoritative Attribute Exchange Service

4.5.8.9 (P8/R9) Business Rule 9 – Physical Access Control – Subclass Type 1 NPE Asset Naming

Business Rule	Description
All Army physical non-person entity names for Army assets must conform to the approved DOD NPE identification and naming standards, and the NPE must be assigned a DOD PKI certificate that will be applied to all physical access policies and controls.	The current DOD NPE attribute and naming standards are in final draft. In addition to digital identities based on these NPE attributes, every NPE will be supported by one or more PKI certificates that will be issued and managed by the DOD. This will allow DOD to issue, revise, or revoke access credentials for any NPE at any time.

Table 62 – Physical Access Control – Subclass Type 1 NPE Asset Naming

(P8/R9) Assumptions

- Subclass 1 physical NPEs are characterized by locations/areas, bases, installations, facilities, buildings, rooms and other Army assets.

(P8/R9) Technical Positions and Patterns

P8/R9 Technical Standards Profile

- ***Technical Profile: Digital*** Certificate (PKI)

4.5.8.10 (P8/R10) Business Rule 10 – Physical Access Control – Subclass Type 2 NPE Asset Naming

Business Rule	Description
All Army physical non-person entity names for Army asset must conform to the approved DOD NPE identification and naming standards and, the NPE must be assigned a DOD PKI certificate that will be applied to all physical access policies and controls.	Any Army asset that is not real property can be transported from one location to another. These are Army property elements and include any physical object that can be identified and tracked. To ensure that only authorized assets are allowed into certain locations, facilities or other Army operating areas, they must be identifiable and manageable using access policies.

Table 63 – Physical Access Control – Subclass Type 2 NPE Asset Naming

(P8/R10) Assumptions

- Subclass 2 physical NPEs include hardware, devices and other Army assets.

(P8/R10) Technical Positions and Patterns

P8/R10 Technical Standards Profile

- ***Technical Profile: Digital*** Certificate (PKI)

4.5.8 (P9) Principle 9 – General IdAM Security Policy

Principle	Description
A comprehensive security policy must exist to address all aspects of identity management services and establish the Cybersecurity/security guidelines required to mitigate threats to related infrastructures, both internal and external to Army and DOD networks.	All IdAM services and their infrastructure components must conform to approved DOD security policies. These may apply to the individual service areas or to specific services within those areas. Many overarching IA standards will also be applicable (e.g., authentication mechanism transport, cross-domain capabilities and information classification restrictions).

Table 64 – General Identity and Access Management (IdAM) Security Policy

4.5.9.1 (P9/R1) Business Rule 1 – Identity Attribute Data Validation

Business Rule	Description
Digital identity attribute data must be validated within Army and DOD networks and systems to ensure that it conforms to relevant DOD-approved standard schema.	Proper access to logical and physical resources will depend on the accuracy of the digital identity data by which they are defined. The IdAM service infrastructure must provide the capability to regularly validate this data. This can only occur if a standard data schema that can be verified/re-verified on both a scheduled and ad hoc basis, as required, is employed. This capability is essential to ensuring that the authorization service executes effectively and securely.

Table 65 – Identity Attribute Data Validation

(P9/R1) Technical Positions and Patterns

P9/R1 Technical Standards Profile

- ***Technical Profile***: Biometric Validation

P9/R1 Policy/Regulation Profile

- ***Technical Profile:*** Policy in Credentialing

4.5.9.2 (P9/R2) Business Rule 2 – Authorization Service Scope

Business Rule	Description
Authorization services must be utilized within Army networks to support access to both Army and DOD systems, applications and other information resources being utilized by the Army.	To ensure that the correct users of Army and JIE information resources (e.g., Enterprise Email) have access to what they require to perform their operational roles, without introducing unwarranted security threats, an authorization service is required to perform this function once requesters have been fully authenticated. This service should be available to any requester across the JIE.

Table 66 – Authorization Service Scope

(P9/R2) Technical Positions and Patterns

P9/R2 Technical Standards Profile

- ***Technical Profile:*** Policy in Credentialing

P9/R2 Policy/Regulation Profile

- ***Technical Profile:*** Policy in Credentialing

4.5.9.3 (P9/R3) Business Rule 3 – Enterprise Information Sharing

Business Rule	Description
Army information resources that enable the sharing or transfer of information across multiple security levels must be centrally planned and coordinated, with proposed service enhancements aimed at optimizing enterprise services to the greatest extent possible.	To ensure that JIE information resources handle the transmission of data over the network securely, SC and DOD organizations must coordinate with each other when planning to implement their boundary protection and content management infrastructure in such a way as to optimize discoverability and usability of information resources.

Table 67 – Enterprise Information Sharing

(P9/R3) Technical Positions and Patterns

P9/R3 Policy/Regulation Profile

- ***Technical Profile:*** Policy in Credentialing
- ***Technical Profile:*** Policy in Authentication

4.5.9.4 (P9/R4) Business Rule 4 – Information Resource Authentication Frequency

Business Rule	Description
All Army networks, applications, information resources and devices must persistently digitally identify and re-authenticate users and/or devices.	Protection of JIE information resources requires that all forms of access be restricted to authorized individuals. To optimize the accuracy of authorization of PE and NPE requesters, all entities will be authenticated every time an attempt is made to access an information resource or a device and/or network that supports the access. Automated timeouts and other default re-authentication prompts must be leveraged to force any requester to re-authenticate after a reasonable period of inactivity or following a lapse in network connectivity.

Table 68 – Information Resource Authentication Frequency

(P9/R4) Technical Positions and Patterns

P9/R4 Technical Standards Profile

- ***Technical Profile:*** Web Services Security
- ***Technical Profile:*** Attribute Management Services

4.5.9.5 (P9/R5) Business Rule 5 – Cross-Domain Security

Business Rule	Description
All Army enterprise-level directory services will preserve cross-domain security while satisfying identity management service requirements that traverse multiple DOD and Army security enclaves.	Currently, the Army and the DOD enterprise are comprised of numerous heterogeneous security enclaves that exist within and across all DOD networks (e.g., NIPRNET, SIPRNET and the Joint Worldwide Intelligence Communications System). They differ in information classification level and/or the type of security infrastructure that protects them. This rule ensures that the enterprise-level directory services provide the path to access the multitude of resources that are accessible via a DOD network or networks. Only appropriate approved information or data elements can be transferred to an authorized requester. Preservation of security for information at its native security classification level must be assured, regardless of the networks it transits.

Table 69 – Cross-Domain Security

(P9/R5) Technical Positions and Patterns

P9/R5 Technical Standards Profile

- ***Technical Profile***: Identity Management

P9/R5 Policy/Regulation Profile

- Army IdAM RA to Army Regulation (AR) 25-2 Mapping

4.5.9.6 (P9/R6) Business Rule 6 – Information Resources Availability

Business Rule	Description
Army information resources, including data assets, services and applications, must be accessible to all authorized DOD requesters, except where limited by law, policy, security classification or unique operational requirements.	Various DOD missions, tasks and projects require authorized DOD personnel (i.e., Soldiers, government civilians and contractors) to access authoritative DOD information services and resources that reside on DOD networks. This business rule mandates that DOD IdAM services and infrastructure conform to all federal, state and local laws, policies and regulations in terms of making the right information available to the right authorized requesters. Enabling network-access enforcement or control points will protect the JIE from potential enemies attempting to access and steal sensitive information, as well as damage key infrastructure components.

