



# U.S. Army – Identity, Credential, and Access Management (ICAM) - Reference Architecture (RA) v1.0

Version 1.0, 19 October, 2012

## Executive Summary

The Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Implementation Roadmap (ESR) Initial Implementation Plan v1.0, 06 September, 2011 has outlined the following problem statement as a basis for its Application and Data Services (ADS2): Identity and Access Management (IdAM) Services efficiency initiative:

*“To enhance the security posture of the infrastructure, anonymity must be eliminated. Further, the Department is encumbered by subjective need-to-know access control decision processes that are independently administered. This restricts the flexibility and agility of the Warfighter (Soldier) and imposes a significant amount of unnecessary overhead.”*

Historically, the DoD, and the DoD Service Components (SCs) (e.g., Army, Air Force, Navy, Marines, Intelligence Community (IC)) have been developing and deploying Identity, Credential, and Access Management (ICAM) services, of which IdAM services are a subset, in a stove-piped manner where access control to information or facilities was provided and maintained largely by the “Resource” owner. Even with the use of the DoD Common Access Card (CAC) or secure token for user “Authentication” using Public Key Infrastructure (PKI) technology, there are still capability gaps between how authenticated information “Requesters” or “Consumers” are identified, and what Resources (i.e., data, facilities, networks, equipment) they should be allowed “Authorization” to. The challenge is to find a way for all DoD and SC ICAM service capabilities and infrastructures to accommodate rapidly changing identity attributes, roles, and access accounts as operational phases and environments change rapidly (i.e., Generating Force, deployed tactical, non-tactical).

This document is a “Business Rules-Based” Army ICAM Reference Architecture (RA) that establishes a core set of functional and technical boundaries for Army ICAM services, including those directly supporting specialized operations. It will be made available to, and can serve as a model for DoD Enterprise and other SC ICAM services and infrastructures. It outlines a set of “Guiding Principles” and “Business Rules” as a framework to specify a set of generic functional components. These will applied to more precisely specify and diagram any ICAM infrastructures, solution level architectures, designs, service offerings, and their required materiel solutions. It specifies the essential technical and regulatory standards that must be followed, and identifies models that if applied across all of the possible operating environments, will increase overall infrastructure interoperability as well as streamline acquisition processes, resulting in reduced cost and more rapid deployment of services.

This ICAM RA provides the Army and its supporting organizations with guidance in the design, development, deployment, transition to, and operational management of an ICAM services framework and infrastructures. It also provides a basis that allows other DoD organizations to follow common service models that define components or service(s) “containers” that can be applied to any implementation, to meet the requirements of any operating environment. Therefore, it can serve as a foundation in the ongoing development of a DoD Enterprise ICAM RA.

Digitally signed by BLOHM.GARY.W.1228949589  
**BLOHM.GARY.W.1228949589**

2 Nov 2012

Mr. Gary W. Blohm

Director – CIO/G6, Army Architecture Integration Center (AAIC)

Date

# Table of Contents

<b>EXECUTIVE SUMMARY .....</b>	<b>I</b>
<b>1 STRATEGIC PURPOSE .....</b>	<b>1</b>
1.1 Introduction .....	1
1.2 End State Vision.....	1
1.3 Background .....	5
1.4 Benefits .....	5
1.5 Intended Audience and Use.....	6
1.6 Alignment with DoD Enterprise Architecture and Key ICAM Strategies .....	7
1.7 Scope/Organization .....	7
<b>2 VOCABULARY .....</b>	<b>10</b>
<b>2.1 Access Types.....</b>	<b>10</b>
2.1.1 Logical Access Control .....	10
2.1.2 Physical Access Control .....	10
2.1.3 Entities .....	10
2.1.3.1 Person Entity (PE).....	10
2.1.3.2 Non-Person Entity (NPE) .....	11
2.1.3.3 Requester.....	11
2.1.3.4 Resource .....	11
<b>2.2 Reference Architecture Evolution .....</b>	<b>11</b>
2.2.1 RA Incremental Development and Versioning .....	11
2.2.2 Limitations.....	12
2.2.3 Key IdAM Architectural Definitions .....	13
2.2.3.1 Rationale .....	13
2.2.3.2 Service Offerings Baseline.....	14
2.2.3.3 Component Categorization .....	14
2.2.3.4 IdAM Component Definitions .....	17
2.2.3.5 Directory Service (DS).....	19
2.2.3.6 Offline Address Book (OAB) .....	20
2.2.3.7 Account Provisioning Service (APS).....	20
2.2.3.8 Single Sign-On Service (SSOS) .....	20
2.2.3.9 Reduced Sign-On Service (RSOS).....	21
2.2.3.10 Rules Engine (RE).....	22
<b>3 GUIDING PRINCIPLES AND BUSINESS RULES .....</b>	<b>24</b>
<b>3.1 Service Area/Services to Guiding Principles and Business Rules Mapping .....</b>	<b>24</b>

<b>3.2</b>	<b>Specifications.....</b>	<b>26</b>
3.2.1	(P1) Principle 1 – Unique Identity and Credentials.....	26
3.2.1.1	(P1/R1) Business Rule 1 – Person Entity (PE) Unique Identifier.....	26
3.2.1.2	(P1/R2) Business Rule 2 – Allowed Identities.....	27
3.2.1.3	(P1/R3) Business Rule 3 – Identity Suitability .....	29
3.2.1.4	(P1/R4) Business Rule 4 – Identity Data Integrity .....	30
3.2.1.5	(P1/R5) Business Rule 5 – Identity Data Discoverability .....	31
3.2.1.6	(P1/R6) Business Rule 6 – Identity Data Conformance .....	32
3.2.1.7	(P1/R7) Business Rule 7 – Authentication and Authorization Service Provisioning.....	33
3.2.1.8	(P1/R8) Business Rule 8 – Enterprise Identity Repository .....	34
3.2.2	(P2) Principle 2 – Identity Authoritative Data Source.....	35
3.2.2.1	(P2/R1) Business Rule 1 – Defense Manpower Data Center (DMDC) Person Entity (PE) Identity Attribute Data Brokering.....	35
3.2.2.2	(P2/R2) Business Rule 2 – Common Access Card (CAC) Usage .....	36
3.2.2.3	(P2/R3) Business Rule 3 – Resource Account Provisioning Service (APS) .....	38
3.2.2.4	(P2/R4) Business Rule 4 – Adding Core PE Identity Attributes .....	39
3.2.2.5	(P2/R5) Business Rule 5 – Adding Core NPE Identity Attributes .....	40
3.2.3	(P3) Principle 3 – Person Entity (PE) and Non-Person Entity (NPE) Identification.....	42
3.2.3.1	(P3/R1) Business Rule 1 – Mobile/Edge Platforms/Devices.....	42
3.2.3.2	(P3/R2) Business Rule 2 – Mobile Device Binding.....	43
3.2.4	(P4) Principle 4 – Global Directory Electronic Mail (E-Mail) Services .....	45
3.2.4.1	(P4/R1) Business Rule 1 – Global Address List (GAL) Distribution .....	45
3.2.4.2	(P4/R2) Business Rule 2 – Global Address List (GAL) Organizational Views.....	46
3.2.4.3	(P4/R3) Business Rule 2 – Global Address List (GAL) Data Schema .....	47
3.2.4.4	(P4/R4) Business Rule 4 – Offline Address Book Availability .....	48
3.2.4.5	(P4/R5) Business Rule 5 – Directory/Global Address List (GAL) Services Availability .....	49
3.2.5	(P5) Principal 5 – Authentication and Authorization.....	51
3.2.5.1	(P5/R1) Business Rule 1 – Authentication and Authorization Scope .....	51
3.2.5.2	(P5/R2) Business Rule 2 – Identity Service For Tactical Edge.....	52
3.2.5.3	(P5/R3) Business Rule 3 – Single DoD Authentication Service Model.....	53
3.2.5.4	(P5/R4) Business Rule 4 – Standard Attribute Model .....	54
3.2.5.5	(P5/R5) Business Rule 5 – Global Information Resource Access.....	55
3.2.5.6	(P5/R6) Business Rule 6 – Access Policy Management Model.....	56
3.2.5.7	(P5/R7) Business Rule 7 – Access Policy Security.....	57
3.2.5.8	(P5/R8) Business Rule 8 – Attribute Access .....	57
3.2.5.9	(P5/R9) Business Rule 9 – DoD and Service Component (SC) Single Sign-On Service (SSOS) and Reduced Sign-On Service (RSOS) Restriction .....	58
3.2.5.10	(P5/R10) Business Rule 10 – Attribute Based Access Control (ABAC) Authorization Service .....	58
3.2.6	(P6) Principle 6 – Dynamic Access Control .....	59
3.2.6.1	(P6/R1) Business Rule 1 – Policy Management.....	59
3.2.6.2	(P6/R2) Business Rule 2 – Policy Change Management.....	60
3.2.6.3	(P6/R3) Business Rule 3 – Policy Attribute Validation .....	60
3.2.7	(P7) Principle 7 – Access to Data, Services and Applications.....	62
3.2.7.1	(P7/R1) Business Rule 1 – Information Resource Types .....	62
3.2.7.2	(P7/R2) Business Rule 2 – Public Key Infrastructure (PKI) Based Authentication .....	63
3.2.7.3	(P7/R3) Business Rule 3 – Data Tagging.....	64
3.2.7.4	(P7/R4) Business Rule 4 – Policy Store (PS) Personally Identifiable Information (PII) Attribute Exposure .....	65
3.2.7.5	(P7/R5) Business Rule 5 – Policy Decision Point (PDP) Personally Identifiable Information (PII) Attribute Data Exposure.....	66
3.2.7.6	(P7/R6) Business Rule 6 – Data Tagging Development .....	67
3.2.7.7	(P7/R7) Business Rule 7 – Standardized Policy Language .....	68
3.2.8	(P8) Principle 8 – Physical Access .....	69

3.2.8.1	(P8/R1) Business Rule 1 – Non-Person Entity (NPE) Unique Identifier .....	69
3.2.8.2	(P8/R2) Business Rule 2 – Access Control Policy .....	69
3.2.8.3	(P8/R3) Business Rule 3 – Non-Person Entity (NPE) Attribute Verification .....	70
3.2.8.4	(P8/R4) Business Rule 4 – Non-Person Entity (NPE) Attribute and Policy Management .....	70
3.2.8.5	(P8/R5) Business Rule 5 – Common Access Card (CAC) Credential Mechanism .....	70
3.2.8.6	(P8/R6) Business Rule 6 – Common Access Card (CAC) Enrollment .....	71
3.2.9	(P9) Principle 9 – General Identity and Access Management (IdAM) Security Policy .....	72
3.2.9.1	(P9/R1) Business Rule 1 – Identity Attribute Data Validation .....	72
3.2.9.2	(P9/R2) Business Rule 2 – DoD Authorization Service .....	72
3.2.9.3	(P9/R3) Business Rule 3 – Information Resources Authorization .....	73
3.2.9.4	(P9/R4) Business Rule 4 – Enterprise Information Sharing .....	74
3.2.9.5	(P9/R5) Business Rule 5 – Information Resource Authentication Frequency .....	74
3.2.9.6	(P9/R6) Business Rule 6 – Cross Domain Security.....	75
3.2.9.7	(P9/R7) Business Rule 7 – Information Resources Availability.....	75
3.2.9.8	(P9/R8) Business Rule 8 – Information/Data Resources Protection .....	76
3.2.9.9	(P9/R9) Business Rule 9 – DoD Enterprise Trust Management .....	77
3.2.9.10	(P9/R10) Business Rule 10 – Enterprise DoD Network Domain.....	77
3.2.9.11	(P9/R11) Business Rule 11 – Alternate Authentication Mechanisms (Non-CAC/Token) .....	77
3.2.9.12	(P9/R12) Business Rule 12 – Data Encryption.....	78
3.2.9.13	(P9/R13) Business Rule 13 – SHA-256: Secure Hashing Algorithm Migration.....	78
3.2.10	(P10) Principle 10 – Single Sign-On (SSO) and Reduced Sign-On (RSO) .....	80
3.2.10.1	(P10/R1) Business Rule 1 – Service Component (SC) Directory Data Population .....	80
3.2.10.2	(P10/R2) Business Rule 2 – Electronic Data Interchange Personal Identifier (EDI-PI) Rendering .....	81
3.2.10.3	(P10/R3) Business Rule 3 – Directory Information Updates .....	81
3.2.11	(P11) Principle 11 – Network Access Controls .....	82
3.2.11.1	(P11/R1) Business Rule 1 – Authorization Policy Network Attributes .....	82
3.2.11.2	(P11/R2) Business Rule 2 – Network-Connected Authentication .....	83
3.2.11.3	(P11/R3) Business Rule 3 – ‘Disconnected’ and/or ‘Network-Disadvantaged’ Authentication .....	84
3.2.11.4	(P11/R4) Business Rule 4 – Network Gateways .....	85
3.2.12	(P12) Principle 12 – Monitoring and Reporting .....	86
3.2.12.1	(P12/R1) Business Rule 1 – Auditing Services .....	86
3.2.12.2	(P12/R2) Business Rule 2 – Identity and Access Management (IdAM) Infrastructure- Monitoring/Reporting.....	86
<b>APPENDIX A - VOCABULARY (INTEGRATED DICTIONARY – AV-2) .....</b>		<b>1</b>
<b>Identity and Attribute Management Vocabulary .....</b>		<b>1</b>
<b>Acronym List.....</b>		<b>5</b>
<b>APPENDIX B - TECHNICAL POSITIONS AND PATTERNS – CORE STANDARDS FOR BUSINESS RULES (BY BUSINESS RULE) .....</b>		<b>1</b>
<b>APPENDIX C – ICAM/IDAM SERVICE AREAS AND SERVICES DEFINITIONS.....</b>		<b>1</b>
Identity Management .....		1
Authentication .....		1
Cryptography.....		2
Authorization .....		2
Privilege Management .....		2
Auditing and Reporting .....		3
Federation .....		3

Web Services (WS)-Federation .....6

**APPENDIX D - ATTRIBUTE BASED ACCESS CONTROL (ABAC) ..... 1**

**Policy-Based Authorization Services ..... 1**

    DPBAC Workflow .....1

    Resource Management.....2

    In-Band and Out-of-Band Access Control .....2

    DoD Implementation Schedule.....3

**APPENDIX E - IDAM SECURITY MANAGEMENT ..... 1**

**National Security Agency (NSA) Enterprise Security Management (ESM) ..... 1**

**APPENDIX F – TECHNICAL PATTERNS OVERVIEW ..... 1**

**Active Directory (AD) Tactical Network Capability Maturity Model ..... 1**

**Tactical Network Operations ..... 3**

**Unclassified Network Administration ..... 4**

**Classified Network Administration ..... 4**

**Theater Network Administration ..... 5**

**Construction and Network Infrastructure and Equipment ..... 5**

**Deployment Planning Phases..... 5**

    Pre-Deployment Phase .....5

    Movement Phase.....6

        Reception, Staging, Onward Movement, and Integration (RSOI) Phase.....6

        Redeployment Phase .....6

**Force Projection Processes and Phases ..... 6**

    Pre-Deployment.....6

        Mobilization .....7

        Deployment.....7

        Employment.....8

        Sustainment .....8

        Redeployment.....8

**Tactical Network Capability Maturity Levels ..... 9**

## TABLES AND FIGURES

Figure 1.1 – Framework of Candidate DoD-Provided Directory Services – 2015 “Vision” .....	3
Figure 1.2 – Army ICAM Architecture Operational View.....	4
Table 2.1 – RA Versioning Matrix .....	12
Table 3.1 – IdAM Service Areas to Guiding Principles Mapping.....	24
Table 3.2 – DoD ICAM Services Framework .....	25
Table 3.3 – DoD ICAM Service Areas to IdAM Service Areas Mapping .....	25
Table 3.4 – Unique Identity and Credentials Principle.....	26
Table 3.5 – Person Entity (PE) Unique Identifier Business Rule .....	26
Table 3.6 – Allowed Identities Business Rule .....	27
Table 3.7 – Identity Suitability Business Rule.....	29
Table 3.8 – Identity Data Integrity Business Rule.....	30
Table 3.9 – Identity Data Discoverability Business Rule .....	31
Table 3.10 – Identity Data Conformance Business Rule.....	32
Table 3.11 – Authentication and Authorization Service Provisioning Business Rule .....	33
Table 3.12 – Enterprise Identity Repository Business Rule .....	34
Table 3.13 – Identity Authoritative Data Source Principle.....	35
Table 3.14 – Defense Manpower Data Center (DMDC) Person Entity (PE) Identity Attribute Data Brokering Business Rule .....	35
Table 3.15 – Common Access Card (CAC) Usage Business Rule.....	36
Table 3.16 – Resource Account Provisioning Service (APS) Business Rule.....	38
Table 3.17 – Adding Core PE Identity Attributes Business Rule.....	39
Table 3.18 – Adding Core NPE Identity Attributes Business Rule.....	40
Table 3.19 – Person Entity (PE) and Non-Person Entity (NPE) Identification Principle.....	42
Table 3.20 – Mobile/Edge Platforms/Devices Business Rule .....	42
Table 3.21 – Mobile Device Binding Business Rule.....	43
Table 3.22 – Global Directory E-Mail Service Principle .....	45
Table 3.23 – Global Access List (GAL) Distribution Business Rule .....	45
Table 3.24 – Global Access List (GAL) Organizational Views Business Rule .....	46
Table 3.25 – Global Address List (GAL) Data Schema Business Rule .....	47
Table 3.26 – Offline Address Book Availability Business Rule .....	48
Table 3.27 – Directory/Global Address List (GAL) Services Availability Business Rule .....	49
Table 3.28 – Authentication and Authorization Principle .....	51
Table 3.29 – Authentication and Authorization Scope Business Rule .....	51
Table 3.30 – Identity Service for the Tactical Edge Business Rule.....	52
Table 3.31 – Single DoD Authentication Service Model Business Rule .....	53
Table 3.32 – Standard Attribute Model Business Rule.....	54
Table 3.33 – Global Information Resource Access Business Rule .....	55
Table 3.34 – Access Policy Management Model Business Rule.....	56
Table 3.35 – Access Policy Security Business Rule.....	57
Table 3.36 – Attribute Access Business Rule.....	57
Table 3.37 – DoD and Service Component (SC) Single Sign-On (SSOS) and Reduced Sign-On (RSOS) Restriction Business Rule.....	58
Table 3.38 – Attribute Based Access Control (ABAC) Authorization Service Business Rule...	58
Table 3.39 – Dynamic Access Control Principle.....	59
Table 3.40 – Policy Management Business Rule.....	59

Table 3.41 – Policy Change Management Business Rule .....	60
Table 3.42 – Policy Attribute Validation Rule .....	60
Table 3.43 – Access to Data, Services and Applications Principle .....	62
Table 3.44 – Information Resource Types Business Rule.....	62
Table 3.45 – Public Key Infrastructure (PKI) Based Authentication Business Rule .....	63
Table 3.46 – Data Tagging Business Rule.....	64
Table 3.47 – Policy Store (PS) Personally Identifiable Information (PII) Attribute Exposure Business Rule.....	65
Table 3.48 – Policy Decision Point (PDP) Personally Identifiable Information (PII) Attribute Data Exposure Business Rule .....	66
Table 3.49 – Data Tagging Development Business Rule .....	67
Table 3.50 – Standardized Policy Language Business Rule.....	68
Table 3.51 – Physical Access Principle .....	69
Table 3.52 – Non-Person Entity (NPE) Unique Identifier Business Rule.....	69
Table 3.53 – Access Control Policy Business Rule.....	69
Table 3.54 – Non-Person Entity (NPE) Attribute Verification Business Rule.....	70
Table 3.55 – Non-Person Entity (NPE) Attribute and Policy Management Business Rule .....	70
Table 3.56 – Common Access Card (CAC) Credential Mechanism Business Rule .....	70
Table 3.57 – Common Access Card (CAC) Enrollment Business Rule.....	71
Table 3.58 – General Identity and Access Management (IdAM) Security Policy Principle .....	72
Table 3.59 – Identity Attribute Data Validation Business Rule .....	72
Table 3.60 – DoD Authorization Service Business Rule.....	72
Table 3.61 – Information Resources Authorization Business Rule.....	73
Table 3.62 – Enterprise Information Sharing Business Rule.....	74
Table 3.63 – Information Resource Authentication Frequency Business Rule .....	74
Table 3.64 – Cross Domain Security Business Rule .....	75
Table 3.65 – Information Resources Availability Business Rule .....	75
Table 3.66 – Information/Data Resources Protection Business Rule.....	76
Table 3.67 – DoD Enterprise Trust Management Business Rule .....	77
Table 3.68 – Enterprise DoD Network Domain Business Rule.....	77
Table 3.69 – Alternate Authentication Mechanisms (Non-CAC/Token) Business Rule .....	77
Table 3.70 – Data Encryption Business Rule .....	78
Table 3.71 – SHA-256 Encryption Migration Business Rule.....	78
Table 3.72 – Single Sign-On (SSO) and Reduced Sign-On (RSO) Principle .....	80
Table 3.73 – Enterprise Directory Service Data Population Business Rule.....	80
Table 3.74 – Electronic Data Interchange Personal Identifier (EDI-PI) Rendering Business Rule .....	81
Table 3.75 – Directory Information Updates Business Rule .....	81
Table 3.76 – Network Access Controls Principle.....	82
Table 3.77 – Authorization Policy Network Attributes Business Rule .....	82
Table 3.78 – Network-Connected Authentication Business Rule .....	83
Table 3.79 – ‘Disconnected’ and/or ‘Network-Disadvantaged’ Authentication Business Rule ..	84
Table 3.80 – Network Gateways Business Rule.....	85
Table 3.81 – Monitoring and Reporting Principle .....	86
Table 3.82 – Auditing Services Business Rule.....	86

Table 3.83 – Identity and Access Management (IdAM) Infrastructure Monitoring/Reporting Business Rule.....	86
Figure C1 – General Data Flow Between Federation Components.....	6
Figure D1 – Dynamic Policy-Based Access Control.....	1
Figure D3 – DoD Information Technology Enterprise Strategy and Implementation Roadmap (ITESR) Initial Implementation Plan v1.0 - ICAM Implementation Schedule .....	3
Figure E1 – NSA Enterprise Security Management Framework.....	1
Table F1 – Deployment Planning Phases .....	1
Table F2 – Force Protection Process Phases.....	2
Table F3 – Tactical Network Maturity Levels.....	2
Figure F4 – Tactical Network Maturity Model Summary .....	3
Figure F5 – Active Directory Structure Decision Tree.....	4
Table F6 – Network Capability Maturity Model Description .....	10
Table F7 – Network Capability Maturity Model Description .....	11

# 1 Strategic Purpose

## 1.1 Introduction

To ensure the security of our facilities, and the people and information that use them, 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) real property and other selective SC materiel (e.g., weapons systems, aircraft, ordinance). The use of automation and the ability to network computers, devices, and the capabilities they provide has transformed how we fight. As the Army's warfighting capability and ability to conduct the fight better, faster, and in many ways safer, even as new cyber security risks arise and increase in number.

Historically, the DoD, the Army, and the other SCs have developed and deployed Identity, Credential and Access Management (ICAM) services in a "stove-piped" 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 using Public Key Infrastructure (PKI) technology, there are still gaps between how authenticated information "Requesters" or "Consumers" are identified, and what they should or should not have access to (Resource Authorization). The 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, and 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 ICAM are often unavailable, a secure and accurate "disconnected" ICAM capability is required. It must also be "dynamic" to accommodate rapidly changing identity attributes, Personas, Roles and access accounts as the battlefield environments change. Further, as soldiers move from a sustaining base and are deployed in theatre, they need continuous access to information 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 ICAM service framework could be made available as soldiers return to their sustaining bases, or for any non-tactical access requirements.

A DoD Enterprise level, "Rules-Based" ICAM Reference Architecture (RA) that meets the needs of Joint, SC, Coalition and "external" partners will address the operational and security gaps that are currently being perpetuated across the DoD.

## 1.2 End State Vision

In future iterations of this RA, the foundation provided by the Business Rules will allow a complete view of the target "End-to-End" DoD ICAM Architecture to be developed. This will

comprise the key DoD ICAM components, logical workflow, and data flows that must occur to accommodate the current DoD and SC environments, but integrating a more robust Authentication and Authorization framework. This would continue to support both the existing and/or transforming DoD, Army and other SC *Microsoft (MS) Windows Active Directory (AD)* architectures and infrastructures, as well as include components required to provide access management services for information Resources using Attribute-Based Access Control (ABAC).

An *Authentication and Authorization Framework (AAF)*, coupled with a *Directory Service (DS)* and an *Account Provisioning Service (APS)*, is currently provided by the capabilities of Commercial-Off-The-Shelf (COTS) products currently used to support DoD Enterprise and SC network and information Resources infrastructures. *Microsoft Windows Active Directory* is an example of one of these COTS offerings that is capable of providing these services using an X.509 certificate-based PKI. The DoD and Army have also built similar Government Off-The-Shelf (GOTS) based infrastructure components.

Figure 1.1 represents the candidate DoD/Defense Information Systems Agency (DISA)-provided Directory Services ‘Vision’, which is a framework for meeting the currently defined DoD and SC Identity and Directory Service requirements. The components shown in Figure 1.1 include those that exist today, those currently being developed, and those on which the DoD and the SCs must still come to consensus (as to which services will be provided by DISA, and which will be the responsibility of the SCs to fund, develop, deploy, and maintain). The ideal scenario would be one where ICAM services are centrally controlled with support for central credential operations with both central and distributed authentication and authorization operations. With a Federation Infrastructure that makes the ICAM services look and operate like a single ICAM services implementation. Given the reality of where DoD/DISA is with their evolving ICAM service offerings, a more generic set of ICAM component definitions and descriptions are required within this RA, to avoid significant vocabulary ambiguities. These terms will be presented and discussed under key ICAM Component Definitions in Section 2. These can be applied to develop specific Operational and System views, schematics, and workflow/data flow models (shown in the Army ICAM Architecture Operational View in Figure 1.2).

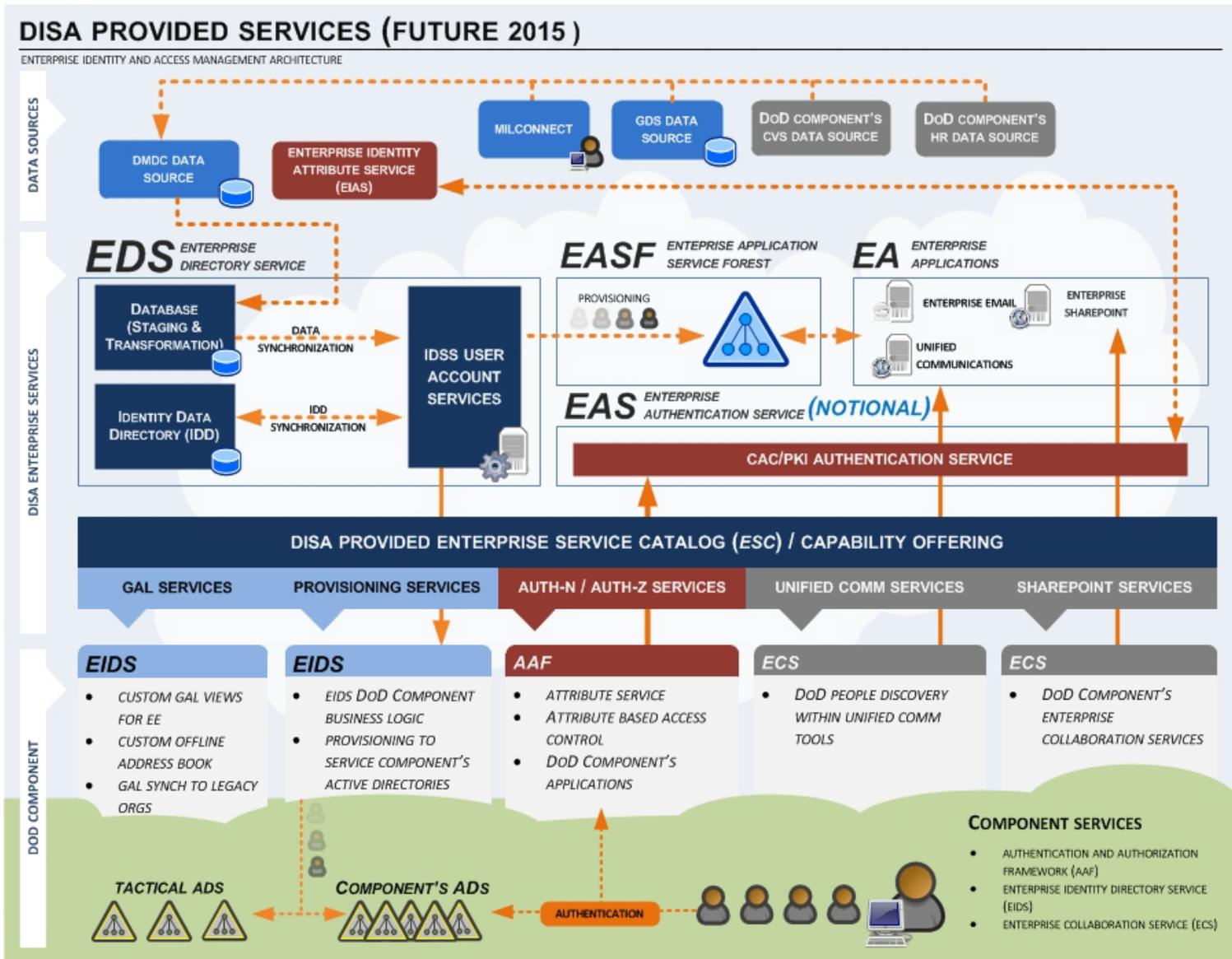


Figure 1.1 – Framework of Candidate DoD-Provided Directory Services – 2015 “Vision”

- Unclassified -

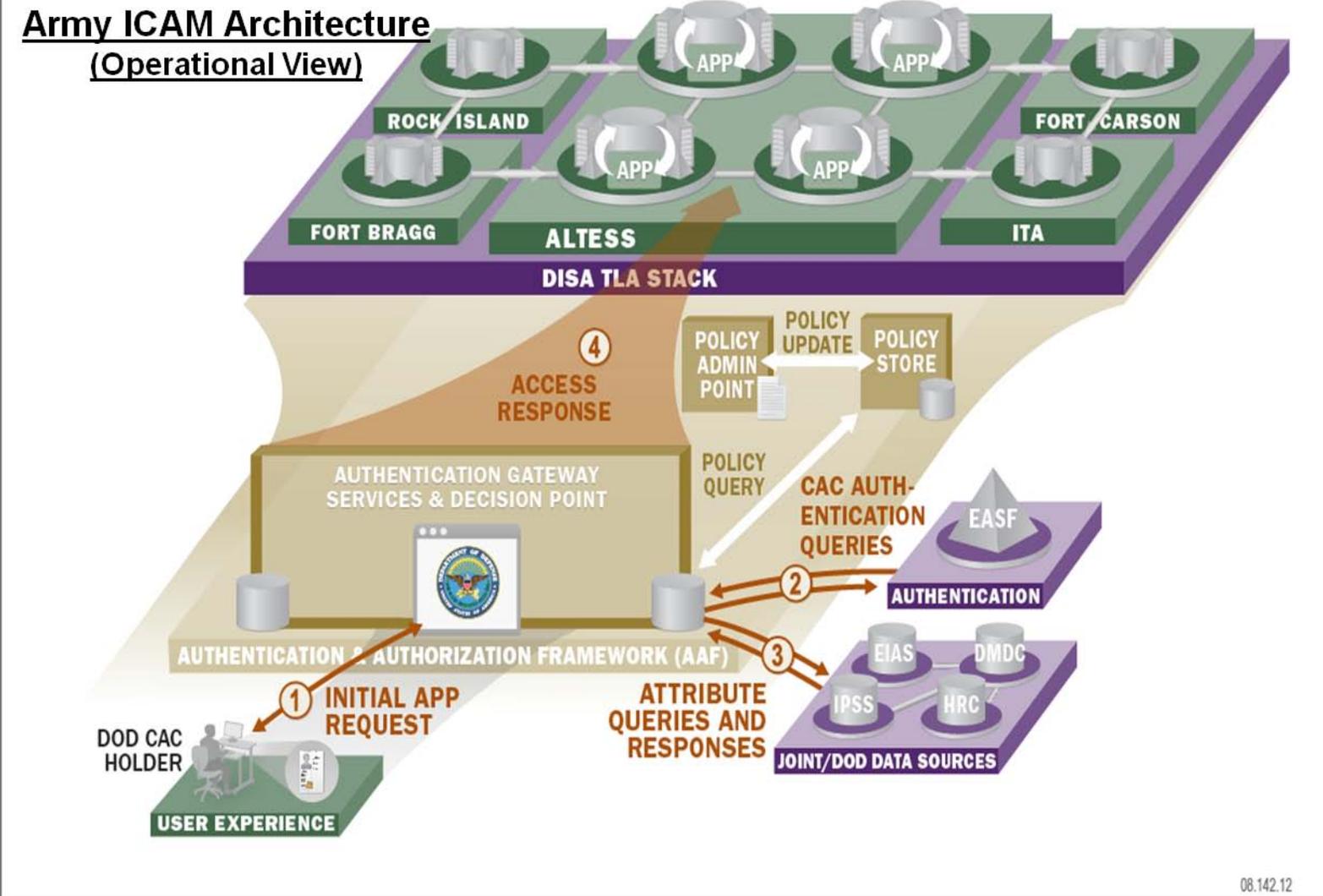


Figure 1.2 – Army ICAM Architecture Operational View

## 1.3 Background

An RA provides an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and the solutions built upon them. As information, services, and infrastructure requirements and solutions continue to evolve, the need for an RA increases.

