Net-Enabled Command Capability

INCREMENT 1 INFORMATION ASSURANCE (IA) ARCHITECTURE

Version 1.0

29 November 2007

Prepared by:

Net-Enabled Command Capability
Joint Program Management Office (JPMO)
P.O. Box 4502
Arlington, VA 22204-4502

In Collaboration with the NECC Component Program Manager's for the Navy, Air Force, Army, Marine Corps, USJFCOM and DISA.

DISTRIBUTION – Distribution authorized to DoD and DoD Contractors only; for administrative/operational use (November 2007). Other requests for this document shall be referred to the NECC Program Management Office.

DESTRUCTION NOTICE – For unclassified, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document.

APPROVAL PAGE

Approved by: Mark J. Kuzma Date: 11/28/07

MARK J. KUZMA
Chief Engineer,
Net-Enabled Command Capability (NECC)

EXECUTIVE SUMMARY

The Net-Enabled Command Capability (NECC) is the Department of Defense's (DoD) principal program for delivering Command and Control Capabilities (C2C) accessible in a net-centric environment. It focuses on providing the commander with the data and information needed to make timely, effective, and informed decisions. The Information Assurance (IA) Architecture discusses and summarizes the NECC approach to address IA requirements.

The *Acquisition Information Assurance Strategy (IAS)* identifies NECC as a "Mission Critical" Program as defined in DoDI 5000.2 and NECC Capability Modules (CMs) will have a baseline Mission Assurance Category (MAC) of I and a baseline Confidentiality Level (CL) of "classified." Security requirements for MAC I, CL classified systems are defined in DoDI 8500.2 and will be allocated to NECC CMs, or other entities such as the operational nodes in *DoD Information Certification and Accreditation Process (DIACAP) Implementation Plans*.

The NECC Increment 1 architecture has been designed in a modular fashion by packaging capabilities into CMs, which represent packages of functionally related software that provide solutions to one or more required capabilities. CMs will be packaged into Capability Packages (CPs) for installation on Global Information Grid (GIG) Computing Nodes (GCNs). The GCNs will be configured to include hypervisors so that the NECC CPs may be installed as Virtual Machines (VMs). NECC Information Assurance functions will be integrated into NECC CMs as they are defined and developed.

NECC will leverage the DoD and Intelligence Community (IC) Public Key Infrastructures (PKI) by using Public Key (PK) certificates for user login and using the Distinguished Name (DN) in the certificates as a unique identifier for users across NECC. User certificates will be the primary means for login to NECC; user identity and password will be used only as a fallback position. In addition, NECC will install server certificates with the CPs to support digitally signing SOAP messages and machine-to-machine authentication using the Transport Layer Security (TLS) protocol.

NECC will leverage the Net-Centric Enterprise Services (NCES) Security Services by using the NCES Robust Certificate Validation Service (RCVS) to validate that user or server certificates have not been revoked. In addition, NECC will use the NCES Attribute Service to obtain attributes from the Joint Enterprise Directory Services (JEDS). NECC will also use the standards identified in the *NCES Service Security Design Specification* and follow the interface requirements identified in the *NCES Service Security Design* and *Interfaces Specifications.*

The architecture defines a User Management (UM) CM to perform authentication, authorization, and auditing of web service messages. The UM CM also provides the capability to define application-specific user roles and access control policies. This allows for a finer granularity of access control than would be supported by the attributes currently available in JEDS. Although Attribute Based Access Control (ABAC) is the goal, the set of enterprise attributes currently available is not yet rich enough to fully support access control needs, so Role Based Access Control (RBAC) will be used in the Increment 1 timeframe.

The architecture addresses both machine-to-machine web services and Representational State Transfer (REST) communications. Web Service Security (WSS) is based on the NCES design,

which employs WSS standards using digitally-signed SOAP messages that place security information (e.g., the user's identity in a Security Assertion Markup Language (SAML) assertion) in the message headers. This supports passing the end user's identity through a chain of web services in a reliable way. Although REST is simpler to implement, it does not provide the same level of security as described above. Consequently, this architecture includes REST in cases where REST is the only viable solution, such as for geospatial access.

Because of the Virtual Machine (VM) Architecture of the GCNs, the IA Architecture describes the need to include software such as Host Based Security Systems (HBSS) in the CPs, not just in the GCN. The architecture also describes testing and distributing Information Assurance Vulnerability Alert (IAVA) patches.

The current process for validating requirements for cross domain data flows and implementing a Cross-Domain Solution (CDS) will be followed on a case-by-case basis in accordance with current policies. Where technical solutions are not available, the NECC Joint Program Management Office (JPMO) will work with the National Security Agency (NSA) and the Defense Information Systems Agency (DISA) to identify requirements for future CDSs.

REVISION HISTORY

REVISION NUMBER	REVIEWER / ORG	CHANGES	REVISION DATE	DATE ENTERED	NAME OF PERSON ENTERING CHANGE
1.0	Noble/MITRE	Baseline version	20 Nov 2007	20 Nov 07	Larry Noble
1.0	Brown/JPMO Program Control	Reformatted document into new template. Edited document and updated acronyms.	27 Nov 2007	29 Nov 07	Dustan Brown

TABLE OF CONTENTS

APPROVAL PAGE ..... **II**

EXECUTIVE SUMMARY ..... **III**

REVISION HISTORY ..... **V**

1 STRATEGY **1**

2 KEY CONCEPTS **2**

2.1 IA REQUIREMENTS 4
2.2 USER MANAGEMENT CAPABILITY MODULE 4
2.3 PUBLIC KEY INFRASTRUCTURE (PKI) 4
2.4 OVERVIEW OF NECC IA ARCHITECTURE 5
2.5 USE CASES 6
2.5.1 Web Browser to Web Server 6
2.5.2 Machine-to-Machine Communications Using SOAP Messages 7
2.5.3 Machine-to-Machine (M2M) Representational State Transfer (REST) Communications 11
2.5.4 Policy Definition and Management 12
2.6 ROLE-BASED ACCESS CONTROL /ATTRIBUTE BASED ACCESS CONTROL 13
2.7 ACCESS TO LEGACY APPLICATIONS AND BACK-OFFICE SYSTEMS 13
2.8 AUDIT 13
2.8.1 Audit Requirements 13
2.8.2 Audit Concept 14
2.9 CONFIDENTIALITY 14
2.9.1 Confidentiality of Data in Transit 14
2.9.2 Confidentiality of Data at Rest 15
2.10 INTEGRITY 15
2.11 AVAILABILITY 16
2.12 WEB SERVICE PROVIDER IMPLEMENTATION OF THE VIRTUALIZED ENVIRONMENT 16
2.13 DATA MARKING AND LABELING 17
2.13.1 Requirements 17
2.13.2 Approach 17
2.14 COMPUTER NETWORK DEFENSE (CND) 18
2.14.1 Requirements 18
2.14.2 Approach to Intrusion Detection Monitoring, Analysis, and Reporting 18
2.14.3 Approach to Vulnerability Analysis and Assessment 19
2.14.4 Approach to Defense-in-Depth 19
2.15 JOINT TECHNICAL OPERATIONS CONTROL CAPABILITY SECURITY 19
2.16 CROSS DOMAIN ENTERPRISE SERVICES 20
2.16.1 Requirement 20
2.16.2 Approach 20
2.17 MULTINATIONAL INFORMATION SHARING (MNIS) 21
2.17.1 Requirement 21
2.17.2 Approach 21

3 IMPLEMENTATION **21**

3.1 ACCESS CONTROL 21
3.2 IMPLEMENTATION BEST PRACTICES 22
3.3 PUBLICATION OF SERVICES AND ESTABLISHING TRUST 22
3.4 SERVER PUBLIC KEY CERTIFICATES 22
3.5 SUMMARY OF REQUIREMENTS FOR CM DEVELOPERS 22
3.6 SUMMARY OF ARCHITECTURAL REQUIREMENTS FOR HOST PROVIDERS 23
3.7 WAIVER PROCESS 23

4 CONCLUSIONS **24**

5 POLICY/DIRECTIVES **24**

APPENDIX A – ACRONYMS **26**

APPENDIX B – LEXICON **29**

APPENDIX C – STANDARDS **32**

C.2 TRANSPORT SECURITY 32
C.3 NCES SECURITY STANDARDS AND PROFILES 32
C.4 NECC IA STANDARDS 33

APPENDIX D – REFERENCES **34**

LIST OF FIGURES

Figure 1: System Security Taxonomy 2
Figure 2: Service Security Taxonomy 3
Figure 3: Overview of NECC IA Architecture 5
Figure 4: Web-Browser to Web Server Using User Management CM 7
Figure 5: M2M SOAP with UM CM Agent 8
Figure 6: M2M SOAP and UM CM, Gateway 9
Figure 7: Authentication and Authorization in Service Chaining 11
Figure 8: REST (M2M) 12
Figure 9: Audit Concept 14
Figure 10: The Virtualized Environment 17
Figure 11: CND Concept 18
Figure 12: JTOCC Security Data Flows 20

1 STRATEGY

The *Net-Enabled Command Capability (NECC) Acquisition Information Assurance Strategy (IAS)* [NJPMO1] describes how Information Assurance (IA) requirements for NECC will be identified. It also identifies sources for IA requirements (e.g., policies and directives); results of risk assessments, particularly for Service Oriented Architectures (SOA) and eXtensible Markup Language (XML)-based web services; and stakeholder requirements.

NECC plans to leverage ongoing programs to meet these requirements. The Public Key Infrastructures (PKI) in the Department of Defense (DoD) and the Intelligence Community (IC) provide reliable means for identifying users and servers, and performing authentication and authorization. The use of PKI also offers the opportunity to include users from other communities that have PKIs with less disruption to the architecture.

The Net-Centric Enterprise Services (NCES) program has defined a web service security architecture and specifications, and built reference implementations. NCES offers two security services: (1) an Attribute Service (AS), and (2) a Robust Certificate Validation Service (RCVS). In addition, NCES offers an NCES Conformance Test Kit (CTK) for checking compliance with the NCES Security Message Format, and the *NCES Service Security Interface Specifications*. NCES does not provide other security services (e.g., Policy Enforcement Point (PEP), Policy Decision Service (PDS), Policy Retrieval Service (PRS), Policy Administration Service (PAS), and local attribute service), but recommends using Commercial-off-the-Shelf (COTS) products that meet the NCES Security Message Format specifications.[1] NECC plans to leverage the NCES security services by using the RCVS and AS, and adhering to the interface specifications. NECC will implement a *User Management Capability Module* (UM CM) to package security services not offered by NCES. This strategy will position NECC to leverage the web service technology in NCES and to be ready to interoperate with future NCES services.

NECC will implement a mix of security mechanisms to cover a range of use cases, and the security policies of NECC services. The security mechanisms include the use of Hypertext Transfer Protocol (HTTP) with Transport Layer Security (TLS), and the Web Service Security (WS-Security) mechanisms. The HTTP authentication with TLS approach will be used for web browser to web server communications, and Machine-to-Machine (M2M) Representational State Transfer (REST) will be used for geospatial data access. The WS-Security standard, including Simple Object Access Protocol (SOAP) message security enhancements, will be used for M2M SOAP communications.

1.1 Related Documents

NECC Increment 1 Software Architecture, version 1.0

NECC Increment 1 Data Architecture, version 1.0

NECC Increment 1 Technical Operations Architecture, version 1.0

NECC Increment 1 Physical Architecture, version 1.0

[1] DISA3 p. 5

2 KEY CONCEPTS

This NECC Increment 1 IA architecture constrains how materiel developers must design the services that compose their Capability Modules (CMs). This guidance includes the standards, external capabilities, and architectural patterns developers must use. It applies to capabilities in all the functional domains addressed by Increment 1.

This IA architecture considers both the measures to protect and defend the NECC IA, e.g., Capability Packages (CPs), and the measures to protect NECC transactions.

