

Unclassified

Active Directory Optimization Reference Architecture

Version 1.0



December 15, 2010

Office of the Assistant Secretary of Defense
for
Networks and Information Integration/DoD Chief Information Officer

CHANGE HISTORY

Version:	Date of Change:	Author(s):	Page(s) Changed:	Comments
v0.90	16 October 2009	Mike McKenna		First Coordination Draft
v0.91	24 May 2010	Mike McKenna		Interim adjudication draft
v0.94	29 July 2010	Mike McKenna		Interim adjudication draft
v0.95	04 August 2010	Joe Paiva		Interim adjudication draft
v0.97	31 August 2010	Mike McKenna		Post adjudication draft – AD WG
v0.97	03 September 2010	Mike McKenna		Post adjudication draft – AD WG
v0.97	28 September 2010	Mike McKenna		Post adjudication draft – AD WG
v0.97	20 October 2010	Mike McKenna		Post adjudication draft – AD WG
v0.97	29 October 2010	Mike McKenna		Post adjudication draft – AD WG
v0.97	12 November 2010	Mike McKenna		Post adjudication draft – AD WG
v0.97	03 December 2010	Mike McKenna		Post adjudication draft – AD WG
v1.0	15 December 2010	Mike McKenna		Signed version with adjudicated comments

TABLE OF CONTENTS

Executive Summary	5
1.0 Strategic Purpose (AV-1).....	7
1.1 Introduction and Background	7
1.2 Goals	8
1.3 High-Level Operational Concept (OV-1)	8
1.4 Purpose.....	9
1.5 Intended Audience and Uses.....	9
1.6 Scope.....	10
1.7 Assumptions.....	10
1.8 Constraints	11
1.9 Linkages to Other Architectures, Programs, and Initiatives	11
1.9.1 The AD Optimization Environment.....	11
1.9.2 External Linkages	12
1.10 Organization of This Document.....	12
2.0 Principles, Rules & Operational Patterns (OV-6a, OV-1s)	13
2.1 Goal 1 – Improving the Security of the DoD AD Infrastructure	13
2.1.1 Principles and Rules.....	13
2.1.2 Operational Concept Graphic	17
2.2 Goal 2 – Global User Logon.....	18
2.2.1 Principles and Rules.....	18
2.2.2 Operational Concept Graphic	19
2.3 Goal 3 – Sharing AD Contact Objects Across Forests	20
2.3.1 Principles and Rules.....	20
2.3.2 Operational Concept Graphic	21
2.4 Goal 4 – Sharing AD-dependent Applications Across Forests.....	22
2.4.1 Principles and Rules.....	22
2.4.2 Operational Concept Graphic	23
2.5 Goal 5 – Optimize Rapid Reconfiguration/Agility.....	24
2.5.1 Principles and Rules.....	24
2.5.2 Operational Concept Graphic	25
2.6 Goal 6 – Optimize Affordability & Efficiency.....	26
2.6.1 Principles and Rules.....	26
2.6.2 Operational Concept Graphics.....	27
3.0 Technical Positions (StdV-1).....	29
Appendix A: Vocabulary (AV-2)	36
Appendix B: References	39
Appendix C: Component AD Consolidation	40
C.1 Component AD Consolidation.....	40
C.2 AD Forest Type.....	40
C.3 Operational Concept Graphic	41
C.4 COCOMs	42
C.5 Other DoD-managed Forests	42

Appendix D: Capability Viewpoint (CV-2)..... 43

- D.1 Global User Logon Capability Taxonomy..... 43
 - D.1.1 Related Initiatives Required To Provide Full Global Logon
Functionality 44
 - D.1.2 Defense ITIL Access Management..... 44
- D.2 Sharing Contact Objects Across AD Forests Capability Taxonomy 45
- D.3 Sharing AD-dependent Applications Across AD Forests Capability Taxonomy..... 45
- D.4 Enterprise Infrastructure for Shared AD-dependent Applications and Services
Capability Taxonomy 46
 - D.4.1 Enterprise Infrastructure for Shared AD-dependent Applications and
Services Operational Concept (OV-1) 47

EXHIBITS

Exhibit 1. AD Optimization High Level Operational Concept Graphic OV-1.....	8
Exhibit 2. Improving the Security of the DoD AD Infrastructure OV-1	17
Exhibit 3. Global Logon OV-1	19
Exhibit 4. Identity Management/Contact Sharing OV-1	21
Exhibit 5. Sharing AD-dependent Applications Using STS OV-1.....	23
Exhibit 6. Separate Authentication & Access Control for Devices and Personas OV-1	25
Exhibit 7. AD Forest Type.....	27
Exhibit 8. AD Service/Resource Forest High Level Architecture OV-1	28
Exhibit 9. Notional Component AD Environment OV-1	41
Exhibit 10. Notional IdSS/EASF OV-1	47

Trademark Information

The terms *Active Directory*, *Microsoft*, *Windows*, *Windows NT*, *Windows Server*, and *Windows Vista* are either registered trademarks or trademarks of the Microsoft Corporation in the United States and/or other countries.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

All other names are registered trademarks or trademarks of their respective companies.

Disclaimer

Active Directory is a X.500-based directory service technology developed by Microsoft Corporation and included as part of Microsoft's Windows Server Operating System. Nothing in this document should be construed as an endorsement of Active Directory or Windows over other vendors' products that provide similar functionality. This vendor specific optimization architecture reflects the reality that Active Directory and Windows are used in the vast majority of DoD computer networks and likely will be for the foreseeable future. This architecture accepts that reality and provides guidance to better use and secure this technology within DoD.

Executive Summary

The DoD Active Directory (AD) Optimization Initiative was developed in response to requests from Military Service CIOs, Combatant Commanders and the Information Assurance (IA) community. Military services need to simplify operation and maintenance of our Active Directory infrastructure to reduce costs and enable service specific management capabilities. COCOM and CJTF Commanders need an Active Directory infrastructure to support cross-component operations and information sharing between military components and mission partners. All stakeholders (including IA professionals within the military services, DISA, OSD and DOT&E) need an AD infrastructure that is more survivable and secure, which can only be achieved by eliminating several known vulnerabilities. Accordingly, the DoD CIO enterprise level plan for Active Directory optimization must balance the three imperatives of: Cost, Capability, and Security.

The DoD plan for Enterprise Active Directory Optimization has four elements:

- An Active Directory Optimization Reference Architecture (ADORA) defining the objective end-state in terms of principles, rules, patterns, and technical positions.
- Support for the delivery of near-term AD optimization capability enhancements within the PACOM theater and to other selected early adopters through a set of solutions that conform to the ADORA.
- Provide input for the development of policy and technical guidance (e.g. STIGs, CTOs) as well as the development of Tactics, Techniques, and Procedures (TTPs) needed to implement the objective end-state architecture. This includes IA/security steps that must be taken by DoD Active Directory forest “owners” to address the most critical known AD vulnerabilities and limitations.
- Support for Military Service AD consolidation and optimization initiatives as well as Enterprise AD infrastructures needed for the deployment of Enterprise E-mail and Enterprise web-based office automation applications.

This document primarily addresses the first of these elements, the ADORA.

The ADORA has been identified as a key source of guidance for the Department’s IT efficiency goals announced by the Secretary of Defense in August 2010. To that end, the ADORA is intended to guide and inform DoD IT Consolidation Roadmap initiatives as well as enterprise and component level AD solutions around six goals:

1. Improving the Security of the DoD AD Infrastructure
2. Global Logon
3. Sharing Active Directory Contact Objects across AD Forests
4. Sharing AD-dependent Applications across AD Forests
5. Rapid Reconfiguration/Agility
6. Affordability/Efficiency

These six goals are completely intertwined and interdependent. Pursuing any one absent the other five would not achieve the results our people and mission partners need to achieve and maintain a decisive information advantage.

This document addresses the objective (~2012/13) end-state only for the DoD Active Directory Infrastructure. It must be read and understood in the context of broader DoD efforts, specifically including those intended to segregate IT Infrastructure “Management” and “Command & Control (C2)” functions from “Authentication” and “Access Control” functions. These efforts include (but are not limited to):

- Implementation of direct PKE Authentication for all DoD Web-based applications in accordance with CTO 07-15.
- Establishment of an Enterprise Application Services Forests within DISA operated Defense Enterprise Computing Centers (DECCs).
- Establishment of DoD DMZs requiring logical and physical separation of public facing systems and applications from their primary systems, applications and data.
- DoD/Microsoft partnership to drive new capabilities in future versions of the Microsoft Windows operating system.
- Various Cyber C2 Initiatives.

The ADORA is only a reference architecture. As such, it is not a policy statement or directive. Any guidance directing implementation of any specific action or changes to networks and AD infrastructure needed to incrementally transition to this end-state will be addressed via separate documents (e.g. DoD Issuances, STIGs, GTGs, CTOs).

The ADORA was developed with extensive input and collaboration from key stakeholders representing the Office of the Secretary of Defense (OSD), the Joint Staff (JS), the Combatant Commanders, each of the three Military Departments, the Defense Information Systems Agency (DISA), the National Security Agency (NSA), and industry partners. Future versions are planned to further refine and sharpen the guidance and to address certain capabilities not included in Version 1. Please address any comments or questions on this reference architecture to the:

Director
Architecture & Infrastructure
Assistant Secretary of Defense for Networks and Information Integration/DoD CIO
1851 S. Bell St, Suite 7000
Arlington, VA 22202

1.0 Strategic Purpose (AV-1)

1.1 Introduction and Background

Combatant Commanders, Military Services, and Defense Agencies (CC/S/A) collectively operate many hundreds of Microsoft AD implementations (forests¹) on the NIPRNET and SIPRNET environments. This largely non-federated, stove-piped architecture limits the ability of authorized users to access needed information from anywhere within the Department as AD forests, by design and DoD implementation, inhibit the sharing of information across forests.

This existing AD architecture does not provide ubiquitous information access for any authorized DoD user as expressed explicitly by this goal of the DoD CIO and the Vice Chairman of the Joint Chiefs of Staff: *“Any authorized user can go anywhere in the DoD, login, and be productive.”*

The current environment is characterized by a number of challenges including:

- The inability for any authorized DoD user to easily logon to any DoD network other than their home station network. This limitation severely constrains the ability of travelling DoD users to be fully productive when away from their home station.
- The limited visibility of DoD users through e-mail global address lists (GALs). Some Service-level white pages and merged GALs are available, but the information is often incomplete, outdated, and littered with duplicate entries. In most current architectures, Active Directory information is manually populated by local system administrators; leading to administrative errors and incorrect contact records.
- The limited ability to share AD-dependent applications and services across AD forests not only limits secured information sharing, but is very inefficient in terms of computing resources. Current AD architectures are characterized by duplicative investments, under-utilization of network infrastructure, and excessive operations and maintenance costs.
- The current AD environment is also susceptible to exploitation and compromise due to the failure of users and system administrators to consistently and fully comply with existing policy and weaknesses in existing Tactics Techniques and Procedures (TTPs); both of which are exacerbated by existing technical vulnerabilities within Active Directory as documented in Bulwark Defender and other sources.

¹An Active Directory forest is a hierarchal collection of every object (including users), its attributes, and rules in the Active Directory. The forest is the core construct of an Active Directory network and serves as the security boundary for the network.

1.2 Goals

The ADORA organizes this future-state vision around six key goals:

1. **Improving the Security of the DoD AD Infrastructure** – The ability to better defend the AD infrastructure from exploitation and minimize the risk of information compromise as documented by Bulwark Defender 2009 and in other studies.
2. **Global Logon** – the ability for any authorized DoD user to logon to any local DoD network (Active Directory forest) connected to the NIPRNET (and later the SIPRNET when PKI hard token is enabled).
3. **Sharing Active Directory Contact Objects Across AD Forests** – The ability for any authorized DoD user to look up and find any other DoD user natively within either the desktop Outlook client, Outlook Web Access, or authorized mobile device (e.g. Blackberry).
4. **Sharing AD-Dependent Applications Across AD Forests** – The ability for an authorized DoD user in one AD forest to securely access applications or systems located in a different AD forest.
5. **Optimize Rapid Reconfiguration/Agility** – Enhance the ability of Windows networks to respond to changing mission needs and the ability to quickly reconstitute following a partial network loss or breach.
6. **Optimize Affordability/Efficiency** – Reduce the overall complexity and cost of operating and defending DoD networks by supporting CC/S/A plans to enhance their networks through AD consolidation and rationalization.