A “Business Rules-Based” RA establishes a core set of “Guiding Principles” and “Business Rules” as a framework for operational and functional components of the architecture; establishing a set of rules that must be followed to guide all related solution architectures, designs, and implementations.

This document addresses both DoD and the Army’s ICAM requirements, but is written from a generic SC perspective. It assumes that it is a DoD objective to provide as many ICAM services to all SCs as possible through DoD Enterprise services. This approach is being driven by U.S. Government and DoD security, funding, manpower, and other resource availability improvement initiatives going forward.

Because there are SC-specific operational activities that control or limit resource access within any DoD SC or its agencies, a crossroads has been reached where the DoD must now assess the best way to provide ICAM services to all of its personnel, with consideration of many worst case scenarios. The ideal end-state would enable any Soldier or authorized entity to access information or facilities at any time, based on who they are and what they need to do, rather than access determined largely by physical location. This end-state requires eliminating logical identity and access barriers that have precluded this capability in the past.

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

## 1.4 Benefits

This ICAM RA describes the required digital identities, authentication and authorization services, and generic functional components that enable them for both the DoD Enterprise and SCs. It is a framework for more informed decision making and a guide for ongoing planning, design, and implementation activities. The architecture provides:

- A way to evaluate applicability of new technologies, products, and services
- A blueprint for future ICAM growth
- A framework for ICAM decision making

- A guide for creating a DoD and Army enabling identity infrastructure for unforeseen new applications, services, and web services
- A target for ICAM migration
- More reliably authenticate the identity of any entity trying to gain access to authorized resources
- Establish and manage access policies and authorization controls for all DoD and SC resources
- Accommodate rapid but reliable changes in Requester and Resource identities, roles and personas
- Provide the infrastructure and management components to perform these functions while assuring the privacy and civil liberties of all entities involved

## 1.5 Intended Audience and Use

This RA will provide DoD, Army, the other SC leadership, and their organizations guidance in the design, development, deployment, transition to, and operational support for a DoD Enterprise ICAM service framework and infrastructure. The key beneficiaries (and their ICAM-specific and related enterprise and SC level products/services/functions that will use this RA) include, but are not limited to:

- The DoD Chief Information Officer (CIO):
  - Strategic planning for Joint operational capabilities
  - DoD-level ICAM policies and compliance requirements
  - SC-level ICAM policies and compliance requirements
- The Army Chief Information Officer (CIO/G-6):
  - Army Enterprise Network (AEN) Architecture development guidance
  - ICAM and Information Assurance (IA) technical standards
  - Systems Certification and Accreditation (C&A) policies and processes
- The Army Cyber Command (ARCYBER):
  - Guidance to DoD to support Army ICAM requirements
  - Strategic Cyber defense planning in support of Army and Joint operations
- The Army Training and Doctrine Command (TRADOC):
  - Identify ICAM Operational Initial Capabilities Document (ICD) gaps
- The Army Deputy Chief of Staff Operations (G3/5/7):
  - ICAM integration planning for all areas of Army operations
  - Operational environment ICAM integration execution management
- The Army Network Command (NETCOM):
  - Network authentication and access control planning
  - Network Solution Architectures
- The Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA(ALT)):

- Solution Architecture development guidance
- Systems and applications development management
- System-of-Systems integration planning

The DoD initiatives and architectures that will be immediately supported by this ICAM RA include, but are not limited to:

- The Joint Information Environment (JIE)
- The Army Enterprise Network (AEN)/LandWarNet Architecture
- The Army Network Interoperability Exercise (NIE) Reference Architecture
- The Army Top-Level Security Reference Architecture (TLA)
- The Army Unified Capability (UC) Reference Architecture
- The Army “Thin” Client Reference Architecture
- The Army Network Operations (NetOps) Architecture (ANA)

## 1.6 Alignment with DoD Enterprise Architecture and Key ICAM Strategies

The 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 the higher level strategies and the guidance. The DoD Information Enterprise Architecture (IEA) comprises the information, information resources, assets, and processes required to achieve an information advantage and share information across the Department and with mission partners. It defines the DoD overarching enterprise architecture “watermark”.

This ICAM RA is principally aligned to the *DoD Information Enterprise Architecture (DoD IEA) v2.0*, and guided by three key DoD roadmaps/strategies:

- *The Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance ,Version 2.0, 02 December 2011*
- *The Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (formerly The DoD Identity, Credential, and Access Management (ICAM) Transition Strategy Transition Plan, Consolidated Version (Draft) 1.3, 08 May 2012*
- *The Department of Defense (DoD) Information Technology IT Enterprise Strategy and Implementation Roadmap (ESR) Initial Implementation Plan, Version 1.0, 06 September 2011*

## 1.7 Scope/Organization

This “Business Rules-Based” ICAM RA addresses the capability gap issues discussed above, and establishes a set of operational “Guiding Principles”. Associated with each “Guiding Principle” is a set of aligning or enabling “Business Rules”. These are functionally specific to ICAM and the appropriate “Service Areas” and “Services” outlined in the *DoD Identity*,

*Credentialing and Access Management (ICAM) Transition Plan (v1.3)*, which is aligned with the *Federal Identity, Credentialing and Access Management (FICAM) Transition Plan (v1.3)*.

The references cited in each Guiding Principle and Business Rule table fall into one of the following categories:

1. A Business Rule extracted verbatim from an authoritative approved Federal, DoD or SC source document(s) (e.g., *The DoD Information Enterprise Architecture (IEA) v2.0*)
2. A Business Rule extracted verbatim from a draft Federal, DoD or SC source document(s) (e.g., *The Draft DoD Identity and Access Way Forward: DoD ICAM Transition, v1.3, 08 May 2012*)
3. A Business Rule derived from an authoritative approved DoD or SC source document(s)
4. A Business Rule derived from a draft Federal, DoD or SC source document(s)
5. A Business Rule derived from a DoD or SC initiative(s), either existing or in development (e.g., *The Joint Information Environment (JIE) Plan of Action and Metrics (JIE POA&M, March 2012)*).
6. A Business Rule derived from a combination of one or more of the above reference categories, where its specification required clarification and expansion on the provision(s) of the applicable reference(s)

The major attributes of any Business Rule are:

Assumptions - a statement about the existing and future environment (operational, functional, or technical) in which a Business Rule will be applied.

Constraints - a boundary (e.g., operational, functional, or technical) that guides implementation of ICAM services.

Technical, political, cultural, and governance inhibitors (e.g., existing legal, regulatory, policy direction) that conflict with Guiding Principles and their applicable Business Rules can comprise one type of “Risk”. The other “Risk” form is operational in nature, where an expected outcome does not occur due to one or more factors. Factors could include an Assumption(s) that was not valid in most cases, or a Constraint(s) that was not met in the application of the Business Rule. The application of any Business Rule does not necessarily mean that in all cases it can be fully realized, and under some circumstances it may not be realizable at all. Subsequent versions of this RA will also outline “Risk Mitigation” strategies for each Risk statement provided.

This RA will assure both accurate and timely logical and physical access to the appropriate resources, while considering all aspects of security and Information Assurance (IA).

Similarly, this RA establishes a set of core technical and/or regulatory standards for each Business Rule, so that any implementation derived from it assures proper interfacing and interoperability between all ICAM infrastructure components, also assuring end-to-end interoperability.

The ICAM “Patterns” are generalized architecture representations that show the relationships between elements and artifacts specified by the technical guidance and standards. Patterns can be expressed in terms of impact on operational environments, both inter- and intra-DoD SC. This RA categorizes these in two areas: Business Mission Areas and Tactical Mission Areas. This provides more specific guidance in meeting the differing implementation requirements of those environments.

## 2 Vocabulary

This RA will use several key constructs, including “Access Type” and “Entities”, which are in turn comprised of two and four constructs, respectively. The possible combinations of these constructs form a logical framework for the evolution of the architecture.

### 2.1 Access Types

The ICAM RA addresses access control in the Logical Access Control (LAC) and Physical Access Control (PAC) domains. Within each domain, the ICAM RA describes who or what requires access, as well as to what access is requested, which are largely defined as information, facilities, networks, and/or other objects. Every Principle and Business Rule defined in the ICAM RA will address all relevant aspects of the LAC and PAC domains, and the requirements that these domains must support for a wide range of DoD Enterprise and SC operational environments.

#### 2.1.1 Logical Access Control

LAC describes access to a system, information, and/or data that is either standalone or available on a network. It requires that both the Identity and Access and, Authentication and Authorization services manage who or what is allowed to see and/or modify data on an available system or information repository, and/or to either send or receive this information via a network. LAC ICAM will be a principal focus area for v1.0 of the RA.

#### 2.1.2 Physical Access Control

PAC describes physical access to a location, facility, data center, or network, and/or the systems and physical resources that reside there. It is comprised of a unique set of Identity, Access, Authentication, and Authorization services that are required to control who is allowed physical access. PAC will be base-lined in v1.0 of this RA, while V2.0 and 3.0 will expand on this discussion.

#### 2.1.3 Entities

Each access type can involve, but is not limited to, people, information, networks, equipment, and building/facilities or bases/installations. The following sections define the key constructs used in this RA to describe the different entities and the relationship between logical or physical access instances.

##### 2.1.3.1 Person Entity (PE)

The PE construct applies to any human being who requires either logical or physical access to information/data or to a location, facility, data center, or network and the systems and resources that reside there. PE ICAM will be a principal focus area of the RA.

### 2.1.3.2 Non-Person Entity (NPE)

The NPE construct applies to any equipment, device, or other “non-human” entity that requires either logical or physical access. It typically applies to, but is not limited to, information/data, or to a location, facility, network, or data center, and the systems and physical resources that reside there. NPE ICAM will be a principal focus area of v1.0 and v2.0 of the RA.

### 2.1.3.3 Requester

A Requester can be either a PE or a NPE. It is any entity that requires either logical and/or physical access.

### 2.1.3.4 Resource

A Resource is any NPE for which a Requester requires logical and/or physical access.

## 2.2 Reference Architecture Evolution

### 2.2.1 RA Incremental Development and Versioning

As the FICAM and DoD ICAM Service definitions continue to evolve over the course of their implementation and execution, so must any associated RA at the DoD Enterprise or SC levels. Similarly, the entire U.S. Government and DoD will gain knowledge and lessons-learned as they implement more complex and secure identity management capabilities and infrastructure.

Therefore, this RA will be developed and released incrementally in three (3) versions, each with progressing maturity of accuracy, detail, and completeness for Access Type and ICAM Services.

RA v.1.0 will initially focus only on Identity and Access Management (IdAM) services, as outlined in the *Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) v1.3, 08 May 2012* Service Framework. As shown in table 2.1, the Credential Service Area will not be addressed until v2.0. Therefore, all references to the ICAM-based Service Areas discussed in this v1.0 will be described henceforth as “IdAM”.

The scope of each RA version, with some degree of overlap, is outlined in Table 2.1.

		ICAM/IdAM Service Areas					
		Identity Data Management	Identity Authentication	Credential Management	Access Authorization	Directory Services	Auditing & Reporting
Access Type	Person Entity (PE) – Logical Access Control (LAC)	V1.0	V1.0	V2.0	V1.0	V1.0	v1.0
	Non-Person Entity (NPE) – Logical Access Control (LAC)	V1.0/2.0	V2.0	V2.0/3.0	V2.0	V1.0/2.0	v1.0/2.0
	Personal Entity (PE) – Physical Access Control (PAC)	V1.0/2.0	V1.0/2.0	V2.0	V1.0/2.0	V1.0/2.0	V1.0/2.0
	Non-Person Entity (NPE) – Physical Access Control (PAC)	V2.0/3.0	V3.0	V2.0/3.0	V3.0	V3.0	V3.0

Table 2.1 – RA Versioning Matrix

## 2.2.2 Limitations

In accordance with Table 1.1, any subject matter not included in v1.0 of the RA in tables and/or discussion sub-sections for any of the Guiding Principles or Business Rules presented in Section 3 will be addressed in following increments of the IdAM RA. The initial content in v1.0 of the RA contains the below known “gaps”:

- **Risk** descriptions (selective)
- **Risk Mitigation Strategies** (aligned to specific Risk descriptions)
- **Core Technical Standards** tables (selective)
- **Patterns** (for all Business Rules)/(ref: Appendix F)
- **Conformance Testing** (for all Business Rules)

Version 2.0 will address most of these initial gaps, and revisit many of the Assumptions, Constraints and Risk descriptions presented in v1.0. It will also provide Risk Mitigation strategies to many of the existing Risk Descriptions. The updates made in v2.0 will be further

addressed and expanded in v3.0. All Business Rule descriptions will then be fully completed, vetted, and aligned to support all of the elements defined in Table 2.1. Additionally, beginning in RA v2.0, a ‘Business Rules-to-DoD/Army ICAM/IdAM requirements and implementation activities/timeline milestones traceability’ matrix will be added and maintained at the beginning of Section 3.

## 2.2.3 Key IdAM Architectural Definitions

### 2.2.3.1 Rationale

Two major objectives of this RA are to:

#### 1. **Halt the development and deployment of “stovepipe” IdAM infrastructure for DoD/Joint Enterprise, SC, 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 application or application type. The implementations are sometimes COTS, GOTS, or integrated COTS and GOTS. The Business Rules in this RA are meant to stop this practice by promoting a more standardized, “cookie cutter” approach to IdAM infrastructure.

#### 2. **Optimize the use of the existing and future DoD Enterprise IdAM services and infrastructure**

The DoD and all of the SCs must first attempt to leverage all of the available DoD deployed, operational, and available enterprise IdAM service offerings, their service capabilities, and their supporting network infrastructures in any solution architecture. This applies to both logical and physical access controls.

In some cases, these objectives cannot be followed either as the standard operating procedure, or as a universal acquisition model. This may be due to factors that include, but are not limited to:

- High security risk
  - Network information vulnerability
  - Lack of credentialing accuracy/consistency/control
- Continuity of Operations (COOP) requirements
  - Absolute real-time information availability
  - On-site disaster recovery infrastructure
- Lack of or poor network availability and performance
- External environmental conditions
  - Extreme climates
  - Natural disasters
- Tactical operating conditions
  - Radio Frequency (RF) jamming
  - Electro Magnetic Interference (EMI)/Pulse
  - Cyber attack

These conditions are most likely to impact forces and the Resources they require access to in theatre. The complexity in mitigating them becomes significantly greater below base/post/camp/station down to all SC-specific forward area echelons. This creates an additional

burden on this RA, as well as any DoD RA in accommodating these conditions through an appropriate and useful set of architectural constructs and definitions. RAs must identify specific services, components, and frameworks to support these unique operational environments.

#### 2.2.3.2 Service Offerings Baseline

The DoD continues to define and deploy specific enterprise IdAM service offerings and infrastructure. The names of these and the service(s) provided by them are likely to continue to evolve. At the time that the references used to develop the Business Rules in this RA were published, many DoD Enterprise and SC (e.g., Army) IdAM service offerings were still being scoped and specified.

Industry (i.e., product-specific) and candidate DoD or Army-provided infrastructure to provide enterprise services (primarily in non-tactical environments) include offerings such as:

- Identity Synchronization Service (IdSS)
- Enterprise Directory Service (EDS)
- Enterprise Authentication Service Framework (EASF)
- Authentication Service Gateway Service (AGS)
- Enterprise Authentication and Authorization Framework (EAAF)
- Microsoft Active Directory (AD)
- DoD Visitor MS AD Provisioning Service (*not for applications account provisioning*)

#### 2.2.3.3 Component Categorization

Ideally, any RA should be “service offering-agnostic”, much in the way that the Army’s Common Operating Environment (COE) is to be largely “hardware/device/make-agnostic”. COE provides a technical model of an end-system (e.g., mobile/handheld, client, server, sensor, platform) that provides functional component layers such as the operating system, runtime libraries, application programming interfaces/middleware, and network services). In any IdAM infrastructure or service offering, one or more of the IdAM services defined within the ICAM Services Framework (ref: Table 3.2) will be used. Therefore, there is a need to establish these as “components” or building blocks within the RA that can be used to create solution models. These models can range from simple DoD Architecture Framework (DODAF) compliant System View Interface Diagram (SV-1) figures to more complex workflow and data flow diagrams (e.g., OV-6c, SV-7). Although it is not within the scope of this rules-based RA to create those models/diagrams, it is necessary for it to provide the essential “generic” containers or component definitions, and extend them where necessary to enable those diagrams and views to be created.

The component definitions provided by this RA are either sub-components of the current established or candidate DoD, SC IdAM service offerings, or are generic components that provide one or more IdAM services. Furthermore, each component has been defined separately to accommodate the greatly differing non-tactical and tactical DoD operational environments.

The non-tactical component definitions are required to support the Generating Forces’ operational environments that will almost exclusively leverage enterprise-level identity, authentication, and authorization services. These non-tactical operational environments will be

supported by a robust and reliable network transport capability, and only in mission-essential environments will they have the ability to perform these IdAM functions on their own.

The tactical component definitions are required to support theatre and forward area ground force deployments, fleets of ships at sea, and aircraft units in flight. These definitions will apply to one or more Mission Environments (ME), as outlined in the Army's *Common Operating Environment (COE) Architecture: Enterprise – Camp/Post/Station, Command Post, Mounted, and Soldier/Sensor*. There are times when these MEs may be characterized as “disconnected” and/or “network-disadvantaged”, when network connectivity is intermittent or significantly degraded at times. The major contributing factor would be the lack of reliable Wide Area Network (WAN) (e.g., Global Information Grid (GIG)) connectivity to support “reach-back” capability to attribute-data and authentication and authorization mechanisms.

Nevertheless, all tactical logical and physical resources will always need to reliably, securely, and persistently authenticate their users, and provide authorization to them for access to applications, data, operating areas, facilities, weapons systems, and other physical entities. They must be able to provide Authentication and Authorization services independent of the availability of enterprise IdAM services and infrastructure the majority of the time. Although the non-tactical and tactical versions of these components would provide the same IdAM services, their deployed components would be forced to function under vastly different external conditions. This is the principal justification for establishing the two groupings of components within this RA. This forces the Business Rules' assumptions, constraints, and risk descriptions in Section 3 to address the full spectrum of possible DoD and SC operational environments.

Therefore, all component definitions have been aligned to each of the following operational environments:

### **Non-Tactical (prefixed with “NT-”)**

DoD/Joint Enterprise: IdAM components and services that support non-tactical logical and physical DoD Enterprise resources (e.g., Joint operations network domains, applications, data and facilities). These will be hosted, managed, and maintained only by DISA, and should include, but not be limited to:

- DoD Enterprise and Regional MS AD Forests and Domains
- Enterprise E-mail
- Enterprise MS SharePoint
- Enterprise Collaboration Services (e.g., Instant Messaging (IM))
- DoD Joint applications (e.g., General Fund Enterprise Business System (GFEBS))
- DoD or Coalition Partner Facilities
  - Joint and/or Coalition Operations Command Centers
  - DISA Enterprise Computing Centers (DECC)
  - DoD Intelligence Community (IC) Facilities

Service Component: IdAM components and services that directly support non-tactical logical and physical SC-specific operations Resources that either belong to, or are

managed by the Army, Navy, Air Force, Marines and/or any other SC organizations, but support non-tactical or business operations. These may be hosted and maintained by either DISA or the SCs, but are not considered DoD Enterprise or Joint services. These would be considered “Specialized SC Resources” and include, but not be limited to:

- Regional SC MS AD Forests and Domains
- Army Stationing and Installation Planning (ASIP)
- Naval Supply Systems Command (NAVSUP) Systems
- SC Facilities and Assets
  - Army/Navy/Marine/Air Force Bases
    - Operational areas
    - Buildings
- **Tactical (prefixed with “T-“)**

DoD/Joint Enterprise: IdAM components and services that support tactical logical and physical DoD Enterprise resources (e.g., Joint operations network domains, applications, data, and facilities). These will be hosted, managed and maintained only by DISA, and should include, but not be limited to:

  - Joint Theatre/Tactical MS AD Forests and Domains
  - Global Command and Control System (GCCS)
  - Global Combat Support System (GCSS)
  - Expeditionary Combat Support System (ECSS)
  - DoD or Coalition Partner Facilities
    - Strategic Command (STRATCOM) Operations Centers
    - Joint Theatre Operations Centers
    - Coalition Partner Bases
      - Operational areas
      - Buildings

Service Component: IdAM components and services that directly support tactical logical and physical SC-specific operations Resources that either belong to, or are managed by the Army, Navy, Air Force, Marines and any other SC organization, but support non-tactical or business operations. These may be hosted and maintained by either DISA or the SCs, but are not considered DoD Enterprise or Joint services. These would be considered ‘Specialized SC Resources’ and would include, but not be limited to:

- SC Theatre/Tactical MS AD Forests and Domains
- Army Blue Force Tracking
- Advanced Forward Area Tactical Data System (AFATDS)
- Naval Tactical Command Support System (NTCSS)
- Theatre Forward Area Facilities and Assets

- Brigade/Platoon Operations Centers
- Mobile Command Centers
- Warfighting Platforms (e.g., tanks, armored personnel carriers)
- Aircraft
- Ships/Submarines

Although this basic distinction is being made between tactical versus non-tactical support, it is not the responsibility of this RA to provide solution or deployment level design criteria as a mitigation mechanism. In all cases, and for all IdAM services addressed by this RA, it is assumed that sufficient infrastructure, to optimize network connectivity and bandwidth/data throughout, will be provided by both DoD/DISA and all of the SCs as required. Therefore, this means that every service, in support of all DoD sustaining base and deployed tactical operations will be as “virtual” as possible.

#### 2.2.3.4 IdAM Component Definitions

The following IdAM component definitions are provided as a basis for the discussions within the *Guiding Principles* and *Business Rules - Section 3* of this document:

##### 2.2.3.4.1 Attributes Data Repository (ADR)

ADR is a generic term for any IdAM service that stores identity attribute fields (by name), and the attribute data applicable to those fields. For example, “rank” is an attribute, and the attribute data can be values such as “COL,” “LTC,” “SGT”, etc. For the entire set of DoD Enterprise authoritative PE and NPE identity attributes and data that is consumed by other DoD Enterprise and SC IdAM services, this function is currently provided by the *Enterprise Identity Attribute Data Repository and Synchronization Service (EIADRSS)* component.

##### 2.2.3.4.2 Enterprise Identity Attribute Data Repository and Synchronization Service (EIADRSS)

EIADRSS is the PE and NPE ADR that functions as the identity attribute data collection service currently provided by DISA’s *DoD Identity Synchronization Service (IdSS)*. It collects PE attribute data from DoD authoritative data sources (e.g., *Defense Enrollment Eligibility Reporting System (DEERS)*, *Defense Manpower Data Center (DMDC)*). It will also collect Resource identity attribute data from NPE authoritative data sources. The identity attribute data is made available to all DoD and SC IdAM services at both the DoD Enterprise and SC levels to support Requester authentication, and authorization to both logical and physical Resources. All directory services and access authorization policies must utilize this enterprise dataset.

##### 2.2.3.4.3 Authentication and Authorization Framework (AAF)

An AAF is a generic integrated service whose principal functions are as follows:

- **Authentication:** Affirm that Requesters are who (or what) they claim to be when attempting to access both physical and logical Resources
- **Authorization:** Based on successful authentication, provide the logic and controls that will authorize a Requester to access logical and physical Resources

This RA will discuss two types of AAFs: a *Non-Tactical Authentication and Authorization Framework (NT-AAF)* and a *Tactical Authentication and Authorization Framework (T-AAF)*. A

*Non-Tactical Authentication Service Framework (NT-ASF)* or a *Tactical Authentication Service Framework (T-ASF)* would be a sub-component of each of these, respectively.

An AAF, coupled with a *Directory Service (DS)* and an *Account Provisioning Service (APS)*, is currently provided by the capabilities of COTS products such as *Microsoft AD* that is capable of providing authentication services using an X.509 certificate-based Public Key Infrastructure (PKI).

#### **2.2.3.4.4 Non-Tactical – Authentication Service Framework (NT-ASF)**

The NT-ASF will provide the DoD/Joint Enterprise and SC level authentication services to support both logical and physical access control to non-tactical Resources. These would include Joint, Coalition, and industry partner information/data, as well as physical facilities, devices, and networks. An NT-ASF can be integral to the NT-AAF, or it can be logically and physically decoupled or standalone where required.

#### **2.2.3.4.5 Tactical – Authentication Service Framework (T-ASF)**

The T-ASF will provide the DoD/Joint Enterprise and SC level authentication services to support both logical and physical access control to tactical Resources. These would include Joint, Coalition and industry partner information/data, as well as physical facilities, devices, and networks. The T-ASF can be integral to the T-AAF, or it can be logically and physically decoupled or standalone where required.

#### **2.2.3.4.6 Non-Tactical – Authentication and Authorization Framework (NT-AAF)**

The NT-AAF will provide the DoD/Joint Enterprise and SC level authentication and authorization services to support both logical and physical access control to non-tactical Resources. A NT-AAF will support non-tactical operating environments that have permanent and/or stable network WAN connectivity to DoD Enterprise IdAM services. All required updates to user or information Resource status and/or attribute and persona data will be executed in real-time (or near real-time) because WAN connectivity is constantly available and reliable. A NT-AAF can support non-tactical network domains, or may simply provide authentication and authorization services within a single application.

#### **2.2.3.4.7 Tactical – Authentication and Authorization Framework (T-AAF)**

The T-AAF will provide the DoD/Joint Enterprise and SC level authentication and authorization services to support both logical and physical access control to tactical Resources. T-AAF is a theater or DoD Enterprise wide capability. It will support any SC deployed tactical operating environment that is either disconnected and/or characterized by network-disadvantaged WAN connectivity to DoD/Joint Enterprise IdAM services. For example, theater-wide Authentication and Authorization services must operate at Army Brigade Combat Team (BCT), Division, and Corps levels where WAN (i.e., GIG) connectivity is not reliable all the time. To optimize security and reduce vulnerabilities and possible security breach impacts, each Combatant Commander (COCOM) would be best served by having its own T-AAF within their theatre of operations. If the framework is penetrated at the level of one single theatre, it will only affect that theater and not the entire DoD or Army tactical forces. All required updates to user or information Resource status and/or attribute and persona data would be executed as completely and as accurately as possible during periods of WAN availability. A T-AAF can support tactical network domains, or may simply provide authentication and authorization services within a single application in theatre. The T-AAF, coupled with a *Directory Service (DS)* and an *Account*

*Provisioning Service (APS)*, is currently provided by the capabilities of COTS products such as *Microsoft Windows Active Directory*. The T-AAF would provide authentication services using a Public Key Infrastructure (PKI).

#### 2.2.3.5 Directory Service (DS)

DS is a generic service that functions as an ADR for attribute data for users, as well as information systems and applications Resources (e.g., e-mail, instant messaging, Unified Communications (UC) services). These require a more limited set of attribute data to identify the users and Resources. A DS will store, organize, and distribute a subset of the attribute data that is collected in the EIADRSS. It provides basic user (i.e., Requester) identity information such as user name(s), location(s), phone number(s), e-mail address(es), and other information required to be known to and used by other users to exchange information. It also provides similar identification data on information systems, applications, databases, and other networked information Resources. These include, but are not limited to, server, portal, database, and printer name(s)/address(es)/location(s). A DS will not contain any attribute data that does not also exist in the EIADRSS.

Within this RA, the two types of DSs that will be discussed are the *Non-Tactical Directory Service (NT-DS)* and the *Tactical Directory Service (T-DS)*.

##### 2.2.3.5.1 Non-Tactical – Directory Service (NT-DS)

The NT-DS is a DS that provides a DoD Enterprise Global Address List (GAL) service, and specialized GAL views, directory search capability, and offline “white pages” services as part of the overall non-tactical level DoD/Joint Enterprise and SC level IdAM infrastructure. It provides a subset of the identity attributes provided by EIADRSS to support these services. NT-DS is principally a capability required within DoD Enterprise e-mail, MS SharePoint, Unified Communications (UC) and other “Joint” applications requiring directory service data to identify users and facilitate communications between them.

##### 2.2.3.5.2 Tactical – Directory Service (T-DS)

The T-DS is a DS that provides a DoD Enterprise Global Address List (GAL) service, and specialized GAL views, directory search capability, and offline “white pages” services as part of the overall tactical level DoD/Joint Enterprise and SC level IdAM infrastructure. Each T-DS will support its own unique GAL services. A T-DS is theater or DoD Enterprise wide capability. This can exist within any ME, and can operate disconnected and/or with network-disadvantaged WAN connectivity to DoD Enterprise IdAM services. For example, theater-wide directory services must operate at Army Brigade Combat Team (BCT), Division, and Corps levels where WAN (i.e., GIG) connectivity is not reliable all the time. To optimize security and reduce vulnerabilities and possible security breach impacts, each Combatant Commander (COCOM) would be best served by having its own T-DS within their theatre of operations. If the T-DS is penetrated at the level of one single theatre, it will only affect that theater and not the entire DoD or Army tactical forces. All required updates to T-DS data would be executed as completely and accurately as possible during periods of WAN availability. A T-DS would be capable of providing directory service data to tactical applications and theatre communications services such as UC nodes.

### 2.2.3.6 Offline Address Book (OAB)

OAB is a generic term for an Offline Address Book that provides DS information. There are times when DoD e-mail and other enterprise services users will not have network access, but still require the ability to access address and contact information to function. The OAB is a critical ICAM service within tactical environments where a non-colocated GAL may not always be available.