Figure 1 shows the relationships and linkages among the elements concerning system security, e.g., protection of the NECC CPs. Host-Based Security Systems (HBSS), which include Host-Based Intrusion Detection Systems (HIDS), antivirus systems, and vulnerability checker software, are contained in CPs. Security Technical Implementation Guides (STIGs) provide configuration requirements for CPs. Information Assurance Vulnerability Alert (IAVA) patches that apply to the software in a CP, are installed on that CP. The Joint Technical Operations Control Capability (JTOCC) provides security-related resources, such as the IAVA patches to CPs and also monitors the CPs with respect to their security postures. The CPs also contain PKI certificates including server certificates and trust anchor certificates, which can be used to validate other certificates.

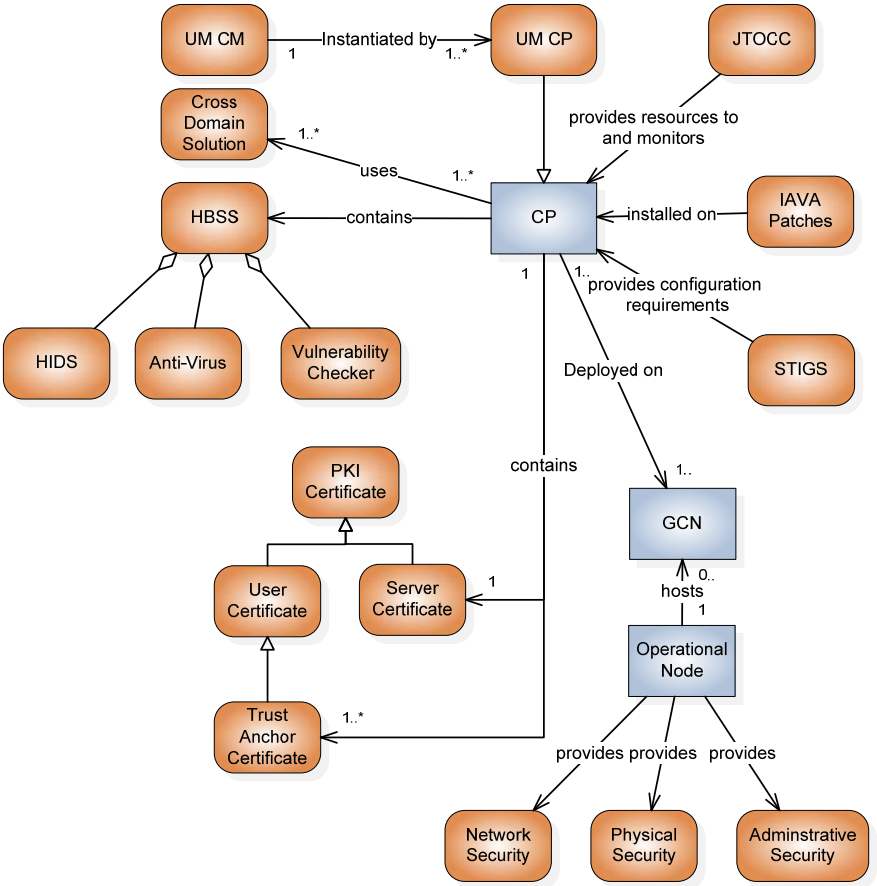

Figure 1: System Security Taxonomy

The second major view of IA for NECC is service security. It addresses the security of NECC service transactions. The elements to provide for security of NECC transactions include the UM CM, which contains incoming and outgoing message handlers. The outgoing message handlers implement the NCES defined SOAP message format and digitally sign the SOAP message. The incoming message handlers authenticate incoming SOAP messages (i.e., validate the message) by means of a digital signature checker that uses the NCES RCVS or the Certificate Revocation List (CRL). The message handlers also include audit loggers to record incoming and outgoing transactions.

A UM CM also contains a PEP that enforces authorization, i.e., ensures that the requestor is authorized to perform the requested function on the requested resource. The authorization process uses access controls that may be either Attribute Based Access Control (ABAC) or Role Based Access Control (RBAC). The UM CM contains a PDS, a PAS (which Creates, Reads, Updates, and Deletes (CRUD) access control policies in the Policy Data Store), and a Principal Attribute Service (PrAS), which provides access to enterprise attributes via the NCES AS and local attributes using legacy authentication and authorization data stores.

Figure 2 shows the relationships and linkages among the elements and other services.

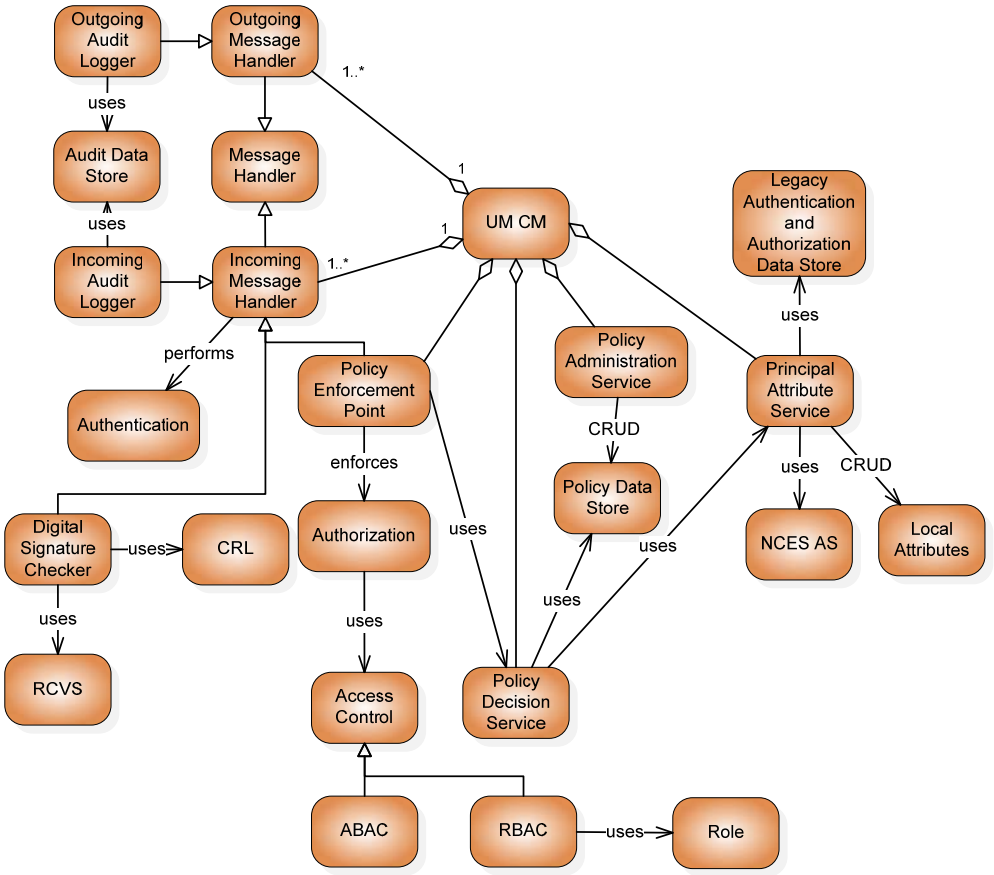

Figure 2: Service Security Taxonomy

2.1 IA Requirements

In order to achieve confidentiality, integrity, and availability, DoD Instruction (DoDI) 8500.2, *Information Assurance (IA) Implementation*, defines required controls for each Mission Assurance Category (MAC) and Confidentiality Level (CL). (If the system is in a Special Compartmented Information (SCI) enclave, Director of Central Intelligence Directive (DCID) 6/3 security requirements apply.) The MAC reflects the importance of information relative to the achievement of DoD goals and objectives, and is primarily used to determine the requirements for availability and integrity. The CL identifies the confidentiality of information a system processes (i.e., classified, sensitive, or public). The *NECC IAS* defines the baseline MAC and CL for NECC CMs as MAC-I Classified. The IA requirements to be addressed by a CM will be included in the *DoD Information Certification and Accreditation Process (DIACAP) Implementation Plan.*

The IA requirements will be satisfied by a combination of controls in NECC components, enclaves, and Global Information Grid (GIG) Computing Nodes (GCNs). The *DIACAP Implementation Plan* identifies the allocation of IA requirements to the host organization, operational node, host system, and the materiel provider.

This architecture focuses on security functions, which are based in the controls. These functions are:

- Authentication
- Authorization (also referred to as access control)
- Audit
- Confidentiality, Integrity, and Availability of data at rest and in-transit
- Data labeling
- Computer Network Defense (CND)
- Cross domain information flows

2.2 User Management Capability Module

NECC will develop a User Management Capability Module (UM CM) to support authentication, authorization, and audit. The UM CM is a Command and Control (C2) cross-functional (e.g., infrastructure) CM that will be used by other CMs to support performing these functions as required. The UM CM will include a PEP, PDS, PAS, PrAS, and audit capability. The PAS will support building and maintaining a database of access control policies, and will provide a Graphical User Interface (GUI). The policy database will be capable of importing and exporting policies in eXtensible Access Control Markup Language (XACML) format. The PrAS will support creating and maintaining a database of NECC-specific users and their attributes and/or roles. The attribute database will be replicated among NECC sites. The audit capability will record NECC transactions.

2.3 Public Key Infrastructure (PKI)

The DoD has established a PKI on the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) and is establishing a PKI on the Secret Internet Protocol Router Network

(SIPRNet). These PKIs provide for issuing and maintaining public key (PK) certificates for registered individuals. A critical function of the PKIs is to maintain a CRL, which identifies certificates that have been revoked. NCES is providing a RCVS for checking the CRL. However, the service will not be reachable when a site is disconnected from the Wide Area Network (WAN); consequently, User Management capability packages at operational sites must store copies of the CRL for use when disconnected from the WAN.

2.4 Overview of NECC IA Architecture

Figure 3 presents an overview of the objective NECC Increment 1 IA architecture. It shows NECC CPs at sites in one security domain (NIPRNet, SIPRNet, etc.). The figure shows a second security domain connected to the first via an Enterprise Cross Domain Solution (CDS).

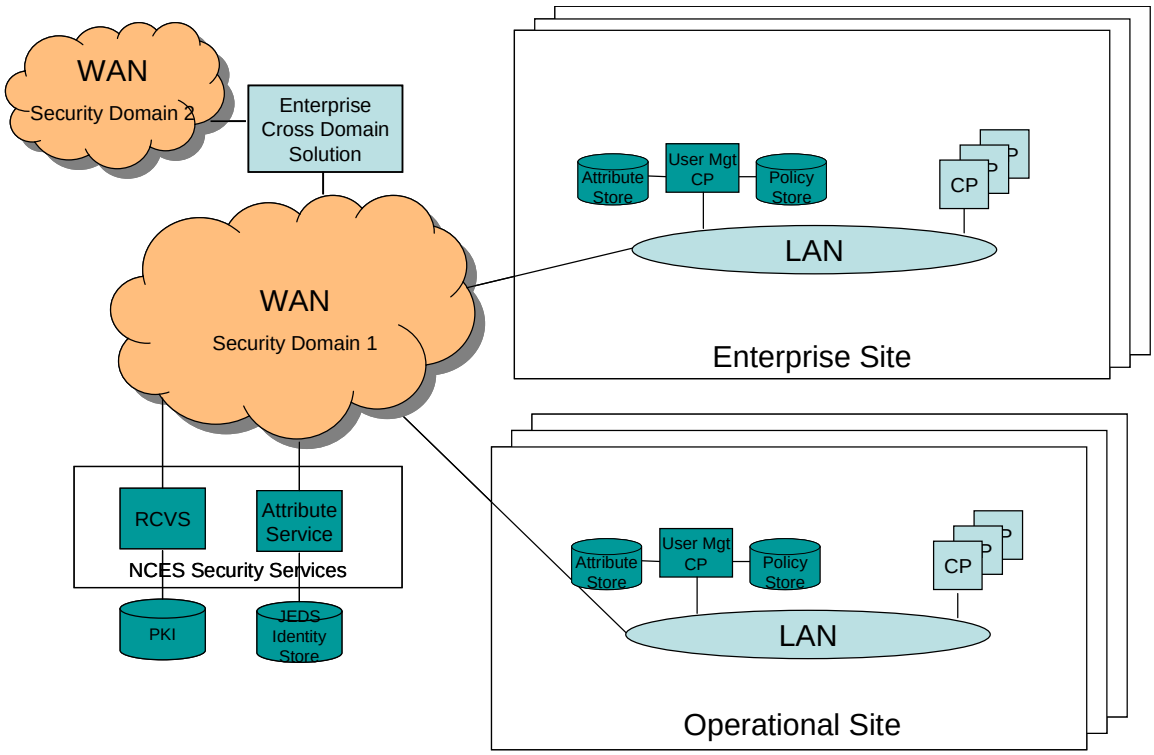

Figure 3: Overview of NECC IA Architecture

For a given security domain, the figure depicts Enterprise and Operational Sites, a UM CP resident at each site, the NCES Attribute Service providing access to the Joint Enterprise Directory Services (JEDS), and the NCES RCVS providing access to the Public Key Infrastructure (PKI). The JEDS attribute set is still being defined. The NCES RCVS will have access points distributed around the domain for improved performance and availability.