1.3 High-Level Operational Concept (OV-1)

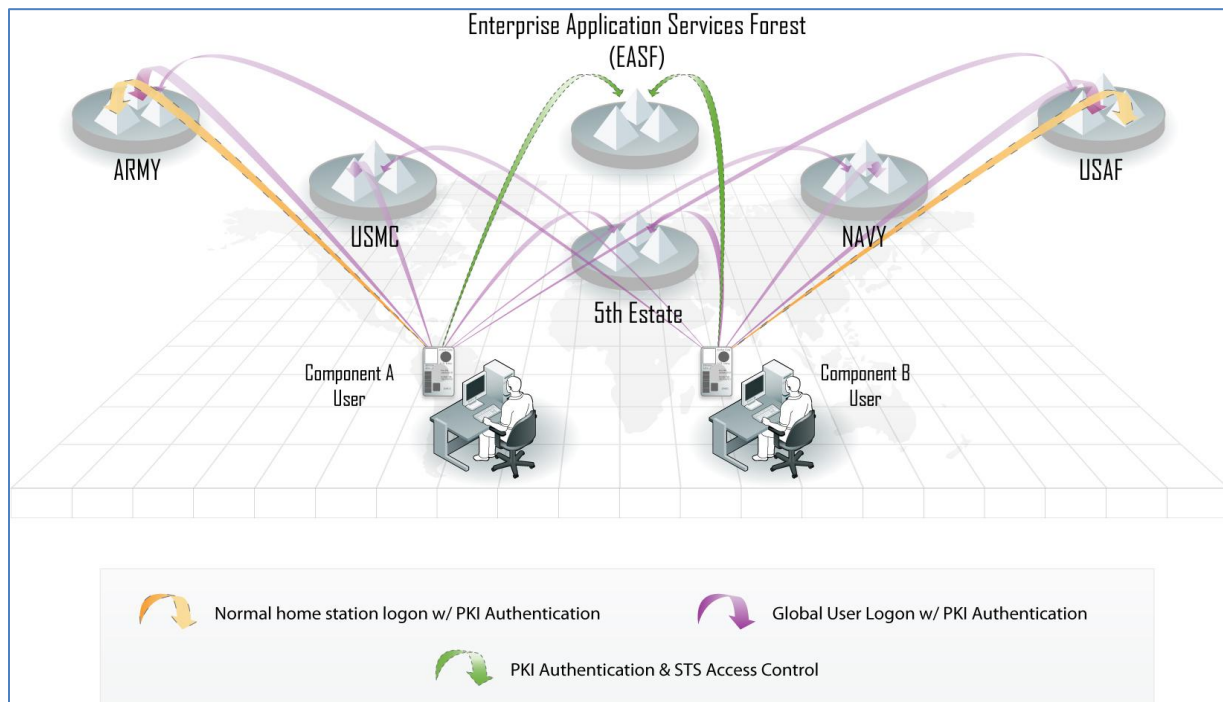


Exhibit 1. AD Optimization High Level Operational Concept Graphic OV-1

Exhibit 1 depicts the over-arching AD optimization operational concept. The key messages of this graphic are:

- Each Component organization (the four Military Services, and as may be determined to be operationally required, the DoD Fourth Estate (OSD and the Defense Agencies/Activities) and COCOMs, will manage and operate a set of AD user and application forests. The number and size of each forest will be determined by the Component. Based on current consolidation plans it is expected that the total number of AD forests across the DoD will shrink significantly by 2013.
- Users will authenticate to AD forests via DoD Public Key Enabling (PKE) or approved Secure Token Service (STS) implementations.
- Any authorized NIPRNET user is able to log into any local DoD network connected to the NIPRNET (a similar capability will exist on the SIPRNET once it is hard token enabled).
- An Enterprise Application Services Forest (notionally a single forest but likely a small set of federated forests) will host all common, shared, DoD Enterprise applications.

1.4 Purpose

This DoD-wide reference architecture is intended to guide and inform DoD Enterprise and CC/S/A efforts to optimize existing AD environments toward the goal of a single logical, seamless and secure DoD Information Environment in a visible, accessible, understandable and trusted manner. The ADORA will be a primary source of guidance for the development of more detailed solution CC/S/A architectures and associated engineering and technical artifacts.

The ADORA presents a high-level, objective end-state vision and framework for AD optimization. It consists of principles, rules, technical positions (standards), and architectural patterns conforming to the DoD Reference Architecture Description v1 (June 2010) and the DoD Architecture Framework v2.0. The ADORA seeks to optimize the structure of the DoD AD environment and enhance the way AD is used in the DoD to make authentication and access decisions. The AD optimization end-state described in the ADORA eliminates the stove pipes created by today's AD footprint and focuses on delivering enhanced capability to the Warfighter through increased collaboration and information portability. Improving the ability to securely share information and communicate across AD forests is an important step toward the vision of a single, seamless DoD Information Environment.

This reference architecture provides the flexibility for a number of different solutions that conform to the rules, standards, and patterns and recognizes that capability must often be phased in over time. Transition planning, as well as development of policy and TTPs needed to affect this end-state, are outside the scope of ADORA and will be addressed via separate initiatives.

1.5 Intended Audience and Uses

This document is intended for Components, Combatant Commanders, and DoD Agencies and Field Activities to collaboratively drive their current AD environments toward the desired end-state. This AD Optimization Reference Architecture provides guidelines to architects and

program managers who are responsible for designing, developing, and implementing IT solutions that use or are affected by the DoD Active Directory environment.

1.6 Scope

The scope of Version 1.0 of the ADORA is intentionally limited, as defined below, to enable the rapid development and implementation of incremental capabilities across the DoD Enterprise. This incremental approach will enable the DoD to rapidly test and field concepts for improved AD-based capabilities using existing assets and technology while other efforts (such as the DISA-led Enterprise User initiative) develop more robust long-term solutions to deliver greater capabilities across the broader Defense Enterprise. Version 1.0 is subject to the following limitations of scope:

- The objective end-state time horizon is 2012/2013.
- It does not include integration or federation with the Intelligence Community (IC) AD environment nor any non-DoD AD environment.
- It applies to all CC/S/A including AD forests managed and operated by the DoD Fourth Estate; however, there is no single entity responsible for the Fourth Estate AD analogous to the role played by the Services for their AD environments. Future versions of this architecture will address Fourth Estate AD optimization/consolidation in more detail.
- The ADORA applies to all DoD AD environments; however, the extent of applicability to less well connected and smaller tactical environments will be addressed in implementation policy.
- AD optimization for the SIPRNET environment will be time dependent on implementation of hard tokens. AD optimization for JWICS or special purpose networking environments is not in the scope of this version of the ADORA.

1.7 Assumptions

- This reference architecture does not address physical access to an approved device. The Defense IT Infrastructure Library (ITIL) process guidance for Access Management requires implementation of a streamlined, standard DoD process for enabling physical access of users to attached end-user devices. It is assumed that all CC/S/A will implement Defense ITIL guidance.
- Compliance with the entire reference architecture will not be achievable upon initial implementation. A phased implementation will be required.
- The integrity of PKI authentication depends on hardware support for key protection. This includes PKI keys issued to non-person entities such as servers or services.
- Access control implementation will vary by system.
- Front-end interfaces are more important than back-end or intra-system interfaces. Workforce Mobility more critically depends on the front-end. The user does not care if the back-end information store is a set of Common Internet File System (CIFS) shares or an Oracle database as long as the front-end is a Web application that can be accessed from anywhere and accepts the user's DoD issued PKI certificates and hard tokens for authentication.

- Where current policy and instructions conflict with the goals, principles, and positions of this reference architecture, the policy and instruction will be changed appropriately, but will be followed until that time.

1.8 Constraints

- The ADORA provides a vision for the future-state (18-24 months) of Active Directory in the DoD through principles, rules, technical positions (standards), and architectural patterns. It does not have the force of policy nor does it direct or authorize the transition to the depicted future state. The policy, TTPs, and other guidance necessary to transition to this future state will be promulgated separately and in collaboration with CC/S/A stakeholders and the IA community.
- This reference architecture will be developed iteratively, meaning it will be revised and updated at regular intervals for the foreseeable future.
- This reference architecture does not address Data at Rest (DAR) Encryption or MAC layer device access. These security measures may be addressed in future versions of this document.
- This reference architecture does not specifically address access to the NIPRNET via VPN technology, but it does not preclude the development of component solutions that include VPN that otherwise comply with this reference architecture, are compliant with DoD IA guidelines and directives, and are approved by the cognizant DAA.
- This version only addresses access from a "DoD network user environment" for designated DoD users who possess DoD issued PKI certificates and hard tokens on the Non-Classified Internet Protocol Router Network (NIPRNET); including active duty military and selected reserves, civilian employees and designated contractors and other designated, non-DoD, federal employees. It does not address access by state and local government personnel, retired military personnel, military dependents, commercial businesses, Allies, coalition partners, or others who do not have DoD issued PKI certificates. Future version may address PKI cross domain Certificate Authority (CA) interoperability with DoD PKI trusted PKI CAs.
- Portable identity credentials such as the Common Access Card (CAC) and other DoD PKI certificates presented on hard tokens will be used to support user authentication.
- This reference architecture does not define authorization attributes.
- This reference architecture does not address funding that may be required, particular technologies that may be implemented, timelines for implementation, or the necessary authority (DAA) for executing certain system changes.

1.9 Linkages to Other Architectures, Programs, and Initiatives

1.9.1 The AD Optimization Environment

The ADORA is just one of the elements necessary to achieve the stated AD optimization goals. The ADORA describes the target state (the what) in terms of principles, rules, technical positions (standards), and architectural patterns but it does not prescribe policy or otherwise address transition to the target state (the how and when). These other elements of AD Optimization to be developed separately include:

- An ADORA Transition Strategy
- An ADORA Transition Policy
- New or Revised TTPs (e.g. CONOPS, STIGs, CTOs, and GTGs)

1.9.2 External Linkages

AD Optimization is directly influenced by the GIG 2.0 effort and addresses multiple capability gaps identified in the GIG 2.0 Initial Capabilities Document. Consequently, the ADORA is identified as a key initiative in the GIG 2.0 Implementation Plan. The ADORA provides guidance that primarily addresses GIG 2.0 Characteristic 1: Global Authentication, Access Control, and Directory Services.

The Enterprise-wide Access to Network and Collaboration Services Reference Architecture (EANCS RA) developed by OSD NII depicts the high-level, long-term future vision for connecting users and devices to Web-enabled enterprise services and applications. The EANCS RA is vendor and technology agnostic: allowing it to serve as a foundation for a range of more specific architectures and solutions. The ADORA is one of these more specific, time limited, architecture that aligns to the EANCS RA vision.

The Enterprise User (EU) program is a joint effort of OSD/NII, the Joint Staff, DISA, NSA, and DMDC intended to enhance the experience of DoD users by streamlining authorized access to DoD networks and information. EU develops solutions that conform to GIG 2.0 ORA Characteristic 1, the EANCS RA, and the ADORA. For example, the EU initiative known as DoD Visitor is one solution that conforms to the ADORA Global Logon capability.

The ADORA Principles were derived by leveraging Defense Information Enterprise Architecture (DIEA) Principles and modifying them to reflect the ADORA's goals and objectives.

The ADORA is a component of a series of DoD IT Infrastructure Optimization initiatives and leverages other components, most notably the Defense ITIL Access Management Process Guidance.

1.10 Organization of This Document

Section 1 is an adaptation of the DoDAF AV-1 and provides the strategic purpose and overview of the reference architecture. Section 2 provides the operational viewpoint in the form of an OV-6a Operational Rules model and a series of OV-1 Operational Concept graphics. Section 3 uses the StdV-1 to convey the technical positions relevant to the reference architecture. The AV-2 Vocabulary and glossary of terms is included as Appendix A. A Capability Taxonomy (CV-2) is provided as Appendix D. Other appendices provide a list of references and an overview of Component AD consolidation.

2.0 Principles, Rules² & Operational Patterns (OV-6a, OV-1s)

Note: This section consists of six tables, one for each of the six goals. For each goal, principles are numbered sequentially starting at “1.” Rules associated with each principle are labeled sequentially with lower case letters starting with “a.”

2.1 Goal 1 – Improving the Security of the DoD AD Infrastructure

2.1.1 Principles and Rules

Goal 1 – Improving the Security of the DoD AD Infrastructure		
#	Principles & Rules	Notes
1.	DoD networks, as components of the GIG, must be conscientiously designed, managed, protected, and defended.	DIEA
2.	The DoD will operate and defend the GIG as a unified, agile, end-to-end information resource.	DIEA
3.	<u>Separation of Device & Persona Authentication & Access Control.</u> Separate AD instantiations will be used for device authentication & access control and persona/people authentication & access control.	To be more fully developed in a future version.
4.	<p><u>Least Privilege.</u> Personnel who are system administrators will logon to domain controllers, servers, and end-user devices only using accounts with the minimum level of authority necessary.</p> <ul style="list-style-type: none"> a. No account is a member of the Forest Enterprise Administrators group and a child of the Domain Administrators group at the same time unless the Forest contains only the one Domain. b. Accounts designated to perform OU or Group administration do not have membership in the Domain or Forest Administrative Groups. c. Accounts designated to perform OU or Group administration will be separate from the individual’s User account. d. OUs containing end-user devices and/or user accounts will not contain servers or service accounts. e. OUs containing servers or service accounts will not contain end-user devices or user accounts. f. Security principles (Users, Groups) granted privileges over OUs containing end-user devices and accounts will not also be granted privileges over OUs containing servers or service accounts. 	Applicability to tactical networks/Active Directory forests will be addressed in ADORA transition planning guidance to be separately promulgated.