### 2.2.3.7 Account Provisioning Service (APS)

APS is a generic term for a service that provides DoD Enterprise administrators with the ability to create, delete, maintain or move user (i.e., Requester) accounts that are required to access both logical and physical Resources. It is to be utilized to manage user access to network, logical domains, applications, data, and other information Resources such as printers and faxes. It is also required to manage accounts that allow for all forms of physical access.

Within this RA, the two types of APSs that will be discussed are: *Non-Tactical – Account Provisioning Service (NT-APS)* and a *Tactical – Account Provisioning Service (T-APS)*.

#### 2.2.3.7.1 Non-Tactical – Account Provisioning Service (NT-APS)

The NT-APS is the DoD/Joint Enterprise and SC level logical and physical non-tactical Resource provisioning service. It will be used to provide application and user network domain account and policy provisioning for all DoD/Joint Enterprise and non-tactical SC information Resources. It is also required to manage accounts that allow for all forms of logical access. This includes access control for applications (e.g., Enterprise E-mail) as well as other Joint information. All required updates to user or information Resource status and/or attribute and persona data will be executed in real-time since WAN connectivity is constantly available and reliable.

#### 2.2.3.7.2 Tactical – Account Provisioning Service (T-APS)

The T-APS provides DoD/Joint Enterprise and SC tactical level logical and physical access provisioning services to theatre MEs as a means to create application and user network domain accounts, and manage their access policies and profiles. It is also required to manage accounts that allow for all forms of physical access in theatre. It would support any ME that is either disconnected and/or characterized by network-disadvantaged WAN connectivity to DoD/Joint Enterprise IdAM services. All required updates to user or information Resource status and/or attribute and persona data would be executed as completely and as accurately as possible during periods of WAN availability.

### 2.2.3.8 Single Sign-On Service (SSOS)

SSOS is a generic term for a service that provides AAF functionality to support a specialized form of access control. This is an authentication and authorization service that controls access to independently managed Resources, where all of the Resources share the same SSOS. It can also be used to allow for similar forms of physical access, such as to selected buildings and/or rooms at a DoD facility. It allows a user to authenticate one time in order to be authorized to access these grouped Resources, without being prompted to re-authenticate multiple times. As an SSOS provides access to many and possibly very sensitive information Resources once the user is initially authenticated, it is vital to consider the potential impact if a user's credentials are compromised by unauthorized persons, and then subsequently misused. Therefore, an SSOS will typically not provide authentication and authorization services to critical resources at the same

time as services to non-critical resources or services to the general public and DoD only resources.

This RA will discuss two types of SSOSs: a *Non-Tactical Single Sign-On Service (NT-SSOS)* and a *Tactical Single Sign-On Service (T-SSOS)*.

#### 2.2.3.8.1 Non-Tactical – Single Sign-On Service (NT-SSOS)

The NT-SSOS is the DoD/Joint Enterprise and SC IdAM service that allows segmented single sign-on capability to be applied to access control for one or more information Resources, such as systems, applications, and/or data Resources that could be accessed based on any PE's or NPE's single authentication transaction. This would be applicable to combinations of DoD Enterprise, Joint Operations, and/or SC-specific information resources (e.g., DoD Enterprise e-mail, MS SharePoint, (UC), or Joint applications). NT-SSOS is currently a proposed component within DISA's *Authentication Gateway Service (AGS)* service offering. It can also be used for similar forms of non-tactical physical access control.

#### 2.2.3.8.2 Tactical – Single Sign-On Service (T-SSOS)

The T-SSOS is the DoD/Joint Enterprise and SC IdAM service that allows segmented Single Sign-On (SSO) access control for one or more information Resources, such as systems, applications, and/or data Resources that can be accessed based on any PE's or NPE's single Authentication transaction. This would be applicable to combinations of DoD Enterprise, Joint Operations, and/or SC-specific tactical information Resources (e.g., fire support systems, forward area intelligence applications). T-SSOS is one component within DISA's proposed (AGS) offering. It would support any DoD/Joint Enterprise and SC deployed tactical operating environment that is either disconnected and/or characterized by network-disadvantaged WAN connectivity to supporting DoD Enterprise IdAM services. All required updates to sign-on policies would be executed as completely and as accurately as possible during periods of WAN availability. It can also be used to allow for similar forms of tactical physical access control.

#### 2.2.3.9 Reduced Sign-On Service (RSOS)

RSOS is a generic term for a service that provides AAF functionality to support a specialized form of access control. It allows a user to authenticate without the use of a "hard" credential such as a CAC or token, but may require multiple-factor Authentication. Authentication is typically in the form of a username/password and a secondary process such as answering one or more security questions (e.g., mother's maiden name), or using one or more forms of biometrics. Like SSOS, RSOS can allow a user to authenticate one time in order to be to be authorized to access these grouped Resources, without being prompted to re-authenticate multiple times. However, when access to sensitive or For Official Use Only (FOUO) information is involved, RSOS may be restricted to information Resources that do not fall into these categories. The purpose of this restriction would be to minimize the potential impact of a user's authentication in the event where a user's "soft" or RSOS credentials are compromised by unauthorized persons. In general, and particularly in the case of a RSOS, it will typically not allow the "keys to the castle" to be granted, but only to certain "rooms within the castle", as required.

This RA will discuss two types of RSOSs: a *Non-Tactical Reduced Sign-On Service (NT-RSOS)* and a *Tactical Reduced Sign-On Service (T-RSOS)*.

#### 2.2.3.9.1 Non-Tactical – Reduced Sign-On Service (NT-RSOS)

The NT-RSOS is the DoD/Joint Enterprise and SC IdAM service that allows a reduced sign-on capability to be applied to access control for one or more information Resources, such as systems, applications, and/or data Resources that could be accessed based on any PE's or NPE's single authentication transaction. An NT-RSOS could achieve its multi-factor Authentication using a username/password, one or more security questions, and/or biometrics with remote validation via any appropriate DoD network. Because of how this RA has characterized the “non-tactical” operating and mission environments, remote network-based Authentication would be the most readily available and cost-effective approach to non-tactical RSOS. This would be applicable to combinations of DoD Enterprise, Joint Operations, and/or SC-specific information resources (e.g., DoD Enterprise e-mail, MS SharePoint, (UC), Joint applications). NT-RSOS is currently a proposed component within DISA's AGS offering. It can also be used to allow for similar forms of non-tactical physical access control.

#### 2.2.3.9.2 Tactical – Reduced Sign-On Service (T-RSOS)

The T-RSOS is the DoD/Joint Enterprise and SC IdAM service that allows a reduced sign-on capability to be applied to access control for one or more information Resources, such as systems, applications, and/or data Resources that can be accessed based on any PE's or NPE's single Authentication transaction. In a T-RSOS, unlike an NT-RSOS, the authentication is done by the centralized service, and the authorization is done locally by the application/system. This would be applicable to combinations of DoD Enterprise, Joint Operations, and/or SC-specific tactical information Resources (e.g., fire support systems, forward area intelligence applications). A T-RSOS could achieve its two-factor Authentication using biometrics and remote validation via any DoD network when available, or would more likely perform authentication locally without being fully dependant on the availability of a network. Because of how this RA has characterized the “tactical” operating and mission environments, this is not always the most practical approach to tactical RSOS authentication. T-RSOS would be one component within DISA's proposed AGS offering. It would support any DoD/Joint Enterprise and SC deployed tactical operating environment that is either disconnected and/or characterized by network-disadvantaged WAN connectivity to supporting DoD Enterprise IdAM services. All required updates to sign-on policies would be executed as completely and as accurately as possible during periods of WAN availability. It can also be used to allow for similar forms of tactical physical access control.

#### 2.2.3.10 Rules Engine (RE)

In the Attribute-Based Access Control (ABAC)/Rule (or Role) Based Access Control (RBAC) model, there is an entity called the “Policy Engine” (often called “PE” in other ABAC/RBAC architectures). In this RA, it is named the “Rules Engine (RE)” to avoid confusion with the term “Person Entity” (also abbreviated as PE). The RE is the generic component that contains the Policy Store (PS), Policy Decision Point (PDP), and the Policy Enforcement Point (PEP), as defined and described in Appendix D. A RE can exist in both the non-tactical and tactical operational environments. Because all enterprise level access policies (i.e., rules) must be the same across the DoD Enterprise, this RA will only refer to a generic form of RE, and not further define unique components for both environments.

### 2.2.3.10.1 Policy Store (PS)

The PS that is referred to in this RA has extended the PS definition provided in Appendix D within the ABAC/RBAC model (ref: Figure D-1). Therefore, the PS in this document is the generic sub-component of the RE that either contains the basic access policy logic structures/templates, or the policies themselves that are to be utilized by the PDP and PEP. A PS can exist in both the non-tactical and tactical operational environments. Because all enterprise level access policies must be the same across the DoD Enterprise, this RA will only refer to a generic form of PS, and not further define unique components for both environments.

### 3 Guiding Principles and Business Rules

#### 3.1 Service Area/Services to Guiding Principles and Business Rules Mapping

As shown in Table 3.1, IdAM Service Areas can be mapped to the “operational” Guiding Principles and Business Rules outlined in this architecture. This is a “one-to-many” mapping that helps depict how these Guiding Principles align with the “functional” components in any IdAM solution.

The IdAM Service Areas are subsets of the ICAM Service Areas defined in the current DoD Identity, Credentialing and Access Management (ICAM) Services Framework, as shown in the grey boxes in Table 3.2. There is one or more associated ICAM service for each ICAM Service Area.

IdAM Service Areas to Guiding Principles Mapping							
IdAM Service Areas							
Identity Data Management		Directory Services	Identity Authentication		Access Authorization		Access Auditing
IdAM Guiding Principles	(P1) Unique Identity & Credentials	(P4) Global Director E-Mail Services	(P5) Authentication & Authorization	(P8) Physical Access	(P5) Persona-Based Access	(P9) General IdAM Security Policy	(P9) General IdAM Security Policy
	(P2) Identity Authoritative Data Source		(P6) Dynamic Access Control	(P9) General IdAM Security Policy	(P6) Dynamic Access Control	(P10) Single Sign-On Capability	
	(P3) Person Entity & NoN-Person Entity Identity	(P9) General IdAM Security Policy	(P7) Access to Data, Services And Applications	(P10) Single Sign-On Capability	(P7) Access to Data, Services and Applications	(P11) Network Access Control	(P12) Monitoring & Reporting
	(P9) General IdAM Security Policy				(P8) Physical Access		

Table 3.1 – IdAM Service Areas to Guiding Principles Mapping

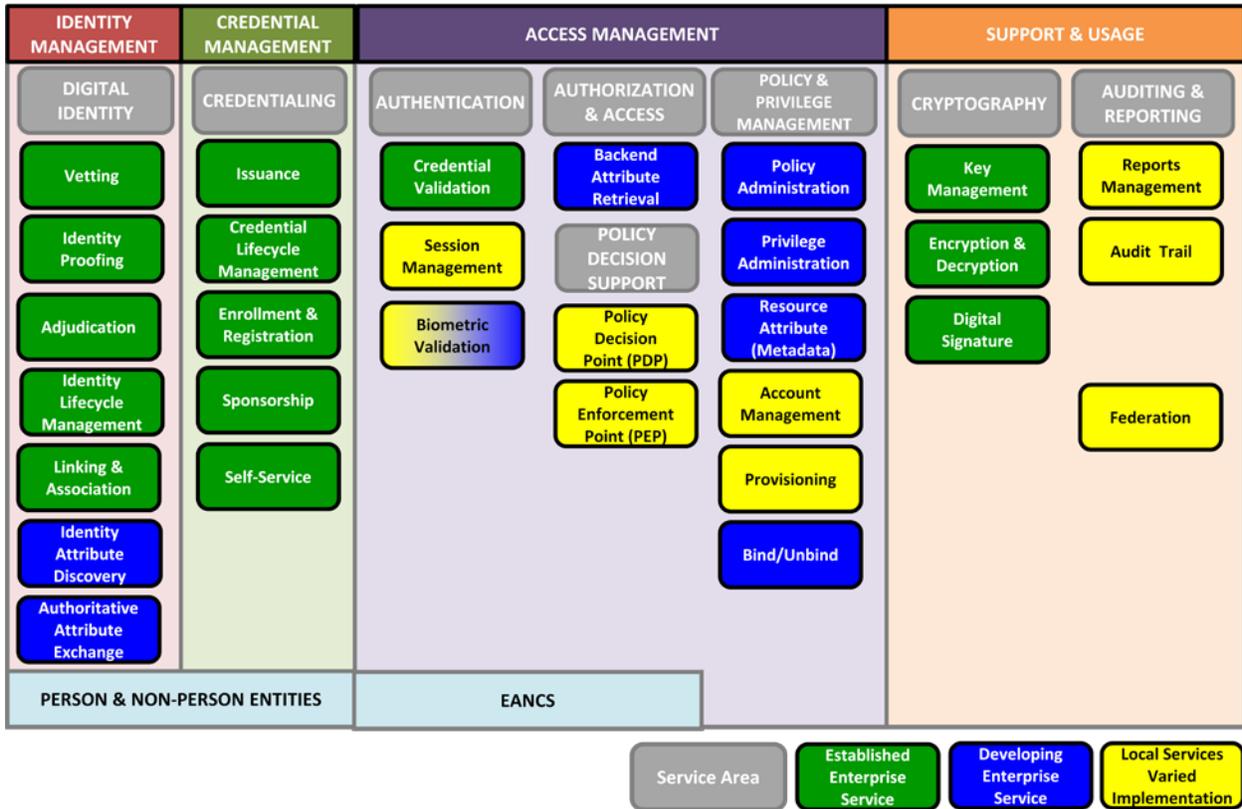


Table 3.2 – DoD ICAM Services Framework

The mapping of the ICAM Services Areas to the IdAM Service Areas is a “many-to-one” relationship, as shown in Table 3.3.

IdAM Service Areas to DoD ICAM Service Areas Mapping					
	IdAM Service Areas				
	Identity Data Management	Directory Services	Identity Authentication	Access Authorization	Access Auditing
DoD ICAM Service Areas	Digital Identity	Authorization & Access	Authentication	Authorization & Access	Auditing & Reporting
	Credentialing		Cryptography	Policy Decision Support Policy & Privilege Management	

Table 3.3 – DoD ICAM Service Areas to IdAM Service Areas Mapping

## 3.2 Specifications

### 3.2.1 (P1) Principle 1 – Unique Identity and Credentials

Principle	Description	References
<i>All authorized Person Entities (PE) and Non-Person Entities (NPE) will have one identity that is recognized by all producers of information and services.</i>	Persons seeking access to information and any physical entities within the DoD Enterprise 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.	Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012

Table 3.4 – Unique Identity and Credentials Principle

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

Business Rule	Description	References
<i>Electronic Data Interchange Personal Identifier (EDI-PI) Personnel Type Code (PTC) and Personnel Category Code (PCC) will be used as the digital identity for all users with Common Access Cards (CAC) or an interim equivalent.</i>	An 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 the DoD through DEERS, and any other similar interim mechanism (e.g., SIPRNET Hard Token) is required to support user authentication. Currently, a person with more than one personnel category is issued a CAC for each persona.	Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 ----- DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012

Table 3.5 – Person Entity (PE) Unique Identifier Business Rule

##### 3.2.1.1.1 (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
- All CACs will be X.509 certificate based
- All SCs use the PCCs

##### 3.2.1.1.2 (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
- Any smart card that is used for access to classified Resources must not allow executable code to be stored or run within it

### 3.2.1.1.3 (P1/R1) Risk

- Constantly shifting personnel strength and responsibilities will increase the level of difficulty associated with creating, modifying, and deleting PE Persona, and linking them with the right EDI-PI

### 3.2.1.1.4 (P1/R1) Technical Positions and Patterns

#### ➤ Core Standards

##### Technical

- ISO/IEC 14443: Specifies the physical characteristics of Proximity Integrated Circuit Cards, (PICC). It applies to identification cards of the ID-1 card type operating in proximity to a coupling device. This part of ISO/IEC 14443 shall be used in conjunction with later parts of ISO/IEC 14443 which are in development. The contactless technology may coexist with other technologies on the same physical medium. Most smartcard manufacturers offer dual interface cards — contact and ISO 14443 contact and contactless, that may support magnetic stripe, barcode and hologram

### 3.2.1.2 (P1/R2) Business Rule 2 – Allowed Identities

Business Rule	Description	References
<i>The DoD will use a single digital identity to uniquely identify an individual or NPE, while denying DoD network access to anonymous.</i>	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 DoD Enterprise without first establishing their identities.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Page 12)

Table 3.6 – Allowed Identities Business Rule

#### 3.2.1.2.1 (P1/R2) Assumptions

- All PEs and NPEs can be assigned unique identifiers that will allow X.509 certificates to be assigned and removed from association with them
- Identification of NPE would not be limited to legacy identification mechanisms and formats (e.g., network Media Access Control (MAC) or Internet Protocol (IP) addresses, Security Identifier (SID))

#### 3.2.1.2.2 (P1/R2) Constraints

- An Electronic Data Interchange Personal Identifier (EDI-PI) must be assigned to every PE
- A globally unique Identifier (GUID) must be assigned to every NPE
- Once established the EDI-PI must remain associated with the PE
- Once established the GUID must remain associated with the NPE

- When a PE or NPE no longer requires access to DoD information, networks, and facilities, the identifier must not be re-assigned, in the event that the same entity is re-issued access in the future

#### 3.2.1.2.3 (P1/R2) Risk

- If identity data is assigned to the wrong PE or NPE, invalid authorization may occur.
- Restriction of anonymous access will only be valid if real-time access to an authoritative identity directory service is maintained (e.g., PKI certificate management services – Online Certificate Status Protocol (OCSP), Certificate Revocation Lists (CRL))
- Unless identity data is regularly audited to assure that it is uniquely associated with a PE or NPE, it is possible that an anonymous or unauthorized entity could be allowed access

#### 3.2.1.2.4 (P1/R2) Technical Positions and Patterns

### ➤ Core Standards

#### Technical

- NIST SP 800-87: Provides the organizational codes necessary to establish the Personal Identity Verification Federal Agency Smart Credential Number (PIV FASC-N) that is required to be included in the FIPS 201 Card Holder Unique Identifier (CHUID); SP 800-86 is a companion document to FIPS 201
- ISO/IEC 19794-5:2011: Provides a face image format. Digital face images are used in many applications, including human examination as well as computer automated face recognition. Although photographic formats have been standardized in some cases (e.g., passports and driver licenses), the DoD needs to define a standard data format for digital face images to allow interoperability among vendors

#### Policy/Regulatory

- DoDI 8520.03: This instruction furnishes DoD policy provides criteria and methodology for determining appropriate identity credentials for identity authentication, information system owners, and persons responsible for allowing access to physical facilities or locations. It requires these individuals to choose the specific type(s) of identity credential used in an identity authentication process based on the sensitivity of the information or facility that can be accessed, the strength of the identity credential, and the environment or location where the identity credential is being presented

## 3.2.1.3 (P1/R3) Business Rule 3 – Identity Suitability

Business Rule	Description	References
<p><i>The DoD 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.</i></p>	<p>Identities are comprised of hierarchical layers of associated attributes. In addition to a unique identifier (i.e., EDI-PI), one or more Persona 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 or NPE's identity lifecycle management will be based on these elements which can serve as major components of access policies across the DoD Enterprise. 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 Reservist CAC for the same person have the same values, and so systems/applications cannot differentiate between the Civil Service persona versus the Reserve 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.</p>	<p>Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Pages 27, 89)</p>

Table 3.7 – Identity Suitability Business Rule

## 3.2.1.3.1 (P1/R3) Assumptions

- PE Persona and their associated Persona definitions will be the basis for “need-to-know” access rules
- PE and NPE Persona will be manageable to accommodate changes in mission, function, and/or location across the DoD Enterprise
- Persona will be portable across the DoD Enterprise

## 3.2.1.3.2 (P1/R3) Constraints

- Persona 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
- A determination of Persona accuracy must be maintained throughout the life cycle of all digital identities

## 3.2.1.3.3 (P1/R3) Risk

- Failure to do regular due-diligence on Persona assignments may result in “hijacking” of Authorization privileges, and access to unauthorized 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

### 3.2.1.3.4 (P1/R3) Technical Positions and Patterns

#### ➤ Core Standards

##### Technical

- IETF RFC 2589: Supports lightweight access to static directory services, allowing relatively fast search and update access. Static directory services store information about people that persists in its accuracy and value over a long period of time

##### Policy/Regulatory

- DoDI 8520.03: This DoD policy, in accordance with Reference (b), provides criteria and methodology for determining appropriate identity credentials for identity authentication, information system owners and persons responsible for allowing access to physical facilities or locations; those individuals shall choose the specific type(s) of identity credential used in an identity authentication process based on the sensitivity of the information or facility that can be accessed, the strength of the identity credential, and the environment or location where the identity credential is being presented

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

Business Rule	Description	References
<i>The consistency and integrity of identity data will be enforced through policies, processes, and tools.</i>	The reliability of identity data is foundational to trust and the ability to access and consume information from a service/agency and multinational environment. Adherence to a standard digital identity “language” format will allow the required access Policies to be created and executed in a non-ambiguous manner.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Page 32)

Table 3.8 – Identity Data Integrity Business Rule

#### 3.2.1.4.1 (P1/R4) Assumptions

- The DoD identity data standards are established and can be applied consistently.
- Identity data attributes will have a consistent set of possible values, meanings, and context at any one point in time

#### 3.2.1.4.2 (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 as limited exposure as possible to all access management components

#### 3.2.1.4.3 (P1/R4) Risk

- Unless identity data integrity is maintained for all non-U.S. or DoD entities requiring access to information, it will be impossible to maintain consistent policies and practices that constrain such access
- Bad or inconsistently applied policies that allow unnecessary or accidental exposure and/or storage of PII could result in a violation of law

#### 3.2.1.4.4 (P1/R4) Technical Positions and Patterns

##### ➤ Core Standards

##### Technical

- RSA Laboratories PKCS #12: Supports direct transfer of personal information under several privacy and integrity modes. The most secure of the privacy and integrity modes require the source and destination platforms to have trusted public/private key pairs usable for digital signatures and encryption, respectively
- ISO/IEC 7816-11: Specifies the usage of inter-industry commands and data objects related to personal verification through biometric methods in integrated circuit cards

#### 3.2.1.5 (P1/R5) Business Rule 5 – Identity Data Discoverability

Business Rule	Description	References
<i>Identity data should be transparent to PE and NPE location, and the attribute data should be discoverable by authorized access policy and control components.</i>	The ability to post and access identity data is reliant upon a known, visible, authoritative Attributes Data Repository (i.e., EIADRSS) and the ability for a Rules Engine to access and utilize in authentication and authorization.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011

Table 3.9 – Identity Data Discoverability Business Rule

#### 3.2.1.5.1 (P1/R5) Assumptions

- Attribute data will be organized so that access by any consumer will be non-ambiguous and reliable
- Coherency between attribute data and access policy rules is assured

#### 3.2.1.5.2 (P1/R5) Constraints

- 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 extended beyond the PDP to any other authorization services

#### 3.2.1.5.3 (P1/R5) Risk

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

### 3.2.1.5.4 (P1/R5) Technical Positions and Patterns

#### ➤ Core Standards

##### Technical

- SP 800-73: Interfaces for Personal Identity Verification (PIV) that specify the PIV data model, command interface, client Application Programming Interface (API), and references to transitional interface specifications
- ISO/IEC 19794-1:2011: Describes the general aspects and requirements for defining biometric data interchange formats. The notation and transfer formats provide platform independence and separation of transfer syntax from content definition

### 3.2.1.6 (P1/R6) Business Rule 6 – Identity Data Conformance

<b>Business Rule</b>	<b>Description</b>	<b>References</b>
<i>Digital identity data will conform to relevant schema and business rules.</i>	The IdAM process will be constructed around agreed-to business processes along with a data schema that allows for specific profiles for attribute exchanges.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Pages 37, 91)

Table 3.10 – Identity Data Conformance Business Rule

#### 3.2.1.6.1 (P1/R6) Assumptions

- A standard data schema can be maintained for all identity data
- All access policies will be based on a standard identity attribute data schema
- Digital identity data will consist of informational attributes, access control attributes, and functional attributes, at a minimum

#### 3.2.1.6.2 (P1/R6) Constraints

- Digital identity data must be comprised of only the essential attributes required to specify any PE or NPE and any required Persona or profile
- Identity data schema must be synchronized across the DoD Enterprise

#### 3.2.1.6.3 (P1/R6) Risk

- Inconsistent data schema will prevent synchronization of data and interoperability
- Without an enterprise view and management capability for identity data schema, attribute management will be extremely difficult; consistent enterprise resource access will not be assured

3.2.1.6.4 (P1/R6) Technical Positions and Patterns

➤ Core Standards

Technical

- SP 800-103: Provides the broadest possible range of identity credentials and supporting documents as they pertain to identity credential issuance. It gives priority to examples of primary and secondary identity credentials issued within the United States. Part 2 of this document will provide Extensible Markup Language (XML) schemas as a framework for retention and exchange of identity credential information

3.2.1.7 (P1/R7) Business Rule 7 – Authentication and Authorization Service Provisioning

Business Rule	Description	References
<i>Any Authentication and Authorization Framework (AAF) shall be provisioned by an Account Provisioning Service (APS) available to both the DoD Enterprise and the Service Components (SC).</i>	Any logical and physical Resource will require use of both an authentication and an authorization service. This is supported by an AAF, or an ASF and an independent authorization service. However, the preference would be to leverage the use of an enterprise level AAF that would be provisioned and managed by an APS.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012

Table 3.11 – Authentication and Authorization Service Provisioning Business Rule

3.2.1.7.1 (P1/R7) Assumptions

- The number of DoD and SC AAFs will be minimized, while optimizing support for Joint warfighting operations
- Provisioning of all AAFs and APSs will utilize a single primary enterprise identity attribute data repository
- A limited attribute dataset will support directory services.
- Tactical operating units (Brigade Combat Team, Regiment, Division, Corps, Army, Fleet, Air Wing) can be supported by their own independent T-AAFs and T-APS

3.2.1.7.2 (P1/R7) Constraints

- SCs must not create any new individual system or applications level directory services that are not also included in the DoD Enterprise directory services dataset
- Any APS must support all form of access account provisioning (e.g., network domains, systems, applications, data, facilities, any physical or NPE assets)

3.2.1.7.3 (P1/R7) Risk

- The inability to update identity attribute data accurately and/or in a timely manner in the EIADRSS (out of the 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

## 3.2.1.8 (P1/R8) Business Rule 8 – Enterprise Identity Repository

Business Rule	Description	References
<i>DoD Components shall not create or utilize a non-approved independent identity repository for authentication.</i>	The continued propagation of “stovepipe” identity data repositories must end. Identities will be initiated by authoritative data sources, then collected and distributed to all consuming IdAM services across the DoD Enterprise. 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 reliance on and/or direct dependence on the Enterprise Identity Attribute Data Repository and Synchronization Service (EIADRSS).	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011

Table 3.12 – Enterprise Identity Repository Business Rule

## 3.2.1.8.1 (P1/R8) Assumptions

- All or most legacy DoD Enterprise non-tactical information Resources will be capable of being transitioned to an enterprise level ADR (i.e., EIADRSS) to support enterprise authentication services
- The EIADRSS assures that non-ambiguous identity data is maintained for use across the DoD information enterprise

## 3.2.1.8.2 (P1/R8) Constraints

- Non-tactical legacy information Resources and systems-of-systems that cannot easily be transitioned to use an EIADRSS must be either subsumed or sunset

## 3.2.1.8.3 (P1/R8) Risk

- If the EIADRSS 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 EIADRSS attribute data concurrency cannot be maintained at the tactical level with minimal latency in accuracy, invalid authentications may occur

## 3.2.1.8.4 (P1/R8) Technical Positions and Patterns

## ➤ Core Standards

Technical

- SP 800-122: Assists Federal agencies in protecting the confidentiality of a specific category of data commonly known as PII. This document provides practical, context-based guidance for identifying PII and determining what level of protection is appropriate for each instance of PII. The document also suggests safeguards that may offer appropriate levels of protection for PII and provides recommendations for developing response plans for breaches involving PII

### 3.2.2 (P2) Principle 2 – Identity Authoritative Data Source

Principle	Description	References
<i>Identities should be tied to universal portable credentials (i.e., enterprise digital identities), and are maintained by an authoritative data source.</i>	Identities established by a centralized authoritative data source will be portable and reusable across the DoD Enterprise.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Page 35)

Table 3.13 – Identity Authoritative Data Source Principle

#### 3.2.2.1 (P2/R1) Business Rule 1 – Defense Manpower Data Center (DMDC) Person Entity (PE) Identity Attribute Data Brokering

Business Rule	Description	References
<i>The Defense Manpower Data Center (DMDC) will be the primary broker for Person Entity (PE) authoritative identity data to define and maintain Personas.</i>	<i>The DMDC maintains the largest archive of personnel, manpower, training, and financial data in the DoD, and is the most qualified source for authoritative personal identity information. It will be used to establish and maintain the authoritative PE attribute dataset. All authoritative attribute data to support all DoD/Joint operations is brokered by DMDC, as shown in Figure 1.2.</i>	DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012

Table 3.14 – Defense Manpower Data Center (DMDC) Person Entity (PE) Identity Attribute Data Brokering Business Rule

##### 3.2.2.1.1 (P2/R1) Assumptions

- DMDC maintains reliable and accurate authoritative identity data from DoD personnel management systems and data sources
- The authoritative data maintained in DMDC can be considered “near real-time” accurate according to established DISA Service Level Agreements (SLAs)

##### 3.2.2.1.2 (P2/R1) Constraints

- All identity data consumed by 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 EIADRSS

##### 3.2.2.1.3 (P2/R1) Risk

- Data value errors in DMDC will propagate across EIADRSS, DSs, ASFs, and AAFs, and will impact the accuracy and effectiveness of APS 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 and/or encounters network-disadvantaged WAN connectivity, unauthorized access to information and physical Resources may be granted
- All IdAM service consumers that 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

3.2.2.1.4 (P2/R1) Technical Positions and Patterns

➤ Core Standards

Policy/Regulatory

- CNSSI Number 1253: Provides all Federal Government departments, agencies, bureaus, and offices with a process for security categorization of National Security Systems (NSS). It references a comprehensive set of security controls and enhancements that may be applied to any NSS. CNSSI No. 1253 also provides tailoring guidance so that organizations may select a robust set of security controls to secure their NSS based on assessed risk

3.2.2.2 (P2/R2) Business Rule 2 – Common Access Card (CAC) Usage

Business Rule	Description	References
<p><i>The Common Access Card will be used as the primary identification credential within the DoD.</i></p>	<p>CAC – PIV v2.0 compliant cards will be used as the preferred authoritative credential mechanism to support any Public Key Infrastructure (PKI)-based access within the 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 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 “smart card” (e.g., SIPRNET Token) must be issued.</p>	<p>Draft DoD Identity and Access Way Forward: DoD ICAM Transition (Pages 40-42)</p> <p>-----</p> <p>DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012</p>

Table 3.15 – Common Access Card (CAC) Usage Business Rule

3.2.2.2.1 (P2/R2) Assumptions

- CAC provisioning is assumed to be accurate at the time the CAC is issued
- The CAC Personal Identification Number (PIN) is uniquely bound to any CAC for any one user
- Loss of physical control of a CAC is identifiable and can be quickly mitigated by a process of certificate revocation

- Loss of physical control of a CAC may also be mitigated by the use of alternate biometrics
- Classified logical and physical Resource access must be supported by a smart card or other separate digital identity mechanism

#### 3.2.2.2.2 (P2/R2) Constraints

- This rule only applies to DoD CAC-holders who require access to information and facilities Resources