The IA Architecture provides two approaches to addressing authentication and authorization: (1) WS-Security using signed SOAP messages, and (2) Hypertext Transfer Protocol Secure (HTTPS) (HTTP over TLS) with HTTP Authentication.

The HTTPS with HTTP Authentication approach has the advantage that it is simple and relatively quick to implement; however, it is limited in its ability to provide the identity of the end-user to downstream services and in its access control functionality. Also, TLS is a point-to-

point protocol which will result in the messages being exposed at intermediate nodes (which risks exposing data with need-to-know restrictions such as social security numbers).

The WS-Security approach is more complex to implement, but provides additional security capability. It supports end-to-end authentication (portable authentication) and provides a means to pass user-identity through a series of services. Also, the use of signed SOAP messages provides non-repudiation and data integrity.

The following guidance is provided to CM developers:

- Use WS-Security and signed SOAP messages for the following situations: (1) M2M transactions using SOAP messages, and (2) Web services that require restricted access to need-to-know information or write access.
- Use HTTP with TLS for the following situations: (1) Web browser-to-web server interactions; and (2) Geospatial data transactions where SOAP messages are not supported.

2.5 Use Cases

The authentication and authorization approach for the following three use cases is illustrated below:

1. Web browser to web server
2. M2M communications using SOAP messages
3. M2M communications using REST for Geospatial data (without SOAP)

2.5.1 Web Browser to Web Server

Authentication in the web browser to web server use case is done through a two-way TLS protocol handshake in which both sides send their PK-certificates to the other for validation. As part of validating the user's certificate, the web server checks whether the user's certificate has been revoked, is in its valid date range, and is signed by a trusted authority. The objective is for all users to have PK-certificates and use them for authentication to web servers; however, a backup capability is provided to allow user identity and password for login. Login with user identity and password requires that the UM CM translate the user identity to a unique identity within NECC (e.g., Distinguished Name (DN) or SIPRNet email address).

If the security policy of the web server requires finer access control than can be provided by HTTP, the web server will access the UM CM to obtain the access policy and user attributes. Figure 4 shows how the web server will obtain user attributes/roles and the access control policy from the UM CM. In order to access a web Server (1), the web browser sends an HTTP request to the web Server (1.1). The web Server and web browser engage in a two-way authentication handshake (1.2). As part of the handshake, both sides validate the other's certificates (1.2.1 and 1.2.2). If the user does not have a PK-certificate, the TLS authentication is one-way (i.e., the browser authenticates the web server), an encrypted connection is established, and the web server prompts the user for a user ID and password to authenticate the user.

After the authentication is complete, the web server extracts the user's DN from the PK-certificate (1.3), and includes it in a query to the UM CM for the user's attributes (1.4). If the user logged in with user ID and password, the web server sends the user ID in the attribute request and the UM CM obtains a corresponding DN for the user (1.4.1). The UM CM then

queries the NCES AS for enterprise attributes (1.4.2). The web server also queries the UM CM to determine the security (access control) policy (1.5). Given the attributes and applicable policy, the web server then makes an authorization decision (1.6).

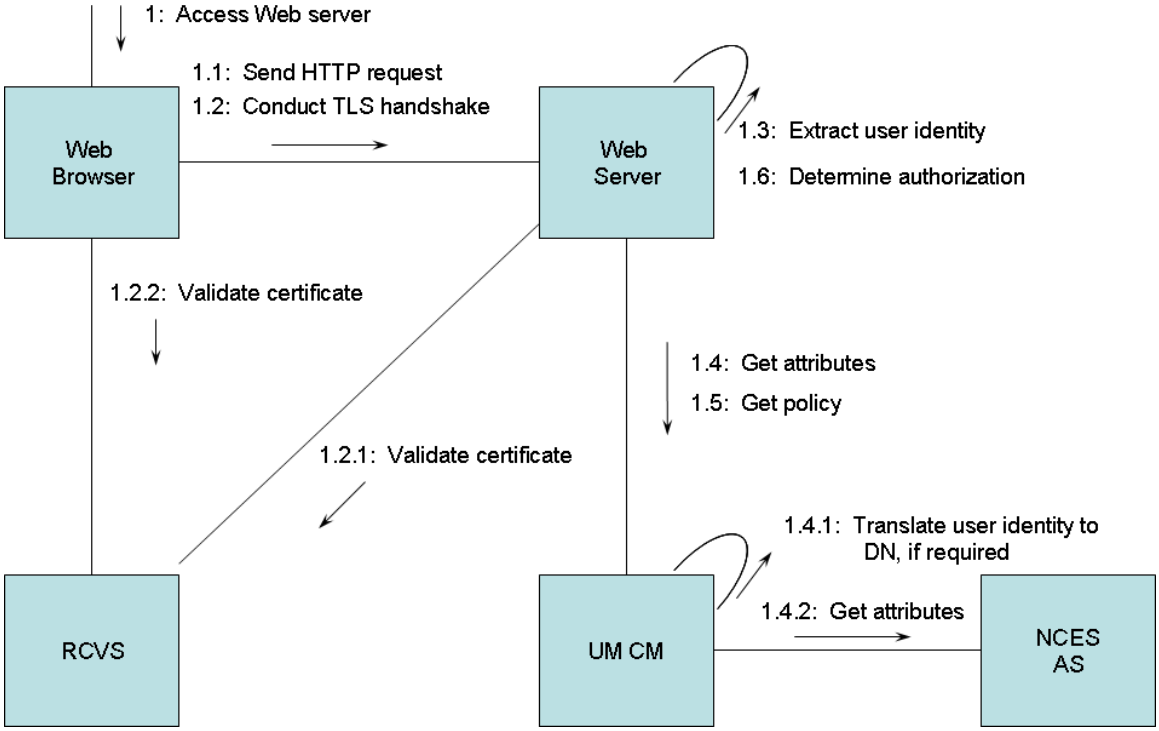

Figure 4: Web-Browser to Web Server Using User Management CM

2.5.2 Machine-to-Machine Communications Using SOAP Messages

Web service messages using SOAP shall comply with the Web Service Message (WSM) format specification as described in *Net-Centric Enterprise Services (NCES) Service Security Interface Specification*, v0.4.5 [DISA2], and *Net-Centric Enterprise Services (NCES) Service Security Design Specification for Service Security v0.4.6* [DISA1]. These documents identify the elements to be included in the SOAP message header, including a Security Assertion Markup Language (SAML) authentication assertion of the user's identity, and which elements will be digitally signed using the private key corresponding to the public key in the CP's PK-certificate.

The UM CM's PEP may be implemented as either an agent in the CP or as a gateway in front of a CP. Figure 5 shows the case in which a PEP and message handlers are included as agent software in the CP. In this case, a service consumer prepares a SOAP message requesting a service (1). The outgoing message handlers prepare the SOAP header including a time stamp, message identifier, security token, and a SAML authentication assertion and digitally sign selected portions of the message (1.1). The CP then sends the message (1.2).

The message handlers on the receiving CP authenticate the incoming SOAP message (1.3), calling the RCVS to check whether the consuming service CP's certificate has been revoked (1.3.1). Once the message is authenticated, a message handler extracts the user's identity from the SOAP header (1.4), and the PEP requests authorization (1.5). If the initiating user logged in with a user ID and password, the PEP includes the user ID in its authorization request, and the

UM CM determines the corresponding DN (1.5.1). The UM CM requests attributes from the NCES AS (1.5.2) and, using the received attributes along with local attributes and local access control policy, makes an authorization decision (1.5.3). If the request is authorized, the Service Provider CP processes the request and prepares a SOAP message with the response. The outgoing message handlers on the CP prepare the SOAP header (1.6), and the CP sends the SOAP message (1.7).

The consuming service CP's message handlers authenticate the incoming message (1.8), calling the RCVS to validate the sender's certificate (1.8.1).

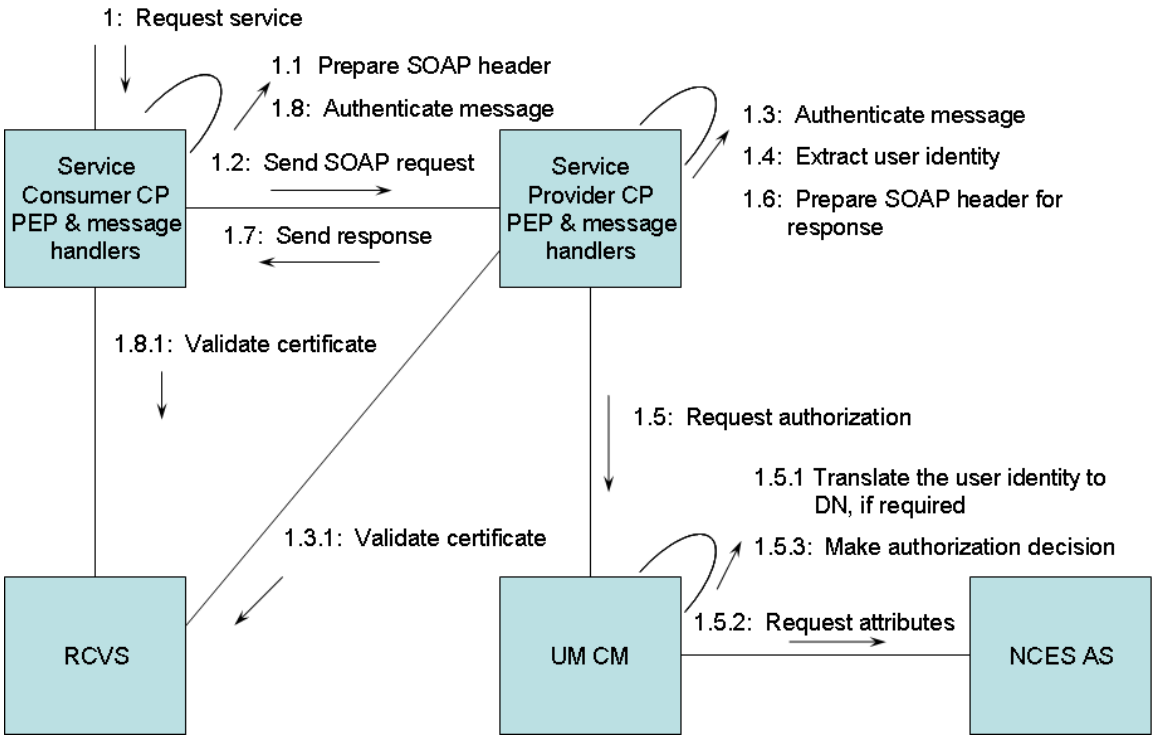

Figure 5: M2M SOAP with UM CM Agent

In Figure 6, the UM CM message handlers and PEP are implemented in a gateway. A request for service is to be sent from a service consumer CP to a service provider CP (1). The service consumer CP prepares the SOAP message requesting a service. The CP's outgoing message handler prepares the SOAP header to conform to the NCES Service Security message format (1.1) and sends the message (1.2).