² Note on Rule Applicability: These rules are not intended to modify official policy documents such as DoDDs, DoDIs, DISA-issued STIGs, accreditation packages approved under DIACAP or FISMA processes, or similar authoritative sources. If there is any question as to the applicability of any rule in this document versus that of an authoritative source, the authoritative source guidance will be followed. Changes to those official documents will be made in those cases where ADORA guidance must be implemented.

	<ul style="list-style-type: none"> g. Groups granted privileges over OUs containing servers and service accounts will not be granted privileges over OUs end-user devices and user accounts. h. Normal user and user workstation Administrators group members are not able to modify the membership of admin groups or to audit & monitor changes to these groups. i. Normal user workstation Administrators group members are not able to manage workstations used by Enterprise or Domain Administrators. j. Functionality of domain administrator accounts is restricted so that only essential applications are available (e.g. no e-mail when logged in as an administrator). k. Personnel who are administrators will logon to administration accounts only when absolutely necessary; normal accounts are used for personal work. l. Logging on to admin accounts or accounts in OU admin groups will be done using a separate token (or approved alternative credential program as directed in DoD or Service TTP) specific to the admin account or group. m. Two-person control will be implemented for management of tokens associated with Forest Enterprise Administrator group level access. n. AD Data Management and Delegation of Administration tools will be used to reduce the number of administrator personnel in privileged groups as part of the implementation of <u>Least Privilege</u>. 	
<p>5.</p>	<p>DoD information programs, applications and computer networks will protect data in transit and at rest according to current DoD policy.</p> <ul style="list-style-type: none"> a. All mobile PCs (Laptops, Tablets) will use hard drive level encryption. 	<p>DoD DAR and TMP Decree: DoD Memorandum “Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media,” July 3, 2007</p>
<p>6.</p>	<p>All DoD information services and applications must uniquely and persistently digitally identify and authenticate users and devices.</p> <ul style="list-style-type: none"> a. All computers and devices will be, if capable, members of an Active Directory domain. b. All services, web services, and applications will use Windows Server based security services to enforce authorized access to information and other services or devices according to specified access control rules and quality of protection requirements for all individuals, organizations, COIs, automated services, and devices. c. Only properly authenticated digital identities are granted 	<p>DoDI 8520.02</p>

	<p>access to hosted resources.</p> <p>d. Users will authenticate to applications and services with PKI credentials or via Secure Token Service based solutions.</p>	
7.	<p>Network/AD security management policies and processes (TTPs) will follow established DoD policy and best practices.</p> <p>a. Each Service and Agency will have an AD Management CONOPS, specifically defining NetOps and Administrator Oversight.</p> <p>b. Each Service and Agency will have a Directory Lockdown Policy consistent with Defense ITIL common TTPs.</p> <p>c. Each Service and Agency will ensure all Windows Servers are maintained with the most recent security patches.</p> <p>d. AD system administrators will be trained and certified per IA best practices and Component policy.</p> <p>e. Proactive Operational Monitoring will be done on all AD servers and services per STIG guidelines.</p> <p>f. Proactive auditing of all AD servers and services (including incident detection & response procedures) will be done per current DoD policy.</p> <p>g. Annual red and blue team assessments are conducted on all AD-enabled environments.</p> <p>h. Processes are in place to define and exercise DNS zone containment.</p> <p>i. Processes are in place to define and exercise suspense of access to accounts with compromised DoD issued PKI certificates and hard tokens (e.g. CAC, PIV).</p> <p>j. Encryption of Data at Rest is implemented per current DoD policy.</p> <p>k. End-user device Operating Systems are Federal Desktop Core Configuration (FDCC) compliant.</p> <p>l. Active Directory Domain Controllers and backups will be secured and physical access will be restricted to authorized personnel only.</p>	<p>DoDI 8520.02</p> <p>DoDD 8570.01-M</p>
8.	<p><u>Intrusion Containment.</u> Systems will be designed to contain a compromise within the compromised system or system component.</p> <p>a. Application servers that use only Direct PKE and/or STS/ADFSv2 for authentication will only be in application forests that</p> <p style="margin-left: 40px;">a. do not have trust relationships with other forests, and</p> <p style="margin-left: 40px;">b. do not also contain</p> <p style="margin-left: 80px;">i. servers that use other means of authentication, or</p> <p style="margin-left: 80px;">ii. end-user devices</p> <p>b. End-user devices will only be contained in Component User Account/Device Forests.</p> <p>c. Mission-critical servers that use Kerberos to authenticate users will not be in the same forest as end-user devices or in forests that may use LANMAN, NTLM, or NTLMv2 for user</p>	<p>DoDI 8500.2</p> <p>DoDI 8520.02</p>

	<p>authentication.</p> <p>d. Mission-critical servers (such as critical logistics application servers) will not be in the same forest as end-user devices or application servers which are not compliant with all DoD IA requirements.</p> <p>e. Forests that host services using LANMAN, NTLM, NTLMv2, or Kerberos authentication will have only a single, one-way trust relationship with the forest containing the applicable end-users and end-user accounts and devices. These forests will not be trusted for user authentication.</p>	
9.	<p><u>Resistance to Compromise.</u> Systems will be designed to be resistant to compromise by unauthorized entities.</p> <p>a. The newest version of the Active Directory/Windows Server Operating System will be used for all domain controllers.</p> <p>b. Network security policy is set to deny incoming LANMAN, NTLM, & NTLMv2 traffic for forests that do not contain apps requiring those authentication types.</p> <p>c. Internal processes and controls are established to ensure no person ever logs on, either directly or by using remote logon, using an account with forest or domain level administrative privileges, to any device other than a domain controller or workstations or servers dedicated to the performance of active directory administrative functions.</p> <p>d. An out-of-band network capability or other capability is in place that prevents forest, domain, or admin accounts other than workstation admin accounts to logon to end-user workstations.</p> <p>e. Security and/or Group Policy will be enforced by the Active Directory/Domain Services and adhered to by all Operating System types.</p> <p>f. Internal processes and controls are in place to require multi-factor authentication for logging on to forest, domain, or OU admin accounts.</p> <p>g. Component networks will comply with DoD NIPRNET DMZ policy for public and private-facing applications.</p>	<p>Windows Server 2008 Security Guide (Version 3.0) p 55</p> <p>NIPRNET DoD DMZ Increment 1 Phase 1 STIG</p> <p>CTO 10-065</p>
10.	<p><u>Early Detection of Compromise.</u> Systems will be designed to detect the compromise of any component.</p>	DIEA
11.	<p><u>Recovery.</u> Systems will be designed and instrumented to ease recovery from a security event.</p>	DIEA

2.1.2 Operational Concept Graphic

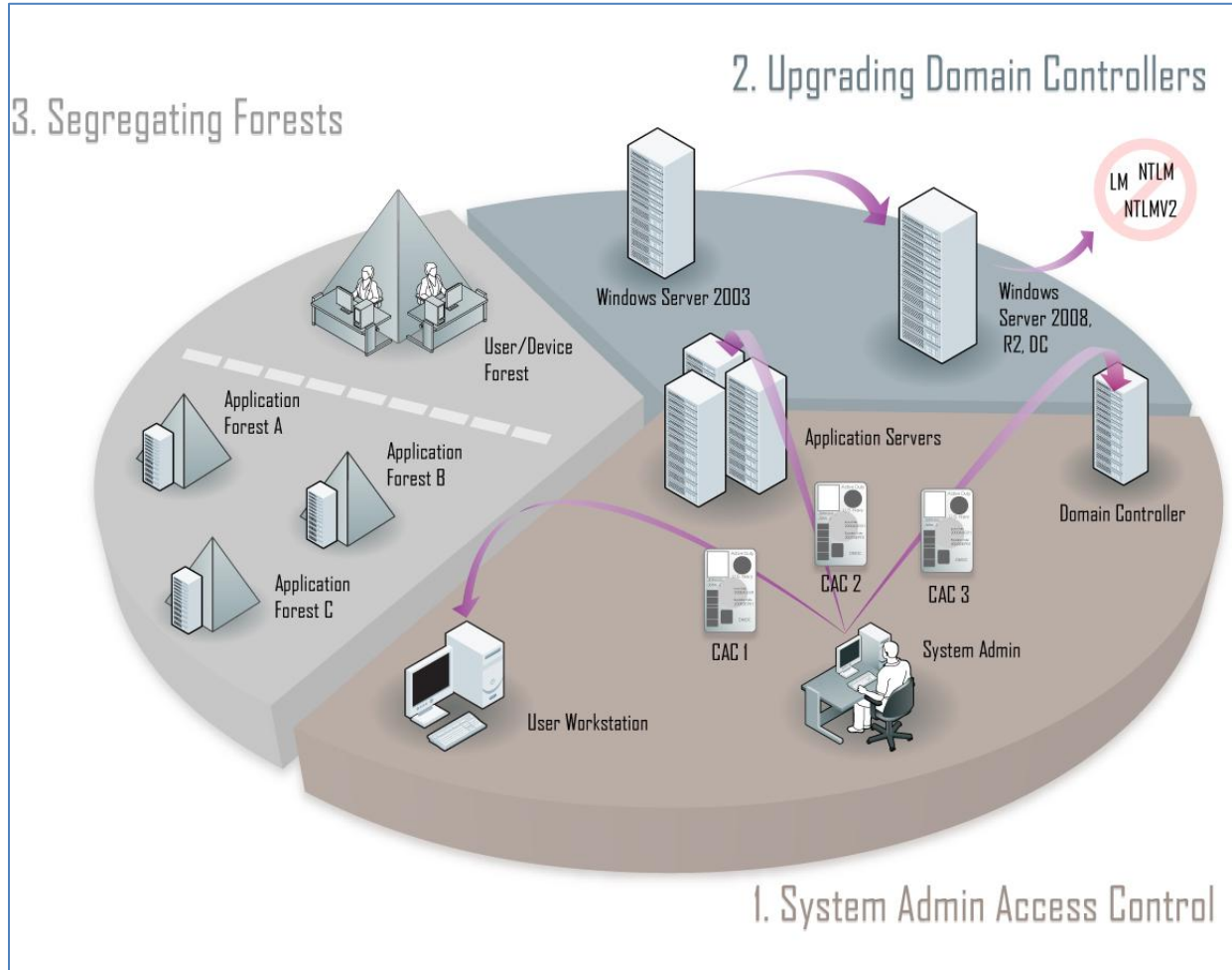


Exhibit 2. Improving the Security of the DoD AD Infrastructure OV-1

Exhibit 2 depicts three key concepts for securing the DoD AD infrastructure that underlie this reference architecture.

The first is constraining the way network system administrators use credentials to authenticate to domain controllers, application servers, and end-user devices. Under the principle of Least Privilege, a system administrator would grant or use no more privilege or authority than necessary for each action.

Some examples:

- Don't use system administrator credentials for normal end-user functions such as browsing the Internet or reading personal email.
- If you are only managing workstations, don't act with an account that also has the authority to manage AD accounts or servers.
- If you are managing a server, don't act with an account that also has the authority to manage AD accounts or workstations.

- If you are managing a lower-level domain, don't act with an account that also has the authority to manage top level domains.

The second key security concept depicted in Exhibit 2 is the upgrading of all domain controllers to run Windows Server 2008 R2 (or later) for those forests that will host applications that only use direct PKE or STS for user authentication. This version of Windows Server allows system administrators, as directed through existing processes (e.g. CTO), to disable certain modes of user authentication that present a significant risk of compromise.

The final key security concept depicted in Exhibit 2 is that of segregating large user/device forests from forests hosting applications.