#### 3.2.2.2.3 (P2/R2) Risk

- Mobile or portable computing devices with network access may not always be able to physically interface with CAC readers
- If a CAC is lost, damaged, or destroyed, an alternate non-CAC authentication methodology must be available
- Tactical environments may not be supported well using CAC-based authentication.
- Tactical environment access (logical and physical) to classified Resources may not be supported well by a smart card

#### 3.2.2.2.4 (P2/R2) Technical Positions and Patterns

### ➤ Core Standards

#### Technical

- FIPS Pub 201-1 (Part two): Provides detailed specifications that will support technical interoperability among the PIV systems of Federal departments and agencies. It describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card
- SP 800-73 – Interfaces for Personal Identity Verification: Specifies the PIV data model, command interface, client Application Programming Interface (API), and references to transitional interface specifications

## 3.2.2.3 (P2/R3) Business Rule 3 – Resource Account Provisioning Service (APS)

Business Rule	Description	References
<p><i>Combined Directory, Authentication, Authorization and Account Management services must be supported by an Account Provisioning Service (APS) for all logical and physical Resource access account lifecycle management.</i></p>	<p>DoD and SC Directory, Authentication, Authorization, and Account Management services are all currently provided within the <i>Microsoft Active Directory Forests and Domains</i> and their supporting infrastructure, by a set of management services for :</p> <ul style="list-style-type: none"> <li>• User accounts</li> <li>• Domain relationships</li> <li>• Lightweight Directory Access Protocol (LDAP) configuration</li> <li>• Authentication</li> <li>• Policies (User and Group)</li> </ul> <p>These are currently used within the existing deployed MS AD infrastructures at the DoD Enterprise/Joint and SC levels to support both non-tactical and tactical operations. In any case, as defined by this RA, an (APS) is required. All PE and NPE access accounts will be created and managed leveraging some or all of the PE and NPE identity attributes made available by the EIADRSS.</p>	<p>Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012</p>

Table 3.16 – Resource Account Provisioning Service (APS) Business Rule

## 3.2.2.3.1 (P2/R3) Assumptions

- The current DoD and SC MS AD Forest/Domain infrastructures are in transition to a new regionalized configuration
- The T-APS will eliminate the need to use external systems (e.g., currently Army *EDS-Lite*) to maintain MS AD identity data in each Forest and its member Domains
- Use of an enterprise/centralized provisioning service is optional for existing and future DoD and SC MS AD Forests and Domains, but must derive authorization policies only from the authoritative enterprise attribute data schema provided by the EIADRSS

## 3.2.2.3.2 (P2/R3) Constraints

- The EIADRSS must maintain synchronization of identity data across all of any one Service’s existing MS AD Forest and domain infrastructures
- The EIADRSS must not identify attributes that are unique to any one SC

3.2.2.4 (P2/R4) Business Rule 4 – Adding Core PE Identity Attributes

Business Rule	Description	References
<p><i>Service Components (SC) can propose or request supplements to the existing core enterprise identity attributes repository, but all DoD enterprise identity data attributes must either already exist in an authoritative identity data source (e.g., DEERS, DMDC), or be approved by DoD to be added to them.</i></p>	<p>If adding additional identity attributes is required for PE or NPE, this can occur in two ways: 1) Existing identity attributes available in the authoritative data sources can be identified, vetted, and approved; or 2) New attributes can be proposed to be included in the core enterprise identity data schema provided by the EIADRSS. Currently, the EIADRSS component is provided by DISA’s <i>Identity Synchronization Service (IdSS)</i>.</p>	<p>Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Pages 60, 61) ----- DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012</p>

Table 3.17 – Adding Core PE Identity Attributes Business Rule

3.2.2.4.1 (P2/R4) Assumptions

- The mechanism for DoD Enterprise access authorization requires a separate repository to contain both Requester and Resource identity attributes
- The required identity attributes do not already exist in the EIADRSS
- The required identity attributes may already exist in a DoD registered and approved authoritative data source
- The ASF will use the EIADRSS identity attribute set

3.2.2.4.2 (P2/R4) Constraints

- Any additional required attributes must not already exist in the EIADRSS
- New attributes must never directly populate the EIADRSS
- The EIADRSS component must never maintain any SC’s unique identity data attributes that are not included in the enterprise authoritative identity attribute data schema provided by the EIADRSS
- Proposed enterprise identity attributes for a SC must be submitted through a governance process that reviews and approves the request(s) prior to use at both the DoD Enterprise and SC levels

3.2.2.4.3 (P2/R4) Risk

- If proposed additional identity attributes are not vetted for non-ambiguity and re-usability by other SCs, accurate access policies cannot be created and used across the DoD Enterprise

3.2.2.4.4 (P2/R4) Technical Positions and Patterns

- Core Standards  
Technical

- UCore DIG v2.0.0: This standard is a Federal information sharing initiative that supports the National Information Sharing Strategy and all associated departmental/agency strategies. UCore enables information sharing by defining an implementable specification (XML Schema) containing agreed upon representations for the most commonly shared and universally understood concepts of who, what, when, and where

Policy/Regulatory

- DoDI 8520.03: Establishes and defines sensitivity levels for purposes of determining appropriate authentication methods and mechanisms
- DoDD 8320.02: States data assets shall be made accessible by making data available in shared spaces. All data assets shall be accessible to all users in DoD except where limited by law, policy, or security classification

3.2.2.5 (P2/R5) Business Rule 5 – Adding Core NPE Identity Attributes

Business Rule	Description	References
<p><i>The DoD may supplement the enterprise identity attributes data repository identity data schema with additional or “extended” attributes as needed, to provide expanded PE and NPE Requester identity data, and to support more fine-grained Resource authorization policies or experience customizations as required.</i></p>	<p>Applications and information Resources may require additional identity attributes to support the execution of required authorization policies. Management of these attributes that are available within the Enterprise Identity Attribute Data Repository and Synchronization Service (EIADRSS)* to the 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 the EIADRSS are derived solely from an authoritative DoD data source, and will never be updated directly to the EIDRSS or any ADR by an SC.</p> <p>* The EIADRSS is the ADR to support DISA’s Enterprise Identity Directory Service (EIDS) offering. EIDS itself will not provide an ADR.</p>	<p>DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012</p>

Table 3.18 – Adding Core NPE Identity Attributes Business Rule

3.2.2.5.1 (P2/R5) Assumptions

- The mechanism for SC access authorization policy utilizes the DoD repository that contains both Requester and Resource identity attributes
- The required “extended” identity attributes do not already exist in the EIADRSS.
- Resource attribute data can be federated to the DoD enterprise level by the SCs, but would be initially treated as candidates to be added to the EIADRSS

3.2.2.5.2 (P2/R5) Constraints

- Any identity attributes added to the DoD Enterprise dataset must be provided by the EIADRSS

- Any “extended” identity attributes and attribute data originate from an authoritative data source (e.g., DEERS, DMDC)
- No SC level identity attributes for either PE or NPE will be created, stored, or distributed by the SCs, either within the SCs or directly to the DoD Enterprise level

#### 3.2.2.5.3 (P2/R5) Risk

- An ABAC service capability leveraging the EIADRSS will not be possible if Resource attribute data cannot be fully and accurately maintained
- If SCs create local “extended” identity attributes themselves, which do not become instantiated in the EIADRSS, this will limit or possibly prevent full Joint interoperability by not supporting access between different SC applications and other information Resources
- If SCs create local “extended” identity attributes and add them to the EIDRSS dataset directly, this may limit or prevent Joint interoperability by not allowing personnel of different SCs to access shared Resources

### 3.2.3 (P3) Principle 3 – Person Entity (PE) and Non-Person Entity (NPE) Identification

Principle	Description	References
<i>Identities should 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.</i>	Identity data must be developed for all PE and NPE, to include both DoD and non-DoD entities and assets.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Pages 12- 19, 73) ----- DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012

Table 3.19 – Person Entity (PE) and Non-Person Entity (NPE) Identification Principle

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

Business Rule	Description	References
<i>A digital identity standard will be established to support mobile/edge platforms/devices.</i>	Enterprise Identity Management must be consistent in terms of identity data and process workflow for all NPE, from business mission areas to tactical-deployed assets, to include all devices that reside in the mobile, platform, or sensor computing environments.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition (Pages 12- 19)

Table 3.20 – Mobile/Edge Platforms/Devices Business Rule

##### 3.2.3.1.1 (P3/R1) Assumptions

- Mobile, edge platforms and devices will have the ability to be credentialed in the same manner as any other NPE
- Mobile, edge platforms and devices will be “CAC-enabled” as well as “Token-enabled” for classified Resource access

##### 3.2.3.1.2 (P3/R1) Constraints

- Mobile, edge platforms and devices (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 for authentication while they are operating in ‘disconnected’ and/or ‘network- disadvantaged’ environments (e.g., classified, tactical)
- No identity data or attributes may be stored on non-volatile media on any mobile, edge platforms or device

3.2.3.1.3 (P3/R1) Risk

- Mobile/Edge platform/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

3.2.3.1.4 (P3/R1) Technical Positions and Patterns

➤ Core Standards

Technical

- IETF RFC 2794: Provides authentication and authorization services for dial-up computers. Such services are likely to be equally valuable for mobile nodes using Mobile IP when the nodes are attempting to connect to foreign domains with Authentication, Authorization, and Accounting (AAA) servers. AAA servers today identify clients by using the Network Access Identifier (NAI)

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

Business Rule	Description	References
<i>A Digital Identity Standard registration and binding service will be provided for mobile devices and their user(s).</i>	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 identifier for a device.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 (page 408) ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Pages 20, 38)

Table 3.21 – Mobile Device Binding Business Rule

3.2.3.2.1 (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

3.2.3.2.2 (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 quickly and automatically unbind a user(s) from a device must be in place

3.2.3.2.3 (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 DoD Enterprise

- Registration and binding services may not operate reliably in mobile ‘disconnected’ and/or ‘network-disadvantaged’ environments (e.g., classified, tactical)

#### 3.2.3.2.4 (P3/R2) Technical Positions and Patterns

#### ➤ Core Standards

##### Technical

- IETF RFC 2794: Defines a way for the mobile node to identify itself by including the NAI along with the Mobile IP Registration Request. This memo also updates RFC 2290, which specifies the Mobile-IPv4 configuration option for Internet Protocol Control Protocol, by allowing the mobile node's home address field of this option to be zero

### 3.2.4 (P4) Principle 4 – Global Directory Electronic Mail (E-Mail) Services

Principle	Description	References
<i>The Enterprise Directory Service (DS) will allow users to find e-mail addresses and contact information for all DoD related personnel and organizations.</i>	The U.S. military forces, in essence, have one mission: protection of the United States of America. Therefore, 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 electronic mail services.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Page 17)

Table 3.22 – Global Directory E-Mail Service Principle

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

Business Rule	Description	References
<i>An enterprise level Directory Service (DS) shall provide the ability to disseminate the Enterprise Global Address List (GAL) views to DoD Component mail systems.</i>	The GAL is a directory service within a Simple Mail Transfer Protocol (SMTP) based email system that contains information for all email users, distribution groups, and Exchange Resources. By providing the GAL to all DoD Component mail systems, DoD email users will have an effective and efficient digital communications capability that is agnostic to the hardware and software being utilizing.	DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012

Table 3.23 – Global Access List (GAL) Distribution Business Rule

##### 3.2.4.1.1 (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 can include both DoD hosted and deployed SC tactical mail systems
- GAL address and contact information can be federated from the SC mail systems to the DoD Enterprise level GAL
- Dissemination of the Enterprise GAL for use by disparate mail systems is based on need-to-know access policies

##### 3.2.4.1.2 (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

##### 3.2.4.1.3 (P4/R1) Risk

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

3.2.4.1.4 (P4/R1) Technical Positions and Patterns

➤ Core Standards

Technical

- Data Encoding Specification for Intelligence Community (IC) Full Service Directory Schema V1.0: Defines detailed specifications for attributes that IC elements are expected to provide to the Intelligence Community Full Service Directory (IC FSD). Its function is to facilitate the availability, accuracy, and standardization of these attributes across the IC Top Secret/Sensitive Compartmented Information (TS/SCI) enterprise, building a consistent basis for capabilities including directory services, email functions, and attribute-based access control decisions

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

Business Rule	Description	References
<i>The DoD's Global Address List (GAL) must allow for segmented views by organization or operating unit.</i>	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 the NT-DSs and T-DSs for DoD organizational views, and could also provide SC-specific GAL views.	DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012

Table 3.24 – Global Access List (GAL) Organizational Views Business Rule

3.2.4.2.1 (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

3.2.4.2.2 (P4/R2) Constraints

- Organizations or 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

3.2.4.2.3 (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 DoD Enterprise services
- Loss of enterprise GAL and SC GAL view synchronization will result in access “gaps” within and among the SCs

3.2.4.2.4 (P4/R2) Technical Positions and Patterns

➤ Core Standards

Technical

- ACP 123 annexes: Contain standards profiles for the definition of the DMS Business Class Messaging (P772) capability and the Message Security Protocol (MSP). Organizational messaging is considered a high-assurance messaging service that requires authentication, delivery confirmation, and encryption

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

Business Rule	Description	References
<i>A Directory Service (DS) shall provide a common data schema to support a Global Address List (GAL) as well as segmented views of the GAL; where the GAL data schema is a subset of the total identity attribute data schema.</i>	DoD email users access the Enterprise Directory Service in multiple fashions (i.e....Outlook, BlackBerry, Webmail, etc.). Regardless of the device and application providing the GAL or GAL views, a common data schema of GAL information is required. NT-DS and T-DSs provide a common data schema, which is a selective set of attributes sourced from the enterprise attribute repository (i.e., EIADRSS).	DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012

Table 3.25 – Global Address List (GAL) Data Schema Business Rule

#### 3.2.4.3.1 (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
- Only authorized users will view information provided by the GAL

#### 3.2.4.3.2 (P4/R3) Constraints

- Applications the use the NT-DS and T-DSs, GAL, and GAL views and search services must have a Certification of Networkiness (CoN)
- Web services used by GAL/Gal view services must utilize a standard web service data protocol

#### 3.2.4.3.3 (P4/R3) Risk

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

#### 3.2.4.3.4 (P4/R3) Technical Positions and Patterns

##### ➤ Core Standards

##### Technical

- IETF RFC 2849: Specifies a set of directory entries, or a set of changes to be applied to directory entries, but not both. There is a one-to-one correlation between LDAP operations that modify directories and the types of change records described as "add", "delete", "modify", and "modrdn" or "moddn"

## 3.2.4.4 (P4/R4) Business Rule 4 – Offline Address Book Availability

Business Rule	Description	References
<i>An Offline Address Book (OAB) must be made available as required by the user.</i>	There are times when DoD email users will not have network access, but still require access to their DoD address book offline. Providing DoD email users with offline access to an instantiation of the GAL will enhance user productivity, regardless of network access challenges.	DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012

Table 3.26 – Offline Address Book Availability Business Rule

## 3.2.4.4.1 (P4/R4) Assumptions

- Both the DoD Enterprise and the user’s organizational or operating unit address book are accessible offline
- An offline address book will support access to address information both internal and external to the user’s organization or operating unit

## 3.2.4.4.2 (P4/R4) Constraints

- OABs shall be protected “at rest” and “in transit”, and must be distributed in a secure manner
- OAB information “at rest” must be encrypted
- OABs must not be made available to offline users who are not properly authenticated, locally, to any approved device

## 3.2.4.4.3 (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 with access to DoD personnel information

## 3.2.4.4.4 (P4/R4) Technical Positions and Patterns

## ➤ Core Standards

Technical

- ACP 123 annexes: This standard contains the standards-profiles for the definition of the Defense Message System (DMS) Business Class Messaging (P772) capability and the Message Security Protocol (MSP). Organizational messaging is considered a high-assurance messaging service that requires authentication, delivery confirmation, and encryption

## 3.2.4.5 (P4/R5) Business Rule 5 – Directory/Global Address List (GAL) Services Availability

Business Rule	Description	References
<p><i>A Directory Service (DS) shall provide all DoD e-mail users with access to all current and valid DoD E-mail user information from anywhere, at anytime, and from any authorized device, via a DoD Global Address List (GAL).</i></p>	<p>Because of the various environments and locations where DoD employees conduct business, users of the DoD Enterprise Directory Service do not always access their email accounts from the same area or digital environment. Fixed and Mobile devices, regardless of hardware/OS type, enable DoD authorized users with capabilities to access email from anywhere, at anytime, from any authorized device, enhancing the communications ability of all DoD email users.</p>	<p>Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Page 17) ----- DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012</p>

Table 3.27 – Directory/Global Address List (GAL) Services Availability Business Rule

## 3.2.4.5.1 (P4/R5) Assumptions

- An e-mail 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)
- User authentication is tied to information/network classification

## 3.2.4.5.2 (P4/R5) Constraints

- OABs must not be made available to offline users who are not properly authenticated, locally, to any approved device

## 3.2.4.5.3 (P4/R5) Risk

- Users of mobile devices may not always use the device in secure areas
- Users sometimes lose mobile devices
- Users may mistakenly transmit sensitive information on the DoD network
- Hardware used to access information may be operational in unsecure areas

## 3.2.4.5.4 (P4/R5) Technical Positions and Patterns

## ➤ Core Standards

Technical

- IETF RFC 1777: Is specifically targeted at simple management applications and browser applications that provide simple read/write interactive access to the X.500 Directory, and is intended to complement the Directory Access Protocol (DAP) itself
- IETF RFC 2605: This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. This memo supersedes RFC 1567, "X.500 Directory Monitoring MIB". This memo

- extends that specification to a more generic MIB for monitoring one or more directory servers each of which may support multiple access protocols
- IETF RFC 3673: Describes an LDAP extension that clients may use to request the return of all operational attributes. This standard extends the Lightweight Directory Access Protocol (LDAP) [RFC3377] to provide a simple mechanism which clients may use to request the return of all operational attributes

### 3.2.5 (P5) Principal 5 – Authentication and Authorization

Principle	Description	References
<i>Requesters will be granted access to logical and physical Resources based on who they are, where they are, and their assigned mission (i.e., mission roles, operational functions).</i>	Access decisions will require dynamic analysis of PE and NPE identity attributes that are 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.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Pages 27, 89)

Table 3.28 –Authentication and Authorization Principle

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

Business Rule	Description	References
<i>All DoD information services and applications must uniquely and persistently digitally identify and authenticate users and devices. These services, applications, and networks shall enforce authorized access to information and other services or devices according to specified access control rules and quality of protection requirements for all individuals, organizations, Communities of Interest (COIs), automated services, and devices.</i>	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 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 MS AD infrastructure, and other components such as the EASF and the AAF.	DoD Information Enterprise Architecture (IEA) Version 2.0 - Draft Vol. II, February 2012

Table 3.29 – Authentication and Authorization Scope Business Rule

##### 3.2.5.1.1 (P5/R1) Technical Positions and Patterns

#### ➤ Core Standards

##### Technical

- FIPS 201: Specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally-controlled government facilities and electronic access to government information systems
- IETF RFC 2865: Describes a protocol for carrying authentication, authorization, and configuration information between Network Access Servers that authenticate links through a shared Authentication Server
- IETF RFC 2845: Allows for transaction-level authentication using shared secrets and one way hashing. It can be used to authenticate dynamic updates as coming from an approved client, or to authenticate responses as coming from an approved recursive name server

- IETF RFC 4252: The Secure Shell Protocol (SSH) is a protocol for secure remote login and other secure network services over an insecure network. This document describes the SSH authentication protocol framework and public key, password, and host-based client authentication methods
- ITU-T X.509: Provides the foundation frameworks for (PKI) and Privilege Management Infrastructure (PMI). ITU X.509 frameworks include Infrastructure Models, Certificate and Certificate Revocation Lists (CRL), Attribute certificates, Directory Schema Definitions and Path Processing Procedures

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

Business Rule	Description	References
<i>An enterprise level Digital Identity Service for both PE (i.e., Persona) and NPE will include support for the tactical edge.</i>	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 the EIADRSS as an enterprise digital identity service, and further supported by an enterprise DS, and by NT-DSs at CONUS (Contiguous United States) base/post/camp/station, and by T-DSs in OCONUS (Outside the Contiguous United States) theatre. All other non-tactical and tactical, DoD Enterprise/Joint and SC IdAM components will be dependent on the receipt and consumption of this data, which applies to PE and NPE Requester identities as well as NPE Resource identity attribute data.	JIE POA&M, March 2012

Table 3.30 – Identity Service for the Tactical Edge Business Rule

#### 3.2.5.2.1 (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 credentials that are trusted to the appropriate internal DoD PE and NPE
- Coalition PE and NPE will not be issued DoD CACs

#### 3.2.5.2.2 (P5/R2) Constraints

- Digital identities at the tactical edge must be also 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

#### 3.2.5.2.3 (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 for unauthorized access to DoD information and physical Resources

- Theatre personas required to support tactical operations may change often enough that they must be maintained real-time or near real-time to assure that authorization is adequately accurate and reliable

### 3.2.5.3 (P5/R3) Business Rule 3 – Single DoD Authentication Service Model

Business Rule	Description	References
<p><i>The DoD Enterprise and the SCs will have a consistent authentication service model that is usable across the DoD Enterprise (non-tactical and tactical), regardless of the logical or physical Resources being requested, that will provide the authentication service as part of any Attribute-Based Access Control (ABAC)*.</i></p> <p>* Phase 1 of DISA’s implementation of the ABAC architecture was the <i>National Senior Leadership Decision Support System (NSLDSS)</i> pilot. DISA is evaluating the use of the existing <i>Metadata Registry (MDR)</i> as an interim policy store to supplement this NSLDSS architecture.</p>	<p>One uniform authentication service model and a corresponding infrastructure will be developed and deployed for all authentication services, and will replace the existing diverse legacy models such as the Army Knowledge Online (AKO) ‘Single Sign-On’. Many of these do not optimally support a secure policy-based authorization capability. This will be required to achieve both DoD and SC IT Resource consolidation objectives, as well expedite user requests for access to the appropriate DoD and SC logical and physical Resources.</p>	<p>DoD Information Enterprise Architecture (IEA) Version 2.0 - Draft Vol. II, February 2012</p>

Table 3.31 – Single DoD Authentication Service Model Business Rule

#### 3.2.5.3.1 (P5/R3) Assumptions

- A DS framework to support both the DoD Enterprise and SC levels is in place.
- DoD will implement authentication mechanisms that support non-MS Active Directory authentication service
- The user’s CAC, token, or other form of PIV is the source of any digital identity required to authenticate any Requester

#### 3.2.5.3.2 (P5/R3) Constraints

- An authentication service must always be available to the DoD Enterprise and SCs
- The authentication service must support both PE and NPE authentication
- The authentication service must allow for full portability of identity credentials (i.e., certificates) across the DoD Enterprise
- All PE and NPE Requesters must be identified by a set of non-ambiguous identity attributes across the DoD Enterprise
- All information and other NPE Resources must be identified by a set of non-ambiguous identity attributes across the DoD Enterprise
- All ABAC access Policies must have an identical structure and use non-ambiguous identity attributes to support an enterprise authorization service
- No Authorization will occur until after the proper level of Requester Authentication has been made

### 3.2.5.3.3 (P5/R3) Risk

- If the authentication service is not available to the authorization service at both the DoD Enterprise and SC levels, then Resources cannot be made available
- Separation of the ABAC components (i.e., PS, PDP, and PEP) through network connections can create access capability outages
- The effective transition to ABAC/RBAC will be highly dependent on the ability to translate and port the existing MS AD Group Policies and Profiles to the ABAC/RBAC's RE

### 3.2.5.4 (P5/R4) Business Rule 4 – Standard Attribute Model

Business Rule	Description	References
<i>A standard attribute model for DoD people, services, and property will be established, registered, and utilized to enable any Attribute-Based Access Control (ABAC).</i>	This includes defining a common set of agreed upon attributes as defined by Communities of Interest and establishing and publishing a standardized format for each agreed upon attribute.	DoD Information Enterprise Architecture (IEA) Version 2.0 - Draft Vol. II, February 2012

Table 3.32 – Standard Attribute Model Business Rule

### 3.2.5.4.1 (P5/R4) Technical Positions and Patterns

#### ➤ Core Standards

#### Technical

- DGIWG FACC: Is a comprehensive dictionary and coding scheme for feature types, feature attributes (properties or characteristics associated with features), and attribute values (domain of feature attributes)
- ANSI INCITS 385: Specifies definitions of photographic (environment, subject pose, focus, etc.) properties, digital image attributes, and a face interchange format for relevant applications, including human examination and computer automated face recognition
- ANSI/INCITS 378: Defines a method of representing fingerprint information using the concept of minutiae. Minutiae are key points located at the ending or division of the ridges in a fingerprint image that includes order and size of fields, presence of all required fields, adherence to range limits on values, and internal consistency (the number of single finger records must match the number of fingers, for example)
- DoD Biometrics IDD v5.0: The authoritative source for DoD biometrics data elements. It defines the data standards that are to be used when data are exchanged among DoD Biometric Systems. The IDD identifies the data elements exchanged across DoD biometric systems, establishes authoritative definitions for those data, and documents standards for them (for example, field size, character type and valid values)

## 3.2.5.5 (P5/R5) Business Rule 5 – Global Information Resource Access

Business Rule	Description	References
<i>The authentication service will support global access to systems, applications, files and data by Requesters anywhere, using any type of device.</i>	The DoD Enterprise must be capable of providing access to information and Resources from any device belonging to any Computing Environment (CE). This requires that devices and their users can be vetted for authentication and then authorized to connect any appropriate requested information resource from any location.	JIE POA&M, March 2012

Table 3.33 – Global Information Resource Access Business Rule

## 3.2.5.5.1 (P5/R5) Assumptions

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

## 3.2.5.5.2 (P5/R5) Constraints

- Requester re-authentication is required when a “disconnected” and/or “network-disadvantaged” (e.g., classified, tactical environments) device is reconnected to any network or network-based Resource

## 3.2.5.5.3 (P5/R5) Technical Positions and Patterns

## ➤ Core Standards

Technical

- ISO/IEC 7816-11:2004: Specifies the use of inter-industry commands and data objects related to personal verification through biometric methods in integrated circuit cards. The inter-industry commands used are defined in ISO/IEC 7816-4. The data objects are partially defined in this International Standard, and partially imported from ISO/IEC 19785-1. ISO/IEC 7816-11 also presents examples for enrollment and verification, and addresses security issues

## 3.2.5.6 (P5/R6) Business Rule 6 – Access Policy Management Model

Business Rule	Description	References
<p><i>The DoD Enterprise and the SCs will have a consistent model for a policy management service consisting of a Rules Engine (RE), of which a major component is a Policy Store,(PS) as part of any Attribute-Based Access Control(ABAC).</i></p>	<p>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 (AAF) to access DoD and/or SC Resources (networks, information &amp; facilities). The RE is responsible for managing user access permissions. The RE consists of three sub-services: 1) Policy Enforcement Point (PEP), 2) Policy Decision Point (PDP), and 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.</p>	<p>Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Page 15)</p>

Table 3.34 – Access Policy Management Model Business Rule

## 3.2.5.6.1 (P5/R6) Assumptions

- The ABAC authentication service will support ABAC/RBAC 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 them real-time or near real-time
- A PS can be a set of complete policies, including all pertinent identity attribute data that is always imbedded in them

## 3.2.5.6.2 (P5/R6) Constraints

- The RE and PS that reside in the DoD IdAM Enterprise Service's ABAC Service must use common syntax
- A PS will function normally, optimally and securely if and only if real-time or near real-time attribute data is available to the policy templates
- When the ABAC Service is not available, users must not be authorized to access DoD networks and information Resources
- The DoD IdAM Enterprise Service's ABAC Service must use eXtensible Access Control Markup Language (XAMCL) wherever possible to define the policies that govern DoD information Resources

## 3.2.5.6.3 (P5/R6) Risk

- Non-virtual DoD IdAM ABAC infrastructure can be a single point of failure for all users of DoD information Resources

### 3.2.5.6.4 (P5/R6) Technical Positions and Patterns

#### ➤ Core Standards

##### Technical

- **XACML**: Defines three top-level policy elements: Business Rule, Policy and Policy Set. The Business Rule contains a Boolean expression that can be evaluated in isolation, but that is not intended to be accessed in isolation by a PDP. The Boolean expression is not intended to form the basis of an authorization decision by itself. It is intended to exist in isolation only within an XACML PDP, where it may form the basic unit of management, and be re-used in multiple policies

### 3.2.5.7 (P5/R7) Business Rule 7 – Access Policy Security

<b>Business Rule</b>	<b>Description</b>	<b>References</b>
<i>The Policy Store (PS) shall be protected in the same manner as the identity Attributes Data Repository (ADR) and a Policy Decision Point (PDP) shall have read-only access to the identity Attributes Data Repository (ADR) and the Policy Store (PS).</i>	Limiting the transport, replication, and remote storage of identity attribute data will minimize the possibilities for its compromise. Authorization components in any IdAM architecture must minimize the exposure of this data to the greatest extent possible.	DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012

Table 3.35 – Access Policy Security Business Rule

### 3.2.5.8 (P5/R8) Business Rule 8 – Attribute Access

<b>Business Rule</b>	<b>Description</b>	<b>References</b>
<i>Should it be operationally appropriate to distribute all or part of the Attributes Data Repository (ADR) and/or the Policy (PS), only the Rules Engine (RE) shall have access to either of these at any point in time.</i>	Authorization components in any IdAM architecture must minimize the exposure of this data to the greatest extent possible. 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).	DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012

Table 3.36 – Attribute Access Business Rule

#### 3.2.5.8.1 (P5/R8) Assumptions

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

### 3.2.5.9 (P5/R9) Business Rule 9 – DoD and Service Component (SC) Single Sign-On Service (SSOS) and Reduced Sign-On Service (RSOS) Restriction

Business Rule	Description	References
<i>The DoD and SCs must not continue to use existing legacy Single Sign-On Services (SSOS), Reduced Sign-On Services (RSOS), and their infrastructures for authentication and authorization to information Resources, and must be integrated into a configurable DoD Enterprise service wherever possible.</i>	The perpetuation of “stove-piped” mechanisms across the DoD Enterprise 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 constraint, and provide the capability to both non-tactical and tactical DoD Enterprise and SC Resources.	DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012

Table 3.37 – DoD and Service Component (SC) Single Sign-On (SSOS) and Reduced Sign-On (RSOS) Restriction Business Rule

#### 3.2.5.9.1 (P5/R9) 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 or DoD/DISA
- The Army Google Docs services will be supported by this DoD Enterprise capability.
- Future Web Apps that are not PKI-ready will be supported by this DoD Enterprise capability

### 3.2.5.10 (P5/R10) Business Rule 10 – Attribute Based Access Control (ABAC) Authorization Service

Business Rule	Description	References
<i>The Authorization Service shall provide Attribute-Based Access Control (ABAC) capabilities.</i>	Persona-based, policy-based, dynamic, and other access control mechanisms involve the use of identity attributes. The more granular the attribute data, the more precise the associated Policies may be, thus enabling a greater degree of authorization control.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Pages 13, 88,-89, 96)

Table 3.38 – Attribute Based Access Control (ABAC) Authorization Service Business Rule

### 3.2.6 (P6) Principle 6 – Dynamic Access Control

Principle	Description	References
<i>Access decisions will be dynamically configurable to support changing mission needs, attack response, and level of information service and networking resource availability, with all access decisions based on both Authentication and Authorization processes.</i>	Dynamic Access Control must provide a flexible and robust decision and enforcement mechanism to accommodate changes in the 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.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Pages 15-15, 26-28, 87)