The gateway intercepts the message and performs the authentication and authorization process. The gateway authenticates the message (1.3), including calling the RCVS to check whether the signing certificate has been revoked (1.3.1). The gateway extracts the user identity (1.4) and, if the user had not logged in with a PK-certificate, translates the user ID to a DN (1.4.1). The gateway then requests enterprise attributes from the NCES Attribute Service (1.5). The gateway includes authorization decision logic and uses the applicable policy and local user attributes/roles along with NCES attributes to make an authorization decision (1.6). It then sends the authorized request to the service provider CP (1.7).

The providing service executes the requested service and prepares a response in a SOAP message and sends it to the gateway (1.8). The outgoing message handlers in the gateway prepare a SOAP header (1.9) and send the message with its header to the consuming service (1.10). The receiving CP authenticates the message (1.11), including validating the certificate of the sender (1.11.1).

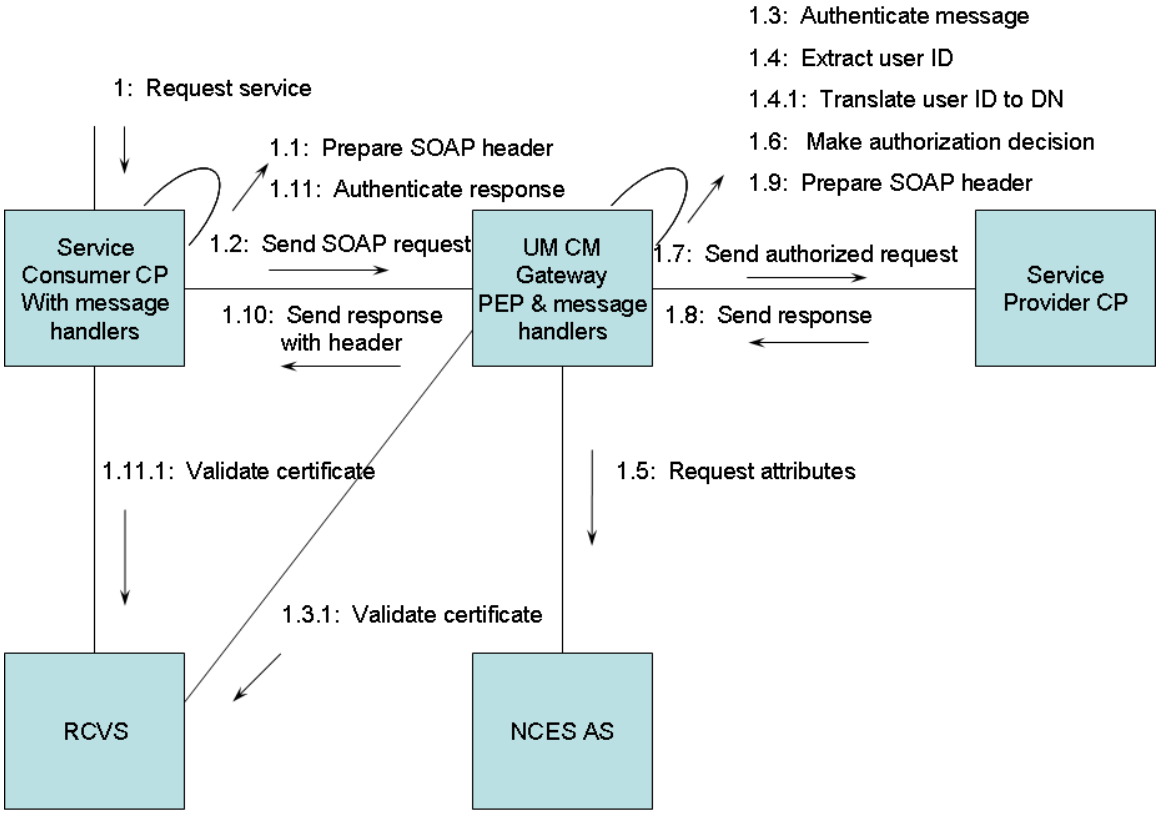

Figure 6: M2M SOAP and UM CM, Gateway

Figure 7 shows authentication and authorization in a chain of NECC services, A and B. The figure shows the sequence of events as follows:

1. The operational user logs into the web server in CP A using 2-way TLS authentication.
2. As part of the TLS handshake, the web server checks whether the user's certificate has been revoked.
3. The web server extracts the user identity and sends an authorization decision request including action to be performed and resource to be accessed to the PDS in the local UM CP. The PDS uses the applicable policy and local and JEDS attributes to make an authorization decision and return it to the web server.
4. If the authorization decision is "Permit", the web server sends a service request to service A. If the decision is "Deny", the web server sends the denial to the web browser.
5. Service A processes the service request. Since Service A needs information from Service B, it formulates a SOAP message request to Service B. It also includes a SAML assertion of the

user's identity in the SOAP message header, which is in the NCES message format. An outgoing message handler in CP A signs the SOAP message using CP A's PK-certificate.

6. The message handlers in CP B authenticate the message, which includes checking whether the CP A's certificate has been revoked.
7. The PEP/message handler extracts the user identity from the SOAP header and formulates an authorization decision request that includes the action to be performed and resource to be accessed to the PDS in the local UM CP. The PDS, using the applicable policy and local and JEDS attributes, makes an authorization decision and returns it to the PEP.
8. If the authorization decision is "Permit," the PEP sends the service request to Service B. If the decision is "Deny," CP B sends the denial to Service A, which returns it to the web browser.
9. Service B processes the service request and generates a SOAP message containing the response. It sends the response to the outgoing message handler, completes putting the message in NCES message format, and signs it using CP B's PK-certificate
10. The PEP/incoming message handlers in CP A validate the message including checking the status of signing certificate (not shown). The PEP sends an authorization decision request to the PDS if required—this is the general process for all incoming messages; however, it may be possible to forego this test since this is the response to a synchronous message. Service A uses the information received from service B and generates a response to the original request.
11. Service A sends the response to the web server.
12. The web server returns the response to the browser over the original TLS connection, or a new TLS connection.

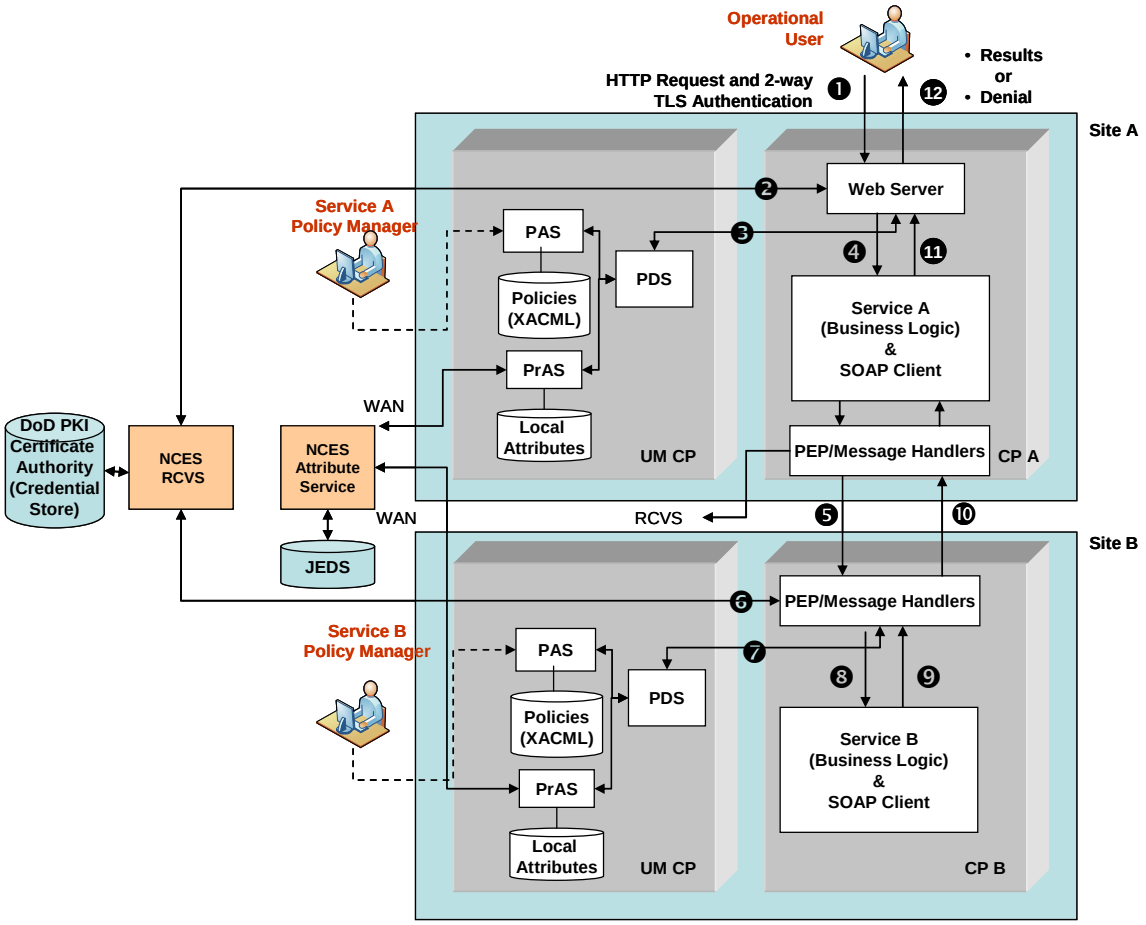

Figure 7: Authentication and Authorization in Service Chaining

2.5.3 Machine-to-Machine (M2M) Representational State Transfer (REST) Communications

REST is a term coined by Roy Fielding to describe an architectural style of networked systems. REST is an architectural style, not a standard. REST uses standards (e.g., HTTP, Uniform Resource Locator (URL), XML, Hypertext Markup Language (HTML), etc.).[2]

REST web services follow a client-server approach using a pull-based interaction style. REST is stateless, i.e., each request from a client to a server must contain all the information necessary to understand the request. All resources are accessed with a generic interface (e.g., GET, POST, PUT, and DELETE). REST-based systems are composed of resources that are named using URLs. Intermediaries, such as proxy servers, cache servers, and gateways, can be inserted between clients and resources to support performance, security, and other quality attributes. [3]

[2] COST2

[3] COST2

Security added to REST communications is generally through the use of the TLS protocol, including two-way authentication and, if required, encryption. As previously mentioned in section 2.1, TLS is point-to-point and provides limited security.

Figure 8 shows a REST transaction that uses the UM CM for authorization. In response to an HTTP request (1.1), there is a two-way TLS authentication of each CP to the other (1.2). As part of the authentication, each CP validates the status of the other CP's certificate via the NCES RCVS (1.2.1, 1.2.2). Following authentication, the Service Provider CP extracts the Service Consumer's identity from its certificate (1.3). The Service Provider then queries the UM CM to get attributes of the Service Consumer CP (1.4). The UM CM queries the NCES AS for attributes of the Consuming Service CP (1.4.1); however, at this time, server attributes are not available in the NCES Attribute Service. The Service Provider queries the UM CM to get the applicable access control policy (1.5). Note that the authorization policy must be based on the CP's attributes and not an initiating user's since the initiating user's identity is not available. To make the initiating user's identity available would require the providing service to specify a way to pass the user's identity (e.g., in a SAML assertion). Once the attributes and policy are obtained, the Service Provider CP makes an authorization decision (1.6), and processes the request if appropriate.