2.2 Goal 2 – Global User Logon

2.2.1 Principles and Rules

Goal 2 – Global User Logon		
#	Principles & Rules	Notes
1.	<p>The GIG will enable connectivity to all authorized users. The objective AD end-state must therefore enable any authorized DoD user at any DoD location to login and be productive on a locally authorized end-user device.</p> <p>a. Each Component must implement the Global User Logon solution on all non-deployed, NIPRNET and SIPRNET user domains per guidance in this architecture and the applicable version of the Directory Services STIG and any CTOs that may be issued.</p>	DIEA
2.	<p>DoD issued PKI certificates and hard tokens are the basis for authenticating users to the network.</p> <p>a. Each user must authenticate via DoD issued PKI certificates and hard tokens.</p> <p>b. Every desktop and laptop must have a device for reading DoD issued hard tokens.</p> <p>c. The administrative entity responsible for the user's permanent location is responsible for the status of the user's credentials.</p> <p>d. The visited location is not responsible for the user's credentials but is responsible for user behavior.</p>	DoDI 8520.02
3.	<p>The Global User Logon solution will provision the visiting user into a visitor account in the local AD forest once the user's DoD issued PKI certificates and hard tokens have been properly authenticated.</p> <p>a. The visitor account will provide, at a minimum, the user with access to a Web browser and to local printing capabilities.</p> <p>b. The Global Logon solution will include the capability for host</p>	

	commands to provide additional capability to the visited user beyond the Web browser and printer.	
4.	<p>Defense ITIL is the authoritative source for ITSM operational best business practices and will be used throughout the DoD.</p> <ul style="list-style-type: none"> a. Defense ITIL Access Management Process guidance will be followed for physical access of visiting users to end-user devices. b. The standard DoD Enterprise IA Training is used as the basis for establishing that a user is in compliance with annual IA training (see Defense ITIL Access Management Process Guidance). 	
5.	The architecture will permit an authorized person to use any DoD workstation to access any resources required for the user to be productive.	Future
6.	The architecture will permit any authorized DoD workstation to access any resources that are required for a user to be productive.	Future

2.2.2 Operational Concept Graphic

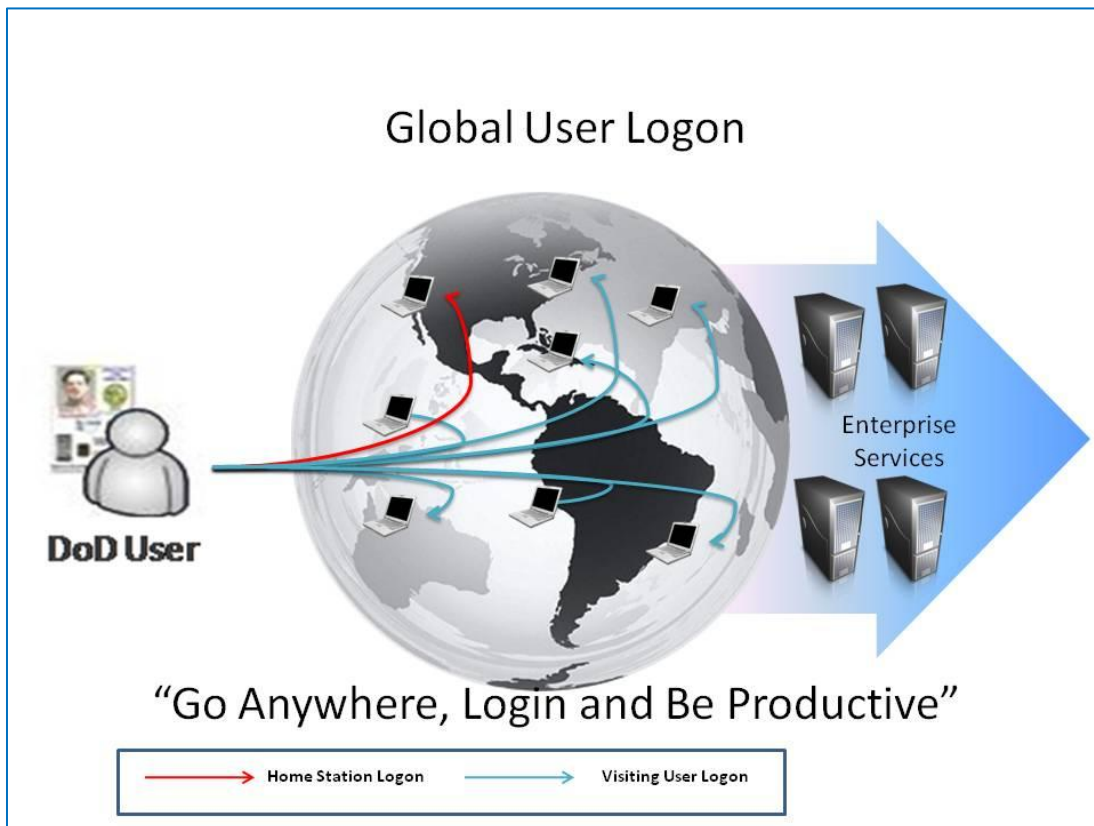


Exhibit 3. Global Logon OV-1

DoD personnel are typically provisioned as users within the Active Directory environment associated with their home station (sometimes referred to as a permanent duty station for military personnel). The AD establishes the ability of a user to function within a local area computer network, access local resources and information, and access enterprise level information and resources (such as the NIPRNET) to which they are authorized. Once the user is provisioned, the involvement of the local system administrator is not required for ongoing user access from within their home station AD environment as long as the user remains in compliance with local and enterprise policy (e.g. annual IA training).

However, access to network-enabled information and resources is limited or not timely when the user is visiting a different DoD installation and different AD environment. Local administrators and information assurance personnel must manually provision a visiting user to provide even a minimal level of access. This administratively intensive process can take anywhere from hours to weeks to complete. These limitations are driven by policy and by the way AD technology is implemented. Taken together, these bureaucratic and technical hurdles effectively prevent the ability for DoD personnel to be fully productive immediately upon arriving at the visited installation. The ADORA addresses this bottleneck and enables dynamic solutions for user provisioning. Given the imperative to share information and to provide access to unanticipated users, this is a critical shortfall that must be corrected.

Exhibit 3 depicts the global logon concept whereby any authorized DoD user with valid DoD issued PKI certificates and hard tokens is able to logon to any local DoD network (unclass/NIPRNET domain first and later Secret/SIPRNET domain). In the case of the user logging into their home station network, the logon process is the standard, normal logon with all of the access and privileges which have been granted to the user. In the case of the user logging in to another network (different Active Directory forest), the user will be provisioned into a special, non-persistent visitor account using their unique EDIPI and granted a limited set of privileges including access to a Web browser and access to local printers. This special account will be deleted once the visiting user removes their CAC.

2.3 Goal 3 – Sharing AD Contact Objects Across Forests

2.3.1 Principles and Rules

Goal 3 – Sharing AD Contact Objects Across Forests		
#	Principles & Rules	Notes
1.	Data assets, services, and applications on the GIG will be visible, accessible, understandable, and trusted to authorized (including unanticipated) users.	DIEA
2.	User contact information will be exposed so as to be readily discoverable and accessible across the DoD IE and available through E-mail client applications, Web-based E-mail applications, and on authorized DoD smartphones. a. Contact object sharing will be provided as a DoD Enterprise-level service, but in the interim, Component-level solutions may be established that conform to this architecture (e.g.	DIEA DoD Enterprise Directory Services Capability Contact Attributes Specification v2.0:July 2009

	<p>PACOM GAL Synchronization solution provided by AFDS and leveraging existing Microsoft Identity Lifecycle Management servers).</p> <p>b. Components may choose other Components or sub-Component organizations with which they wish to share their AD contact information.</p> <p>c. Sharing contacts across AD forests must be done in accordance with this reference architecture, the DoD CIO contact specification, and any subordinate solution architectures that may be developed.</p>	
--	--	--

2.3.2 Operational Concept Graphic

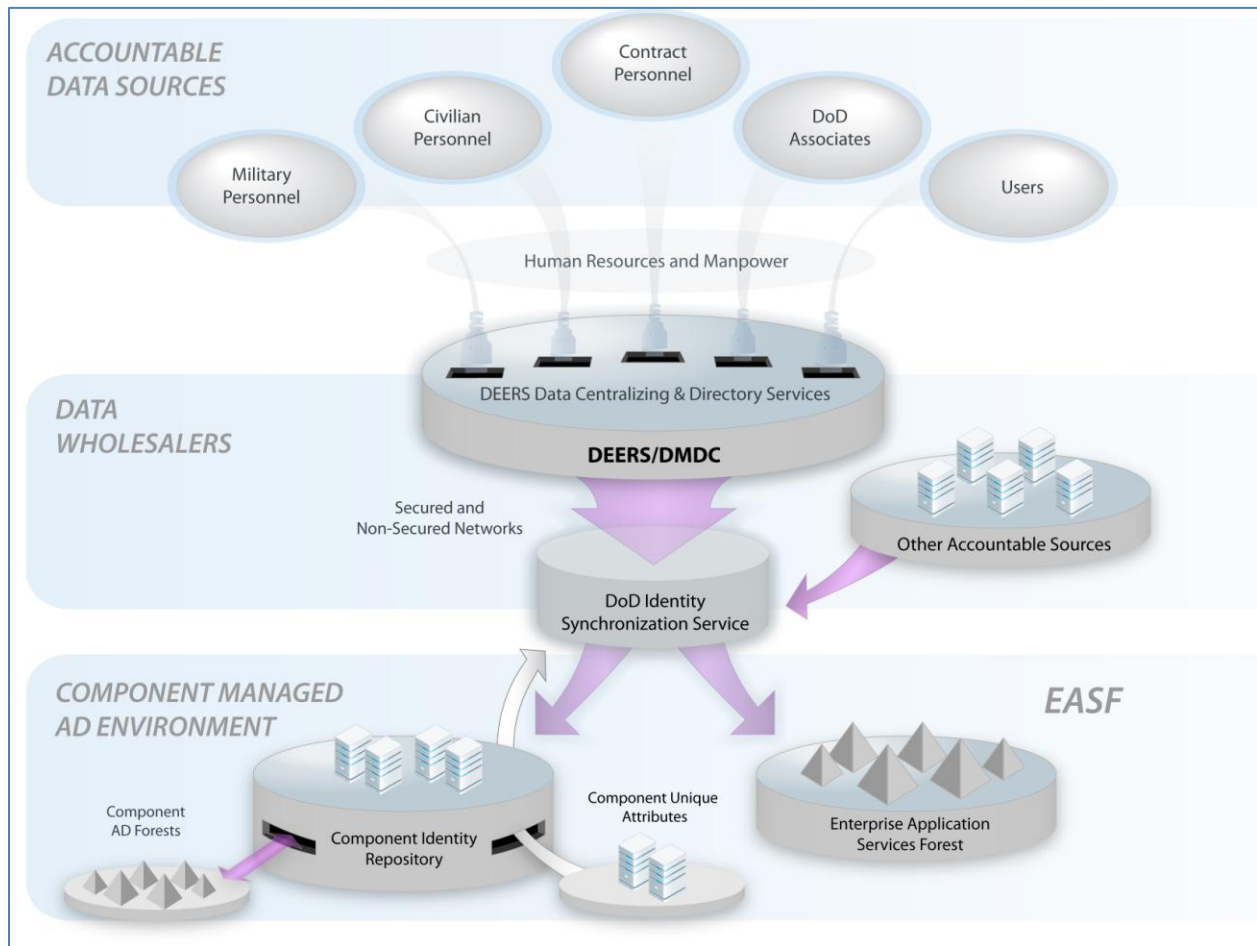


Exhibit 4. Identity Management/Contact Sharing OV-1

In the future, core AD identity and attribute information for all DoD users will flow from accountable data sources through an Enterprise (Joint) Identify and Directory Service, then pushed to component identity repositories, and finally used to populate local AD domains. AD will be a consumer of identity information rather than a provider as is the case today. Users will be able to look-up GAL contact information for the entire DoD Enterprise through a service that is integrated with their e-mail client.

Exhibit 4 depicts this high level concept and also shows that component unique attributes will be accommodated by designing an extensible enterprise identity data schema. Exhibit 4 also shows how the enterprise attribute and identity management service will be used to provide access for all authorized DoD users to the applications and services managed within the Enterprise Support Forest.

2.4 Goal 4 – Sharing AD-dependent Applications Across Forests

2.4.1 Principles and Rules

Goal 4 – Sharing AD-dependent Applications Across Forests		
#	Principles & Rules	Notes
1.	Data assets, services, and applications on the GIG will be visible, accessible, understandable, and trusted to authorized (including unanticipated) users.	DIEA
2.	Computing infrastructure must support all missions of the DoD and provide the tactical edge with effective, on-demand, secure access to shared spaces and information assets across functional, security, national, and interagency domains.	DIEA
3.	DoD Enterprise-level data and information will be discoverable and readily accessible by all authorized users across all AD account forests (used to perform user/device/server/policy management) and application forests within the NIPRNET and SIPRNET domains. <ol style="list-style-type: none"> a. All active directories (component and enterprise level) obtain core user information data (for attribute-based access control decisions) from the Enterprise Identity/Attribute Service provided by DISA and DMDC. b. The DoD Enterprise attribute data management schema will be configured so as to allow for the addition of Component unique attributes to the core enterprise attributes for making access control decisions within Component or Enterprise AD environments. 	DIEA
4.	Component and/or sub-Components may determine other Component and/or sub-Component organizations with which they wish to share Component-level data and information. <ol style="list-style-type: none"> a. Sharing applications across AD forests must be done in accordance with this reference architecture and any subordinate solution architectures that may be developed in the future. b. Components who own the license for a Commercial-off-the-Shelf (COTS) application must ensure license compliance prior to sharing use of the application with other Component and/or sub-Component organizations. 	

5.	Direct DoD issued PKI certificates and hard tokens or approved DoD Secure Token Services (STS) solutions are used for sharing AD-dependent applications across forests.	
6.	Active Directory application forests that are separate from AD account forests will provide identity and access control service to Microsoft-based enterprise applications (such as Exchange and Sharepoint) for all valid (licensing compliance requirements are satisfied) DoD and partner/affiliate users from any point in the GIG.	