Table 70 – Information Resources Availability

4.5.9.7 (P9/R7) Business Rule 7 – Information/Data Resources Protection

Business Rule	Description
Army information resources, including applications and computer networks, must protect data in transit and at rest according to their confidentiality level, Mission Assurance Category and level of exposure when executing identity management and encryption services.	Data protection begins by assuring that only authorized users are authenticated to the required networks and information resources. The next step is to assure that the users are accurately authorized to access the resources themselves. It is equally important to protect the data generated, transmitted and stored by resources that DOD personnel utilize. They must have the capability to encrypt data so that they are only consumable by authorized DOD personnel. This encryption must protect the data regardless of status (i.e., in transit, at rest). The encryption strength, the level of protection and the exposure of encryption keys should be aligned with the various levels of information or resource sensitivity.

Table 71 – Information/Data Resources Protection

(P9/R7) Technical Positions and Patterns

P9/R7 Technical Standards Profile

- ***Technical Profile***: Cybersecurity

P9/R7 Policy/Regulation Profile

- ***Technical Profile:*** Policy in Credentialing
- Army IdAM RA to Army Regulation (AR) 25-2 Mapping

4.5.9.8 (P9/R8) Business Rule 8 – DOD Enterprise Trust Management

Business Rule	Description
DOD Trust Management policies shall be established and enforced to provide common identity management processes across the Army.	In order to accomplish a cohesive and interoperable information resource-sharing environment, DOD must develop a policy that directs all DOD organizations to employ a common identity authentication processes. These policies must be in accordance with federal guidance and direction that addresses trust negotiation among DOD components, mission, and coalition and industry partners to provide assured access to all authorized entities. Established and maintainable trust relationships, both intra- and inter-DOD (e.g., coalition partners, commercial contractors) will allow the level of granularity of access policies to be minimized, relying on those higher-level trusts to a greater degree.

Table 72 – DOD Enterprise Trust Management

(P9/R8) Technical Positions and Patterns'

P9/R8 Technical Standards Profile

P9/R8 Policy/Regulation Profile

- ***Technical Profile:*** Policy in Credentialing
- Army IdAM RA to Army Regulation (AR) 25-2 Mapping

4.5.9.9 (P9/R9) Business Rule 9 – Alternate Authentication Mechanisms (Non-CAC/Token)

Business Rule	Description
Alternate authentication mechanisms must be provided for all non-CAC requesters of Army resources, as well as supplemental authentication for Army requesters using CACs or other hard-token credentials to access Army and/or DoD resources.	CAC/PKI-only authentication to network services, which includes content delivery systems, hampers soldier, civilian and contractor access to training and education content at the point of need. Further, populations that are ineligible for a CAC, such as the Individual Ready Reserve, ROTC cadets, new recruits, state agency partners, first responders and verified family members, cannot access applications that require PKI-based authentication.

Table 73 – Alternate Authentication Mechanisms (Non-CAC/Token)

(P9/R9) Assumptions

- Non-DoD entities and assets will be able to present trusted and verifiable credentials for access to both information and physical facilities and networks.

(P9/R9) Technical Positions and Patterns (Reference Appendix B – Pattern View)

P9/R9 Technical Standards Profile

P9/R9 Policy/Regulation Profile

- ***Technical Profile:*** Policy in Credentialing
- Army IdAM RA to Army Regulation (AR) 25-2 Mapping

4.5.9.10 (P9/R10) Business Rule 10 – Data Encryption

Business Rule	Description
All Army digital identity data will use encryption methods to ensure data integrity and protection of sensitive and regulated information (e.g., PII) and authentication data transport.	Though DOD networks have many layers of security across multiple security enclaves/boundaries, the identities of individuals with access to information resources and facilities must be protected at all times, within and between them. Encryption of PII, other identity attribute data, secure token exchanges and rules engine components, along with securing the network infrastructure itself, is required.

Table 74 – Alternate Authentication Mechanisms (Non-CAC/Token)

(P9/R10) Technical Positions and Patterns

P9/R10 Technical Standards Profile

- ***Technical Profile:*** Encryption & Decryption
- ***Technical Profile***: Cryptography Algorithms

P9/R10 Policy/Regulation Profile

- ***Technical Profile:*** Policy in Credentialing
- Army IdAM RA to Army Regulation (AR) 25-2 Mapping

4.5.9.11 (P9/R11) Business Rule 11 – SHA-256: Secure Hashing Algorithm Migration

Business Rule	Description
All new Army information systems and enterprise IdAM infrastructure components will implement Secure Hash Algorithm (SHA)-256 encryption where possible, or must develop a plan to migrate all systems supported by PKI to SHA-256.	The SHA is one of a number of cryptographic hash functions published by the National Institute of Standards and Technology as a U.S. Federal Information Processing Standard. SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512) designed by the National Security Agency. SHA-256 uses 32-bit words when hashing. Directing all DOD enterprise PKI and IdAM services and their corresponding infrastructure components to implement the SHA-256 standard ensures a more powerful and common encryption capability.

Table 75 – SHA-256: Secure Hashing Algorithm Migration

(P9/R11) Technical Positions and Patterns

P9/R11 Technical Standards Profile

- ***Technical Profile***: Credential Management
- ***Technical profile:*** Authoritative Attribute Exchange Service

4.5.9 (P10) Principle 10 – Single Sign-On and Reduced Sign-On

Principle	Description
Army identity and access management services must allow requesters to access information, services and physical resources without having to be authenticated and authorized to each individual resource, with or without the use of a credential mechanism.	The Army must minimize the number of authentication prompts that users are required to face. SSO and RSO services that can be utilized in both non-tactical and tactical operating environments are needed at the DOD and SC levels. SSO will be used to provide access to resources that must be limited on a need-to-know basis or according to organizational, functional or operational areas, where a requester does not need to be authenticated for every resource access request. RSO can include an imbedded SSO function, but the requester does not have to possess a hard digital identity credential (e.g., CAC, token smart card).

Table 76 – Single Sign-On (SSO) and Reduced Sign-On (RSO)

4.5.10.1 (P10/R1) Business Rule 1 – SSO and RSO Directory Data Population

Business Rule	Description
Identity information used by the Army to enable single sign-on or reduced sign-on services must be automatically populated from a DOD enterprise directory service.	The EIADRSS will provide all identity attribute data to the NT-DSs and T-DSs using an automated mechanism (e.g., Simple Object Access Protocol call, web service "pull" or "push").

Table 77 – SSO and RSO Directory Data Population

(P10/R1) Assumptions

- Core identity attributes are made available via the EIADRSS and user address information via the NT-DSs and T-DSs.
- SC directory services can be directly managed by the SCs.
- Identity records are enduring, unless deactivated or deleted based upon administrative decision and action.

(P10/R1) Risk

- The quality of SC-level directory service concurrency depends on the combined level of latency of all identity information passing from the DOD authoritative data sources to the NT-DSs and T-DSs.

(P10/R1) Technical Positions and Patterns

P10/R1 Technical Standards Profile

- ***Technical Profile:*** Identity Based Access Control (IBAC)
- ***Technical profile:*** Authentication Management Services

4.5.10.2 (P10/R2) Business Rule 2 – Electronic Data Interchange Personal Identifier (EDI-PI)

Business Rule	Description
For Army single sign-on and reduced sign-on services, the Army will use the DOD Electronic Data Interchange Personal Identifier (EDI-PI) to tie any PE uniquely to a DOD DMDC-formatted enterprise user name or DOD Enterprise Email display name format.	All EDI-PI will be uniquely linked to a single enterprise DOD requester or user. A consistent approach for the naming of any DOD PE (i.e., requester) must be utilized to establish a standard linkage to the EDI-PI.

