Department of Defense

Enterprise-wide Access to Network and Collaboration Services (EANCS)

Reference Architecture

Version 1.0

December 2009

Prepared by the Office of the DoD CIO

FOREWORD

Recently, the Vice Chairman of the Joint Chiefs of Staff (VCJCS) made a statement that established the requirement for the Enterprise-wide Access to Network and Collaboration Services Reference Architecture (EANCS RA). The VCJCS said he wants the ability to "go anywhere in the DoD, login, and be productive." This statement echoes the Department's Net-Centric vision and emphasizes a key characteristic of the *Global Information Grid (GIG) 2.0 Concept of Operations (CONOPS).* The key characteristic: Global Authentication, Access Control and Directory Services, ensures any authorized user can access the global network infrastructure from any location with common and portable identity credentials which enable visibility of, and access to, all warfighting, business support, or intelligence related information, services and applications related to their mission and COI. This characteristic includes single sign–on and anytime/anywhere access to the network, IT/NSS services, and the entire DoD Global Address List.

The EANCS RA supports one of several ongoing efforts aimed towards achieving this characteristic. This RA focuses on that portion of the characteristic dealing with global authentication, authorization and access control to globally accessible resources. It is intended to guide the development of solution architectures and support the development of specific implementation guidance for achieving this capability. The Department of Defense (DoD) must move forward in implementing incremental solutions to realize the Net-Centric vision as described in the DoD Information Enterprise Architecture (DoD IEA) and fulfill the *GIG 2.0 CONOPS*. The EANCS RA is aligned with the DoD IEA and reflects the DoD's recognition that global authentication and access control will result in an enhancement of secure information sharing capabilities for all DoD operations, thereby increasing operational effectiveness.

1 Introduction

The Enterprise-wide Access to Network and Collaboration Services (EANCS) Reference Architecture (RA) supports development of EANCS implementation guidance and solution architecture. This effort, in combination with the Active Directory and Enterprise User efforts, has an objective of providing the means for global authentication, access control and directory services. The motivation for these efforts is the VCJCS statement "I want to go anywhere in the DoD, login, and be productive." The EANCS RA, with respect to this stated requirement, focuses on network login, global authentication, and authorization and access control enabling use of designated enterprise services.

1.1 Overview

Reference Architecture abstracts and normalizes the institutional understanding of capabilities at the enterprise level, and provides a common set of principles/rules, process patterns, and technical positions for use within the DoD to guide development of Enterprise, Segment, or Solution architectures.

The purpose of the EANCS RA is to describe the capability to access collaboration services in support of secure information sharing across the Department. It provides architectural patterns to guide, standardize, and enable the most rapid and cost-effective implementation of global authentication, authorization and access control capabilities. It uses the following DoD Architecture Framework (DoDAF) views and models to describe the required capabilities:

- AV-1 Overview & Summary Document - Describes the EANCS purpose, scope, and context.
- AV-2 Integrated Dictionary - Defines the EANCS activities, process steps, swim lanes, and information elements.
- OV-1 High-Level Operational Concept Graphic - Graphically and textually describes the EANCS concept for global authentication, authorization, and access control from a consumer and service provider perspective.
- OV-5a Operational Activity Decomposition Tree - Organizes the EANCS activities for providing global authentication and authorization and access control in a hierarchal structure.
- OV-6a Operational Rules Model - Identifies business rules that constrain global authentication and authorization and access control to enable access to enterprise services.
- OV-6c Event-Trace Description - Describes the EANCS activities as a sequence of events (process pattern) that must be accomplished to provide global authentication and authorization and access control capabilities in a net-centric DoD Information Enterprise (IE).

- StdV-1 Standards Profile - Lists the known high level policies and standards that must be applied to solutions developed to enable global authentication and authorization and access control as envisioned in the EANCS OV-1.

1.2 Scope

The EANCS RA is a "to-be" architectural description of an objective capability and requirements. It describes the objective requirements, rules, patterns, and standards for authentication and authorization and access control that apply throughout DoD. These descriptions can then be applied to selected use cases to develop authentication and authorization implementation guidance based on a specific set of conditions.

The scope of this RA is limited to:

- Approved DoD Networks
- Authentication of designated users with portable identity credentials
- Access to designated, globally accessible enterprise services via end user devices that are hardwired (not wirelessly connected) to a network
- Control of access to designated enterprise services based on user attributes.

This RA provides guidance for Authentication to approved DoD networks using portable identity credentials and Authorization and Access Control to enterprise services as part of a broader, overarching DoD Enterprise Services Security Foundation (ESSF).

The DoD IEA defines three different perspectives with respect to interactions in the DoD IE. The three perspectives are:

- Production/provision of data and services (i.e., the architecture describes how data and services are developed and provided to users)
- Management/operation of data and services (i.e., the architecture describes how data and services are managed or controlled)
- Consumption/use of data and services (i.e., the architecture describes how data and services are used)

The perspectives described in this RA are that of a Service Provider (Production/Provision) and a User/Consumer (Consumption/Use).

1.3 Key Authoritative Sources

The content of this RA was extracted or derived primarily from five authoritative sources:

- Enterprise Security Management (ESM) Documents (Draft) - Describe the functions associated with ESM. These functions provide dynamic management and control of IA services, processes, and devices to optimize the enterprise for mission operations. The EANCS RA focuses on the ESM authentication and privilege management functions.
- Global Information Grid (GIG) 2.0 Operational Reference Architecture (ORA) - Provides a functional decomposition of the activities associated with

the GIG 2.0 attributes. The EANCS RA focuses on the authentication and authorization activities within the GIG 2.0 ORA "Global Authentication, Access Control and Directory Services" attribute.

- Enterprise Services Security Foundation (ESSF) Implementation Roadmap (Draft) - The unifying construct for aligning security-related efforts to enable the delivery of DoD Enterprise Service (ES) capabilities. Provides a taxonomy and description for the security services. The EANCS RA focuses on the ESSF Authentication and Authorization & Access Control services.
- Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance (Draft) - Outlines a common framework for ICAM within the Federal Government and provides supporting implementation guidance for program managers, leadership, and other stakeholders as they plan and execute segment architecture for ICAM management programs. The EANCS RA focuses on the FICAM "Grant Logical Access" use case, standards, and guidance.
- DoD Information Enterprise Architecture (IEA) v1.1 - Highlights the key principles, rules, constraints and best practices to enable agile, collaborative net-centric operations. The EANCS RA focuses on the principles and rules for the DoD IEA Secured Availability (SA) and Data & Services Deployment (DSD) priority areas.

2 Context

Development of this RA is guided by the key authoritative sources and the Department's Net-centric vision, as described in the DoD IEA, to function as one unified DoD Enterprise, creating an information advantage for DoD and mission partners.

2.1 Guiding Principles

Selected principles and rules from the key authoritative sources were used to provide context and guide the development of this RA. **Table 1**, Guiding Principles and Rules, lists and describes the selected principles and rules.

Table 1 - Guiding Principles and Rules

#	Principle/Rule	Description	Source Document
Guiding Principles and Rules (Source Documents)			
1	GIG Resources Visibility, Accessibility, and Understandability	Data assets, services, and applications on the GIG shall be visible, accessible, understandable, and trusted to authorized (including unanticipated) users.	DoD IEA v1.1, Global Principles, pg. 5
2	Data and Services Accessibility	Authoritative data assets, services, and applications shall be accessible to all	DoD IEA v1.1, Data and Services

		authorized users in the Department of Defense, and accessible except where limited by law, policy, security classification, or operational necessity.	Deployment (Business Rule), pg. 11
3	Seamless Defense Information Enterprise	Global missions and globally dispersed users require global network reach. Information Assurance mechanisms and processes must be designed, implemented, and operated so as to enable a seamless Defense Information Enterprise.	DoD IEA v1.1, Secured Availability Principles, pg. 15
4	Digital Authentication and Access Enforcement	All DoD information services and applications must uniquely and persistently digitally identify and authenticate users and devices. These services, applications, and networks shall enforce authorized access to information and other services or devices according to specified access control rules and quality of protection requirements for all individuals, organizations, COIs, automated services, and devices.	DoD IEA v1.1, Secured Availability Rule, pg. 15
5	Access Management	Manage and control how individuals are granted access to resources by leveraging identities and credentials, during authentication, to obtain a level of assurance in the identity of the individual attempting to access resources.	FICAM, Access Management, pg. 13
6	Global Authentication and Access Control	Provide secure, adaptive, and rapid access across trusted and authenticated domains to all authorized entities requesting interaction with GIG resources from any location, at any time with common and portable identity attributes.	GIG 2.0 ORA, pg. 24
7	Universal Credentials	All authorized entities have one identity and universal credentials are recognized by all producers of information and service.	GIG 2.0 ORA, Operational Outcome (Principle), pg. 24

8	Credential Management	GIG entities will request access to GIG information, services, and communications resources by asserting a claimed identity and all the inherent rights and privileges associated with that identity. Credential management shall provide the critical process for identifying and authenticating entities to confirm that they are who they claim to be and relies upon a trusted attestation of the identity – in the form of a credential.	ESM, pg. 9
9	Attribute Management	Provide for the publication of entity attributes, to the enterprise, (for use by GIG people, devices, and services) that can impact the accesses or privileges an entity can have in the system.	ESM, pg. 11
10	Authentication	Authentication (used here to refer to electronic identity authentication - Entity Authentication/Data Origin) shall provide a process of establishing confidence in user identities presented to an information system, or confidence in the source and integrity of data within the system.	ESM, pg. 12
11	Privilege Management	Provide processes involved in enforcing the permission for an entity to perform some action against some resource, by shifting the focus of access/authorization, from purely who needs access (by name or organization) to why access is needed (e.g., the user is a U.S. citizen with a Top Secret clearance)	ESM, pg. 14-15
12	Policy Management	Provide the set of standardized and automated activities required to define, generate, deconflict, and translate digital policy throughout the GIG enterprise.	ESM, pg. 16
13	Manage Digital IA	Remotely manage and control IA	Net Centric IA

	Policy	attributes in all communications devices, computing resources, and services; Includes the protection of management and control (e.g., signaling, routing) of information flowing between communications devices, computing resources, and services to support policy enforcement, user and device authentication, end-to-end connectivity, quality of service (QoS), and prioritization.	Strategy, pg. 23

The principles and rules described in Table 1 are used to guide the development of the OV-1 high-level operational concept graphic, the OV-5a activity decomposition, and the OV-6c process pattern. These guiding principles and rules will also influence implementation guidance and solution architecture development.

2.2 Constraints and Assumptions

Constraints and assumptions that have a potential impact on the development and use of authentication and authorization and access control capabilities are identified to properly constrain and bound the development of the EANCS RA. These constraints and assumptions also assist the reader in understanding certain descriptions in the RA.

2.2.1 Constraints

a. This version of the RA focuses only on the requirements for network login, authenticating, and checking the authorization of end users so they can gain access to designated, globally accessible enterprise services, to include enterprise e-mail and portals. This RA specifically addresses logical access by persons. It does not address authentication of non-persons (e.g., devices, services) or authorization itself (e.g., authorization policy management, attribute management), nor does it address physical access. It does address the requirements for access to shared information resources such as information contained in an access-controlled repository.

b. This RA only addresses access from a “DoD network user environment"[1] for designated DoD users, such as active duty military and Selected Reserves, civilian employees and designated contractors and other designated, non-DoD, federal employees on approved DoD networks, such as the Non-Classified Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet). It does not address access by state and local government personnel, retired military personnel, military dependents, commercial businesses, nor Allies

[1] DoD network user environment is where the identity credential is presented to an asset owned by the DoD, which is physically connected to a DoD network.

or coalition partners, unless they have been granted an approved DoD portable identity credential.

c. This RA describes the principles, rules, patterns, and standards required for authentication and authorization for accessing designated enterprise services and the network.

d. This RA abstractly models, using architectural artifacts specified in the DoDAF, those identified core processes associated with authentication and authorization to designated networks and enterprise services.

e. Terminology, concepts, and components for this reference architecture follow those established in the Enterprise Security Management (ESM) Context Overview, as aligned with the Enterprise Services Security Foundation (ESSF) Implementation Roadmap, Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, DoD IE Architecture (IEA), Global Information Grid (GIG) 2.0 Operational Reference Architecture, Information Assurance (IA) Component of the GIG Integrated Architecture, and the Identity Management Strategic Plan.

2.2.2 Assumptions

a. The aspects of authorization excluded in the constraints may be addressed in future DoD RA efforts.

b. All supporting applications, services, processes, and infrastructure will be developed and/or available to fully enable the capabilities specified herein. The capabilities described in this RA are authentication and authorization and access control to globally accessible enterprise services and the network. These capabilities are dependent on functions external to this RA, to include digital identity management, credential management, cryptography management, policy management, and auditing and reporting.

c. Portable identity credentials, such as the Common Access Card (CAC) or other DoD smartcards or hard tokens with PKI certificates, will be used to support user authentication.

d. This RA assumes that required authorization attributes for attribute based access control to designated enterprise services have already been defined, collected, regularly updated, and made available through standard interfaces from reliable attribute sources.