2.4.2 Operational Concept Graphic

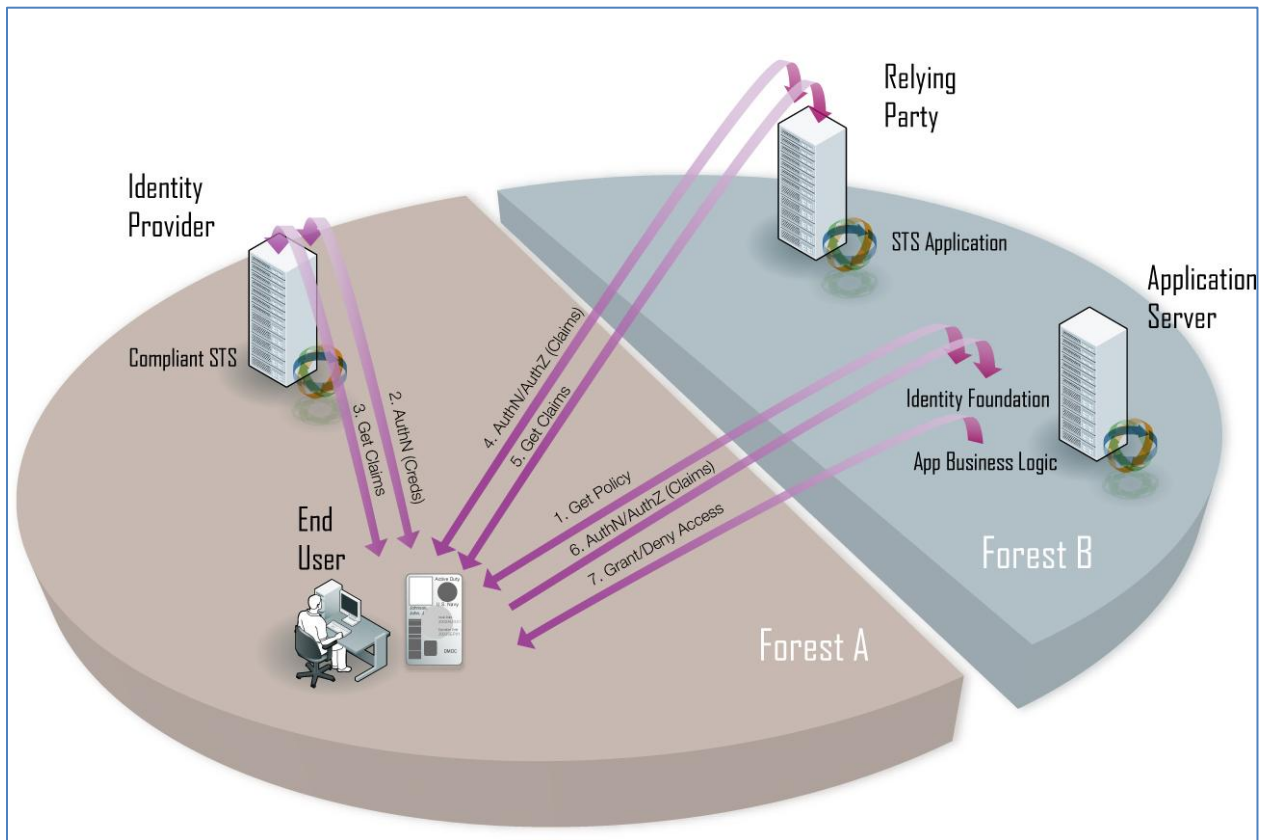


Exhibit 5. Sharing AD-dependent Applications Using STS OV-1

The target state envisioned by this reference architecture is characterized by the use of secure means for users to authenticate to applications within and across AD forests. The two authentication technologies allowed under this architecture are direct PKI and those based on industry standard Secure Token Service (STS).

Exhibit 5 describes how STS is used between two forests. Forest A is a user/account forest with an end user that needs to access an application in Forest B (the relying party). These two forests must have previously established a federated trust (not the same as an AD trust) between them. The user presents his/her credentials to the servicing STS and if authenticated, the STS provides a one-time token to the user with the imbedded claims information. This claim is then presented to the relying party which grants or denies access based on the policy established.

2.5 Goal 5 – Optimize Rapid Reconfiguration/Agility

2.5.1 Principles and Rules

Goal 5 – Optimize Rapid Reconfiguration/Agility		
#	Principles & Rules	Notes
1.	The GIG infrastructure must be rapidly scalable, changeable, deployable and manageable, while anticipating the effects of the unexpected user.	DIEA
2.	GIG infrastructure capabilities must be survivable, resilient, redundant, and reliable to enable continuity of operations and disaster recovery in the presence of attack, failure, accident, and natural or man-made disaster.	DIEA
3.	The AD Infrastructure must be designed, implemented, and operated so as to enable and support the transition to a seamless Defense Information Enterprise.	DIEA
4.	The AD Infrastructure must be designed, implemented, and operated so as to enable rapid and precise changes in information access and flow, and resource allocation or configuration.	DIEA
5.	The Computing Infrastructure (CI) will be consolidated, to the greatest extent possible, so that fixed global/regional and deployed virtual CI resources are used efficiently.	DIEA
6.	The Computing Infrastructure will be responsive to and supportive of the capability needs and requirements of the edge environment, despite intermittent connectivity or limited bandwidth.	DIEA
7.	GIG communications systems will provide the flexibility to support network connectivity to all GIG nodes and users, including those changing their points of attachment among alternate operational and network domains and/or communities of interest.	DIEA
8.	Authoritative data assets, services, and applications will be accessible to all authorized users in the DoD, and accessible except where limited by law, policy, security classification, or operational necessity.	DIEA
9.	To support NetOps functions at all operational levels (strategic, operational, and tactical), all devices will have DoD issued certificates. Authentication and access control for devices (e.g. end-user devices, servers, and network control devices) will be provided by a separate and distinct future enterprise service offered by PMO PKI and DISA, not by the Active Directory infrastructure.	ADORA WG
10.	Applicable GIG programs must ensure that products and services provide the capability to allow a high degree of automation for NetOps C2, and must support dynamic adjustment of configuration and resource allocation.	DIEA
11.	Regularly scheduled backups of all AD servers and services will be done as well as periodic testing of backups.	
12.	Annual tests of forest-wide, domain-wide recovery plan (to include	DODI 8500.02

	accidental, malicious, natural disaster, etc) are conducted.	
13.	Well defined operational best practices (Change Mgt, Patch Mgt, Release Mgt, Incident Mgt, Problem Mgt, Disaster Recovery Planning and Execution) will be followed.	DIEA
14.	Standard Configuration Change/Control, Visibility & Support processes for Desktops/Laptops/handhelds and other AD-enabled devices will be implemented.	
15.	A Test Environment is in place to validate approved changes to AD configurations prior to implementation.	
16.	Centralized administration of all domain controllers will be implemented to the maximum extent possible, recognizing the need for deployable forces to be capable of independent operations.	
17.	The architecture will provide for enterprise hosting of enterprise services.	

2.5.2 Operational Concept Graphic

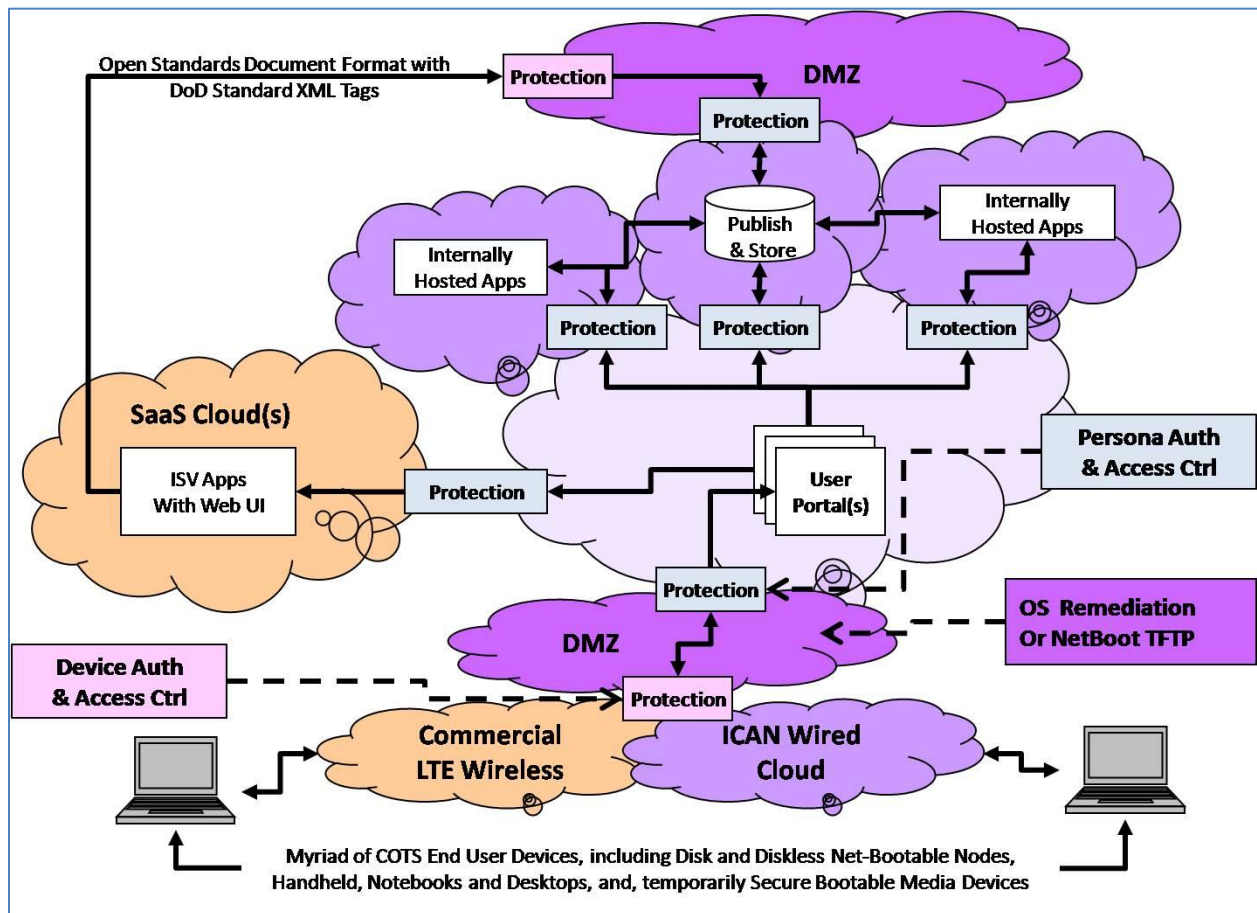


Exhibit 6. Separate Authentication & Access Control for Devices and Personas OV-1

Exhibit 6 depicts a future state in which authentication and access control decisions for personas (people) is facilitated using an AD infrastructure that is separate from the one used to make authentication and access control decisions for devices. This concept requires the implementation of a device PKE certificate infrastructure and associated policy and governance. This concept will be more fully developed in a future version of the ADORA.






2.6 Goal 6 – Optimize Affordability & Efficiency

2.6.1 Principles and Rules

Goal 6 – Optimize Affordability & Efficiency		
#	Principles & Rules	Notes
1.	Only Handle Information Once (the OHIO principle). AD information that exists should be reused rather than recreated.	DIEA
2.	Consolidation of computing infrastructure fixed-node operations is a desired result with respect to cost efficiencies. It will not be accomplished, however, at the expense of degrading mission capabilities and operational effectiveness.	DIEA
3.	Each Military Department will determine its own appropriate number of user device and legacy application forests based on the risks and benefits of different size forests and the specific resources managed within each in accordance with the rules and principles found within this document.	
4.	COCOM users may be part of an AD User Forest managed by their Executive Agent (Army, Navy, and Air Force). COCOMs may also implement and operate their own forests as operational needs may dictate.	
5.	Windows-based applications which use IIS, SQL Server, and Windows Server will be developed and fielded using standard DISA shared infrastructure services.	
6.	Components may implement forests for Component-unique applications and services, but all applications or services that are shared by two or more Components will reside in the DoD EASF unless operational security requirements necessitate a separate EASF.	
7.	Existing enterprise data, services and end-user interfaces will be used whenever possible, practical, and appropriate, instead of re-creating those assets.	

2.6.2 Operational Concept Graphics

2.6.2.1 AD Forest Type

Forest Type	Host	Governance	Apps	Allowable Authentication	Trusts	User Accounts	Devices
	DISA	DISA	Shared Enterprise	PKE STS	No	DoD Account Metaverse	No
	DISA	Component	Shared Component	PKE STS	No	Component Account Metaverse	No
	DISA	Component	Scoped to a single Component DAA	Kerberos LM/NTLM/NTLMv2	Yes, to corresponding UDF	No	No
	Component	Component	Scoped to a single Component DAA	Kerberos LM/NTLM/NTLMv2	Yes, to corresponding LARF	Yes, local	Yes
	Component	Component	Apps that cannot be managed within a DECC or UDF	Kerberos LM/NTLM/NTLMv2	Yes, to corresponding UDF	No	No

EASF: Enterprise Applications Services Forest UDF: User/Device Forest (Component) ORF: Optional Resource Forest (Component)
DASF: Dedicated Applications Services Forest LARF: Legacy Applications Services Forest

Exhibit 7. AD Forest Type

The future DoD AD infrastructure will consist of a small number of DoD Enterprise and Component AD forests that are logically interconnected (see Exhibit 8) and together provide all DoD users with access to all Enterprise and Component-specific applications to which they are authorized. Exhibit 7 is a table that identifies the types of AD forests along with information on the rules for each forest type in terms of hosting, governance, applications, trusts, user accounts, and end-user devices.