Table 78 – Electronic Data Interchange Personal Identifier (EDI-PI)

(P10/R2) Technical Positions and Patterns

P10/R2 Technical Standards Profile

- ***Technical Profile:*** Identity Based Access Control (IBAC)
- ***Technical profile:*** Authentication Management Services

4.5.10.3 (P10/R3) Business Rule 3 - SSO and RSO Services Availability

Business Rule	Description
The Army must utilize DOD enterprise single sign-on and reduced sign-on services when connectivity to the Global Information Grid (GIG) is available, and utilize local services when it is not.	Re-synchronization of SSO and RSO services will be required after periods of network outage, when connectivity to GIG and Army networks is restored and reasonable stable. The Army will have to establish time thresholds for outages to determine when re-synchronization will be required.

Table 79 – SSO and RSO Services Availability

(P10/R3) Technical Positions and Patterns

P10/R3 Technical Standards Profile

- ***Technical profile: Authoritative*** Attribute Exchange Service

P10/R3 Policy/Regulation Profile

- Army IdAM RA to ***Army*** Regulation (AR) 25-2 Mapping

4.5.10 (P11) Principle 11 – Network Access Controls

Principle	Description
Permission to or denial of access to Army and DoD network nodes for any device must be based on access policies that leverage specific sets of networking attributes.	The interconnectedness of the Internet puts information resources of DoD systems at risk. Requesters of DoD services may want to access desired and/or required resources from unknown or unauthorized digital environments. Providing access to requesters operating in these environments has the potential to jeopardize the security of DoD systems and networks. Empowering the identity and access management system with the capability to control DoD systems and network access based on predefined digital characteristics of a network (e.g., TCP ports or range of ports, IP addresses, devices ID, etc.) adds another layer of security to the protection of DoD resources.

Table 80 – Network Access Controls

4.5.11.1 (P11/R1) Business Rule 1 – Authorization Policy Network Attributes

Business Rule	Description
Army authorization policies must utilize one or more network attributes, as required, to identify information resources available on the Global Information Grid and any Army network.	Remote users attempting to acquire access to DoD networked resources can introduce unintentional security risk into an Army or DoD/JIE system. Though a user may have the proper credentials to access the JIE under normal conditions, at times the remote network environment by which a user is trying to access the JIE may be unknown or known to be untrustworthy. In these and similar scenarios, the JIE must have established protection policies that enable it to make decisions on whether to permit or deny access to a user based upon the network that is being utilized to gain access.

Table 81 – Authorization Policy Network Attributes

(P11/R1) Assumptions

- Authorization access policies are established by DISA and the governing SC.
- All JIE information or system resources will be listed in the DoD NT-DSs and T-DSs.

(P11/R1) Constraints

- Common network attributes must be used to identify all DoD information resources.

(P11/R1) Risk

- Access to the NT-DSs and T-DSs will provide an unauthorized user access to information pertaining to all DoD resources that are available to the JIE.

(P11/R1) Technical Positions and Patterns

P11/R1 Technical Standards Profile

- ***Technical Profile:*** Attribute Management Services

P11/R1 Policy/Regulation Profile

- ***Technical Profile:*** Policy in Authentication

4.5.11.2 (P11/R2) Business Rule 2 – Network-Connected Device Authentication

Business Rule	Description
For all Army network-connected devices, prior to granting authorization to enterprise resources, user authentication must first be executed at the standalone-device level, then at the enterprise Army or DoD level using an enterprise authentication service.	Authentication is required to authorize access to local devices and information, as well as networked resources. Redundant authentication provides synchronization between local devices and their stored information as well as DoD networks. It ensures that proper access rights are given to proper users regardless of whether network connectivity is available.

Table 82 – Network-Connected Device Authentication

(P11/R2) Assumptions

- Electronic devices that have access to DoD resources and networks have a local authentication service installed.
- Local and DoD enterprise authentication services are synchronized.
- The DoD enterprise authentication service is the authoritative source for verifying and authenticating a user's credentials.
- Synchronization between local and DoD enterprise authentication services occurs when a device has connectivity to the DoD network.

(P11/R2) Constraints

- Electronic devices must be password protected.
- Electronic devices must be encrypted.
- A user has a set number of device incorrect log-in attempts to gain access to the device and network before the user is locked out of the local device and DoD networks.

(P11/R2) Risk

- Long periods without connectivity to DoD authentication services could allow unauthorized access to a local device.

(P11/R2) Technical Positions and Patterns (Reference Appendix B – Pattern View)

P11/R2 Technical Standards Profile

- ***Technical Profile:*** Identity Based Access Control (IBAC)
- ***Technical Profile:*** Common Access Card (CAC)

4.5.11.3 (P11/R3) Business Rule 3 –Disconnected, Intermittent or Low-Bandwidth Authentication

Business Rule	Description
For all Army Network-Disadvantaged Disconnected, Intermittent or Low-Bandwidth devices, identity authentication will be executed by the local device authentication service, but authorization to information resources will be limited to resources on that standalone device until the requester is authenticated at the DoD enterprise level or by an Army network or domain authentication service.	Digital information required by DoD personnel resides on resources accessed via DoD networks. Electronic devices (i.e., desktop and laptop computers, mobile phones, digital checkpoints) are the platforms that utilize DoD information. These devices must be operational and connected to and/or disconnected from DoD networks. When connected to the DoD network, the DoD enterprise authentication service authenticates the user for access to the device, network or entrance point. When a device is disconnected from the JIE, consumers of DoD information must still be able to access information stored locally on DoD devices. User devices not connected to DoD networks will need a local authentication service to approve access to those devices that cannot access the DoD enterprise authentication service.

Table 83 – Network-Disadvantaged Disconnected, Intermittent or Low-Bandwidth Authentication

(P11/R3) Assumptions

- Authentication to all DoD devices, connected and/or disconnected, is required.
- The user's CAC holds the proper credentials used for authentication to the local device.

(P11/R3) Constraints

- Authentication for a new user to access a local device and DoD networks must initially be performed by the DoD Enterprise IdAM services.
- Access should be denied to a user trying to access an unconnected device for the first time.

(P11/R3) Risk

- CAC credentials/certificates are the only means to control or revoke access to a disconnected device.

(P11/R3) Technical Positions and Patterns (Reference Appendix B – Pattern View)

P11/R3 Technical Standards Profile

- ***Technical Profile***: Identity Management
- ***Technical Profile:*** Common ***Access*** Card (CAC)

P11/R3 Policy/Regulation Profile

- Army IdAM RA to Army Regulation (AR) 25-2 Mapping

4.5.11.4 (P11/R4) Business Rule 4 – Network Gateway Authentication and Authorization

Business Rule	Description
The Army must be able to access both Army and DoD information systems and services using standard extensions or common network gateways for integration between network domains.	Secure DoD enterprise authentication and authorization service access requires that common gateways be made available to extended DoD networks that support individuals in a particular collaborative virtual environment. Extended DoD networks (physical and logical) employing the use of these gateways will provide connectivity to enterprise authentication and authorization services and further extend access to the resources that are spread across multiple network domains or enclaves.

