



U.S. Army – Identity and Access Management (IdAM) Reference Architecture (RA) v2.0

Version 2.0

Executive Summary

The Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Implementation Roadmap (ESR) Initial Implementation Plan v1.0, dated 6 September 2011, 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, DoD, and the DoD Service Components (SCs) (e.g., Army, Air Force, Navy, Marines, Intelligence Community (IC)), have developed and deployed Identity, Credential and Access Management (ICAM) services, of which IdAM services are a subset, in a stovepipe 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” via Public Key Infrastructure (PKI) technology, capability gaps remain between how authenticated information “requesters” or “consumers” are identified and to which resources (i.e., data, facilities, networks, equipment) they should be allowed “authorization”. The challenge is to find a way for all DoD and SC IdAM service capabilities and infrastructures to accommodate rapidly changing identity attributes, roles and access accounts as operational phases and environments change (i.e., Generating Force, deployed tactical, non-tactical).

While this document has been called “Business Rules-Based” Army IdAM Reference Architecture (RA), it establishes the core set of functional and technical boundaries for both Army and DoD enterprise IdAM services, including those directly supporting the specialized operations within the other SCs. It outlines a set of guiding principles and business rules as a framework for the generic functional guidelines that are required to define specific IdAM capability components. These components can then be used to specify and diagram any IdAM infrastructures, solution-level architectures, designs, service offerings or their required materiel solutions. This document specifies the essential technical and regulatory standards that must be followed, and identifies models that, if applied across all of the possible DoD operating environments, will increase overall infrastructure interoperability and streamline acquisition processes, resulting in reduced cost and more rapid deployment of services.

This IdAM RA v2.0 supersedes Army IdAM RA v1.0, and provides Army leadership and their supporting organizations expanded architectural guidance to support the design, development, deployment, transition to and operational management of a Joint Information Environment (JIE) IdAM service framework and infrastructure. It also provides guidance that is valuable to any DoD SC and its organizations following common service models to define components or service(s) “containers” that can be applied to any implementation to meet the requirements of any operating environment.

BLOHM.GARY.W.1228949589

Digitally signed by BLOHM.GARY.W.1228949589
DN: cn=BLOHM.GARY.W.1228949589,
ou=DoD, o=US Government, ou=USDA,
c=US

Mr. Gary W. Blohm

Director – CIO/G-6, Army Architecture Integration Center (AAIC)

Date

Table of Contents

EXECUTIVE SUMMARY	I
1 STRATEGIC PURPOSE.....	1-1
1.1 Introduction.....	1-1
1.2 End State Vision	1-2
1.3 Background	1-5
1.4 Benefits	1-6
1.5 Intended Audience and Use.....	1-6
1.6 Alignment with DoD Enterprise Architecture and Key IdAM Strategies.....	1-7
1.7 Scope/Organization	1-8
1.8 Major Considerations	1-9
2 VOCABULARY.....	2-1
2.1 Access Types.....	2-1
2.1.1 Logical Access Control	2-1
2.1.2 Physical Access Control	2-1
2.1.3 Entities.....	2-1
2.1.3.1 Person Entity (PE).....	2-1
2.1.3.2 Non-Person Entity (NPE).....	2-1
2.1.3.3 Requester.....	2-2
2.1.3.4 Resource.....	2-2
2.2 Reference Architecture Evolution.....	2-2
2.2.1 RA Incremental Development and Versioning.....	2-2
2.2.2 Updates, Additions and Limitations	2-3
2.2.3 Key IdAM Architectural Definitions.....	2-4
2.2.3.1 Rationale	2-4
2.2.3.2 Service Offerings Baseline.....	2-6
2.2.3.3 Component Categorization.....	2-6
2.2.3.4 IdAM Component Definitions	2-10
3 GUIDING PRINCIPLES AND BUSINESS RULES.....	3-1
3.1 Service Area/Services to Guiding Principles and Business Rules Mapping	3-1
3.2 RA Versioning versus Services and Infrastructure Component Delivery Timeline	3-3
3.3 Specifications	3-4

3.3.1	(P1) Principle 1 – Unique Identity and Credentials	3-4
3.3.1.1	(P1/R1) Business Rule 1 – Person Entity (PE) Unique Identifier	3-4
3.3.1.2	(P1/R2) Business Rule 2 – Allowed Identities	3-5
	P1/R2 Technical Standards Profile	3-5
	P1/R2 Policy/Regulation Profile	3-5
3.3.1.3	(P1/R3) Business Rule 3 – Persona Life-cycle Management	3-6
	P1/R3 Technical Standards Profile	3-6
	P1/R3 Policy/Regulation Profile	3-6
3.3.1.4	(P1/R4) Business Rule 4 – Identity Data Integrity	3-7
	P1/R4 Technical Standards Profile	3-7
	P1/R4 Policy/Regulation Profile	3-7
3.3.1.5	(P1/R5) Business Rule 5 – Person Entity (PE) - Identity Data Discoverability	3-7
	P1/R5 Technical Standards Profile	3-8
	P1/R5 Policy/Regulation Profile	3-8
3.3.1.6	(P1/R6) Business Rule 6 – Non-Person Entity (NPE) - Identity Data Discoverability	3-8
	P1/R6 Technical Standards Profile	3-9
	P1/R6 Policy/Regulation Profile	3-9
3.3.1.7	(P1/R7) Business Rule 7 – Identity Data Conformance	3-9
	P1/R7 Technical Standards Profile	3-9
	P1/R7 Policy/Regulation Profile	3-9
3.3.1.8	(P1/R8) Business Rule 8 – Authentication and Authorization Service Provisioning	3-10
	P1/R8 Technical Standards Profile	3-10
	P1/R8 Policy/Regulation Profile	3-10
3.3.1.9	(P1/R9) Business Rule 9 – Enterprise Identity Attribute Utilization	3-11
	P1/R9 Technical Standards Profile	3-11
	P1/R9 Policy/Regulation Profile	3-11
3.3.2	(P2) Principle 2 – Authoritative Identity Data Source	3-12
3.3.2.1	(P2/R1) Business Rule 1 – Authoritative Person Entity (PE) Identity Attribute Data	3-12
	P2/R1 Technical Standards Profile	3-13
3.3.2.2	(P2/R2) Business Rule 2 – Authoritative Non-Person Entity (NPE) Identity Attribute Data	3-13
	P2/R2 Policy/Regulation Profile	3-13
3.3.2.3	(P2/R3) Business Rule 3 – Common Access Card (CAC) Usage	3-13
	P2/R3 Technical Standards Profile	3-14
3.3.2.4	(P2/R4) Business Rule 4 – Resource Account Provisioning Service (APS)	3-14
	P2/R4 Technical Standards Profile	3-15
	P2/R4 Policy/Regulation Profile	3-15
3.3.2.5	(P2/R5) Business Rule 5 – Adding Core Person Entity (PE) Identity Attributes	3-15
	P2/R5 Technical Standards Profile	3-16
3.3.2.6	(P2/R6) Business Rule 6 – Adding Core Non-Person Entity (NPE) Identity Attributes	3-16
	P2/R6 Technical Standards Profile	3-17
3.3.2.7	(P2/R7) Business Rule 7 – Non-Person Entity (NPE) Resource Data Federation	3-17
	P2/R7 Technical Standards Profile	3-17
3.3.2.8	(P2/R8) Business Rule 8 – Directory Information Updates	3-18
	P2/R8 Technical Standards Profile	3-18
3.3.3	(P3) Principle 3 – Person Entity (PE) and Non-Person Entity (NPE) Identification	3-19
3.3.3.1	(P3/R1) Business Rule 1 – Mobile/Edge Platforms/Devices	3-19
	P3/R1 Technical Standards Profile	3-20
	P3/R1 Policy/Regulation Profile	3-20
3.3.3.2	(P3/R2) Business Rule 2 – Mobile Device Binding	3-20
	P3/R2 Technical Standards Profile	3-20
3.3.4	(P4) Principle 4 – Global Directory Services for Enterprise Services	3-21
3.3.4.1	(P4/R1) Business Rule 1 – Global Address List (GAL) Distribution	3-21
	P4/R1 Technical Standards Profile	3-22

3.3.4.2	(P4/R2) Business Rule 2 – Global Address List (GAL) Views	3-22
	P4/R2 Technical Standards Profile	3-22
3.3.4.3	(P4/R3) Business Rule 2 – Global Address List (GAL) Data Schema	3-22
	P4/R3 Technical Standards Profile	3-23
3.3.4.4	(P4/R4) Business Rule 4 – Local Offline Address Book (OAB) Availability	3-23
	P4/R4 Technical Standards Profile	3-24
3.3.4.5	(P4/R5) Business Rule 5 – Directory/Global Address List (GAL) Information Concurrency	3-24
	P4/R5 Technical Standards Profile	3-24
3.3.5	(P5) Principal 5 – Authentication and Authorization	3-25
3.3.5.1	(P5/R1) Business Rule 1 – Authentication and Authorization Scope	3-25
	P5/R1 Technical Standards Profile	3-25
3.3.5.2	(P5/R2) Business Rule 2 – Identity Service For Tactical Edge.....	3-25
	P5/R2 Technical Standards Profile	3-26
3.3.5.3	(P5/R3) Business Rule 3 – Global Information Resource Access.....	3-26
	P5/R3 Policy/Regulation Profile	3-27
3.3.5.4	(P5/R4) Business Rule 4 – Access and Policy Security	3-27
	P5/R4 Technical Standards Profile	3-27
3.3.5.5	(P5/R5) Business Rule 5 – Availability of DoD Enterprise Authentication and Authorization Services	3-27
	P5/R5 Technical Standards Profile	3-28
	P5/R5 Policy/Regulation Profile	3-28
3.3.5.6	(P5/R6) Business Rule 6 – Availability of Army (Non-DoD Enterprise) Authentication and Authorization Services	3-28
	P5/R6 Technical Standards Profile	3-28
3.3.6	(P6) Principle 6 – Dynamic Access Policy Management	3-29
3.3.6.1	(P6/R1) Business Rule 1 – Policy Management Service Scope.....	3-29
3.3.6.2	(P6/R2) Business Rule 2 – Standard Attribute Model	3-29
3.3.6.3	(P6/R3) Business Rule 3 – Standard Access Policies	3-30
3.3.6.4	(P6/R4) Business Rule 4 – Policy Change Management Responsibility	3-30
3.3.6.5	(P6/R5) Business Rule 5 – Policy Attribute Validation	3-31
3.3.7	(P7) Principle 7 – Access to Data, Services and Applications.....	3-32
3.3.7.1	(P7/R1) Business Rule 1 – Information Resource Types	3-32
3.3.7.2	(P7/R2) Business Rule 2 – Logical NPE Layered Logical Access Control	3-33
	P7/R2 Technical Standards Profile	3-33
3.3.7.3	(P7/R3) Business Rule 3 – Public Key Infrastructure (PKI) Based Authentication.....	3-33
	P7/R3 Policy/Regulation Profile	3-34
3.3.7.4	(P7/R4) Business Rule 4 – Data Resource Identification.....	3-34
3.3.7.5	(P7/R5) Business Rule 5 – Rules Engine (RE) Personally Identifiable Information (PII) Attribute Exposure	3-35
3.3.7.6	(P7/R6) Business Rule 6 – Data Tagging Development	3-36
	P7/R6 Technical Standards Profile	3-36
	P7/R3 Policy/Regulation Profile	3-36
3.3.7.7	(P7/R7) Business Rule 7 – Standardized Policy Languages	3-37
	P7/R7 Technical Standards Profile	3-37
3.3.7.8	(P7/R8) Business Rule 8 – Access Policy Data Tagging Metadata Standards.....	3-37
	P7/R8 Technical Standards Profile	3-37
	P7/R8 Policy/Regulation Profile	3-37
3.3.8	(P8) Principle 8 – Physical Access	3-38
3.3.8.1	(P8/R1) Business Rule 1 – Non-Person Entity (NPE) Unique Identifier	3-38
	P8/R1 Technical Standards Profile	3-38
3.3.8.2	(P8/R2) Business Rule 2 – Physical Access Control Policies	3-38
	P8/R2 Technical Standards Profile	3-38
3.3.8.3	(P8/R3) Business Rule 3 – Non-Person Entity (NPE) Attribute Verification	3-38

P8/R3 Technical Standards Profile	3-39
3.3.8.4 (P8/R4) Business Rule 4 – Facilities Attributes Management	3-39
P8/R4 Technical Standards Profile	3-39
3.3.8.5 (P8/R5) Business Rule 5 – Common Access Card (CAC) Credential Mechanism.....	3-39
P8/R5 Technical Standards Profile	3-39
3.3.8.6 (P8/R6) Business Rule 6 – Common Access Card (CAC) Enrollment	3-39
P8/R6 Technical Standards Profile	3-39
3.3.8.7 (P8/R7) Business Rule 7 – Layered Physical Access Control for Subclass Type 1 Physical NPEs 3-40	
P8/R7 Technical Standards Profile	3-40
3.3.8.8 (P8/R8) Business Rule 8 – Layered Physical Access Control for Subclass Type 2 Physical NPEs 3-40	
P8/R8 Technical Standards Profile	3-40
3.3.8.9 (P8/R9) Business Rule 9 – Physical Access Control – Subclass Type 1 NPE Asset Naming	3-40
P8/R9 Technical Standards Profile	3-41
3.3.8.10 (P8/R10) Business Rule 10 – Physical Access Control – Subclass Type 2 NPE Asset Naming	3-41
P8/R10 Technical Standards Profile	3-41
3.3.9 (P9) Principle 9 – General Identity and Access Management (IdAM) Security Policy.....	3-42
3.3.9.1 (P9/R1) Business Rule 1 – Identity Attribute Data Validation	3-42
P9/R1 Technical Standards Profile	3-42
P9/R1 Policy/Regulation Profile	3-42
3.3.9.2 (P9/R2) Business Rule 2 – Authorization Service Scope.....	3-42
P9/R2 Technical Standards Profile	3-42
P9/R2 Policy/Regulation Profile	3-42
3.3.9.3 (P9/R3) Business Rule 3 – Enterprise Information Sharing.....	3-43
P9/R3 Policy/Regulation Profile	3-43
3.3.9.4 (P9/R4) Business Rule 4 – Information Resource Authentication Frequency	3-43
P9/R4 Technical Standards Profile	3-43
3.3.9.5 (P9/R5) Business Rule 5 – Cross-Domain Security	3-43
P9/R5 Technical Standards Profile	3-44
P9/R5 Policy/Regulation Profile	3-44
3.3.9.6 (P9/R6) Business Rule 6 – Information Resources Availability	3-44
3.3.9.7 (P9/R7) Business Rule 7 – Information/Data Resources Protection	3-44
P9/R7 Technical Standards Profile	3-44
P9/R7 Policy/Regulation Profile	3-44
3.3.9.8 (P9/R8) Business Rule 8 – DoD Enterprise Trust Management	3-45
P9/R8 Technical Standards Profile	3-45
P9/R8 Policy/Regulation Profile	3-45
3.3.9.9 (P9/R9) Business Rule 9 – Alternate Authentication Mechanisms (Non-CAC/Token).....	3-45
P9/R9 Technical Standards Profile	3-45
P9/R9 Policy/Regulation Profile	3-45
3.3.9.10 (P9/R10) Business Rule 10 – Data Encryption	3-46
P9/R10 Technical Standards Profile	3-46
P9/R10 Policy/Regulation Profile	3-46
3.3.9.11 (P9/R11) Business Rule 11 – SHA-256: Secure Hashing Algorithm Migration.....	3-46
P9/R11 Technical Standards Profile	3-46
3.3.10 (P10) Principle 10 – Single Sign-On (SSO) and Reduced Sign-On (RSO)	3-47
3.3.10.1 (P10/R1) Business Rule 1 – SSO and RSO Directory Data Population.....	3-47
P10/R1 Technical Standards Profile	3-47
3.3.10.2 (P10/R2) Business Rule 2 – Electronic Data Interchange Personal Identifier (EDI-PI)	3-47
P10/R2 Technical Standards Profile	3-48
3.3.10.3 (P10/R3) Business Rule 3 - SSO and RSO Services Availability	3-48
P10/R3 Technical Standards Profile	3-48

P10/R3 Policy/Regulation Profile	3-48
3.3.11 (P11) Principle 11 – Network Access Controls	3-49
3.3.11.1 (P11/R1) Business Rule 1 – Authorization Policy Network Attributes	3-49
P11/R1 Technical Standards Profile	3-49
P11/R1 Policy/Regulation Profile	3-49
3.3.11.2 (P11/R2) Business Rule 2 – Network-Connected Device Authentication	3-49
P11/R2 Technical Standards Profile	3-50
3.3.11.3 (P11/R3) Business Rule 3 – Disconnected and/or Network-Disadvantaged Authentication	3-50
P11/R3 Technical Standards Profile	3-51
P11/R3 Policy/Regulation Profile	3-51
3.3.11.4 (P11/R4) Business Rule 4 – Network Gateway Authentication and Authorization	3-51
P11/R4 Technical Standards Profile	3-52
3.3.12 (P12) Principle 12 – Monitoring and Reporting	3-53
3.3.12.1 (P12/R1) Business Rule 1 – Auditing Services	3-53
P12/R1 Technical Standards Profile	3-53
P12/R1 Policy/Regulation Profile	3-53
3.3.12.2 (P12/R2) Business Rule 2 – Identity and Access Management (IdAM) Infrastructure- Monitoring/Reporting	3-53
P12/R2 Technical Standards Profile	3-53
P12/R2 Policy/Regulation Profile	3-53
APPENDIX A - VOCABULARY (INTEGRATED DICTIONARY – AV-2)	54
APPENDIX B - TECHNICAL POSITIONS AND PATTERNS	64
Technical Profile Tables	64
Technical Profile: Digital Certificate (PKI)	64
Technical Profile: Key Exchange	64
Technical Profile: Cryptographic Key Management	64
Standard Title	64
Technical Profile: Cryptography Algorithms	64
Standard Title	64
Technical Profile: Attribute Management Services	65
Standard Title	65
Related Principle & Business Rule	65
Technical profile: Authentication Management Services	65
Standard Title	65
Technical profile: Authoritative Attribute Exchange Service	65
Standard Title	65
Technical Profile: Biometric Validation	66
Standard Title	66
Technical Profile: Common Access Card (CAC)	66
Standard Title	66
Technical Profile: Credential Management	67
Standard Title	67
Technical Profile: Encryption & Decryption	67
Standard Title	67
Technical Profile: Firewall Protection	67
Standard Title	67
Technical Profile: Identity Based Access Control (IBAC)	68
Standard Title	68

Technical Profile: Identity Management	68
Standard Title	68
Technical Profile: Identity Proofing	68
Standard Title	68
Technical Profile: Information Assurance	69
Standard Title	69
Technical Profile: IPSec Advanced Encryption	69
Standard Title	69
Standard Title	69
Technical Profile: IPSec Mechanisms	69
Standard Title	69
Technical Profile: Key Management	69
Standard Title	69
Technical Profile: Global Directory Services for Enterprise Services	70
Standard Title	70
Technical Profile: Policy in Authentication	70
Standard Title	70
Technical Profile: Policy in Credentialing	70
Standard Title	70
Technical Profile: Secure Shell	71
Standard Title	71
Technical Profile: Web Services Security	71
Standard Title	71
Technical Profile: Standardized Policy Languages	71
Standard Title	71
Army IdAM RA to Army Regulation (AR) 25-2 Mapping	72
Pattern Views for Business Rules (by Business Rule)	73
P1/R1 PE Unique Identifier (Connected)	73
P1/R1 PE Unique Identifier (Disconnected)	74
P1/R8 Authentication and Authorization Service Provisioning	75
P2/R4 Resource Account Provisioning Service	76
P2/R5 Adding Core PE Identity Attributes	77
P2/R6 Adding Core NPE Identity Attributes	78
P3/R2 Mobile Device Binding	79
P4/ R1 Global Address List (GAL) Distribution	80
P4/R4 Local Offline Address Book (OAB) Availability	81
P4/R5 Directory/ Global Address List (GAL) Services Availability	82
P5/R2 Identity Service for Tactical Edge	83
P5/R3 Global Information Resource Access	84
P6/R1 Policy Management Service Scope & P6/R4 Policy Change Management Responsibility	85
P7/R5 Policy Store (PS) Personally Identifiable Information (PII) Attribute Exposure	86
P9/R9 Alternate Authentication Mechanisms (Non-CAC/Token)	87
P11/R2 Network-Connected Authentication	88
P11/R3 'Disconnected' and/or 'Network-Disadvantaged' Authentication	89
P11/R3 'Disconnected' and/or 'Network-Disadvantaged' Authentication	90

TABLES AND FIGURES

Figure 1-1 – Framework of Candidate DoD-Provided Directory Services – 2015 “Vision”	1-3
Figure 1-2 – Army IdAM Architecture Operational View	1-4
Table 1-1 – Major Army IdAM Development Considerations.....	1-9
Table 2-1 – RA Versioning Matrix	2-3
Table 3-1 – ICAM Service Areas Mapped to RA Guiding Principles	3-1
Figure 3-1 – DoD ICAM Services Framework.....	3-2
Table 3-2 – DoD ICAM Service Areas to IdAM Service Areas Mapping.....	3-2
Figure 3-2 – RA Versioning versus Services and Infrastructure Delivery Timeline.....	3-3
Table 3-3 – Unique Identity and Credentials.....	3-4
Table 3-4 – Person Entity (PE) Unique Identifier	3-4
Table 3-5 – Allowed Identities	3-5
Table 3-6 – Persona Life-cycle Management	3-6
Table 3-7 – Identity Data Integrity	3-7
Table 3-8 – Person Entity (PE) - Identity Data Discoverability	3-7
Table 3-9 – Non-Person Entity (NPE) - Identity Data Discoverability	3-8
Table 3-10 – Identity Data Conformance	3-9
Table 3-11 – Authentication and Authorization Service Provisioning.....	3-10
Table 3-12 – Enterprise Identity Attribute Utilization.....	3-11
Table 3-13 – Authoritative Identity Data Source.....	3-12
Table 3-14 – Authoritative Person Entity (PE) Identity Attribute Data	3-12
Table 3-15 – Authoritative Non-Person Entity (NPE) Identity Attribute Data	3-13
Table 3-16 – Common Access Card (CAC) Usage	3-14
Table 3-17 – Resource Account Provisioning Service (APS)	3-14
Table 3-18 – Adding Core Person Entity (PE) Identity Attributes	3-15
Table 3-19 – Adding Core Non-Person Entity (NPE) Identity Attributes.....	3-16
Table 3-20 – Non-Person Entity (NPE) Resource Data Federation	3-17
Table 3-21 – Directory Information Updates.....	3-18
Table 3-22 – Person Entity (PE) and Non-Person Entity (NPE) Identification.....	3-19
Table 3-23 – Mobile/Edge Platforms/Devices.....	3-19
Table 3-24 – Mobile Device Binding	3-20
Table 3-25 – Global Directory Services for Enterprise Services.....	3-21
Table 3-26 – Global Address List (GAL) Distribution.....	3-21
Table 3-27 – Global Address List (GAL) Views.....	3-22
Table 3-28 – Global Address List (GAL) Data Schema.....	3-22
Table 3-29 – Local Offline Address Book (OAB) Availability	3-23
Table 3-30 – Directory/Global Address List (GAL) Information Concurrency.....	3-24
Table 3-31 – Authentication and Authorization	3-25
Table 3-32 – Authentication and Authorization Scope.....	3-25
Table 3-33 – Identity Service for Tactical Edge.....	3-25
Table 3-34 – Global Information Resource Access.....	3-26
Table 3-35 – Access and Policy Security	3-27
Table 3-36 – Availability of DoD Enterprise Authentication and Authorization Services	3-27
Table 3-37 – Availability of Army (Non-DoD Enterprise) Authentication and Authorization Services	3-28
Table 3-38 – Dynamic Access Policy Management	3-29

Table 3-39 – Policy Management Service Scope	3-29
Table 3-40 – Standard Attribute Model	3-29
Table 3-41 – Standard Access Policies	3-30
Table 3-42 Policy Change Management Responsibility.....	3-30
Table 3-43 – Policy Attribute Validation.....	3-31
Table 3-44 – Access to Data, Services and Applications	3-32
Table 3-45 – Information Resource Types	3-32
Table 3-46 – Logical NPE Layered Logical Access Control	3-33
Table 3-47– Public Key Infrastructure (PKI) Based Authentication.....	3-33
Table 3-49 – Data Resource Identification	3-34
Table 3-50 – Rules Engine (RE) Personally Identifiable Information (PII) Attribute Exposure	3-35
Table 3-51 – Data Tagging Development.....	3-36
Table 3-52 – Standardized Policy Languages.....	3-37
Table 3-53 – Access Policy Data Tagging Metadata Standards	3-37
Table 3-54 – Physical Access	3-38
Table 3-55 – Non-Person Entity (NPE) Unique Identifier	3-38
Table 3-56 – Physical Access Control Policies	3-38
Table 3-57 – Person Entity (NPE) Attribute Verification	3-38
Table 3-58 – Facilities Attributes Management.....	3-39
Table 3-59 – Common Access Card (CAC) Credential Mechanism	3-39
Table 3-60 – Common Access Card (CAC) Enrollment	3-39
Table 3-61 – Layered Physical Access Control for Subclass Type 1 Physical NPEs	3-40
Table 3-62 – Layered Physical Access Control for Subclass Type 2 Physical NPEs	3-40
Table 3-63 – Physical Access Control – Subclass Type 1 NPE Asset Naming	3-40
Table 3-64 – Physical Access Control – Subclass Type 2 NPE Asset Naming	3-41
Table 3-65 – General Identity and Access Management (IdAM) Security Policy	3-42
Table 3-66 – Identity Attribute Data Validation.....	3-42
Table 3-67 – Authorization Service Scope	3-42
Table 3-68 – Enterprise Information Sharing	3-43
Table 3-69 – Information Resource Authentication Frequency	3-43
Table 3-70 – Cross-Domain Security	3-43
Table 3-71 – Information Resources Availability	3-44
Table 3-72 – Information/Data Resources Protection	3-44
Table 3-73 – DoD Enterprise Trust Management.....	3-45
Table 3-74 – Alternate Authentication Mechanisms (Non-CAC/Token).....	3-45
Table 3-75 – Alternate Authentication Mechanisms (Non-CAC/Token).....	3-46
Table 3-76 – SHA-256: Secure Hashing Algorithm Migration.....	3-46
Table 3-77 – Single Sign-On (SSO) and Reduced Sign-On (RSO).....	3-47
Table 3-78 – SSO and RSO Directory Data Population.....	3-47
Table 3-79 – Electronic Data Interchange Personal Identifier (EDI-PI)	3-47
Table 3-80 – SSO and RSO Services Availability.....	3-48
Table 3-81 – Network Access Controls	3-49
Table 3-82 – Authorization Policy Network Attributes.....	3-49
Table 3-83 – Network-Connected Device Authentication.....	3-50
Table 3-84 – Disconnected and/or Network-Disadvantaged Authentication	3-50

Table 3-85 – Network Gateway Authentication and Authorization3-51
Table 3-86 – Monitoring and Reporting3-53
Table 3-87 – Auditing Services3-53
Table 3-88 – Identity and Access Management (IdAM) Infrastructure-Monitoring/Reporting3-53

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) assets and other selected SC materiel (e.g., weapons systems, aircraft, ordnance). The use of automation and the ability to network computers, devices and the capabilities they provide has transformed how we fight. As the Army's warfighting capability and ability to conduct the fight must be better, faster and, in many ways, safer, even as new cyber security risks arise and increase in number.