2.3 Alignment with Joint Capability Areas (JCAs) and DoD IEA Priority Areas

To meet net-centric needs, the DoD IEA requires a DoD architecture's context to address the JCA structure, providing the architect with the net-centric capabilities the architecture must describe. The JCAs are collections of like DoD capabilities functionally grouped to support capability analysis, strategy development, investment decision making, capability

portfolio management, and capabilities-based force development and operational planning. The architect uses the common capability language of selected net-centric JCAs to describe capabilities in the architecture so they enable net-centric operations.

In addition, the DoD IEA requires each DoD architecture to conform with the DoD Net-Centric Vision. This conformance is achieved by addressing how the architecture will meet the challenges to this Vision described by DoD IEA priority areas. The following paragraphs describe EANCS RA alignment with key net-centric JCAs and appropriate Rules associated with the DoD IEA priority areas of Secured Availability (SA) and Data and Services Deployment (DSD).

Authentication and authorization and access control, as described in this RA, are key elements of the User Access JCA within the Net-Centric/Enterprise Services (ES)/Core Enterprise Services JCA hierarchy. The User Access JCA defines "the ability to access user defined DoD Enterprise Services through a secure single entry point." Authentication and authorization and access control make such an access point secure by providing functionality meeting requirements of the SA priority area. By limiting access to enterprise services, authentication and authorization and access control will enable the User Access JCA to provide users with SA-required trust and confidence. This trust and confidence will ensure:

- The integrity of critical information is being maintained
- Enterprise services will be there when needed and will remain under DoD control
- Adversaries will not be able to compromise and exploit these same services

In a net-centric DoD IE, there is a need to counter the increased threat to services and their related data resulting from greater interconnectivity and interdependency. Authentication and authorization and access control, as critical "gate-keepers" to enterprise services, are essential to meeting this SA challenge. To be effective, these functions must be implemented to provide mechanisms complying with SA Rule (SAR) 07 by providing the ability to:

- Uniquely and persistently digitally identify and authenticate users and
- Enforce authorized access to information and other services or devices according to specified access control rules.

Authentication and authorization and access control indirectly support capabilities integral to the Protect Data and Networks JCA in the Net-Centric/Information Assurance JCA hierarchy. Authentication and authorization and access control provide the means to limit access to local networks and capabilities, as well as enterprise services. This in turn provides a critical enabler for the Tier 4 JCAs of Protect Against Network Infiltration, Protect Against Denial or Degradation of Services, and Protect Against Disclosure or Modification of Data.

In order to be effective in the net-centric DoD IE, authentication and authorization and access control must also be implemented to meet requirements specified by the DSD priority area. Solutions delivering these functions should be made available as services in the net-centric environment. Such services must be widely available, easily discoverable,

usable, and trusted across the DoD IE. Data produced by authentication and authorization and access control must also be made visible and accessible in accordance with DSD specifications. Data visibility and accessibility is critical to enabling monitoring and auditing of authentication and authorization transactions to prevent and respond to incidents threatening DoD IE operations. The services delivering authentication and authorization and access control and the data produced by these services must conform to DSD Rule (DSDR) 01.

3 Service Capability Description

The service capabilities described in the EANCS RA are authentication and authorization and access control. **Figure 1**, OV-1 Concept Diagram (Consumer Perspective), depicts a DoD User perspective of these capabilities.

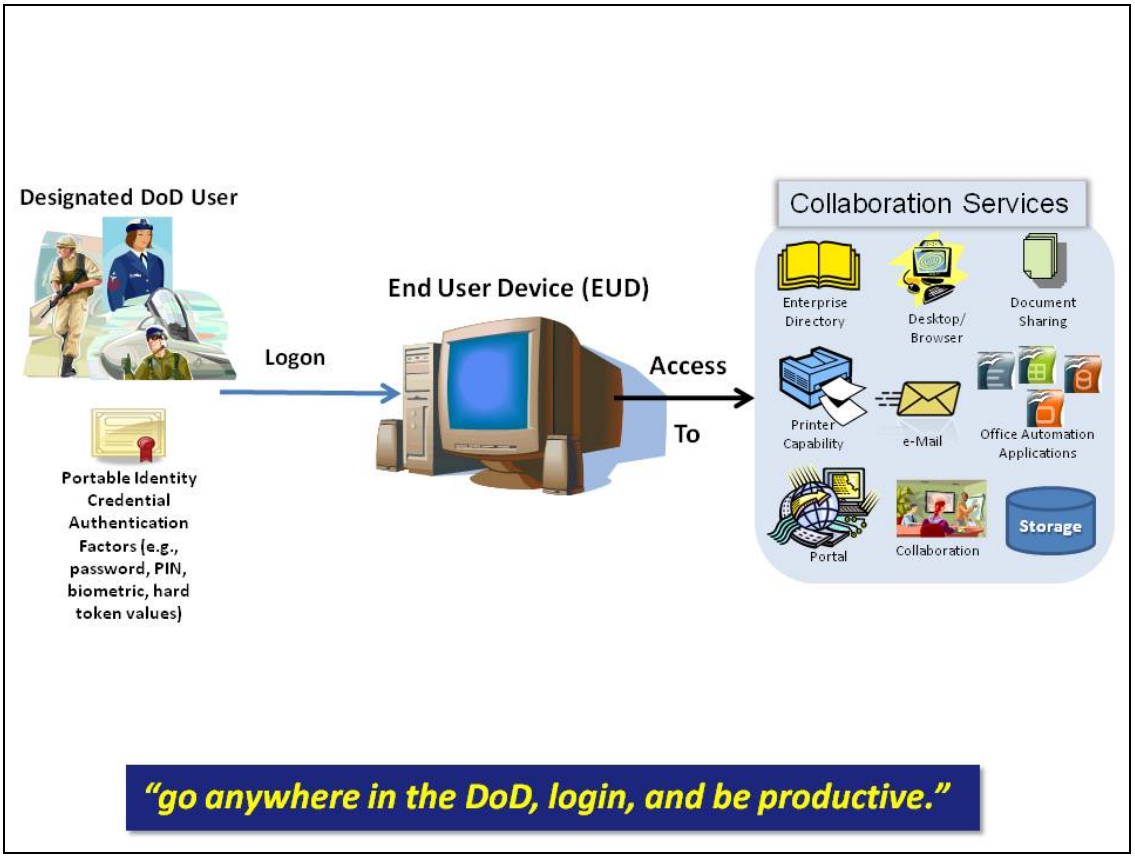


Figure 1: OV-1 Concept Diagram (Consumer Perspective)

Figure 1 diagrams an operational capability requirement that is described in the GIG 2.0 ORA as, *any designated user can access global network infrastructure from any location within DoD using common, portable identity credentials which enable visibility of, and access to, designated warfighting, business support, and/or intelligence information, services, and applications.* The user perspective describes the operational capability required to be productive, but it does not describe the underlying functional capabilities

that must be provided. **Figure 2**, OV-1 Concept Diagram (Service Provider Perspective), depicts the concept of the functional capabilities and interactions required to provide a user access to enterprise services. This is a service provider perspective.

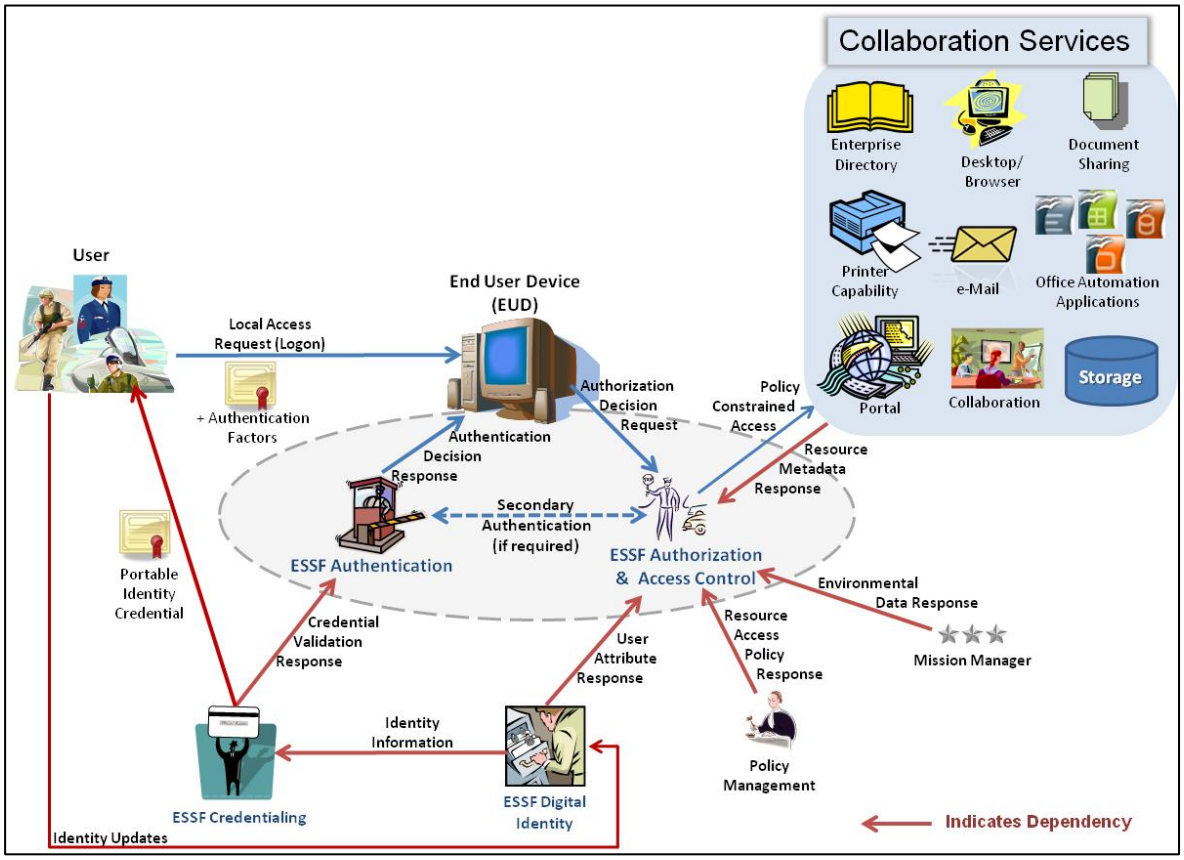


Figure 2: OV-1 Concept Diagram (Service Provider Perspective)

The functional capabilities and interactions required are network login and access to designated enterprise services through service provider supplied authentication and attribute based access control. A user must be authenticated to the network before gaining access to a designated enterprise service. Authorized access to some resources (e.g., printer, browser) may only require that the requesting user be properly authenticated, while access to other services may require evaluation of additional user attributes. The authentication decision is based on confirmation of the user's claimed identity and a validation of the user's portable identity credential. An authenticated user may request and gain access to a designated enterprise service with a favorable authorization decision. Access control decisions are governed by resource access policy and based on resource metadata, user attributes, and environmental data (mission attributes), as applicable. Authorization policies will vary among enterprise services. The authorization and access control function may require re-authentication of the user.

The authentication and authorization and access control functional capabilities are highly dependent on several external functions to include credentialing, digital identity, policy management, and privilege management. In addition, Authentication and Authorization & Access Control will make use of mandated DoD Enterprise Services, as defined in the

DoD IEA, absent a compelling operational need or documented business case. These services are vetted, common, globally accessible services that the DoD CIO has mandated for use in a net-centric environment. Current mandated DoD Enterprise Services are: Collaboration Services, Content Discovery Services, Content Delivery Services, Geospatial Visualization Service, and DoD Enterprise Directory Service.

3.1 Authentication

Authentication is the process of establishing confidence in an entity's identity that is electronically presented to an information system. This process includes:

- validation of the credential,
- proof of the claimed identity binding,
- determination of authentication assurance level (includes multiple factors), and
- determination of an authentication decision and making that decision available to other processes for their use in establishing access.

In Figure 2, the authentication functional capability verifies a user's claimed (or assumed) identity, providing a basis for access to an End User Device (EUD), network, and associated authentication-based capabilities. This function fulfills the DoD IEA requirement to "uniquely and persistently digitally identify and authenticate users" (SAR 07).

3.2 Authorization & Access Control

Authorization is the process of establishing policy for who should have access to information processing services and provisioning the rules and attributes used to control access to those services. Access control is the logical process of granting or denying specific requests for obtaining and using information processing services based on established policy rules and associated user attributes.

In Figure 2, the authorization & access control functional capability grants or denies requests for an authenticated user to access and use designated enterprise services based on digital policy. This meets the DoD IEA requirement to "enforce authorized access to information and other services or devices according to specified access control rules" (SAR 07).