Table 84 – Network Gateway Authentication and Authorization

(P11/R4) Assumptions

- The DoD enterprise authentication service is the authoritative source for verifying and authenticating a user's identity and credentials.
- All extended networks have resident (local) authentication and authorization services available.
- All users accessing DoD networks and JIE information resources must possess a CAC.

(P11/R4) Constraints

- Common gateways must meet DoD cross-domain security requirements and policies, where applicable.
- Extended networks without a common gateway will not have access to DoD enterprise authentication and authorization services.

(P11/R4) Risk

- A network gateway that allows access to DoD enterprise authentication and authorization services can also provide a possible intruder point of entry to another network and its available information resources.

(P11/R4) Technical Positions and Patterns

P11/R4 Technical Standards Profile

Technical Profile: Cryptography Algorithms

4.5.11 (P12) Principle 12 – Monitoring and Reporting

Principle	Description
Provide for both proactive and reactive monitoring and reporting on all forms of Army logical and physical access.	Auditing services will need to comply with all established DoD service-level agreements for both the DoD network and information systems/applications/data services. This is required to assure an appropriate level of Cybersecurity, as well as to optimize both network and information systems reliability and response time.

Table 85 – Monitoring and Reporting

4.5.12.1 (P12/R1) Business Rule 1 – Auditing Services

Business Rule	Description
Access management auditing shall be provided by the Army to support both real-time and historical logical and physical access control activity, as well as a security-event analysis capability.	It will be necessary to complement the IdAM service infrastructure monitoring and reporting capabilities with the ability to easily and readily analyze both real-time and historical data. This will improve the overall Cyber defense capability, as well as serve as a basis for creating and maintaining access authorization policies across the JIE.

Table 86 – Auditing Services

(P12/R1) Assumptions

- Offline Address Books (OAB) will be auditable.

(P12/R1) Technical Positions and Patterns

P12/R1 Technical Standards Profile

- ***Technical Profile***: Cryptography Algorithms

P12/R1 Policy/Regulation Profile

- ***Technical Profile: Policy*** in Authentication
- Army ***IdAM*** RA to Army Regulation (AR) 25-2 Mapping

4.5.12.2 (P12/R2) Business Rule 2 – Identity and Access Management (IdAM) Infrastructure-Monitoring/Reporting

Business Rule	Description
The status of both Army and DoD enterprise-level authentication and authorization services infrastructure shall be monitored in accordance with pertinent GIG-wide Service-Level Agreements (SLAs) in order to detect, isolate and react to intrusions, disruption of service or other incidents that threaten Army and DoD-wide operations.	Auditing services will need to comply with all established DoD SLAs for DoD network and information systems, applications and data services. This is required to assure an appropriate level of Cybersecurity, as well as to optimize both network and information systems reliability and response time.

Table 87 – Identity and Access Management (IdAM) Infrastructure-Monitoring/Reporting

(P12/R2) Technical Positions and Patterns

P12/R2 Technical Standards Profile

- ***Technical Profile:*** Global Directory Services for Enterprise Services

P12/R2 Policy/Regulation Profile

- Army IdAM RA to Army Regulation (AR) 25-2 Mapping

Appendix B - Vocabulary and Terms

TERM	DEFINITION	AUTHORITATIVE SOURCE
Access Control	The capability of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).	CNSSI 4009 DoD IdAM RA OV-1, AV-1, OV-1, AV-2 EOC-SA AV-2 EOC-SA Enterprise Goal to Capability Relationship CV-4 EOC-SA CV-2 JIE EOC RA AV-2, 9/22/2013 JIE_NNT_WAV_AV2-JIE-WAN_V0.3_Draft_2013-09-16 JIE_I1_WAN_CV2_Submitted_V0.2_2013-05-03 JIE_WAN_NNT_CV1-JIE WAN_V0.2_Draft_2013-03-29 JIE_NNT_WAN_CV-Capabilities to Requirements Mapping_V0.1_Draft_2013-09-16 JIE_NNT_WAN_CV-2-Multi-Variant Analysis_V0.1_Draft_2013-09-16 JIE_I1_NNT_CV4_Submitted_V0.1_2013-03-29, 9/16/2013 JIE EA C2.1.3 and JIE IdAM CV-2 AB DoD IEA, v1.2, 7 May 2010 DoD JIE-EA, 9 April 2013 JIE EA C2.2 and JIE IdAM CV-2 A2, 9/16/2013 DoD JIE-EA, 9 April 2013
Access	Controlling access to systems and resources based on established identity information and access policies that determine an enforceable decision	JIE_NNT_WAV_AV2-JIE-WAN_V0.3_Draft_2013-09-16
Account	The set of attributes that together define a security principal in a given service. Each service may define a unique set of attributes to define an account. An account defines a security principal or system's access to a resource or service.	Army IdAM RA V3.0
Attribute	A named quality or characteristic inherent in or ascribed to someone or something.	National Strategy for Trusted Identities in Cyberspace

TERM	DEFINITION	AUTHORITATIVE SOURCE
Authentication	The ability to verify the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.	JIE EA C2.1.3.2
Authoritative Data Source	A recognized or official data production source with a designated mission statement or source/product to publish reliable and accurate data for subsequent use by customers. An authoritative data source may be the functional combination of multiple, separate data sources.	DOD Directive 8320.03
Authorization	The process of granting or denying specific requests for obtaining and using information processing services or data and to enter specific physical facilities.	DOD IdAM RA v0.7
Authorization Attributes	IdAM data elements used to make authorization decisions. Examples include security clearance, citizenship, billet, organizational affiliation, certifications of training or education, and other specific attributes. Authorization attributes can include attributes from other data categories.	DOD IdAM RA v0.7
Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.	FICAM Roadmap and Implementation Guidance Version 1.0
Credentialing	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.	FICAM Roadmap and Implementation Guidance Version 1.0
Data	Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities	Joint Publication 1-02, January 31, 2011

TERM	DEFINITION	AUTHORITATIVE SOURCE
	to which meaning is or might be assigned.	
Digital Identity	The unique set of attribute values (i.e., characteristics) by which an entity can be distinguished from any other entity in a digital environment.	DOD IdAM RA v0.7
Directory	An information source used to store information about objects.	Army IdAM RA V3
Directory Service	A Directory Service is a structured repository of information commonly used for managing data about DOD users, computers, and resources. Within the DOD, Directory Services are widely used to manage end-user devices, user accounts, resource authorization, and policies required to maintain positive control of an IT environment.	AV-2 IdAM AGS Integrated Dictionary AV-2 IdAM Directory Services Descriptions DRAFT SV-1 IdAM AV-2 IdAM Integrated Dictionary
Dynamic Access Control	Automated, data driven authentication and authorization decisions to DOD resources, anywhere, at any time.	DOD IdAM Strategy
Entity	An independent unit or distinguishable person, place, thing, event, or concept about which information is kept that has distinct features, objects, or attributes associated with it.	DOD IdAM Strategy
Federated Identity	A principal's identity is federated between a set of providers when there is an agreement between the providers on a set of identifiers and/or attributes to use to refer to the principal.	OASIS Security Assertion Markup Language (SAML) V2.0
Federation	A server-to-server link that permits the exchange of Presence information and IM between two systems.	UCR 2008 Change 3
Identity	A set of characteristics by which an entity (e.g., human, application, device, service or process) is recognizable and is	DOD Identity Management Strategic Plan