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

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

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 IdAM Architecture to be developed. The architecture will comprise key DoD IdAM components, logical workflow and data flows that must occur to accommodate the current DoD and SC environments, and will integrate a more robust authentication and authorization framework. This will support both existing and transforming DoD, Army and other SC Directory Service architectures and infrastructures, and will include components required to provide access management services for information resources using Dynamic Access Policy Management Services (DAPMS). DAPMS can be account-based, where access policies are developed and maintained using identity attributes that are directly associated with a requester/user account; created in a network domain, at a specific location; or associated with a particular DoD or Army organization. Account-based DAPMS requester/user accounts also include attribute data related to the resources to which a requester/user is authorized. In non-account-based DAPMS, the requester/user attributes used for access policies reside in a general Attribute Data Repository (ADR) but are tied directly to an individual, not to an account that includes specific resource information or actual imbedded policies. In either account- or non-account-based DAPMS, access workflow is the same, with authentication first, followed by execution of one of these forms of authorization.

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 used to support DoD enterprise and SC network and information resource 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. DoD and the Army have also built infrastructure components based on government-off-the-shelf (GOTS) technology. 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 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 IdAM services are centrally controlled and support central credential operations, with both central and distributed authentication and authorization operations, and a federation infrastructure that makes the IdAM services look and operate like a single IdAM services implementation. Given the reality of where DoD and DISA are with their evolving IdAM service offerings, a more generic set of IdAM component definitions and descriptions is required within this RA to avoid significant vocabulary ambiguities. These terms will be presented and discussed under key IdAM Component Definitions in Section 2, and can be applied to develop specific operational and system views, schematics and workflow/data flow models (shown in the Army IdAM Architecture Operational View in Figure 1-2).

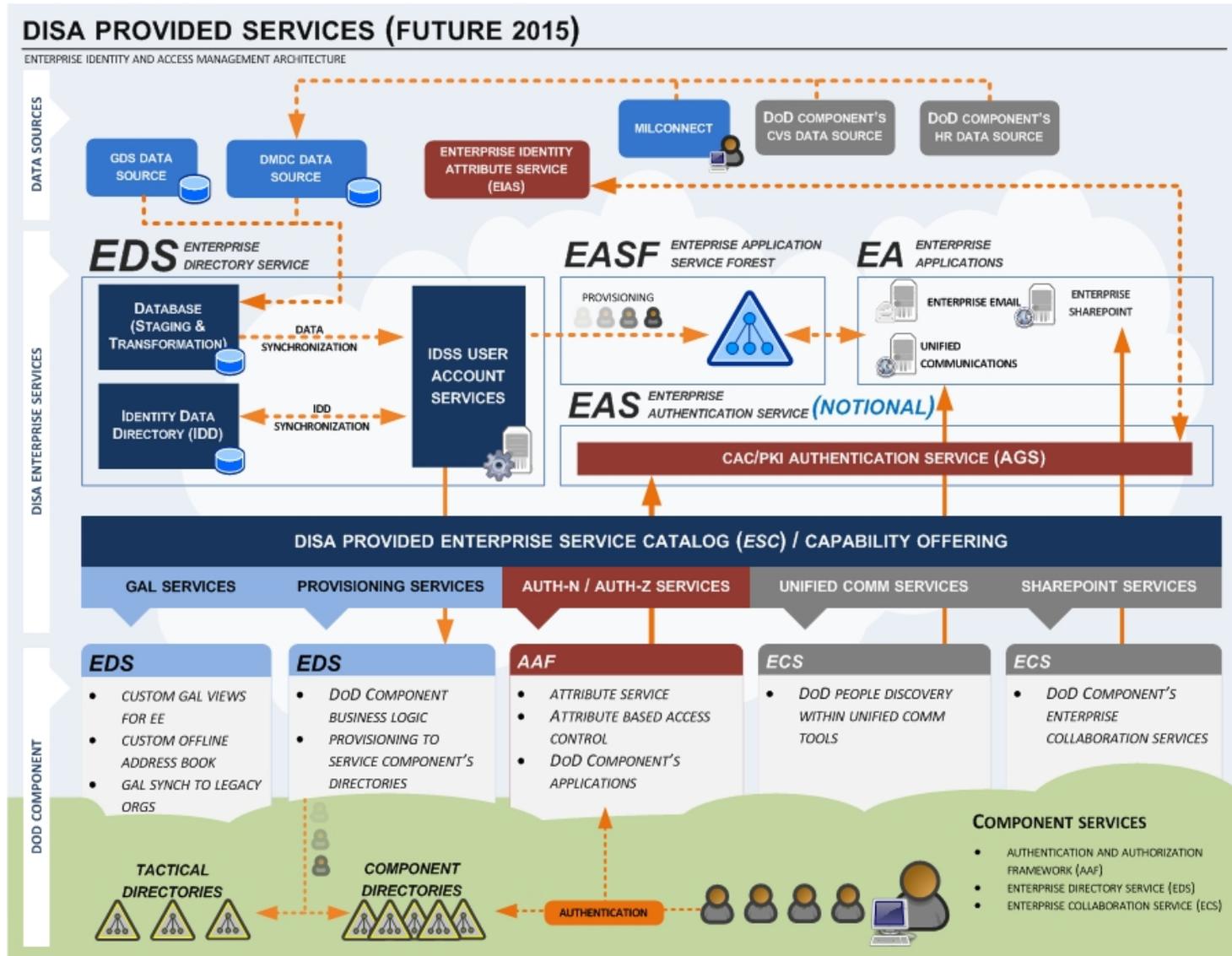


Figure 1-1 – Framework of Candidate DoD-Provided Directory Services – 2015 “Vision”

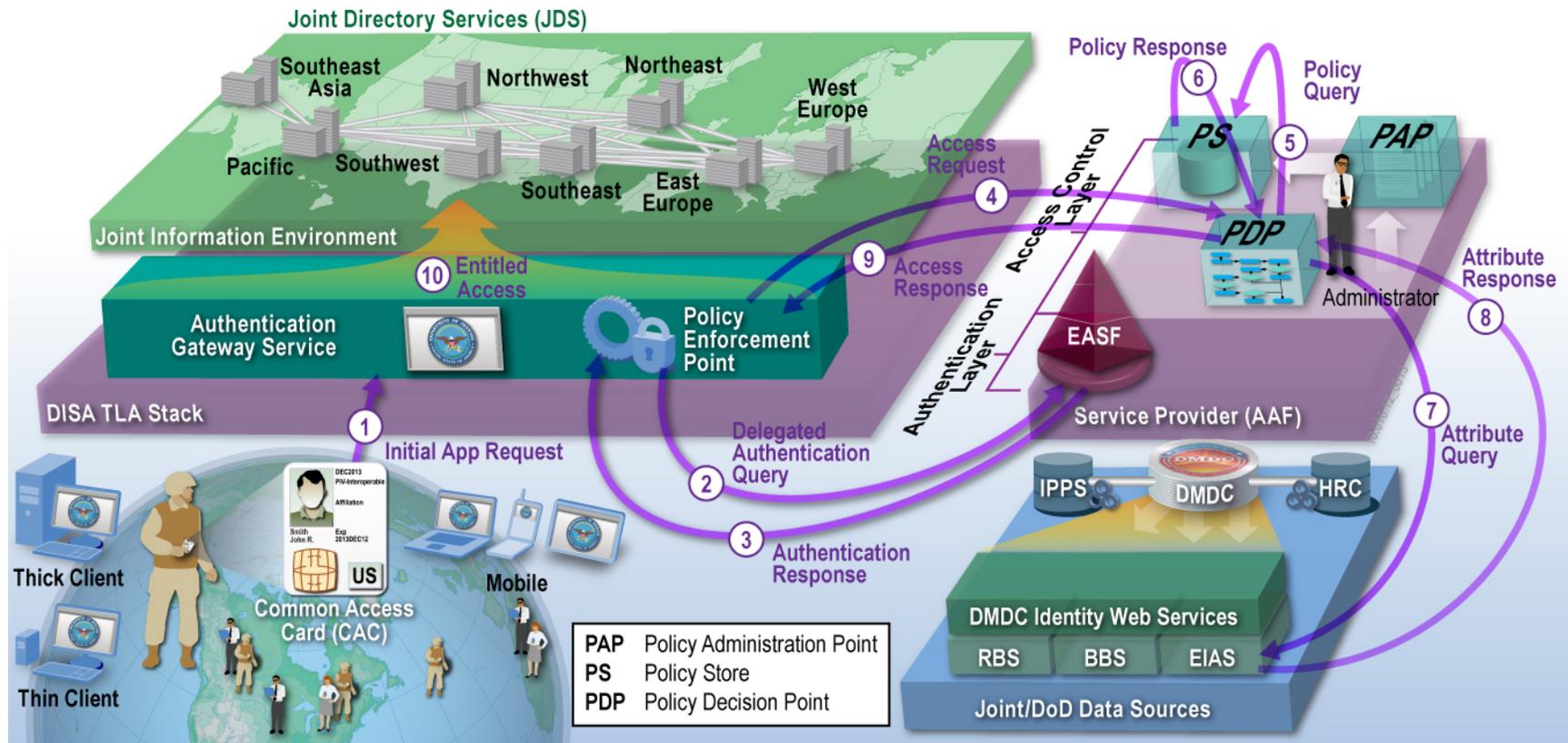


Figure 1-2 – Army IdAM Architecture Operational View

1.3 Background

An RA provides an authoritative source of information about a specific subject area to guide and constrain 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. These rules also must be followed for all related solution architectures, designs and implementations.

This document addresses both DoD and Army IdAM requirements but is written from the perspective of the Army as a consumer of DoD-provided enterprise IdAM services. It also deals with environments where these enterprise services are not always available (i.e., when adequate network connectivity to the enterprise services does not exist). Therefore, an attempt has been made to make this RA as generic as possible from a DoD SC perspective. However, this RA version has more thoroughly focused on the Army and the way that it operates from post/camp/station and in forward-area tactical environments across both its generating and operating forces. It is assumed that it is a DoD objective to provide as many IdAM services to all SCs as possible, and that the Army’s first choice will be to utilize DoD offerings. This approach is being driven by U.S. Government and DoD security, funding, manpower and other resource availability improvement initiatives.

Because there are SC-specific operational activities that control or limit resource access within any DoD SC or its agencies, DoD has reached a crossroads where it must now assess the best way to provide IdAM services to all of its personnel, regardless of the environment. The ideal end state would enable any Soldier or authorized entity to access information or facilities at any time, based on who he is and what he needs to do, rather than access determined largely by physical location. This end state requires eliminating the 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 IdAM services environment while allowing distributed tactical operations. This will enhance coalition and non-DoD-partner secure access, as well as internal DoD operations. An enterprise IdAM services environment presents many challenges, both technically and in terms of ensuring that overall resource security is preserved while providing more extensive IdAM capabilities. Well-planned and executed access policy management will be the key to achieving these objectives and is a major focus of this RA.

1.4 Benefits

This IdAM RA describes the required digital identities, authentication and authorization services, and the generic functional components that enable them for both the DoD enterprise and the SCs, with an emphasis on the Army. 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 IdAM growth
- A framework for IdAM decision making
- A guide for creating a DoD- and an Army-enabling identity infrastructure for unforeseen new applications and services
- A target for IdAM migration
- A way to more reliably authenticate the identity of any entity trying to gain access to authorized resources
- A method to establish and manage access policies and authorization controls for all DoD and SC resources
- A way to accommodate rapid but reliable changes in requester and resource identities, roles and personas
- The infrastructure and management components to perform these functions while assuring the privacy and civil liberties of all entities involved
- A way to reduce administrative costs, improve user efficiency, enhance user experiences, conform better to regulatory compliance requirements, and promote Army business process improvement

1.5 Intended Audience and Use

This RA will provide DoD, the Army, the other SCs' leadership and their organizations guidance for the design, development, deployment, transition to and operational support of a DoD enterprise IdAM service framework and infrastructure. The key beneficiaries (and their IdAM-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 IdAM policies and compliance requirements
 - SC-level IdAM 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
- Army Cyber Command (ARCYBER):

- Guidance to DoD to support Army ICAM requirements
- Strategic Cyber defense planning in support of Army and Joint operations
- Army Training and Doctrine Command (TRADOC):
 - Identify ICAM Operational Initial Capabilities Document (ICD) gaps
- The Army Deputy Chief of Staff, G-3/5/7:
 - ICAM integration planning for all areas of Army operations
 - Operational environment IdAM integration execution management
- Army Network Enterprise Technology Command (NETCOM):
 - Network authentication and access control planning
 - Network Solution Architectures
- The Assistant Secretary of the Army (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 IdAM RA include, but are not limited to:

- The Joint Information Environment (JIE)
- The Army Enterprise Network (AEN)/LandWarNet Architecture
- The Army Network Integration Evaluation (NIE) Reference Architecture
- The Army Information Architecture (AIA)
- The Army Network Security Reference Architecture
- The Army Unified Capability (UC) Reference Architecture
- The Army “Thin/Zero” Client Reference Architecture
- The Army Network Operations Architecture (ANA)

1.6 Alignment with DoD Enterprise Architecture and Key IdAM Strategies

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

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

- *The Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0, 2 December 2011*

- *The draft DoD Identity and Access Management (IdAM) Strategy, Version 0.5, 9 May 2013*
- *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), 8 May 2012*
- *The Department of Defense (DoD) Information Technology IT Enterprise Strategy and Implementation Roadmap (ESR) Initial Implementation Plan, Version 1.0, 6 September 2011*

1.7 Scope/Organization

This “business rules-based” IdAM 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 (BR). These are functionally specific to IdAM 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)*. Credentialing, although defined as a key service area, is considered in this Army RA only from a service consumer perspective (the RA does not intend to conflict with DoD’s purview to set and maintain standards). There are specific ways that the Army must apply these credentials; they are addressed within each relevant BR definition and description.

The major areas of discussion for each of the IdAM business rules 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 IdAM services.

Risks - 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.

Technical Positions and Patterns - This RA establishes a set of core technical and/or regulatory standards for each business rule so that any implementation derived from it ensures proper interfacing and interoperability among all IdAM infrastructure components, also assuring end-to-end interoperability. Both technical and regulatory standards for business rules that have been deemed as requiring these in this document have been linked or bookmarked to one or more “profile” tables in Appendix B; the name of each appears as blue text.

IdAM 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 intra-Army and intra-DoD, to include inter-SC. This RA categorizes these environments in two areas: the Business Mission Area and the Tactical Mission Area. This division provides more specific guidance in meeting the differing implementation requirements of those environments. Although these patterns can be represented in standardized DoD Architecture Framework (DoDAF) views (e.g., OV-2, SvcV/TV-1, SV), in compliance with the *DoD Reference Architecture (RA) Framework and Guidance, June 2010*, and as a way to optimize each pattern to each BR, a standard object/component template has been developed and utilized to create patterns that may be combinations of standard DoDAF views. For the Business Rules requiring Patterns, these are provided in the second section of Appendix B.

1.8 Major Considerations

There are several overarching considerations that the Army must take into account in the transition to a comprehensive IdAM capability and infrastructure. These are noted in Table 1-1 below.

Major Considerations		
#	Constraint	Rationale
1	The Defense Manpower Data Center (DMDC) will be the Authoritative Data Provider for Person Entity (PE) and Non-Person Entity (NPE), and will define Persona for the Army.	DMDC will broker HR data in addition to EDI-PI, and aggregate identity data from Army Authoritative Sources.
2	DoD will provide enterprise account provisioning services to manage Army identity life cycles and to populate directories. This service will be accomplished through the current Enterprise Directory Services (EDS) initiative.	All PE and NPE accounts will be created and managed within Army Directories through the EDS.
3	All services, applications and networks will be required to enforce authorized access to information or devices according to specified access control rules and requirements for all individuals, organizations, Communities of Interest (COIs), automated services and devices.	Person and Non-Person Entities vetted by the DoD enterprise 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).
4	The Army Enterprise Identity Service for PE and NPE must include support for the tactical edge.	Mission-critical applications and services operations will require provisioning from EDS.
5	Army applications will need to migrate from legacy infrastructures for authentication and authorization to the Enterprise Authentication Gateway and Access Management framework once instantiated.	Army networks must be capable of providing access to information and resources from any end-device to any resource available on the LandWarNet. This requires that devices and their users be vetted for authentication and then authorized to connect any appropriate requested information resource from any location.

Table 1-1 – Major Army IdAM Development Considerations

2 Vocabulary

This RA will use several key constructs, that include 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 evolution of the reference architecture.

2.1 Access Types

The IdAM RA addresses access control in the Logical Access Control (LAC) and Physical Access Control (PAC) domains. Within each domain, the IdAM RA describes who or what requires access and to what access is requested, which is largely defined as information, facilities, networks and/or other objects. Every principle and business rule defined in the IdAM RA will address 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 are either standalone or available on a network.

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.

2.1.3 Entities

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

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. This RA has categorized NPE as either logical or physical; one logical NPE type, and two types of physical NPE as follows:

Logical NPE: Groups, distribution lists, systems, software/applications, data and other Army intellectual or informational assets

Physical NPEs (Type 1): Locations/areas, bases, installations, facilities, buildings, rooms and other Army real-property assets

Physical NPEs (Type 2): Hardware, devices and other Army assets

2.1.3.3 Requester

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

2.1.3.4 Resource

A resource is any NPE to 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 versions, each with progressing maturity of accuracy, detail and completeness for access type and IdAM services.

RA v2.0 is the second version/release of the three, with v1.0 having been approved, signed and published on the CIO/G-6 website in January 2013

(<http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>).

The scope of each RA version, with some degree of overlap, is outlined in Table 2-1. Green-shaded table cells indicate that adequate subject matter exists to address the service areas in the referenced versions, but they may still need to undergo further updates and expansion in the future. The yellow-shaded cells mean that the subject matter foundation is not mature enough to address the service areas by the time that the referenced versions are to be published. Grey-shaded cells indicate that there is not enough information at the present time in these areas to develop them adequately in the referenced versions. These assessments are based upon the current status of industry standards, DoD policies and standards, and to a lesser degree Army operational objectives and capability definitions.

		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 Updates, Additions and Limitations

Table 2-1 shows the subject matter v1.0 already addressed, what is included in v2.0 (green shading) and what remains to be addressed in v3.0. Additionally, because v2.0 has now limited the scope of discussion to the Army as a consumer of DoD credential management services, its related column also shows as yellow. The initial content in v1.0 of the RA was not complete in the following sub-sections:

- **Risk** descriptions
- **Core Technical Standards** tables (ref: Appendix B) – The core standards and policy/regulation associated with this business rule can be found in the Technical Profiles located in ‘Appendix A (Feb 2012) to the Guidance for ‘End-State’ Army Enterprise Network Architecture’.
- **Patterns** (ref: Appendix B)

Version 2.0 addresses many of these initial sub-section content gaps, and has added, deleted, combined and updated the initial set of 68 business rules, of which there are now 73. The definitions, descriptions, assumptions, constraints and risk statements presented in v1.0 have been updated, eliminated or promoted to an overarching Major Consideration. This version has updated the corresponding baseline technical and regulatory standards profiles presented in v1.0 identified the BRs that require a pattern and provided views that show the IdAM service components and the relationships that comprise the associated BR. Both the profiles and patterns were developed by conducting a thorough functional decomposition and assessment, and identifying their key BR components. Risk mitigation strategies remain a continually maturing area for the RA that will not be completed until v3.0 is published. References provided in v1.0 for both guiding principles and business rules have not yet been fully updated, pending further output from the DoD CIO that will occur after release of RA v2.0.

This RA v2.0 has made changes to the set of appendixes that were included in RA v1.0; several have been removed. The decision to remove these in this version was made for several reason:

- DoD had developed updated versions of the same information in new draft documents
- Terminology has changed for certain IdAM capabilities
- Information was determined as background that was not required to understand the RA

These original appendixes and their corresponding RA versions impacted or that will be impacted include:

Expanded: Appendix B (v1.0) – Technical Positions and Patterns

This appendix now includes specifications of both technical standards and regulations that apply to each guiding principal and business rule. Pattern views have been added.

Added: Appendix D (v2.0) - Warfighter IdAM Capability Timeline

A timeline has been added showing the fiscal year/quarter (FY13-17) when key DoD and Army IdAM services will be provided to the warfighter. These services are ones that either Soldiers do not currently have, or the quality and extensibility of the current capabilities are very limited.

To Be Added: Appendix C (v3.0) – Operational Gap BR Alignment

This appendix will outline the underlying Army operational gaps and problems that are related to each of the 73 BRs in v2.0. At the present time, this should be considered as notional only and not official as it has not been generated or approved by TRADOC or the G-3/5/7.

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. 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 and federated approach to IdAM infrastructure.

2. Optimize the use of existing and future DoD enterprise IdAM services and infrastructure.

DoD and all of the SCs must first attempt to leverage all of the available DoD deployed, operational and 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 be 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 to which they require access while in theater. 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, to accommodate these conditions through an appropriate and useful set of architectural constructs and definitions. RAs must identify generic services, components and frameworks to support these unique operational environments.

2.2.3.2 Service Offerings Baseline

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 defined and in deployment, but many were still being scoped and specified by the DoD.

- Industry (i.e., product-specific) and candidate DoD or Army-provided infrastructure for enterprise services (primarily in non-tactical environments) include offerings such as:
- Identity Synchronization Service (IdSS)
- Enterprise Directory Service (EDS)
- Account Provisioning Service (APS)
- 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”. The COE provides a technical model of an end system (e.g., mobile/handheld, client, server, sensor, and platform) with 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, within the RA these elements must be established as components or building blocks 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.

More specific component names/specifications (e.g., NT-ADR, T-ADR) have been used in this RA in business rules descriptions, assumptions, constraints, and risk statements. These can be used to describe the current established or candidate DoD and Army IdAM service offerings, or generic components that provide one or more IdAM services. The distinction between non-tactical and tactical components has only been used when use of a generic definition is not adequate to describe a component's function in a particular Army operating environment.

Non-tactical components are required to support the Generating Forces' operational environments, which 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 independent of the GIG or the LandWarNet backbone.

Tactical components are required to support theater 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 (MEs), as outlined in the Army's Common Operating Environment (COE) Architecture: Enterprise – Camp/Post/Station, Command Post, Mounted, and Soldier/Sensor. When network connectivity is intermittent or significantly degraded, these MEs may be characterized as "DIL", meaning "disconnected, intermittent, and/or of limited bandwidth (i.e., network-disadvantaged). 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 authenticate users reliably, securely and persistently, and provide them authorization to access 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 and forces the business rule assumptions, constraints and risk descriptions in Section 3 to address the full spectrum of possible JIE, Army and general DoD SC operational environments.

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

Non-Tactical IdAM Components

DoD/JIE: 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 Email
- Enterprise Collaboration Services (e.g., Instant Messaging (IM), MS SharePoint)
- 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

Army and Other Services: 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 Army, but are not considered DoD enterprise or Joint services. They would be considered “Specialized Army Resources”, and would 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 IdAM Components

DoD/JIE: 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 Theater/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 Theater Operations Centers
- Coalition Partner Bases
- Operational areas
- Buildings

Army and Other Services: IdAM components and services that directly support tactical logical and physical Army-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. They would be considered “Specialized Army Resources”, and would include, but not be limited to:

- SC Theater/Tactical MS AD Forests and Domains
- Army Blue Force Tracking
- Advanced Forward Area Tactical Data System (AFATDS)
- Naval Tactical Command Support System (NTCSS)
- Theater Forward Area Facilities and Assets
- Brigade/Platoon Operations Centers
- Mobile Command Centers
- Warfighting Platforms (e.g., tanks, armored personnel carriers)
- Aircraft
- Ships/Submarines

Although a 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 infrastructure sufficient to optimize network connectivity and bandwidth/data throughout will be provided by DoD, DISA and all of the SCs, as required. This means that every service, in support of all DoD sustaining base and deployed tactical operations, will have virtual service presence to the greatest degree that both infrastructure and network connectivity will allow.

2.2.3.4 IdAM Component Definitions

The IdAM components defined in this section is provided as a basis for the discussions within Section 3 (Guiding Principles and Business Rules) of this document. Each component listed can be realized in the form of a piece of infrastructure that can be categorized as non-tactical or tactical, where tactical infrastructure components may be required to function offline as well as online.

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. When disconnected from the Army networks and/or the GIG, components deployed in theatre may have to function as proxy services for the DoD enterprise level components and services. The ownership and management of these components can be done by DISA, or by a combination of DISA and the Army depending on who has the best level of access to and control of them and their current datasets at any point in time.

Theater-wide authentication and authorization services must operate at times using DoD GIG-based enterprise services and infrastructure, or using services extended to or available at an Army Brigade Combat Team (BCT), Division and Corps level. To optimize security and reduce operational risk, vulnerabilities and possible security breaches, each Combatant Command (COCOM) would be best served by having its own local AAF as an offline proxy service within the theater of operations. So if the framework is ever penetrated at the single theater level, it will only affect that theater and not other Army tactical force networks and resources, as well as anything within the JIE. However, if and when this AAF's network capability is restored, even temporarily, it would convert its function to a pass-through mode to allow DoD enterprise level AAF services to be resumed to that theatre or theatre segment. If then disconnected from the network again, it's local, but updated, AAF functions would be resumed. Therefore, the Army's risk assumed is the time where the connectivity is not available, where there is some level of either invalid authentication and/or authorizations that can occur.

➤ **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 are 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. However, other Army ADRs will be required that broker the attribute data from the DoD EIDRSS, but do not provide services to the entire JIE. In this document, when the term "ADR" is used, it will apply only to Army ADRs unless otherwise specified.

➤ **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), and resource identity attribute data from NPE authoritative data sources. The identity attribute data are made available to all DoD and Army IdAM services at both levels to support requester authentication and authorization to both logical and physical resources. All directory services and access authorization policies must utilize this enterprise data set.

➤ **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

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* which can supply authentication services using an X.509 certificate-based Public Key Infrastructure (PKI).

➤ **Authentication Service Framework (ASF)**

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

➤ **Directory Service (DS)**

DS is a generic service that functions as an ADR for user attribute data, as well as information systems and applications resources (e.g., email, instant messaging, Unified Capabilities (UC) services). These require a more limited set of attribute data to identify the users and resources. An ADR will store, organize and distribute a subset of the attribute data that are collected in the EIADRSS. It provides basic user (i.e., requester) identity information, such as user name(s), location(s), phone number(s), email 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) and location(s). An ADR will not contain any attribute data that do not also exist in EIADRSS.

➤ **Offline Address Book (OAB)**

OAB is a generic term for an offline address book that provides DS information. There are times when DoD email and other enterprise service users will not have network access but still require

the ability to access address and contact information to function. The OAB is a critical IdAM service within tactical environments where a non-located GAL may not always be available.

➤ **Account Provisioning Service (APS)**

APS is a generic term for a service that provides DoD enterprise administrators 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 the network, logical domains, applications, data and other information resources, such as printers and faxes. It also is required to manage accounts that allow for all forms of physical access.