2.6.2.2 AD Service/Resource Forest High Level Architecture

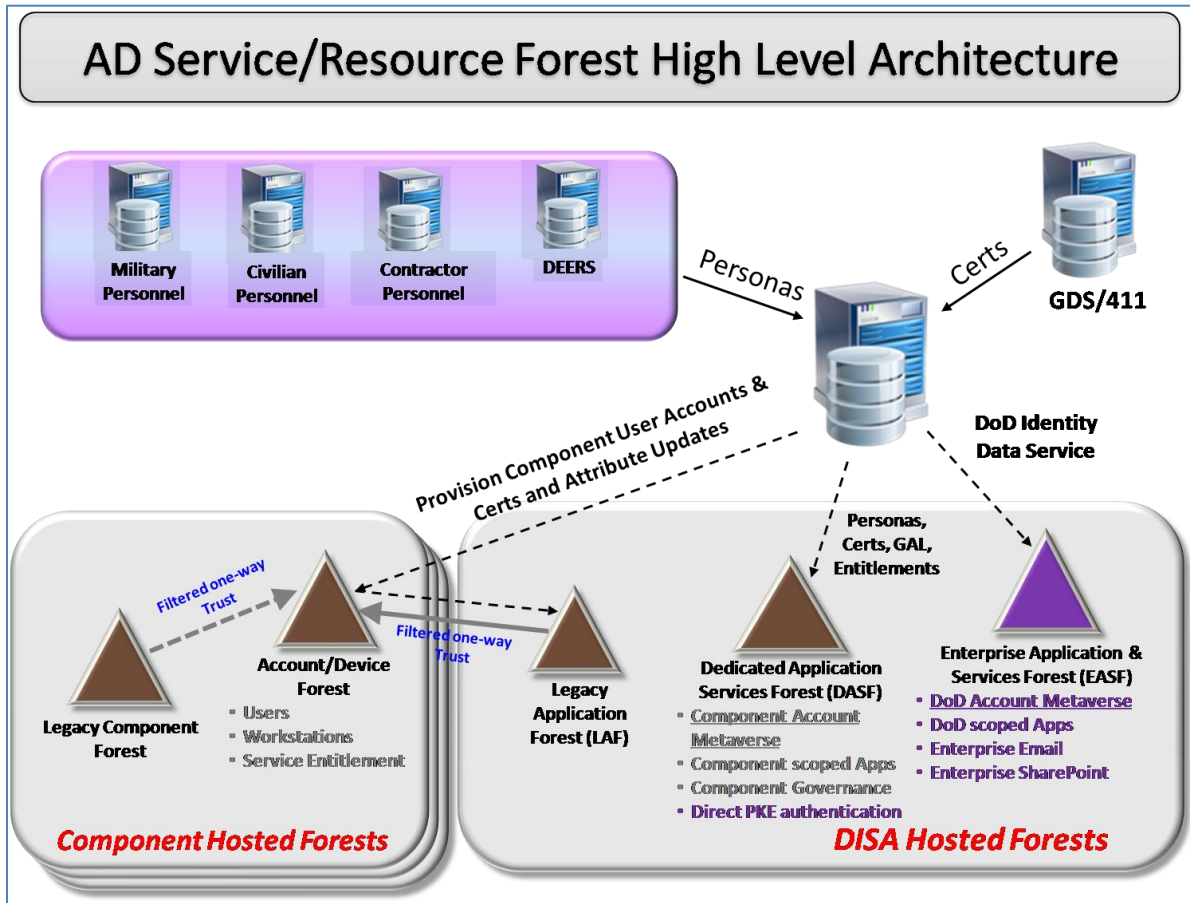


Exhibit 8. AD Service/Resource Forest High Level Architecture OV-1

Exhibit 8 depicts the notional, DoD Enterprise & Component AD forest architecture optimized for security and affordability. This architecture consists of a minimal set³ of AD forests split between those hosted by the DoD Enterprise (e.g. DISA) and those hosted by a Component. The EASF will host all web-based applications configured for direct PKE or STS authentication, will be hosted and governed by DISA, and will contain accounts for all DoD users (~ 4.5 million). A DASF will follow the same rules as the EASF but the governance and user accounts will be aligned to the Component for which the forest is hosted. A LARF will contain applications of a particular Component or sub-Component that require Kerberos, LANMAN, NTLM or NTLMv2 authentication. A LARF will have a one-way trust with the corresponding forest that contains accounts and devices for the users of those applications. An Account/Device forest (UDF) will contain Component or sub-component user accounts and devices and may also contain Component or sub-Component applications that cannot be hosted by DISA. A Legacy Component Forest is an optional forest for Component or sub-Component applications that cannot be hosted by DISA and that the Component or sub-Component chooses host outside of a UDF. Additional information on the AD forest structure can be found in C.2.

³ Although only a single forest of each type is shown, the actual implementation may consist of several actual forests that are logically managed as a single forest. Not all forest types shown will necessarily be in place for all Components. Only the EASF will be mandatory.

3.0 Technical Positions (StdV-1)

Standard Identifier	Standard Title	Abstract	Applicability
DODI 8500.2	Information Assurance (IA) Implementation	Implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks.	This standard is applicable to all of the capabilities being implemented.
	DoD Directory Services – Security Technical Implementation Guide Version 1, Release 1: August 2007	Security Technical Implementation Guide (STIG) providing security configuration and implementation guidance for application server products designed to the Java™ 2 Platform, Enterprise Edition (J2EE™).	This standard applies to the Contact Sharing capability being implemented.
	DoD Active Directory User Object Attribute Specification	Document developed to provide common naming and attribute guidance to DoD Components that deploy AD. The document specifies the naming convention and acceptable values for some of the attributes of AD User objects.	This standard is applicable to the Contact Sharing capability being implemented.
DODI 8551.1	Ports, Protocols, and Services Management (PPSM)	Defines restrictions on the use of the associated ports, protocols, and services in order to protect network-accessible DoD resources due to vulnerabilities identified for some network services.	This standard is applicable to the Contact and Resource Sharing capabilities being implemented.
	DoD Enterprise Director Services Capability Contact Attributes Specification v2.0:July 2009	Defines a set of contact attributes to be supplied to the Joint Enterprise Directory Services (JEDS) and included in the Enterprise Contact List (ECL) in support of DoD White Pages and Enterprise Global Address List (GAL) service capability.	This standard is applicable to the Contact Sharing capability being implemented.

Standard Identifier	Standard Title	Abstract	Applicability
DODI 8510.01	DoD Information Assurance (IA) Certification and Accreditation Process (DIACAP)	A process to ensure that risk management is applied on information systems (IS), defining a DoD-wide formal and standard set of activities, general tasks and a management structure process for the certification and accreditation (C&A) of a DoD IS that will maintain the information assurance (IA) posture throughout the system's life cycle.	This standard applies to all of the capabilities being implemented.
ITU-T X.500	Information Technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services	Certification representative of a series of computer networking standards covering electronic directory services.	This standard is applicable to the Application Sharing capability being implemented.
ITU-T X.509:2005	Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, August 2005	This Recommendation/International Standard provides the foundation frameworks for Public Key Infrastructure (PKI) and Privilege Management Infrastructure (PMI), upon which industry profiles can be defined by other standards groups and industry forums. ITU X.509 frameworks include Infrastructure Models, Certificate and Certificate Revocation Lists (CRL), Directory Schema Definitions and Path Processing Procedures. Many of the features defined as optional in these frameworks may be mandated for use in certain environments through profiles.	This standard should be used in an IT enterprise requiring digital signature-based secure connections between a clients and servers.
	Microsoft SharePoint 2010	A content management system with integrated search functionality that allows for the management of an organization with respect to their hierarchy levels and allows for third-party developers to develop custom modifications to extend functionality.	This standard is applicable to all of the capabilities being implemented.

Standard Identifier	Standard Title	Abstract	Applicability
STS WS- Federation WS-Trust	Security Token Service	Used to assert one's identity electronically in addition to or in place of a password.	This standard is applicable to the Application Sharing capability being implemented.
	Windows Server 2008 R2 +	A server operating system produced by Microsoft with the ability to share files and printers, act as an application server, host message queues, provide email services, authenticate users, act as an X.509 certificate server, provide LDAP directory services, serve streaming media, as well as perform other server-oriented functions.	This standard is applicable to all of the capabilities being implemented.
LDAP v3	Lightweight Directory Access Protocol	An application protocol for querying and modifying data using directory services running over TCP/IP. LDAPS is the SSL enabled version of LDAP and is the preferred PPSM protocol version for LDAP use in GAL and authentication directory communications.	This standard is applicable to the Application Sharing and third-party GAL contact list capabilities being implemented.

Standard Identifier	Standard Title	Abstract	Applicability
ANSI/INCITS 359-2004	Information technology - Role Based Access Control (RBAC)	<p>The RBAC Reference Model defines sets of basic RBAC elements (e.g., users, roles, permissions, operations and objects) and relations as types and functions that are included in this standard. The RBAC reference model serves two purposes. First, the reference model defines the scope of RBAC features that are included in the standard. This identifies the minimum set of features included in all RBAC systems, aspects of role hierarchies, aspects of static constraint relations, and aspects of dynamic constraint relations. Second, the reference model provides a precise and consistent language, in terms of element sets and functions for use in defining the functional specification.</p> <p>http://www.incits.org/scopes/1544.htm</p>	<p>There are many proprietary implementations providing role-based access control capabilities. This standard describes role-based access control features that have achieved acceptance in the commercial marketplace.</p>
CMS/XML Digital Signature Profiles v1.1	DoD Digital Signature Implementation Profiles	<p>Over the last several years, the DoD has made significant progress in improving the manner in which users are authenticated to Web applications and networks using the capabilities supported by the DoD Public Key Infrastructure (PKI). PKI-based digital signature capabilities are the cornerstone for transforming authenticated forms, documents and Web transactions to a paperless environment. Moving to a paperless environment must be accomplished without diminishing the interoperability required to collaborate and conduct warfighting jointly and seamlessly.</p>	<p>Any DoD application (Web or client based) that uses digital signatures with forms, documents, and/or Web objects to create legally binding DoD transactions.</p>

Standard Identifier	Standard Title	Abstract	Applicability
IEEE Std. 802.1D:2004	Local and Metropolitan Area Networks - Common Specifications - Part 3: Media Access Control (MAC) Bridges, 2004	Architecture for the interconnection of IEEE 802 Local Area Networks (LANs) below the MAC Service boundary is defined. MAC Bridges, as specified by this standard, allow communications between end stations attached to separate LANs, each with its own separate MAC, to be transparent to logical link control (LLC) and network layer protocols, just as if the stations were attached to the same LAN.	IEEE 802 LANs can be connected using Media Access Control (MAC) Bridges. Each individual LAN has its own independent MAC. The Bridged LAN created allows the interconnection of stations as if they were attached to a single LAN, even though they are in fact attached to separate LANs each with its own MAC. IEEE 802.1D specifies the Spanning Tree Protocol (STP) as a mechanism to enable loop-free, redundant bridging paths between routers.
SAML 2.0 OASIS	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005	OASIS SAML 2.0 defines the syntax and semantics for XML-encoded assertions about authentication, attributes and authorization, and for the protocol that conveys this information. The specifications define the syntax and semantics for XML-encoded SAML assertions, protocol requests, and protocol responses. These constructs are typically embedded in other structures for transport using SOAP 1.1 over HTTP.	Other titles are: Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005. Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005.

Standard Identifier	Standard Title	Abstract	Applicability
SPML v1.0	Service Provisioning Markup Language (SPML) Version 1.0	SPML (Services Provisioning Markup Language) is an XML-based framework specification for exchanging user, resource, and service related provisioning information among applications, organizations, corporations, or agencies. Provisioning, according to the OASIS Provisioning Services Technical Committee, is "the automation of all the steps required to manage (setup, amend, & revoke) user or system access entitlements or data relative to electronically published services."	SPML is part of an identity management infrastructure, and is the basis for integrating single sign-on and provisioning software for Web services.
FIPS 140.3	Federal Information Processing Standard (FIPS) Version 140.3	Revised version of the Federal Information Processing Standards Publication 140-2: Security Requirements for Cryptographic Modules. The standard provides a set of cryptographic modules (algorithms) – requirements that must be satisfied by a product before being considered for government acquisition.	In Windows Server 2008, only members of the Cryptographic Operators group can edit the crypto settings in the IPsec policy of the Windows Firewall.
DoDI 8410.02	DoDI 8410.02, NetOps for the Global Information Grid (GIG)	Institutionalizes NetOps as an integral part of the GIG, establishes policy, and assigns responsibilities for implementing and executing NetOps, the DoD-wide operational, organizational, and technical capabilities for operating and defending the GIG.	This standard is applicable to all of the capabilities being implemented.