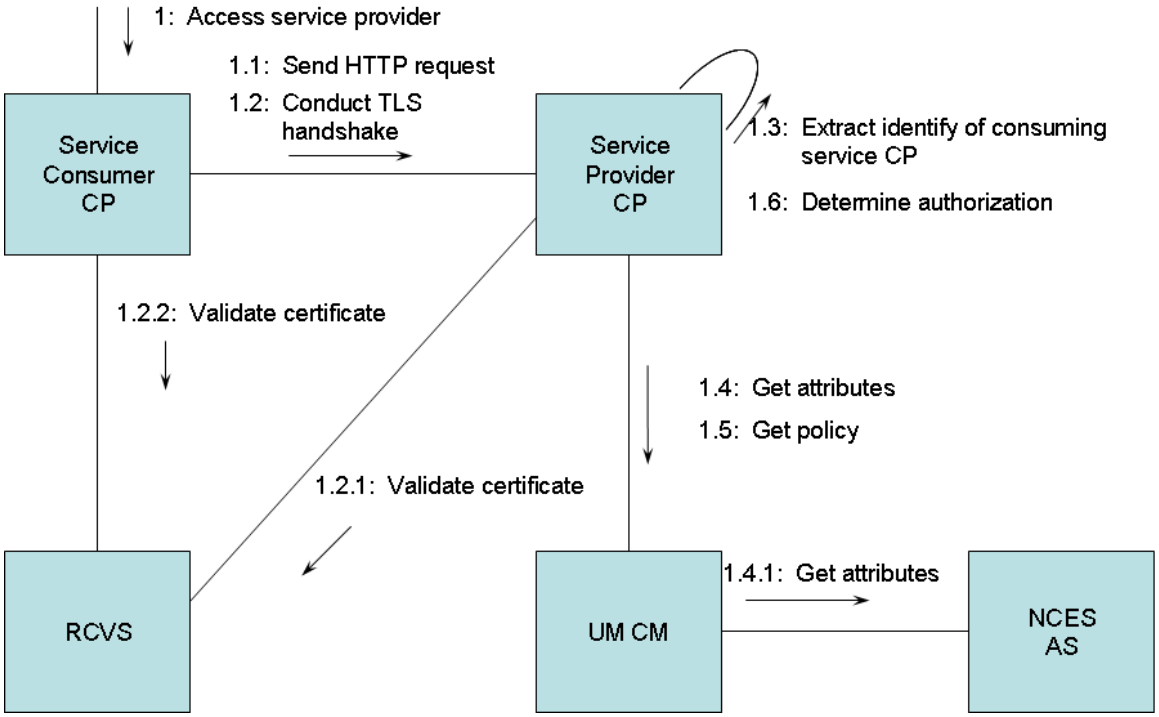

Figure 8: REST (M2M)

2.5.4 Policy Definition and Management

Figure 7 shows Policy Managers for Services A and B entering their local security policies into policy stores using PASs. This design allows for unique policies determined by the appropriate authorities (e.g., data owners) for each service, as well as enterprise authorization policies.

2.6 Role-Based Access Control /Attribute Based Access Control

Authorization policy may be based on the identity of the operational user and/or based on attributes of the user (e.g., clearance, rank, and organization). The *NCES Service Security Design Specification* describes the RBAC model as based on one attribute for a subject that is a role, while ABAC is based on many attributes for both subjects and resources and the possible combinations of the two.[4] A key element of ABAC is that the attributes are not application specific; while in RBAC, the roles may be application specific. For example, a user may have an editor role for application A, which provides the privilege of reading and updating A's data, but this does not mean that the user has an editor role for application B.

RBAC is a well-established model. The Organization for the Advancement of Structured Information Standards (OASIS) has defined an RBAC profile [OASIS1], which defines RBAC as a model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.

If authorization is based on a user's identity, the user would need to be registered before gaining access. This presents a significant problem in populating and maintaining the authorization data stores. However, if authorization is based on user attributes, the attributes of potential users need to be recorded just once and shared by PDSs. Figure 7 shows the PDSs calling PrASs, requesting the attributes for the user. Some attributes may come from enterprise databases (e.g., JEDS), while other may be unique to NECC, or local.

In NECC Increment 1, the CM Developer shall identify roles with accompanying access privileges. The NECC UM CM will be used to maintain databases of user identities and their associated roles for each CM. The business process for registering users and assigning them roles needs to be defined.

2.7 Access to Legacy Applications and Back-Office Systems

NECC CMs may require access to legacy applications and back-office systems, which have their own security policies and means of authentication and authorization. A legacy application or back-office system may require a CM to perform both authentication and authorization on its behalf, or it may require that the CM pass it the authenticated user identity so that it can perform authorization. These back-end interfaces will be addressed by the CM developers.

2.8 Audit

2.8.1 Audit Requirements

DoDI 8500.2 requires recording transactions in audit trails, and a capability for continuous monitoring of audit logs and alerting of unusual or inappropriate activity. This requires that NECC SOA request and response transactions, in addition to other activities (e.g., Operating System (OS) and database management system transactions), be auditable. CMs shall implement other audit functions allocated to them in the *DIACAP Implementation Plan*.

[4] DISA1, sec. 5.4.1.2

2.8.2 Audit Concept

Figure 9 illustrates the concept for collecting, storing, analyzing, and reporting audit data. Since SOAP request and response transactions take place at the application layer and in a virtual machine, these transactions will be recorded by message handlers in the UM CM. REST and user access to web server transactions will be recorded by the appropriate CM.

Generally, audit data is held on the collecting platform for a limited time, after which it is stored elsewhere in accordance with a system's security policy. The NECC audit logs will be sent to the hosting operational node's operations center and copies sent to the NECC JTOCC. The operational node will be responsible for reporting, including reporting to the Joint Task Force – Global Network Operations (JTF-GNO).

In order to be able to correlate audit logs collected at different locations, clocks in the GCNs shall be synchronized.

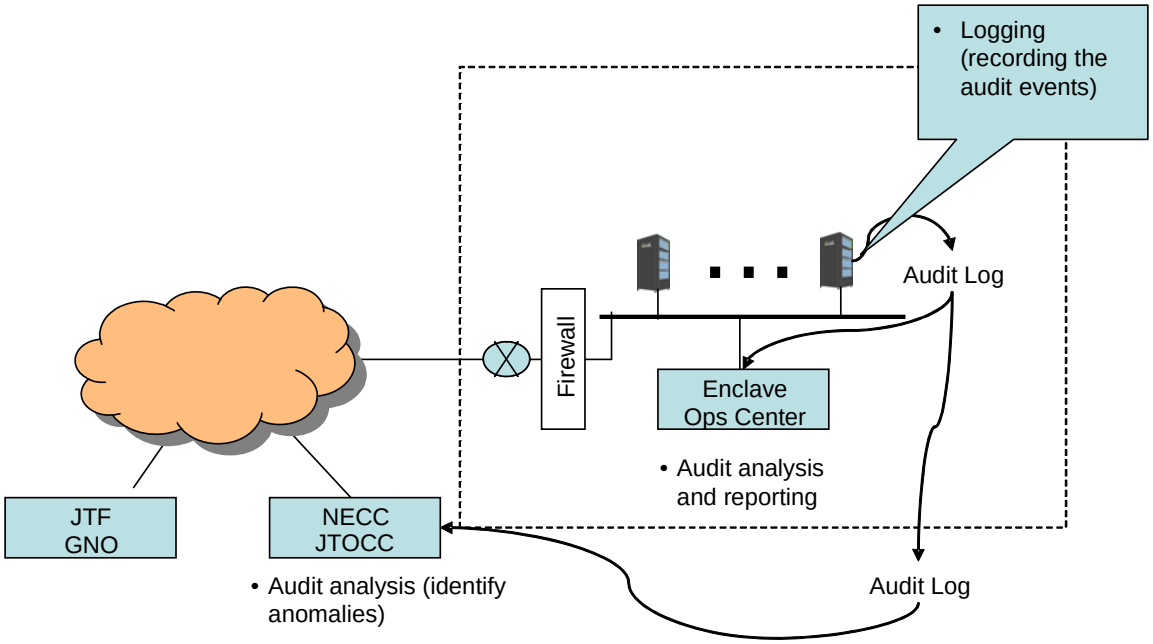

Figure 9: Audit Concept

2.9 Confidentiality

DoDI 8500.2 defines controls to achieve confidentiality of data in transit and data at rest. In either case, information owners identify the need for confidentiality protection beyond that provided by the network and environment (that is for need-to-know protection). The *DIACAP Implementation Plan* addresses the allocation of controls to the CM developer, host organization, operational node, or host system.

2.9.1 Confidentiality of Data in Transit

DoDI 8500.2 defines encryption requirements for National Institute of Standards and Technology (NIST)-certified or National Security Agency (NSA)-approved cryptography for

protecting data in transit requiring need-to-know protection. This is encryption to separate data based on defined Communities of Interest (CoI) or based on special requirements levied by the data owner; it would normally be by exception rather than by default.

The *NCES Service Security Design Specification* points out that when required to counter identified threats, two general options are available to achieve confidentiality for service messages: (1) rely on underlying communications security (e.g., physical layer or transport layer encryption); or (2) encrypted SOAP messages. Due to performance concerns in message level encryption, the transmission confidentiality techniques shall be used.[5]

2.9.2 Confidentiality of Data at Rest

DoDI 8500.2 and DoD Chief Information Officer (CIO) Memorandum, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media," 3 July 2007 define encryption requirements for protecting the confidentiality of data at rest. File and/or media encryptors will be used as required.

2.10 Integrity

The *National Information Assurance (IA) Glossary* [CNSS1] defines integrity as the quality of an information system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data. Also, in a formal security mode, integrity is interpreted more narrowly to mean protection of unauthorized modification or destruction of information.[6]

DoDI 8500.2 defines a number of controls to provide integrity. These controls include administrative functions such as establishing control boards, design functions such as developing and maintaining a functional architecture, and other functions such as protection against malicious mobile code, and use of best practices. These controls will be allocated to the CM developer or host, in accordance with the *DIACAP Implementation Plans*.

Providing the ability to detect when information has been tampered with is another view of integrity. O'Neill states that such data integrity relies on hashing algorithms.[7] The integrity and confidentiality of SOAP messages is provided by compliance with the OASIS WS-Security specifications. Digital signatures provide message integrity since intended recipients of the data can use the digital signature to verify that the data has not been altered.[8] REST transactions will be done over TLS connections providing data integrity. In addition, best practices call for CMs to implement validation of input data.

---

[5] DISA1, C.1

[6] CNSS1

[7] ONEILL1, p. 27

[8] OASIS3, p. 11

2.11 Availability

The *National Information Assurance (IA) Glossary* [CNSS1] defines availability as timely, reliable access to data and information services for authorized users. DoDI 8500.2 Controls for a MAC I Classified system include controls for availability. These controls will be allocated to the CM developer, or host in accordance with the *DIACAP Implementation Plan*.

Specifically related to web service availability, the NIST Special Publication (SP) 800-95, *Guide to Secure Web Services* [NIST2] includes best practices for addressing availability. The guide describes approaches to the design, implementation, and sustainment (operation and maintenance) of a web service that will increase its ability to recognize, resist, and recover from Denial of Service (DoS) attacks.

The *Guide to Secure Web Services* summarizes as follows:

> "Availability is increasingly becoming a concern with web services, so Quality of Service (QoS) is becoming increasingly important. For mission critical applications to be built with the SOA paradigm, the SOA must be able to withstand one or more services becoming unavailable, either due to a DoS or a failure. Web services' support for dynamic discovery and binding allows for failover web services to be accessed when a DoS occurs. Similarly, reliable messaging technologies can be used to ensure that messages will be received in spite of a DoS attack. Finally, QoS technologies can be used to prioritize web service traffic so that high priority web services will still remain functional in the face of an attack on the availability of the network."[9]

2.12 Web Service Provider Implementation of the Virtualized Environment

Figure 10 shows the virtualized environment on a GCN and security related software that will be included in each CP. The incoming and outgoing message handlers are part of the UM CM. They may be part of an external gateway or installed as software agents in the CP depending on the UM CM implementation. HBSS software shall be installed in the CP. In addition, all applicable trust anchor certificates for validating that incoming certificates have been signed by a trusted signer shall be installed in the CP. Also, when a CP is installed on a GCN, a server certificate shall be installed.