➤ **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 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.

➤ **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 authorized to access these grouped resources without being prompted to authenticate again. 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, an RSOS typically will not grant "keys to the castle" but will grant access to certain "rooms within the castle", as required.

➤ **Dynamic Access Policy Management Service (DAPMS)**

Dynamic Access Policy Management Service (DAPMS) will provide a flexible decision and enforcement mechanism to accommodate changes in user privileges and policy related to resource access decisions. It 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. It

can be an enterprise-level service or be deployed locally in tactical operating environments with no or disadvantaged network connectivity. Local DAPMSs must be re-synchronized with their DoD enterprise counterparts whenever network connectivity is restored.

➤ **Rules Engine (RE)**

In the DAPMS/Rule (or Role)-Based DAPMS model, there is an entity called the “policy engine” (often called PE in other DAPMS-like 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), the policy decision point (PDP) and the Policy Enforcement Point (PEP), as defined and described in Appendix D. An 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 will not further define unique components for both environments.

➤ **Policy Store (PS)**

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 will 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, DoD ICAM 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 ICAM Service Areas are subsets of the DoD ICAM Service Areas defined in the current DoD Identity, Credentialing and Access Management (ICAM) Services Framework, as shown in the grey boxes in Figure 3-1. There are one or more ICAM services associated with each ICAM Service Area.

ICAM Service Areas to Guiding Principles Mapping							
DoD ICAM Service Areas							
Army IdAM RA Guiding Principles	Identity Data Management	Directory Services	Identity Authentication		Access Authorization		Access Auditing
	(P1) Unique Identity & Credentials	(P4) Email Global Directory Services	(P5) Authentication & Authorization	(P8) Physical Access	(P5) Authentication & Authorization	(P9) General IdAM Security Policy	(P9) General IdAM Security Policy
	(P2) Identity Authoritative Data Source		(P6) Dynamic Access Policy Management	(P9) General IdAM Security Policy	(P6) Dynamic Access Policy Management	(P10) SSO and RSO Capability	
	(P3) Person Entity & Non-Person Entity Identification	(P9) General IdAM Security Policy	(P7) Access to Data, Services And Applications	(P10) SSO and RSO 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 – ICAM Service Areas Mapped to RA Guiding Principles

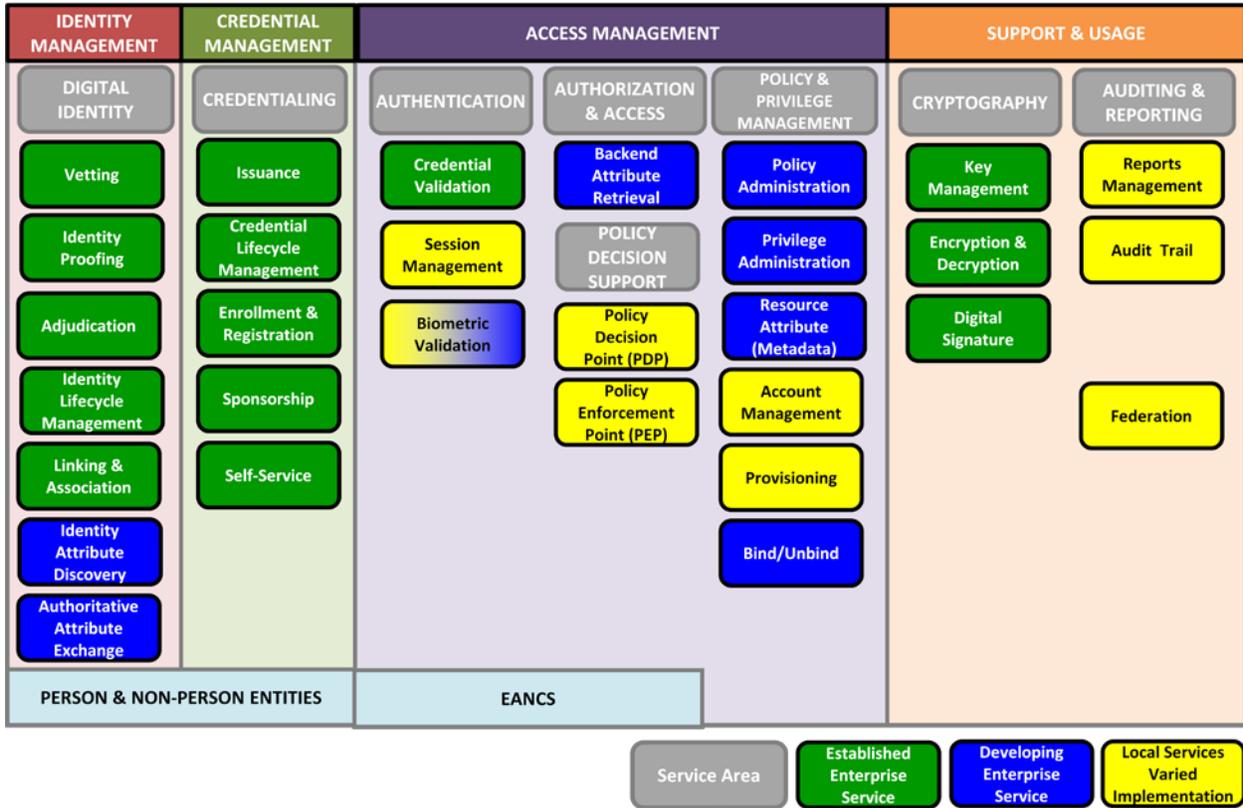


Figure 3-1 – DoD ICAM Services Framework

The mapping of the ICAM Services Areas to the IdAM Service Areas is a “many-to-one” relationship, as shown in Table 3-2.

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 3-2 – DoD ICAM Service Areas to IdAM Service Areas Mapping

3.2 RA Versioning versus Services and Infrastructure Component Delivery Timeline

Based on the Army CIO/G-6 Cyber Directorate’s draft Strategic IdAM Implementation Roadmap, Figure 3-2 shows the capabilities, services and the enabling infrastructure components that are expected to be made available to the Army through DoD/DISA-provided enterprise or Army-provided IdAM infrastructures.

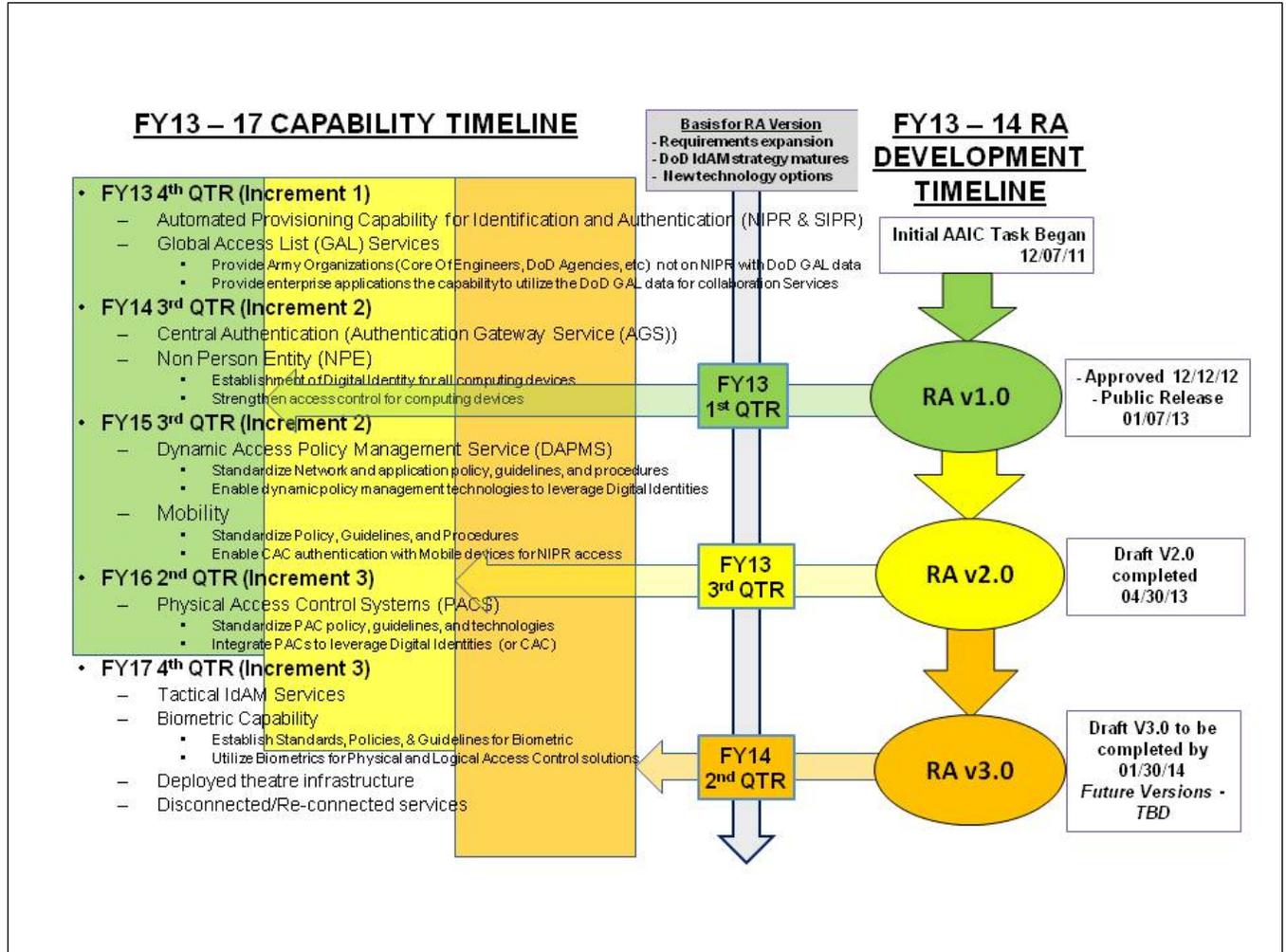


Figure 3-2 – RA Versioning versus Services and Infrastructure Delivery Timeline

3.3 Specifications

3.3.1 (P1) Principle 1 – Unique Identity and Credentials

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

Table 3-3 – Unique Identity and Credentials

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

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

Table 3-4 – Person Entity (PE) Unique Identifier

- **(P1/R1) Assumptions**
 - EDI-PI is unique to a person, not to a persona or role.
 - EDI-PIs can be associated with one or more persona per PE.
 - The Army and the other SCs use the Personal Category Codes (PCC) as a key identity attribute.
 - Authoritative Data Sources will synchronize Identity data.
- **(P1/R1) Constraints**
 - There may be multiple authoritative sources containing different sets of data about any PE, but all must be associated with only one EDI-PI.
 - EDI-PIs must be reconciled on a regular basis to ensure that there are neither redundant identifiers nor the same PE with different identifiers.
 - The CAC must not be used as a credential to authenticate users on a classified network.
- **(P1/R1) Risk**
 - Constantly shifting personnel strength and responsibilities will increase the level of difficulty associated with creating, modifying and deleting PE personas and linking them with the right EDI-PI.
 - Personas associated with any EDI-PI may be accidentally inherited when a PE is re-enrolled if they are not purged every time a CAC is revoked or expires.

- **(P1/R1) Technical Positions and Patterns (Reference Appendix B – Pattern View)**
- (P1/R1) Technical Standards Profiles:**
 - *Common Access Card (CAC)*
- (P1/R1) Policy/Regulation Profiles:**
 - *Army IdAM RA to Army Regulation (AR) 25-2 Mapping*

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

Business Rule	Description
<i>The Army will require that all person entity and non-person entity digital identities be authenticated.</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 JIE without first establishing their identities.

Table 3-5 – Allowed Identities

- **(P1/R2) Assumptions**
 - All PEs and NPEs can be assigned unique identifiers that will allow X.509 certificates to be assigned to and removed from association with them.
 - Globally Unique Identifiers (GUIDs) for NPE would be in addition to use of PKI/X.509 certificates.
- **(P1/R2) Constraints**
 - A GUID must be assigned to every NPE.
 - Once established, the EDI-PI must remain associated with a unique PE.
 - Once established, the GUID must remain associated with a unique NPE.
- **(P1/R2) Risk**
 - If an EDI-PI or GUID is assigned to the wrong PE or NPE, invalid authorization may occur.
 - Unless identity data are regularly audited to assure that it is uniquely associated with a PE or NPE, it is possible that an unauthorized entity could be allowed access.
- **(P1/R2) Technical Positions and Patterns**
 - P1/R2 Technical Standards Profile**
 - *Identity Proofing*
 - P1/R2 Policy/Regulation Profile**
 - *Policy in Authentication*

3.3.1.3 (P1/R3) Business Rule 3 – Persona Life-cycle Management

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

Table 3-6 – Persona Life-cycle Management

- **(P1/R3) Assumptions**
 - PE personas and their associated persona definitions will be the basis for need-to-know access rules.
 - PE and NPE personas will be manageable to accommodate changes in mission, function and/or location for Army and DoD personnel.
 - Personas will be portable across the JIE.
- **(P1/R3) Constraints**
 - Personas must be based on a standard set of identity attributes that are captured during the initial credentialing process.
 - Identity attributes must be able to support multiple personas on a single credential mechanism.
 - Persona accuracy must be maintained throughout the life cycle of all digital identities.
- **(P1/R3) Risk**
 - Failure to do regular due-diligence on persona assignments may result in “hijacking” of authorization privileges and unauthorized access to information and/or facilities.
 - Failure to perform regular due diligence on persona definitions and assignments may result in loss of information or required physical access.
- **(P1/R3) Technical Positions and Patterns**
 - P1/R3 Technical Standards Profile**
 - *Identity Management*
 - P1/R3 Policy/Regulation Profile**
 - *Policy in Authentication*

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

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

Table 3-7 – Identity Data Integrity

- **(P1/R4) Assumptions**
 - Both PE and NPE DoD identity data standards exist and are applied consistently across the JIE.
 - Identity data attributes will have a consistent set of possible values, meanings and context at any one point in time.
- **(P1/R4) Constraints**
 - Human intervention and governance of identity data policies and management processes must be required.
 - Tools required for management of identity data integrity must consistently apply the required rules and policies, and be able to validate each identity attribute associated with each PE and NPE.
 - Identity data (i.e., Personally Identifiable Information (PII)) must have limited exposure to all access management components.
- **(P1/R4) Risk**
 - Unless identity data integrity is maintained for all non-U.S. or non-DoD entities that require access to information, it will be impossible to maintain consistent policies and practices that constrain access appropriately.
 - Accidental exposure and/or storage of PII could result in violation of federal laws and/or DoD and Army regulations.
- **(P1/R4) Technical Positions and Patterns**
 - P1/R4 Technical Standards Profile**
 - *Digital Certificate (PKI)*
 - *Common Access Card (CAC)*
 - P1/R4 Policy/Regulation Profile**
 - *Army IdAM RA to Army Regulation (AR) 25-2 Mapping*

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

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

Table 3-8 – Person Entity (PE) - Identity Data Discoverability

- **(P1/R5) Assumptions**
 - Attribute data will be organized so that access by any consumer will be non-ambiguous and reliable.
 - There is consistency and concurrency between attribute data in an ADR and the access policies that they are applied to.
- **(P1/R5) Constraints**
 - The utilization of local ADRs must be minimized or eliminated, with emphasis on use mainly in tactical environments with DIL.
 - Avoidance of unnecessary or accidental exposure and/or storage of PII and other sensitive identity attribute data must be assured.
 - Requester attribute data must not be disseminated beyond the PDP to any other authorization services.
- **(P1/R5) Risk**
 - Unavailability of selective attribute data may prevent proper authentication of a PE requesting access.
 - Unavailability of selective attribute data may restrict or prevent proper authorization of a PE to resources controlled by attribute-based policies.
- **(P1/R5) Technical Positions and Patterns**
 - P1/R5 Technical Standards Profile**
 - *Identity Proofing*
 - P1/R5 Policy/Regulation Profile**
 - *Army IdAM RA to Army Regulation (AR) 25-2 Mapping*

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

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

Table 3-9 – Non-Person Entity (NPE) - Identity Data Discoverability

- **(P1/R6) Assumptions**
 - Attribute data will be organized so that access by any consumer will be non-ambiguous and reliable.
 - There is consistency and concurrency between attribute data in an ADR and the access policies that they are applied to.
- **(P1/R6) Constraints**
 - All forms of logical NPE must be supported.
 - Both types of physical NPEs must be supported.

- **(P1/R6) Risk**
 - Unavailability of selective “entitlement” attribute data may restrict or prevent proper authorization of a NPE to resources controlled by attribute-based policies.
 - Outdated, retired, invalid or NPE resource attribute data that fails to federate to the enterprise level will result in failed authorizations and possibly orphaned access policies.
- **(P1/R6) Technical Positions and Patterns**
 - P1/R6 Technical Standards Profile**
 - *Credential Management*
 - P1/R6 Policy/Regulation Profile**
 - *Army IdAM RA to Army Regulation (AR) 25-2 Mapping*

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

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

Table 3-10 – Identity Data Conformance

- **(P1/R7) Assumptions**
 - A standard data schema is maintained at the DoD enterprise level for all identity data.
 - All access policies will be based on the standard identity attribute data schema.
 - Both PE and NPE digital identity data will consist of informational attributes, access control attributes and functional attributes.
- **(P1/R7) Constraints**
 - Digital identity data must be comprised of only the essential attribute data that are required to specify any PE or NPE and any corresponding persona.
 - Identity data schema must continually be synchronized across the JIE.
- **(P1/R7) Risk**
 - Continued use of stovepipe data schema will prevent synchronization of data and limit or prevent proper identity interoperability and portability.
 - Without an enterprise view and the ability to manage identity data schema, attribute data management will be extremely difficult and consistent enterprise resource access cannot be assured.
- **(P1/R7) Technical Positions and Patterns**
 - P1/R7 Technical Standards Profile**
 - *Credential Management*
 - P1/R7 Policy/Regulation Profile**
 - *Army IdAM RA to Army Regulation (AR) 25-2 Mapping*

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

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

Table 3-11 – Authentication and Authorization Service Provisioning

- **(P1/R8) Assumptions**
 - Tactical operating units (Brigade Combat Team, Regiment, Division, Corps, Army, Fleet, and Air Wing) can be supported by their own independent T-AAFs and T-APSs.
- **(P1/R8) Constraints**
 - The number of DoD and SC AAFs will be minimized, while optimizing support for Joint warfighting operations.
 - Provisioning of all AAFs will utilize a single primary enterprise identity attribute data repository.
 - The Army and the other SCs must not create any new individual system- or applications-level directory services if the DoD enterprise directory service is readily network-available.
 - Any APS must support all forms of access account provisioning (e.g., network domains, systems, applications, data, facilities, any physical or NPE assets).
- **(P1/R8) Risk**
 - The inability to update identity attribute data accurately and/or in a timely manner in the EIADRSS (from authoritative data sources) will impact the accuracy and overall capability of an APS.
 - The inability to provision network domains and resource accounts in an accurate and timely manner will impact the effectiveness of any AAF.
- **(P1/R8) Technical Positions and Patterns (Reference Appendix B – Pattern View)**
 - P1/R8 Technical Standards Profile**
 - *Attribute Management Services*
 - *Authoritative Attribute Exchange Service*
 - P1/R8 Policy/Regulation Profile**
 - *Policy in Credentialing*

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

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

Table 3-12 – Enterprise Identity Attribute Utilization

- **(P1/R9) Assumptions**
 - All or most legacy JIE non-tactical information resources can be transitioned to an enterprise-level ADR (i.e., EIADRSS) to support enterprise authentication services.
 - The EIADRSS will assure that non-ambiguous identity data are maintained for use across the JIE.
- **(P1/R9) Constraints**
 - Non-tactical legacy information resources and systems-of-systems that cannot easily be transitioned to use an ADR must be either subsumed or sunsetted.
- **(P1/R9) Risk**
 - If an ADR does not fully and consistently support both the legacy and current attribute data requirements, potential impacts on authentication and authorization services may affect both the non-tactical and tactical environments and their corresponding operations.
 - If an ADR's attribute data concurrency cannot be maintained at the tactical level with minimal latency in accuracy, invalid authentications may occur.
 - Army tactical operations will have to accept some level of latency between PE enrollment and revocation at the DoD enterprise level.
- **(P1/R9) Technical Positions and Patterns**
 - P1/R9 Technical Standards Profile**
 - *Attribute Management Services*
 - *Authoritative Attribute Exchange Service*
 - P1/R9 Policy/Regulation Profile**
 - *Policy in Authentication*
 - *Army IdAM RA to Army Regulation (AR) 25-2 Mapping*

3.3.2 (P2) Principle 2 – Authoritative Identity Data Source

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

Table 3-13 – Authoritative Identity Data Source

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

Business Rule	Description
<i>The Army must utilize authoritative identity data sources as the primary broker to define and maintain person-entity personas.</i>	DMDC maintains the largest archive of personnel, manpower, training and financial data in DoD, and is the most qualified source for authoritative personal identity information. It will be used to establish and maintain the authoritative PE attribute data set. All authoritative attribute data to support all DoD/Joint operations are brokered by DMDC, as shown in Figure 1-2. PEs can have one or more personas that define role(s) and/or function(s) for any requester. All identity attribute data that comprise a PE persona must reside within or under the control of the DMDC.

Table 3-14 – Authoritative Person Entity (PE) Identity Attribute Data

- **(P2/R1) Assumptions**
 - DMDC maintains reliable and accurate authoritative identity data from DoD personnel management systems and data sources.
 - The authoritative data maintained in an authoritative data source is at a minimum near-real-time accurate according to established DISA Service-Level Agreements.
- **(P2/R1) Constraints**
 - All PE identity data consumed by Army IdAM services and components sourced from DMDC must be indexed by an EDI-PI.
 - DMDC-based identity data cannot be directly modified; changes must not occur in the originating systems and data sources without first being instantiated in the appropriate ADR.
- **(P2/R1) Risk**
 - Data value errors in an authoritative data source will propagate across ADRs and AAFs, and could impact the accuracy and effectiveness all IdAM components.
 - If the DMDC>EIADRSS>DS data propagation is not near real-time, unauthorized access to information resources may be granted.
 - When a T-DS is disconnected and/or encounters network-disadvantaged WAN connectivity, unauthorized access to information and physical resources may be granted.
 - All IdAM service consumers who do not define their acceptable risk levels, based on assessments of the range of possible data propagation latencies, may experience both unexpected and negative operational and security impacts.

➤ **(P2/R1) Technical Positions and Patterns**

P2/R1 Technical Standards Profile

- *Identity Management*

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

Business Rule	Description
<i>The Army will utilize authoritative identity data sources as the primary broker to define and maintain non-person entity personas.</i>	DMDC maintains the largest archive of personnel, manpower, training and financial data in DoD, and is the most qualified source for authoritative personal identity information. All authoritative attribute data to support all DoD/Joint operations are brokered by DMDC, as shown in Figure 1-2. Once established by the DoD for the JIE, all NPE identity attribute data and NPE persona would reside within or at least under the control of the DMDC. NPEs may have one or more personas that define the function and purpose as a form of NPE requester (e.g., device, service) or as an NPE resource (e.g., system, application, or facility).

Table 3-15 – Authoritative Non-Person Entity (NPE) Identity Attribute Data

➤ **(P2/R2) Assumptions**

- (Same as for P2/R1)

➤ **(P2/R2) Constraints**

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

➤ **(P2/R2) Risk**

- (Same as for P2/R1)

➤ **(P2/R2) Technical Positions and Patterns**

P2/R2 Policy/Regulation Profile

- *Policy in Credentialing*

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

Business Rule	Description
<i>The Army will use a DoD-issued personal identity verification (PIV) mechanism for Public Key Infrastructure certificates and other key person entity identity data.</i>	CAC – PIV v2.0-compliant cards will be used as the preferred authoritative credential mechanism to support any Public Key Infrastructure-based access within DoD. However, the DoD-issued CAC is an official identification mechanism that is currently used to support authentication and access control to unclassified DoD networks and information resources. Due to information spillage restrictions, the CAC cannot be and is not currently used to support digital identity data for access to classified information systems. This is due to security restrictions that prohibit a physical mechanism containing classified information, including the digital identity data related to classified access that would have to be resident on a CAC, from being physically connected to a classified system/user device.

	Therefore, a separate PIV mechanism (e.g., smartcard, SIPRNET token) must be issued.
--	--

Table 3-16 – Common Access Card (CAC) Usage

- **(P2/R3) Assumptions**
 - CAC provisioning is accurate at the time the CAC is issued.
 - The CAC Personal Identification Number (PIN) is uniquely bound to every CAC. Classified logical and physical resource access must be supported by a smart card or other separate digital identity mechanism.
- **(P2/R3) Constraints**
 - The CAC will be the primary form of PIV for any PE.
 - This business rule applies only to DoD CAC-holders who require access to logical NPE and both types of physical NPE resources.
 - If a CAC is lost, damaged or destroyed, an alternate non-CAC authentication methodology must be available.
- **(P2/R3) Risk**
 - Mobile or portable computing devices with network access may not always be able to interface physically with CAC readers.
 - Tactical environment access (logical and physical) to unclassified resources may not be capable of being supported by CAC-based authentication.
 - Tactical environment access (logical and physical) to classified resources may not be capable of being supported by smart cards alone.
- **(P2/R3) Technical Positions and Patterns**
 - P2/R3 Technical Standards Profile**
 - *Common Access Card (CAC)*
 - *Digital Certificate (PKI)*

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

Business Rule	Description
<p><i>Network domain, application and data resource accounts must be enabled by an enterprise directory service that supports all account provisioning as part of the access life-cycle management of all Army logical and physical resources.</i></p>	<p>DoD and SC directory, authentication, authorization and account management services are all currently provided within Microsoft Active Directory Forests and Domains and their supporting infrastructure, via a set of management services for :</p> <ul style="list-style-type: none"> • User accounts • Domain relationships • Lightweight Directory Access Protocol (LDAP) configuration • Authentication • Policies (User and Group) <p>An APS can support these existing Microsoft AD services generically as a set of IdAM components: ADR, DS and ASF/AAF. These IdAM components can exist in both non-tactical and tactical operations. In any case, as defined by this RA, an APS will be required. All PE and NPE access accounts will be created and managed by leveraging some or all of the PE and NPE identity attributes made available by the appropriate ADR.</p>

Table 3-17 – Resource Account Provisioning Service (APS)

- **(P2/R4) Assumptions**
 - The current DoD, Army and other SC Microsoft AD Forest/Domain infrastructures are being reconfigured.
 - The APS will eliminate the need to use external systems (e.g., currently Army EDS-Lite) to maintain ADR, DS and ASF/AAF identity data in each account.
 - Use of an enterprise/centralized provisioning service is an option for existing and future DoD, Army and other SC ADR, DS and ASF/AAF, but they must derive authorization policies only from the authoritative enterprise attribute data schema.
- **(P2/R4) Constraints**
 - Future DoD, Army and other SC ADRs and AAFs must derive authorization policies only from the authoritative enterprise attribute data schema.
 - The EIADRSS must maintain synchronization of identity data across all existing ADR, DS and ASF/AAF infrastructures across the JIE.
 - The EIADRSS must not identify attributes that are unique only to the Army or any one SC.
- **(P2/R4) Technical Positions and Patterns (Reference Appendix B – Pattern View)**
 - P2/R4 Technical Standards Profile**
 - *Digital Certificate (PKI)*
 - P2/R4 Policy/Regulation Profile**
 - *Policy in Authentication*

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

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

Table 3-18 – Adding Core Person Entity (PE) Identity Attributes

- **(P2/R5) Assumptions**
 - The required PE identity attributes do not already exist in the EIADRSS.
 - The required PE identity attributes may already exist in a DoD registered and approved authoritative data source.
- **(P2/R5) Constraints**
 - New attributes must never directly populate the EIADRSS.
 - The EIADRSS component must never maintain any Army or SC-unique PE identity data.
 - Proposed enterprise PE identity attributes for the Army must be submitted through a governance process that reviews and approves the request(s) prior to use by the Army or any SC within the JIE.