TERM	DEFINITION	AUTHORITATIVE SOURCE
	sufficient to distinguish that entity from every other entity.	
Identity Management	The ability to create, define, govern, and synchronize the ownership, utilization, and safeguarding of identity information	JIE EA C2.1.1
Non-Person Entity	An entity with a digital identity that is not a person. Examples include an organization, facility (building, conference room, and installation), application, device, network, and unstructured data (documents, imagery, etc.).	DOD IdAM Strategy
Person Entity	A human being with a digital identity.	DOD IdAM Strategy
Physical Access Control System	- A human, automated, or electronic system or procedure that controls the ability of people or vehicles to enter a protected area, by means of authentication and authorization at designated Access Control Points. - An automated system that manages the passage of people or assets through an opening(s) in a secure perimeter(s) based on a set of authorization rules.	- DOD IdAM Strategy - DOD Security Lexicon - FICAM Roadmap and Implementation Guidance Version 2.0
Policy Management	Ability to create and manage policies used to enable rapid modification of access, resource allocation, or prioritization (e.g., bandwidth, processing, and storage) through enterprise-wide, policy-based management in response to changing mission needs or threats	DOD IEA v1.2d

TERM	DEFINITION	AUTHORITATIVE SOURCE
Security Principal	A digital identity with an account and one or more credentials that can be authenticated and authorized to interact with the system and resources on the network.	Army IdAM RA V3
Single Sign On	A mechanism by which a single act of user authentication and log on enables access to multiple independent resources.	FICAM 2.0
Trust	A state that describes the agreements between different parties and systems for sharing identity information.	Army IdAM RA V3

Appendix C - Acronyms

Acronym	Definition
AAF	Authentication and Authorization Framework
AD	Active Directory
ADA	Authorized Data Access
AES	Advanced Encryption Standard
AKO	Army Knowledge Online
APS	Account Provisioning Service
ARFORGEN	Army Force Generation
AR	Army Regulation
BMA	Business Mission Area
C2	Command and Control
C4I	Command, Control, Communications, Computers, and Intelligence
CA	Certificate Authority
CAC	Common Access Card
CGA	Cryptographically Generated Addresses
CI	Critical Infrastructure
CMS	Cryptographic Message Syntax
COI	Communities of Interest
CONOPS	Concept of Operations
COTS	Commercial Off-The-Shelf
CRL	Certificate Revocation Lists
DBC	Defense Business Council
DCGS	Distributed Common Ground System
DEERS	Defense Enrollment and Eligibility Reporting System
DI2E	Defense Intelligence Information Enterprise
DIEA	Defense Information Enterprise Architecture
DIL	Disconnected, Intermittent or Low-Bandwidth
DIMA	Defense Intelligence Mission Area
DISA	Defense Information Systems Agency
DMDC	Defense Manpower Data Center
DOD	Department of Defense
DS	Directory Service
E2E	Enterprise to Enterprise
EA	Enterprise Architecture
EDI-PI	Electronic Data Interchange Personal Identifier
EDS	Enterprise Directory Services
EFS	Encrypting File System
EIEMA	Enterprise Information Environment Mission Area
ePACS	Electronic physical access control systems
ESP	Encapsulation Security Payload
ESR	Enterprise Strategy and Implementation Roadmap

Acronym	Definition
ETA	Enhanced Trusted Agent
FDCC	Federal Desktop Configuration Control
FICAM	Federal Identity Credential and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAL	Global Address List
GIG	Global Information Grid
GOTS	Government Off-The-Shelf
GRC	Government Risk and Compliance
GUID	Globally Unique Identifiers
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
IBAC	Identity Based Access Control
ICAM	Identity Credential and Access Management
IdAM	Identity and Access Management
IEA	Information Enterprise Architecture
IPSEC	Internet Protocol Security
IPT	Integrated Planning Team
ISC	Interagency Security Committee
IT	Information Technology
JIE	Joint Information Environment
JIOC	Joint Intelligence Operations Center
JROC	Joint Requirements Oversight Council
JS JS	Joint Staff J6
JTF-GNO	Joint Task Force-Global Network Operations
LRA	Local Registration Authority
MitM	Man in the Middle
NAP	Network Access Protection
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
OAB	Offline Address Book
OCSP	Online Certificate Status Protocol
OMB	Office of Management and Budget

Acronym	Definition
P/C/S	posts/camps/stations
PACS	Physical Access Control Systems
PCC	Personal Category Code
PDP	Policy Decision Point
PE	Person Entity
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RA	Reference architecture
RA	Registration Authority
RBAC	Role Based Access Control
RE	Rules Engine
RFID	wireless non-contact use of radio-frequency electromagnetic fields to transfer data
RP	Relying Party
SAML	Security Assertion Markup Language
SCAP	Security Content Automation Protocol
SC	Service Component
SCEP	Simple Certificate Enrollment Protocol
SLA	Service Level Agreement
SOA	Service-Oriented Architecture
SSO, RSO	Single Sign-on, Reduced Sign-on
TA	Trusted Agent
TMS	Token Management System
UBE	User-based enforcement
USGCB	United States Government Configuration Baseline
WMA	Warfighter Mission Area
XML	Extensible Markup Language

Appendix D - Industry Standards

ISO/IEC 24760-1 A framework for identity management—Part 1: Terminology and concepts
ISO/IEC CD 24760-2 A Framework for Identity Management—Part 2: Reference architecture and requirements
ISO/IEC WD 24760-3 A Framework for Identity Management—Part 2: Practice
ISO/IEC 29115 Entity Authentication Assurance
ISO/IEC WD 29146 A framework for access management
ISO/IEC WD 29003 Identity Proofing and Verification
ISO/IEC 29100 Privacy framework
ISO/IEC 29101 Privacy Architecture
ISO/IEC 29134 Privacy Impact Assessment Methodology

Appendix E - References

Advanced Encryption Standard (AES 256)
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135)
http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf

DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act" http://uscgaux8er.info/DHS11000-9.pdf

DHS 4300A DHS Sensitive System Policy
http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf

DHS 4300A Sensitive Systems Handbook
http://www.uscg.mil/acquisition/nais/RFP/SectionJ/dhs-4300A-handbook.pdf

DHS MD 0565 Personal Property Management Directive
http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_0565_personal_property_management_direc tive.pdf

DHS MD 11042.1 Safeguarding Sensitive But Unclassified (For Official Use Only) Information
http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_110421_safeguarding_sensitive_but_unclassified_information.pdf

DHS MD 4010.2 Section 508 Program Management Office & Electronic and Information Technology Accessibility.
https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_40102_section_508_program_man agement_office_and_information_technology_accessibility.pdf

FD Form 258, "Fingerprint Card" (2 copies) http://fd258.com/ Federal Information Security Management Act of 2002
http://www.govitwiki.com/wiki/Federal_Information_Security_Management_Act

Foreign National Relatives or Associates Statement
http://www.metlang.com/docs/ICE%20Foreign%20Relatives.pdf

HSPD-12 —Policies for a Common Identification Standard for Federal Employees and Contractors http://www.dhs.gov/homeland-security-presidential-directive-12

Interagency Security Committee (ISC) Physical Security Criteria for Federal Facilities guide dated April 12, 2010 http://www.dhs.gov/interagency-security-committee-standards-and- best-practices

NIST FIPS 201 —Personal Identity Verification (PIV) of Federal Employees and Contractors http://csrc.nist.gov/publications/PubsFIPS.html

NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

NIST SP 800-61, Computer Security Incident Handling Guide
http://csrc.nist.gov/publications/drafts/800-61-rev2/draft-sp800-61rev2.pdf?fuseAction=1998Amend

NIST SP 800-63 —Electronic Authentication Guideline
http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

OMB Circular A-130 http://www.whitehouse.gov/omb/circulars_a130_a130trans4/ OMB M-06-16 —Acquisition of Products and Services for Implementation of HSPD-12

http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf

OMB M-10-15 —FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf

OMB M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors
http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf

Privacy Act of 1974 http://www.justice.gov/opcl/privstat.htm

Section 508 1194.2, Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220)
http://www.section508.gov/index.cfm

Section 552a of title 5, United States Code (the Privacy Act)
http://www.justice.gov/opcl/privstat.htm

Standard Form 86, “Questionnaire for National Security Positions”
http://www.opm.gov/Forms/pdf_fill/SF86.pdf

Support Security Content Automation Protocol (SCAP) http://scap.nist.gov/

Title 48, Code of Federal Regulations, Part 1520, as amended, “Policies and Procedures of
Safeguarding and Control of SSI,” as http://www.ecfr.gov/cgi-bin/searchECFR

Title 6, Code of Federal Regulations, Part 29 as amended http://www.ecfr.gov/cgi-bin/searchECFR

U.S. Federal Desktop Configuration Control (FDCC) http://nvd.nist.gov/fdcc/index.cfm

United States Government Configuration Baseline (USGCB) regulations,
http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc

“Framework for Improving Critical Infrastructure Cybersecurity," version 1.0 National Institute of Standards and Technology, February 12, 2014

Appendix F - Technical Positions and Patterns

Technical Profile Tables

DISR Status Values
E - Emerging
M - Mandated
N - Net-centric

IdAM Related Technical Profiles		
Technical Profile: Digital Certificate (PKI)		
Standard ID	**Standard Title**	**DISR Status**
RSA Labs PKCS #12 v1.0:1999 with Corrigendum	PKCS #12: Personal Information Exchange Syntax Standard, version 1.0, and PKCS #12 v1.0 Technical Corrigendum	M
ITU-T X.509:2012	Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, November 2012	M
IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008	M
IETF RFC 2560	IETF Public Key Infrastructure X.509 (PKIX) Online Certificate Status Protocol (OCSP), RFC 2560, June 1999	M
IETF RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)	M
Related Principle & Business Rule		
P1/R4 Technical Standards Profile P2/R3 Technical Standards Profile P2/R2 Policy/Regulation Profile	P4/R1 Technical Standards Profile P5/R1 Technical Standards Profile P8/R9 Technical Standards Profile	P8/R10 Technical Standards Profile
Technical Profile: Key Exchange		
Standard ID	**Standard Title**	**DISR Status**
IETF RFC 4109	Algorithms for Internet Key Exchange version 1 (IKEv1), May 2005	N
IETF RFC 3526	More Modular Exponential (MODP) Diffie-Hellman Groups for Internet Key Exchange (IKE), April 2002	M
IETF RFC 5996	Internet Key Exchange Protocol Version 2 (IKEv2)	M

IETF RFC 4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2), December 2005	M
Related Principle & Business Rule		

Technical Profile: Cryptographic Key Management		
Standard ID	**Standard Title**	**DISR Status**
FIPS Pub 140-2	Security Requirements for Cryptographic Modules, 25 May 2001	M
Related Principle & Business Rule		

Technical Profile: Cryptography Algorithms		
Standard ID	**Standard Title**	**DISR Status**
IETF RFC 4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH), April 2007	M
ANSI/INCITS 359-2004	Information technology - Role Based Access Control (RBAC)	M
CAPP	Controlled Access Protection Profile for Basic Robustness/C2 systems, Version 1.d, NSA, 8 October 1999	M
Related Principle & Business Rule		
P9/R10 Technical Standards Profile P8/R2 Technical Standards Profile	P11/R4 Technical Standards Profile	P12/R1 Technical Standards Profile

Technical Profile: Attribute Management Services		
Standard ID	**Standard Title**	**DISR Status**
ISO/IEC 19794-6:2005	Information technology - Biometric data interchange formats, Part 6: Iris image data, 10 June 2005	M
SAML V2.0 Attribute Sharing Profile for X.509 A-BS	SAML V2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems, Committee Specification 01	E
OASIS SPML v2.0	Service Provisioning Markup Language (SPML) Version 2.0, 1 April 2006	M

DoD EBTS v2.0	DoD Electronic Biometric Transmission Specification, Version 2.0, 27 March 2009	M
ISO/IEC 19794-7:2007 w/Cor1:2009	ISO/IEC 19794-7:2007 w/Cor1:2009	M

Related Principle & Business Rule		
P1/R8 Technical Standards Profile P1/R9 Technical Standards Profile P2/R5 Technical Standards Profile	P2/R6 Technical Standards Profile P8/R2 Technical Standards Profile P8/R3 Technical Standards Profile	P8/R4 Technical Standards Profile P9/R4 Technical Standards Profile P11/R1 Technical Standards Profile

Technical profile: Authentication Management Services

Standard ID	Standard Title	DISR Status
IETF RFC 4302	IP Authentication Header, December 2005	M
IETF RFC 2207	RSVP Extensions for IPSEC Data Flows, September 1997	E
IETF RFC 4303	IP Encapsulating Security Payload (ESP), December 2005	M
	Java Security Services (http://java.sun.com/javase/technologies/security/)	N
IETF RFC 4120	The Kerberos Network Authentication Service (V5), July 2005	M
IETF RFC 2865	Remote Authentication Dial-In User Services (RADIUS), June 2000	

Related Principle & Business Rule		
P5/R4 Technical Standards Profile P5/R6 Technical Standards Profile P8/R7 Technical Standards Profile	P8/R8 Technical Standards Profile P10/R1 Technical Standards Profile	P10/R3 Technical Standards Profile P10/R2 Technical Standards Profile

Technical profile: Authoritative Attribute Exchange Service

Standard ID	Standard Title	DISR Status
SAML 2.0 OASIS	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005	M
W3C Canonical XML 2.0	Canonical XML, Version 2.0, W3C Recommendation, April 2013	M
FIPS Pub 186-4	Digital Signature Standard (DSS) Digital Signature Algorithm (DSA), 19 July 2013	M

XML Signature	XML Signature Syntax and Processing, W3C Recommendation, 12 February 2002	M
	Biometric APIs (u)	
ISO/IEC 24709-1:2007	Conformance testing for the biometric application programming interface (BioAPI) - Part 1: Methods and procedures, 2007-01-29 Mandated DISR DISR 09-2.0 DISR 09-2.0	M
ISO/IEC 24709-2:2007	Conformance testing for the biometric application programming interface (BioAPI) - Part 2: Test assertions for biometric service providers, 2007-02-02	M
Related Principle & Business Rule		
P1/R8 Technical Standards Profile P1/R9 Technical Standards Profile P2/R5 Technical Standards Profile P2/R6 Technical Standards Profile P2/R7 Technical Standards Profile	P2/R8 Technical Standards Profile P5/R6 Technical Standards Profile P8/R1 Technical Standards Profile P8/R4 Technical Standards Profile	P8/R7 Technical Standards Profile P8/R8 Technical Standards Profile P9/R11 Technical Standards Profile P10/R3 Technical Standards Profile
Technical Profile: Biometric Validation		
Standard ID	**Standard Title**	**DISR Status**
ANSI INCITS 385-2004	Face Recognition Format for Data Interchange, May 13, 2004	M
ANSI/INCITS 378-2004	Finger Minutiae Format for Data Interchange	M
ANSI/INCITS 381-2004	Finger Image-Based Data Interchange Format	M
ANSI/INCITS 385-2004	Face Recognition Format for Data Interchange, May 13, 2004	M
ISO/IEC 19794-5:2011	Biometric Data Interchange Formats -- Part 5: Face image data	
Related Principle & Business Rule		
P9/R1 Technical Standards Profile		
Technical Profile: Common Access Card (CAC)		
Standard ID	**Standard Title**	**DISR Status**