3.3 Activity Decomposition

The Authentication, Authorization, and Access Control functional capabilities decompose into a specific set of activities. The activity decomposition describes the capabilities in terms of the activities required to provide the capabilities. **Figure 3**, OV-5a EANCS RA Activity Decomposition, is the activity decomposition for the EANCS RA. The **A0-Enable Enterprise-wide access to Network and Collaboration Services** activity "provides the capability for any designated user to access global network infrastructure from any location with common and portable identity credentials which enable authentication and authorization to (i.e., visibility of, and access to) designated enterprise

services." It decomposes into two activities, **A1-Provide Authentication** and **A2-Provide Authorization and Access Control**. The definitions and first level decomposition for the A1 and A2 activities are:

- **A1-Provide Authentication** - This activity provides authentication mechanisms, validates the authenticity of credentials, and verifies identities to establish non-repudiation and control information dissemination.
    - **A1.1-Authenticate Entity (User)** - Verifies that an entity ("claimant") communicating with a verifier has the claimed or assumed identity. Entity authentication may be unilateral, where one party verifies the other, or mutual, where both parties are verified. Entity authentication requires an authentication context (a session, conversation, or association) to ensure that data from one context cannot be successfully replayed in a different context. Validates the entity credential by querying Credential Management.

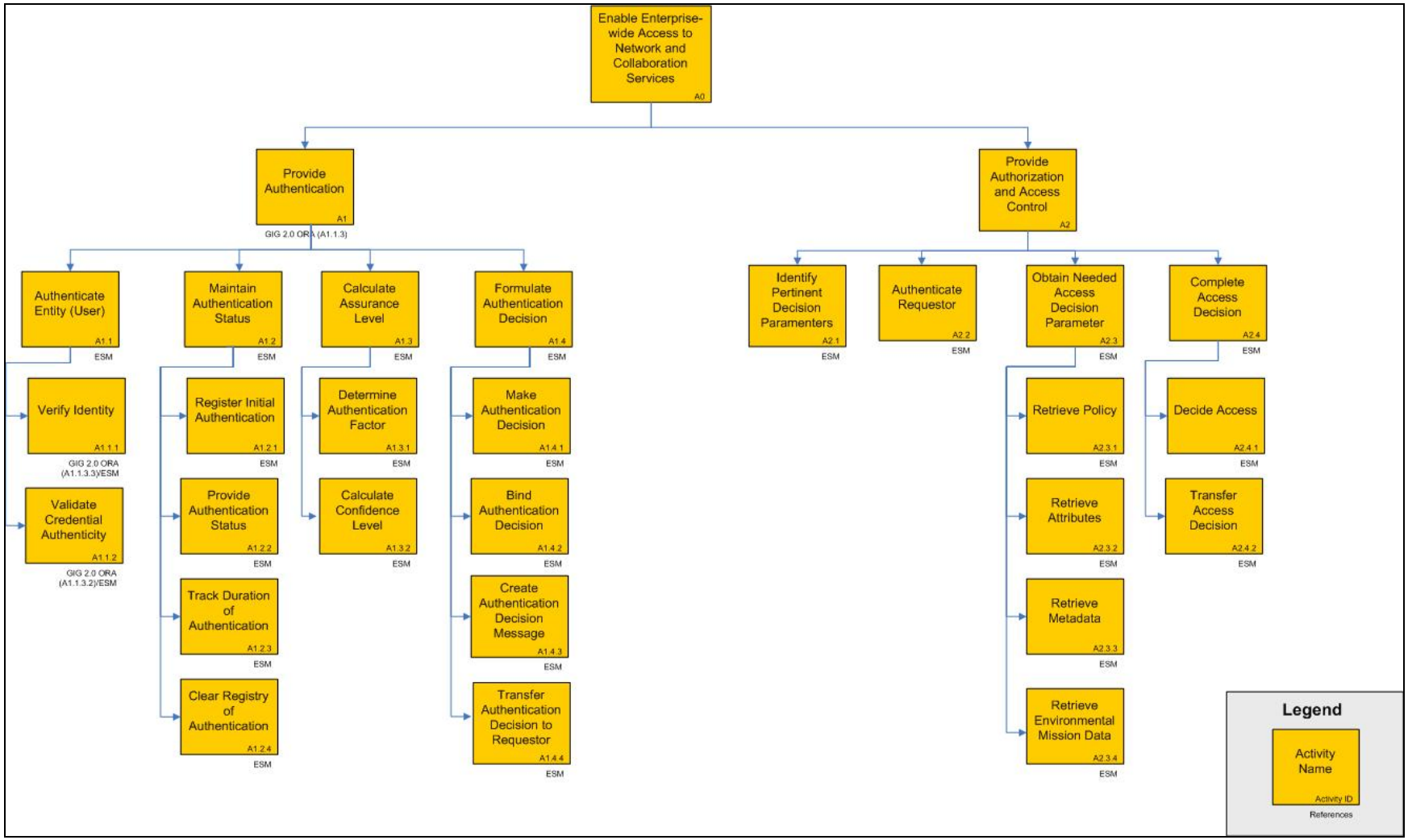


Figure 3: EANCS RA Activity Decomposition

- **A1.2-Maintain Authentication Status** - This activity provides to requestors the identity of entities that currently have validated proof of identity. Note: this function supports "single sign-on" and reduced sign-on.
- **A1.3-Calculate Assurance Level** - This activity calculates authentication assurance level, namely, Confidence Level (CL).
- **A1.4-Formulate Authentication Decision** - This activity creates an authentication decision response message in accordance with established authentication policy.

- **A2-Provide Authorization and Access Control** - This activity controls access to information, services, and applications based on predefined attributes and rules.
  - **A2.1-Identify Pertinent Decision Parameters** - This activity parses the Access Request to determine the requestor, requested resource, and requested action.
  - **A2.2-Authenticate Requestor** - This activity verifies that the requestor has the claimed or assumed identity using the Authenticate Function.
  - **A2.3-Obtain Needed Access Decision Parameter** - This activity retrieves parameter values to enable an access decision.
  - **A2.4-Complete Access Decision** - This activity creates an access decision using the resource access control policy to evaluate the retrieved parameter values.

Definitions for all activities in the EANCS RA activity decomposition are in the AV-2 Integrated Dictionary at Annex B. The OV-5a Activity Decomposition and OV-1 Concept Diagram provide a basis to establish EANCS principles/rules and process patterns.

4 Principles/Rules and Process Pattern(s)

Earlier we described a set of Guiding Principles, extracted from key source documents that provided context and guided the development of the EANCS RA. The description of activities in the OV-5 Activity Decomposition allows us to establish principles and rules associated with performing the activities. Once we identify relevant principles and rules, we apply them in the development of process patterns for authentication and authorization and access control.

4.1 EANCS RA Principles and Rules

The EANCS RA principles/rules provide guidance on how to apply the activities in a process pattern. They are based on understanding the activities, how they relate to each other, and the role they play in providing the capabilities. **Table 2**, OV-6a EANCS Principles and Rules, lists and describes the EANCS principles and rules.

Table 2: OV-6a EANCS RA Principles and Rules

EANCS RA Principles and Rules		
#	**Principle/Rule**	**Description**
1	Portable Identity Credentials	All Users must have a portable identity credential for authentication.
2	Authentication Based Access	User authentication is required to access a designated set of basic capabilities.
3	Common Set of Functions	All instances of authentication, authorization, and access control shall utilize the same set of designated functions described by the Enterprise Services Security Foundation (ESSF).
4	Points of Access	Some form of authentication and authorization occurs at every point of access.
5	Key Dependencies	Authentication, authorization, and access control are highly dependent on information elements provided by five key functions: identity management, credential management, policy management, privilege management, and attributes management.

The five principles and rules described in Table 2 are applicable to all enterprise, segment and solution architectures describing authentication and authorization and access control. They were applied in developing the process patterns for authentication and authorization and access control.

4.2 Process Pattern (s)

The process pattern for authentication and the process pattern for authorization and access control are closely related. Authentication is a pre-requisite for authorization and access control. As such, an overarching process pattern depicting the relationship between the two is provided in **Figure 4**, OV-6c Combined Process Pattern. This process pattern presents a best practice for achieving DoD IEA SA Rule 07 (Digital Authentication and Access Enforcement), as described in Table 1.

4.2.1 Combined Process Pattern

The combined process pattern in Figure 4 describes the common set of process steps required to provide authentication and authorization and access control capabilities. The pattern incorporates activities from the OV-5a activity decomposition, groups them as process steps, and indicates where they are performed. This is a logical pattern that is applicable to all implementations and solutions for authentication and authorization and access control. A follow on effort will develop a set of use cases with specific implementation conditions, apply the process pattern to these use cases, analyze the use cases, and identify gaps/issues specific to the use cases.

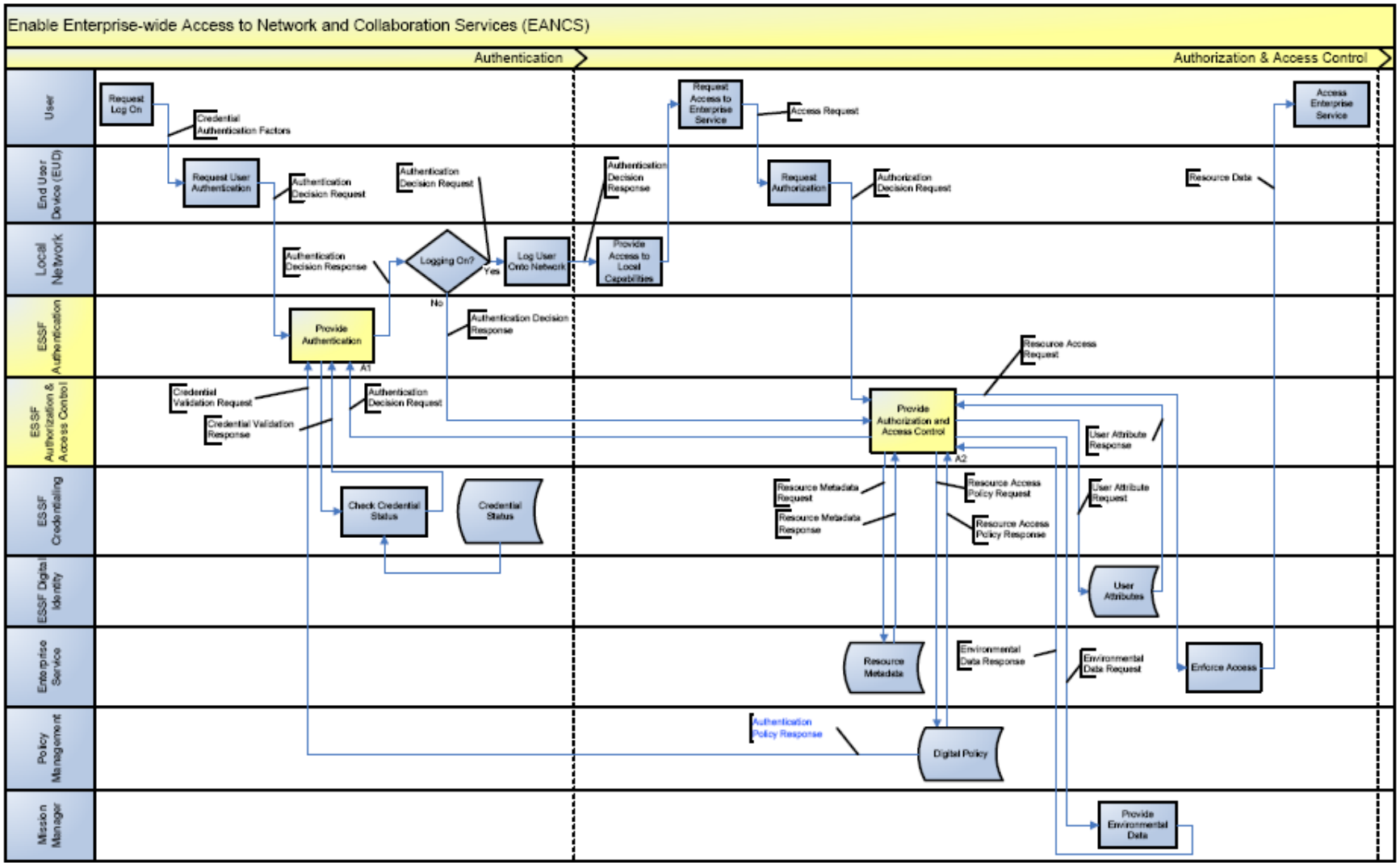


Figure 4: OV-6c Combined Process Pattern

The authentication and authorization process patterns will be discussed separately. The purpose for this combined process pattern is to describe interactions between the authentication process and the authorization process. In Figure 4, the authentication process steps are performed in the ESSF Authentication swim lane and the authorization process steps are performed in the ESSF Authorization & Access Control swim lane. There are two direct interactions between the authentication and authorization processes.