- **(P2/R5) Risk**
 - If proposed additional PE identity attributes are not vetted for non-ambiguity and re-usability by the Army and the other SCs, consistent and executable access policies cannot be inserted into the JIE.
- **(P2/R5) Technical Positions and Patterns (Reference Appendix B – Pattern View)**
 - P2/R5 Technical Standards Profile**
 - *Attribute Management Services*
 - *Authoritative Attribute Exchange Service*

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

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

Table 3-19 – Adding Core Non-Person Entity (NPE) Identity Attributes

- **(P2/R6) Assumptions**
 - The required “extended” NPE identity attributes do not already exist in the EIADRSS.
 - Resource NPE attribute data can be federated to the DoD enterprise level by the Army and the other SCs, but would be initially treated only as candidates to be added to the EIADRSS.
- **(P2/R6) Constraints**
 - Any NPE identity attributes added to the JIE data set must be provided by the EIADRSS.
 - Any “extended” NPE identity attributes and attribute data originate from a DoD authoritative data source.
 - No Army or SC-unique identity attributes for NPE will be created, stored or distributed within the Army or the JIE.
- **(P2/R6) Risk**
 - A Dynamic Access Policy Management Service (DAPMS) capability leveraging the EIADRSS will not be possible if NPE resource attribute data cannot be fully and accurately maintained.

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

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

P2/R6 Technical Standards Profile

- *Attribute Management Services*
- *Authoritative Attribute Exchange Service*

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

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

Table 3-20 – Non-Person Entity (NPE) Resource Data Federation

➤ **(P2/R7) Assumptions**

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

➤ **(P2/R7) Constraints**

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

➤ **(P2/R7) Risk**

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

➤ **(P2/R7) Technical Positions and Patterns**

P2/R7 Technical Standards Profile

- *Authentication Management Services*

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

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

Table 3-21 – Directory Information Updates

- **(P2/R8) Assumptions**
 - DoD/the Office of the Secretary of Defense (OSD) will provide retired military and civilian employees a uniform DoD identification card that can be easily recognized at any DoD base or facility within the United States and its territories or possessions.
- **(P2/R8) Constraints**
 - Access to DMDC (web site) requires a DoD certificate.
- **(P2/R8) Technical Positions and Patterns**
 - P2/R8 Technical Standards Profile**
 - *Authoritative Attribute Exchange Service*

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

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

Table 3-22 – Person Entity (PE) and Non-Person Entity (NPE) Identification

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

Business Rule	Description
<i>The Army will use the digital identity standards established by DoD 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 the Business Mission Area to tactical deployed assets, to include all devices that reside in the mobile, platform or sensor computing environments.

Table 3-23 – Mobile/Edge Platforms/Devices

- **(P3/R1) Assumptions**
 - Mobile/edge platforms and devices will have the ability to be credentialed in the same manner as any other NPE.
 - CAC or smartcard/token credentials will be the primary mechanism for user authentication for all Mobile/edge platforms and devices.
 - Classified user authentication and authorization will use a read-only smartcard/token and not a CAC.
 - Other forms of authentication will be available to authenticate and authorize users of Mobile/edge platforms and devices (e.g., explicit login, multiple PINs, test questions).
- **(P3/R1) Constraints**
 - Mobile/edge platforms and devices (such as NPEs) will each have a unique identifier and/or X.509 certificate(s).
 - Mobile/edge platforms and devices must have the ability to allow authentication while they are operating 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 devices.
 - A mobile device's unique ID or GUID must be a hardware integrated component of the device that cannot be redefined by users.
- **(P3/R1) Risk**
 - Mobile/edge platforms/devices (portable) may not be able to easily interface with CAC readers.
 - Resources can easily be compromised if portable computing/communications devices do not provide for at least two-factor authentication.

➤ **(P3/R1) Technical Positions and Patterns**

P3/R1 Technical Standards Profile

- *Identity Management*

P3/R1 Policy/Regulation Profile

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

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

Business Rule	Description
<i>Authorized mobile devices connected to Army networks will be bound to one or more user groups, and linked to a unique non-person entity identifier and DoD-issued PKI certificate using a digital identity standard registration and binding service.</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 device identifier.

Table 3-24 – Mobile Device Binding

➤ **(P3/R2) Assumptions**

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

➤ **(P3/R2) Constraints**

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

➤ **(P3/R2) Risk**

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

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

P3/R2 Technical Standards Profile

- *Identity Management*

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

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

Table 3-25 – Global Directory Services for Enterprise Services

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

Business Rule	Description
<i>The DoD enterprise global directory shall provide the ability to disseminate address lists to users of DoD and Army information and communications services.</i>	<p>The GAL is a directory service that contains information for users of Enterprise Email and other services, to include collaboration tools, instant messaging and Unified Capability services (i.e., integrated voice, data and video). JIE enterprise services users will utilize the Enterprise Directory GAL Service in multiple forms, to include but not be limited to:</p> <ul style="list-style-type: none"> • Voice over Internet working protocol (VoIP) lookups • File/information resource-sharing user information • Unclassified email service account identification • Classified email service account identification (a separate GAL based on the Enterprise Directory Service) • Peer-to-peer or broadcast video teleconferencing distribution

Table 3-26 – Global Address List (GAL) Distribution

- **(P4/R1) Assumptions**
 - DISA creates and manages the DoD GAL out of the NT-DS and T-DS data sourced from the EIADRSS.
 - DoD component mail systems will have the ability to include both DoD hosted and deployed SC tactical mail systems.
 - GAL addresses and contact information is federated from Army and other SC mail systems to the DoD enterprise GAL.
 - Dissemination of the enterprise GAL for use by disparate mail systems is based on need-to-know access policies.
- **(P4/R1) Constraints**
 - Any federated SC GAL address and contact information must first be reviewed and approved at the DoD level before being added to an enterprise-level DS and GAL/GAL views.
 - Access to the GAL to support email services must be network-specific, depending on information resource security classification.
 - GAL service structure and content must be agnostic to the hardware and software that it supports.
- **(P4/R1) Risk**
 - Significant impact to operations and information security would occur in the event that GAL information and GAL updates were intercepted by unauthorized entities.

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

P4/R1 Technical Standards Profile

- *Digital Certificate (PKI)*

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

Business Rule	Description
<i>DoD's global address list must allow for segmented views by Army organization, location/facility and/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 NT-DSs and T-DSs for DoD organizational views, and could also provide SC-specific GAL views. Distribution groups and views of any form of requester must also be supported. Similarly, resource views must also be provided as subsets of the resources identified in the DoD GAL.

Table 3-27 – Global Address List (GAL) Views

➤ **(P4/R2) Assumptions**

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

➤ **(P4/R2) Constraints**

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

➤ **(P4/R2) Risk**

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

(P4/R2) Technical Positions and Patterns

P4/R2 Technical Standards Profile

- *Global Directory Services for Enterprise Services*

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

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

Table 3-28 – Global Address List (GAL) Data Schema

- **(P4/R3) Assumptions**
 - The software and hardware used to access the GAL and GAL views comply with DISA Security Technical Implementation Guides (STIGs).
 - EIADRSS will provide NT-DS and T-DS attribute data using either scheduled or triggered web service data calls.
 - The directory service data schema is agnostic to the device and applications utilizing the GAL or GAL views, regardless of the information being delivered to the end user.
- **(P4/R3) Constraints**
 - Applications that use the NT-DS, T-DSs, GAL and GAL views and search services must have a Certification of Networkiness (CoN).
 - Web services used by GAL/GAL view services must utilize a standard web service data protocol.
 - The NT-DS and T-DS GAL data schemas must be based on a common data schema, which is a selective set of attributes sourced from the enterprise attribute repository (i.e., EIADRSS).
- **(P4/R3) Risk**
 - Changes to the NT-DS and T-DS data schema may impact the accuracy and effectiveness of all GAL services used by applications.
 - Application software updates may create security vulnerabilities or introduce interoperability problems within applications that utilize GAL services.
- **(P4/R3) Technical Positions and Patterns**
 - **P4/R3 Technical Standards Profile**
 - *Global Directory Services for Enterprise Services*

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

Business Rule	Description
<p><i>Army personnel will have access to a local directory address book that is available when network connectivity is not available, and that is synchronized with a DoD directory service when network connectivity is available.</i></p>	<p>There are times when Army email and other enterprise services users will not have network access, but still require access to a GAL and GAL views. An offline service will allow users to properly identify the correct resources that can be accessed. Because this service is subject to regular change, including removal of authorized requesters and resources, it must be regularly synchronized with EDSs when network connectivity is sufficiently available. The Army must determine the acceptable time lapse between sync points, and be willing to assume any consequential security and/or operational risks involved.</p>

Table 3-29 – Local Offline Address Book (OAB) Availability

- **(P4/R4) Assumptions**
 - Both the JIE and the user’s organizational or operating unit address book are accessible offline.
 - An offline address book will support access to address information both internal and external to the user’s organization or operating unit.
 - The local OAB synchronizes with a DoD directory service when network connectivity outages occur, and re-synchronized when connectivity is re-established.

- **(P4/R4) Constraints**
 - OAB information at rest and in transit must be protected by encryption, and must be distributed in a secure manner..
 - OABs must not be made available to offline users who are not locally authenticated.
- **(P4/R4) Risk**
 - Mobile hardware devices that have downloaded an address book could be lost or stolen.
 - Digital artifacts of a downloaded address book may remain on decommissioned or reassigned hardware, potentially providing unauthorized users access to DoD personnel information.
- **(P4/R4) Technical Positions and Patterns (Reference Appendix B – Pattern View)**
 - P4/R4 Technical Standards Profile**
 - *Global Directory Services for Enterprise Services*

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

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

Table 3-30 – Directory/Global Address List (GAL) Information Concurrency

- **(P4/R5) Assumptions**
 - An email user can be authenticated from any device.
 - The device being used to access DoD email is capable of assuring reliable and secure authentication mechanisms (i.e., tokens).
- **(P4/R5) Constraints**
 - User authentication must be tied to information/network classification.
- **(P4/R5) Risk**
 - Users sometimes lose mobile devices.
 - Users may mistakenly transmit sensitive information on the DoD network.
 - Hardware used to access information may be operational in unsecured areas.
- **(P4/R5) Technical Positions and Patterns (Reference Appendix B – Pattern View)**
 - P4/R5 Technical Standards Profile**
 - *Global Directory Services for Enterprise Services*

3.3.5 (P5) Principal 5 – Authentication and Authorization

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

Table 3-31 – Authentication and Authorization

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

Business Rule	Description
<i>All Army information services and applications must uniquely identify and authenticate users and devices using a common DoD authentication service model, regardless of the logical or physical resources to which access is being requested.</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 a certain persona. The effectiveness of any authorization service can be impacted by not performing this due diligence. This function can be provided by the current and collapsing DoD Microsoft AD infrastructure and other components, such as the EASF and the AAF.

Table 3-32 – Authentication and Authorization Scope

➤ (P5/R1) Technical Positions and Patterns

P5/R1 Technical Standards Profile

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

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

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

Table 3-33 – Identity Service for Tactical Edge

- **(P5/R2) Assumptions**
 - Internal DoD SCs and Joint PE and NPE will have established identities based on DoD-provisioned and -managed credentials (i.e., X.509 Certificates).
 - External non-DoD and coalition PE and NPE will have pre-established trusted credentials to the appropriate internal DoD PE and NPE.
 - Coalition PE and NPE will not be issued DoD CACs.
- **(P5/R2) Constraints**
 - Digital identities at the tactical edge must be portable and reusable during all phases of the ARFORGEN cycle.
 - Non-DoD and coalition partner trusted credentials must assure a high degree of non-repudiation.
- **(P5/R2) Risk**
 - The limited ability to establish the preferred and optimally reliable non-DoD and coalition partner credentialing mechanism (i.e., X.509 Certificates) for authentication will create a greater possibility of unauthorized access to DoD information and physical resources.
 - Theater personas required to support tactical operations may change often enough that they must be maintained in real time or near-real time to assure that authorization is adequately accurate and reliable.
- **(P5/R2) Technical Positions and Patterns (Reference Appendix B – Pattern View)**
 - P5/R2 Technical Standards Profile**
 - *Identity Based Access Control (IBAC)*

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

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

Table 3-34 – Global Information Resource Access

- **(P5/R3) Assumptions**
 - The Authentication Service is Computing Environment/device agnostic.
 - Mobile devices will use the same authentication service mechanisms and protocols as fixed or non-mobile clients.
- **(P5/R3) Constraints**
 - Requester re-authentication is required when a disconnected and/or network-disadvantaged (e.g., classified, tactical environments) device is reconnected to any network or network-based resource.
- **(P5/R3) Technical Positions and Patterns (Reference Appendix B – Pattern View)**
 - P5/R3 Technical Standards Profile**
 - *Secure Shell*

P5/R3 Policy/Regulation Profile

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

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

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

Table 3-35 – Access and Policy Security

- **(P5/R4) Assumptions**
 - An administrative interface is available to the PS to accommodate additional, modified or updated policies.
- **(P5/R4) Constraints**
 - Army access policies shall allow read-only capability to access control services and the components that utilize them.
 - Authorization components in any IdAM architecture must minimize the exposure of identity attribute data.
 - All authentication and authorization services and their supporting infrastructures must assure minimal exposure of sensitive identity data, at rest or in transit (e.g., PII, persona attribute data).
 - RE components shall have read-only access to identity ADRs.
- **(P5/R4) Technical Positions and Patterns**
 - P5/R4 Technical Standards Profile**
 - *Identity Based Access Control (IBAC)*
 - *Authentication Management Services*
 - *Secure Shell*

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

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

Table 3-36 – Availability of DoD Enterprise Authentication and Authorization Services

- **(P5/R5) Assumptions**
 - The current AKO SSO and RSO services will be replaced.
 - Any SSOS and RSOS will support either public or private cloud services, hosted by either a commercial service provider (e.g., Google Apps, Microsoft Azure) or DoD/DISA.
 - Future Web Apps that are not PKI-ready will be supported by DoD Enterprise Authentication and Authorization services.

➤ **(P5/R5) Technical Positions and Patterns**

P5/R5 Technical Standards Profile

- *Secure Shell*

P5/R5 Policy/Regulation Profile

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

3.3.5.6 **(P5/R6) Business Rule 6 – Availability of Army (Non-DoD Enterprise) Authentication and Authorization Services**

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

Table 3-37 – Availability of Army (Non-DoD Enterprise) Authentication and Authorization Services

➤ **(P5/R6) Assumptions**

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

➤ **(P5/R6) Constraints**

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

➤ **(P5/R6) Technical Positions and Patterns**

P5/R6 Technical Standards Profile

- *Authentication Management Services*
- *Authoritative Attribute Exchange Service*

3.3.6 (P6) Principle 6 – Dynamic Access Policy Management

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

Table 3-38 – Dynamic Access Policy Management

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

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

Table 3-39 – Policy Management Service Scope

➤ (P6/R1) Assumptions

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

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

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

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

Table 3-40 – Standard Attribute Model

➤ **(P6/R2) Technical Positions and Patterns**

Core Standards and Pattern View (Ref: Appendix B)

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

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

Table 3-41 – Standard Access Policies

➤ **(P6/R3) Assumptions**

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

➤ **(P6/R3) Constraints**

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

➤ **(P6/R3) Risk**

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

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

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

Table 3-42 Policy Change Management Responsibility

- **(P6/R4) Assumptions**
 - A common DoD information resource portal service will use all resource access policies that have been created and are being maintained for them.
- **(P6/R4) Constraints**
 - Access Policy changes to JIE-available Army resources must not be solely managed by the Army.
 - Policy template, structures and syntax must be identical across the JIE.
 - All access policies must be in compliance with federal laws and DoD guidance, as well as SC regulations.
- **(P6/R4) Risk**
 - If access policy management cannot be automated and governed rapidly and reliably, the process for implementing new or modifying existing access policies may be lengthy, thus causing possible operational capability functional gaps and delays.
- **(P6/R4) Technical Positions and Patterns (Reference Appendix B – Pattern View)**

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

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

Table 3-43 – Policy Attribute Validation

- **(P6/R5) Assumptions**
 - An alternative form of trusted credentials for non-DoD and coalition PE and NPE has been issued.
 - External non-DoD and coalition PE and NPE credentials are trusted by the appropriate internal DoD NPE.
 - Policy decisions are based on current and executable policies.
- **(P6/R5) Constraints**
 - Coalition PE must not be issued DoD CACs
 - DoD access control components must accept alternative credentials.
 - Non-DoD and coalition partner trusted credentials must assure a high degree of non-repudiation.
 - Non-DoD and coalition partner trusted credentials must be capable of supporting two-factor authentication.
 - Before an access policy is fully executed and authorization controls are applied, attributes utilized in the policy’s execution must be affirmed, as well as the basic structure, taxonomy and language of the policies themselves.

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

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

Table 3-44 – Access to Data, Services and Applications

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

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

Table 3-45 – Information Resource Types

- **(P7/R1) Assumptions**
 - All information systems and data resources are classified as NPE.
 - A set of identity attributes exists for each information resource type and data element.
- **(P7/R1) Constraints**
 - Every information system/device (as an NPE) must have a valid and unique credential (i.e., PKI certificate).
 - Every information system/device will have a unique permanent NPE identifier, and any PE will have an EDI-PI (e.g., mobile device Electronic Serial Number).
 - Access to information resources must be dictated by a managed and automated set of security policies.
- **(P7/R1) Risk**
 - Changes in information resource attributes that are not conveyed either in real time or near-real time to RE mechanisms may impact authorization requests.
 - Portability of information JIE-available resources requires careful management and distribution of their identity attributes and associated access policies across the entire JIE.

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

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

Table 3-46 – Logical NPE Layered Logical Access Control

- **(P7/R2) Assumptions**
 - Logical NPE is characterized by groups, distribution lists, systems, software/applications, data and other Army intellectual or informational assets.
- **(P7/R2) Technical Positions and Patterns**
 - P7/R2 Technical Standards Profile**
 - *Standardized Policy Languages*

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

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

Table 3-47– Public Key Infrastructure (PKI) Based Authentication

- **(P7/R3) Assumptions**
 - An X.509 certificate management service will be available at all times, unless there is a loss of infrastructure and/or local or wide-area network connectivity failure impacting it. In such cases, any Army authentication and/or access authorization service will limit access to one or more local devices only.
- **(P7/R3) Constraints**
 - PKI transactions will be transported across network boundaries encapsulated in Security Assertion Markup Language (SAML) tokens for Web Service (WS) or WS-protocols
 - Kerberos, Simple Sockets Application Programming Interface (SSAPI) and Secure Socket Layer (SSL)/Transport Layer Security (TLS) protocols and their secure transport will be used when SAML/WS cannot.

- **(P7/R3) Risk**
 - An unauthorized user or malicious hacker may attempt to hijack a SAML token and replay it to gain illicit access to DoD information resources (i.e., a replay attack).
- **(P7/R3) Technical Positions and Patterns**
 - P7/R3 Policy/Regulation Profile**
 - *Army IdAM RA to Army Regulation (AR) 25-2 Mapping*

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

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

Table 3-48 – Data Resource Identification

- **(P7/R4) Assumptions**
 - Data tagging is standardized for all JIE information resources.
 - Data tagging is XML based and conforms to a standard metadata schema.
- **(P7/R4) Constraints**
 - Data tagging must conform to approved DoD standards (i.e., DoD IT Standards Registry).
 - The DoD enterprise DAPMS must confirm that a data tag has been applied to all data resources to which authorization policy can be applied.
 - Data tags must be maintained and synchronized in all attribute data that identify information resources (e.g., in a DAPMS PS with NPE resource attribute data provided by the EIADRSS).
- **(P7/R4) Risk**
 - Without regular auditing to ensure the consistency of data tags at both the JIE and SC levels, resources will not be correctly identified and authorization policies cannot be executed correctly.
 - Failure to synchronize data tags in all ADRs may prevent authorized resource access or allow unauthorized resource access.

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

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

Table 3-49 – Rules Engine (RE) Personally Identifiable Information (PII) Attribute Exposure

- **(P7/R5) Assumptions**
 - If the PS is not co-located with the other sub-components of RE, requester PII data will be required to transit a network in order to be consumed by an RE.
 - The PDP will render decisions based on the same PII attribute data that are used by the DoD enterprise AAF and SSOS.
- **(P7/R5) Constraints**
 - PS will not be collocated with PII when adequate networking capability is available.
 - All PII attribute data in transit and temporarily at rest must be encrypted.
 - The PDP must internally and automatically delete all PII attribute data after it has rendered its access decision.
 - PE identity attribute data must be accessed, utilized and deleted by the RE sub-services (i.e., PDP and PS).
 - The EIADRSS must provide all PII attribute data to the RE.
 - The PDP must retrieve all PII attribute data that are required to render an access decision via the DoD enterprise AAF, SSOS and RSOS, which are sourced from the EIADRSS.
 - If not collocated with the RE, the PS must internally and automatically delete all PII attribute data after it has completed providing services to the PDP.
 - The PEP must never receive any PII attribute data.
- **(P7/R5) Risk**
 - Any failure to deliver authoritative and accurate PII attribute data to the RE will result in an authorization failure and allow access to unauthorized resources.
 - Separation and duplication of ADR sources and PSs to support the RE over a network increase the possibility of PII compromise.
- **(P7/R5) Technical Positions and Patterns (Reference Appendix B – Pattern View)**

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

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

Table 3-50 – Data Tagging Development

- **(P7/R6) Assumptions**
 - Data tagging is standardized, at a minimum, within the individual SC information resources.
 - Data tagging is XML-based, and conforms to a standard metadata schema.
- **(P7/R6) Constraints**
 - Data tagging must conform to approved DoD (i.e., DISR) standards.
 - A DoD enterprise RE must constantly re-confirm that a data tag has been applied to all application and data resources to which authorization policy can be applied.
 - Data tags will be maintained and synchronized in a DAPMS PS with those utilized by the EIADRSS.
 - All Service Components will use a common SDK.
 - All SCs must use the same standards schema and syntax.
- **(P7/R6) Risk**
 - Without regular auditing to ensure the consistency of data tags at both the JIE and SC levels, resources will not be correctly identified and authorization policies cannot be executed correctly.
 - Failure to synchronize data tags in all ADRs may prevent authorized resource access or allow unauthorized resource access.
 - Unless data tagging is protected on the information resource side as well as at the RE, a flaw in XML encryption can leave web services carrying tag metadata vulnerable to attacks and “hijacking”.
- **(P7/R6) Technical Positions and Patterns**
 - P7/R6 Technical Standards Profile**
 - *Standardized Policy Languages*
 - P7/R3 Policy/Regulation Profile**
 - *Army IdAM RA to Army Regulation (AR) 25-2 Mapping*

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

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

Table 3-51 – Standardized Policy Languages

- **(P7/R7) Assumptions**
 - DoD and the SCs will create, concur on and collectively maintain XACML-based access policies using the same SDK for all authorization services that can be supported by XACML.
- **(P7/R7) Constraints**
 - Existing legacy systems must create and implement a migration plan if they are not currently compliant.
- **(P7/R7) Technical Positions and Patterns**
 - P7/R7 Technical Standards Profile**
 - *Standardized Policy Languages*

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

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

Table 3-52 – Access Policy Data Tagging Metadata Standards

- **(P7/R8) Technical Positions and Patterns**
 - P7/R8 Technical Standards Profile**
 - *Policy in Credentialing*
 - P7/R8 Policy/Regulation Profile**
 - *Army IdAM RA to Army Regulation (AR) 25-2 Mapping*

3.3.8 (P8) Principle 8 – Physical Access

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

Table 3-53 – Physical Access

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

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

Table 3-54 – Non-Person Entity (NPE) Unique Identifier

➤ (P8/R1) Technical Positions and Patterns

P8/R1 Technical Standards Profile

- *Authoritative Attribute Exchange Service*

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

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

Table 3-55 – Physical Access Control Policies

➤ (P8/R2) Technical Positions and Patterns

P8/R2 Technical Standards Profile

- *Cryptography Algorithms*
- *Attribute Management Services*

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

Business Rule	Description
<i>The Army must implement processes to continuously verify and maintain attributes related to physical assets/non-person entities.</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, ordnance and other physical DoD assets.

Table 3-56 – Person Entity (NPE) Attribute Verification

➤ (P8/R3) Assumptions

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

➤ **(P8/R3) Technical Positions and Patterns**

P8/R3 Technical Standards Profile

- *Attribute Management Services*

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

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

Table 3-57 – Facilities Attributes Management

➤ **(P8/R4) Technical Positions and Patterns**

P8/R4 Technical Standards Profile

- *Attribute Management Services*
- *Authoritative Attribute Exchange Service*

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

Business Rule	Description
<i>The principal credential mechanism for identity authentication to allow access to any facility or physical asset will be the Common Access Card -DoD PIV credential.</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 support multiple physical access systems, but the desired environment is CAC-based PKI, the same as for access control to all logical resources. Access to classified and/or tactical resources currently requires use of a separate token smart card.

Table 3-58 – Common Access Card (CAC) Credential Mechanism

➤ **(P8/R5) Technical Positions and Patterns**

P8/R5 Technical Standards Profile

- *Common Access Card (CAC)*

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

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

Table 3-59 – Common Access Card (CAC) Enrollment

➤ **(P8/R6) Technical Positions and Patterns**

P8/R6 Technical Standards Profile

- *Common Access Card (CAC)*

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

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

Table 3-60 – Layered Physical Access Control for Subclass Type 1 Physical NPEs

- **(P8/R7) Assumptions**
 - Subclass 1 physical NPEs are characterized by locations/areas, bases, installations, facilities, buildings, rooms and other Army real property assets.
- **(P8/R7) Technical Positions and Patterns**
 - P8/R7 Technical Standards Profile**
 - *Authentication Management Services*
 - *Authoritative Attribute Exchange Service*

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

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

Table 3-61 – Layered Physical Access Control for Subclass Type 2 Physical NPEs

- **(P8/R8) Assumptions**
 - Subclass 2 physical NPEs include hardware, devices and other Army assets.
- **(P8/R8) Technical Positions and Patterns**
 - P8/R8 Technical Standards Profile**
 - *Authentication Management Services*
 - *Authoritative Attribute Exchange Service*

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

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

Table 3-62 – Physical Access Control – Subclass Type 1 NPE Asset Naming

- **(P8/R9) Assumptions**
 - Subclass 1 physical NPEs are characterized by locations/areas, bases, installations, facilities, buildings, rooms and other Army assets.