[9] NIST2 p. 3-44

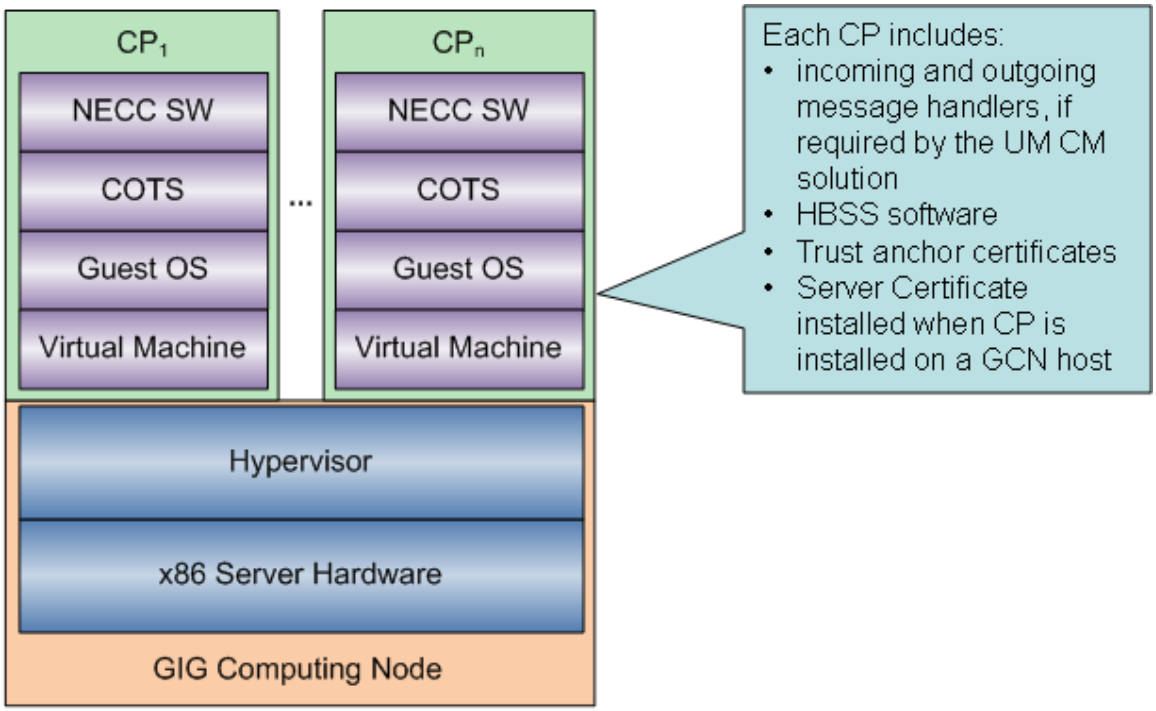

Figure 10: The Virtualized Environment

2.13 Data Marking and Labeling

2.13.1 Requirements

The NECC Capability Development Document (CDD) requires that NECC "enable information producers to describe their products accurately using established search words and descriptions, and label them using standardized metadata (including classification)."[10] DoDI 8500.2 includes requirements to mark/label data that is not approved for public release. "Marking" typically refers to the physical marking of hardcopy output – or human readable marking of an onscreen display. "Labeling" typically refers to the electronic tagging of data elements, usually in a machine readable format. The marking/labeling reflect the classification or sensitivity level, if applicable, and any special dissemination, handling, or distribution instructions. It also requires that mechanisms are in place to assure the integrity of labels on transmitted information.

2.13.2 Approach

The NECC Data Strategy calls for data to be labeled in accordance with the IC Information Security Marking (IC ISM) XML schema. It also plans for a "Tearline Approach," which is modeled on the IC's "Tearline" concept. The data labeling has the potential for enabling automated dissemination.

[10] DoD3, sec 6.1.4

2.14 Computer Network Defense (CND)

CND consists of actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and networks.[11]

2.14.1 Requirements

Requirements for CND include both monitoring and implementing defense-in-depth. There must be robust infrastructure and IA practices, such as vulnerability analysis and assessment, and dissemination and compliance process for IA advisories and alerts.

2.14.2 Approach to Intrusion Detection Monitoring, Analysis, and Reporting

Figure 11 shows the concept for CND. Within an operational node, host monitoring mechanisms are placed on the GCN. These mechanisms are monitoring systems such as HIDS that are included in the CPs. Monitoring, analysis, and reporting will be done in accordance with the operational node procedures, but copies of the reports will also be sent to the JTOCC. The strategy for implementing Intrusion Detection needs to be flexible enough to support operational sites and Local GCNs that may have a different Intrusion Detection System (IDS) reporting hierarchy.

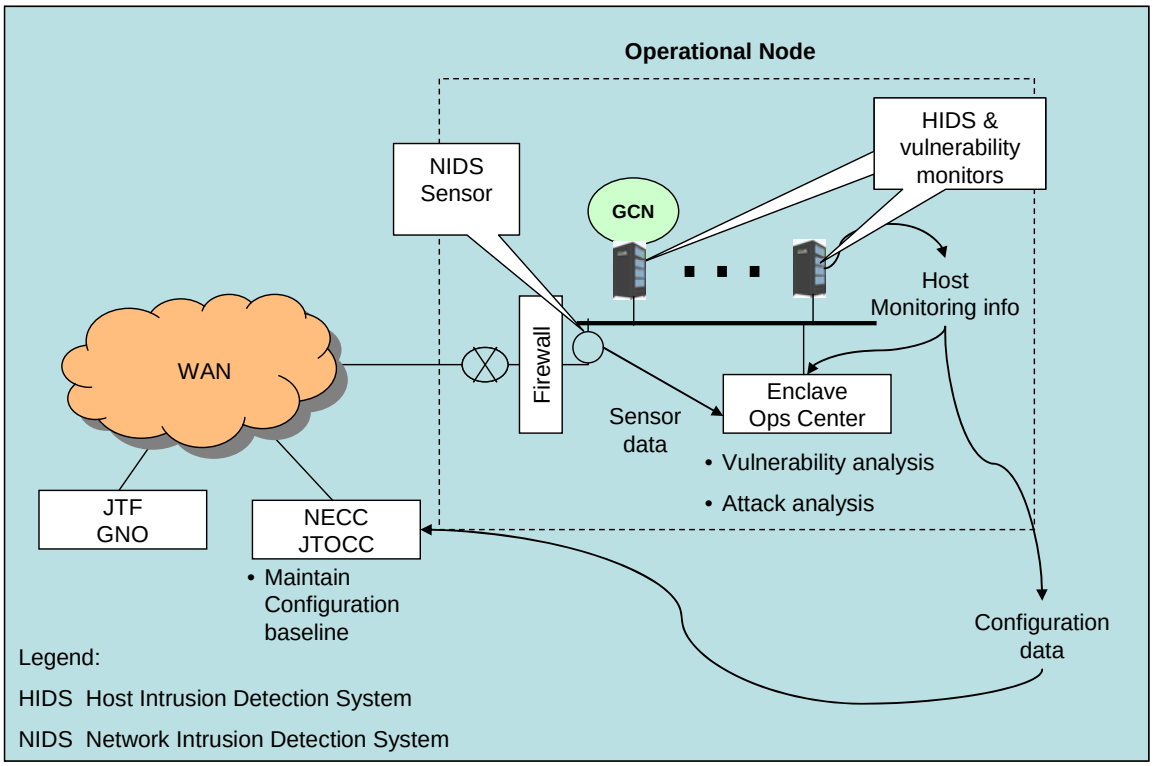

Figure 11: CND Concept

JTF-GNO CTO 07-12, "Deployment of the Host Based Security System (HBSS)," identifies the requirement for installing standard security software (including HIDS) on hosts, and includes a

[11] DoD6, E2.1.12

waiver process. If certain sites have received a waiver, the Component Program Management Office (CPMO) developers must obtain this information so that they can prepare CPs that do not have the waived software installed or do not use the software.

2.14.3 Approach to Vulnerability Analysis and Assessment

HBSS includes agent software to monitor system configurations for vulnerabilities, e.g., whether security patches have been installed. The operational nodes will follow their procedures for use of the agents, with the additional requirement to inform the NECC JTOCC so that it can maintain the configuration baseline including status of installation of patches.

2.14.4 Approach to Defense-in-Depth

Defense-in-depth may be viewed as including network and infrastructure protection, enterprise security management, server and desktop platform protection, and applications and data protection. The firewall policies for sites hosting NECC CMs will need to be coordinated with NECC required flows to ensure that NECC ports and protocols are consistent with the firewall policies. In addition, encryption of NECC data in transit will need to be coordinated with host site firewall and network monitoring policies.

NECC ports and protocols shall be consistent with the DoD standard, (DoDI 8551.1, *Ports, Protocols, and Services (PPS) Management),* which should be the expectation for host operational nodes. NECC authorized exceptions to the DoD PPS shall be documented so that host operational nodes can modify their firewall policy, if appropriate, to allow authorized NECC work flows.

Protection against web service attacks is not generally provided by common firewalls and IDSs; consequently, operational nodes may choose to install XML firewalls to protect their resources including NECC CPs. In addition, commercial XML firewalls are potential candidates for the UM CM. If an XML firewall is the choice for UM CM, it would be provisioned by NECC for that express purpose. This would be done consistently by NECC and would not be an operational node's decision.

CMs must address the DoD standard packages for CND including antivirus, antispyware, configuration validation, remediation, and host-based security.

2.15 Joint Technical Operations Control Capability Security

Figure 12 shows security-related data flows for the JTOCC.

A NECC procedure for managing IAVA patches will be developed. This procedure will address testing, installing, and monitoring the status of IAVA patches. At this time it is envisioned that:

- CM providers will test the patches via the Federated Development and Certification Environment (FDCE) and, if the patches break a CM, update the CM so that the patch may be applied.[12]
- The CP Configuration Item (CI) in the JTOCC-maintained Definitive Software Library (DSL) will then be updated to include the patch.

[12] The question of who does testing of IAVA patches will be coordinated with Technical Operations architecture

- The JTOCC will then distribute the tested patches to the GCNs at the operational nodes, and then update the installed baseline information to reflect the status of patches.
- The host operational nodes will scan for installation of patches and report in accordance with established procedures and also inform the JTOCC of the results of scans of the NECC CPs.