ISO/IEC 7816-11:2004	ISO/IEC 7816-11:2004 - Identification cards - Integrated circuit cards - Part 11: Personal verification through biometric methods	M
ISO/IEC 7816-9:2004	ISO/IEC 7816-9:2004 - Identification Cards - Integrated Circuit(s) Cards with Contacts - Part 9: Additional Inter-industry Commands and Security Attributes (formerly ANSI/ISO/IEC 7816-9:2000)	M
ISO/IEC 14443-1:2000	ISO/IEC 14443-1: 2000 - Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 1: Physical characteristics	M
ISO/IEC 14443-2:2001 w/ Amd 1:2005	Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 2: Radio frequency power and signal interface, 28 June 2001 with Amendment 1: Bit rates of fc/64, fc/32 and fc/16, 2 June 2005	M
ISO/IEC 14443-3:2001 w/ Amd1:2005, Amd1/Cor1:2006, Amd3:2006	Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 3: Initialization and Anti-collision, 1 February 2001 with Amendment 1: Bit rates of fc/64, fc/32 and fc/16, 15 June 2005; Amendment 3: Handling of reserved fields	M

Related Principle & Business Rule		
P1/R1) Technical Standards **Profile** P1/R4 Technical Standards Profile P2/R3 Technical Standards Profile	P8/R5 Technical Standards Profile P8/R6 Technical Standards Profile	P11/R2 Technical Standards Profile P11/R3 Technical Standards Profile

Technical Profile: Credential Management		
Standard ID	**Standard Title**	**DISR Status**
NIST SP 800-103	An Ontology of Identity Credentials Part 1: Background and Formulation	N
CIMCPP	The Certificate Issuing and Management Components (CIMC) Family of Protection Profiles (PPs)	
IETF RFC 5272	Certificate Management over CMS	
IETF RFC 3162	RADIUS (Remote Authentication Dial In User Service) and IPv6 August 2001	M
IETF RFC 2865	Remote Authentication Dial In User Services (RADIUS), June 2000	M
	Digital Signature	
IETF RFC 3852	Cryptographic Message Syntax (CMS)	M
ISO/IEC 14888-3:2006	Information Technology -- Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms	N
FIPS Pub 186-4	Digital Signature Standard (DSS)	M

NIST FIPS Pub 180-3	Secure Hash Standard (SHS), October 2008	M
Related Principle & Business Rule		
P5/R1 Technical Standards Profile P1/R6 Technical Standards Profile	P1/R7 Technical Standards Profile	P9/R11 Technical Standards Profile

Technical Profile: Encryption & Decryption		
Standard ID	**Standard Title**	**DISR Status**
HAIPE 3.0.2	High Assurance Internet Protocol Encryptor (HAIPE) Interoperability Specification, Version 3.0.2, December 2006	M
SLOSPP	Protection Profile for Single-level Operating Systems in Environments Requiring Medium Robustness	M
NIST SP 800-78-1	Cryptographic Algorithms and Key Sizes for Personal Identity Verification	N
FIPS Pub 197	Advance Encryption Standard (AES), 26 November 2001	M
XML-Encryption W3C	XML Encryption Syntax and Processing, W3C Recommendation, 10 December 2002	M
Related Principle & Business Rule		
P9/R10 Technical Standards Profile		

Technical Profile: Firewall Protection		
Standard ID	**Standard Title**	**DISR Status**
PP_FW_TF_MR_v1.1 (Traffic Filt. Firewall - Med. Robustness)	U.S. Government Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, Version 1.1, 2007-07-25	M
PP_FWPP-MR	U.S. Government Firewall Protection Profile for Medium Robustness Environments	M
Traffic Filtering Firewall - Low Risk	U.S. Government Traffic Filter Firewall Protection Profile for Low Risk Environments, Version 1.1, April 1999	M
Related Principle & Business Rule		

Technical Profile: Identity Based Access Control (IBAC)		
Standard ID	**Standard Title**	**DISR Status**
IETF RFC 4282	The Network Access Identifier, December 2005	E

ISO/IEC 7816-8:2004	ISO/IEC 7816-8:2004 - Identification Cards - Integrated Circuit(s) Cards with Contacts - Part 8: Security Related Inter-industry Commands (formerly ANSI/ISO/IEC 7816-8:1999)	M
IETF RFC 2845	Secret Key Transaction Authentication for DNS (TSIG), May 2000	M
Related Principle & Business Rule		
P5/R1 Technical Standards Profile P5/R2 Technical Standards Profile P5/R4 Technical Standards Profile	P10/R1 Technical Standards Profile P10/R2 Technical Standards Profile	P11/R2 Technical Standards Profile
Technical Profile: Identity Management		
Standard ID	**Standard Title**	**DISR Status**
IETF RFC 3972	Cryptographically Generated Addresses (CGA), March 2005	E
PIV-I	Personal Identity Verification Interoperability For Non-Federal Issuers	
IETF RFC 5408	Identity-Based Encryption Architecture and Supporting Data Structures	
FIPS Pub 201-1	Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006	M
IETF RFC 2794	Mobile IP Network Access Identification Extension for IPv4, March 2000	
Related Principle & Business Rule		
P1/R3 Technical Standards Profile P2/R2 Policy/Regulation Profile P3/R1 Technical Standards Profile	P3/R2 Technical Standards Profile P5/R1 Technical Standards Profile	P9/R5 Technical Standards Profile P11/R3 Technical Standards Profile
Technical Profile: Identity Proofing		
Standard ID	**Standard Title**	**DISR Status**
NIST Special Publication 800-76-2	Biometric Data Specification for Personal Identity Verification, July 2013	M
NIST SP 800-73-3	Interfaces for Personal Identity Verification – Part 1: End-Point PIV Card Application Namespace, Data Model and Representation	N
NIST SP 800-87 Rev 1	Codes for Identification of Federal and Federally-Assisted Organizations	N
Related Principle & Business Rule		
P1/R2 Technical Standards	P1/R5 Technical	

Profile	Standards Profile	

Technical Profile: Cybersecurity		
Standard ID	**Standard Title**	**DISR Status**
NIST SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories	N
FIPS-199	Standards for Security Categorization of Federal Information and Information Systems	N
NIST SP 800-126 Rev. 2	The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2, September 2011	M
DoD CJCSI 6510	Cybersecurity (IA) and Computer Network Defense	
Related Principle & Business Rule		
P9/R7 Technical Standards Profile		

Technical Profile: IPSec Advanced Encryption		
Standard ID	**Standard Title**	**DISR Status**
IETF RFC 3686	Using Advanced Encryption Standard (AES) Counter Mode with IPsec Encapsulation Security Payload (ESP)	M
Related Principle & Business Rule		