- **(P8/R9) Technical Positions and Patterns**

- P8/R9 Technical Standards Profile**

- *Digital Certificate (PKI)*

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

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

Table 3-63 – Physical Access Control – Subclass Type 2 NPE Asset Naming

- **(P8/R10) Assumptions**
 - Subclass 2 physical NPEs include hardware, devices and other Army assets.

- **(P8/R10) Technical Positions and Patterns**

- P8/R10 Technical Standards Profile**

- *Digital Certificate (PKI)*

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

Principle	Description
<i>A comprehensive security policy must exist to address all aspects of identity management services and establish the information assurance/security guidelines required to mitigate threats to related infrastructures, both internal and external to Army and DoD networks.</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 those areas. Many overarching IA standards will also be applicable (e.g., authentication mechanism transport, cross-domain capabilities and information classification restrictions).

Table 3-64 – General Identity and Access Management (IdAM) Security Policy

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

Business Rule	Description
<i>Digital identity attribute data must be validated within Army and DoD networks and systems to ensure that it conforms to relevant DoD-approved standard schema.</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 that can be verified/re-verified on both a scheduled and ad hoc basis, as required, is employed. This capability is essential to ensuring that the authorization service executes effectively and securely.

Table 3-65 – Identity Attribute Data Validation

➤ (P9/R1) Technical Positions and Patterns

P9/R1 Technical Standards Profile

- *Biometric Validation*

P9/R1 Policy/Regulation Profile

- *Policy in Credentialing*

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

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

Table 3-66 – Authorization Service Scope

➤ (P9/R2) Technical Positions and Patterns

P9/R2 Technical Standards Profile

- *Policy in Credentialing*

P9/R2 Policy/Regulation Profile

- *Policy in Credentialing*

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

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

Table 3-67 – Enterprise Information Sharing

➤ (P9/R3) Technical Positions and Patterns

P9/R3 Policy/Regulation Profile

- *Policy in Credentialing*
- *Policy in Authentication*

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

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

Table 3-68 – Information Resource Authentication Frequency

➤ (P9/R4) Technical Positions and Patterns

P9/R4 Technical Standards Profile

- *Web Services Security*
- *Attribute Management Services*

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

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

Table 3-69 – Cross-Domain Security

➤ **(P9/R5) Technical Positions and Patterns**

P9/R5 Technical Standards Profile

- *Identity Management*

P9/R5 Policy/Regulation Profile

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

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

Business Rule	Description
<i>Army information resources, including data assets, services and applications, must be accessible to all authorized DoD requesters, except where limited by law, policy, security classification or unique operational requirements.</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 networks. This business rule mandates that DoD IdAM services and infrastructure conform to all federal, state and local laws, policies and regulations in terms of making the right information available to the right authorized requesters. Enabling network-access enforcement or control points will protect the JIE from potential enemies attempting to access and steal sensitive information, as well as damage key infrastructure components.

Table 3-70 – Information Resources Availability

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

Business Rule	Description
<i>Army information resources, including applications and computer networks, must protect data in transit and at rest according to their confidentiality level, Mission Assurance Category and level of exposure when executing identity management and encryption services.</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 they are only consumable by authorized DoD personnel. This encryption must protect the data regardless of status (i.e., in transit, at rest). The encryption strength, the level of protection and the exposure of encryption keys should be aligned with the various levels of information or resource sensitivity.

Table 3-71 – Information/Data Resources Protection

➤ **(P9/R7) Technical Positions and Patterns**

P9/R7 Technical Standards Profile

- *Information Assurance*

P9/R7 Policy/Regulation Profile

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

3.3.9.8 (P9/R8) Business Rule 8 – DoD Enterprise Trust Management

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

Table 3-72 – DoD Enterprise Trust Management

➤ (P9/R8) Technical Positions and Patterns'

P9/R8 Technical Standards Profile

P9/R8 Policy/Regulation Profile

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

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

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

Table 3-73 – Alternate Authentication Mechanisms (Non-CAC/Token)

➤ (P9/R9) Assumptions

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

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

P9/R9 Technical Standards Profile

P9/R9 Policy/Regulation Profile

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

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

Business Rule	Description
<i>All Army digital identity data will use encryption methods to ensure data integrity and protection of sensitive and regulated information (e.g., PII) and authentication data transport.</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 components, along with securing the network infrastructure itself, is required.

Table 3-74 – Alternate Authentication Mechanisms (Non-CAC/Token)

➤ (P9/R10) Technical Positions and Patterns

P9/R10 Technical Standards Profile

- *Encryption & Decryption*
- *Cryptography Algorithms*

P9/R10 Policy/Regulation Profile

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

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

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

Table 3-75 – SHA-256: Secure Hashing Algorithm Migration

➤ (P9/R11) Technical Positions and Patterns

P9/R11 Technical Standards Profile

- *Credential Management*
- *Authoritative Attribute Exchange Service*

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

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

Table 3-76 – Single Sign-On (SSO) and Reduced Sign-On (RSO)

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

Business Rule	Description
<i>Identity information used by the Army to enable single sign-on or reduced sign-on services must be automatically populated from a DoD enterprise directory service.</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 call, web service “pull” or “push”).

Table 3-77 – SSO and RSO Directory Data Population

- **(P10/R1) Assumptions**
 - Core identity attributes are made available via the EIADRSS and user address information via the NT-DSs and T-DSs.
 - SC directory services can be directly managed by the SCs.
 - Identity records are enduring, unless deactivated or deleted based upon administrative decision and action.
- **(P10/R1) Risk**
 - The quality of SC-level directory service concurrency depends on the combined level of latency of all identity information passing from the DoD authoritative data sources to the NT-DSs and T-DSs.
- **(P10/R1) Technical Positions and Patterns**
 - P10/R1 Technical Standards Profile**
 - *Identity Based Access Control (IBAC)*
 - *Authentication Management Services*

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

Business Rule	Description
<i>For Army single sign-on and reduced sign-on services, the Army will use the DoD Electronic Data Interchange Personal Identifier (EDI-PI) to tie any PE uniquely to a DoD DMDC-formatted enterprise user name or DoD Enterprise Email display name format.</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.

Table 3-78 – Electronic Data Interchange Personal Identifier (EDI-PI)

➤ **(P10/R2) Technical Positions and Patterns**

P10/R2 Technical Standards Profile

- *Identity Based Access Control (IBAC)*
- *Authentication Management Services*

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

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

Table 3-79 – SSO and RSO Services Availability

➤ **(P10/R3) Technical Positions and Patterns**

P10/R3 Technical Standards Profile

- *Authoritative Attribute Exchange Service*

P10/R3 Policy/Regulation Profile

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

3.3.11 (P11) Principle 11 – Network Access Controls

Principle	Description
<i>Permission to or denial of access to Army and DoD network nodes for any device must be based on access policies that leverage specific sets of networking attributes.</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 DoD systems and networks. Empowering the identity and access management system with the capability to control DoD systems and network access based on predefined digital characteristics of a network (e.g., TCP ports or range of ports, IP addresses, devices ID, etc.) adds another layer of security to the protection of DoD resources.

Table 3-80 – Network Access Controls

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

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

Table 3-81 – Authorization Policy Network Attributes

- **(P11/R1) Assumptions**
 - Authorization access policies are established by DISA and the governing SC.
 - All JIE information or system resources will be listed in the DoD NT-DSs and T-DSs.
- **(P11/R1) Constraints**
 - Common network attributes must be used to identify all DoD information resources.
- **(P11/R1) Risk**
 - Access to the NT-DSs and T-DSs will provide an unauthorized user access to information pertaining to all DoD resources that are available to the JIE.
- **(P11/R1) Technical Positions and Patterns**
 - P11/R1 Technical Standards Profile**
 - *Attribute Management Services*
 - P11/R1 Policy/Regulation Profile**
 - *Policy in Authentication*

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

Business Rule	Description
<i>For all Army network-connected devices, prior to granting authorization to</i>	Authentication is required to authorize access to local devices and information, as well as networked resources.

<p><i>enterprise resources, user authentication must first be executed at the standalone-device level, then at the enterprise Army or DoD level using an enterprise authentication service.</i></p>	<p>Redundant authentication provides synchronization between local devices and their stored information as well as DoD networks. It ensures that proper access rights are given to proper users regardless of whether network connectivity is available.</p>
---	--

Table 3-82 – Network-Connected Device Authentication

- **(P11/R2) Assumptions**
 - Electronic devices that have access to DoD resources and networks have a local authentication service installed.
 - Local and DoD enterprise authentication services are synchronized.
 - The DoD enterprise authentication service is the authoritative source for verifying and authenticating a user’s credentials.
 - Synchronization between local and DoD enterprise authentication services occurs when a device has connectivity to the DoD network.
- **(P11/R2) Constraints**
 - Electronic devices must be password protected.
 - Electronic devices must be encrypted.
 - A user has a set number of device incorrect log-in attempts to gain access to the device and network before the user is locked out of the local device and DoD networks.
- **(P11/R2) Risk**
 - Long periods without connectivity to DoD authentication services could allow unauthorized access to a local device.
- **(P11/R2) Technical Positions and Patterns (Reference Appendix B – Pattern View)**
 - **P11/R2 Technical Standards Profile**
 - *Identity Based Access Control (IBAC)*
 - *Common Access Card (CAC)*

3.3.11.3 **(P11/R3) Business Rule 3 – Disconnected and/or Network-Disadvantaged Authentication**

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

Table 3-83 – Disconnected and/or Network-Disadvantaged Authentication

- **(P11/R3) Assumptions**
 - Authentication to all DoD devices, connected and/or disconnected, is required.
 - The user's CAC holds the proper credentials used for authentication to the local device.
- **(P11/R3) Constraints**
 - Authentication for a new user to access a local device and DoD networks must initially be performed by the DoD Enterprise IdAM services.
 - Access should be denied to a user trying to access an unconnected device for the first time.
- **(P11/R3) Risk**
 - CAC credentials/certificates are the only means to control or revoke access to a disconnected device.
- **(P11/R3) Technical Positions and Patterns (Reference Appendix B – Pattern View)**
 - P11/R3 Technical Standards Profile**
 - *Identity Management*
 - *Common Access Card (CAC)*
 - P11/R3 Policy/Regulation Profile**
 - *Army IdAM RA to Army Regulation (AR) 25-2 Mapping*

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

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

Table 3-84 – Network Gateway Authentication and Authorization

- **(P11/R4) Assumptions**
 - The DoD enterprise authentication service is the authoritative source for verifying and authenticating a user's identity and credentials.
 - All extended networks have resident (local) authentication and authorization services available.
 - All users accessing DoD networks and JIE information resources must possess a CAC.
- **(P11/R4) Constraints**
 - Common gateways must meet DoD cross-domain security requirements and policies, where applicable.
 - Extended networks without a common gateway will not have access to DoD enterprise authentication and authorization services.

- **(P11/R4) Risk**
 - A network gateway that allows access to DoD enterprise authentication and authorization services can also provide a possible intruder point of entry to another network and its available information resources.
- **(P11/R4) Technical Positions and Patterns**
 - P11/R4 Technical Standards Profile**
 - *Cryptography Algorithms*

3.3.12 (P12) Principle 12 – Monitoring and Reporting

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

Table 3-85 – Monitoring and Reporting

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

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

Table 3-86 – Auditing Services

- (P12/R1) Assumptions
 - Offline Address Books (OAB) will be auditable.
- (P12/R1) Technical Positions and Patterns
 - P12/R1 Technical Standards Profile**
 - *Cryptography Algorithms*
 - P12/R1 Policy/Regulation Profile**
 - *Policy in Authentication*
 - *Army IdAM RA to Army Regulation (AR) 25-2 Mapping*

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

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

Table 3-87 – Identity and Access Management (IdAM) Infrastructure-Monitoring/Reporting

- (P12/R2) Technical Positions and Patterns
 - P12/R2 Technical Standards Profile**
 - *Global Directory Services for Enterprise Services*
 - P12/R2 Policy/Regulation Profile**
 - *Army IdAM RA to Army Regulation (AR) 25-2 Mapping*

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

Identity and Attribute Management Vocabulary

Access Control: The collection of all controls used to assure that a person, as well as non-person entities, would have access only to information processing facilities for which he or she is 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 principal's or system's 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, 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 and 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 the number of discrepancies.

Proxy: An entity authorized to act for another.

- a) Authority or power to act for another.

b) A document giving such authority. [Merriam-Webster's.]

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 principal.

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: A set of "groups" that have a set of permissions and policies to which security principals are assigned.

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 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 failure 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 to access resources by using a single set of credentials to access systems and/or 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 the computer programs that process them. [XML]

Acronym List

AAF	Authentication and Authorization Framework
AC	Access Control (this acronym is used when referencing the Access Control family)
ACP	Allied Communications Publications
AD	Active Directory
ADR	Attributes Data Repository
ADS2	Application and Data Services
AEN	Army Enterprise Network
AFATDS	Advanced Forward Area Tactical Data System
AGS	Authentication Gateway Service
AKO	Army Knowledge Online
ANSI	American National Standards Institute
API	Application Programming Interface
APS	Account Provisioning Service
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
BCT	Brigade Combat Team
C&A	Certification and Accreditation
C2	Command and Control
CAC	Common Access Card
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COCOM	Combatant Command
COE	Common Operating Environment
COI	Communities of Interest
COL	Colonel
CoN	Certification of Networthiness
CONUS	Continental United States
COOP	Continuity of Operations Plan

COTS	Commercial off the Shelf
DECC	DISA Enterprise Computer Center
DEERS	Defense Enrollment Eligibility Reporting System
DES	Data Encoding Specification
DIG	Description and Implementation Guide
DISA	Defense Information Systems Agency
DISR	DoD IT Standards Registry
DMDC	Defense Manpower Data Center
DDMS	DoD Discovery Metadata Specification
DNS	Domain Name Service
DoD	Department of Defense
DoDAF	DoD Architecture Framework
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DS	Directory Service
EAAF	Enterprise Authentication and Authorization Framework
EASF	Enterprise Authentication Service Framework
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
EMI	Electro-magnetic Interface
ESR	Enterprise Strategy and Implementation Roadmap
FACC	Feature and Attribute Coding Catalogue
FICAM	Federal Identity, Credential and Access Management
FIPS	Federal Information Processing Standard
FOUO	For Official Use Only
G-3/5/7	Army Deputy Chief of Staff for Operations
GAL	Global Address List
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GFEBs	General Fund Enterprise Business System
GIG	Global Information Grid
GOTS	Government off the Shelf
GUID	Global Unique Identifier
HR	Human Resources
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
IC	Intelligence Community
ICAM	Identity, Credential and Access Management
ICD	Initial Capabilities Document
ID	Identification
IdAM	Identity and Access Management
IDC	Identity Consumer
IDD	Integrated Data Dictionary
IdSS	Identity Synchronization Service
IEA	Information Enterprise Architecture
IEC	International Electrotechnical Commission

IETF	Internet Engineering Task Force
IM	Instant Messaging
INCITS	International Committee for Information Technology Standards
IP	Internet Protocol
IT	Information Technology
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
JIE	Joint Information Environment
LAC	Logical Access Control
LDAP	Lightweight Directory Access Protocol
LTC	Lieutenant Colonel
ME	Mission Environment
MIB	Management Information Base
MS	Microsoft
NAVSUP	Naval Supply Systems Command
NETCOM	Network Enterprise Technology Command
NIE	Network Integration Evaluation
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
NSA	National Security Agency
NSPD	National Security Presidential Directive
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
OAB	Offline Address Books
OASIS	Organization for the Advancement of Structured Information Standards
OSD	Office of the Secretary of Defense
OV	Operational View
PAC	Physical Access Control
PCC	Personnel Category Code
PDP	Policy Decision Point
PE	Person Entity
PEP	Policy Enforcement Point
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIP	Personnel Identity Protection
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification Interoperable
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
PS	Policy Store
RA	Reference Architecture
RBAC	Role-Based Access Control
RE	Rules Engine
RF	Radio Frequency

RFC	Request for Comments
RSA	Rivest, Shamir and Adleman
RSOS	Reduced Sign-On Services
SAML	Security Assertion Markup Language
SC	Service Component
SDK	Software Development Kit
SGT	Sergeant
SHA	Secure Hash Algorithm
SLA	Service-Level Agreement
SOAP	Simple Object Access Protocol
SP	Special Publication
SSAPI	Simple Sockets API
SSH	Secure Shell Protocol
SSL	Secure Socket Layer
SSO	Single-Sign On
SSOS	Single-Sign On Service
STIG	Security Technical Implementation Guide
STRATCOM	Strategic Command
SV	System View
T-AFF	Tactical Authentication and Authorization Framework
T-APS	Tactical Accounts Provisioning Service
T-ASF	Tactical Authentication Service Framework
TCP	Transmission Control Protocol
T-DS	Tactical Directory Service
TLS	Transport Layer Security
TRADOC	Training and Doctrine Command
T-RSOS	Tactical Reduced Sign-On Service
T-SSOS	Tactical Single Sign-On Service
U.S.	United States
UC	Unified Capabilities
UCore	Universal Core
URL	Uniform Resource Locator
WAN	Wide Area Network
WS	Web Service
WSF	Web Services Framework
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

Army IdAM RA Principles and Business Rules References

Draft DoD Identity and Access Way Forward: DoD ICAM Transition, (Draft) 1.3, 08 May 2012	
Principle or Rule	
P1 – Unique Identity and Credentials	
P1/R1 – Person Entity (PE) Unique Identifier	
P1/R2 – Allowed Identities	
P1/R3 – Persona Life Cycle Management	
P1/R4 – Identity Data Integrity	
P1/R7 – Identity Data Conformance	
P2 – Authoritative Identity Data Source	
P2/R3 – Common Access Card (CAC) Usage	

P2/R5 – Adding Core Person Entity (PE) Identity Attributes	
P3 – Person Entity (PE) and Non-Person Entity (NPE) Identification	
P3/R1 – Mobile/Edge Platforms/Devices	
P3/R2 – Mobile Device Binding	
P4 – Global Directory Services for Enterprise Services	
P4/R5 – Directory/Global Address List (GAL) Information Concurrency	
P5 – Authentication and Authorization	
P6 – Dynamic Access Policy Management	
P6/R1 – Policy Management Service Scope	
P6/R3 – Standard Access Policies	
P6/R4 – Policy Change Management Responsibility	
P7 – Access to Data, Services and Applications	
P7/R1 – Information Resource Types	
P7/R2 – Logical NPE Layered Logical Access Control	
P7/R3 – Public Key Infrastructure (PKI) Based Authentication	
P7/R4 – Data Resource Identification	
P7/R6 – Data Tagging Development	
P7/R7 – Standardized Policy Languages	
P7/R8 – Access Policy Data Tagging Metadata Standards	
P8 – Physical Access	
P8/R1 – Non-Person Entity (NPE) Unique Identifier	
P8/R2 – Physical Access Control Policies	
P8/R3 – Non-Person Entity (NPE) Attribute Verification	
P8/R4 – Facilities Attributes Management	
P8/R5 – Common Access Card (CAC) Credential Mechanism	
P8/R6 – Common Access Card (CAC) Enrollment	
P8/R7 – Layered Physical Access Control for Subclass Type 1 Physical NPEs	
P8/R8 – Layered Physical Access Control for Subclass Type 2 Physical NPEs	
P8/R9 – Physical Access Control – Subclass Type 1 NPE Asset Naming	
P8/R10 – Physical Access Control – Subclass Type 2 NPE Asset Naming	
DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), March 20, 2012	
Principle or Rule	
P1/R1 – Person Entity (PE) Unique Identifier	
P1/R8 – Authentication and Authorization Service Provisioning	
P2/R1 – Authoritative Person Entity (PE) Identity Attribute Data	
P2/R2 – Authoritative Non-Person Entity (NPE) Identity Attribute Data	
P2/R3 – Common Access Card (CAC) Usage	
P2/R4 – Resource Account Provisioning Service (APS)	
P2/R5 – Adding Core Person Entity (PE) Identity Attributes	
P2/R6 – Adding Core Non-Person Entity (NPE) Identity Attributes	
P2/R7 – Non-Person Entity (NPE) Resource Data Federation	
P2/R8 – Directory Information Updates	
P3 – Person Entity (PE) and Non-Person Entity (NPE) Identification	
P4/R1 – Global Address List (GAL) Distribution	
P4/R2 – Global Address List (GAL) Views	
P4/R3 – Global Address List (GAL) Data Schema	
P4/R4 – Local Offline Address Book (OAB) Availability	
P4/R5 – Directory/Global Address List (GAL) Information Concurrency	
P5/R4 – Access and Policy Security	
P5/R5 – Availability of DoD Enterprise Authentication and Authorization Services	
P5/R6 – Availability of Army (Non-DoD Enterprise) Authentication and Authorization Services	
P6/R1 – Policy Management Service Scope	
P6/R4 – Policy Change Management Responsibility	

P6/R5 – Policy Attribute Validation	
P7/R3 – Public Key Infrastructure (PKI) Based Authentication	
P7/R4 – Data Resource Identification	
P7/R5 – Rules Engine (RE) Personally Identifiable Information (PII) Attribute Exposure	
P7/R6 – Data Tagging Development	
P9/R2 – Authorization Service Scope	
FICAM Roadmap and Implementation Guidance v2.0 – December, 2011	
Principle or Rule	
P1/R2 – Allowed Identities	
P1/R3 – Persona Life Cycle Management	
P1/R4 – Identity Data Integrity	
P1/R5 – Person Entity (PE) – Identity Data Discoverability	
P1/R6 – Non-Person Entity (NPE) – Identity Data Discoverability	
P1/R7 – Identity Data Conformance	
P1/R8 – Authentication and Authorization Service Provisioning	
P1/R9 – Enterprise Identity Attribute Utilization	
P2 – Authoritative Identity Data Source	
P2/R4 – Resource Account Provisioning Service (APS)	
P2/R5 – Adding Core Person Entity (PE) Identity Attributes	
P3 – Person Entity (PE) and Non-Person Entity (NPE) Identification	
P3/R1 – Mobile/Edge Platforms/Devices	
P3/R2 – Mobile Device Binding	
P4 – Global Directory Services for Enterprise Services	
P4/R5 – Directory/Global Address List (GAL) Information Concurrency	
P5 – Authentication and Authorization	
P6 – Dynamic Access Policy Management	
P6/R1 – Policy Management Service Scope	
P6/R4 – Policy Change Management Responsibility	
P7 – Access to Data, Services and Applications	
P7/R1 – Information Resource Types	
P7/R3 – Public Key Infrastructure (PKI) Based Authentication	
P7/R4 – Data Resource Identification	
P7/R6 – Data Tagging Development	
P7/R7 – Standardized Policy Languages	
P7/R8 – Access Policy Data Tagging Metadata Standards	
P8 – Physical Access	
P8/R1 – Non-Person Entity (NPE) Unique Identifier	
P8/R2 – Physical Access Control Policies	
P8/R3 – Non-Person Entity (NPE) Attribute Verification	
P8/R4 – Facilities Attributes Management	
P9 – General Identity and Access Management (IdAM) Security Policy	
P9/R1 – Identity Attribute Data Validation	
P9/R10 – Data Encryption	
P10 – Single Sign-On (SSO) and Reduced Sign-On (RSO)	
P10/R1 – SSO and RSO Directory Data Population	
DoD Information Enterprise Architecture (IEA) Version 2.0 - Draft Vol. II, February 2012	
Principle or Rule	
P5/R1 – Authentication and Authorization Scope	
P6/R2 – Standard Attribute Model	
P9/R3 – Enterprise Information Sharing	
P9/R4 – Information Resource Authentication Frequency	
P9/R5 – Cross-Domain Security	
P9/R6 – Information Resources Availability	

P9/R7 – Information/Data Resources Protection	
P9/R8 – DoD Enterprise Trust Management	
P9/R9 – Alternate Authentication Mechanisms (Non-CAC/Token)	
P11/R4 – Network Gateway Authentication and Authorization	
P12/R2 – Identity and Access Management (IdAM) Infrastructure-Monitoring/Reporting	
JIE POA&M, March 2012	
Principle or Rule	
P5/R2 – Identity Service For Tactical Edge	
P5/R3 – Global Information Resource Access	
P12 – Monitoring and Reporting	
P12/R1 – Auditing Services	
DoD CIO memo, subject: DoD’s Migration to Use of Stronger Encryption Algorithms, 14 October 2010	
Principle or Rule	
P9/R11 – SHA-256: Secure Hashing Algorithm Migration	
P11 – Network Access Controls	
P11/R1 – Authorization Policy Network Attributes	
DoD IdAM, Guiding Principles and Rules - Draft Version 0.6 (CIO/G-6 Cyber Directorate), 20 March 2012	
Principle or Rule	
P10 – Single Sign-On (SSO) and Reduced Sign-On (RSO)	
P10/R1 – SSO and RSO Directory Data Population	
P10/R2 – Electronic Data Interchange Personal Identifier (EDI-PI)	
P10/R3 – SSO and RSO Services Availability	
P11/R2 – Network-Connected Device Authentication	
P11/R3 – Disconnected and/or Network-Disadvantaged Authentication	

Appendix B - Technical Positions and Patterns

Technical Profile Tables

IdAM Related Technical Profiles		
Technical Profile: Digital Certificate (PKI)		
Standard ID	Standard Title	DISR Status
RSA Labs PKCS #12 v1.0:1999 with Corrigendum	PKCS #12: Personal Information Exchange Syntax Standard, version 1.0, and PKCS #12 v1.0 Technical Corrigendum	M
ITU-T X.509:2005	Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, August 2005	M
IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008	M
IETF RFC 2560	IETF Public Key Infrastructure X.509 (PKIX) Online Certificate Status Protocol (OCSP), RFC 2560, June 1999	M
IETF RFC 3279	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	N
IETF RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)	M
Related Principle & Business Rule		
P1/R4 Technical Standards Profile P2/R3 Technical Standards Profile P2/R2 Technical Standards Profile	P4/R1 Technical Standards Profile P5/R1 Technical Standards Profile P8/R9 Technical Standards Profile	P8/R10 Technical Standards Profile
Technical Profile: Key Exchange		
Standard ID	Standard Title	DISR Status
IETF RFC 4109	Algorithms for Internet Key Exchange version 1 (IKEv1), May 2005	N
IETF RFC 3526	More Modular Exponential (MODP) Diffie-Hellman Groups for Internet Key Exchange (IKE), April 2002	M
IETF RFC 5996	Internet Key Exchange Protocol Version 2 (IKEv2)	M
IETF RFC 4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2), December 2005	M
Related Principle & Business Rule		
Technical Profile: Cryptographic Key Management		
Standard ID	Standard Title	DISR Status
IETF RFC 5480	Elliptic Curve Cryptography Subject Public Key Information	N
FIPS Pub 140-2	Security Requirements for Cryptographic Modules, 25 May 2001	M
Related Principle & Business Rule		
Technical Profile: Cryptography Algorithms		
Standard ID	Standard Title	DISR Status