The first interaction is an authentication decision request that is an output from the authorization process and an input to the authentication process. The authentication decision request is a message asking to confirm or verify the identity of a user prior to granting that user access to an enterprise service. The message will include user credential information to include private information needed to confirm credential ownership unlocked using the authentication factors entered by the user. This interaction occurs anytime the authorization process requires verification of the identity of a user (i.e., re-authentication).

The second interaction is an authentication decision response that is an output from the authentication process and an input to the authorization process. The authentication decision response is a message either confirming or denying a user's identity, as represented by the presented credential. The content of this message determines if the user can be granted access to designated capabilities. This interaction occurs in response to the authentication decision request from the authorization process when the user needs to be re-authenticated.

4.2.2 Authentication Process Pattern

The OV-6c Authentication process pattern in **Figure 5** describes the process steps involved in the authentication process. The Provide Authentication process step incorporates activities from the Provide Authentication activity in the OV-5a activity decomposition as indicated below each process step. The Provide Authentication process step uses authentication mechanisms to validate the authenticity of credentials and verify the identity of a user.

DoD IEA activity A2.8.4 Oversee Authentication Processes and its sole child activity A2.8.4.1 Manage Authentication Processes enable and constrain the Authentication process described here. As described in DoD IEA v1.1, SA authorities will use the Oversee Authentication Processes activity to “ensure the DoD transition to two-factor authentication mechanisms” and to enhance “interoperability among service and agency authentication systems.” This DoD IEA activity, then, governs the development of specific requirements for authentication mechanisms performing the process depicted here, in order to advance to two-factor authentication. In doing so, it will constrain exactly how the Authentication process pattern described here is to be carried out. SA authorities will further “identify, test, and certify” any authentication mechanisms developed and used to perform this process pattern in accordance with the DoD IEA Manage Authentication Processes activity (A2.8.4.1) to ensure they meet these specific requirements.

The authentication process begins with receipt of an authentication decision request from the Request User Authentication process step in the EUD swim lane or, in the case of a

need to re-authenticate a user prior to determining access, from the Authenticate Requestor process step in the Authorization & Access Control swim lane. The authentication decision request is a message asking to confirm or verify the identity of a user prior to granting that user access to a network and local capabilities and eventually to enterprise services. The message includes information needed to verify the credential and confirm credential ownership.

Credential information is provided to the Validate Credential Authenticity process step to determine if a presented credential is valid and meets all security requirements based on the operating environment. This step interacts with an external process step, Check Credential Status, to check the issue date and validity period of a credential and whether the credential has been revoked.

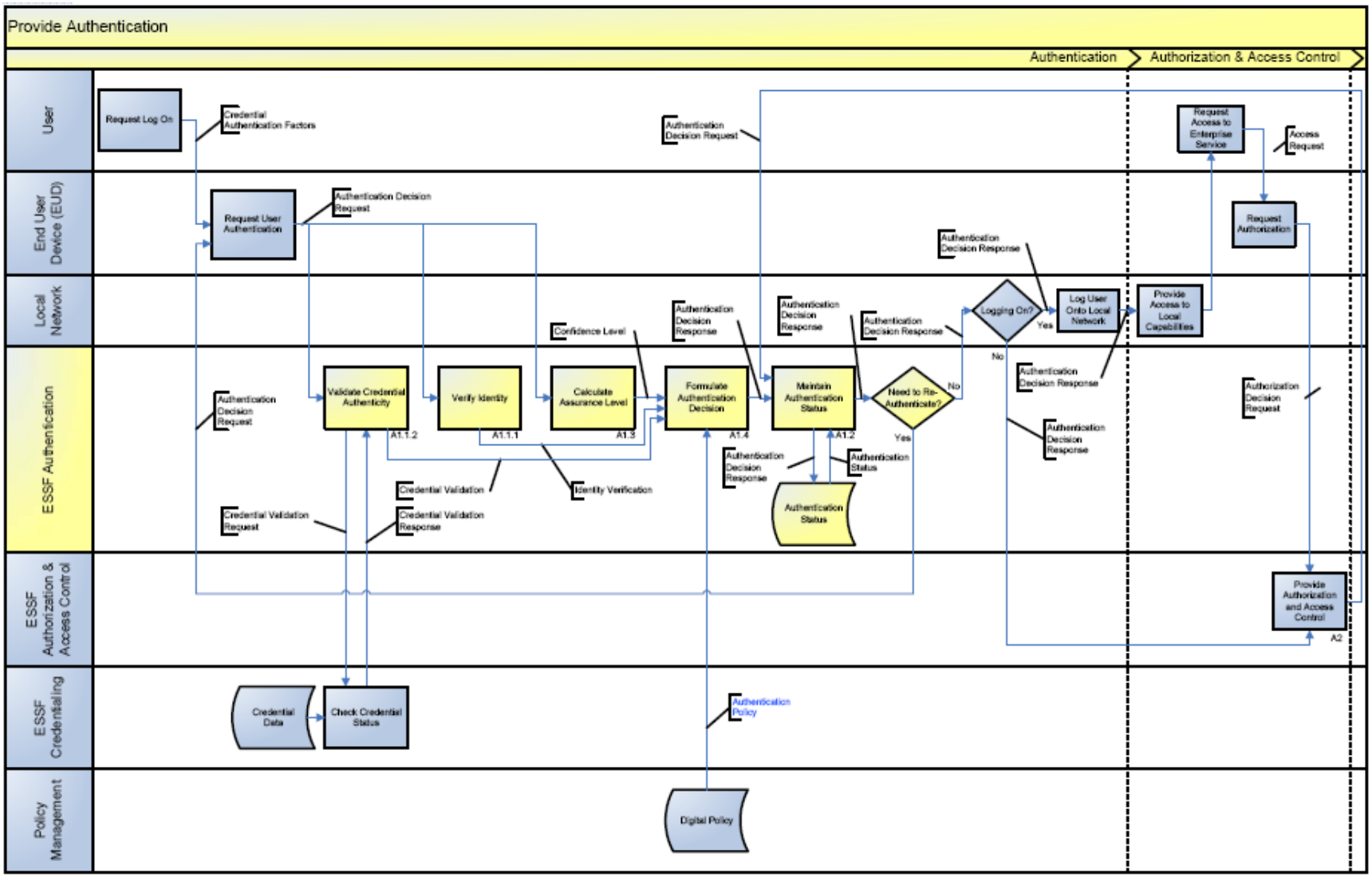


Figure 5: OV-6c Authentication Process Pattern

Additional credential information, such as the private key from the identity certificate contained on the credential and unlocked by authentication factors provided by the user are used by the Verify Identity step to ensure the user presenting the credential is the one whose identity the credential represents.

Additional credential information unlocked by the user's authentication factors is also provided to the Calculate Assurance Level step to calculate an authentication Confidence Level (CL).

The credential validation, identity verification, and confidence level information is provided to the Formulate Authentication Decision process step. This step uses authentication policy to make a positive or negative authentication decision based on provided information. It binds the user's identity, applicable attributes, and the authentication decision via a cryptographic process, and creates an authentication decision response based on a message template. The authentication decision response is provided to the Maintain Authentication Status process step.

The Maintain Authentication Status process step receives an authentication decision response, appends an appropriate time limit, and stores the result so it is visible and accessible in accordance with the DoD IEA; this visibility and accessibility is especially critical to external auditing and monitoring processes required by the SA priority area. When requested, the process step can provide the status of the authentication of any given user. The process step also determines if the identity of a user needs to be re-authenticated.

Once authenticated, the user must be actually logged into the local network from which the user can obtain access to local capabilities and enter the Authorization and Access Control process to gain rights to use designated enterprise services. Granting access to the local network and local capabilities involves an additional process not described in detail here since it is outside the scope of this RA. This process involves determining if a user is already provisioned on the local network, and if not, granting that user some type of temporary or transient network identity and access. This additional process is critical to allowing users access to capabilities anywhere in DoD, specifically outside their assigned network domain. The requirements associated with this additional process are currently under development and will be addressed in other architecture descriptions related to this RA.

4.2.3 Authorization and Access Control Process Pattern

The OV-6c Authorization and Access Control process pattern in **Figure 6**, describes the process steps involved in the authorization and access control process. This process incorporates activities from the Provide Authorization and Access Control activities in the OV-5a activity decomposition as indicated below each process step. The Provide Authorization and Access Control process step controls access to information, services, and applications on the Global Information Grid (GIG) based on predefined policy.

DoD IEA Activity A2.8.5 Oversee Privilege Management Initiative enables and constrains the Authorization and Access Control process. As described in DoD IEA v1.1, SA authorities will use this activity "to develop and maintain an attribute management infrastructure for the Department." Such an infrastructure is essential for carrying out

authorization and access control, as shown in the process pattern, in a net-centric DoD IE. By governing available attributes and associated mechanisms enabling the Authorization and Access Control process, the DoD IEA activity will constrain how the process steps defined here will be carried out.

The Authorization and Access Control process begins with receipt of an authorization decision request by the Identify Pertinent Decision Parameters process step. The authorization decision request is a message asking for a determination as to whether a user can be granted access to a requested enterprise service. This message contains the service ID, resource identifier (for the requested enterprise service), user ID and/or device ID, access request type, and authentication decision. The Identify Pertinent Decision Parameters process step parses an authorization decision request to determine the requestor, requested resource, and requested action. This information defined as access decision parameters, is then used to direct metadata retrieval and provide information needed to check the validity of requestor authentication. Access decision parameters are provided as input for two process steps: Authenticate Requestor and Retrieve Metadata.

The Authenticate Requestor process step invokes the Provide Authentication function to verify the identity of a user requesting access to an enterprise service. This process step sends an authentication decision request to the Provide Authentication process step to verify the identity of a user. The resulting authentication decision response is used when completing the access decision; this decision may simply be the previously completed authentication, if still valid, or the result of a re-authentication of the requestor.

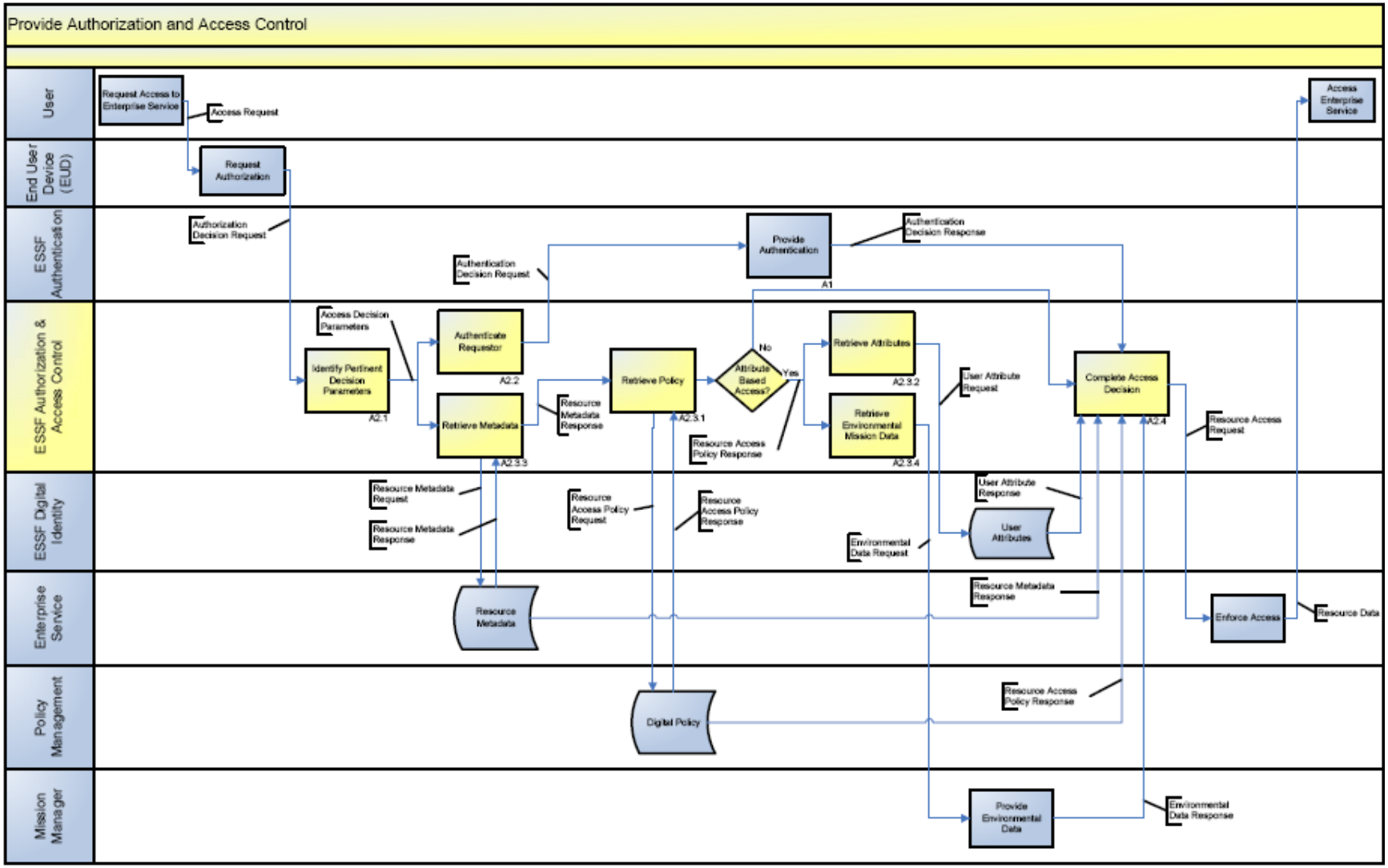


Figure 6: OV-6c Authorization and Access Control Process Pattern

The Retrieve Metadata process step asks for metadata for a requested enterprise service. In accordance with the DoD IEA, enterprise service providers must register their services, publishing associated metadata describing those services, to ensure that potential users can locate and use the service. Included in service metadata will be pointers to policy governing access to the requested service. This process step sends a resource metadata request asking for the metadata required to determine the requirements for accessing a requested enterprise service, to include pointers to the appropriate Resource Access Policy. This message contains the service ID, resource identifier (for requested enterprise service), and metadata request. The resulting resource metadata response provides the metadata for a requested enterprise service. This message contains the service ID and resource metadata, which includes pointers to the resource (i.e., requested enterprise service) and its associated access policy. The resource metadata response is provided to the Retrieve Policy process step.