Table 3.39 – Dynamic Access Control Principle

#### 3.2.6.1 (P6/R1) Business Rule 1 – Policy Management

Business Rule	Description	References
<i>IdAM services will offer a policy management service consisting of a Policy Engine(PE) and repository that can be modified/updated to accommodate both changes in identity attributes and related Persona, and attributes of the Resources for which access is being requested.</i>	To provide secure, timely control and access to all Resources, accurate, reliable, and timely information about the Resources, users, and devices is required. Pairing this information results in the creation of rules/policies that define what attributes a Requester must have in order to access a particular resource. The <i>Policy Decision Point (PDP)</i> identifies the relevant access policies, and provides direction based on those policies back to a <i>Policy Enforcement Point (PEP)</i> , where an authorization protocol is executed to either permit or deny an access request.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Pages 15, 29-30) ----- DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012

Table 3.40 – Policy Management Business Rule

##### 3.2.6.1.1 (P6/R1) Assumptions

- The authentication service will be based on identity attributes that are made available by the EIADRSS
- 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

3.2.6.2 (P6/R2) Business Rule 2 – Policy Change Management

Business Rule	Description	References
<p><i>The responsible owner of any access-controlled resource/system will have the ability to request new and/or modified access policies.</i></p>	<p>Resource owners are responsible for identifying and tagging their information Resources (all levels) as a major enabler of Attribute-Based Access Control (ABAC) policies. A Resource is defined as a digital object, information service or repository, a facility or other NPE that is made accessible to any Requester.</p>	<p>Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Page 27) ----- DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012, (Page 9)</p>

Table 3.41 – Policy Change Management Business Rule

3.2.6.2.1 (P6/R2) Assumptions

- A common DoD information Resource portal service will use all Resource access Policies that have been created and are being maintained for them

3.2.6.2.2 (P6/R2) Constraints

- Policy changes to SC Resources that are to be available to the DoD Enterprise must not be directly managed by the SC
- Policy template, structures, and syntax must be identical across the DoD Enterprise
- All access Policies must be in compliance with Federal laws and DoD guidance, as well as SC Regulations

3.2.6.2.3 (P6/R2) 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

3.2.6.3 (P6/R3) Business Rule 3 – Policy Attribute Validation

Business Rule	Description	References
<p><i>The policy decision process shall return an appropriate trusted token to the requesting Policy Enforcement Point (PEP) to permit the access authorization, only if all identity attributes and attribute data are determined to be consistent and valid within the Policy Store (PS).</i></p>	<p>Policy decisions must based on valid and current policies. Before an access policy is fully executed and authorization controls are applied, attributes utilized in the policy execution must be affirmed, as well as the basic structure, taxonomy, and language of the policies themselves. Only when validated can the appropriate secure tokens be created and passed to the proper Authorization (i.e., connection) service.</p>	<p>DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012</p>

Table 3.42 – Policy Attribute Validation Rule

#### 3.2.6.3.1 (P6/R3) 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

#### 3.2.6.3.2 (P6/R3) Constraints

- Coalition PE and NPE must not be issued DoD CACs, and 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

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

Principle	Description	References
<i>All authorized entities, using approved devices, will have timely access to and sharing of critical data, information, services, and applications from anywhere in the DoD information enterprise.</i>	Information resource access can only be made available to computing/communications devices used within the DoD Enterprise 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 though both authentication and authorization services.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Page 29)

Table 3.43 – Access to Data, Services and Applications Principle

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

Business Rule	Description	References
<i>Secure access to DoD information Resources will include systems, databases, applications/services, files, data queries, and granular data elements.</i>	Both PE and NPE will require access to information/data provided by multiple resource types. This will range from systems that support one or more applications, databases, files and data, to individual applications, software and networking service instances, to 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 that they require.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Page 41)

Table 3.44 – Information Resource Types Business Rule

##### 3.2.7.1.1 (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

##### 3.2.7.1.2 (P7/R1) Constraints

- Every information system/device (as a 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 (ESN)*)
- Access to information Resources must be dictated by a managed and automated set of security policies

##### 3.2.7.1.3 (P7/R1) Risk

- Changes in information resource attributes that are not conveyed either real-time or near real-time to the PE, PDP and PEP mechanisms may impact authorization requests

- Portability of information Resources across the DoD Enterprise requires careful management of their attributes and associated access polices

3.2.7.2 (P7/R2) Business Rule 2 – Public Key Infrastructure (PKI) Based Authentication

Business Rule	Description	References
<p><i>The Authentication Service will provide Public Key Infrastructure cryptographic-based Authentication to all systems, databases, applications/services, files, data queries, and granular data elements.</i></p>	<p>Verifiable PKI-based credentials issued by the DoD in the form of CACs and other “hard” tokens (e.g., SIPRNET token smart cards) must be made available to every PE that 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 can be 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.</p>	<p>Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Pages 21, 47) ----- DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012</p>

Table 3.45 – Public Key Infrastructure (PKI) Based Authentication Business Rule

3.2.7.2.1 (P7/R2) Assumptions

- X.509 certificate management service is available at all times

3.2.7.2.2 (P7/R2) Constraints

- PKI transactions will be transported across network boundaries encapsulated in SAML tokens for WS-protocols
- Kerberos, SSAPI, and SSL/TLS protocols and their secure transport will be used when SAML/WS cannot

3.2.7.2.3 (P7/R2) Risk

- An unauthorized user or malicious hacker may attempt to hijack a Security Assertion Markup Language (SAML) token and replay it to gain illicit access to DoD information Resources (i.e., a Replay Attack)

3.2.7.3 (P7/R3) Business Rule 3 – Data Tagging

Business Rule	Description	References
<p><i>Data owners must tag data to enforce access control policies for all information Resources within the DoD Enterprise.</i></p>	<p>The DoD Enterprise must migrate to tagging all applications or standalone data at rest. The DoD applications/software development and COTS procurement organizations must begin building their information services and Programs of Record (PORs) using a standardized XML-based resource/data tagging methodology, taxonomy. Legacy information Resources must be analyzed to see if this migration can be executed or if their data and services should be consolidated to an environment where the 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 (ADR) and/or the Policy Store (PS).</p>	<p>Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Pages 31, 50) ----- DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012</p>

Table 3.46 – Data Tagging Business Rule

3.2.7.3.1 (P7/R3) Assumptions

- Data tagging is standardized for all DoD Enterprise information Resources
- Data tagging is XML based, and conforms to a standard metadata schema

3.2.7.3.2 (P7/R3) Constraints

- Data tagging must conform to approved DoD (i.e., DoD IT Standards Registry (DISR)) standards
- The DoD Enterprise ABAC Service 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 identifies information Resources (e.g., In an ABAC/RBAC PS with NPE Resource attribute data provided by the EIADRSS)

3.2.7.3.3 (P7/R3) Risk

- Without regular auditing to assure the consistency of data tags at both the DoD Enterprise and SC levels, Resources will not be correctly identified and the authorization Policies cannot be executed correctly
- Failure to synchronize data tags in all ADR may prevent authorized Resource access or allow unauthorized Resource access to Resources

3.2.7.3.4 (P7/R3) Technical Positions and Patterns

➤ Core Standards

Policy/Regulatory

- DoDD 8320.02: Specifies that data assets shall be made visible by creating and associating metadata (“tagging”), including discovery metadata, for each asset. Discovery metadata shall conform to the Department of Defense Discovery Metadata Specification (reference (d)). DoD metadata standards shall comply with applicable national and international consensus standards for metadata exchange whenever possible. All metadata shall be discoverable, searchable, and retrievable using DoD-wide capabilities
- DoDD 8320.03: Provides joint policy and guidance for Information Assurance (IA) and computer network defense (CND) operations in accordance with (IAW) references. The DOD CND mission is to coordinate and direct the defense operations of DoD computer networks from unauthorized activity, by employing communications, law enforcement, counterintelligence and Intelligence Community (IC) capabilities in response to specific or potential threats. The Commander, United States Strategic Command (CDRUS-STRATCOM) coordinates and directs DOD-wide CND

3.2.7.4 (P7/R4) Business Rule 4 – Policy Store (PS) Personally Identifiable Information (PII) Attribute Exposure

Business Rule	Description	References
<i>The Policy Store (PS) will not store or retain Personally Identifiable Information (PII) attribute data, if the PS, the Attribute Data Repository (ADR), and the Policy Decision Point (PDP) are not co-located and integrated components of the Rules Engine” (RE).</i>	When the Policy Store (PS) is not a co-located component of a 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 decision.	DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012

Table 3.47 – Policy Store (PS) Personally Identifiable Information (PII) Attribute Exposure Business Rule

3.2.7.4.1 (P7/R4) Assumptions

- If the PS is not co-located with the RE, Requester PII data will be required to transit a network in order to be consumed by a RE
- The EIADRSS contains all Authoritative PII attribute data
- The PDP will render decisions based on the same PII attribute data that is used by the DoD Enterprise AAF and SSOS

3.2.7.4.2 (P7/R4) Constraints

- 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 is 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

3.2.7.4.3 (P7/R4) Risk

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

3.2.7.4.4 (P7/R4) Technical Positions and Patterns

➤ Core Standards

Technical

- XACML: Defines three top-level policy elements: Business Rule, Policy, and Policy Set. The Business Rule contains a Boolean expression that can be evaluated in isolation, but that is not intended to be accessed in isolation by a PDP. The Boolean expression is not intended to form the basis of an authorization decision by itself. It is intended to exist in isolation only within an XACML PAP, where it may form the basic unit of management, and be re-used in multiple policies

3.2.7.5 (P7/R5) Business Rule 5 – Policy Decision Point (PDP) Personally Identifiable Information (PII) Attribute Data Exposure

Business Rule	Description	References
<p><i>The Policy Decision Point (PDP) will not store or retain Personally Identifiable Information (PII) attribute data, if the PS, the Attribute Data Repository (ADR), and the Policy Decision Point (PDP) are not co-located and integrated components of the RE.</i></p>	<p>Similar to the PS PII Data Exposure Business Rule, this rule establishes that the PDP must also 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 this data. This eliminates one additional possible point of PII exposure and compromise across DoD networks.</p>	<p>DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012</p>

Table 3.48 – Policy Decision Point (PDP) Personally Identifiable Information (PII) Attribute Data Exposure Business Rule

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

Business Rule	Description	References
<p><i>Where possible, identity attribute data at rest and in transit across the DoD Enterprise must conform to guidelines to reduce storage and network transport overhead, and must be developed using a common Software Development Kit (SDK).</i></p>	<p>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 Identity Attribute Data Repository (ADR) and/or the Policy Store (PS). Data tagging guidelines must be developed to establish limits as to what data at what level must be tagged, to reduce network transport requirements, as well as the complexity of storage and management of information Resources.</p>	<p>Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Pages 31, 50). ----- DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012</p>

Table 3.49 – Data Tagging Development Business Rule

3.2.7.6.1 (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

3.2.7.6.2 (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 an ABAC PS with the EIADRSS
- All Services Components will use a common SDK
- All SCs must use the same standards schema and syntax

3.2.7.6.3 (P7/R6) Risk

- Without regular auditing to assure the consistency of data tags, at both the DoD Enterprise and SC levels, Resources will not be correctly identified and the authorization policies cannot be executed correctly
- Failure to synchronize data tags in all ADRs may prevent authorized Resource access or allow unauthorized Resource access to Resources
- Unless data tagging is protected at 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”

## 3.2.7.7 (P7/R7) Business Rule 7 – Standardized Policy Language

Business Rule	Description	References
<i>Systems, applications, and/or data asset owners will be responsible for creating and maintaining XACML-based Policies required for secure access to the greatest extent possible and/or outline and then implement an XACML migration plan.</i>	XACML is a current standard access policy rules markup language, and should be used for all new DoD systems/applications access wherever possible. If current DoD Authorization services such as within MS 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 assure interoperability with legacy information Resources.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012

Table 3.50 – Standardized Policy Language Business Rule

## 3.2.7.7.1 (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

## 3.2.7.7.2 (P7/R7) Constraints

- All SC-originated Policies must be federated to the DoD level, and approved as DoD enterprise access policies before being activated/utilized
- XACML-based access Policies must use a common syntax schema
- Incorrectly created XACML-based access Policies will result in a denial of access

## 3.2.8 (P8) Principle 8 – Physical Access

Principle	Description	References
<i>All authorized entities will have timely access to physical facilities and assets anywhere in the DoD environment.</i>	All PEs will require access to DoD installations and facilities to perform their mission functions. This ranges from Post/Camp/Station to deployed tactical environments. Access policies must control who gains access to what, and be able to revoke this access as required.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Pages 39-41)

Table 3.51 – Physical Access Principle

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

Business Rule	Description	References
<i>To establish an enduring index for all other attributes related to any Resource, a unique identifier that can be established in an Attribute Data Repository (ADR) that the authentication and authorization services can use to grant or deny access will be required to identify all NPE.</i>	A unique identifier will be required to identify all NPE that can be established in the EIADRSS that the authentication and authorization services will use to grant or deny access. 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.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition (Pages 39-41)

Table 3.52 – Non-Person Entity (NPE) Unique Identifier Business Rule

## 3.2.8.2 (P8/R2) Business Rule 2 – Access Control Policy

Business Rule	Description	References
<i>Physical access to facilities and other NPE assets will be enforced by access control policies across the DoD Enterprise.</i>	Similar to access Policies related to information Resources, access Policies that define who gains access to what facility, equipment, or any other physical NPE will be required.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Pages 39-41)

Table 3.53 – Access Control Policy Business Rule

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

<b>Business Rule</b>	<b>Description</b>	<b>References</b>
<i>Continuing certification and verification of physical assets identification attributes will be maintained.</i>	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, ordinance and other physical DoD assets.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Pages 39-41)

Table 3.54 – Non-Person Entity (NPE) Attribute Verification Business Rule

## 3.2.8.4 (P8/R4) Business Rule 4 – Non-Person Entity (NPE) Attribute and Policy Management

<b>Business Rule</b>	<b>Description</b>	<b>References</b>
<i>Owners of physical facilities and assets will be responsible for maintaining the required identity attributes, and must create and publish the applicable rules for access based on a standard structure and taxonomy.</i>	The responsibility of correctly identifying all NPE will be responsibility of 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.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0 – December, 2011 ----- Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012 (Pages 39-41)

Table 3.55 – Non-Person Entity (NPE) Attribute and Policy Management Business Rule

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

<b>Business Rule</b>	<b>Description</b>	<b>References</b>
<i>The principal credential mechanism for identity authentication to allow access to any physical facility or asset will be the Common Access Card (CAC)-DoD PIV Credential.</i>	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 therefore support multiple physical access systems, but the desired environment should be that of 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.	Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012

Table 3.56 – Common Access Card (CAC) Credential Mechanism Business Rule

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

<b>Business Rule</b>	<b>Description</b>	<b>References</b>
<i>For physical access, credential validation must be supported by visual inspection of a CAC, enrolling the CAC in a local access control system, or issuance of a separate card associated with a local physical access system.</i>	If physical access authorization cannot be provided adequately for given environments (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.	Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012

Table 3.57 – Common Access Card (CAC) Enrollment Business Rule

### 3.2.9 (P9) Principle 9 – General Identity and Access Management (IdAM) Security Policy

Principle	Description	References
<i>A comprehensive security policy will be developed that addresses all aspects of Identity Management, Authentication and Authorization services, and provides for realistic opportunities to enforce the greater Information Assurance (IA) policy requirements aimed at reducing the threat from both internal and external DoD Enterprise entities.</i>	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 them. Many overarching IA standards will also be applicable (e.g., authentication mechanism transport, cross domain capabilities, and information classification restrictions).	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance Version 2.0 December 2, 2011

Table 3.58 – General Identity and Access Management (IdAM) Security Policy Principle

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

Business Rule	Description	References
<i>Digital identity data will be validated by the network and the systems to ensure it conforms to relevant schema and business rules.</i>	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 is employed, that can be verified/re-verified on both a scheduled and ad-hoc basis as required. This capability is essential to ensuring that the Authorization service executes effectively and securely.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance Version 2.0 December 2, 2011

Table 3.59 – Identity Attribute Data Validation Business Rule

#### 3.2.9.2 (P9/R2) Business Rule 2 – DoD Authorization Service

Business Rule	Description	References
<i>An Authorization Service must be provided for the DoD Enterprise that supports access to DoD Enterprise applications and other information Resources.</i>	To ensure that the correct users of the DoD Enterprise level information Resources (e.g., Enterprise E-mail) 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 DoD Enterprise.	DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012

Table 3.60 – DoD Authorization Service Business Rule

### 3.2.9.2.1 Technical Positions and Patterns

#### ➤ Core Standards

##### Technical

- SP 800-122: Assists Federal agencies in protecting the confidentiality of a specific category of data commonly known as PII. This document provides practical, context-based guidance for identifying PII and determining what level of protection is appropriate for each instance of PII

##### Policy/Regulatory

- DoDI 8520.03: Provides that the information system or DoD network shall ensure that any credential used for identity authentication is appropriate for the authenticating entity's environment or physical location and the sensitivity level of the information or force protection level of the facility or other Resources for which the information system facilitates access or privilege

### 3.2.9.3 (P9/R3) Business Rule 3 – Information Resources Authorization

<b>Business Rule</b>	<b>Description</b>	<b>References</b>
<i>DoD Service Components' (SC) users of applications and other information Resources must use an Authorization Service for access control.</i>	Each DoD SC has common and unique computing and information Resources that users require access to. To ensure that the correct SC users of SC information Resources (e.g., <i>Army - Enhanced Position Location and Reporting System (EPLRS)</i> , <i>Army – Advanced Forward Area Tactical Data System (AFATDS)</i> ) 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 within an SC.	DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012

Table 3.61 – Information Resources Authorization Business Rule

### 3.2.9.3.1 (P9/R3) Technical Positions and Patterns

#### ➤ Core Standards

##### Policy/Regulatory

- DoDI 8510.01: Establishes a Certification and Accreditation (C&A) process to manage the implementation of IA capabilities and services and provide visibility of accreditation decisions regarding the operation of DoD ISs, including core enterprise services- based and Web services-based software systems and applications

## 3.2.9.4 (P9/R4) Business Rule 4 – Enterprise Information Sharing

Business Rule	Description	References
<i>All DoD services that enable the sharing or transfer of information across multiple security levels shall be centrally planned and coordinated, with proposed service enhancements considered first at the enterprise-wide level, then at the regional/organizational level (e.g., DoD Component), and finally at the service or application level.</i>	To ensure that DoD Enterprise information Resources handle the transmission of data over its 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.	DoD Information Enterprise Architecture (IEA) Version 2.0 - Draft Vol. II, February 2012

Table 3.62 – Enterprise Information Sharing Business Rule

## 3.2.9.4.1 (P9/R4) Technical Positions and Patterns

## ➤ Core Standards

Policy/Regulatory

- NSPD-59/HSPD-24: Establishes a framework to ensure that Federal executive departments and agencies use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of individuals' biometric and associated biographic and contextual information in a lawful and appropriate manner, while respecting their information privacy and other legal rights under United States law

## 3.2.9.5 (P9/R5) Business Rule 5 – Information Resource Authentication Frequency

Business Rule	Description	References
<i>All DoD applications and networks shall enforce authorized access to information and other services or devices, and must uniquely and persistently digitally identify and authenticate users and devices according to specified access control policies, while imposing quality of protection requirements for all individuals, organizations, COIs, automated services, and devices.</i>	Protection of the DoD Enterprise 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 within a reasonable period of inactivity or when network connectivity is not available.	DoD Information Enterprise Architecture (IEA) Version 2.0 - Draft Vol. II, February 2012

Table 3.63 – Information Resource Authentication Frequency Business Rule

## 3.2.9.5.1 (P9/R5) Technical Positions and Patterns

## ➤ Core Standards

Technical

- WS – Security 1.1: Is flexible and is designed to be used as the basis for securing Web services within a wide variety of security models including PKI, Kerberos, and SSL (Secure Socket Layer). Specifically, this specification provides support for multiple security token formats, multiple trust domains, multiple signature formats, and multiple encryption technologies

- SAML 2.0: Is an industry standard for web SSO and web services authentication, attribute exchange, and authorization. SAML-based federation is the basis for Level 1 and Level 2 authentication under the E-Authentication framework

### 3.2.9.6 (P9/R6) Business Rule 6 – Cross Domain Security

Business Rule	Description	References
<i>Enterprise-level directory services will preserve cross domain security while satisfying authentication and authorization requests.</i>	Currently, the DoD Enterprise is comprised of numerous heterogeneous security enclaves that exist within and across all DoD networks (e.g., <i>NIPRNET</i> , <i>SIPRNET</i> , and the <i>Joint Worldwide Intelligence Communications System (JWICS)</i> ). 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.	DoD Information Enterprise Architecture (IEA) Version 2.0 - Draft Vol. II, February 2012

Table 3.64 – Cross Domain Security Business Rule

#### 3.2.9.6.1 (P9/R6) Assumptions

- For WS-Federation services, all cross-domain SAML token transfers, in-band and out-of-band will be supported

### 3.2.9.7 (P9/R7) Business Rule 7 – Information Resources Availability

Business Rule	Description	References
<i>DoD Information Resources, including data assets, services, and applications shall be accessible to all authorized users in the DoD, and accessible except where limited by law, policy, security classification, or operational necessity.</i>	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 Enterprise 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 DoD Enterprise from potential enemies attempting to access and steal sensitive information, as well as damage key infrastructure components.	DoD Information Enterprise Architecture (IEA) Version 2.0 - Draft Vol. II, February 2012

Table 3.65 – Information Resources Availability Business Rule

## 3.2.9.8 (P9/R8) Business Rule 8 – Information/Data Resources Protection

Business Rule	Description	References
<i>DoD information programs, applications, and computer networks shall protect data in transit and at rest according to their confidentiality level, Mission Assurance category, and level of exposure using authentication, authorization, and encryption services.</i>	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 it is 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.	DoD Information Enterprise Architecture (IEA) Version 2.0 - Draft Vol. II, February 2012

Table 3.66 – Information/Data Resources Protection Business Rule

## 3.2.9.8.1 (P9/R8) Technical Positions and Patterns

## ➤ Core Standards

Policy/Regulatory

- DoD CJCSI 6510: Provides joint policy and guidance for IA and Computer Network Defense (CND) operations in accordance with Information Assurance Workshop (IAW) references. The DoD CND mission is to coordinate and direct the defense operations of DoD computer networks from unauthorized activity by employing communications, law enforcement, counterintelligence, and IC capabilities in response to specific or potential threats. The Commander, United States Strategic Command (CDRUSSTRATCOM) coordinates and directs DOD-wide CND
- DoDD 1000.25: Establishes policy and assigns responsibility under the DoD Personnel Identity Protection (PIP) Program. The PIP shall be the Department of Defense's program for: addressing threats to the individual personal privacy of its Members, employees, and beneficiaries; establishing a secure and authoritative process for the issuance and use of identity credentials in the Department of Defense; and ensuring that DoD benefits and access to DoD physical and logical assets are granted based on authenticated and secure identity information
- DoDD 8500.01E: All DoD information systems shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that reflect a balance among the importance and sensitivity of the information and information assets; documented threats and vulnerabilities; the trustworthiness of users and interconnecting systems; the impact of impairment or destruction to the DoD information system; and cost effectiveness

## 3.2.9.9 (P9/R9) Business Rule 9 – DoD Enterprise Trust Management

Business Rule	Description	References
<i>Policy will be established and enforced to provide common identity management and authentication processes across DoD in accordance with Federal guidance and direction, addressing trust negotiation between DoD components and mission partners for providing assured access to all authorized entities.</i>	In order to accomplish a cohesive and interoperable information resource-sharing environment, the DoD must develop a policy that directs all DoD organizations to employ a common identity authentication processes. 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.	DoD Information Enterprise Architecture (IEA) Version 2.0 - Draft Vol. II, February 2012

Table 3.67 – DoD Enterprise Trust Management Business Rule

## 3.2.9.10 (P9/R10) Business Rule 10 – Enterprise DoD Network Domain

Business Rule	Description	References
<i>Provide a single, secure, and consolidated network domain.</i>	Providing a single, secure, consolidated network, that utilizes common standards, technologies and processes, ensures that access security is consistent across the DoD Enterprise, regardless of what network component (e.g., NIPRNET, SIPRNET, JWICS) is involved.	DoD Information Enterprise Architecture (IEA) Version 2.0 - Draft Vol. II, February 2012

Table 3.68 – Enterprise DoD Network Domain Business Rule

## 3.2.9.10.1(P9/R10) Technical Positions and Patterns

## ➤ Core Standards

Technical

- ANSI/SIA OSIPS-IDM: 200x describes identities and carrier claims of identity that are authenticated by comparing reference authentication factors with presented credentials

## 3.2.9.11 (P9/R11) Business Rule 11 – Alternate Authentication Mechanisms (Non-CAC/Token)

Business Rule	Description	References
<i>Alternate authentication mechanisms must be provided for all non-CAC and other hard token-based user access.</i>	CAC-PKI “only” authentication to network services, which includes content delivery systems, hampers soldiers, Leaders, Civilians, and Contractors from accessing training and education content at the point of need. Further, non-CAC eligible populations such as the Individual Ready Reserve, ROCT Cadets, New Recruits, State Agency Partners, First Responders, and verified family members cannot access applications that require PKI –based authentication.	DoD Information Enterprise Architecture (IEA) Version 2.0 - Draft Vol. II, February 2012

Table 3.69 – Alternate Authentication Mechanisms (Non-CAC/Token) Business Rule

### 3.2.9.11.1 (P9/R11) 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

### 3.2.9.12 (P9/R12) Business Rule 12 – Data Encryption

Business Rule	Description	References
<i>Digital Identity will use encryption methods to ensure data integrity and protection of sensitive or regulated information (e.g., PII), and assure protection of authentication data transport.</i>	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 (RE) components, along with securing the network infrastructure itself, is required.	Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance Version 2.0 December 2, 2011

Table 3.70 – Data Encryption Business Rule

### 3.2.9.12.1 (P9/R12) Technical Positions and Patterns

#### ➤ Core Standards

#### Technical

- FIPS PUB -197: The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plaintext

### 3.2.9.13 (P9/R13) Business Rule 13 – SHA-256: Secure Hashing Algorithm Migration

Business Rule	Description	References
<i>All new information systems and Enterprise IdAM infrastructure components will implement the Secure Hash Algorithm (SHA)-256 encryption algorithm where possible, or must develop a plan to migrate all systems supported by PKI to SHA-256.</i>	The SHA is one of a number of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS). SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512) designed by the National Security Agency (NSA). 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.	DoD CIO Memo, <i>DoD's Migration to Use of Stronger Encryption Algorithms</i> , 14 October, 2010

Table 3.71 – SHA-256 Encryption Migration Business Rule

### 3.2.9.13.1(P9/R13) Technical Positions and Patterns

#### ➤ Core Standards

##### Technical

- FIPS 180-3: Is used to detect whether message have been changed since the digests were generated. When a message is of any length (less than) 2<sup>64</sup> BITS (SHA-256) the result is an output called a message digest. Secure hash algorithms are typically used with other cryptographic algorithm, such as digital algorithm and keyed-hash message authentication codes
- OASIS SAML 2.0: Defines the syntax and semantics for XML-encoded assertions about authentication, attributes and authorization, and for the protocol that conveys this information. The specifications define the syntax and semantics for XML-encoded SAML assertions, protocol requests, and protocol responses

### 3.2.10 (P10) Principle 10 – Single Sign-On (SSO) and Reduced Sign-On (RSO)

Principle	Description	References
<i>The identity and access management services will provide network administrators and users with a single sign-on (SSO) and reduced-sign-on (RSO) access framework to required information and services, regardless of location, through standardized identities and access mechanisms.</i>	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, 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 where the Requester does not have to possess a “hard” digital identity credential (e.g., CAC, token smart card).	DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012, <i>FICAM Roadmap version 2.0</i>

Table 3.72 – Single Sign-On (SSO) and Reduced Sign-On (RSO) Principle

#### 3.2.10.1 (P10/R1) Business Rule 1 – Service Component (SC) Directory Data Population

Business Rule	Description	References
<i>Identity information used by a Service Component (SC) will be automatically populated from a DoD Enterprise Directory Service.</i>	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 (SOAP) call, web service “pull” or “push”).	DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012, <i>FICAM Roadmap version 2.0</i>

Table 3.73 – Enterprise Directory Service Data Population Business Rule

##### 3.2.10.1.1 (P10/R1) Assumptions

- The 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

##### 3.2.10.1.2 (P10/R1) Constraints

- Identity records are enduring, unless deactivated or deleted based upon an administrative decision and action

##### 3.2.10.1.3 (P10/R1) Risk

- The quality of SC-level directory service concurrency must depend on the combined level of latency of all identity information passing from the DoD authoritative data sources to the NT-DSs and T-DSs
- The quality of SC level directory services must largely depend on the ability of the SCs to maintain current views of user/Requester addresses

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

<b>Business Rule</b>	<b>Description</b>	<b>References</b>
<i>An Electronic Data Interchange Personal Identifier (EDI-PI) will be uniquely tied to a unique PE in the form of a standardized DoD DMDC-formatted enterprise User Name, or using a DoD Enterprise E-mail Display Name format.</i>	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.	DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012

**Table 3.74 – Electronic Data Interchange Personal Identifier (EDI-PI) Rendering Business Rule**

### 3.2.10.3 (P10/R3) Business Rule 3 – Directory Information Updates

<b>Business Rule</b>	<b>Description</b>	<b>References</b>
<i>DoD Business Systems, and DoD personnel, when necessary, will populate up-to-date organizational and contact information in DMDC.</i>	The Defense Manpower Data Center (DMDC) serves provides and utilizes the personnel, manpower, training, financial, and other data for the DoD. This data catalogues the history of personnel in the military and their family for purposes of healthcare, retirement funding and other administrative needs.	DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012

**Table 3.75 – Directory Information Updates Business Rule**

#### 3.2.10.3.1 (P10/R3) Assumptions

- *Office of the Assistant Secretary of Defense for Manpower & Reserve Affairs (OASD (M&RA))* established DMDC to collect and maintain accurate, readily available manpower and personnel data
- DoD/Office of the Secretary of Defense (OSD) will provide retired military and civilian employees with 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

#### 3.2.10.3.2 (P10/R3) Constraints

- Access to the DMDC (web site) requires a DoD certificate

### 3.2.11 (P11) Principle 11 – Network Access Controls

Principle	Description	References
<i>Permit or deny access to network nodes by devices based on policies and/or specific sets of networking attributes (e.g., TCP ports or range of ports, IP Addresses, devices ID, etc.).</i>	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 the 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 adds another layer of security to the protection of DoD Resources.	JIE POA&M, March 2012

Table 3.76 – Network Access Controls Principle

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

Business Rule	Description	References
<i>Authorization policies may utilize one or more network attributes, as required, to identify information Resources available on DoD networks.</i>	Remote users attempting to acquire access to DoD networked Resources can introduce unintentional security risk into the DoD Enterprise system. Though a user may have the proper credentials to access the DoD Enterprise under normal conditions, at times the remote network environment by which a user is trying to access the DoD Enterprise may be unknown or known to be untrustworthy. In these and similar scenarios, the DoD Enterprise 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.	JIE POA&M, March 2012

Table 3.77 – Authorization Policy Network Attributes Business Rule

##### 3.2.11.1.1 (P11/R1) Assumptions

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

##### 3.2.11.1.2 (P11/R1) Constraints

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

##### 3.2.11.1.3 (P11/R1) Risk

- Access to the NT-DSs and T-DSs will provide an unauthorized user with access to information pertaining to all DoD Resources that are available to the DoD Enterprise

## 3.2.11.2 (P11/R2) Business Rule 2 – Network-Connected Authentication

Business Rule	Description	References
<i>For network-connected devices, user authentication will be executed via the local device and enterprise network resident authentication services, authorizing users to access information Resources on both a standalone device and information Resources on a network.</i>	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 whether or not they have network connectivity available.	DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012

Table 3.78 – Network-Connected Authentication Business Rule

## 3.2.11.2.1 (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

## 3.2.11.2.2 (P11/R2) Constraints

- Synchronization between local and DoD Enterprise Authentication Services occurs when a device has connectivity to the DoD network
- 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

## 3.2.11.2.3 (P11/R2) Risk

- Long periods without connectivity to DoD Authentication Services could allow unauthorized access to a local device

### 3.2.11.3 (P11/R3) Business Rule 3 – ‘Disconnected’ and/or ‘Network-Disadvantaged’ Authentication

Business Rule	Description	References
<p><i>For non-networked, disconnected, and network disadvantaged devices, identity authentication will be permitted via the local device authentication service, limiting authorization of information Resources to a standalone device until the Requester is re-authenticated to the network and/or enterprise information Resources .</i></p>	<p>Digital information required by DoD personnel resides on Resources accessed via DoD networks. Electronic devices (i.e., desktops &amp; 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 DoD Enterprise, 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 a device that cannot access the DoD Enterprise Authentication Service. Accessing information on local device will require authentication for access to the disconnected device.</p>	<p>DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012</p>

**Table 3.79 – ‘Disconnected’ and/or ‘Network-Disadvantaged’ Authentication Business Rule**

#### 3.2.11.3.1 (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

#### 3.2.11.3.2 (P11/R3) Constraints

- Authentication for a new user to access a local device and DoD networks must initially be performed locally to that device
- If a user with a CAC attempts to access a disconnected device for the first time, authentication and local access only must be granted

#### 3.2.11.3.3 (P11/R3) Risk

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

## 3.2.11.4 (P11/R4) Business Rule 4 – Network Gateways

Business Rule	Description	References
<i>DoD Enterprise information systems and services will provide standard extensions, or common network gateways, for integration between network domain to support connectivity to Authentication and Authorization services.</i>	Secure DoD Enterprise Authentication and Authorization service access requires 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 further extend access to the Resources that are spread across multiple network domains or enclaves.	DoD Information Enterprise Architecture (IEA) Version 2.0 - Draft Vol. II, February 2012

Table 3.80 – Network Gateways Business Rule

## 3.2.11.4.1 (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 DoD Enterprise information Resources must possess a CAC

## 3.2.11.4.2 (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 the DoD Enterprise authentication and authorization services

## 3.2.11.4.3 (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

### 3.2.12 (P12) Principle 12 – Monitoring and Reporting

Principle	Description	References
<i>Provide for both proactive and reactive monitoring and reporting on all forms of logical and physical access across the DoD Enterprise.</i>	Auditing services will need to comply with all established DoD Service Level Agreements (SLA) for both the DoD network and information systems/applications/data services. This is required to assure an appropriate level of information assurance, as well as optimize both network and information systems reliability and response time.	JIE POA&M, March 2012

Table 3.81 – Monitoring and Reporting Principle

#### 3.2.12.1 (P12/R1) Business Rule 1 – Auditing Services

Business Rule	Description	References
<i>Access management auditing will support both real-time and historical activity, as well as provide a forensic analysis capability.</i>	It will be necessary to compliment the IdAM service infrastructure monitoring and reporting capabilities with the ability to easily and readily analyze data from both real-time and historical data. This will serve to improve overall Cyber defense capability, as well as serve as a basis for creating and maintain access authorization policies across the DoD Enterprise.	JIE POA&M, March 2012

Table 3.82 – Auditing Services Business Rule

##### 3.2.12.1.1 (P12/R1) Assumptions

- Offline Address Books (OAB) will be auditable

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

Business Rule	Description	References
<i>DoD information services and computer networks shall be monitored in accordance with pertinent GIG-wide Service Level Agreements (SLA) in order to detect, isolate, and react to intrusions, disruption of service, or other incidents that threaten DoD operations.</i>	Auditing services will need to comply with all established DoD SLAs for both DoD network and information systems/applications/data services. This is required to assure an appropriate level of information assurance, as well as optimize both network and information systems reliability and response time.	DoD Information Enterprise Architecture (IEA) Version 2.0 - Draft Vol. II, February 2012

Table 3.83 – Identity and Access Management (IdAM) Infrastructure Monitoring/Reporting Business Rule

## Appendix A - Vocabulary (Integrated Dictionary – AV-2)

### Identity and Attribute Management Vocabulary

**Access Control:** The collection of all controls used to assure that person as well as non-person entities would have access only to information processing facilities for which they are authorized.