IETF RFC 4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH), April 2007	M
ANSI/INCITS 359-2004	Information technology - Role Based Access Control (RBAC)	M
CAPP	Controlled Access Protection Profile for Basic Robustness/C2 systems, Version 1.d, NSA, 8 October 1999	M
Related Principle & Business Rule		
P9/R10 Technical Standards Profile P8/R2 Technical Standards Profile	P11/R4 Technical Standards Profile	P12/R1 Technical Standards Profile
Technical Profile: Attribute Management Services		
Standard ID	Standard Title	DISR Status
ISO/IEC 19794-6:2005	Information technology - Biometric data interchange formats, Part 6: Iris image data, 10 June 2005	M
SAML V2.0 Attribute Sharing Profile for X.509 A-BS	SAML V2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems, Committee Specification 01	E
OASIS SPML v2.0	Service Provisioning Markup Language (SPML) Version 2.0, 1 April 2006	M
DoD EBTS v2.0	DoD Electronic Biometric Transmission Specification, Version 2.0, 27 March 2009	M
ISO/IEC 19794-7:2007 w/Cor1:2009	ISO/IEC 19794-7:2007 w/Cor1:2009	M
Related Principle & Business Rule		
P1/R8 Technical Standards Profile P1/R9 Technical Standards Profile P2/R5 Technical Standards Profile	P2/R6 Technical Standards Profile P8/R2 Technical Standards Profile P8/R3 Technical Standards Profile	P8/R4 Technical Standards Profile P9/R4 Technical Standards Profile P11/R1 Technical Standards Profile
Technical profile: Authentication Management Services		
Standard ID	Standard Title	DISR Status
IETF RFC 4302	IP Authentication Header, December 2005	M
IETF RFC 2207	RSVP Extensions for IPSEC Data Flows, September 1997	E
IETF RFC 4303	IP Encapsulating Security Payload (ESP), December 2005	M
	Java Security Services (http://java.sun.com/javase/technologies/security/)	N
IETF RFC 4120	The Kerberos Network Authentication Service (V5), July 2005	M
IETF RFC 2865	Remote Authentication Dial-In User Services (RADIUS), June 2000	
Related Principle & Business Rule		
P5/R4 Technical Standards Profile P5/R6 Technical Standards Profile P8/R7 Technical Standards Profile	P8/R8 Technical Standards Profile P10/R1 Technical Standards Profile	P10/R3 Technical Standards Profile P10/R2 Technical Standards Profile
Technical profile: Authoritative Attribute Exchange Service		
Standard ID	Standard Title	DISR Status

SAML 2.0 OASIS	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005	M
W3C Canonical XML 1.0	Canonical XML, Version 1.0, W3C Recommendation, 15 March 2001	M
FIPS Pub 186-2	Digital Signature Standard (DSS) Digital Signature Algorithm (DSA), 27 January 2000	M
XML Signature	XML Signature Syntax and Processing, W3C Recommendation, 12 February 2002	M
	Biometric APIs (u)	
ISO/IEC 24709-1:2007	Conformance testing for the biometric application programming interface (BioAPI) - Part 1: Methods and procedures, 2007-01-29 Mandated DISR DISR 09-2.0 DISR 09-2.0	M
ISO/IEC 24709-2:2007	Conformance testing for the biometric application programming interface (BioAPI) - Part 2: Test assertions for biometric service providers, 2007-02-02	M
Related Principle & Business Rule		
P1/R8 Technical Standards Profile P1/R9 Technical Standards Profile P2/R5 Technical Standards Profile P2/R6 Technical Standards Profile P2/R7 Technical Standards Profile	P2/R8 Technical Standards Profile P5/R6 Technical Standards Profile P8/R1 Technical Standards Profile P8/R4 Technical Standards Profile	P8/R7 Technical Standards Profile P8/R8 Technical Standards Profile P9/R11 Technical Standards Profile P10/R3 Technical Standards Profile
Technical Profile: Biometric Validation		
Standard ID	Standard Title	DISR Status
ANSI INCITS 385-2004	Face Recognition Format for Data Interchange, May 13, 2004	M
ANSI/INCITS 378-2004	Finger Minutiae Format for Data Interchange	M
ANSI/INCITS 381-2004	Finger Image-Based Data Interchange Format	M
ANSI/INCITS 385-2004	Face Recognition Format for Data Interchange, May 13, 2004	M
ISO/IEC 19794-5:2011	Biometric Data Interchange Formats -- Part 5: Face image data	
Related Principle & Business Rule		
P9/R1 Technical Standards Profile		
Technical Profile: Common Access Card (CAC)		
Standard ID	Standard Title	DISR Status
ISO/IEC 7816-11:2004	ISO/IEC 7816-11:2004 - Identification cards - Integrated circuit cards - Part 11: Personal verification through biometric methods	M
ISO/IEC 7816-9:2004	ISO/IEC 7816-9:2004 - Identification Cards - Integrated Circuit(s) Cards with Contacts - Part 9: Additional Inter-industry Commands and Security Attributes (formerly ANSI/ISO/IEC 7816-9:2000)	M
ISO/IEC 14443-1:2000	ISO/IEC 14443-1: 2000 - Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 1: Physical characteristics	M
ISO/IEC 14443-2:2001 w/ Amd 1:2005	Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 2: Radio frequency power and signal interface, 28 June 2001 with Amendment 1: Bit rates of fc/64, fc/32 and fc/16, 2 June 2005	M

ISO/IEC 14443-3:2001 w/ Amd1:2005, Amd1/Cor1:2006, Amd3:2006	Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 3: Initialization and Anti-collision, 1 February 2001 with Amendment 1: Bit rates of fc/64, fc/32 and fc/16, 15 June 2005; Amendment 3: Handling of reserved fields	M
Related Principle & Business Rule		
P1/R1 Technical Standards Profile P1/R4 Technical Standards Profile P2/R3 Technical Standards Profile	P8/R5 Technical Standards Profile P8/R6 Technical Standards Profile	P11/R2 Technical Standards Profile P11/R3 Technical Standards Profile
Technical Profile: Credential Management		
Standard ID	Standard Title	DISR Status
NIST SP 800-103	An Ontology of Identity Credentials Part 1: Background and Formulation	N
CIMCPP	The Certificate Issuing and Management Components (CIMC) Family of Protection Profiles (PPs)	
IETF RFC 5272	Certificate Management over CMS	
IETF RFC 3162	RADIUS (Remote Authentication Dial In User Service) and IPv6 August 2001	M
IETF RFC 2865	Remote Authentication Dial In User Services (RADIUS), June 2000	M
	Digital Signature	
IETF RFC 3852	Cryptographic Message Syntax (CMS)	M
ISO/IEC 14888-3:2006	Information Technology -- Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms	N
FIPS Pub 186-3	Digital Signature Standard (DSS)	M
NIST FIPS Pub 180-3	Secure Hash Standard (SHS), October 2008	M
Related Principle & Business Rule		
P5/R1 Technical Standards Profile P1/R6 Technical Standards Profile	P1/R7 Technical Standards Profile	P9/R11 Technical Standards Profile
Technical Profile: Encryption & Decryption		
Standard ID	Standard Title	DISR Status
HAIPE 3.0.2	High Assurance Internet Protocol Encryptor (HAIPE) Interoperability Specification, Version 3.0.2, December 2006	M
SLOSPP	Protection Profile for Single-level Operating Systems in Environments Requiring Medium Robustness	M
NIST SP 800-78-1	Cryptographic Algorithms and Key Sizes for Personal Identity Verification	N
FIPS Pub 197	Advance Encryption Standard (AES), 26 November 2001	M
XML-Encryption W3C	XML Encryption Syntax and Processing, W3C Recommendation, 10 December 2002	M
Related Principle & Business Rule		
P9/R10 Technical Standards Profile		
Technical Profile: Firewall Protection		
Standard ID	Standard Title	DISR Status

PP_FW_TF_MR_v1.1 (Traffic Filt. Firewall - Med. Robustness)	U.S. Government Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, Version 1.1, 2007-07-25	M
PP_FWPP-MR	U.S. Government Firewall Protection Profile for Medium Robustness Environments	M
Traffic Filtering Firewall - Low Risk	U.S. Government Traffic Filter Firewall Protection Profile for Low Risk Environments, Version 1.1, April 1999	M
Related Principle & Business Rule		
Technical Profile: Identity Based Access Control (IBAC)		
Standard ID	Standard Title	DISR Status
IETF RFC 4282	The Network Access Identifier, December 2005	E
ISO/IEC 7816-8:2004	ISO/IEC 7816-8:2004 - Identification Cards - Integrated Circuit(s) Cards with Contacts - Part 8: Security Related Inter-industry Commands (formerly ANSI/ISO/IEC 7816-8:1999)	M
IETF RFC 2845	Secret Key Transaction Authentication for DNS (TSIG), May 2000	M
Related Principle & Business Rule		
P5/R1 Technical Standards Profile P5/R2 Technical Standards Profile P5/R4 Technical Standards Profile	P10/R1 Technical Standards Profile P10/R2 Technical Standards Profile	Error! Reference source not found. P11/R2 Technical Standards Profile
Technical Profile: Identity Management		
Standard ID	Standard Title	DISR Status
IETF RFC 3972	Cryptographically Generated Addresses (CGA), March 2005	E
PIV-I	Personal Identity Verification Interoperability For Non-Federal Issuers	
IETF RFC 5408	Identity-Based Encryption Architecture and Supporting Data Structures	
FIPS Pub 201-1	Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006	M
IETF RFC 2794	Mobile IP Network Access Identification Extension for IPv4, March 2000	
Related Principle & Business Rule		
P1/R3 Technical Standards Profile P2/R2 Technical Standards Profile P3/R1 Technical Standards Profile	P3/R2 Technical Standards Profile P5/R1 Technical Standards Profile	P9/R5 Technical Standards Profile P11/R3 Technical Standards Profile
Technical Profile: Identity Proofing		
Standard ID	Standard Title	DISR Status
NIST Special Publication 800-76-1	Biometric Data Specification for Personal Identity Verification, January 2007	M
NIST SP 800-73	Interfaces for Personal Identity Verification – Part 1: End-Point PIV Card Application Namespace, Data Model and Representation	N
NIST SP 800-87	Codes for Identification of Federal and Federally-Assisted Organizations	N
Related Principle & Business Rule		
P1/R2 Technical Standards Profile	P1/R5 Technical Standards Profile	

Technical Profile: Information Assurance		
Standard ID	Standard Title	DISR Status
NIST SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories	N
FIPS-199	Standards for Security Categorization of Federal Information and Information Systems	N
NIST SP 800-126 Rev. 2	The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2, September 2011	M
DoD CJCSI 6510	Information Assurance (IA) and Computer Network Defense	
Related Principle & Business Rule		
P9/R7 Technical Standards Profile		
Technical Profile: IPsec Advanced Encryption		
Standard ID	Standard Title	DISR Status
IETF RFC 3686	Using Advanced Encryption Standard (AES) Counter Mode with IPsec Encapsulation Security Payload (ESP)	M
Related Principle & Business Rule		
Technical Profile: IPsec Cryptographic Management Services		
Standard ID	Standard Title	DISR Status
IETF RFC 4308	Cryptographic Suites for IPsec, December 2005	M
IETF RFC 4869	Suite B Cryptographic Suites for IPsec, May 2007	M
Related Principle & Business Rule		
Technical Profile: IPsec Mechanisms		
Standard ID	Standard Title	DISR Status
IETF RFC 3776	Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents, June 2004	E
IETF RFC 4301	Security Architecture for the Internet Protocol, December 2005	M
Related Principle & Business Rule		
Technical Profile: Key Management		
Standard ID	Standard Title	DISR Status
RSA Labs PKCS #15:2000	Cryptographic Token Information Format Standard, Version 1.1, RSA, 6 June 2000	M
RSA PKCS #11 v2.20	RSA PKCS #11 v2.20: Cryptographic Token Interface Standard	M
IETF RFC 3585	IPsec Configuration Policy Information Model, Aug 2003	M
IETF RFC 3566	The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec, Sept 2003	M
CIMCPP	The Certificate Issuing and Management Components (CIMC) Family of Protection Profiles (PPs)	M
Related Principle & Business Rule		

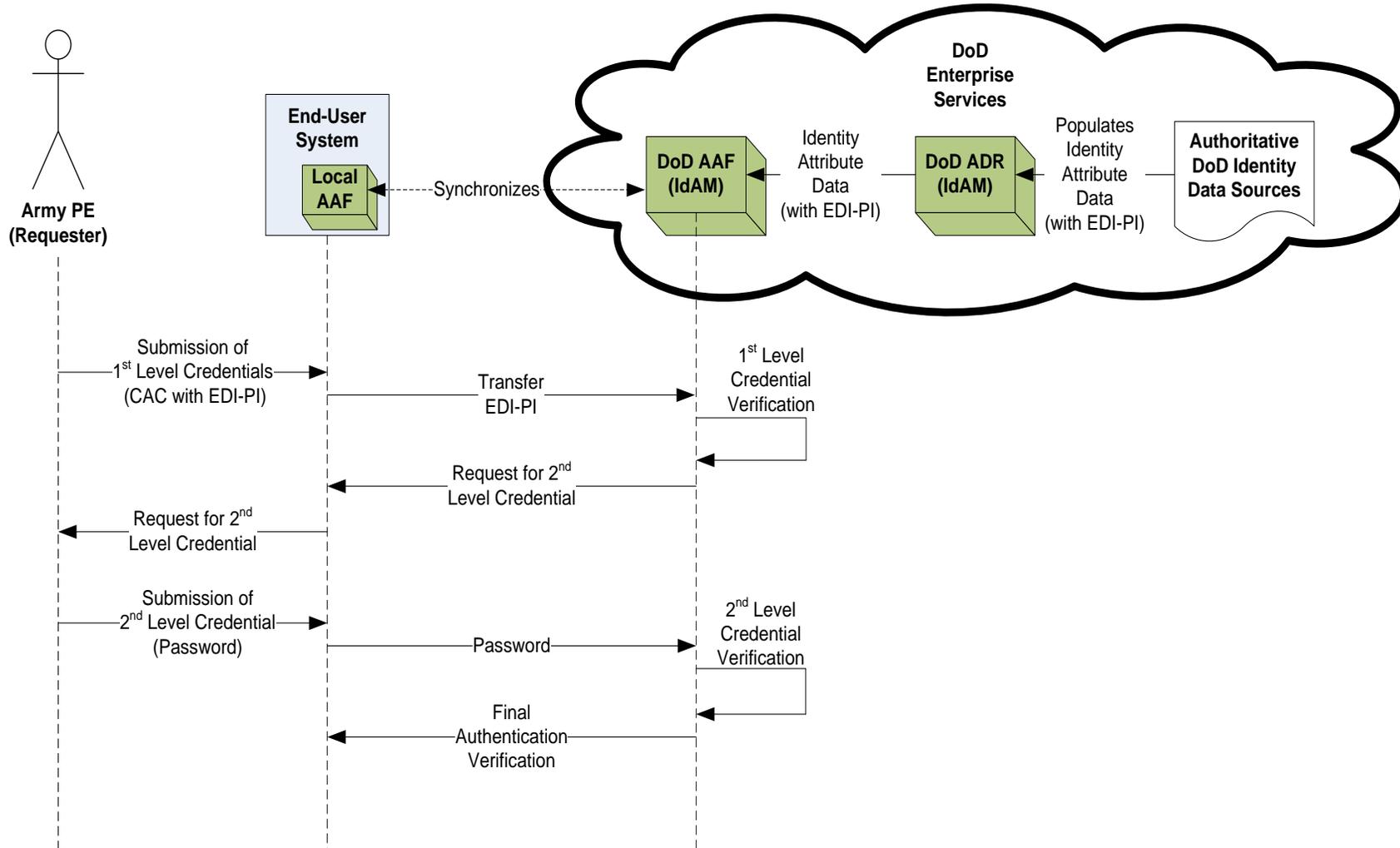
Technical Profile: Global Directory Services for Enterprise Services		
Standard ID	Standard Title	DISR Status
ACP 123(B)	Common Messaging Strategy and Procedures, May 2009	M
IETF RFC 3850	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling, July 2004	M
IETF RFC 4104	Policy Core Extension Lightweight Directory Access Protocol Schema (PCELS), June 2005	M
IETF RFC 3673	Lightweight Directory Access Protocol version 3 (LDAPv3): All Operational Attributes, December 2003	M
IETF RFC 2849	The LDAP Data Interchange Format (LDIF), June 2000	M
IETF RFC 2605	Directory Server Monitoring MIB, June 1999	M
Related Principle & Business Rule		
P4/R2 Technical Standards Profile P4/R3 Technical Standards Profile	P4/R4 Technical Standards Profile P4/R5 Technical Standards Profile	P12/R2 Technical Standards Profile
Technical Profile: Policy in Authentication		
Standard ID	Standard Title	DISR Status
NSPD-59 / HSPD-24	Biometrics for Identification and Screening to Enhance National Security	
DoDD 8320.02	Data Sharing in a Net-Centric Department of Defense	
DoD Instruction 8520.03	Identity Authentication for Information Systems	
DoDD 8320.03	Unique Identification (UID) Standards for a Net-Centric Department of Defense	
DoDD 1000.25	DoD Personnel Identity Protection (PIP) Program	
DODD 8500.01E	Information Assurance (IA)	
DoD 5200.28-STD	Department of Defense Trusted Computer System Evaluation Criteria	
Related Principle & Business Rule		
P1/R2 Policy/Regulation Profile P1/R3 Policy/Regulation Profile P1/R9 Policy/Regulation Profile	P7/R8 Policy/Regulation Profile P9/R3 Policy/Regulation Profile	P11/R1 Policy/Regulation Profile P12/R1 Policy/Regulation Profile
Technical Profile: Policy in Credentialing		
Standard ID	Standard Title	DISR Status
SP 800-103	An Ontology of Identity Credentials, Part 1: Background and Formulation	
SP 800-122	Guide for Protecting the Confidentiality of Personally Identifiable Information (PII)	
DODI 8510.01	DoD Information Assurance Certification and Accreditation Process (DIACAP)	
DODI 8510.01	DoD Information Assurance Certification and Accreditation Process (DIACAP)	
DoD Instruction 8520.02	Public Key Infrastructure (PKI) and Public Key (PK) Enabling	
Related Principle & Business Rule		

P2/R2 Technical Standards Profile P9/R1 Policy/Regulation Profile P1/R8 Policy/Regulation Profile P7/R8 Policy/Regulation Profile	P9/R2 Technical Standards Profile P9/R3 Policy/Regulation Profile P9/R7 Policy/Regulation Profile	P9/R8 Policy/Regulation Profile P9/R9 Policy/Regulation Profile P9/R10 Policy/Regulation Profile
Technical Profile: Secure Shell		
Standard ID	Standard Title	DISR Status
IETF RFC 4254	The Secure Shell (SSH) Connection Protocol, January 2006	M
IETF RFC 4252	The Secure Shell (SSH) Authentication Protocol, January 2006	M
IETF RFC 4251	The Secure Shell (SSH) Protocol Architecture, January 2006	M
IETF RFC 4250	The Secure Shell (SSH) Protocol Assigned Numbers, January 2006	M
Related Principle & Business Rule		
P5/R1 Technical Standards Profile	P5/R3 Technical Standards Profile	P5/R5 Technical Standards Profile
Technical Profile: Web Services Security		
Standard ID	Standard Title	DISR Status
W3C WS Addressing 1.0 - Core	Web Services Addressing 1.0 - Core, W3C Recommendation, 9 May 2006	M
IETF RFC 4347	Datagram Transport Layer Security, April 2006	M
WS-Security 1.1	Web Services Security v1.1, February 2006	
Related Principle & Business Rule		
P9/R4 Technical Standards Profile		
Technical Profile: Standardized Policy Languages		
Standard ID	Standard Title	DISR Status
EKMS 308E	Revision E, Data Tagging and Delivery Standard, April 2008	
EKMS 308 Appendix A	EKMS Data Tagging and Delivery Standard, Appendix A, Shared Fixed ID and Command.req FDU Assignments, 22 April 2009	
EKMS 308 App C 24Apr09	EKMS Data Tagging and Delivery Standard, U.S. National Appendix C, Non-shared Fixed ID and Command.req FDU Assignments, 24 April 2009	
XACML 2.0 OASIS	eXtensible Access Control Markup Language (XACML) Version 2.0, OASIS Standard, 1 February 2005	
Related Principle & Business Rule		
P7/R6 Technical Standards Profile	P7/R7 Technical Standards Profile	P7/R2 Technical Standards Profile

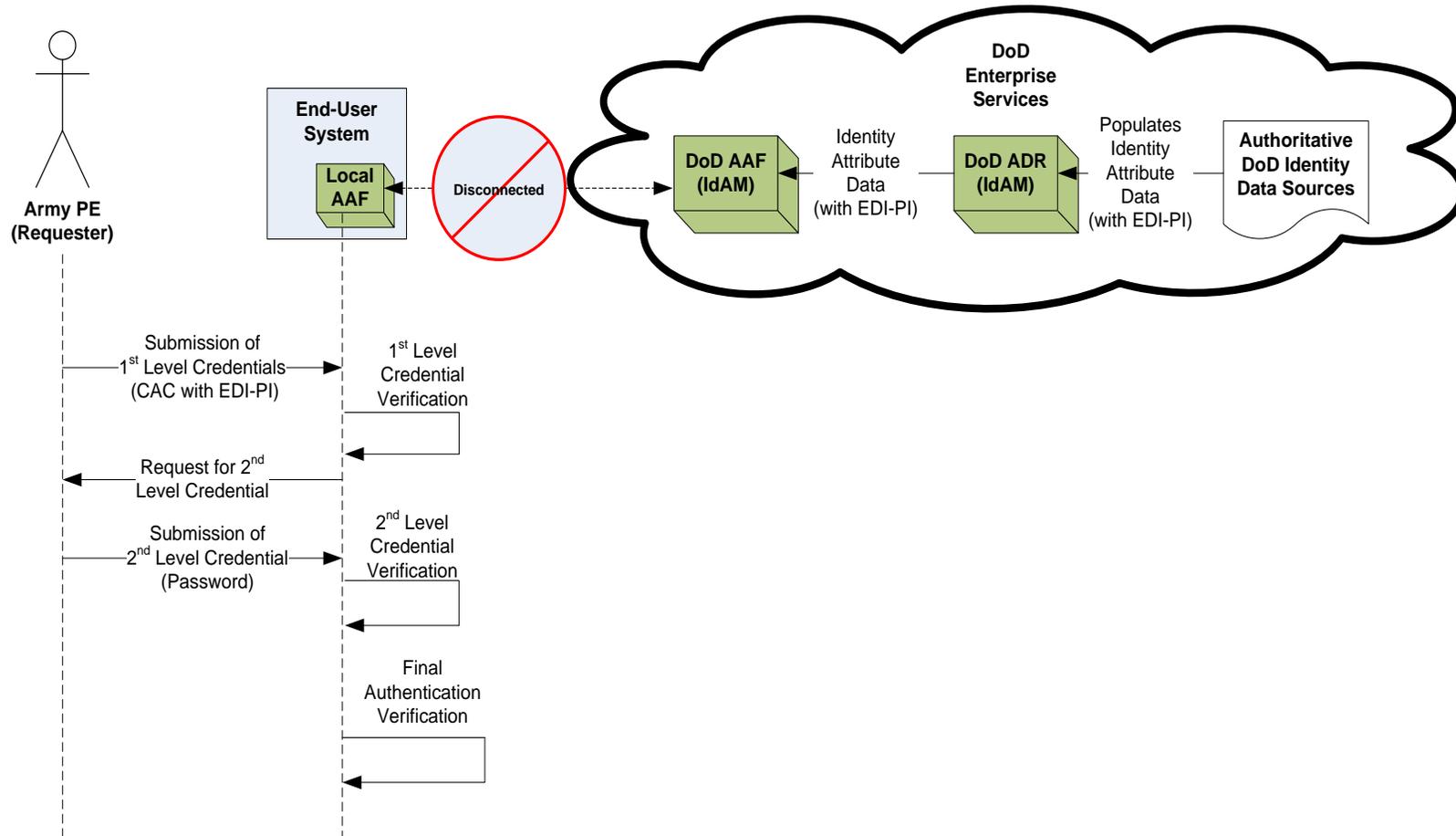
Army IdAM RA to Army Regulation (AR) 25-2 Mapping	
AR 25-2 Chapter/Section	Army IdAM RA Principle/Rule
Chapter 2: Responsibilities	
Section 2-x	P3/R1 Policy/Regulation Profile
Chapter 3: Army Information Assurance Program Personnel Structure	
Section 3-2: Information assurance personnel structure	P3/R1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

Pattern Views for Business Rules (by Business Rule)

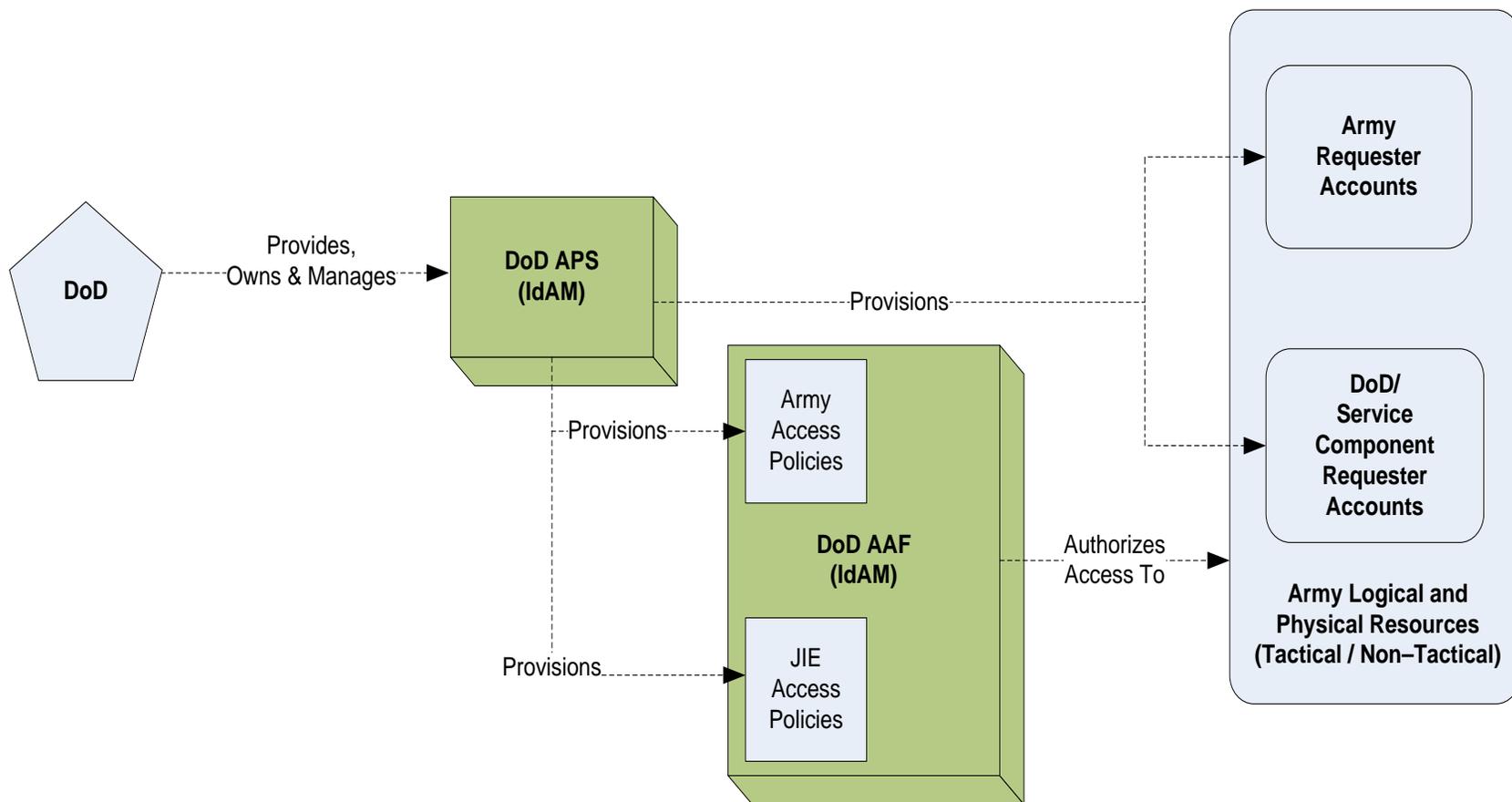
P1/R1 PE Unique Identifier (Connected)