The Retrieve Policy process step uses pointers provided in service metadata to discover and retrieve the applicable policy governing access to and use of the requested enterprise service. The Retrieve Policy process step sends out a resource access policy request asking for the policy required to make an authorization decision. This message contains the service ID, resource identifier (for requested enterprise service), and policy request. The Retrieve Policy process step receives a resource access policy response containing the policy required to make an authorization decision for the requested enterprise service. This process step provides the resource access policy to three process steps, depending on whether the policy requires attribute based access or not. If attribute based access is not required, the resource access policy response is provided to the Complete Access Decision process step for an access decision. If attribute based access is required, the resource access policy response is provided to the Retrieve Attributes and Retrieve Environmental Mission Data process steps.

The Retrieve Attributes process step uses applicable policy to determine and obtain the additional user attributes required for making an authorization decision for a requested enterprise service. These additional attributes further identify a user and are used to effectively determine, based on policy, if the user can be granted access to the requested enterprise service. The Retrieve Attributes process step sends out a user attribute request asking for information describing specific characteristics of a user for use in determining if the user is authorized to access the requested enterprise service. This message contains the service ID, user ID, and/or device ID, and user access rights (role, privileges, etc.) request. The resulting user attribute response containing requested user attributes is provided to the Complete Access decision process step.

The Retrieve Environmental Mission Data process step requests from a Mission Manager the environmental factors applicable to determining authorization for access to and use of the requested enterprise service, based on policy. This process step sends out an environmental data request containing a request for environmental factors to be enforced as criteria for access to the requested resource (i.e., enterprise service). The resulting environmental data response is provided to the Complete Access Decision process step.

The Complete Access Decision process step uses applicable policy to direct an assessment of pertinent factors (resource metadata, user attributes, and environmental

data) to establish a user's authorization to access and use a requested enterprise service. At this point, all the information required to make an access decision has been provided to the Complete Access Decision process step from other process steps internal and external to the Authorization and Access Control swim lane. Based on the provided information, the Complete Access Decision process step sends out a resource access request message to the Enforce Access process step requesting that access to a requested enterprise service be granted to an authorized user. This message contains the service ID, resource identifier (for requested enterprise service), user ID, and/or device ID, resource access request, and authorization decision. In accordance with the DoD IEA, the authorization decision will also be made visible and accessible for use by authorized users, anticipated and unanticipated, especially those involved in monitoring and auditing ESSF.

The Enforce Access process step controls a user's access to and use of an enterprise service based on the authorization decision. Effectively, it provides policy enforcement. It sends a resource data message granting or denying a user access to a requested enterprise service. This message contains the resource data (for enterprise service), enforcement decision, user ID, and/or device ID, and resource ID (for enterprise service).

5 Technical Position

A set of high level policies and guidance have been selected that begin to establish a common direction for developing standards and technologies. These policies and standards are applicable to the solutions being developed to enable authentication, authorization and access control. More detailed technical standards are provided in developing use cases based on the specific operating environments and conditions in effect. The selected policies and guidance are listed in **Table 3**, StdV-1 EANCS RA Standards Profile.

Table 3: EANCS RA StdV-1 Standards Profile

GROUP	TYPE	NAME	DESCRIPTION
OMB	Policy	M-04-04	This guidance requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. It establishes and describes four levels of identity assurance for electronic transactions requiring authentication. Assurance levels also provide a basis for assessing Credential Service Providers (CSPs) on behalf of Federal agencies. This document will assist agencies in determining their e-government needs. Agency business-process owners bear the primary responsibility to identify assurance levels

GROUP	TYPE	NAME	DESCRIPTION
			and strategies for providing them. This responsibility extends to electronic authentication systems.
OMB	Policy	M-05-05	This memo requires the use of a shared service provider to mitigate the risk of commercial managed services for public key infrastructure (PKI) and electronic signatures.
OMB	Policy	M-05-24	This memorandum provides implementing instructions for HSPD-12 and FIPS-201.
OMB	Policy	M-06-18	This memorandum provides updated direction for the acquisition of products and services for the implementation of Homeland Security Presidential Directive-12 (HSPD-12) “Policy for a Common Identification Standard for Federal Employees and Contractors” and also provides status of implementation efforts.
Presidential Directive	Policy	HSPD-12	HSPD-12 calls for a mandatory, government-wide standard for secure and reliable forms of ID issued by the federal government to its employees and employees of federal contractors for access to federally-controlled facilities and networks.
NIST	Guidance	SP 800-87	This document provides the organizational codes for federal agencies to establish the Federal Agency Smart Credential Number (FASC-N) that is required to be included in the FIPS 201 Card Holder Unique Identifier. SP 800-87 is a companion document to FIPS 201.
NIST	Guidance	SP 800-103	This document provides the broadest possible range of identity credentials and supporting documents insofar as they pertain to identity credential issuance. Priority is given to examples of primary and secondary identity credentials issued within the United States. Part 2 of this document will provide Extensible Markup Language (XML) schemas, as a framework for retention and exchange of identity credential information.

GROUP	TYPE	NAME	DESCRIPTION
NIST	Standard	FIPS 201-1	This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems.
E-Authentication	Guidance	E-Authentication Certificate Credential Assessment Profile	This profile specifies the criteria for certificate-based Credential Services (CSs) that authenticate public key certificates. It is based upon guidance specified in National Institute of Standards and Technology (NIST) Special Publication 800-63, version 1.0.1
FPKIA	Guidance	Bridge-Enabling Web Servers	This document discusses technical steps necessary to enable a web server to accept PKI based user credentials and validate them through a certificate bridge (e.g., the FBCA).
IAB	Guidance	DoD CAC Middleware Requirements Release 3.0	The Middleware Requirements defines the standard set of services, interfaces, and configuration options that must be implemented by all middleware for use on supported Microsoft-Intel (WINTEL) server and desktop operating systems platforms within the DoD. Additionally, this document identifies recommended and optional capabilities that middleware providers should consider implementing to differentiate their products and provide added value.
N/A	Standard	Security Assertion Markup Language (SAML)	Security Assertion Markup Language (SAML) 2.0 is an industry standard for web SSO and web services authentication, attribute exchange, and authorization. SAML-

GROUP	TYPE	NAME	DESCRIPTION
			based federation is the basis for Level 1 and Level 2 authentication under the E-Authentication framework.
N/A	Standard	Extensible Access Control Markup Language (XACML)	XACML was chartered "to define a core schema and corresponding namespace for the expression of authorization policies in XML against objects that are themselves identified in XML.

Appendix A. Acronyms

Acronym	Definition
AV-1	All View - 1 Overview and Summary Information
AV-2	All View - 2 Integrated Dictionary
CAC	Common Access Card
CL	Confidence Level
COI	Community of Interest
CS	Collaboration Services
DoDAF	DoD Architecture Framework
EANCS	Enterprise-wide Access to Network and Collaboration Services
	Enterprise-wide Access to Network and Collaboration Services
EANCS RA	Reference Architecture
ESM	Enterprise Security Management
ESSF	Enterprise Services Security Foundation
EUD	End User Device
FICAM	Federal Identity, Credential, and Access Management
GIG	Global Information Grid
GIG 2.0	
CONOPS	Global Information Grid 2.0 Concept of Operations
IA	Information Assurance
ID	Identity
IE	Information Enterprise
IEA	Information Enterprise Architecture
NIPRNET	Non-classified Internet Protocol Router Network
OV - 1	Operational View -1 High Level Operational Concept Graphic
OV - 5a	Operational View - 5a Operational Activity Decomposition Tree
OV - 6a	Operational View - 6a Operational Rules Model
OV - 6c	Operational View - 6c Event-Trace Description
PKI	Private Key Infrastructure
QoS	Quality of Service
RA	Reference Architecture
SIPRNET	Secret Internet Protocol Router Network
VCJCS	Vice Chairman of the Joint Chiefs of Staff

Appendix B. AV-2 Integrated Dictionary

EANCS RA AV-2: Activities			
Level #	**Operational Activity Name**	**Operational Activity Description**	**Source**
A0	Enable Enterprise-wide Access to Network and Collaboration Services	This activity provides the capability for any designated user to access global network infrastructure from any location with common and portable identity credentials which enable authentication and authorization to (i.e., visibility of, and access to) designated enterprise services.	EANCS CONOP's and GIG 2.0 ORA
A1	Provide Authentication	This activity provides authentication mechanisms, validates the authenticity of credentials, and verifies identities to establish non-repudiation and control information dissemination.	GIG 2.0 ORA (A1.1.3)
A1.1	Authenticate Entity (User)	Verifies that an entity ("claimant") communicating with a verifier has the claimed or assumed identity. Entity authentication may be unilateral, where one party verifies the other, or mutual, where both parties are verified. Entity authentication requires an authentication context (a session, conversation, or association) to ensure that data from one context cannot be successfully replayed in a different context. Validates the entity credential by querying Credential Management.	ESM
A1.1.1	Verify Identity	This activity ensures that the entity presenting the credential is the identity associated with the credential. This may include checking a biometric.	GIG 2.0 ORA (A1.1.3.3)
A1.1.2	Validate Credential Authenticity	This activity ensures that the presented credential is valid and meets all security requirements based on the operating environment, and determines if a presented credential is valid	GIG 2.0 ORA (A1.1.3.2)

EANCS RA AV-2: Activities			
Level #	**Operational Activity Name**	**Operational Activity Description**	**Source**
		by checking its issue date and validity period and further checking to ensure that it has not been revoked.	
A1.2	Maintain Authentication Status	This activity provides to the requesters the identity of entities that currently have validated proof of identity. Note: this function supports "single sign-on" and reduced sign-on.	ESM
A1.2.1	Register Initial Authentication	This activity document that an entity has been successfully authenticated.	ESM
A1.2.2	Provide Authentication Status	This activity verifies the currency of authentication and transfer authentication status to requesting entities.	ESM
A1.2.3	Track Duration of Authentication	This activity monitors currency of authentication and trigger re-authentication in compliance with policy.	ESM
A1.2.4	Clear Registry of Authentication	This activity removes a record of entity from authentication registry. Note: The "Authentication Registry" is a portion of the Authentication Repository.	ESM
A1.3	Calculate Assurance Level	This activity calculates authentication assurance level, namely, Confidence Level (CL).	ESM
A1.3.1	Determine Authentication Factor	This activity determines authentication factors used in Access Request message.	ESM
A1.3.2	Calculate Confidence Level	This activity Calculates Access Request CL.	ESM
A1.4	Formulate Authentication Decision	This activity creates an authentication decision response message.	ESM
A1.4.1	Make Authentication Decision	This activity makes authentication decision, either Yes or No, based upon the assessment of authorization factors.	ESM
A1.4.2	Bind Authentication Decision	This activity binds entity’s identity, applicable attributes, and decision via cryptographic process**.**	ESM

EANCS RA AV-2: Activities			
Level #	**Operational Activity Name**	**Operational Activity Description**	**Source**
A1.4.3	Create Authentication Decision Message	This activity creates an authentication decision response based on message template.	ESM
A1.4.4	Transfer Authentication Decision to Requestor	This activity sends an Authentication Decision Message containing the Authentication Decision to the Requestor.	ESM
A2	Provide Authorization and Access Control	This activity controls access to information, services, and applications based on predefined attributes and rules.	Derived from composite sources (ORA, ESM, CJCSI 6510.01E)
A2.1	Identify Pertinent Decision Parameters	This activity parses the Access Request to determine the requestor, requested resource, and requested action.	
A2.2	Authenticate Requestor	This activity verifies that the requestor has the claimed or assumed identity using the Authenticate Function.	
A2.3	Obtain Needed Access Decision Parameter	This activity retrieves parameter values to support access decision.	
A2.3.1	Retrieve Policy	This activity obtains policy from Policy Management for Access Request.	
A2.3.2	Retrieve Attributes	This activity obtains attributes from Attribute Management for the Access Request.	
A2.3.3	Retrieve Metadata	This activity gets metadata from Metadata Management for Access Request	
A2.3.4	Retrieve Environmental Mission Data	This activity obtains environmental mission data from authorized sources for the Access Request.	
A2.4	Complete Access Decision	This activity creates an access decision using the resource access control policy to evaluate the retrieved parameter values.	
A2.4.1	Decide Access	This activity evaluates request, policy and parameters to make	

EANCS RA AV-2: Activities			
Level #	**Operational Activity Name**	**Operational Activity Description**	**Source**
		access decision.	
A2.4.2	Transfer Access Decision	This activity assembles enforcement response and transfers to enforcement.	