**Access Management:** The processes and technologies for controlling and monitoring access to resources consistent with governing policies. Access management includes authentication, authorization, trust, and security auditing.

**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 principals or systems access to a resource or service.

**Affiliation, Affiliation Group:** A set of system entities that share a single namespace (in the federated sense) of identifiers for principals.

**Assertion:** A piece of data produced by a Security Assertions Markup Language (SAML) authority regarding an act of authentication performed on a subject, attribute information about the subject, or authorization data applying to the subject with respect to a specified resource.

**Asserting Party:** An administrative domain that hosts one or more SAML authorities. Informally, it is an instance of a SAML authority.

**Attribute:** A distinct characteristic of an object (in SAML, of a subject). An object's attributes are said to describe it. Attributes are often specified in terms of physical traits, such as size, shape, weight, and color, etc., for real-world objects. Objects in cyberspace might have attributes describing size, type of encoding, network address, and so on. Attributes are often represented as pairs of "attribute name" and "attribute value(s)", e.g. "foo" has the value 'bar', "count" has the value 1, "gizmo" has the values "frob" and "2", etc. Often, these are referred to as "attribute value pairs".

**Authentication:** A process of determining, to a specified level of confidence, the credentials of a security principal either by verification or by identification. (From SAML Glossary: To confirm a system entity's asserted principal identity with a specified, or understood, level of confidence.)

**Authentication Assertion:** An assertion that conveys information about a successful act of authentication that took place for a subject.

**Authentication Authority:** A system entity that produces authentication assertions.

**Authorization:** The process of resolving a security principal's entitlements with the permissions configured on a resource in order to control access.

**Credential:** Digital attributes related to or derived from a secret that a digital identity possesses, although secrets are not involved in all cases.

**Credentials:** Data that is transferred to establish a claimed principal identity.

**Credentialing:** Sets up (and maintains) the digital attributes used to validate identity.

**Digital Identity:** The unique identifier and descriptive attributes that define a security principal, i.e., person, group, role, device, or service.

**Directory:** An information source used to store information about objects.

**Directory Service:** Making objects in a directory and their content available.

**Domain:** A uniquely named collection of computers that share a common directory database.

**Entitlement:** A set of attributes that specify the access rights and privileges of an authenticated security principal.

**Extensible Markup Language:** See XML

**Federated Identity:** A principal's identity is said to be 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.

**Federated Identity Management:** The administration of attributes, associated with security principals, between organizations.

**Federation:** A special kind of trust relationship established beyond internal network boundaries between distinct organizations that enables access granted in one domain based on authentication in another.

**Identity:** A set of attributes that uniquely identifies a system entity such as a person, an organization, a service, or a device.

**Identity Consumer (IDC):** Also called a relying party. A type of service provider that consumes identity assertions from trusted identity providers within a federation.

**Identity Federation:** The act of creating a federated identity on behalf of a Principal.

**Identity Management:** Management of the attributes that name and describe a security principal within a context that may be local, organizational, national or global in scope.

**Identity Provider (IDP):** A kind of service provider that creates, maintains, and manages identity information for principals and provides principal authentication to other service providers (consumers) within a federation, such as with web browser profiles.

**Identity Store:** A repository that contains digital identities.

**Identity Synchronization:** The process of ensuring that multiple identity stores contain consistent data for a given digital identity.

**Identifier:** A data element that maps to a security principal that uniquely identifies the entity.

**Name Qualifier:** A string that disambiguates an identifier that may be used in more than one namespace (in the federated sense) to represent different principals.

**Permission:** Approval to perform an operation on one or more protected resources.

**Policy Management:** Provides the ability to manage access policies across the enterprise reducing the number of policies managed, and reducing discrepancies.

**Proxy:** An entity authorized to act for another.

- a) Authority or power to act for another.
- b) A document giving such authority. [Merriam]

**Proxy Server:** A computer process that relays a protocol between client and server computer systems, by appearing to the client to be the server and appearing to the server to be the client. [RFC2828]

**Principal:** A system entity whose identity can be authenticated.

**Profile:** Key information that describes the security principal and contains personal, working environment, operational, and security information associated with the security principle.

**Relying Party:** A system entity that decides to take an action based on information from another system entity. For example, a SAML relying party depends on receiving assertions from an asserting party (a SAML authority) about a subject.

**Requester, SAML Requester:** A system entity that utilizes the SAML protocol to request services from another system entity (a SAML authority, a responder). The term "client" for this notion is not used because many system entities simultaneously or serially act as both clients and servers. In cases where the SOAP (Simple Object Access Protocol) binding for SAML is being used, the SAML requester is architecturally distinct from the initial SOAP sender.

**Responder, SAML Responder:** A system entity (a SAML authority) that utilizes the SAML protocol to respond to a request for services from another system entity (a requester). The term "server" for this notion is not used because many system entities simultaneously or serially act as both clients and servers. In cases where the SOAP binding for SAML is being used, the SAML responder is architecturally distinct from the ultimate SOAP receiver.

**Role-Based Access Control:** Set of "groups" that have a set of permissions and policies which security principals are assigned to.

**SAML Authority:** An abstract system entity in the SAML domain model that issues assertions. See also attribute authority, authentication authority, and policy decision point (PDP).

**SAML Artifact:** A small, fixed-size, structured data object pointing to a typically larger, variably-sized SAML protocol message. SAML artifacts are designed to be embedded in URLs and conveyed in HTTP messages, such as HTTP response messages with "3xx Redirection" status codes, and subsequent HTTP GET messages. In this way, a service provider may indirectly, via a user agent, convey a SAML artifact to another provider, who may subsequently dereference the SAML artifact via a direct interaction with the supplying provider, and obtain the SAML protocol message. Various characteristics of the HTTP protocol and user agent implementations provided the impetus for concocting this approach. The HTTP Artifact binding section of [SAMLBind] defines both the SAML Artifact format and the SAML HTTP protocol binding incorporating it.

**Schema:** The organizing structure of an XML document or a database system. A physical database schema is the actual structure of a database as is implemented. A logical database schema is a database model or representation, like a blueprint, used in understanding data organization and planning database construction. The logical schema usually differs from the

actual physical schema that results when a database is implemented and optimized for system performance.

**Security Auditing:** Process a system uses to detect and record security related events such as success and failures to create, access, or delete objects such as files.

**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.

**Service Provider:** A role assumed by a system entity, where the system entity provides services to principals or other system entities.

**Single Sign On:** The ability for reduced complexity in accessing resources by using a single set of credentials to access systems and/or using a single authentication to access resources.

**Trust:** A state that describes the agreements between different parties and systems for sharing identity information.

**XML:** Extensible Markup Language, abbreviated XML, describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them. [XML]

**XML Attribute:** An XML data structure that is embedded in the start-tag of an XML element and that has a name and a value. For example, the italicized portion below is an instance of an XML attribute:

```
<Address AddressID="A12345">...</Address>
```

**XML Element:** An XML data structure that is hierarchically arranged among other such structures in an XML document and is indicated by either a start-tag and end-tag or an empty tag. For example:

```
<Address AddressID="A12345">
  <Street>105 Main Street</Street>
  <City>Springfield</City>
  <StateOrProvince>
    <Full>Massachusetts</Full>
    <Abbrev>MA</Abbrev>
  </StateOrProvince>
  <Post Code="56789"/>
</Address>
```

## Acronym List

(Items highlighted in green are definitions unique to this RA)

I:n	One-to-Many
AAA	Authentication, Authorization, and Accounting
AAAA	Authentication, Authorization, Access Control and Auditing
AAES	Authoritative Attribute Exchange Service
AAF	Authentication and Authorization Framework
ABAC	Attribute-Based Access Control
AC	Access Control (this acronym is used when referencing the Access Control family)
ACL	Access Control List
ACP	Allied Communications Publications
AD	Active Directory
ADFS	Active Directory Federation Services
ADR	Attributes Data Repository
ADS	Active-Directory Service
ADS2	Application and Data Services
AEN	Army Enterprise Network
AES	Advanced Encryption Standard
AFATDS	Advanced Forward Area Tactical Data System
AGS	Authentication Gateway Service
AKO	Army Knowledge Online
ALT	Acquisition, Logistics and Technology
ANSI	American National Standards Institute
AO	Area of Operations
AOR	Area of Responsibility
API	Application Programming Interface
APL	Approved Products List
APS	Account Provisioning Service
AR	Attributes Repositories
ARCYBER	Army Cyber Command
ARFORGEN	Army Generating Force
ASA(ALT)	Assistant Secretary of the Army for Acquisition, Logistics and Technology
ASF	Authentication Service Framework
ASIP	Army Stationing and Installation Planning
AU	Audit and Accountability (this acronym is used when referencing the Audit and Accountability control family)
AWG	Architecture Working Group
BAE	Backend Attribute Exchange
BCT	Brigade Combat Team
BIO (-A)	PIV Biometrics (-Attended)
C&A	Certification and Accreditation
C2	Command and Control
CA	Certification Authority

CA (cont)	Security Assessment and Authorization (this acronym is used when Referencing the Security Assessment and Authorization control family)
CAC	Common Access Card
CAK	Card Authentication Key
CCB	Change Control Board
CDC	Centers for Disease Control and Prevention
CDRUSSTRATCOM	Commander, United States Strategic Command
CE	Computing Environment
CHUID	Cardholder Unique Identifier
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CMM	Capability Maturity Model
CND	Computer Network Defense
CNSS	Committee of National Security Systems
CNSSI	Committee on National Security Systems Instruction
COCOM	Combatant Command
COE	Common Operating Environment
COFG	Citizen Outreach Focus Group
COI	Communities of Interest
COL	Colonel
COMMON	Federal PKI Common Policy Framework
CoN	Certification of Networthiness
CONUS	Continental United States
COOP	Continuity of Operations Plan
COTS	Commercial Off-The-Shelf
CPIC	Capital Planning and Investment Control
CPS	Certification Practice Statement
CRL	Certificate Revocation Lists
CUI	Controlled Unclassified Information
CVS	Central Verification System
DAP	Directory Access Protocol
DECC	DISA Enterprise Computer Center
DEERS	Defense Enrollment Eligibility Reporting System
DEFCON	Defense Readiness Condition
DES	Data Encoding Specification
DGWIG	Digital Geographic Information Working Group
DHS	Department of Homeland Security
DIG	Description and Implementation Guide
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISR	DoD IT Standards Registry
DMDC	Defense Manpower Data Center
DME	Development, Modernization, and Enhancement
DMS	Defense Management System
DMZ	Demilitarized Zone
DNS	Domain Name Service
DOB	Date of Birth
DoD	Department of Defense
DoDAF	DoD Architecture Framework

- Unclassified -

DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DPBAC	Dynamic Policy-Based Access Control
DS	Directory Service
DSA	Digital Signature Algorithm
E.O.	Executive Order
EA	Enterprise Architecture
EAAF	Enterprise Authentication and Authorization Framework
EADPS	Enterprise Active-Directory Provisioning Service
EAPS	Enterprise Account Provisioning Service
EAS	Enterprise Authentication Service
EASF	Enterprise Authentication Service Framework
EASR	Enterprise Architecture Segment Report
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECS	Enterprise Collaboration Service
ECSS	Expeditionary Combat Support System
EDI-PI	Electronic Data Interchange – Personal Identifier
EDS	Enterprise Directory Service
EIADRSS	Enterprise Identity Attribute Data Repository and Synchronization Service
EIAS	Enterprise Identity Attribute Service
EIDS	Enterprise Identity Directory Service
EMI	Electro Magnetic Interface
EPLRS	Enhanced Position Location and Reporting System
e-QIP	Electronic Questionnaires for Investigations Processing
e-RA	E-authentication Risk and Requirements Assessment
ESC	Enterprise Service Catalog
ESIGN	Electronic Signatures In Global and National
ESM	Enterprise Security Management
ESN	Electronic Serial Number
ESR	Enterprise Strategy and Implementation Roadmap
ESSF	Enterprise Services Security Framework
F/ERO	Federal/Emergency Response Official
FACC	Feature and attribute Coding Catalogue
FAR	Federal Acquisition Regulation
FASC-N	Federal Agency Smart Credential Number
FBCA	Federal Bridge Certification Authority
FBI	Federal Bureau of Investigation
FBI CJIS	Federal Bureau of Investigation Criminal Justice Information System
FBI IAFIS	Federal Bureau of Investigation Integrated Automated Fingerprint Identification System
FCPCA	Federal Common Policy Certification Authority
FDCC	Federal Desktop Core Configuration
FEA	Federal Enterprise Architecture
FEMA	Federal Emergency Management Agency
FICAM	Federal Identity, Credential, and Access Management
FICC	Federal Identity Credentialing Committee
FIPPS	Fair Information Practice Principles
FIPS	Federal Information Processing Standard

- Unclassified -

FISMA	Federal Information Security Management Act
FIWG	Federation Interoperability Working Group
FiXs	Federation for Identity and Cross Credentialing Systems
FM	Field Manual
FPKI	Federal PKI
FPKIMA	Federal PKI Management Authority
FPKIPA	Federal PKI Policy Authority
FRAC	First Responder Access Card
FRCA	Federal Root Certification Authority
FSAM	Federal Segment Architecture Methodology
FSD	Full Service Directory
FSL	Facility Security Level
G2B	Government-to-Business
G2C	Government-to-Citizen
G2G	Government-to-Government
G3/5/7	Army Deputy Chief of Staff for Operations
GAL	Global Address List
GAO	Government Accountability Office
GCC	Geographic Combatant Command
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GFEBs	General Fund Enterprise Business System
GFIPM	Global Federated Identity and Privilege Management
GIG	Global Information Grid
GNEC	Global Network Enterprise Construct
GNOSC	Global Network Operations and Security Center
GOTS	Government Off-the-Shelf
GPEA	Government Paperwork Elimination Act
GSA	General Services Administration
GUID	Global Unique Identifier
HHS	Health and Human Services
HR	Human Resources
HSC	Homeland Security Council
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
IAFIS	Integrated Automated Fingerprint Identification System
IAM	Identity Access Management
IAW	in accordance with
IAW	Information Assurance Workshop
IC	Intelligence Community
ICAM	Identity, Credential and Access Management
ICAMSC	Identity, Credential and Access Management Subcommittee
ICC	Integrated-Circuit Chip
ICD	Initial Capabilities Document
ICF	Information Card Foundation
ICI-IPC	Information and Communications Infrastructure Interagency Policy Committee
ID	Identification
IdAM	Identity and Access Management

- Unclassified -

IDC	Identity Consumer
IDD	Integrated Data Dictionary
IDM	Intrusion Prevention System (IPS) Device Manager ((ANSI/SIA OSIPS-IDM)
IdM	Identity Management
IDMS	Identity Management System
IdP	Identity Provider
IdSS	Identity Synchronization Service
IdSS	Identity Synchronization Service
IEA	Information Enterprise Architecture
IEC	International Electrotechnical Commission
IEE	Internal Effectiveness & Efficiency
IETF	Internet Engineering Task Force
IG	Inspector General
IIS	Internet Information Services
IM	Instant Messaging
IMI	Identity Metasystem Interoperability
INCITS	Inter-National Committee for Information Technology Standards
INFOCON	Information Operations Condition
IOC	Initial Operational Capability
IP	Internet Protocol
IPC	Interagency Policy Committee
IPCP	Internet Protocol Control Protocol
IPSec	Internet Protocol Security
IRC	Information Resources Catalog
IRS	Internal Revenue Service
IRTPA	Intelligence Reform and Terrorism Prevention Act
IS	
ISC	Interagency Security Committee
ISE	Information Sharing Environment
ISIMC	Information Security and Identity Management Committee
ISO	International Organization for Standardization
IT	Information Technology
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
JFC	Joint Force Commander
JIE	Joint Information Environment
JP	Joint Publication
JPAS	Joint Personnel Adjudication System
JWICS	Joint Worldwide Intelligence Communications System
KRA	Key Recovery Agent
LAC	Logical Access Control
LACS	Logical Access Control System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LOA	Level of Assurance
LRA	Local Registration Agent
LTC	Lieutenant Colonel
M&RA	Manpower & Reserve Affairs
MAC	Media Access Control

MAS	Multiple Award Schedule
MDR	Metadata Registry
ME	Mission Environment
MIB	Management Information Base
-MINEX	Minutia Exchange
MS	Microsoft
MSP	Message Security Protocol
NAC	National Agency Check
NACI	National Agency Check with Written Inquiries
NAI	Network Access Identifier
NARA	National Archives Records Administration
NASA	National Aeronautics and Space Administration
NAVSUP	Naval Supply Systems Command
NCES	Net-Centric Enterprise Service
NCIC	National Crime Information Center
NETCOM	Network Command
NetOps	Network Operations
NFI	Non-Federal Issuers
NFPA	National Fire Protection Agency
NIE	Network Interoperability Exercise
NIEM	National Information Exchange Model
NIPP	National Infrastructure Protection Plan
NIPRNet	Non-Secure Internet Protocol Router Network
NISC	Network and Infrastructure Security Sub Committee
NIST	National Institute of Standards and Technology
NIST-ITL	National Institute of Standards and Technology Information Technology Lab
NOS	Network Operating System
NOSC	Network Operations and Security Center
NPE	Non-Person Entity
NSA	National Security Agency
NSC	National Security Council
NSLDSS	National Senior Leadership Decision Support System
NSPD	National Security Presidential Directive
NSS	National Security Systems
NSTC	National Science and Technology Council
NT-AAF	Non-Tactical Authentication and Authorization Framework
NT-APS	Non-Tactical Account Provisioning Service
NT-ASF	Non-Tactical Authentication Service Framework
NT-DS	Non-Tactical Directory Services
NT-RSOS	Non-Tactical Reduced Sign-On Service
NT-SSOS	Non-Tactical Single Sign-On Service
O&M	Operations and Maintenance
OAB	Offline Address Books
OASD(M&RA)	Office of the Assistant Secretary of Defense for Manpower and Reserve Affairs
OASIS	Organization for the Advancement of Structured Information Standards
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OCISO	Office of the Chief Information Security Officer
OCSP	Online Certificate Status Protocol

- Unclassified -

OID	Object Identifier
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPCON	Operational Control
OPM	Office of Personnel Management
OSD	Office of the Secretary of Defense
OSIPS	Open, Systems Integration and Performance Standards
OTM	On-The-Move
OU	Organizational Unit
OV	Operational View
PAC	Physical Access Control
PACS	Physical Access Control System
PAP	Policy Administration Point
PBAC	Policy-Based Access Control
PBAS	Policy-Based Authorization Service
PBS	Public Building Service
PCC	Personnel Category Code
PCI	PIV Card Issuers
PDA	Personal Digital Assistant
PDP	Policy Decision Point
PDVAL	Path Discovery and Validation
PE	Person Entity
PEP	Policy Enforcement Point
PIA	Privacy Impact Assessment
PICC	Proximity Integrated Circuit Card
PII	Personally Identifiable Information
PIMM	PIV Card Implementation Maturity Model
PIN	Personal Identification Number
PIP	Personnel Identity Protection
PIPS	Personnel Investigations Processing System
PIV	Personal Identity Verification
PIV-AUTH	PIV Authentication Key
PIV-FASC-N	Personnel Identify Verification Federal Agency Smart Card Credential Number
PIV-I	Personal identity Verification Interoperable
PKCS	Public-Key Cryptography Standards
PKE	PKI-Enabled
PKI	Public Key Infrastructure
PKITS	Public Key Interoperability Test Suite
PMI	Privilege Management Infrastructure
PMO	Program Management Office
POA&M	Plan of Action and Milestones
POD	Port of Debarkation
POR	Program of Record
PRM	Performance Reference Model
PRQP	PKI Resource Query Protocol
PS	Policy Store
PTC	Personnel Type Code
RA	Reference Architecture
RAAdAC	Risk-Adaptable Access Control

- Unclassified -

RBAC	Role-Based Access Control
RDT	Roadmap Development Team
RE	Rules Engine
RF	Radio Frequency
REBCA	Research & Education Bridge Certification Authority
RFC	Request for Comments
RMF	Risk Management Framework
ROI	Return on Investment
RSA	Rivest, Shamir and Adleman
RSO	Retirement Services Office
RSOI	Reception, Staging, Onward Movement, and Integration
RSOS	Reduced Sign-On Services
SAML	Security Assertion Markup Language
SASC	Security Acquisitions Sub Committee
SASO	Stability and Support Operations
SC	Service Component
SCRM	Service Component Reference Model
SCVP	Server-based Certificate Validation Protocol
SDK	Software Development Kit
SDLC	System Development Life Cycle
SF	Standard Form
SGT	Sergeant
SHA	Secure Hash Algorithm
SIA	Security Industry Association
SID	Security Identifier
SIN	Special Item Number
SIP	Shared Infrastructure Provider
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SMS	Security Management System
SMTP	Simple Mail Transfer Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOD	Segregation of Duties
SORN	System of Records Notice
SP	Special Publication
SPMS	Security Program Management Subcommittee
SSAPI	Simple Sockets API
SSH	Secure Shell Protocol
SSL	Secure Socket Layer
SSN	Social Security Number
SSO	Single-Sign On
SSOS	Single-Sign On Service
SSP	Shared Service Provider
STIG	Security Technical Implementation Guide
STRATCOM	Strategic Command
STS	Security Token Service
SV	System View
T-AFF	Tactical Authentication and Authorization Framework

- Unclassified -

TAMP	Trust Anchor Management Protocol
T-APS	Tactical Accounts Provisioning Service
T-ASF	Tactical Authentication Service Framework
TCP	Transmission Control Protocol
TDA	Tables of Distribution and Allowances
T-DS	Tactical Directory Service
TFP	Trust Framework Provider
TFPAP	Trust Framework Provider Adoption Process
TIC	Trusted Internet Connection
TLA	Top-Level Security Reference Architecture
TLS	Transport Layer Security
TOGAF	The Open Group Architecture Framework
TRADOC	Training and Doctrine Command
T-RSOS	Tactical Reduced Sign-On Service
TRUI	Treasury Unique Identifier
TS/SCI	Top Secret / Sensitive Compartmented Information
TSCP	Trans-global Secure Collaboration Program
T-SSOS	Tactical Single Sign-On Service
U.S.	United States
UC	Unified Communications
UCore	Universal Core
UL	Underwriters Laboratories
UPN	User Principal Name
URL	Uniform Resource Locator
USB	Universal Serial Bus
UUID	Universally Unique Identifier
VAM	Visual Authentication Mechanism
VMS	Visitor Management System
VPN	Virtual Private Network
WAN	Wide Area Network
WS	Web Service
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language
XML	eXtensible Markup Language
WS	Web Services

## Appendix B - Technical Positions and Patterns – Core Standards for Business Rules (by Business Rule)

Principle – P1		Principle Title: Unique Identity and Credentials						
Business Rule – P1/R1		Business Rule Title: Person Entity (PE) Unique Identifier						
Standard ID	Standard Title	Standard Type (Technical (T), Policy/Regulatory (P/R))	DISR Status (Mandated (M), Emerging (E), Retired (R))	Specified in Appendix A? (Y/N)	Access Type Applicable Service			
					Logical / Person Entity (PE)	Logical /Non-Person Entity (NPE)	Physical / Person Entity (PE)	Physical / Non-Person Entity (NPE)
ISO/IEC 14443-1:2000	Identification Cards -- Contactless Integrated Circuit(s) Cards - - Proximity Cards -- Part 1: Physical Characteristics, 2000	T	M	Y				

Principle – P1		Principle Title: Unique Identity and Credentials						
Business Rule – P1/R2		Business Rule Title: Allowed Identities						
Standard ID	Standard Title	Standard Type (Technical (T), Policy/Regulatory (P/R))	DISR Status (Mandated (M), Emerging (E), Retired (R))	Specified in Appendix A? (Y/N)	Access Type Applicable Service			
					Logical / Person Entity (PE)	Logical /Non-Person Entity (NPE)	Physical / Person Entity (PE)	Physical / Non-Person Entity (NPE)
SP 800-87	Codes for Identification of Federal and Federally-Assisted Organizations	T	N	N				
ISO/IEC 19794-5:2011	Biometric Data Interchange Formats -- Part 5: Face Image Data	T	E	Y				
DoDI 8520.03	Identity Authentication for Information Systems	P/R	N	N				

<b>Principle – P1</b>		<b>Principle Title: Unique Identity and Credentials</b>						
<b>Business Rule – P1/R3</b>		<b>Business Rule Title: Identity Suitability</b>						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
FIPS Pub 201-1	Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006	T	M	Y				
IETF RFC 2589	Lightweight Directory Access Protocol (v3): Extensions for Dynamic Directory Services, June 2000	T	M	Y				
DODI 8520.03	Identity Authentication for Information Systems	P/R	N	N				

<b>Principle – P1</b>		<b>Unique Identity and Credentials: Unique Identity and Credentials</b>						
<b>Business Rule – P1/R4</b>		<b>Business Rule Title: Identity Data Integrity</b>						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
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	T	M	Y				
ISO/IEC 7816-11:2004	Identification Cards - Integrated Circuit Cards - Part 11: Personal Verification Through Biometric Methods, 2004	T	M	Y				

<b>Principle – P1</b>		<b>Principle Title:</b> Unique Identity and Credentials						
<b>Business Rule – P1/R5</b>		<b>Business Rule Title:</b> Identity Data Discoverability						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
SP 800-73	Interfaces for Personal Identity Verification	T	M	Y				
ISO/IEC 19794-1:2011	Biometric Data Interchange Formats -- Part 1: Framework, 7/1/2011	T	M	Y				

<b>Principle – P1</b>		<b>Principle Title:</b> Unique Identity and Credentials						
<b>Business Rule – P1/R6</b>		<b>Business Rule Title:</b> Identity Data Conformance						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
SP 800-103	An Ontology of Identity Credentials, Part 1: Background and Formulation	T	N	N				

<b>Principle – P1</b>		<b>Principle Title:</b> Unique Identity and Credentials						
<b>Business Rule – P1/R8</b>		<b>Business Rule Title:</b> Enterprise Identity Repository						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
SP 800-122	Guide for Protecting the Confidentiality of Personally Identifiable Information (PII)	T	N	N				

<b>Principle – P2</b>		<b>Principle Title:</b> Identity Authoritative Data Source						
<b>Business Rule – P2/R1</b>		<b>Business Rule Title:</b> Defense Manpower Data Center (DMDC) Use Person Entity (PE)						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
CNSSI Number 1253	Security Categorization and Control Selection for National Security Systems Version 1 (CNSS Instruction Number 1253), October 2008	P/R	N	N				

<b>Principle – P2</b>		<b>Principle Title:</b> Identity Authoritative Data Source						
<b>Business Rule – P2/R2</b>		<b>Business Rule Title:</b> Common Access Card (CAC) Usage						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
FIPS Pub 201-1	Part 2: Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006	T	M	Y				
SP 800-73	Interfaces for Personal Identity Verification	T	N	N				