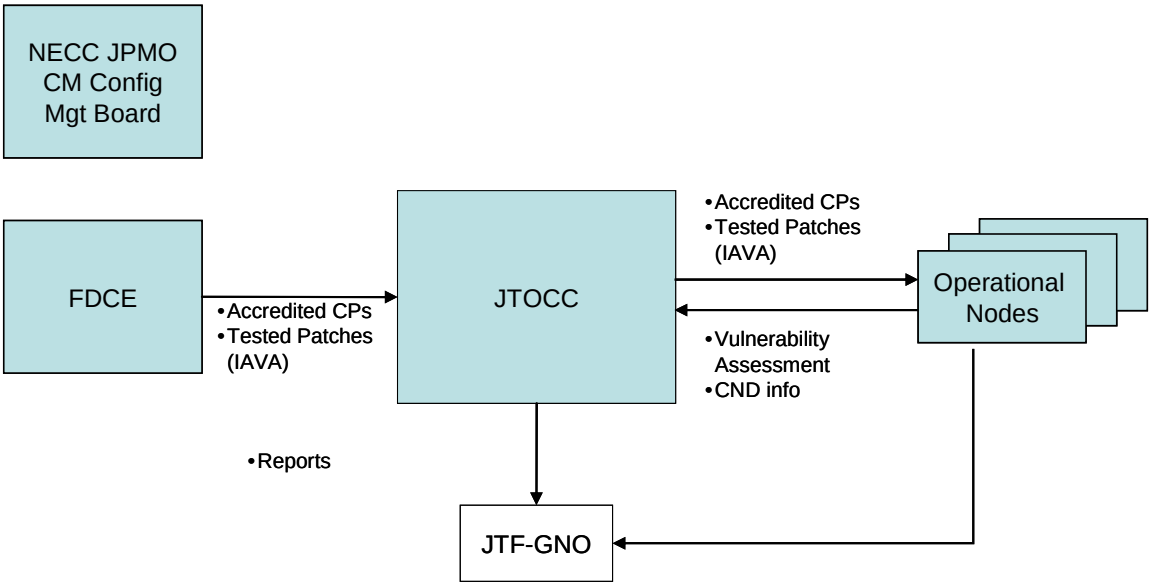

Figure 12: JTOCC Security Data Flows

2.16 Cross Domain Enterprise Services

2.16.1 Requirement

NECC cross domain requirements include the capability to exchange information across multiple security domains. This includes Top Secret/SCI, Top Secret, Secret, Unclassified, Joint, IC, DoD and non-DoD Agencies, and multinational components. Capability for low-to-high and high-to-low information exchange (point-to-point) is required. The threshold requirement is for the following data formats: email with attachments, text, graphics, and imagery. The objective requirement is for collaboration via: text chat, web -browsing, whiteboard, and shared applications.[13]

2.16.2 Approach

Some cross domain requirements are feasible using existing CDS technology, while others require development of enhanced technology. The NECC Joint Program Management Office (JPMO) will work with the NSA and the Defense Information Systems Agency (DISA) to define requirements for future CDSs.

The current process for validating requirements for cross-domain data flows will be followed on a case-by-case basis in accordance with current policies (e.g., Chairman of the Joint Chiefs of Staff (CJCS) Instruction 6211.02B). In other words, if a CM requires moving data from one

[13] DoD7, 9.2

domain to another, this requirement will be validated and prioritized by the appropriate process. It is expected that future Capability Definition Packages (CDPs) will identify requirements for specific cross-domain information flows. Once the requirement for a cross-domain flow is validated, engineering resources from DISA and/or NSA will be assigned to devise a solution.

A candidate solution is to use enterprise cross-domain services. DISA and the Defense Intelligence Agency (DIA) currently operate cross-domain capabilities. DISA is establishing a Cross-Domain Enterprise Service that provides a family of solutions to move data between the NIPRNet and SIPRNet. Use of such a service shortens the time to approval for adding a cross domain data flow to an operational CDS and relieves the users of the burden of operations and management of the CDS. The Unified Cross-Domain Management Office (UCDMO) and the Defense Information System Network (DISN) Security Accreditation Working Group (DSAWG) are interested in ensuring the service is used where appropriate.

The DIA Regional Service Centers (RSC) provide cross-domain services to move data to/from SCI networks.

The NSA is developing future CDS technology in response to identified needs (e.g., to support web services and XML). In addition, NSA has published *XML Schema Guidance for Cross Domain Security Policy Enforcement.*[14]

2.17 Multinational Information Sharing (MNIS)

2.17.1 Requirement

Multinational Information Sharing (Increment 1) includes the following requirement:

- NECC shall provide efficient, effective, and accreditable solutions for the connection of Multinational Information Sharing (MNIS) Combined Enterprise Regional Information Exchange System (CENTRIXS) networks to US networks, and between/within various MNIS CENTRIXS network security and information domains.
- Integration of GIG Enterprise Services (GES)-based capability into NECC Mission Capability Packages (MCPs). (THRESHOLD)[15]

2.17.2 Approach

The approach to addressing this requirement is the same as that in section 2.16

3 IMPLEMENTATION

3.1 Access Control

Full ABAC as an enterprise capability is not expected during the Increment 1 time frame. ABAC depends on populated user attribute stores with appropriate attributes for making authorization decisions. There are ongoing activities to define a set of common attributes and identifying authoritative sources; however, these are not planned to be available during NECC Increment 1. The UM CM will provide for a policy database containing permissions based on

[14] NSA3

[15] DoD7, 9.6.2

roles defined on a per CM basis and attributes available from JEDS via the NCES Attribute Service. The attributes available from JEDS may not be applicable to the access control policy for any given CM. The access control policy for a CM must be determined in coordination with the data owners for all data used by the CM.

3.2 Implementation Best Practices

Developers should follow best practices (e.g., NIST SP 800-95) during CM development and testing. This includes ensuring that applicable IAVA patches and applicable STIGs are applied during development to comply with DoD requirements and reduce the likelihood of failing security testing.

3.3 Publication of Services and Establishing Trust

It is necessary to ensure that all services published to a service registry have been properly validated and accredited. The FDCE process is intended to validate services and support accreditation of CPs.

3.4 Server Public Key Certificates

Servers require PK-certificates for use in public-private key encryption and digital signatures. Such certificates are obtained from the appropriate PKI and installed when the CP is provisioned to a GCN. Given the virtualization approach employed by NECC, each CP is treated as a server and requires a PK-certificate.

3.5 Summary of Requirements for CM Developers

The following list summarizes the IA-driven requirements for CM developers. This list does not substitute for reading this architecture description or coordinating planned implementation with the Designated Approving Authority (DAA).

- The CP shall address all requirements allocated to it in the *DIACAP Implementation Plan.*
- SOAP messages shall comply with NCES message format specifications. The UM CM will provide message handlers to implement this requirement. (sec. 2.5.2)
- The UM CM agent software shall be installed in the CP, if applicable. (The UM CM may be implemented as an external gateway or proxy, in which case this requirement would not apply.) (sec. 2.5.2)
- TLS two-way authentication shall be used for REST transactions. (sec. 2.5.3)
- The CM Developer shall ensure that access control policies of the data owners are addressed.
- The CM Developer shall identify roles with accompanying access privileges. (sec. 2.6)
- CM developers shall address interface requirements to back-office systems and legacy applications (sec. 2.7)
- CM developers shall implement audit functionality as identified in the *DIACAP Implementation Plan.* REST and user access to web server transactions will be recorded by the appropriate CM. (sec. 2.8)

- Clocks in platforms on which CPs are installed shall be synchronized with NECC standards. (sec. 2.8.2)
- When need-to-know protection of data in transit is required, transmission confidentiality techniques shall be used. (sec. 2.9.1)
- The CM should validate input data as a best practice. (sec. 2.10)
- The CM developer should address best practices described in NIST SP 800-95. (sec. 2.11)
- The designated HBSS software shall be installed in the CP. (sec. 2.12)
- All applicable trust anchor certificates shall be installed in the CP. (sec. 2.12)
- When a CP is installed on a GCN, a server certificate shall be installed within the CP. (sec. 2.12)
- CMs shall conform to the NECC Data Strategy with respect to security labeling. (sec. 2.13.2)
- All ports or protocols used shall be compliant with the DoD standard, (DoDI 8551.1, *Ports, Protocols, and Services (PPS) Management)*. (sec. 2.14.4)
- Firewall policies for sites hosting NECC CPs shall be coordinated with NECC required flows to ensure that NECC ports and protocols are consistent with the firewall policies. (sec. 2.14.4)
- Encryption of NECC data in transit shall be coordinated with host site firewall and network monitoring policies. (sec. 2.14.4)
- Applicable IAVA patches and applicable STIGs should be applied during development to comply with DoD requirements and reduce the likelihood of failing security testing. (sec. 3.2)
- Mechanisms for encrypting and signing messages, and implementing TLS shall comply with applicable Federal Information Processing Standards. (sec. C.2)

3.6 Summary of Architectural Requirements for Host Providers

- The operational node shall address all requirements allocated to it in the *DIACAP Implementation Plan.*

3.7 Waiver Process

Under certain circumstances materiel developers may request waivers and the JPMO may grant waivers for compliance with the specifications contained in this document. Some specifications and standards can be waived, some cannot be waived, and some can be waived for a limited period of time.

In accordance with security policy and the *NECC Acquisition IA Strategy*, the Certification Authority (CA) and DAA will evaluate IA-related waiver requests and can approve the tailoring of the IA requirements.[16] This will be accomplished by identifying the requirements for a CM in

[16] NJPMO1, sec. 7

its *DIACAP Implementation Plan* and obtaining stakeholder including the DAA, the Certification Authority, the data owners, and the user representative agreement in accordance with the NECC certification and accreditation process.

4 CONCLUSIONS

This document describes the major NECC IA architecture concepts and implementation guidance applicable for NECC Increment 1. This document discusses SOA security realized through the use of WS-Security as defined in the NCES security design, PKI, NCES security services, and security services provided by the UM CM. In addition, this document describes the approach to securing CPs through the use of controls in the CP and controls implemented by the operational node.

5 POLICY/DIRECTIVES

DoDI 8500.2 defines required security controls for information systems and applies to NECC implementations on NIPRNet and SIPRNet. DCID 6/3 defines security requirements for information systems processing SCI and Special Access Programs (SAP), and applies to NECC implementations in SCI environments. The controls and/or requirements must be allocated to operational nodes, hosts, and NECC CMs as part of the implementation process.

The following is a list of policies and guidance that may be applicable to CMs:

- Department of Defense Directive (DoDD) 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 5 May 04
- DoDD 5000.1, The Defense Acquisition System, 12 May 03
- DoD Directive (DoDD) 8500.1, Information Assurance (IA)
- DoDI 8550.2, Information Assurance (IA) Implementation
- DoDI 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling
- DoDI 8551.1, Ports, Protocols, and Services Management
- DoDI 8552.01, Use of Mobile Code Technologies in DoD Information Systems
- DoDD O-8530.1, Computer Network Defense (CND)
- Chairman of the Joint Chiefs of Staff (CJCS) Instruction 6211.02B, Defense Information System Network (DISN): Policy, Responsibilities and Processes
- CJCS Instruction 6510.01D, Information Assurance (IA) and Computer Network Defense (CND)
- DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems
- NSA System and Network Attack Center (SNAC) guides
- DISA Field Security Office: Security Technical Implementation Guides (STIGs)
- DoD CIO Memo, “Interim DoD Information Assurance Certification and Accreditation Process Guidance (DIACAP),” July 6, 2006.
- DoDD 8500.1, Information Assurance, 24 Oct 02

- DoDD 8570.1, Information Assurance Training, Certification, and Workforce Management, August 15, 2004
- DoDI 4630.8, Procedures for Interoperability and Supportability of IT and NSS, 30 Jun 04
- DoDI 5000.2, Operation of the Defense Acquisition System, 12 May 03
- DoDI 8500.2, Information Assurance Implementation, 6 February 03
- DoD CIO Memorandum, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media," 3 July 2007
- National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products," Jan 00

APPENDIX A – ACRONYMS

Acronym	Definition
ABAC	Attribute-Based Access Control
AS	Attribute Service
C2	Command and Control
CA	Certificate Authority
CDD	Capability Development Document
CDP	Capability Definition Package
CDS	Cross Domain Solution
CENTRIXS	Combined Enterprise Regional Information Exchange System
CI	Configuration Item
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CL	Confidentiality Level
CM	Capability Module
CND	Computer Network Defense
CoI	Community of Interest
COTS	Commercial off-the-Shelf
CP	Capability Package
CPMO	Component Program Management Office
CRL	Certificate Revocation List
CRUD	Create, Read, Update, Delete
CTK	Conformance Test Kit
DAA	Designated Approving Authority
DCID	Director of Central Intelligence Directive
DIA	Defense Intelligence Agency
DIACAP	Department of Defense (DoD) Information Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DISR	DoD Information Technology Standards Registry
DN	Distinguished Name
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	DoD Instruction
DoS	Denial of Service
DRM	Digital Rights Management
DSAWG	DISN Security Accreditation Working Group
DSL	Definitive Software Library