EANCS RA AV-2: Process Steps		
Name	**Description**	**Source of Description**
Access Enterprise Service	In this process step a user accesses and uses an enterprise service in accordance with a previously issued authorization decision.	EANCS Concept of Operations (CONOPS), Oct 2009
Authenticate Requestor	This process step invokes the Provide Authentication function to verify the identity of a user requesting access to an enterprise service.	Derived from composite sources (GIG 2.0 ORA, ESM, CJCSI 6510.01E)
Calculate Assurance Level	This process step uses credential information to calculate an authentication Confidence Level (CL).	ESM Annex for Authentication, v0.8, 25 Sep 2009, based on definition for Acth.5 (App E)
Check Credential Status	This process step checks the issue date and validity period of a credential and whether the credential has been revoked.	ESM Context Overview Presentation, 20 Mar 2009, Slide 33 (derived from description of Credential Validation Request, Sequence Step 2)
Complete Access Decision	This process step uses applicable policy to direct an assessment of pertinent factors (resource metadata, user attributes, and environmental data) to establish a user's authorization to access and use a requested enterprise service.	ESM Context Overview Presentation, 20 Mar 2009, Slide 33 (derived from description of Resource Access Request, Sequence Step 12)
Enforce Access	In this process step a user's access to and use of an enterprise service is controlled in accordance with a previously issued authorization decision.	EANCS Concept of Operations (CONOPS), Oct 2009
Formulate Authentication Decision	This process step makes authentication decision, either Yes or No. It binds the user's identity, applicable attributes, and the authentication decision via a cryptographic process, creates an authentication decision response based on a message template, and sends an Authentication Decision Message containing the Authentication Decision to the Requestor.	ESM Annex for Authentication, v0.8, 25 Sep 2009, based on definition for Acth.6 (App E)

EANCS RA AV-2: Process Steps		
Name	**Description**	**Source of Description**
Identify Pertinent Decision Parameters	This process step parses an access request to determine the requestor, requested resource, and requested action.	ESM Annex for Privilege Management, v0.8, 25 Sep 2009, based on definition for PvM 1.1 (App E)
Log User into Local Network	This process step uses an Authentication Decision previously made to determine whether or not a user should be allowed to logon to the local network and use local resources to access and use designated enterprise services. Local user logon is the first step in achieving access to enterprise services. This process step determines if a user is provisioned to the local network and grants an authenticated temporary user restricted use of local capabilities as designated by policy to access and use enterprise-level collaboration services.	EANCS Concept of Operations (CONOPS), Oct 2009
Maintain Authentication Status	This process step receives an Authentication Decision Response, appends an appropriate time limit, and stores the result. When requested, it provides the status of the authentication of any given user. The process step also determines if the identity of a user needs to be re-authenticated. This process step supports "single sign-on" and reduced sign-on.	ESM Annex for Authentication, v0.8, 25 Sep 2009, Definition for Acth.2 (App E)
Provide Access to Local Capabilities	This process step determines if a user is provisioned to the local network; if so, the user receives access to all local capabilities consistent with local policy and the user's network account. If the user is not provisioned to the local network, the user is granted access to a restricted set of local capabilities, as determined by policy. These resources are currently restricted to a local printer and web browser.	EANCS Concept of Operations (CONOPS), Oct 2009
Provide Authentication	This process step uses authentication mechanisms to validate the authenticity of credentials and verify the	GIG 2.0 ORA, definition for activity A1.1.3

EANCS RA AV-2: Process Steps		
Name	**Description**	**Source of Description**
	identity of a user.	
Provide Authorization and Access Control	This process step controls access to information, services, and applications on the Global Information Grid (GIG) based on predefined policy.	Derived from composite sources (ORA, ESM, CJCSI 6510.01E)
Request Access to Enterprise Service	This process step asks permission to use an enterprise service. The process step prepares and publishes an Access Request. This Access Request may contain a signed, authenticated identity for the user.	EANCS Concept of Operations (CONOPS), Oct 2009
Request Authorization	This process step asks for a determination of the access a user may be granted to a requested enterprise service. The request will include an identifier for the requested enterprise service, user identification, and an authentication decision.	ESM Context Overview Presentation, 20 Mar 2009, Slide 33 (derived from description of Authorization Decision Request, Sequence Step 4)
Request Log On	This process step enables a user to request log on to an End User Device (EUD) connected to a network to gain access to designated capabilities. The user presents a portable identity credential to the EUD so that the data on the credential can be used to verify the user's identity. When presenting the credential, the user may also be required to enter authentication factors (e.g., Personal Identification Number (PIN), password, hard token values, biometric) for use in verifying identity represented by the credential.	EANCS Concept of Operations (CONOPS), Oct 2009; DRAFT DoD Enterprise Security Foundation Implementation Roadmap, p. 6 (derived from definition for Authentication Service)
Request User Authentication	This process step requests verification of a user's identity claims. To enable this verification, the process provides data from the entered credential, to include private data unlocked by authentication factors entered by the User (e.g., PIN, password, hard token values, and biometric (s)).	DRAFT DoD Enterprise Security Foundation Implementation Roadmap, p. 6 (derived from definition for Authentication Service)
Retrieve Attributes	As directed by policy, this process step obtains additional user attributes required to make an authorization decision	ESM Context Overview Presentation, 20 Mar 2009, Slide 33 (derived from

EANCS RA AV-2: Process Steps		
Name	**Description**	**Source of Description**
	for a requested enterprise service. An attribute is a quality or characteristic inherent to or ascribed to a subject or resource. These additional attributes further identify a user and are used to effectively determine, based on policy, if the user can be granted access to the requested enterprise service.	description of User Attribute Request, Sequence Step 9a); attribute definition from Annex A of IA Component of GIG Integrated Architecture, p. A-4
Retrieve Environmental Mission Data	Based on policy, this process step requests from a Mission Manager the environmental factors applicable to determining authorization for access to and use of a requested enterprise service.	ESM Context Overview Presentation, 20 Mar 2009, Slide 37 (derived from description of Environmental Data Request)
Retrieve Metadata	This process step asks for metadata (i.e., data that allows discovery and understanding of the service) for a requested enterprise service. Enterprise service providers register their services, publishing associated metadata describing those services, to ensure that potential users can locate and use the service. Included in service metadata will be pointers to policy governing access to the service.	DoD Net-Centric Services Strategy, 4 May 2007, pp. 6-7; ESM Context Overview Presentation, 20 Mar 2009, Slide 33 (derived from description of Resource Metadata Request, Sequence Step 5)
Retrieve Policy	This process step uses pointers provided in service metadata to ask for applicable policy governing access to and use of a requested enterprise service.	ESM Context Overview Presentation, 20 Mar 2009, Slide 33 (derived from description of Resource Access Policy Request, Sequence Step 7)
Validate Credential Authenticity	This process step determines if a presented credential is valid and meets all security requirements based on the operating environment.	GIG 2.0 ORA, definition for activity A1.1.3.2
Verify Identity	This process step ensures that the user presenting a credential is the one whose identity the credential represents. This process requires checking private information on the credential which must be unlocked using	GIG 2.0 ORA, derived from definition for activity A1.1.3.3

EANCS RA AV-2: Process Steps		
Name	**Description**	**Source of Description**
	authentication factors entered by the user (e.g., personal identification number (PIN), password, hard token values, biometric).	

EANCS RA AV-2: Swim Lanes		
Name	**Description**	**Source of Description**
Enterprise Service	A designated service providing common functionality to authenticated and authorized users. Enterprise services may consist of such things as: enterprise e-mail, enterprise directory (e.g., Joint Enterprise Directory Service (JEDS)), collaboration (e.g., Defense Connect On-line (DCO)), document sharing, portals (e.g., Defense Knowledge On-line (DKO)), and other web-based capabilities, as permitted by DoD policy.	EANCS Concept of Operations (CONOPS), Oct 2009
End User Device (EUD)	Non-person entity (NPE) providing a user with access to a network connected to the Global Information Grid (GIG). The EUD is assumed to be approved for use on the GIG and recognized as a valid device by the network.	EANCS Concept of Operations (CONOPS), Oct 2009
ESSF Authentication	An Enterprise Services Security Foundation (ESSF) service that uses the digital identities and credentials presented by a user to verify the claimed or assumed identity of that user. The service enables authorized entities to access shared resources (e.g., systems, service, and information) and to prevent unauthorized entities from obtaining access to those resources. Authentication includes credential validation, identity verification, session management, and assurance level calculation.	DRAFT DoD Enterprise Security Foundation Implementation Roadmap, p. 6
ESSF Authorization & Access Control	An Enterprise Services Security Foundation (ESSF) service that grants or denies specific requests for obtaining and using information processing services. This service ensures individuals can only use those resources they are entitled to use and then only for approved purposes, enforcing security policies governing access throughout the enterprise. The service determines if access conditions are met by the requesting authenticated entity and provides a decision to grant (or deny) access to the requested resource (e.g., systems, services, information). Authorization and Access Control includes backend attribute retrieval; policy	DRAFT DoD Enterprise Security Foundation Implementation Roadmap, p. 7

EANCS RA AV-2: Swim Lanes		
Name	**Description**	**Source of Description**
	administration, enforcement, and decision; and cross domain mediation.	
ESSF Credentialing	An Enterprise Services Security Foundation (ESSF) service that issues and manages identity credentials. The service issues identity credentials that bind the identifier of the user, and possibly certain user attributes, with information about the credential itself (i.e., validity dates) and the issuer's authority. Credentials may be instantiated in hardware (e.g., DoD Common Access Card) or software (e.g., PKI-based PKCS-12), depending upon the acceptable assurance level for the environment and the mission. Credentialing includes credential generation, validation, distribution, issuance, and maintenance.	DRAFT DoD Enterprise Security Foundation Implementation Roadmap, p. 5
ESSF Digital Identity	An Enterprise Services Security Foundation (ESSF) service managing the life cycle of enterprise unique identifiers and serving as an authoritative source of DoD identity information. The service registers human users, maintains identity evidence information, and distributes such information. It includes those processes required to capture and validate information to uniquely identity an individual, determine suitability, and create and manage a digital identity over its lifecycle. Digital Identity includes identity proofing, vetting, adjudication, digital identity lifecycle management, identity attribute discovery, and linking/association.	DRAFT DoD Enterprise Security Foundation Implementation Roadmap, p. 4
Local Network	Information Technology (IT) environment to which the End User Device (EUD) is connected and which provides access to local resources and designated enterprise services.	EANCS Concept of Operations (CONOPS), Oct 2009
Mission Manager	The official overseeing all aspects of a given operational mission.	Enterprise Security Management Services Glossary and List of Acronyms, p. 2

EANCS RA AV-2: Swim Lanes		
Name	**Description**	**Source of Description**
Policy Management	Function composing, modifying, managing, and controlling access to policies.	DRAFT DoD Enterprise Security Foundation Implementation Roadmap, p.7 (based on definition for Policy Administration)
User	Human being attempting to access and use one or more enterprise services.	EANCS Concept of Operations (CONOPS), Oct 2009