<b>Principle – P2</b>		<b>Principle Title:</b> Identity Authoritative Data Source						
<b>Business Rule – P2/R4</b>		<b>Business Rule Title:</b> Adding Core PE Identity Attributes						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
UCore DIG v2.0.0	Universal Core (UCore) Description and Implementation Guide (DIG), Version 2.0.0, 13 August 2009	T	Active	N				
DODI 8520.03	Identity Authentication for Information Systems	P/R	N	N				
DODD 8320.02	Data Sharing in a Net-Centric Department of Defense	P/R	N	N				

<b>Principle – P3</b>		<b>Principle Title:</b> Person Entity (PE) and Non-Person Entity Identification						
<b>Business Rule – P3/R1</b>		<b>Business Rule Title:</b> Mobile/Edge/Platforms/Devices						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
IETF RFC 2794	Mobile IP Network Access Identification Extension for IPv4, March 2000	T	M	Y				

<b>Principle – P3</b>		<b>Principle Title:</b> Person Entity (PE) and Non-Person Entity Identification						
<b>Business Rule – P3/R2</b>		<b>Business Rule Title:</b> Mobile Device Binding						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
IETF RFC 2794	Mobile IP Network Access Identification Extension for IPv4, March 2000	T	M					

<b>Principle – P4</b>		<b>Principle Title:</b> Global Directory Electronic Mail (E-Mail) Services						
<b>Business Rule – P4/R1</b>		<b>Business Rule Title:</b> Global Address List (GAL) Distribution						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
DES for IC Full Service Directory Schema V1.0	Data Encoding Specification for the IC Full Service Directory Schema V1.0, 14 December 2011	T	E	Y				

<b>Principle – P4</b>		<b>Principle Title:</b> Global Directory Electronic Mail (E-Mail) Services						
<b>Business Rule – P4/R2</b>		<b>Business Rule Title:</b> Global Address List (GAL) Organizational Views						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
ACP 123A:2001	Common Messaging Strategy and Procedures, Edition A, 26 June 2001	T	R	N				

<b>Principle – P4</b>		<b>Principle Title:</b> Global Directory Electronic Mail (E-Mail) Services						
<b>Business Rule – P4/R3</b>		<b>Business Rule Title:</b> Global Address List (GAL) Data Schema						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
IETF RFC 2849	The LDAP Data Interchange Format (LDIF), June 2000	T	M	Y				

<b>Principle – P4</b>		<b>Principle Title: Global Directory Electronic Mail (E-Mail) Services</b>						
<b>Business Rule – P4/R4</b>		<b>Business Rule Title: Offline Address Book Availability</b>						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
The ACP 123 annexes	Common Messaging Strategy and Procedures, Edition A, U.S. Supplement No. 1, 26 June 2001	T	R	N				

<b>Principle – P4</b>		<b>Principle Title: Global Directory Electronic Mail (E-Mail) Services</b>						
<b>Business Rule – P4/R5</b>		<b>Business Rule Title: Directory/Global Address List (GAL) Services Availability</b>						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
IETF RFC 1777	Lightweight Directory Access Protocol, March 1995	T	R	N				
IETF RFC 2605	Directory Server Monitoring MIB, June 1999	T	M	Y				
IETF RFC 3673	Lightweight Directory Access Protocol version 3 (LDAPv3): All Operational Attributes, December 2003	T	M	Y				

<b>Principle – P5</b>		<b>Principle Title:</b> Authentication and Authorization						
<b>Business Rule – P5/R1</b>		<b>Business Rule Title:</b> Authentication and Authorization Scope						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
FIPS Pub 201-1	Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006	T	M	Y				
IETF RFC 2865	Remote Authentication Dial In User Services (RADIUS), June 2000	T	M	Y				
IETF RFC 2845	Secret Key Transaction Authentication for Domain Name System (DNS,TSIG), May 2000	T	M	Y				
IETF RFC 4252	The Secure Shell (SSH) Authentication Protocol, January 2006	T	M	Y				
ITU-T X.509:2005	Information Technology - Open Systems Interconnection - The Directory: Public-key and Attribute Certificate Frameworks, August 2005	T	M	Y				

<b>Principle – P5</b>		<b>Principle Title:</b> Authentication and Authorization						
<b>Business Rule – P5/R3</b>		<b>Business Rule Title:</b> Single DoD Authentication Service Model						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
IETF RFC 4251	The Secure Shell (SSH) Protocol Architecture, January 2006	T	M	Y				

<b>Principle – P5</b>		<b>Principle Title:</b> Authentication and Authorization						
<b>Business Rule – P5/R4</b>		<b>Business Rule Title:</b> Standard Attribute Model						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
DGIWG FACC	DGIWG Feature and Attribute Coding Catalogue	T	M	Y				
ANSI INCITS 385-2004	Face Recognition Format for Data Interchange, May 13, 2004	T	M	Y				
ANSI/INCITS 378-2004	Finger Minutiae Format for Data Interchange	T	M	Y				
DoD Biometrics IDD v5.0	DoD Biometrics Integrated Data Dictionary v5.0, 8 December 2011	T	M	Y				

<b>Principle – P5</b>		<b>Principle Title:</b> Authentication and Authorization						
<b>Business Rule – P5/R5</b>		<b>Business Rule Title:</b> Global Information Resource Access						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
ISO/IEC 7816-11:2004	Identification Cards - Integrated Circuit Cards - Part 11: Personal Verification Through Biometric Methods, 2004	T	M	Y				

<b>Principle – P5</b>		<b>Principle Title: Authentication and Authorization</b>						
<b>Business Rule – P5/R6</b>		<b>Business Rule Title: Access Policy Management Model</b>						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
eXtensible Access Control Markup Language (XACML) Version 2.0, OASIS Standard, 1 February 2005	eXtensible Access Control Markup Language (XACML) Version 2.0, OASIS Standard, 1 February 2005	T	M	Y				

<b>Principle – P7</b>		<b>Principle Title: Access to Data, Services and Applications</b>						
<b>Business Rule – P7/R3</b>		<b>Business Rule Title: Data Tagging</b>						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
DODD 8320.02	Data Sharing in a Net-Centric Department of Defense	P/R	N	N				
DODD 8320.03	Unique Identification (UID) Standards for a Net-Centric Department of Defense	P/R	N	N				

<b>Principle – P7</b>		<b>Principle Title: Access to Data, Services and Applications</b>						
<b>Business Rule – P7/R4</b>		<b>Business Rule Title: Policy Store (PS) Personally Identifiable Information (PII)</b>						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
XACML 1.0 OASIS	eXtensible Access Control Markup Language (XACML) Version 1.0, OASIS Standard, 18 February 2003	T	M	Y				

<b>Principle – P9</b>		<b>Principle Title:</b> General Identity and Access Management (IdAM) Security						
<b>Business Rule – P9/R2</b>		<b>Business Rule Title:</b> DoD Authorization Service						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
SP 800-122	Guide for Protecting the Confidentiality of Personally Identifiable Information (PII)	T	N	N				
DODI 8520.03	Identity Authentication for Information Systems	P/R	N	N				

<b>Principle – P9</b>		<b>Principle Title:</b> General Identity and Access Management (IdAM) Security						
<b>Business Rule – P9/R3</b>		<b>Business Rule Title:</b> Information Resource Authorization						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
DODI 8510.01	DoD Information Assurance Certification and Accreditation Process (DIACAP)	P/R	N	N				

<b>Principle – P9</b>		<b>Principle Title:</b> General Identity and Access Management (IdAM) Security						
<b>Business Rule – P9/R4</b>		<b>Business Rule Title:</b> Enterprise Information Sharing						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
NSPD-59 / HSPD-24	Biometrics for Identification and Screening to Enhance National Security	P/R	N	N				

<b>Principle – P9</b>		<b>Principle Title:</b> General Identity and Access Management (IdAM) Security						
<b>Business Rule – P9/R5</b>		<b>Business Rule Title:</b> Information Resource Authentication Frequency						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
Web Services Security (WS – Security) 1.1	Web Services Security v1.1, February 2006	T	M	Y				
Security Assertion Markup Language (SAML) 2.0	OASIS Standard, 15 March 2005	T	M	Y				

<b>Principle – P9</b>		<b>Principle Title:</b> General Identity and Access Management (IdAM) Security						
<b>Business Rule – P9/R8</b>		<b>Business Rule Title:</b> Information/Data Resources Protection						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
DoD CJCSI 6510	Information Assurance (IA) and Computer Network Defense	P/R	Active	N				
DoDD 1000.25	DoD Personnel Identity Protection (PIP) Program	P/R	N	N				
DODD 8500.01E	Information Assurance (IA)	P/R	N	N				

<b>Principle – P9</b>		<b>Principle Title:</b> General Identity and Access Management (IdAM) Security						
<b>Business Rule – P9/R10</b>		<b>Business Rule Title:</b> Enterprise DoD Network Domain						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
ANSI/SIA OSIPS IDM-01:20xx	Identity and Carrier Management	T	N	N				

<b>Principle – P9</b>		<b>Principle Title:</b> General Identity and Access Management (IdAM) Security						
<b>Business Rule – P9/R12</b>		<b>Business Rule Title:</b> Data Encryption						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
SP 800-67	Recommendation for the Tripe Data Encryption Algorithm (TDEA) Block Cipher	T	R	N				

<b>Principle – P9</b>		<b>Principle Title:</b> General Identity and Access Management (IdAM) Security						
<b>Business Rule – P9/R13</b>		<b>Business Rule Title:</b> SHA-256 Encryption Migration						
<b>Standard ID</b>	<b>Standard Title</b>	<b>Standard Type (Technical (T), Policy/Regulatory (P/R))</b>	<b>DISR Status (Mandated (M), Emerging (E), Retired (R))</b>	<b>Specified in Appendix A? (Y/N)</b>	<b>Access Type Applicable Service</b>			
					<b>Logical / Person Entity (PE)</b>	<b>Logical /Non-Person Entity (NPE)</b>	<b>Physical / Person Entity (PE)</b>	<b>Physical / Non-Person Entity (NPE)</b>
FIPS 180-3	Secure Hash Standard (SHS), October 2008	T	M	Y				
OASIS SAML 2.0	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005	T	M	Y				

## Appendix C – ICAM/IdAM Service Areas and Services Definitions

### Identity Management

The Identity Management functions maintain and manage the identities, credentials and attributes for persons and non-person entities. Relying Parties require information about users as a basis for granting access. User identity is validated through the proofing and vetting processes and then linked to credentials such as PKI certificates, user ID/passwords, and biometrics. Attributes further describe users to aid in access decisions and are either contained within the credential or made available through an enterprise service or through local processes. Examples of attributes include citizenship, date of birth, organizational affiliation, security clearance, and privileges.

Currently, the Federal government has focused primarily on person entities. Some agencies – for example, DoD DISA – are beginning to direct attention to assigning identities to NPEs such as devices – desktops, servers, laptops, Personal Digital Assistants (PDAs), etc. Eventually, these devices will contain strong identity credentials and they will be associated with the following NPE attributes:

- Identity Store
  - A repository that contains digital identities
- Identity Store Types
  - Enterprise Identity Store
    - Primarily used to store digital identities at the DoD enterprise level and populate operational identity stores
  - Operational Identity Store
    - Primarily used to store digital identities at the at the organizational level (e.g., Army, Theater, Brigade Combat Team (BCT)) and are used to support network authentication & authorization processes
- Identity stores can take many forms based on different technologies.
  1. Database
  2. Lightweight Directory Access Protocol (LDAP) Directory
    1. *Microsoft (MS) Windows Active Directory (AD)*
    2. Flat file

### Attribute Management

Attribute Management plays a central role in enabling dynamic policy based access control. Attributes must be managed for identities, resources and the environment. They are key to making policy-based decisions by further defining characteristics beyond simple identity for users, resources, and the environment.

### Authentication

Authentication is the process of verifying that a claimed identity is genuine and based on valid credentials. Authentication typically leads to a mutually shared level of assurance by the relying

parties in the identity. Authentication may occur through a variety of mechanisms including challenge/response, time-based code sequences, biometric comparison, PKI or other techniques.

Users must have been issued valid and acceptable credentials. For Federal Government employees and certain Federal contractors, the acceptable credential is the Personal Identity Verification (PIV) card. The DoD Common Access Card (CAC) is DoD's PIV. Authentication occurs when a user's credential is electronically validated. The authentication process includes validating both the user and credentials.

## Cryptography

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

The encryption standards set by NIST and the DoD are constantly evolving. The current SHA-1 algorithm has been slated to be replaced with SHA-256 by the end of CY2013. This will better protect information by increasing the complexity of what is required to decrypt the data stream without immediate possession of the keys by several orders of magnitude. As computing hardware and their operating systems becomes more powerful and can execute more instructions faster, it will be necessary to assure that all applied cryptography techniques and algorithms used by the DoD at least keep pace with their capability to hack data streams either in transit or at rest.

## Authorization

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

## Privilege Management

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

- Entitlement Attributes – characteristics of an entity that are used to determine access privileges.
- Resource Attributes – data about a resource that inform additional access, protection and handling controls (these can be used to inform the Policy Store (PS)); they are also known as metadata within the DoD Data Strategy.
- Environmental Factors (or Environmental Attributes) – data about the current environment that inform additional access, protection and handling controls.

- Unclassified -

## Auditing and Reporting

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

## Federation

Data and information are created and stored across the network by many diverse organizations and operations that, due to the sensitivity of the content, must retain control over who has access and ability to change the content. At the same time, the need for raw data and processed information that can be accessed by anticipated and unanticipated consumers is demanded by the fast tempo of the modern battlefield.

Today, Warfighters have an account in each application that normally has a component residing in a server enclave, with user permissions set internally in the application and in the resources supporting the application (i.e., database, web server, application server). This requires a complicated process in which each application's administrators must create, manage and delete accounts for users located in the supported region and, in some cases, across the globe. The solution to ease this administrative burden is to create an automated account provisioning system that creates and maintains the same digital identity and identity verification process (i.e., password, X.509 certificate) for each user in each identity store.

With over 2.4 million personnel in the DoD, establishing and keeping digital identities synchronized across all identity stores is impractical. DoD requires the capability to federate authentication and authorization processes and procedures between a user's local network identity store and each supporting server enclave's security infrastructure, without the user having an account in each enclave. Further, ensuring that a user has the same digital identity in each enclave allows auditing to identify suspicious activity across the GIG.

Federation is normally implemented under two concepts:

1. Hub-and-spoke
2. Common peer-to-peer

The hub-and-spoke concept is based on a centralized Identity Store and PDP that services all the enrolled applications and services. The DISA Net-Centric Enterprise Service (NCES) Security Service and Attribute Service follow this construct. Because of the DoD's need to operate in a distributed fashion and independent of the GIG, the hub-and-spoke concept is not part of this reference architecture. The federation concept in this architecture is based on the ability of each enclave in the DoD to operate independently on the GIG and, when required, to interoperate or interface with systems or services in other enclaves. The Federation principle is to operate on a common peer-to-peer basis. The intent is not to preclude a Federation hub-and-spoke implementation, as it can be done between applications and services inside an enclave – but it should be done across the GIG if any of the users or their organizations/units may be deployed forward.

DoD network users and computers primarily operate as members of a Microsoft Windows Active Directory (AD) domain. With AD providing digital identity store services and an authentication, authorization, access control and auditing (AAAA) framework under which to perform network operations. However, there are also a number of personal computers that are

- Unclassified -

configured in a stand-alone mode that must be supported by this concept *and* architecture. But AD is not the only enclave AAAA framework provider and this architecture applies equally to all.

Most mission applications in use today are applications running locally (heavy client) but the trend in application development is well on the way toward web based applications delivered from an application server, with components and business logic running on the server. For performance reasons, many applications are designed to operate with components that download in the background and run on the client. Web-based applications are increasingly moving toward the service oriented architecture (SOA) model. In the SOA model, the enterprise is a collection of services that is available across the enterprise. In this model, an application or a portion of an application is a service that another application or person can utilize without extensive custom coding. The Security Assertion Markup Language (SAML) was developed in conjunction with web-based application development to provide authentication and authorization services between disparate network operations – meaning applications running in different AAAA frameworks.

The trend in industry and in Service Component (SC) specific applications and services has been to make ones that contain Identity Stores (i.e., have their own AAAA framework) and to make them SAML compliant. The principle outlined in this architecture is for a SAML-based authentication and authorization framework that will support client/server, N-tier web based applications, and applications built from web services. Combined with a common digital identity for each entity on the network allows for a single GIG level identity management and AAAA framework to operate.

There are two primary types of Federation; both are based on the Service Oriented Architecture (SOA) standards and principles. First is a group of entities agreeing to use a common Identity Management (IdM) system concept, which enables these entities to share selected identity information about users with others in defined trust relationships. Second is a group of web services that establish a trust agreement to federate their services. The Federation type described here is the use of a common IdM system across enclaves and organizations that follow the same guidance and governance model.

Not all client-side mission applications need to implement this profile if user access is controlled by the underlying operating system's authentication and authorization SAML capable processes. SAML is an XML standard for exchanging authentication and authorization data between security domains; that is, between an identity provider and a service provider. SAML assertions and protocol messages are encoded in XML and use XML namespaces. They are typically embedded in other structures for transport, such as HTTP POST requests or XML-encoded SOAP messages. SAML assertions are usually transferred from identity providers to service providers (identity consumers). Assertions contain statements that service providers use to make access control decisions. Three types of statements are provided by SAML:

1. Authentication statements
2. Attribute statements (claims)
3. Authorization decision statements

Authentication statements assert to the service provider that the principal did indeed authenticate with the identity provider at a particular time using a particular method of authentication. Other information about the principal may be disclosed in an authentication statement. The concept proposed in this paper is based on the ability to assert other information about the principal. SAML allows organizations to federate authentication and authorization processes across the GIG.

Auditing is not directly addressed in this concept. Auditing will continue to be a local operating system or application function. The intent in this concept is to support local auditing functions by integrating the users' or service's digital identity with the underlying AAAA framework so that logs identify the accessing identity.

A GIG enterprise-level authentication and authorization framework requires:

1. A **common trust framework** for reciprocal trust that supports secure accessing of network resources between geographically or operationally separated nodes.
2. **Common business and operating rules** for users and organizations that will deploy across the globe and require authentication to the local instantiation of the same network resources normally accessed from their home station without having to establish a new logon account to each new local resource.
3. **Common technical infrastructure** (i.e., architecture, protocols, ports, data models, schema) for technical interoperability.
4. **Common identity model** for identity federation and interoperability between nodes/organizations.

Systems in use today across the GIG encompass SAML functionality. As an example, the Windows server operating system provides SAML support through the Active Directory Federation Services (ADFS). ADFS can be configured to integrate with and provide SAML services for digital identities in an Active Directory (AD) identity store. ADFS retrieves user attributes from Active Directory, and authenticates the user's digital identity to trusting identity consumers. By using SAML based authentication, organizations employing ADFS can extend their existing Active Directory infrastructure to provide secure access to resources across the GIG.

The AD forest structure defines the security perimeter within which forest members can easily collaborate. Within the forest, an application simply refers back to the directory where forest account data is stored. This access model breaks down quickly when users who want to access the application hold accounts in other forests. Microsoft introduced a work-around to this problem called AD Forest Trusts, which in effect tie partner forests together under a joint security model. AD Trusts require significant infrastructure investment between locations that wish to participate in the trust. This approach also has significant security implications.

An alternative approach is adopting the federated identity model, which permits security information pertaining to a user to pass across traditional security boundaries, like AD forests. Federation allows partner organizations to share identity information based on standards in a secure manner and Active Directory Federation Services provides this capability for environments already leveraging AD. Additionally, the federation model is proving to be the

security model of choice by cloud service providers that want to provide access to applications based upon proof of identity sourced by the user's own preferred security service, reducing the need for cloud providers to maintain identity stores.

The federation model is ideal for enabling identity and access management controls between two separate enterprises or between organizations within an enterprise that are separated by security boundaries (AD forests, etc.). The model is also ideal for enabling access to cloud-based resources.

### Web Services (WS)-Federation

The federated identity model involves an assortment of components that, in concert, orchestrate events based on the third-party authentication model or broker model. This model is supported on systems that involve web-based applications. There are four core concepts/components to the model:

1. *An Application/Service* that depends on the token service (STS) to authenticate the client rather than providing authentication services on its own.
2. A *Security Token Service (STS)* that verifies the credentials of the user or entity and contains claims typically signed with a crypto key.
3. *Tokens* are the currency for trading identity information in the form of claims.
4. *Claims*, passed within the token, are statements made about one trusted entity by another.

The following figure describes the general flow of interaction between components in a WS-Federation solution. The general flow is that once a user attempts to access the application from his/her browser, the application redirects the browser to check the service provider's STS, who then redirects the browser to the identity provider (IdP) STS to verify the user is indeed an authenticated member of that organization. This flow is depicted in Figure C1 below.

### WS-Federation extends WS-Trust

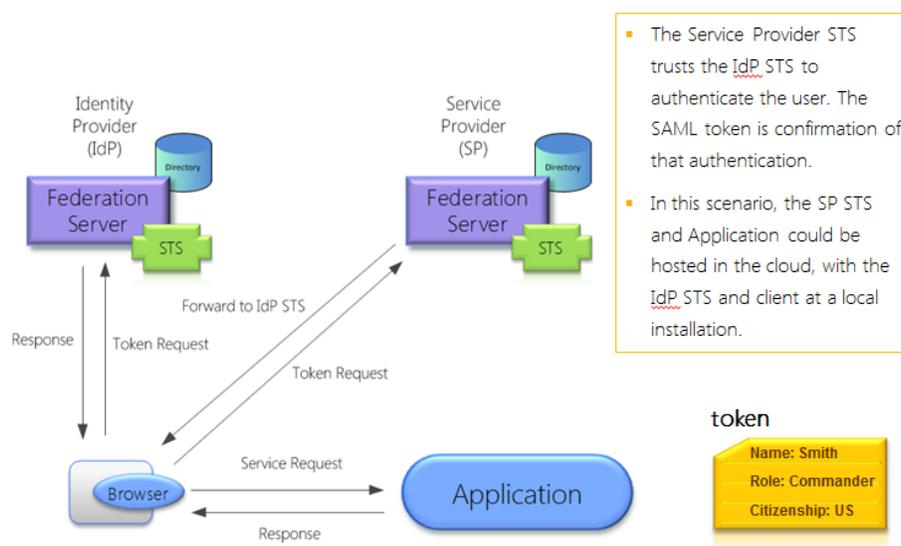


Figure C1 – General Data Flow Between Federation Components

- Unclassified -

Proof of authentication and any required attributes pulled from the user's IdP directory are stored in a SAML token. In this example, the token contains claims defining the user's name (John Smith), role (Commander), and his citizenship (US). The IdP STS and SP STS first establish a *federated* trust before interacting – this form of trust is set by policy. Each STS gets a copy of the other's federation metadata document which articulates terms of the trust relationship. Most interaction occurs via re-directs through the browser; however the WS-Federation standard permits other profiles that enable different sequences of interaction.

## Federation Principles

### 1. All enclaves have a Federation gateway with a Security Token Service (STS)

All security enclaves with an embedded identity store shall have a Federation gateway that, at a minimum, has an STS capability that supports the establishment of one or more one-way or two-way trusts.

### 2. Common open standards and profiles

All Federation Gateways and STS implementations must support the standards below. The movement to new versions of each standard must be coordinating across the DoD to ensure interoperability is maintained:

#### Security Assertion Markup Language

(SAML v2.0), an 'Organization for the Advancement of Structured Information Standards' (OASIS) standard, provides the ability to exchange authentication, attribute, and authorization decision information.

#### WS-Security v1.0

This is an OASIS standard that provides the ability to secure SOAP Web services by supplying mechanisms for message integrity and confidentiality that are independent of the underlying transport, and for associating security tokens with a message context. This Identity Federation reference architecture uses WS-Security as the open standard to secure Web services in conjunction with other standards, such as XML-Signature and XML-Encryption.

**WS-Trust** uses the secure messaging mechanisms of WS-Security to define additional primitives and extensions for security token exchange to enable the issuance and dissemination of credentials within different trust domains. This Identity Federation reference architecture uses WS-Trust as the open standard to establish trust relationships between security enclaves.

**WS-Federation** defines mechanisms for allowing disparate security enclaves to broker information on identities, identity attributes and authentication. It extends the basic model provided by WS-Security, WS-Trust, and WS-Security Policy by describing how the claim transformation model inherent in security token exchanges can enable richer trust relationships and advanced federation of services. This Identity Federation reference architecture uses WS-Federation to enable federation between enclaves and their embedded identity stores. WS-Trust was initially designed for web service interoperability and WS-Federation was built on top of WS-Trust to support authentication of users between enclaves.

**3. Common Schema**

All identity stores will follow the DoD common digital identity schema with the designated core attributes. The enclave's identity store does not have to internally store all the core attributes and metadata but it must support the concept of sending and receiving the standard core attributes with other Federation gateways.

**4. Follow Common Trust Framework**

Each enclave federation implementation will follow the DoD federation guidance.

1

2

## Appendix D - Attribute Based Access Control (ABAC)

### Policy-Based Authorization Services

The Policy-Based Authorization Services (PBAS) (top-middle rectangle with rounded corners of Figure D1) receives the access request for a user from a resource. Based on information from the Policy Store (PS), the PBAS analyzes the required user attributes for access to the resource and requests them from the identity and/or attribute provider. Based on policy applicable to a resource and a user's attributes, an access decision of either grant or deny is enforced at the Policy Enforcement Point (PEP).

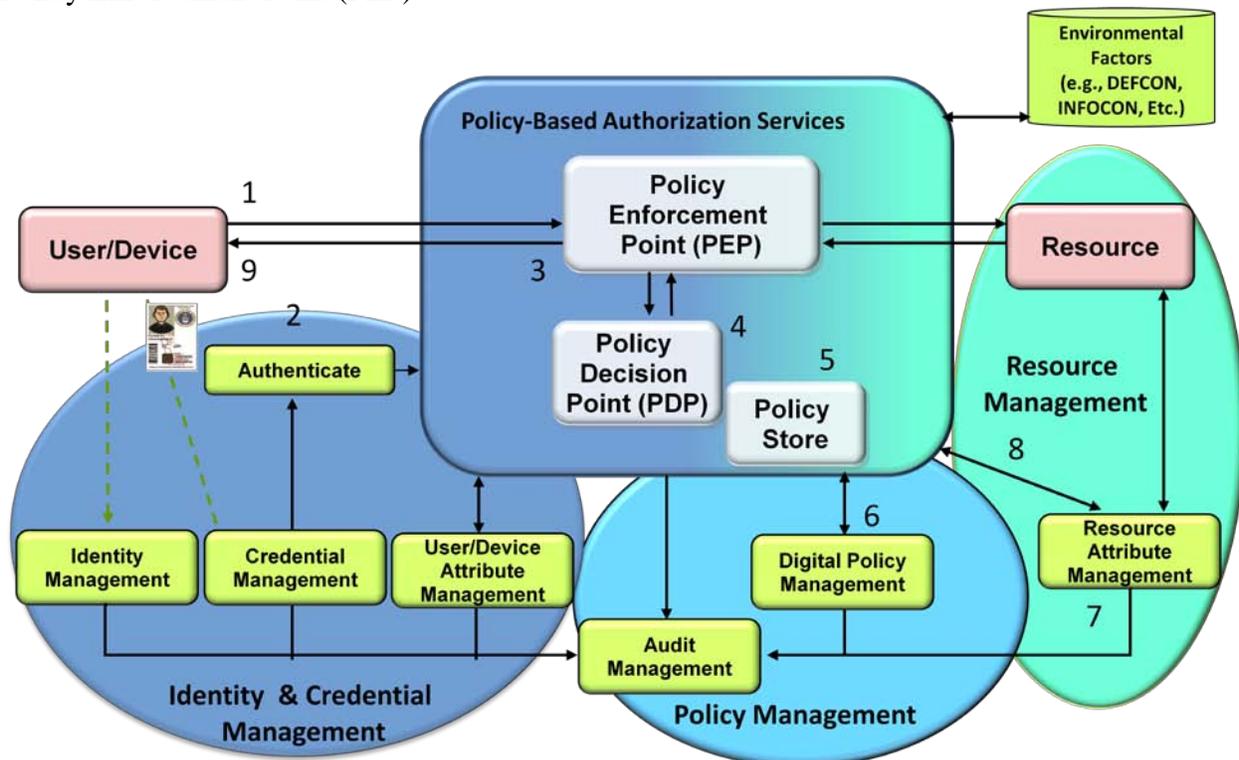


Figure D1 – Dynamic Policy-Based Access Control

Dynamic Policy-Based Access Control (DPBAC) does not require users to have pre-existing accounts with the relying party to gain access. It depends on user characteristics or attributes, current environmental conditions, and the access policies or rules of the resource being accessed. DPBAC requires implementation of Attribute Based Access Control (ABAC) and Digital Policy services at the enterprise level. A conceptual representation of a Dynamic Access Control model that reflects alignment with FICAM is shown in Figure D1 above.

### DPBAC Workflow

The concept of operations for DPBAC includes the following steps (marked 1 through 9 in Figure D1):

1. A user/NPE requests access to a resource.
2. The resource authenticates the user by electronically validating the credential presented.

- Unclassified -

3. Authentication is communicated to the Policy Enforcement Point (PEP).
4. The PEP provides the PDP with attributes of the resource for which access is requested .
5. Based on those resource attributes, the PDP requests the relevant policies from the Policy Store (PS).
6. The PS retrieves and provides the appropriate policies to the PDP.
7. Based on the policies, the PDP requests required attributes from the user attribute service.
8. The user attributes are compared to the access policy.

Access is either granted or denied as a result. In order to leverage attributes, they must be made available to the Policy Decision Point (PDP) and/or relying parties. To make attributes available, FICAM specifies the establishment of three services: Identity Attribute Discovery, Authoritative Attribute Exchange Service (AAES), and Backend Attribute Retrieval.

## Resource Management

A Resource is defined as a digital object, facility, service or person that is made accessible to other resources in the system or network. The Resource Management function (right side “oval” of Figure D1) is the binding of attributes to a resource that allow it to be digitally identified and defined. Resource owners are responsible for identifying and tagging their resources to facilitate DPBAC.

## In-Band and Out-of-Band Access Control

These steps and the functions that comprise them can be implemented using one of two approaches:

- 1) In-Band Management – Authentication and Authorization mechanisms are integrated into the accessed resource’s data/information exchange streams.
- 2) Out-of-Band Management - Authentication and Authorization mechanisms are implemented using separate data exchanges and are not imbedded in the accessed resource’s data/information exchange streams.

In most virtual or Cloud service environments, the Out-Of-Band model is more practical and will provide a higher degree of assurance of information control (i.e., the right data gets to the right person or entities, and not to unauthorized persons or entities). This is because Out-of-Band authentication requests and responses will precede the actual data/information transfers to the requesting entity.