Standard Identifier	Standard Title	Abstract	Applicability
DoDI 8520.02	DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling	Implements policy, assigns responsibilities, and prescribes procedures for developing and implementing a DoD-wide Public Key Infrastructure (PKI) and enhancing the security of DoD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption.	Applicable to all DoD unclass/class info systems including networks (e.g. NIPRNET, SIPRNET, web servers, and e-mail systems). Excludes SCI and info systems falling under DCID 6/3.
DoDD 8570.01-M	DoDD 8570.01-M, Information Assurance Workforce Improvement Program	Provides guidance and procedures for the training, certification, and management of the DoD workforce conducting Information Assurance (IA) functions in assigned duty positions.	Applies to Information Assurance workforce improvement for DoD Components.
NIST SP800-33	SP800-33: Underlying Technical Models for Information Technology Security	Provides a description of the technical foundations (models) that underlie secure information technology (IT) and should be considered in the design and development of technical security capabilities. (Lessons learned, best practices, and specific technical considerations.)	Applicable to all of the capabilities being implemented.
NIST SP800-14	SP800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems	Offers generally accepted principles based on the premise that (most) everyone applies these when developing or maintaining a system.	Applicable to all of the capabilities being implemented.

Appendix A: Vocabulary (AV-2)

<i>Term</i>	<i>Definition</i>
AD	Active Directory
CAC	Common Access Card
CC/S/A	Combatant Commander/Military Service/Defense Agency or Field Activity
CIFS	Common Internet File System
CJTF	Commander Joint Task Force
COCOM	Combatant Commander
Component	OSD, the Military Departments (including the National Guard and Reserve components), the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the DoD, the Defense Agencies, DoD Field Activities, and all other organizational entities of the DoD ⁴
CONOPs	Concept of Operations
COOP	Continuity Of Operations Plan
CTO	Certificate to Operate
DAA	Designated Accrediting Authority
DC	Domain Controller
DCID	Certification and accreditation process used by federal agencies working on intelligence projects (e.g. CIA)
DECC	Defense Enterprise Computing Center
DEERS	Defense Eligibility Enrollment System
Department	Department of Defense, unless otherwise noted
DIACAP	Defense Information Assurance Certification & Accreditation Process
DISA	Defense Information Systems Agency
DTIL	Defense ITIL
DMDC	Defense Manpower Data Center
DMZ	Data Management Zone
EANCS	Enterprise-wide Access to Network & Collaboration Services
EASF	Enterprise Application Service Forest
ERF	Enterprise Resource Forest
ESSF	Enterprise Services Security Foundation
EU	Enterprise User
FDCC	Federal Desktop Core Configuration
Fourth Estate	The DoD Agencies, Field Activities, Office of the Secretary of Defense, the Joint Staff, and other organizational entities not aligned to a Service or

⁴ “Transforming Through Base Realignment & Closure (BRAC) 2005 – Joint Basing”, Memorandum from the Deputy Secretary of Defense, January 22, 2008

	COCOM executive agent
FISMA	Federal Information Security Management Act of 2002
FOGO	Flag Officer/General Officer
GAL	Global Address List
GIG	Global Information Grid
GPO	Group Policy Object
GTG	GIG Technical Guidance
IA	Information Assurance
IEEE	Institute of Electrical & Electronics Engineers, Inc.
IIS	Internet Information Services
Installation	Base, Station, Camp, or Post
ISV	Independent Software Vendor
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	IT Service Management
JEDS	Joint Enterprise Directory Service
JWICS	Joint World-wide Intelligence Communication System
Kerberos	Computer network authentication protocol which allows nodes communicating over a non-secure network to prove their identity to one another in a secure manner
LAF	Legacy Application Forest
LAN	Local Area Network
LANMAN	One of the formats that Microsoft LAN Manager and Microsoft Windows versions prior to Windows Vista use to store user passwords that are fewer than 15 characters long
LTE	Long Term Evolution
MAC	Media Access Control
MILDEP	Military Department (e.g. Department of the Navy, Department of the Army, Department of the Air Force)
NIPRNET	Non-classified Internet Protocol Routed Network
NOSC	Network Operations Security Center
NTLM/NTLMv2	NT LAN Manager (not to be confused with LAN Manager)
OU	Organizational Unit
PKE	Public Key Enabling
PKI	Public Key Infrastructure
Principles	Enduring guidelines that describe the way in which an organization should fulfill its mission. Principles express an organization's intentions so that design and investment decisions can be made from a common basis of understanding.

Rules (Business or Technical)	Business rules are definitive statements that constrain operations to implement the principle and associated policies
SaaS	Software as a Service
SAML	Security Assertion Markup Language
Service	One of the four military services (Army, Air Force, Navy, Marine Corps)
SIPRNET	Secret Internet Protocol Routed Network
SQL	Structured Query Language
SSL	Secure Socket Layer
STIG	Security Technical Implementation Guide

Appendix B: References

- a) Joint Pub 6-0, Joint Communication Systems, March 20, 2006
- b) GIG 2.0 Operational Reference Architecture, Version 1.5b, January 27, 2010
- c) GIG 2.0 Initial Capabilities Document, May 29, 2009
- d) GIG 2.0 Implementation Plan, Version DRAFT, April 27, 2010
- e) Defense Information Enterprise Architecture, Version 1.1, May 27, 2009
- f) Directory Services Security Technical Implementation Guide (STIG), Version 1, Release 1, August 24, 2007
- g) Network Infrastructure Security Technical Implementation Guide (STIG), Version 7, Release 1, October 25, 2007
- h) Access Control in Support of Information Systems Security Technical Implementation Guide (STIG), Version 2, Release 2, December 26, 2008
- i) Defense ITIL Access Management Process Guide, Version 1.0, December 21, 2009
- j) USSTRATCOM Concept of Operations for Global Information Grid Enterprise, Active Directory, Revision 2.0, November 10, 2005
- k) USSTRATCOM JTF-GNO CTO 07-15 DoD PKI Implementation, Phase 2, Dec 11, 2007

Appendix C: Component AD Consolidation

C.1 Component AD Consolidation

Each of the four Military Services has plans or current initiatives to transform their AD environment to one characterized by far fewer AD forests, better support for transitioning users (e.g. garrison to deployed), better collaboration across forests, and the ability to share contact information across Service AD environments. There are also initiatives underway to look at the potential integration of Component identity and directory services (e.g. Air Force Directory Services) with the Enterprise Identity Synchronization Service and Enterprise Application Services Forest which will be hosted and managed by DISA. The extent of this integration, and whether it will eventually encompass all Services, COCOMs, and the DoD Fourth Estate, will be reflected in a future version of the ADORA.

This ADORA does not prescribe a “one size fits all” approach for AD consolidation. Each Service is afforded maximum flexibility to architect their end-state AD vision as they determine best supports their needs as long as those architectures comply with the minimally intrusive required rules and standards contained in this architecture. Key constraints imposed by this architecture on Service AD consolidations include the following:

- Mission critical applications must not be contained within forests that also contain end-user accounts or devices. (Ideally, user/account forests will not contain any functional applications but low value legacy applications might be appropriate at the discretion of the applicable DAA).
- User device and account forests may only be connected to a single LAF via external (forest-to-forest) AD trust and may not be connected via AD trusts to any EASF.
- Component legacy applications that are not IA-compliant or that require trusts with two or more other forests will remain within the Component AD environment until such a time as the application is made compliant (and able to move to the EASF or a LAF) or until the application is sunset.

C.2 AD Forest Type

The future DoD AD infrastructure will consist of a small number of DoD Enterprise and Component AD forests that are logically interconnected (see Exhibit 8) and together provide all DoD users with access to all Enterprise and Component-specific applications to which they are authorized. Exhibit 7 is a table that identifies the types of AD forests along with information on the rules for each forest type in terms of hosting, governance, applications, trusts, user accounts, and end-user devices.

C.3 Operational Concept Graphic

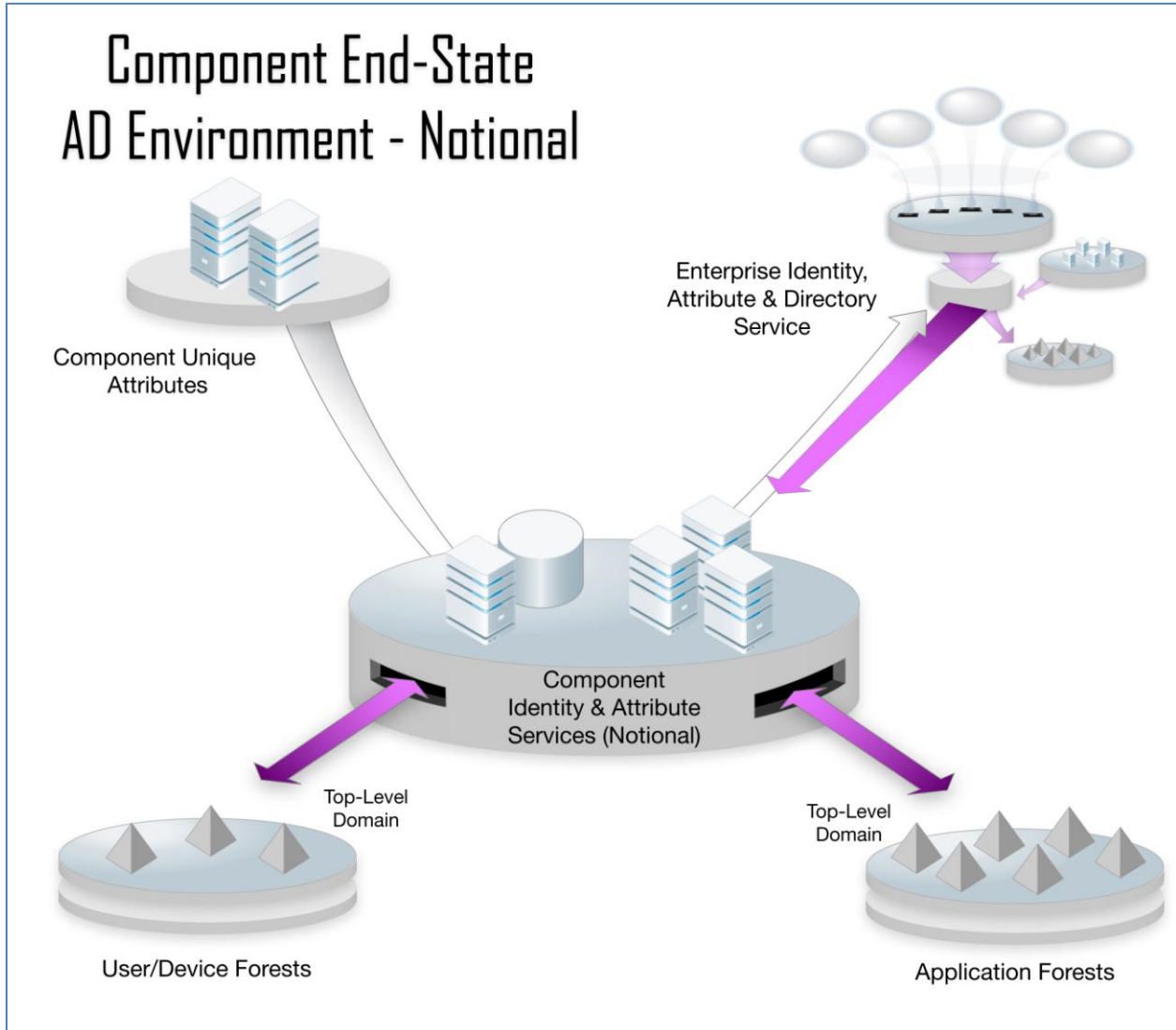


Exhibit 9. Notional Component AD Environment OV-1

Exhibit 9 exemplifies a notional future-state Service AD environment that aligns to the above requirements and realizes a significant consolidation of existing AD forests. This notional environment includes a single Component-managed user account forest (but does not preclude multiple user forests), a small number of Component-managed application forests, and a Component-level Identity & Attribute Service that would provide Component-unique personnel and IT attributes to the Enterprise Directory & Attribute Service. The combined Enterprise and Component attributes will be used as the basis for provisioning users within the Enterprise and Component AD environments. Users in the Component account forest would access applications in the EASF via approved, secure means such as Direct PKI or an approved standards-based (e.g. SAML or WS-*) implementation based on enterprise AD accounts in the EASF (i.e. the Component AD account is not used for user access of applications in the EASF).

C.4 COCOMs

This reference architecture assumes that COCOM user and resource forests are managed by one of the four Military Services or that COCOM users are provisioned within Service AD environments. It is understood and acknowledged that there may be some cases where a COCOM has a valid requirement for managing their own AD environment. Those situations will be addressed on a case-by-case basis.