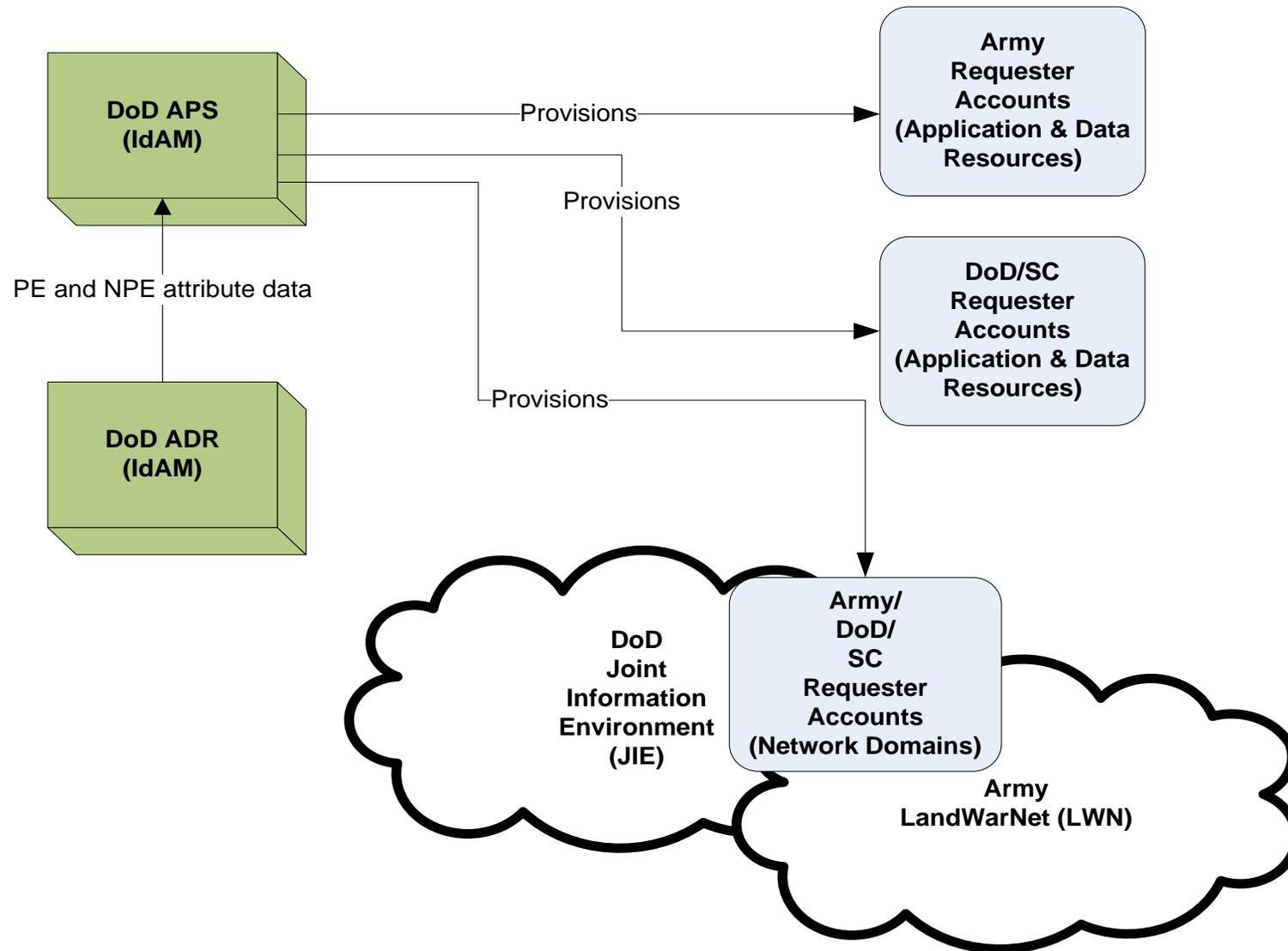
P1/R1 PE Unique Identifier (Disconnected)



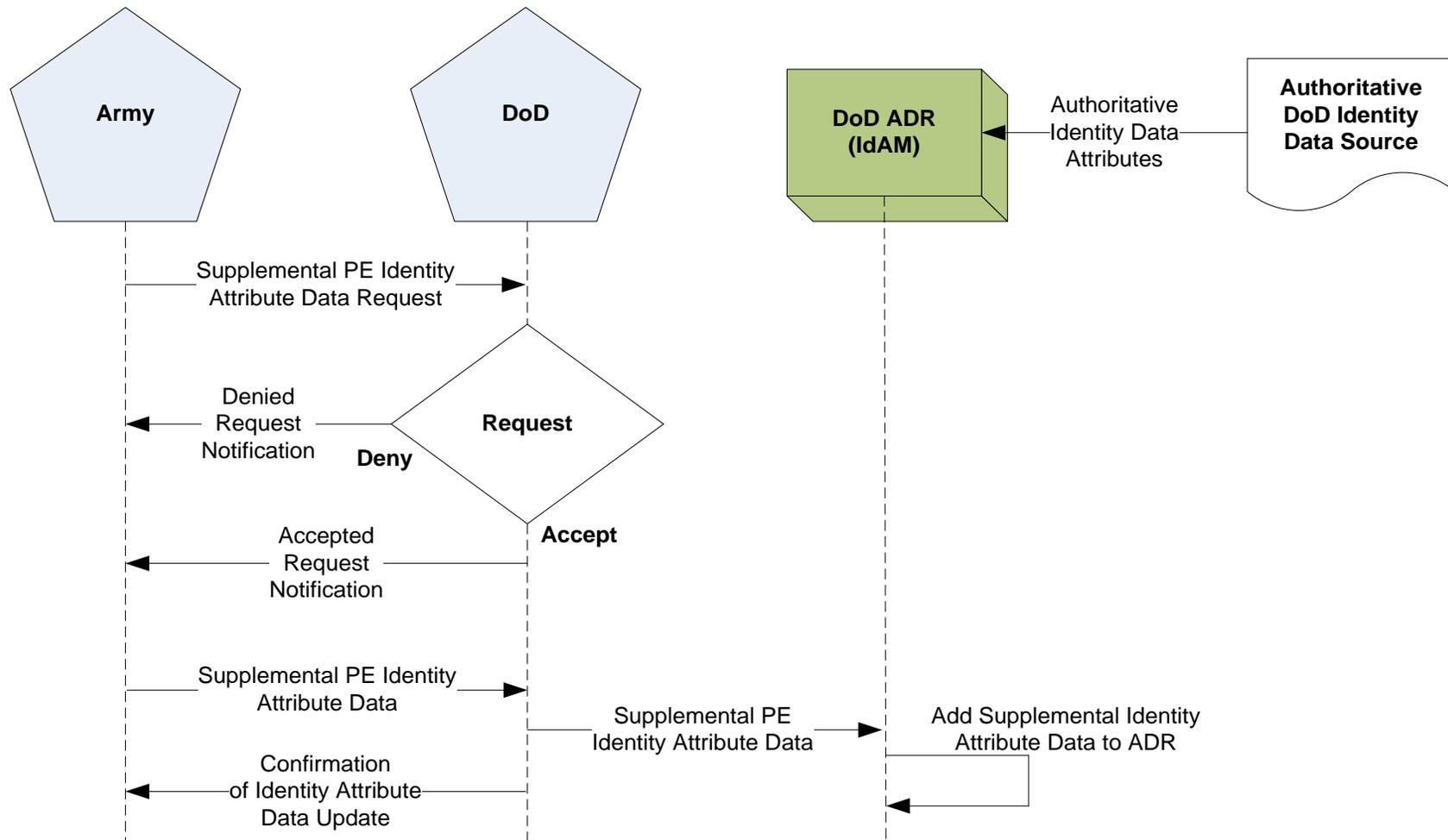
P1/R8 Authentication and Authorization Service Provisioning



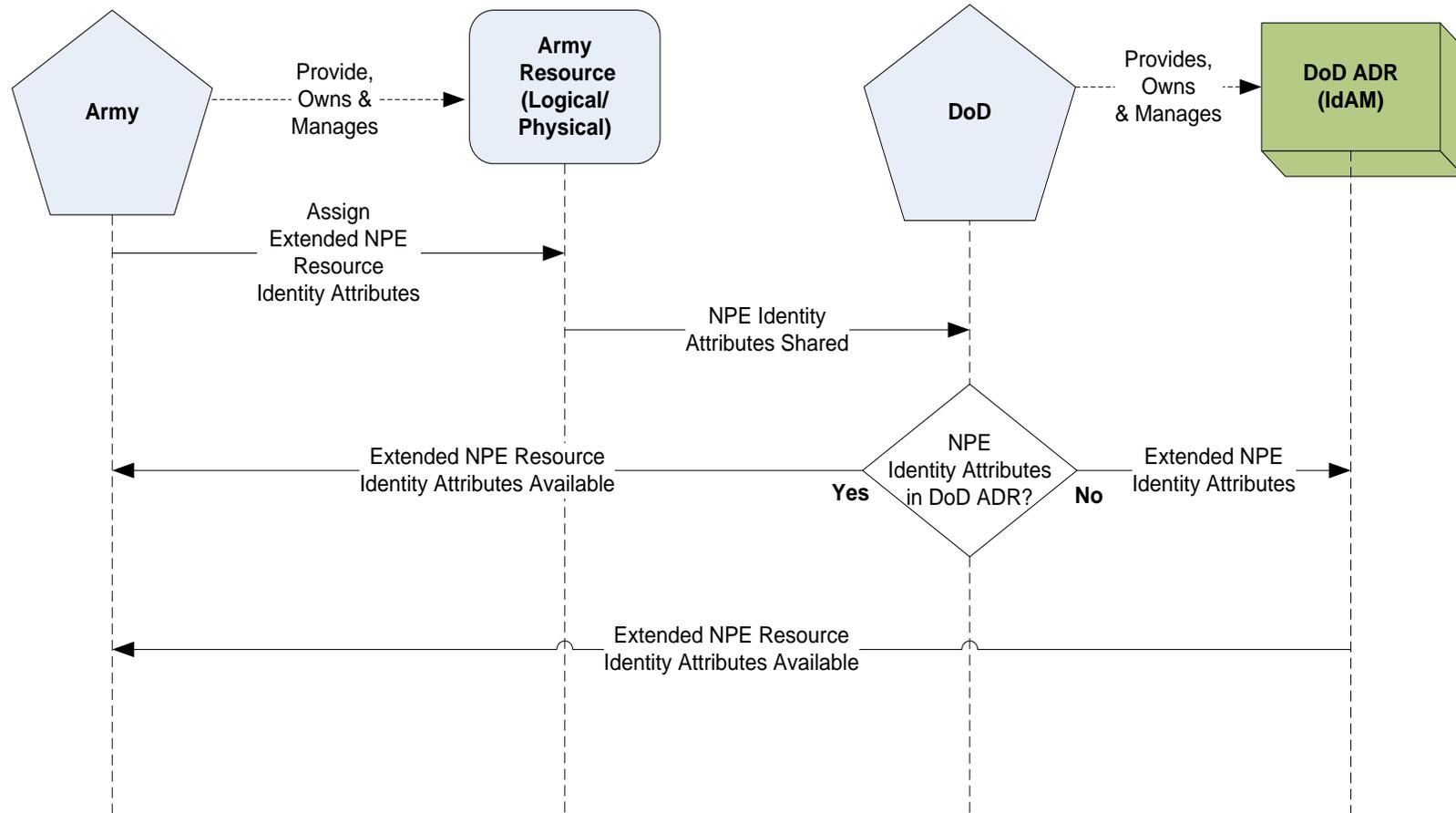
P2/R4 Resource Account Provisioning Service



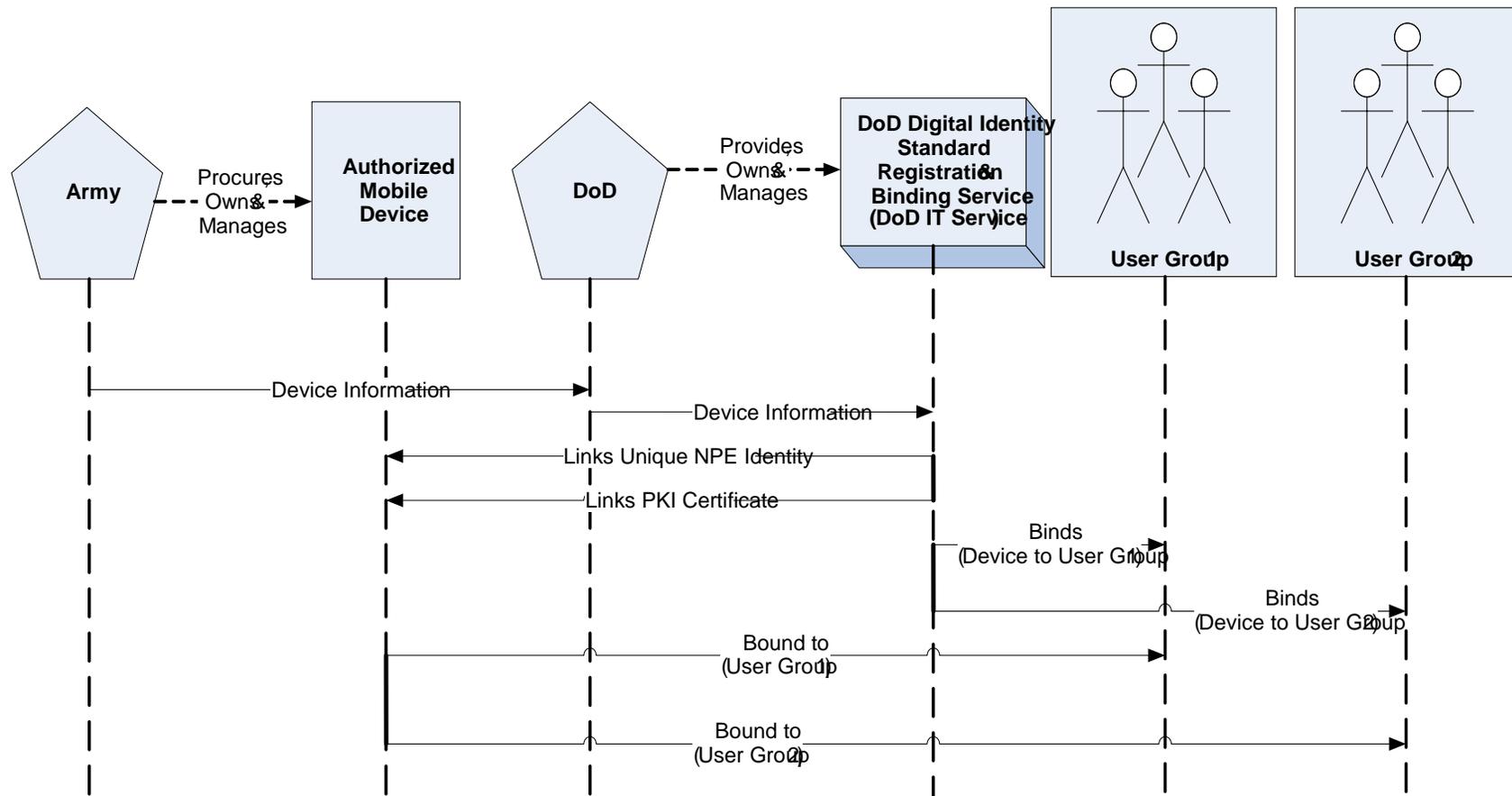
P2/R5 Adding Core PE Identity Attributes



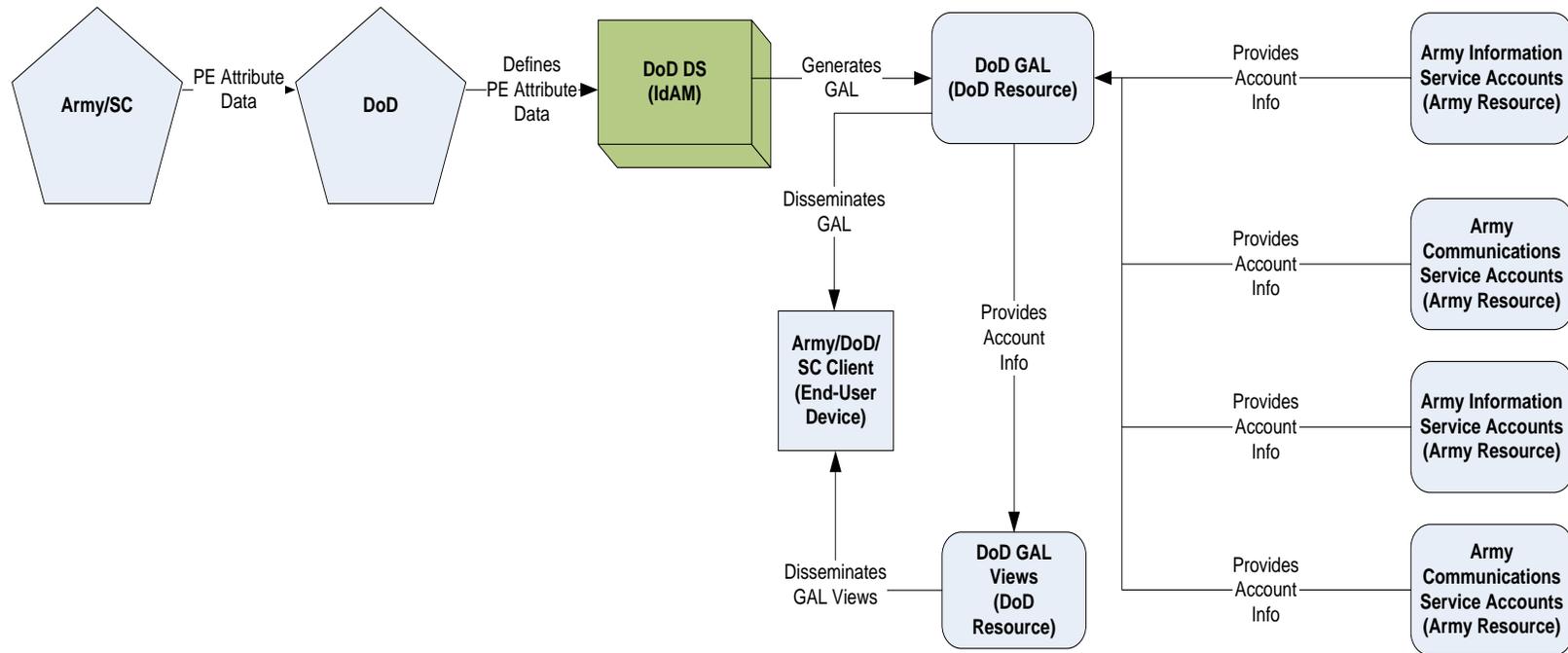
P2/R6 Adding Core NPE Identity Attributes



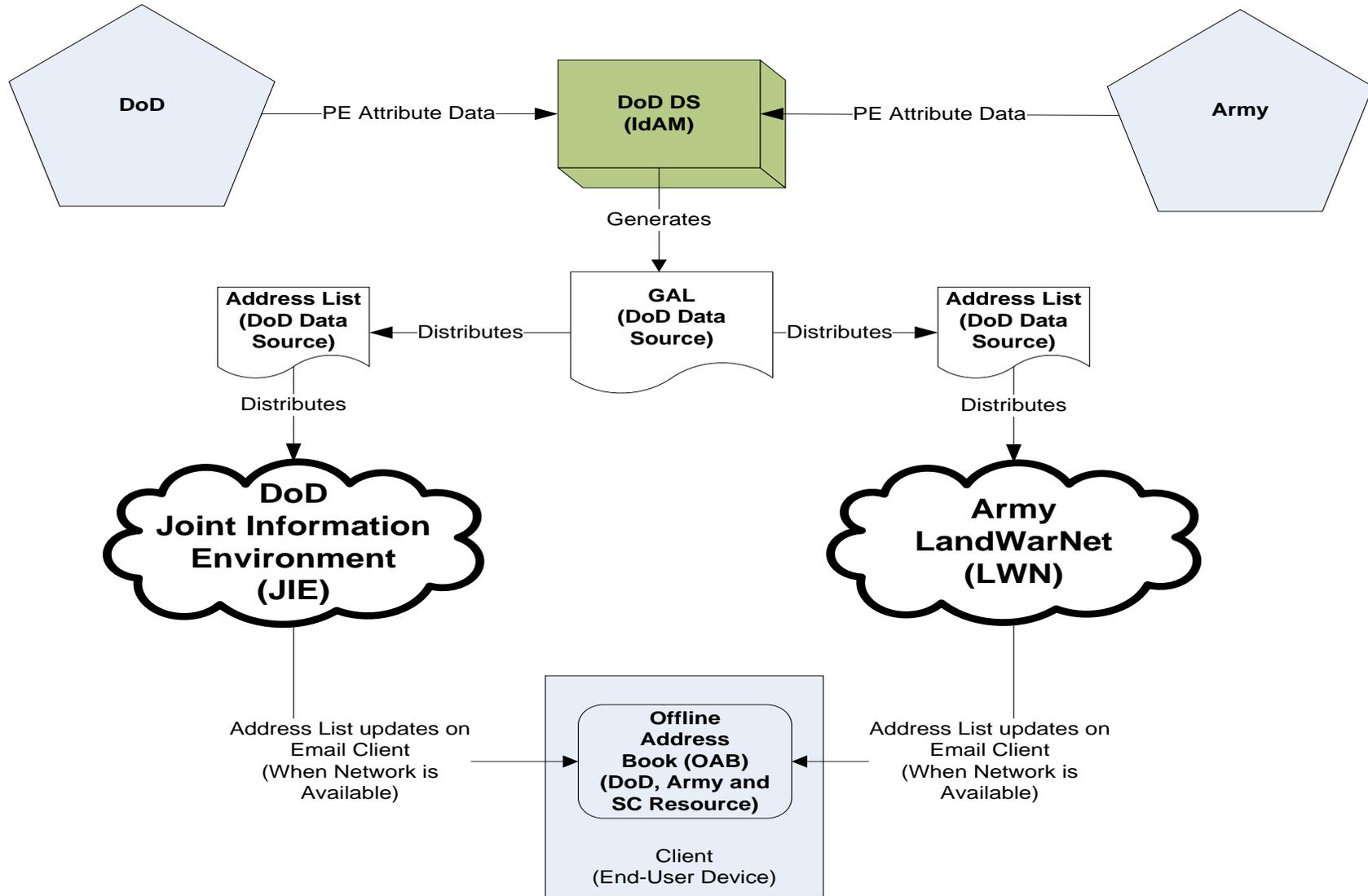
P3/R2 Mobile Device Binding



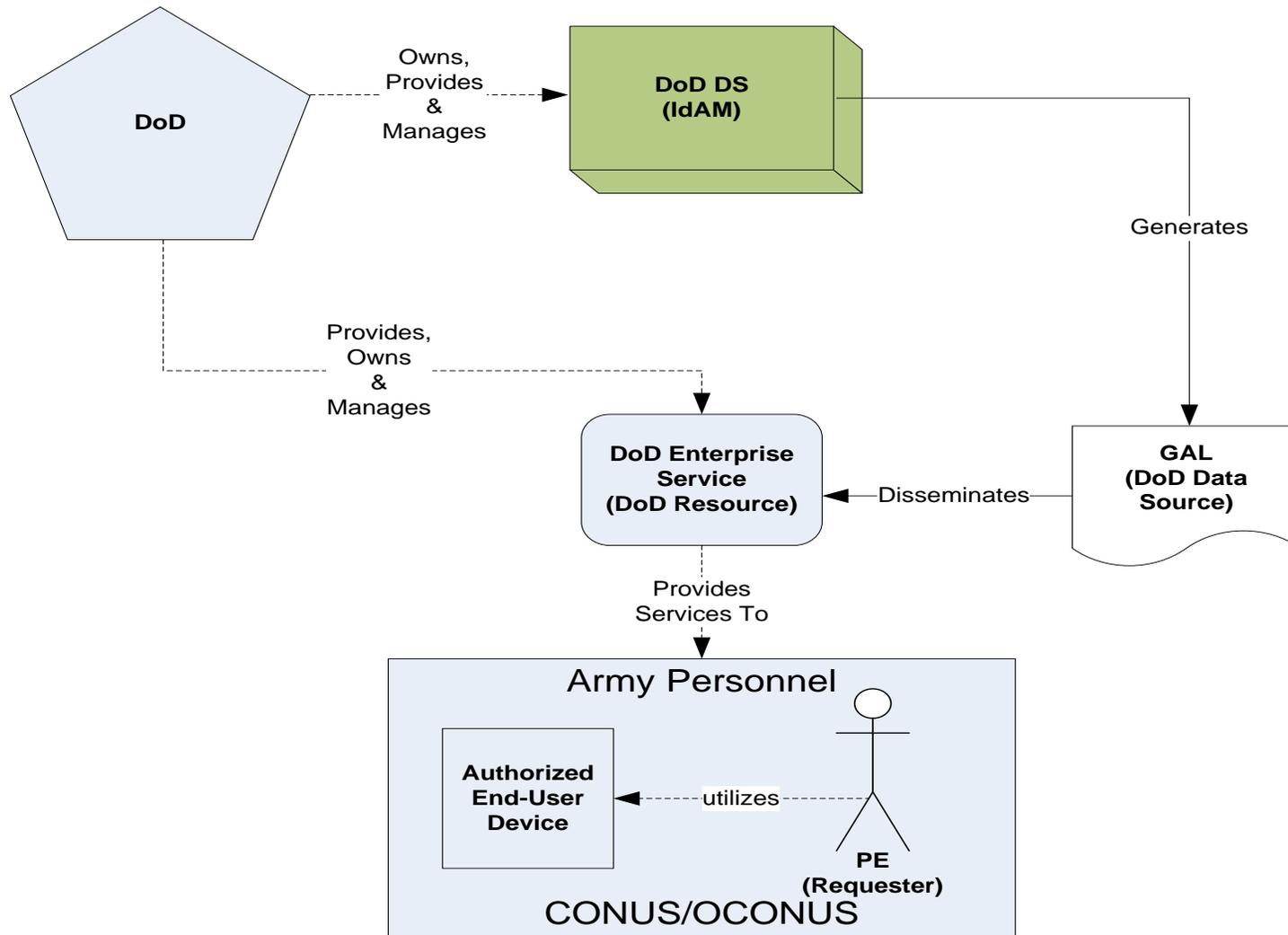
P4/ R1 Global Address List (GAL) Distribution