0

EANCS RA AV-2: Information Elements		
Name	**Description**	**Source of Description**
Access Decision Parameters	Message derived from access request containing requestor, requested resource, and requested action, used to direct metadata retrieval and provide information needed to check validity of requestor authentication.	ESM Annex for Privilege Management v0.8, 25 Sep 2009, derived from definition for PvM.1.1
Access Request	Message asking to be authorized to use an enterprise service. This message contains authentication information, user ID, device ID (optionally as required by policy), resource identifier (for requested enterprise service), and access request type. The access request type represents one or more fields containing, for example, a specific request type, identifiers, etc.	Derived from Enterprise Security Management (ESM) Context Overview Briefing, 20 Mar 2009, Authentication, Authorization, and Enforcement Data Dictionary, p. 36
Authentication Decision Request	Message asking to confirm or verify the identity of a user. The message will include user credential information to include private data to confirm credential ownership unlocked by authentication factors entered by the user.	Derived from Definition for Validate User Identity (IdM.1.1) in ESM Spreadsheet (2009-06-18_Post18MayMtg_ FunctionalDecomp_lel_V1.xls)
Authentication Decision Response	Message either confirming or denying a user's identity, as represented by the presented credential. The content of this message determines if the user is granted access to designated capabilities.	Derived from Definition for Respond to Requests (AttrM.2.3.1) ESM Spreadsheet (2009-06-18_Post18MayMtg_ FunctionalDecomp_lel_V1.xls)
Authentication Policy	Rules guiding the confirmation or verification of the identity of a user, based on the user presenting a credential.	EANCS Concept of Operations (CONOPS), Oct 2009
Authentication Status	Message providing the currency of a given authentication decision.	ESM Annex for Authentication, v0.8, 25 Sep 2009, derived from definition for AthC.2.2

EANCS RA AV-2: Information Elements		
Name	**Description**	**Source of Description**
Authorization Decision Request	Message asking for a determination as to whether a user can be granted access to a requested enterprise service. This message contains the service ID, resource identifier (for requested enterprise service), user ID, and/or device ID, access request type, and authentication decision.	Derived from Enterprise Security Management (ESM) Context Overview Briefing, 20 Mar 2009, Authentication, Authorization, and Enforcement Data Dictionary, p. 36
Credential Information	Information contained on an object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.	NIST SP 800-63, as quoted in Federal Identity, Credential, and Access Management (ICAM) Roadmap and Implementation Guidance, v0.2, p. 10
Credential Validation	Information describing whether or not a presented credential has been determined to be valid.	ESM Annex for Authentication, v0.8, 25 Sep 2009, derived from definition for Athc.1.2
Credential Validation Request	Message asking for a determination of the legitimacy of a presented credential; contains the service ID, user credential information, and validation request.	Derived from Enterprise Security Management (ESM) Context Overview Briefing, 20 Mar 2009, Authentication, Authorization, and Enforcement Data Dictionary, p. 36
Credential Validation Response	Message containing the credential validation decision, either yes or no.	Derived from Enterprise Security Management (ESM) Context Overview Briefing, 20 Mar 2009, Authentication, Authorization, and Enforcement Data Dictionary, p. 36
Environmental Data Request	Message containing a request for environmental factors to be enforced as criteria for access to a requested resource (i.e., enterprise service).	Derived from Enterprise Security Management (ESM) Context Overview Briefing, 20 Mar 2009, Authentication, Authorization, and Enforcement Data

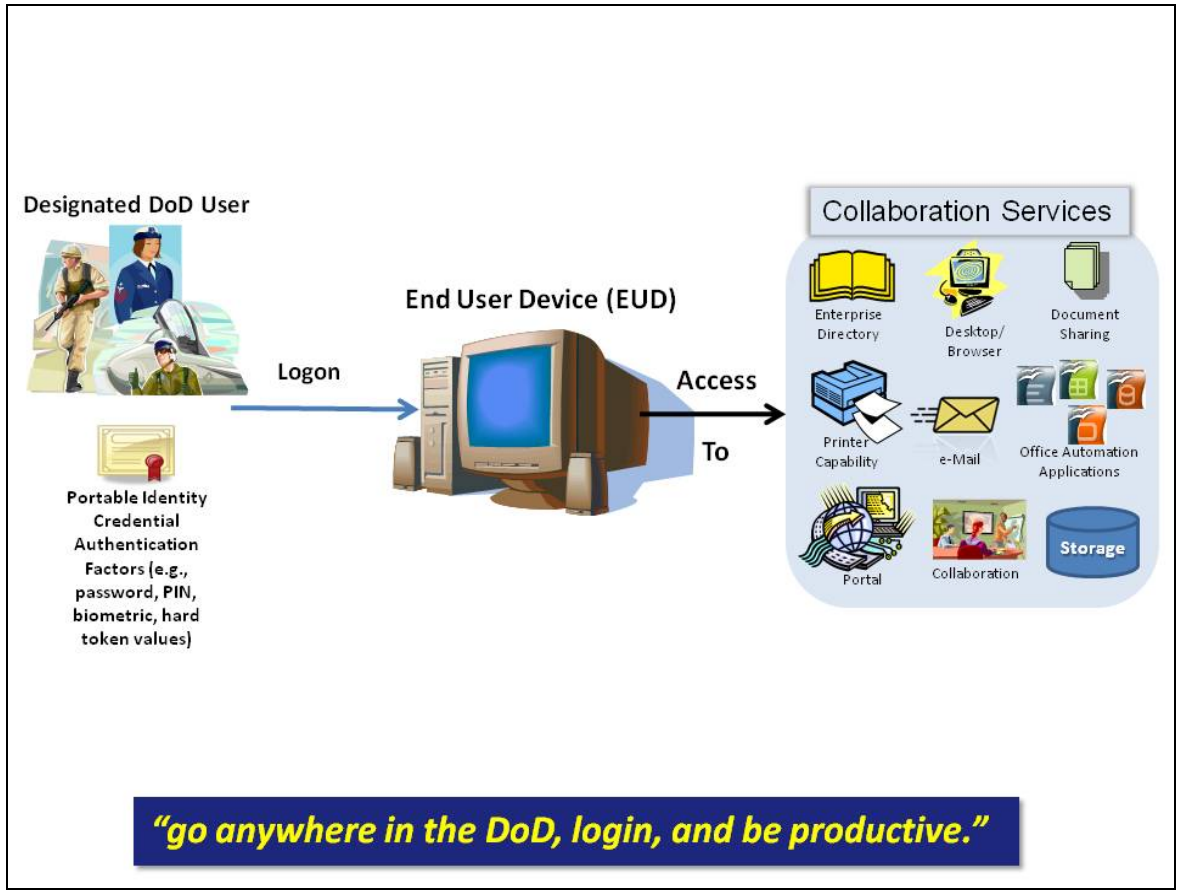
EANCS RA AV-2: Information Elements		
Name	**Description**	**Source of Description**
		Dictionary, p. 37
Environmental Data Response	Information describing the environmental factors to be enforced as criteria for access to a requested enterprise service.	Derived from Enterprise Security Management (ESM) Context Overview Briefing, 20 Mar 2009, Authentication, Authorization, and Enforcement Data Dictionary, p. 37
Identity Verification	Information describing whether a presented credential belongs to the user presenting it.	ESM Annex for Authentication, v0.8, 25 Sep 2009, derived from definition for Athc.5
Resource Access Policy Request	Message asking for the policy required to make an authorization decision regarding a requested enterprise service. This message contains the service ID, resource identifier (for requested enterprise service), and policy request.	Derived from Enterprise Security Management (ESM) Context Overview Briefing, 20 Mar 2009, Authentication, Authorization, and Enforcement Data Dictionary, p. 37
Resource Access Policy Response	Message containing the rules required to make an authorization decision regarding a requested enterprise service.	Derived from Enterprise Security Management (ESM) Context Overview Briefing, 20 Mar 2009, Authentication, Authorization, and Enforcement Data Dictionary, p. 37
Resource Access Request	Message requesting that access to a requested enterprise service be granted to an authorized user. This message contains the service ID, resource identifier (for requested enterprise service), user ID, and/or device ID, resource access request, and authorization decision.	Derived from Enterprise Security Management (ESM) Context Overview Briefing, 20 Mar 2009, Authentication, Authorization, and Enforcement Data Dictionary, p. 37
Resource Data	Message granting a user access to requested enterprise service. This message contains the resource data (for	Derived from Enterprise Security Management (ESM) Context Overview

EANCS RA AV-2: Information Elements		
Name	**Description**	**Source of Description**
	enterprise service), enforcement decision, user ID, and/or device ID, and resource ID (for enterprise service).	Briefing, 20 Mar 2009, Authentication, Authorization, and Enforcement Data Dictionary, p. 37
Resource Metadata Request	Message asking for the metadata required to determine the requirements for accessing a requested enterprise service, to include pointers to the appropriate Resource Access Policy. This message contains the service ID, resource identifier (for requested enterprise service), and metadata request.	Derived from Enterprise Security Management (ESM) Context Overview Briefing, 20 Mar 2009, Authentication, Authorization, and Enforcement Data Dictionary, p. 36
Resource Metadata Response	Message providing the metadata for a requested enterprise service. This message contains the service ID and resource metadata, which includes pointers to resource (i.e., requested enterprise service) and associated access policy.	Derived from Enterprise Security Management (ESM) Context Overview Briefing, 20 Mar 2009, Authentication, Authorization, and Enforcement Data Dictionary, p. 36
User Attribute Request	Message asking for information describing specific characteristics of a user for use in determining if the user is authorized to access a requested enterprise service. An attribute is a quality or characteristic inherent to or ascribed to a subject or resource. This message contains the service ID, user ID, and/or device ID, and user access rights (role, privileges, etc.) request.	Derived from Enterprise Security Management (ESM) Context Overview Briefing, 20 Mar 2009, Authentication, Authorization, and Enforcement Data Dictionary, p. 37; attribute definition from Annex A of IA Component of GIG Integrated Architecture, p. A-4
User Attribute Response	A message containing requested user attributes for use in making an authorization decision. An attribute is a quality or characteristic inherent to or ascribed to a subject or resource. The message contains the user attributes and/or a yes/no indication of compliance to a	Derived from Enterprise Security Management (ESM) Context Overview Briefing, 20 Mar 2009, Authentication, Authorization, and Enforcement Data Dictionary, p. 37; attribute definition from

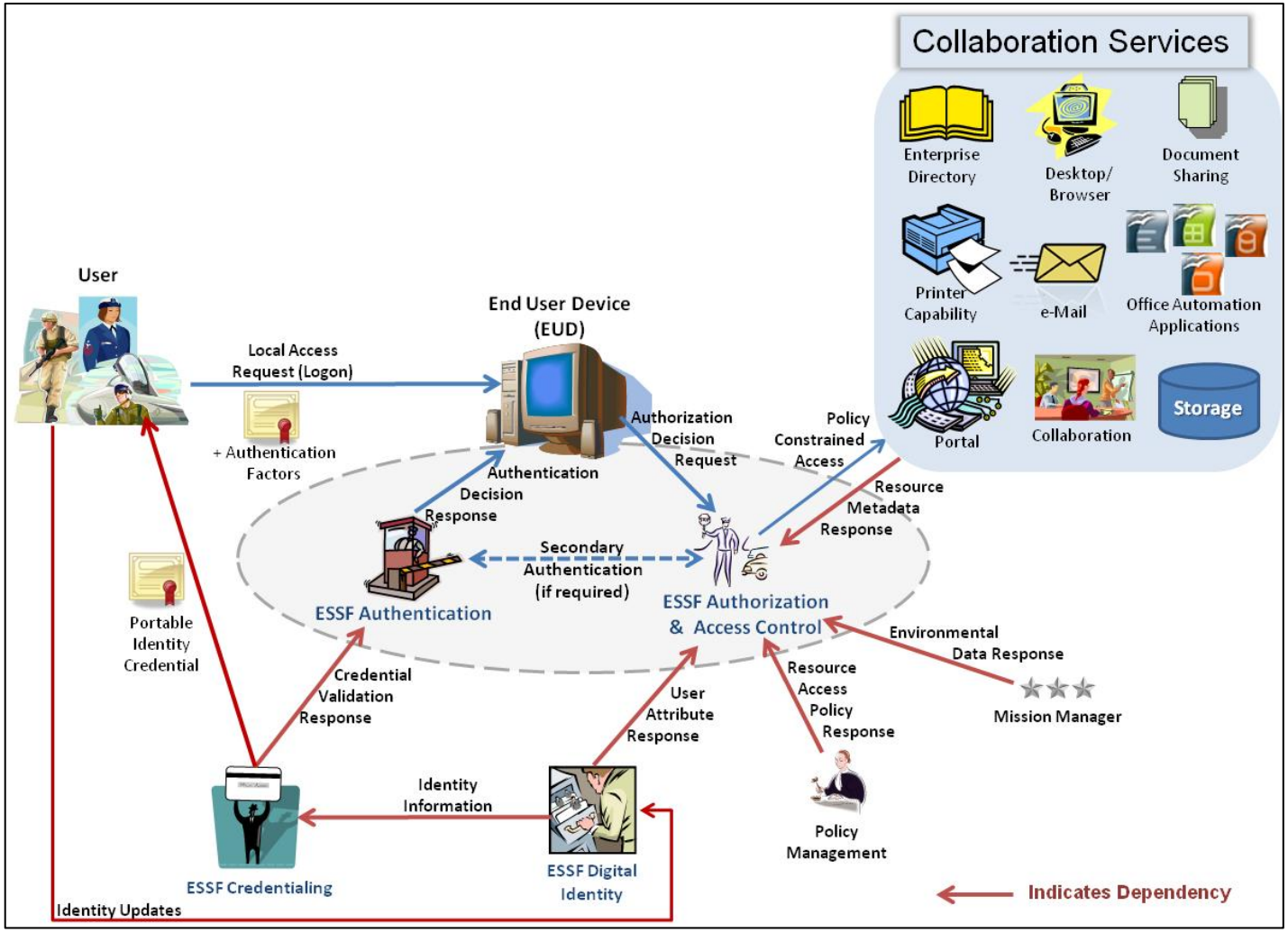
EANCS RA AV-2: Information Elements		
Name	**Description**	**Source of Description**
	required attribute (e.g., Does the user possess at least a Secret clearance?).	Annex A of IA Component of GIG Integrated Architecture, p. A-4