Technical Profile: IPSec Cryptographic Management Services		
Standard ID	**Standard Title**	**DISR Status**
IETF RFC 4308	Cryptographic Suites for IPsec, December 2005	M
IETF RFC 4869	Suite B Cryptographic Suites for IPsec, May 2007	M
Related Principle & Business Rule		

Technical Profile: IPSec Mechanisms		
Standard ID	**Standard Title**	**DISR Status**
IETF RFC 3776	Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents, June 2004	E
IETF RFC 4301	Security Architecture for the Internet Protocol, December 2005	M
Related Principle & Business Rule		

Technical Profile: Key Management		
Standard ID	**Standard Title**	**DISR Status**
RSA Labs PKCS #15:2000	Cryptographic Token Information Format Standard, Version 1.1, RSA, 6 June 2000	M
RSA PKCS #11 v2.20	RSA PKCS #11 v2.20: Cryptographic Token Interface Standard	M
IETF RFC 3585	IPsec Configuration Policy Information Model, Aug 2003	M
IETF RFC 3566	The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec, Sept 2003	M
CIMCPP	The Certificate Issuing and Management Components (CIMC) Family of Protection Profiles (PPs)	M
Related Principle & Business Rule		

Technical Profile: Global Directory Services for Enterprise Services		
Standard ID	**Standard Title**	**DISR Status**
ACP 123(B)	Common Messaging Strategy and Procedures, May 2009	M
IETF RFC 3850	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling, July 2004	M
IETF RFC 4104	Policy Core Extension Lightweight Directory Access Protocol Schema (PCELS), June 2005	M
IETF RFC 3673	Lightweight Directory Access Protocol version 3 (LDAPv3): All Operational Attributes, December 2003	M
IETF RFC 2849	The LDAP Data Interchange Format (LDIF), June 2000	M
IETF RFC 2605	Directory Server Monitoring MIB, June 1999	M
Related Principle & Business Rule		
P4/R2 Technical Standards Profile P4/R3 Technical Standards Profile	P4/R4 Technical Standards Profile P4/R5 Technical Standards Profile	P12/R2 Technical Standards Profile

Technical Profile: Policy in Authentication		
Standard ID	**Standard Title**	**DISR Status**
NSPD-59 / HSPD-24	Biometrics for Identification and Screening to Enhance National Security	
DoDD 8320.02	Data Sharing in a Net-Centric Department of Defense	
DoD Instruction 8520.03	Identity Authentication for Information Systems	

DoDD 8320.03	Unique Identification (UID) Standards for a Net-Centric Department of Defense	
DoDD 1000.25	DoD Personnel Identity Protection (PIP) Program	
DODD 8500.01E	Cybersecurity (IA)	
DoD 5200.28-STD	Department of Defense Trusted Computer System Evaluation Criteria	

Related Principle & Business Rule		
P1/R2 Policy/Regulation Profile P1/R3 Policy/Regulation Profile P1/R9 Policy/Regulation Profile	Technical Profile: Policy in Credentialing P7/R8 Policy/Regulation Profile P9/R3 Policy/Regulation Profile	P11/R1 Policy/Regulation Profile P12/R1 Policy/Regulation Profile

Technical Profile: Policy in Credentialing

Standard ID	Standard Title	DISR Status
SP 800-103	An Ontology of Identity Credentials, Part 1: Background and Formulation	
SP 800-122	Guide for Protecting the Confidentiality of Personally Identifiable Information (PII)	
DODI 8510.01	DoD Information Assurance Certification and Accreditation Process (DIACAP)	
DODI 8510.01	DoD Information Assurance Certification and Accreditation Process (DIACAP)	
DoD Instruction 8520.02	Public Key Infrastructure (PKI) and Public Key (PK) Enabling	

Related Principle & Business Rule		
P2/R2 Policy/Regulation Profile P9/R1 Policy/Regulation Profile P1/R8 Policy/Regulation Profile Technical Profile: Policy in Credentialing P7/R8 Policy/Regulation Profile	P9/R2 Technical Standards Profile P9/R3 Policy/Regulation Profile P9/R7 Policy/Regulation Profile	P9/R8 Policy/Regulation Profile P9/R9 Policy/Regulation Profile P9/R10 Policy/Regulation Profile

Technical Profile: Secure Shell

Standard ID	Standard Title	DISR Status
IETF RFC 4254	The Secure Shell (SSH) Connection Protocol, January 2006	M
IETF RFC 4252	The Secure Shell (SSH) Authentication Protocol, January 2006	M
IETF RFC 4251	The Secure Shell (SSH) Protocol Architecture, January 2006	M

IETF RFC 4250	The Secure Shell (SSH) Protocol Assigned Numbers, January 2006	M
Related Principle & Business Rule		
P5/R1 Technical Standards Profile	P5/R3 Technical Standards Profile	P5/R5 Technical Standards Profile

Technical Profile: Web Services Security		
Standard ID	**Standard Title**	**DISR Status**
W3C WS Addressing 1.0 - Core	Web Services Addressing 1.0 - Core, W3C Recommendation, 9 May 2006	M
IETF RFC 4347	Datagram Transport Layer Security, April 2006	M
WS-Security 1.1	Web Services Security v1.1, February 2006	
Related Principle & Business Rule		
P9/R4 Technical Standards Profile		

Technical Profile: Standardized Policy Languages		
Standard ID	**Standard Title**	**DISR Status**
EKMS 308E	Revision E, Data Tagging and Delivery Standard, April 2008	
EKMS 308 Appendix A	EKMS Data Tagging and Delivery Standard, Appendix A, Shared Fixed ID and Command.req FDU Assignments, 22 April 2009	
EKMS 308 App C 24Apr09	EKMS Data Tagging and Delivery Standard, U.S. National Appendix C, Non-shared Fixed ID and Command.req FDU Assignments, 24 April 2009	
XACML 2.0 OASIS	eXtensible Access Control Markup Language (XACML) Version 2.0, OASIS Standard, 1 February 2005	
Related Principle & Business Rule		
P7/R6 Technical Standards Profile	P7/R7 Technical Standards Profile	P7/R2 Technical Standards Profile

Army IdAM RA to Army Regulation (AR) 25-2 Mapping	
AR 25-2 Chapter/Section	**Army IdAM RA Principle/Rule**
Chapter 2: Responsibilities	
Section 2-x	P3/R1 Policy/Regulation Profile
Chapter 3: Army Information Assurance Program Personnel Structure	
Section 3-2: Information assurance personnel structure	P3/R1 Policy/Regulation Profile
Chapter 4: Information Assurance Policy	
Section 4-3: Information assurance training	P7/R3 Policy/Regulation Profile
Section 4-5: Minimum information assurance requirements	(P1/R1) Policy/Regulation **Profile** P1/R4 Policy/Regulation Profile P9/R7 Policy/Regulation Profile P11/R3 Policy/Regulation Profile P12/R1 Policy/Regulation Profile P12/R1 Policy/Regulation Profile
Section 4-12: Password control	P1/R6 Policy/Regulation Profile P1/R7 Policy/Regulation Profile P1/R9 Policy/Regulation Profile
Section 4-14: Personnel security standards	P1/R5 Policy/Regulation Profile
Section 4-19: Cross-domain security interoperability	P5/R3 Policy/Regulation Profile P5/R5 Policy/Regulation Profile P9/R5 Policy/Regulation Profile P9/R9 Policy/Regulation Profile P9/R10 Policy/Regulation Profile
Section 4-20: Network security	P10/R3 Policy/Regulation Profile