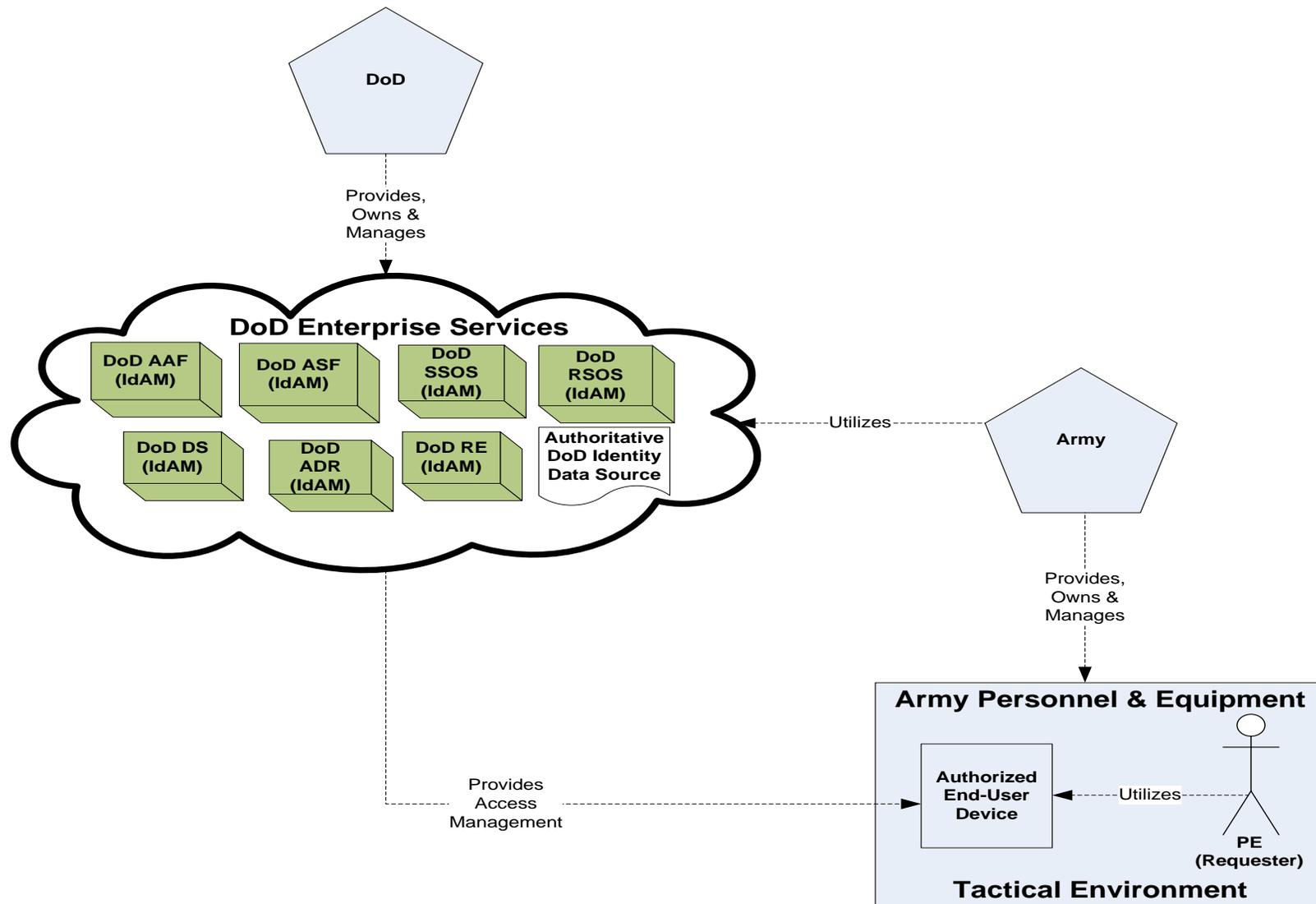
P4/R4 Local Offline Address Book (OAB) Availability



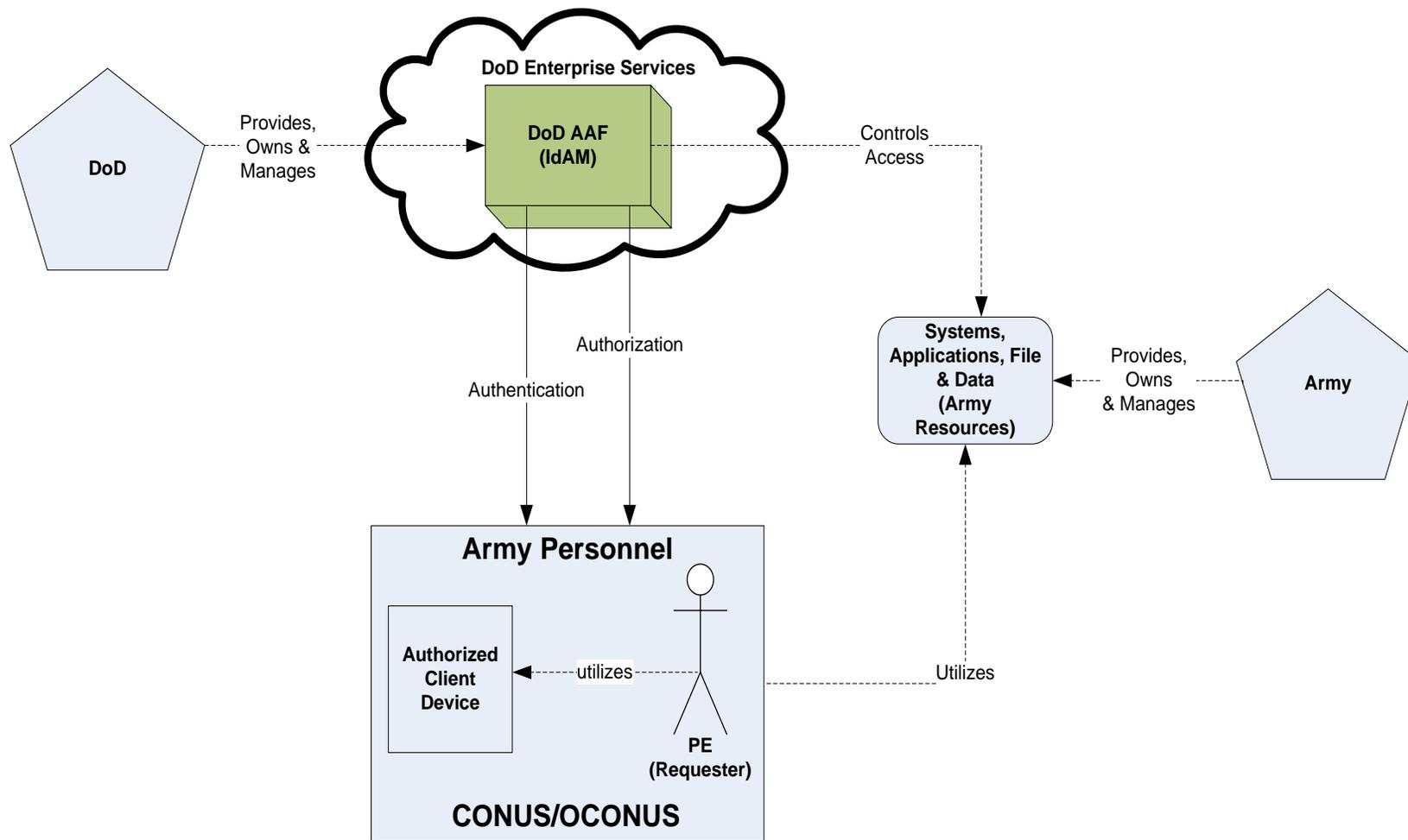
P4/R5 Directory/ Global Address List (GAL) Services Availability



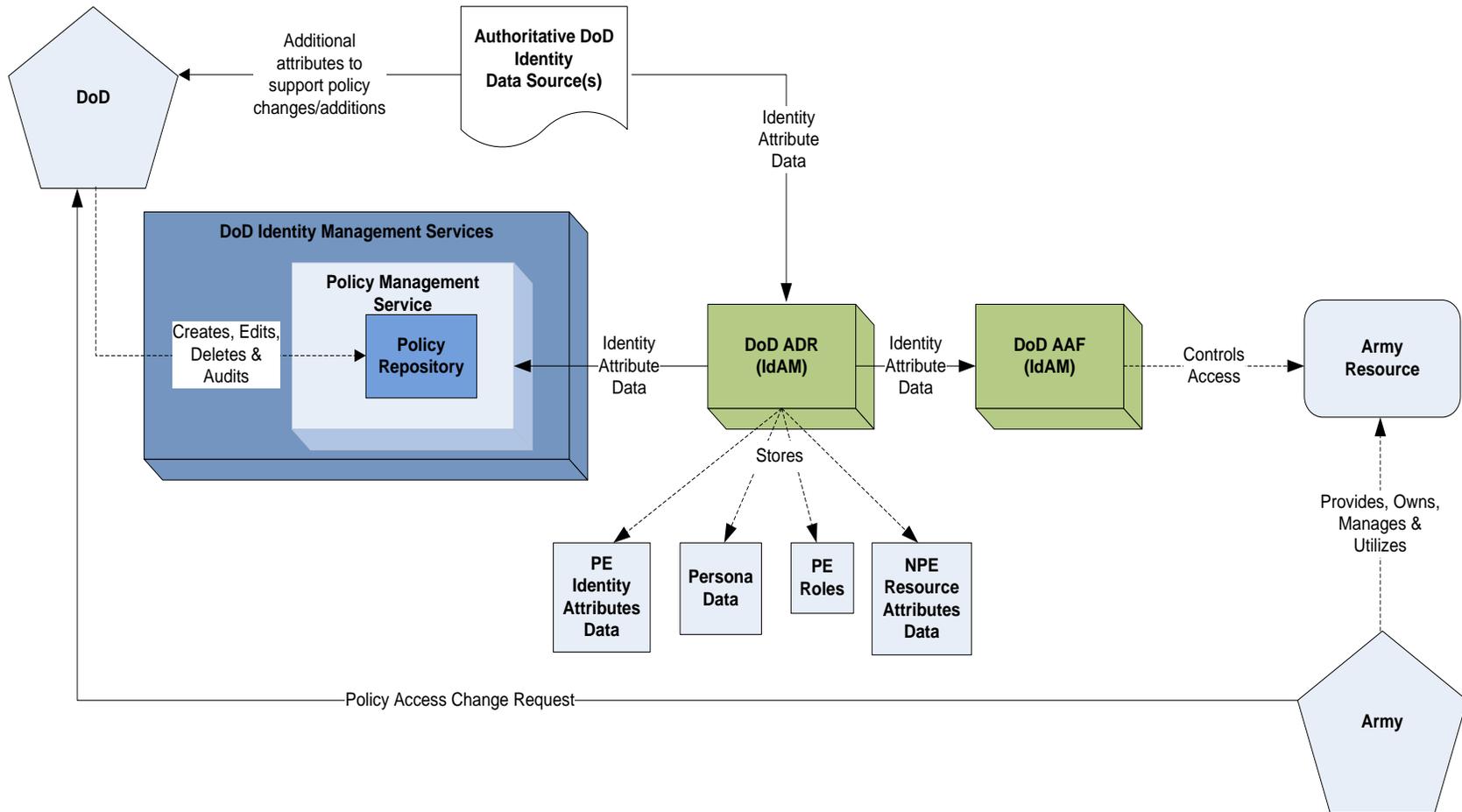
P5/R2 Identity Service for Tactical Edge



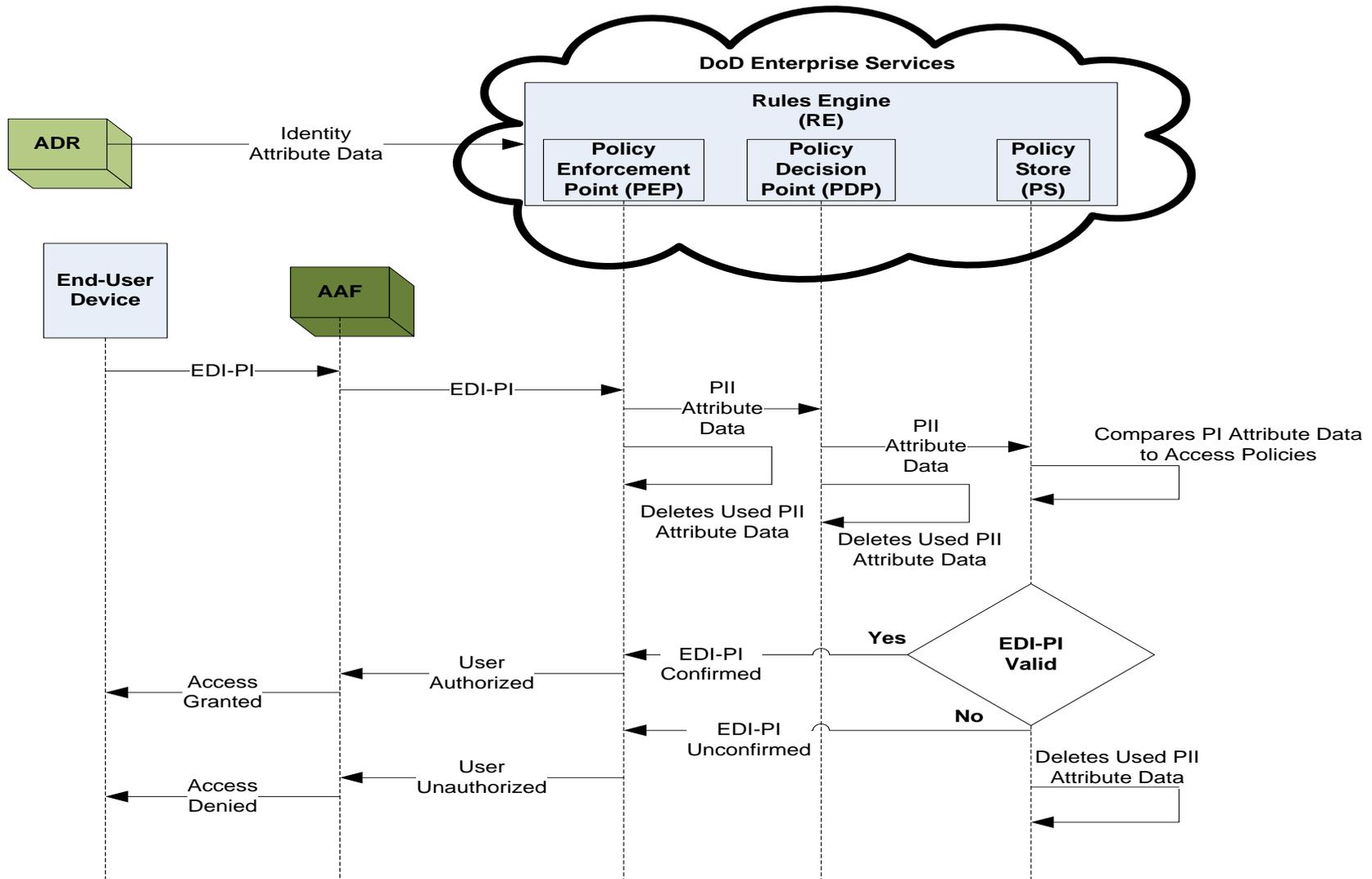
P5/R3 Global Information Resource Access



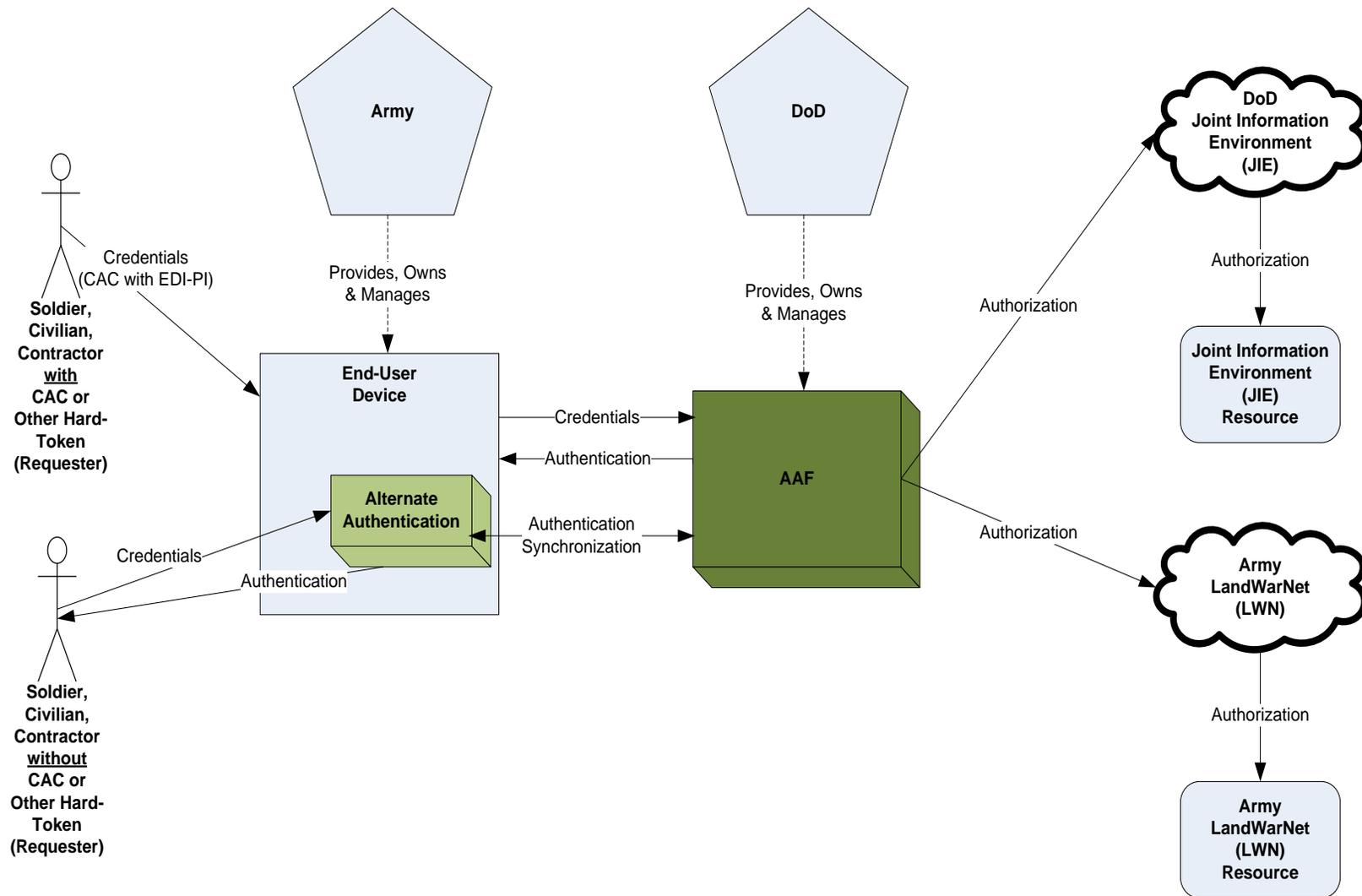
P6/R1 Policy Management Service Scope & P6/R4 Policy Change Management Responsibility



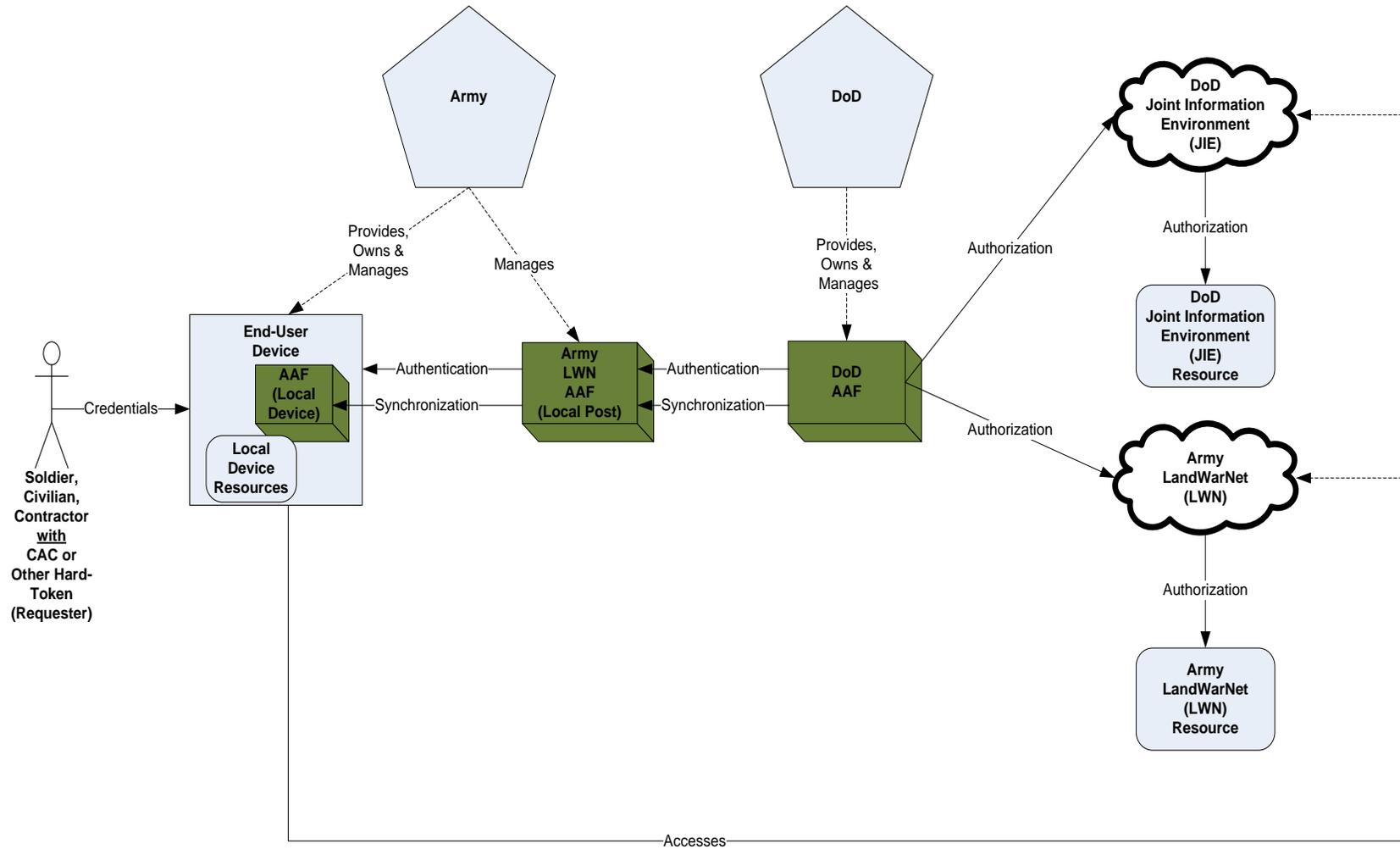
P7/R5 Policy Store (PS) Personally Identifiable Information (PII) Attribute Exposure



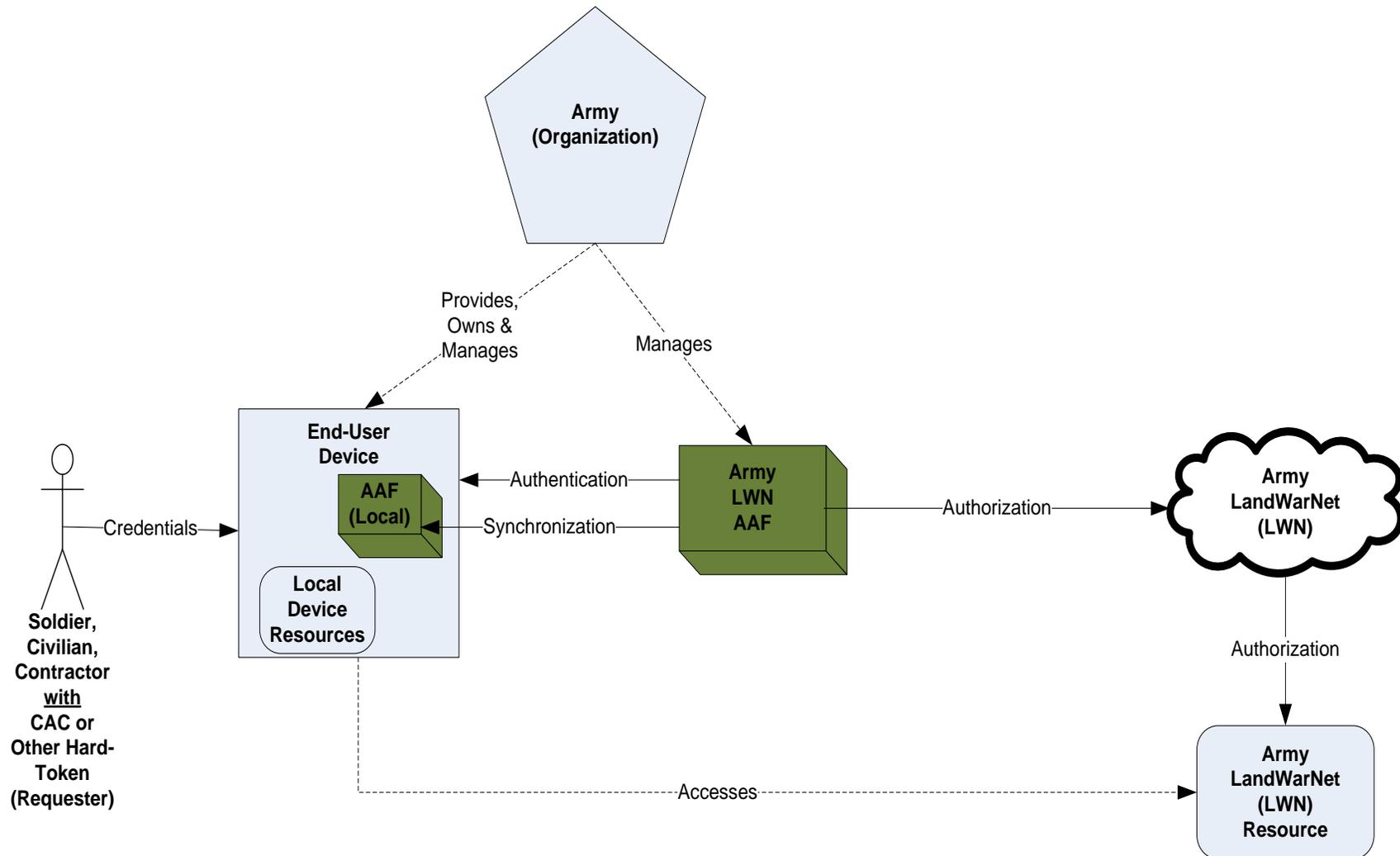
P9/R9Alternate Authentication Mechanisms (Non-CAC/Token)



P11/R2 Network-Connected Authentication



P11/R3 'Disconnected' and/or 'Network-Disadvantaged' Authentication



P11/R3 'Disconnected' and/or 'Network-Disadvantaged' Authentication