Appendix C. OV-1, OV-5a, and OV-6c Diagrams

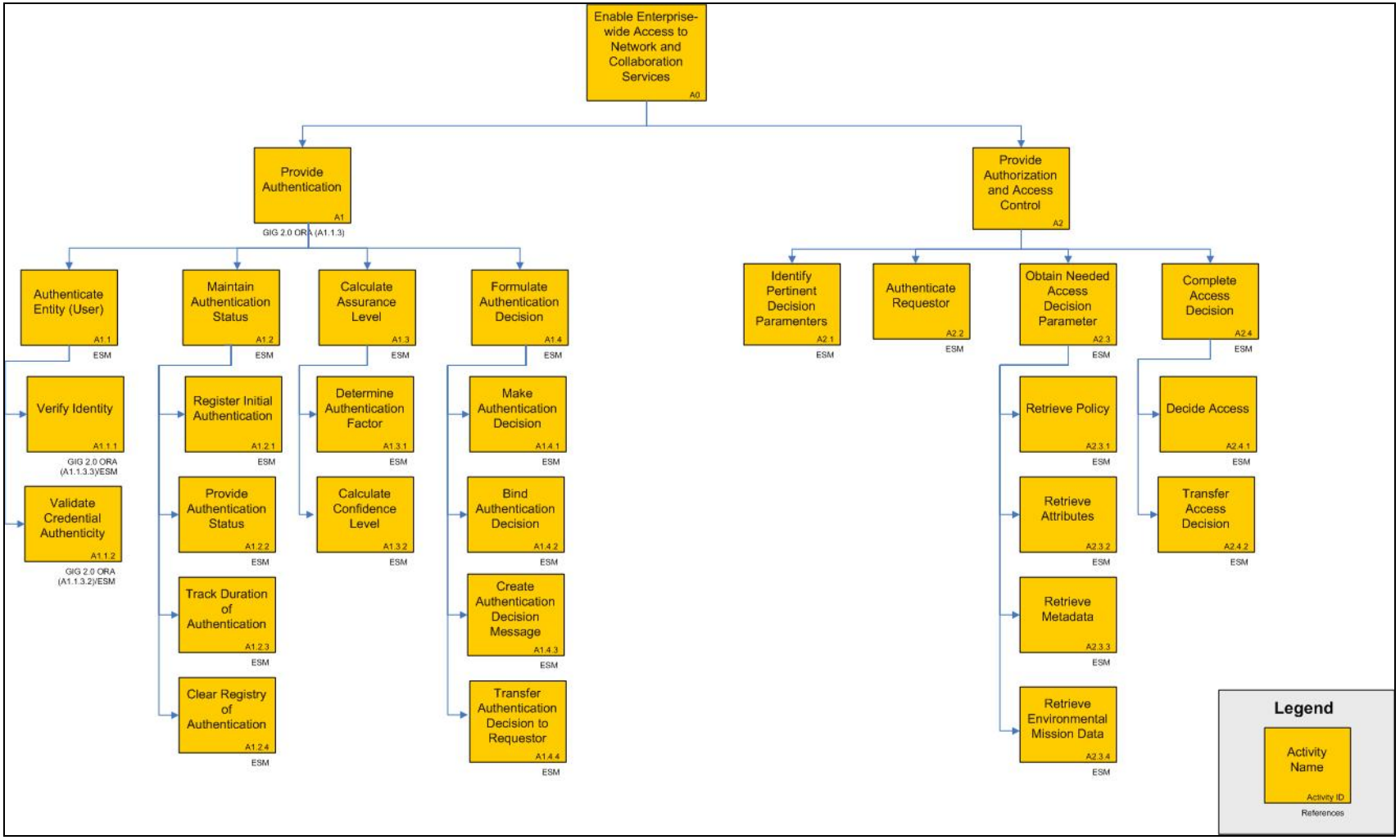
EANCS RA OV-1 High-Level Operational Concept Graphic (User Perspective)



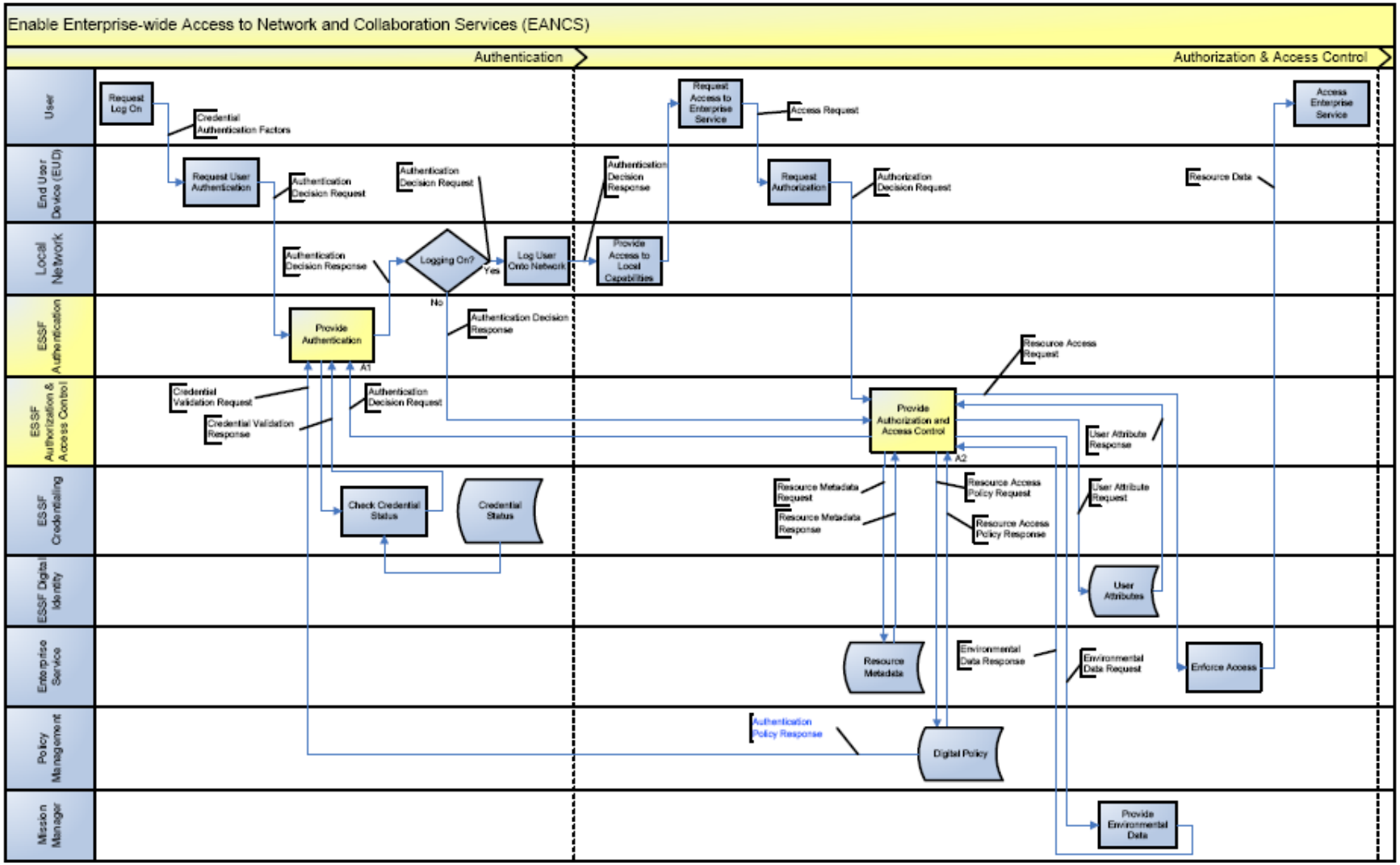
EANCS RA OV-1 High-Level Operational Concept Graphic (Service Provider Perspective)



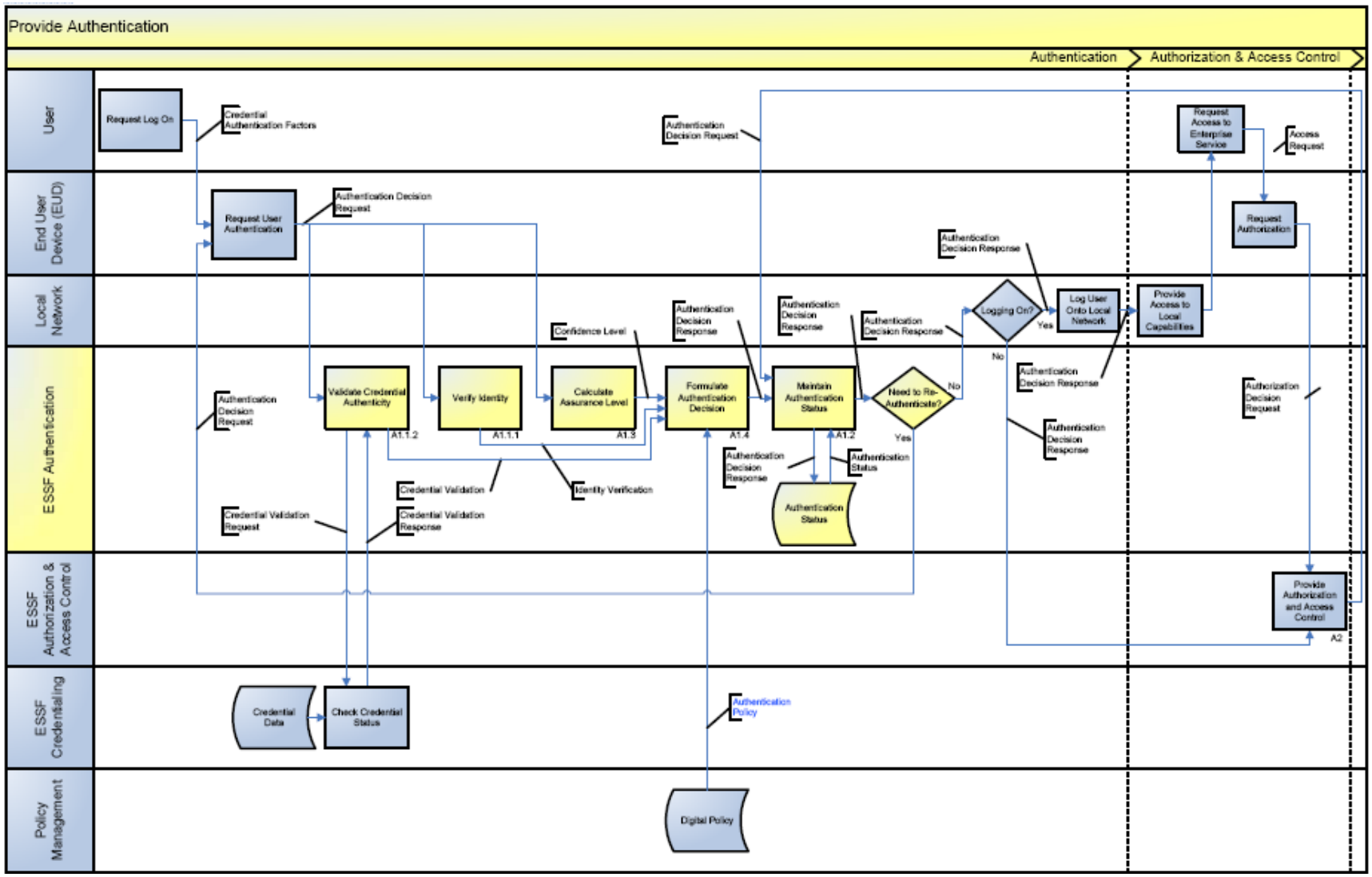
EANCS RA OV-5a Operational Activity Model



EANCS RA OV-6c Event Trace Description (Combined Process Pattern)



EANCS RA OV-6c Event Trace Description (Authentication Process Pattern)



EANCS RA OV-6c Event Trace Description (Authorization Process Pattern)