C.5 Other DoD-managed Forests

This version of the reference architecture also applies to AD environments operated by or on behalf of DoD Agencies, Field Activities, OSD, and other DoD organizations not aligned to a Service executive agent. Unlike the AD environment within a Military Service, the collection of AD forests operated by or for these organizations are not centrally managed or resourced by any one organization. This makes any notion of consolidation or rationalization a more challenging endeavor. This version of the reference architecture does not address consolidation of these forests, but the core AD requirements specified in this architecture do apply to any future consolidation of these “other” forests.

Appendix D: Capability Viewpoint (CV-2)

D.1 Global User Logon Capability Taxonomy

Capability: Global User Logon (GUL)		
<p>Problem Statement: The existing DoD AD environment, consisting of multiple non-federated CC/S/A AD forests, does not support the ability of an authorized DoD user, using any authorized DoD end-user device, to quickly and easily log into an AD forest (the local network) that is not their home-station AD forest.</p> <p>GIG 2.0 Capability Gaps Addressed By GUL: GA_1, GA_2, GA_3, CP_2, CP_8, JI_1, JI_3</p>		
Desired End-State Capabilities		
Number	Capability Description	Comments
GUL 1	This capability will be provided for DoD NIPRNET users.	
GUL 1.1	A DoD user away from their home-station AD (a traveling user) will be able to assert their credentials and be provisioned into the local AD (network) as a DoD visitor once they are granted authorized access to a DoD facility and to an end-user device already connected to the wide area network at that facility.	
GUL 1.1.1	It will not be necessary for the DoD traveling user to have been previously provisioned into the visited AD by local system administrator action. This capability envisions an automated agent running on the AD platform that will identify the user as not being part of the local AD each time the user asserts their credentials, verify the user's credentials, and then provision the user as a "User" in the "Visitor User Group" (using a standardized group policy object that loads at execution).	
GUL 1.1.2	The delay between the time the user asserts their credentials and the time the user is granted access to the local network will be seconds; not hours, days or weeks.	
GUL 1.1.3	The DoD traveling user will not be granted all of the rights, privileges, and authorizations as would be provided to regularly assigned members of the visited local network. The automated agent will provide the traveling user with: (1) the ability to access Web-enabled resources to which they are authorized via a Web browser, and (2) the ability to print documents at the visited location.	
GUL 1.1.3.1	The automated agent should be configurable so that additional local access can be provided at the discretion of the visited organization.	
GUL 1.2	This capability extends GUL 1.1 to include the ability of the DoD traveling user to connect any authorized DoD end-user device to any local DoD network at a visited location and be provided the same capabilities as those in GUL 1.1.	

GUL 1.3	This capability extends GUL 1.1 and GUL 1.2 to include the ability of the DoD traveling user to connect wirelessly to any authorized DoD local network that is configured for wireless connection. This capability assumes the Global Logon solution and the local network conform to all security policies that may be in force regarding wireless networks.	
GUL 2	This capability will be provided for DoD SIPRNET users.	Future
GUL 3	This capability will be provided for Intelligence Community (IC) users.	Future
GUL 4	This capability will be provided for DoD and coalition partners using coalition networks.	Future
GUL 5	This capability will be provided for DoD and Federal partners using Federal networks.	Future

D.1.1 Related Initiatives Required To Provide Full Global Logon Functionality

The Global Logon process begins when a traveling user authenticates to a networked device at the visited location via DoD issued PKI certificates and hard tokens. This action triggers the provisioning of a highly restricted account that enables connection to the NIPRNET via a Web browser, access to locally installed office applications, non-persistent local storage⁵, and the ability to print to local printers. However, Global Logon *does not* address physical access to the device. The ability of the visiting user to be allowed access to the physical location of a networked end-user device within the visited facility is paramount to the success of Global Logon. Additionally, while Global Logon solutions may provide the visiting user with access to office automation applications and non-persistent storage, this reliance on the end-user device limits the ability for the user to access needed information from anywhere in the Enterprise. These two challenges are addressed through the Defense ITIL Access Management Process Guide and the implementation of the Shared DoD Enterprise Infrastructure, respectively, and briefly summarized here. Taken together, the access management standards and policy, the Global Logon solutions, and the Shared Enterprise Infrastructure with Web office applications will provide DoD users with the ability to access information and services needed to conduct DoD business from anywhere in the DoD Enterprise.

D.1.2 Defense ITIL Access Management

The *Defense ITIL Standard Process Guidance for Access Management* and related implementing issuance provides standard, DoD-wide guidance and policy on access to DoD IT resources by authorized DoD users. It will supersede the existing array of non-standard, local guidance adopted by individual installations or commands by establishing a standard set of compliance requirements that will be recognized as sufficient for access throughout the DoD. These requirements are:

⁵ Non-persistent storage implies that anything stored on local drives during the session will be deleted when the session is terminated (i.e. when the CAC is removed).

1. The user must complete the online DoD information assurance training and certification on an annual basis.
2. The user must complete the DD2875 System Authorization Access Request form.
3. The user must sign the standard User Agreement form.

The home station of the visiting user will substantiate the user's compliance with these requirements to the visited installation by including an appropriate endorsement on the user's travel orders. The visiting user will present their travel orders to the access control point of the visited installation and follow any local security requirements for the opportunity to insert their CAC into an available, networked device, without requiring intervention of a local system administrator. In the future, these standard access requirements may be developed as attributes associated with the user's CAC which will be checked automatically each time the user inserts their CAC, thus further streamlining the physical access process.

D.2 Sharing Contact Objects Across AD Forests Capability Taxonomy

Sharing Contact Information Across AD Forests (SCAF)		
Problem Statement: The existing DoD AD environment, consisting of multiple CC/S/A AD forests with their own separate directories of contacts and associated attributes, does not support the ability of an authorized DoD user provisioned in one AD forest to quickly and easily find contact information on users provisioned in any other AD forest.		
GIG 2.0 Capability Gaps Addressed By SCAF: GA_3, GA_5, CP_2, JI_4		
Desired End-State Capabilities		
Number	Capability Description	Comment
SCAF 1	A DoD user provisioned in one AD forest will be able to securely lookup contact information on DoD users provisioned in other AD forests.	
SCAF 1.1	Using the GAL in their client E-mail application.	
SCAF 1.2	Using the contacts feature of Web-based E-mail clients (e.g. OWA).	
SCAF 1.3	Using the contacts feature of any approved smartphone or other mobile device (e.g. Blackberry).	

D.3 Sharing AD-dependent Applications Across AD Forests Capability Taxonomy

AD Dependent Application Sharing (ADAS)		
Problem Statement: The existing DoD AD environment, consisting of multiple CC/S/A AD forests each containing AD-dependent resources and applications, does not support the ability of an authorized DoD user provisioned in one AD forest to easily and securely access needed AD-dependent applications located in other AD forests. This often results in the non-availability of needed information or the inefficient re-hosting and replication of the same information in multiple AD forests.		
GIG 2.0 Capability Gaps Addressed By ADAS: CP_2, CP_3, CP_7, CP_8, CP_9, JI_1, JI_3, JI_4, JI_5		

Desired End-State Capabilities		
Number	Capability Description	Comment
ADAS 1	DoD users will be able to find and securely access needed AD-dependent applications in any DoD AD environment in which they are authorized.	
ADAS 2	Applications and services that are used by or benefit two or more components will be logically managed as DoD Enterprise assets within the Enterprise Infrastructure for Shared AD-dependent Applications.	
ADAS 3	The ADAS capability must include processes to manage license usage and associated cost recovery across CC/S/A forests.	

D.4 Enterprise Infrastructure for Shared AD-dependent Applications and Services Capability Taxonomy

Enterprise Infrastructure for Shared AD-dependent Applications & Services (EISA)		
<p>Problem Statement: (1) The existing DoD AD environment consists of multiple, component-managed AD forests housing many thousands of applications and services. In many cases these applications and services are duplicated across many component forests owing to the fact that current technology and DoD IA policy limit secure and seamless sharing across forests. No central, enterprise-wide capability exists to allow applications and services to be shared by multiple component organizations.</p> <p>(2) The current DoD IT infrastructure relies on office productivity solutions (word processors, spreadsheets, etc) that are typically accessed as client-based applications loaded on end-user devices (typically desktop and laptop/notebook PCs). This arrangement unnecessarily limits the productivity of users with small, mobile, Web-enabled devices or users that only have access to a Web browser on a connected end-user device (such as DoD traveling users using the DoD Visitor solution).</p> <p>GIG 2.0 Capability Gaps Addressed By EISA: CP_3, CP_7, CP_8, CP_11, JI_1, JI_3, JI_4, JI_5</p>		
Desired End-State Capabilities		
Number	Capability Description	Comment
EISA 1	A logical, DoD Enterprise-managed infrastructure for common, shared applications that can be accessed securely via Web technology by all DoD users.	
EISA 2	A DoD user will be able to securely access shared, enterprise, Web-based office automation solutions to which they are authorized. The user will be able to create, edit, and store files within this enterprise shared environment.	

D.4.1 Enterprise Infrastructure for Shared AD-dependent Applications and Services Operational Concept (OV-1)

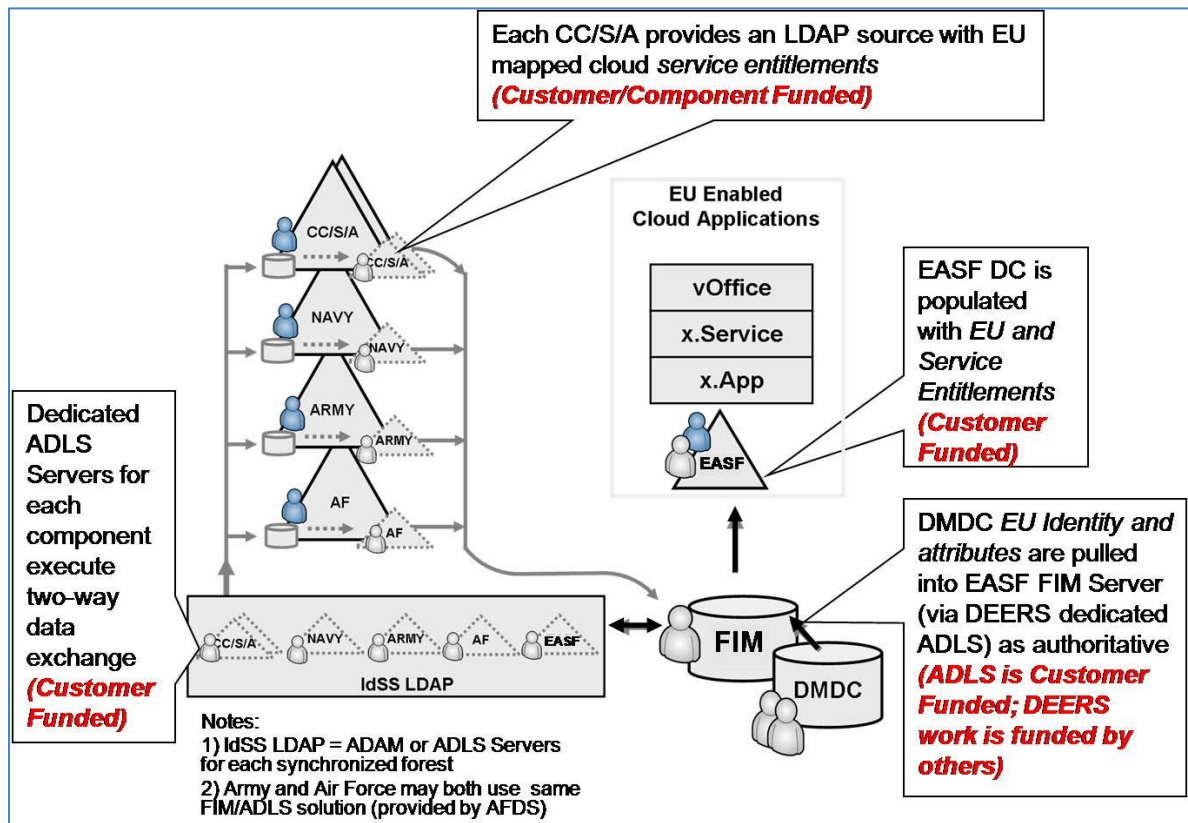


Exhibit 10. Notional IdSS/EASF OV-1

The notional enterprise infrastructure for AD-dependent applications is shown in Exhibit 10. It depicts an Enterprise Application Services Forest (EASF) populated with all DoD users and their associated attributes. The EASF provides access for all DoD users to DoD Enterprise applications that may include such offerings as Virtual Office (Web-based office automation applications) and Enterprise E-mail. Also depicted is the notion of an Enterprise Attribute Service populated through authoritative personnel and human resource data from DEERS and other sources. The Forefront Identity Manager (FIM) server is one particular technology for synchronizing identity information among Service and Enterprise identity repositories. This Enterprise level synchronization also provides the ability for DoD users in any CC/S/A forest to view contact information on users in any other CC/S/A forest.