## DoD Implementation Schedule

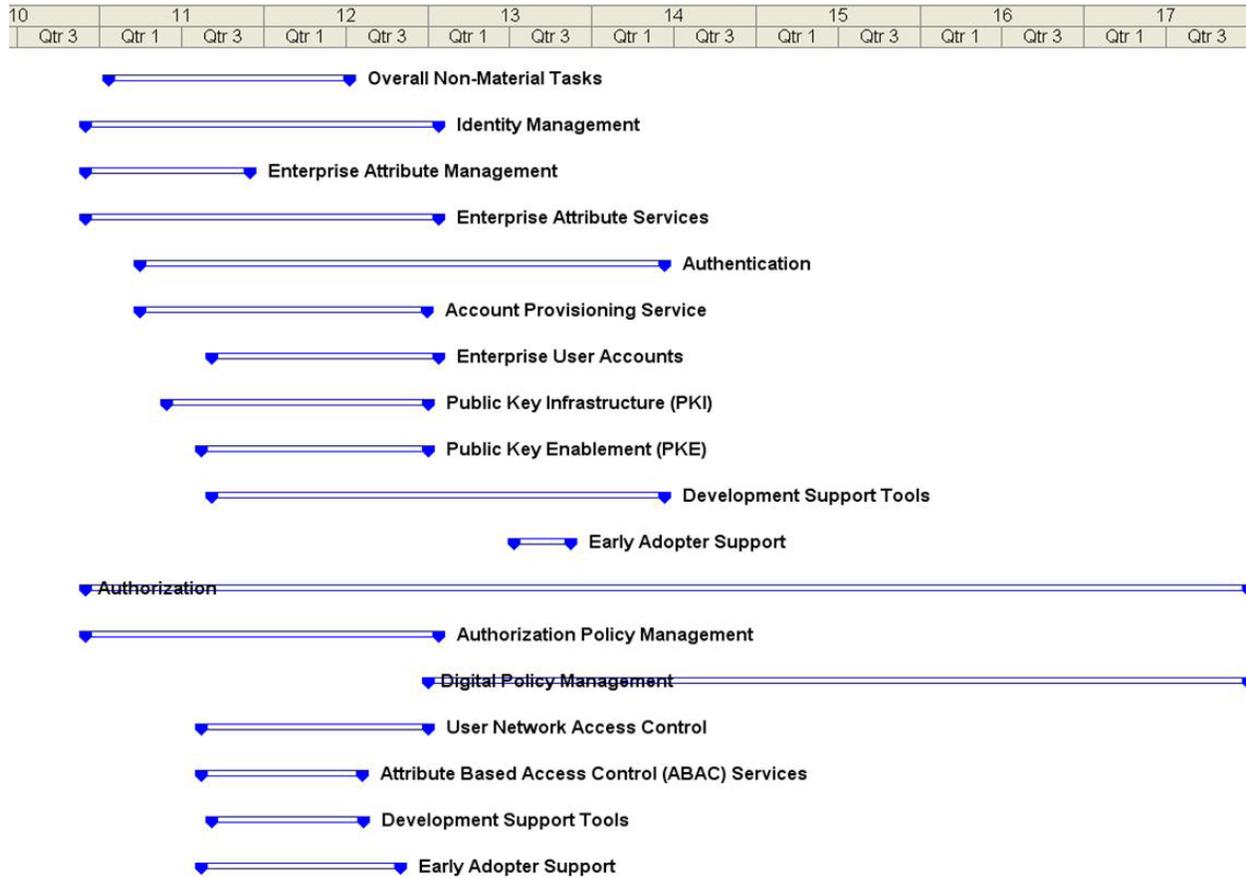


Figure D3 – DoD Information Technology Enterprise Strategy and Implementation Roadmap (ITESR) Initial Implementation Plan v1.0 - ICAM Implementation Schedule

## Appendix E - IdAM Security Management

### National Security Agency (NSA) Enterprise Security Management (ESM)

Developed by the NSA, the Enterprise Security Management (ESM) Context Review Documents describe the systems, processes, and personnel required to order, create, disseminate, modify, suspend, and terminate management controls to provision and operate information assurance (IA) services, processes, and devices across an enterprise. IdAM is subset of the IA capabilities outlined in the ESM framework (ref: Figure E1). ESM consists of a number of services that provide dynamic management and control of IA services, processes, and devices to optimize the enterprise for mission operations. There are nine ESM services that are described in Figure E1 include Identity Management, Credential Management, Attribute Management, Policy Management, Privilege Management, Authentication, Configuration Management, Audit Management, and Cryptographic Key Management. The ESM components together provide an efficient management process of IA services and enable a dynamic information sharing process.

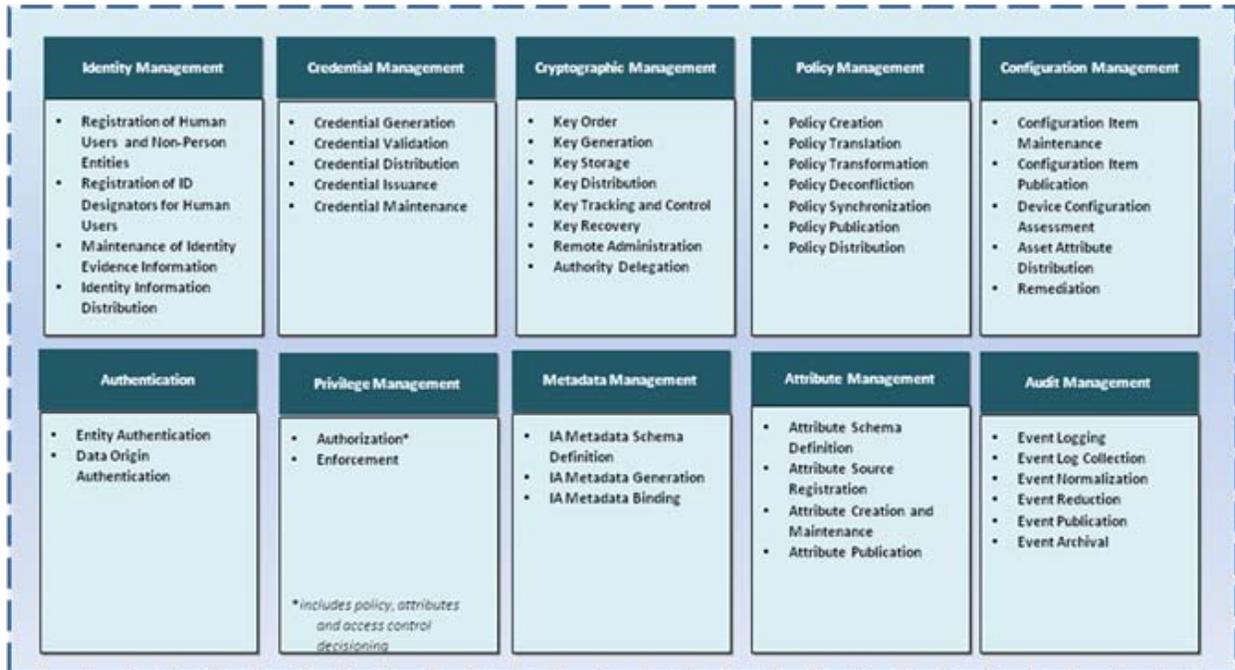


Figure E1 – NSA Enterprise Security Management Framework

## Appendix F – Technical Patterns Overview

### Active Directory (AD) Tactical Network Capability Maturity Model

This section introduces the concept of a tactical network capability maturity model and describes in detail the Active Directory Capability Maturity Model. A network capability maturity model allows the DoD to evaluate and determine the organizational structure and technological direction, and optimize the doctrine for establishing, operating and building up (maturing) a tactical network infrastructure in a theater of operations.

The Open Group Architecture Framework (TOGAF)<sup>1</sup> describes a Capability Maturity Model as a method an organization can use to gain control over and improve its IT-related development processes. The capability maturity model described in this section is based on the architecture framework provided by TOGAF and was developed with contributions from the U.S. Air Force Theater Deployable Communications Program Office.

The deployment and force projection processes are interrelated and overlap in the terms used. The phases for each process, their corresponding names, and description are provided here to clarify how each process related to the model. The deployment phases a unit goes through are described in Field Manual (FM) 3-35. The deployment phases described in this section are derived from FM 3-35, but with an orientation toward establishing a physical network and a network management and security infrastructure centered on Active Directory. The Table F1 provides the phase number and the corresponding name.

Phase	Name
0	Pre-Deployment Activities
1	Movement
2	Reception, Staging, Onward Movement, and Integration
3	Redeployment

**Table F1 – Deployment Planning Phases**

Force projection is the systematic and rapid movement of military forces in response to operational requirements, as demonstrated by the DoD's ability to alert, mobilize, rapidly deploy, and operate effectively anywhere on the globe<sup>2</sup>. Table F2 provides the Force Protection Process's Phases. The tactical network capability maturity levels are provided in Table F3.

<sup>1</sup> The Open Group Architecture Framework (TOGAF) Version 9, Chapter 51

<sup>2</sup> FM 3-35 Army Deployment and Redeployment

Phase	Name
0	Pre-Deployment
1	Mobilization
2	Deployment
3	Employment
4	Sustainment
5	Redeployment

Table F2 – Force Protection Process Phases

Level	Name
1	None
2	Initial
3	Under development
4	Managed
5	Enterprise under development
6	Enterprise Managed
7	Optimizing

Table F3 – Tactical Network Maturity Levels

The deployment planning phases provide a set of reference points and a timeline against which DoD can measure the network and Active Directory capability maturity levels. The maturity model should not be used to measure the level of success in establishing and operating a network. The model should be used to identify the capabilities and their characteristics that are missing or incomplete, and to help plan a roadmap to mature the theater's network and its internal AD operations.

The model described here is provided to illustrate the normal process operational forces use to implement, over time, a physical network infrastructure with operational and management capabilities that support units without internal network capabilities, and integrate in networks from units with internal networking capabilities.

Figure F4 is a capability maturity model for tactical networks and is provided to show how network operations and the supporting network operating system (NOS) centered on active

directory remains stable on the unclassified network, changes on the classified network as enterprise level operations are implemented, and on the theater network as it starts from the ground up as the Joint and Coalition forces are identified and organized over time as the theater matures.

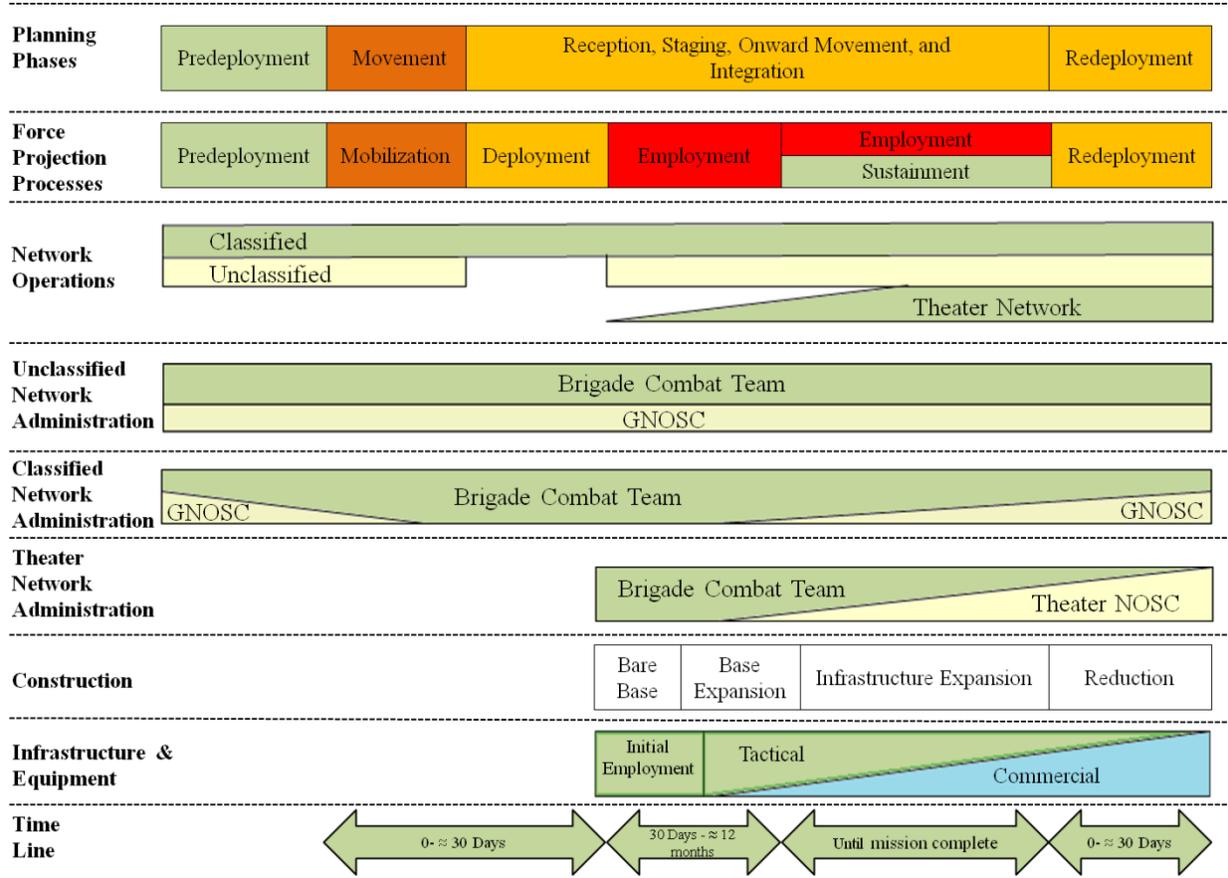


Figure F4 – Tactical Network Maturity Model Summary

## Tactical Network Operations

The classified network AD structure is expected to continuously operate and provide an operational security enclave with services through all phases. The unclassified AD structure is expected to operate through all phases except deployment. For immature theaters, the theater-specific AD structure may start up for the deployed unit after arrival in theater, as the theater-level operations are established and the deployed unit is integrated into the structure. For mature theaters, with an established AD structure, deploying units may join the theater AD forest upon arrival in the theater, or may opt to join the AD forest during the deployment phase to initiate early network operations with the theater command and deployed units.

Part of the network operations planning process is to determine how the AD forest structure should look. Should the BCT maintain its own forest or become a child domain in the tactical forest or an Organizational Unit (OU) under a domain? The decision tree, depicted in Figure F5, is provided to help determine the AD structure to be implemented.

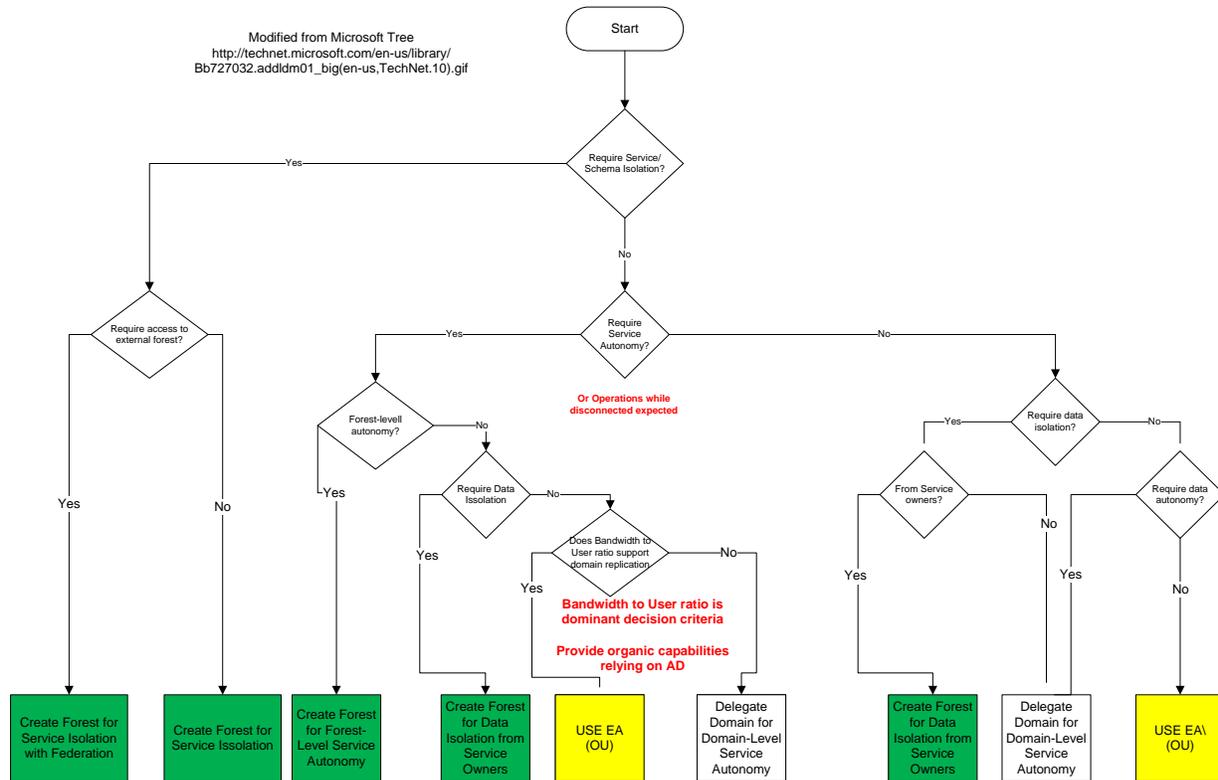


Figure F5 – Active Directory Structure Decision Tree

## Unclassified Network Administration

The administration of the AD structure and the applications and services operating inside the structure will be layered between the AD forest/domain operated by the Global Network Operations and Security Center (GNOSC) and the directory structure (Organizational Unit or child domain) delegated to the BCT/Task Force. The administration model of the AD forest, email and other enterprise services will follow the home station implementation, whether that be an independent AD forest and email structure or Service Component's (SC) AD forest that the post has migrated into. The BCT AD structure will be an integral component of the AD forest, with Brigade network administrators delegated authority to administrate the security principals (people and computers) assigned to the BCT.

To ensure a high level of training and operation experience is sustained by the BCT administrators, the AD and email components deployed in the BCT should be administrated by the BCT administrators while in garrison. The connection and integration with the home station provided enterprise services must be maintained, so the Soldier can continue to send/receive email and interact with other enterprise services. The unclassified AD and enterprise services deployed with the BCT are expected to remain with the Brigade during the deployment phase, but may not be connected to the network.

## Classified Network Administration

The BCT/Task Force AD forest with one domain and the services operating inside the enclave or that make up the enclave will be maintained and administrated by the units' internal network administrators. The intent is to have all Brigades maintain the same AD structure and services as

designated in this architecture, to ensure that upon deployment to a theater of operations or an exercise, the Warfighter will have the required services delivered in a secure environment. The teams' administrators will operate within the guidance provided by the GNOSC and will interface with the enterprise services like DNS.

Upon employment into an immature theater, the team is expected to employ the BCT AD forest to establish and perform independent network operations. This will provide a security enclave to operate the network within, which can protect the services and applications supporting the Warfighter. As the theater matures and the non-tactical transport layer becomes pervasive, and theater or SC-level operations are established, the teams' administrators will work with and follow the higher level administrators.

## Theater Network Administration

The BCT administrators will maintain and administrate the components required to join and integrate with a theater-level AD structure and corresponding services while in garrison. For an immature theater, the brigade administrators may be responsible for establishing the initial theater-specific AD structure and corresponding services. As the theater matures and the joint and coalition forces establish an AD structure and corresponding security enclave, the administrators in a brigade will turn over administration to the theater administrators.

## Construction and Network Infrastructure and Equipment

Construction of a physical network infrastructure normally follows the construction of a base. The level of technology and availability of capacity from the commercial network infrastructure in the theater of operations will drive the time line. Establishing a network infrastructure and the accompanying AD structure on a bare base will be based on the use of the inherent network components of the deployed tactical forces and the supporting signal forces. As the base facilities are improved, the internal base network is also improved and capabilities and capacities are expanded to provide better and more redundant services. As the theater matures, the infrastructure between bases will go from operations utilizing tactical signal components to the use of commercial assets, freeing up tactical equipment for new deployments. As the theater enters the reduction phase, network operations and management will continue the phase-out of tactical transport and network management assets and use greater amounts of commercial assets. The use of the theater AD structure and the aligned management structure will normally be commercialized as part of the infrastructure expansion. Management of the operational forces' AD structure will continue to be administrated and maintained by the tactical forces.

## Deployment Planning Phases

An SC's deployment planning process and phases are built upon the DoD process, but do deviate in that the planning phases are a part of each phase, rather than a separate phase executed before the others. The deployment planning phases described below are a synopsis of the guidance provided in FM 3-35.

### Pre-Deployment Phase

During the pre-deployment phase, units plan for various contingencies and hone their deployment skills. When units train and exercise their pre-deployment activities, they become second nature and are accomplished efficiently. Units should be trained in NetOps; personnel

- Unclassified -

must be nearly 100 percent compliant with network operations orders and have in place a process to move from their current AD environment to another one.

## Movement Phase

At the installation staging areas, unit movement data is verified and equipment is inspected and configured for movement. The installation coordinates and/or provides support to assist the deploying force by using non-deploying units, installation resources, or contracted support. The Mission Support Element is a Table of Distribution and Allowances (TDA)-augmentation capability used by the mission commander to develop and maintain the deployment support plan. Deploying units immediately configure for deployment, reduce/prepare vehicles, computers and aircraft for movement, properly stow and tie down secondary loads, construct pallets and prepare the required documentation.

### Reception, Staging, Onward Movement, and Integration (RSOI) Phase

RSOI is the process that delivers combat power to the Joint Force Commander (JFC) in the operational theater through the expeditious processing of personnel and equipment throughout the deployment pipeline. RSOI support, whether provided by theater support contracts, external support contracts, regionally available commercial host nation support, and/or military assets, must be sufficient to immediately support the arrival of deploying units. Effective RSOI matches personnel with their equipment, minimizes staging and sustainment requirements while transiting the PODs (Ports of Debarkation), and begins onward movement as quickly as possible. A plan to accomplish integration and maintain combat readiness must be understood, trained, and ready to implement upon arrival.

### Redeployment Phase

Redeployment involves the return of personnel, equipment, and materiel to home and/or demobilization stations and is considered an operational movement critical in reestablishing force readiness. The same elements that operate and manage the theater distribution system during deployment and sustainment will usually perform support roles during redeployment. Redeployment planning is an integral part of employment planning and should be coordinated with mission termination or transition plans.

## Force Projection Processes and Phases

The planning required for each phase is similar for the three tactical networks (classified, unclassified, and Theater) as they are each based on the same technologies. Any minor differences for each of the three tactical networks' AD architectures will be called out and described as appropriate in each sub-section.

### Pre-Deployment

The train-as-you-work philosophy drives tactical active directory operational capabilities for each of the networks. Prior to mobilization and deployment, the focus is on day-to-day operations with planning, training and sustainment in support of preparation and readiness for future operations. The BCT's classified AD-based enclave operations may be minimally manned with at least two domain controllers on line to keep the directory current and to provide infrastructure services. The unclassified AD brigade-level enclave maybe operated in conjunction with and as an extension to the Division's or post's AD structure structure if the post

has migrated into the GNEC AD structure. A Theater AD enclave is normally not operational in the pre-deployment phase unless the brigade is stationed in the Theater.

### Mobilization

Mobilization is the process by which the armed forces in whole or part are brought to a state of readiness for war or national emergency. The DoD assembles and organizes resources to support national objectives. Mobilization includes activating all or part of the reserve components, and assembling and organizing personnel, supplies and materiel (see Joint Publication (JP) 4-05; FM 3-35).

The classified and unclassified networks should operate in the tactical environment the same as they did prior to mobilization. During mobilization, the deploying unit initiates planning for Theater-specific network AD operations with the responsible GCC and task force command.

### Deployment

Deployment is the movement of forces and materiel from their point of origin to the area of operations (AO). Deployment will impact each of the network's active directory operations the same way in changes to trusts with other forests, the DNS structure, and subnet structure that impacts site designations. Deployment may include the movement to a training center and integration with or interoperability with the center's active directory structure. Strategic and mobile capabilities are provided en route by area support communications units/elements, the deploying unit, the joint forces and commercial assets as appropriate. The AD architecture must be capable of supporting for each of the networks AD structure:

- Interfacing with the AD forest at the training center.
- Joining or interfacing with the AD forest at the point of entry into the theater.
- Interfacing with the area support communications unit's AD and transport service operations encountered in route to the operations area.

All tactical networks of deployed forces in support of Command and Control (C2) to the operational units will be under the operational control (OPCON) of the geographic combatant command (GCC). The combination of the Theater network and deployed force's tactical network comprises the Theater network of the GCC. The GCC's Theater network is organized into theater-level enclaves consisting of the systems and devices owned by the deployed forces which connect directly to the Global Information Grid (GIG) and Defense Information Systems Network (DISN). The Theater network will provide deployed tactical forces in-theater access to the DISN and theater-specific information services. The Army's portion of the GIG is called LandWarNet and includes the classified, unclassified, and Theater networks.

The AD structure for all three networks must be capable of independent operations. The three networks may operate within the same transport mechanism but are logically separated from each other. The AD architecture and operations on each network environment must support not only the connection and interfacing with the network infrastructure at each location, but also the capability to disconnect from the appropriate network infrastructure in support of a deployment and move to a new AO and the next set of network environments.

The unclassified and theater-specific AD structures will normally not be implemented or operated during the deployment phase. The classified tactical AD structure and its supporting services (such as Exchange, DNS and IP addressing) are expected to provide services to the

combat team during each phase and to operate independently or interface with the enterprise services in each AO during deployment.

### Employment

Employment is the conduct of operations to support a Joint Forces Command (see JP 3-0 series; FM 100.7; FM 4-01.011). Employment encompasses a wide array of operations, including, but not limited to:

- Entry operations (opposed or unopposed).
- Shaping operations (lethal and non-lethal).
- Decisive operations (combat or support).
- Post-conflict operations (prepare for follow-on missions or redeployment).

The AD structure and architecture are essential to provide a security enclave the combat team can securely operate within, to support command and control, situational awareness and Joint fires to accomplish the initial entry or assigned mission into the area of responsibility (AOR). Tactical and on-the-move (OTM) AD capabilities are provided by internal BCT forces.

The unclassified AD and supporting network operations and services are not mission-critical and will be set up and operated as sufficient transport services and connectivity become available. The theater AD structure and services will be operated based upon guidance from the theater COCOM network operations center.

### Sustainment

Sustainment involves providing and maintaining levels of personnel and materiel required to sustain the operation throughout its duration. It is essential to generating combat power. Transport and network infrastructure capabilities are provided by a combination of strategic, tactical and commercial assets, as the theater matures, the percentage of commercial assets are expected to increase. The AD architecture for each of the networks should not require any change, as the transport layer provider morphs over time as the theater matures.

**Stability and Support Operations (SASO):** SASO military operations are designed to support social, political, security, informational and economic stability within the AO and/or area of interest. Major combat operations have ceased, but minor combat may continue. Units are in a stationary-base environment and this allows the realignment of networks and the BCT's AD structure with the theater AD structure and operations. The tactical networks and corresponding AD structure will continue to provide the primary services to maintain a security enclave capable of independent operations and supporting ongoing combat operations in the AO. The AD architecture must be capable of providing services and supporting operations if the combat team is deployed to a new AO. The BCT and encompassing task force must be capable of responding to a new mission and moving into another employment phase at any time.

### Redeployment

Redeployment is the process by which units and materiel re-posture themselves in the same theater; transfer forces and materiel to support another JFC's operational requirements; or return personnel, equipment, and materiel to the home or demobilization station upon completion of the mission. The unclassified AD structure, if operational, is expected to change configuration to

continue to interface with the home station or DoD enterprise structure. The theater AD implementation is expected to be closed down prior to the unit's departure from the theater.

## Tactical Network Capability Maturity Levels

The characteristics, criteria and other factors that can be used to measure and describe an effective tactical network implementation at each phase are provided and described in this section. The model described in Table F6 is provided to illustrate the normal process operational forces implement, over time, in an operational network and a NOS structure to operate, manage, and defend the network and the resources contained within it.

This model describes:

1. The processes required to establish a tactical network and NOS infrastructure.
2. The phases and changes to the tactical network and infrastructure as the theater matures.
3. A framework that organizations can use to measure the level of network maturity.

An understanding of the model is required to better manage and guide the changes in the network infrastructure and the operations on top of the infrastructure as the Theater matures. The model provides a yardstick that can be used to measure the level of network infrastructure maturity and a framework within which the DoD can manage improvement efforts while ensuring tactical capabilities are not lost.

Level	Name	Description
1	None	No network operations
2	Initial	Ad hoc operations with few, if any, defined processes, with isolated unit-based local area networks with no access to the wide area networks.
3	Under development	Ad hoc operations with few defined processes established to operate the network, such as IP addressing, DNS and network time. Isolated tactical unit-operated local area networks with access over limited bandwidth satellite connections to the wide area network (SIPRNet).
4	Managed	Processes are in place for management, security, and engineering activities, such as patch management, that are documented, standardized, and integrated with the discipline to repeat success as new units arrive in Theater. Expanded local area networks with two or more units participating, with access over limited bandwidth satellite connections to the wide area networks (NIPRNet & SIPRNet).

Level	Name	Description
5	Enterprise under development	Limited theater wide area network with ad hoc processes in place for connecting established local area networks into a theater wide area network. Limited terrestrial-based network backbone and expanded satellite bandwidth connections to the wide area networks (NIPRNet & SIPRNet). Limited automation of wide area network management processes.
6	Enterprise Managed	Theater-wide area network with processes in place for connecting new units and deprecation of departing units. Stable terrestrial-based network backbone with connections to the wide area networks (NIPRNet & SIPRNet). Processes are in place for automation of network management and support processes. Limited COOP capability for enterprise services.
7	Optimizing	Network operations are monitored with detailed measures in place to collect and analyze network operations and bandwidth utilization. Continuous process improvement is enabled. Theater is part of global terrestrial-based backbone with redundant connections and bandwidth. Detailed and measured COOP for enterprise services.

Table F6 – Network Capability Maturity Model Description

A more detailed description of the capabilities that exist or do not exist at each level is provided in Table F7 below.

<b>Level 1 – None</b>
<b>No operational local area or wide area networks</b>
<b>No defined processes</b>

<b>Level 2: Initial</b>
<b>Isolated unit terrestrial based local area networks, utilizing only internal network assets</b>
<b>Few, if any, defined processes, such as IP address management, DNS, network time, or policy management</b>
<b>No external wide area network access (NIPRNet, SIPRNet)</b>

<b>Level 3: Under development</b>
<b>Ad hoc SIPRNet network operations between two or more units, with few defined processes</b>
<b>Limited external SIPRNet network connection through satellites</b>

- Unclassified -

<b>No NIPRNet connectivity</b>
<b>Independently operating unit and Task Force Active Directory forests</b>
<b>No cross forest or domain trusts</b>
<b>Tactical unit's Active Directory name space registered in SIPRNet DNS</b>

<b>Level 4: Managed</b>
<b>Processes for management, security, and engineering activities such as patch management, common group policy and interface</b>
<b>Expanded local area networks that contain two or more units</b>
<b>Limited use of commercial network facilities</b>
<b>Process and discipline necessary to repeatedly bring new units into the theater SIPRNet environment</b>

<b>Level 5: Enterprise under development</b>
<b>Stationary tactical units have SIPRNet connectivity with most other stationary units</b>
<b>Limited operational terrestrial-based network backbone</b>
<b>Augmentation of unit internal satellite bandwidth capability</b>
<b>Ad hoc automation of theater wide area network management processes</b>
<b>Ad hoc NIPRNet connectivity</b>
<b>Limited network intrusion capability</b>

<b>Level 6: Enterprise Managed</b>
<b>Theater wide area network with processes for connecting new units and deprecation of departing units</b>
<b>Theater wide network backbone with connectivity to stationary units</b>
<b>Automation of network management and operational processes</b>
<b>Limited theater network backbone connections to SIPRNet and NIPRNet</b>
<b>Limited COOP of enterprise services</b>
<b>Network intrusion detection capability</b>

<b>Level 7: Optimizing</b>
<b>Theater network operations are monitored with detailed measures in place to collect and analyze network operations and usage</b>
<b>Continuous process improvement is in place</b>
<b>Theater is an integral part of the global terrestrial based backbone with redundant connections and bandwidth</b>
<b>Detailed and measured COOP for enterprise services</b>

Table F7 – Network Capability Maturity Model Description