Acronym	Definition
FDCE	Federated Development and Certification Environment
GCN	GIG Computing Node
GES	GIG Enterprise Service
GIF	Graphics Interchange Format
GIG	Global Information Grid
GUI	Graphical User Interface
HBSS	Host Based Security System
HIDS	Host Intrusion Detection System
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IA	Information Assurance
IAS	Information Assurance Strategy
IAVA	Information Assurance Vulnerability Alert
IC	Intelligence Community
IC ISM	Intelligence Community Information Security Marking
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
ISM	Information Security Marking
IT	Information Technology
JEDS	Joint Enterprise Directory Services
JPEG	Joint Photographic Experts Group
JPMO	Joint Program Management Office
JTF-GNO	Joint Task Force - Global Network Operations
JTOCC	Joint Technical Operations Control Capability
M2M	Machine-to-Machine
MAC	Mission Assurance Category
MCP	Mission Capability Package
MNIS	Multinational Information Sharing
NCES	Net Centric Enterprise Services
NECC	Net-Enabled Command Capability
NIPRNet	Unclassified but Sensitive Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSP	National Security Telecommunications and Information Systems Security Policy
OASIS	Organization for the Advancement of Structured Information Standards
OS	Operating System
PAS	Policy Administration Service
PDP	Policy Decision Point

Acronym	Definition
PDS	Policy Decision Service
PEP	Policy Enforcement Point
PK	Public Key
PKI	Public Key Infrastructure
PPS	Ports, Protocols, and Services
PrAS	Principal Attribute Service
PRS	Policy Retrieval Service
QoS	Quality of Service
RBAC	Role Based Access Control
RCVS	Robust Certificate Validation Service
REST	Representational State Transfer
RSC	Regional Service Center
RSS	Really Simple Syndication
SAML	Security Assertion Markup Language
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SIPRNet	Secret Internet Protocol Router Network
SOA	Service Oriented Architecture
SOAP	SOAP is no longer an acronym; it originally stood for: Simple Object Access Protocol
SP	Special Publication
STIG	Security Technical Implementation Guide
TLS	Transport Layer Security
UCDMO	Unified Cross Domain Management Office
UDDI	Universal Description, Discovery, and Integration,
UM CM	User Management Capability Module
URL	Uniform Resource Locator
VM	Virtual Machine
W3C	World Wide Web Consortium
WAN	Wide Area Network
WSDL	Web Services Description Language
WSM	Web Service Message
WSS	Web Services Security
WS-Security	Web Services - Security
XACML	eXtensible Access Control Markup Language
XKMS	XML Key Management Specification
XML	eXtensible Markup Language

APPENDIX B – LEXICON

TERM	DEFINITION
Access Control	Limiting access to information system resources only to authorized users, programs, or processes, or other systems[17]
Attribute Based Access Control (ABAC)	Access control based on policies (access rules) that use attributes. Access Rules determine whether a subject with attributes (x1, x2) can access resource y to perform z. Attribute Based Access Control (ABAC) is based on many attributes for both subjects and resources and the possible combinations of the two.[18]
Authentication	Security measure designed to establish the validity of a transmission, message, or originator or a means of verifying an individual's authorization to receive specific categories of information[19]
Authorization	Access privileges granted to a user, program, or process[20]
Enclave	Collection of computing environments that is connected by one or more internal networks and is under the control of a single authority and security policy.[21]
Integrity	Quality of an information system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data. Note that in a formal security mode, integrity is interpreted more narrowly to mean protection of unauthorized modification or destruction of information.[22]
Labeling	Electronic "tagging" of data elements in a machine readable format to support automated access or release decisions.
Marking	Typically used to mean the physical marking of hardcopy output – or human readable marking of an onscreen display.
Mission Assurance Category	Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the war fighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The DoD has three defined mission assurance categories: MAC I, II, and III[23]
Mission Assurance Category I (MAC I).	Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

[17] CNSS1

[18] DISA1, sec. 5.4.1.2

[19] CNSS1

[20] CNSS1

[21] DoD2, E3.4.1.2

[22] CNSS1

[23] DoD2 E2.1.38.

TERM	DEFINITION
Mission Assurance Category II (MAC II).	Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure assurance.
Mission Assurance Category III (MAC III) .	Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices
Policy Decision Point (PDP)	The system entity that evaluates applicable policy and renders an authorization decision.[24]
Policy Enforcement Point (PEP)	The system entity that performs access control, by making decision requests and enforcing authorization decisions.
REST	Architectural style for developing web services based on defined set of standards, which includes HTTP, URL, XML, HTML, GIF, and JPEG. REST web services follow a client-server approach using a pull-based interaction style. REST services are stateless, i.e., each request from a client to a server must contain all the information necessary to understand the request. All resources are accessed with a generic interface (e.g., GET, POST, PUT, and DELETE). The system is composed of resources that are named using a URL. Intermediaries, such as proxy servers, cache servers, gateways, etc., can be inserted between clients and resources to support performance, security, etc.
Role	A job function within the context of an organization that has associated semantics regarding the authority and responsibility conferred on the user assigned to the role[25]
Role Based Access Control (RBAC)	A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.[26] The RBAC model is based on one attribute for a subject that is a role.[27]
RSS	Lightweight technology for disseminating notification information. The notification typically contains a link to another document which has the "full story." An RSS document is a simple XML document that contains brief descriptions of news, i.e., the headline, and a link back to the full story, i.e., the article.[28]
SOAP	A way for a program running in one kind of operating system (such as Windows 2000) to communicate with a program in the same or another kind of an operating system (such as Linux) by using the World Wide Web's HTTP and its XML as the mechanisms for information exchange.[29]

[24] OASIS2, p. 8

[25] OASIS1, sec. 1.2

[26] OASIS1, sec. 1.2

[27] DISA1, sec. 5.4.1.2

[28] COS1

[29] SRCH1

TERM	DEFINITION
Web Services	XML applications mapped to programs, objects, or databases or to comprehensive business functions. Using an XML document created in the form of a message, a program sends a request to a web service across the network, and, optionally receives a reply, also in the form of an XML document. Web services standards define the format of the message, interfaces, conventions, and mechanisms for publishing and discovering web services.[30]
XACML	XACML (Extensible Access Control Markup Language) is an open standard XML-based language designed to express security policies and access rights to information for web services, Digital Rights Management (DRM), and enterprise security applications.

[30] NEWC1, p. 2

APPENDIX C – STANDARDS

C.1 Encryption:

FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*.

C.2 Transport Security

TLS 1.0

C.3 NCES Security Standards and Profiles

Each CM that uses web service SOAP messages shall comply with the Web Service Message format specification as described in *Net-Centric Enterprise Services (NCES) Service Security Interface Specification*, v0.4.5 [DISA2], and *Net-Centric Enterprise Services (NCES) Service Security Design Specification for Service Security v0.4.6* [DISA1].

The following lists NCES Service Security standards and profiles that are to be used in NECC.

BODY	SPECIFICATION	VERSION	NOTE
W3C	SOAP	1.2	
W3C	WSDL	1.1	
OASIS	UDDI	3.0.2	
WS-I	WS-Interoperability	Basic Profile 1.2	
OASIS	XACML	1.1	Although DISA1 does not include XACML 2.0, it is expected that XACML 2.0 will be used for PEP-PDS communications in the future.
OASIS	SAML	1.1 & 2.0	
W3C	XML Signature	W3C Recommendation 2002-02-12	
W3C	XKMS 2.0	W3C Recommendation 2005-06-28	
OASIS	WSS	1.1 – Core Specification 1.1 – X.509 Token Profile 1.1 – SAML Token Profile	
IETF	RFC 2459		X.509 certificate must be validated in accordance with RFC 2459

C.3.1 SOAP

For secured communications, Service Security utilizes SOAP messages that are secured in accordance with the WSS core specifications, the SAML specification, and the proposed WSS SAML Interoperability Scenarios draft document (WSS-SAML-I). In addition, XML Signature is utilized for digitally signing SOAP messages.

The rules for preparing a SOAP message are defined in [DISA1] section 7.2.1.1, “Message Sender Processing Rules.”

The rules for recipients of SOAP messages are defined in [DISA1] section 7.2.1.2.1, “Message Recipient Processing Rules.”

C.3.2 WSDL

The Web Services Description Language (WSDL) for Service Security interfaces is defined using the WSDL 1.1 specification. An example WSDL is provided in [DISA1] section 7.2.2.

C.3.3 XACML

See [DISA1] section 7.2.5.

C.3.4 SAML

See [DISA1] section 7.2.6 for NCES profile of SAML Authentication Assertions, Attribute Requests, Attribute Assertions, Authorization Decision Requests, and Authorization Decision Assertions.

C.3.4 XML Signature

The Service Security XML Signature profile is defined in the processing rules for message senders and recipients in [DISA1] section 7.2.7.

C.3.4 WSS

All NECC SOAP messages must be secured in accordance with the WSS specifications The NCES Service Security WSS profile is defined in the processing rules for message senders and recipients in [DISA1] section 7.2.8.

C.4 NECC IA Standards

NECC will comply with IA standards specified in the DoD Information Technology Standards Registry (DISR) online**.**

APPENDIX D – REFERENCES

Committee on National Security Systems (CNSS)

CNSS1 CNSS Instruction No. 4009, *National Information Assurance (IA) Glossary*, June 2006 http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

Director of National Intelligence (DNI)

DNI1 DNI Office of the Chief Information Officer, "Certification and Accreditation Transformation," February 2007

DCI DCI Directive 6/3, *Protecting Sensitive Compartmented Information within Information Systems*, 23 December 2003 (Unclassified//For Official Use Only)

Department of Defense (DoD)

DoD1 DoD Instruction (DoDI) 8510.bb, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, DRAFT

DoD2 DoDI 8500.2, *Information Assurance (IA) Implementation*, 6 February 2003

DoD3 DoD, *Net-Enabled Command Capability (NECC) Capability Development Document (CDD), DRAFT, Increment: I*, 10 May 2006

DoD4 *Interim Department of Defense (DoD) Certification and Accreditation (C&A) Process*, 6 July 2006

DoD5 DoD CIO Memorandum, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media," 3 July 2007

DoD6 DoDD O-8530.1, Computer Network Defense (CND)

DoD7 DoD, *Net-Enabled Command Capability (NECC) , Capability Development Document (CDD) Linked Extension D – Mission Capability Package (MCP) List and Description*

Defense Information Systems Agency (DISA)

DISA1 DISA, *Net-Centric Enterprise Services (NCES) Service Security Design Specification for Service Security v0.4.6*, January 2, 2007

DISA2 DISA, *Net-Centric Enterprise Services (NCES) Service Security Interface Specification, v0.4.5*, June 4, 2007

DISA3 Truong, Hung, Brian Purdy, Aaron Temin, "NCES Service Security Architecture," briefing, September 20, 2007

JJPMO1 JC2 Capability Joint Program Management Office, Joint Command and Control (JC2) Acquisition Information Assurance (IA) Strategy in Support of Milestone A Approval, Version 1.0, 12 December 2005

Joint Task Force – Global Network Operations (JTF-GNO)

JTFGNO1 JTF-GNO WARNORD 07-034, *Deployment of Host Based Security System (HBSS)*,

JTFGNO2 JTF-GNO CTO 07-12

NECC Joint Program Management Office (JPMO)

NJPMO1 NJPMO, *Net-Enabled Command Capability Acquisition Information Assurance Strategy (IAS) Version 0.1.0*, 19 July 2007

National Security Agency (NSA)

NSA1 NSA I813, *Extensible Markup Language (XML) Cross Domain Solution (CDS) (XCDS) Execution and Acquisition Strategy*, 1 March 2007 (Unclassified//For Official Use Only)

NSA2 NSA Information Assurance Directorate (IAD), *Information Assurance (IA) Component of the Global Information Grid (GIG) Integrated Architecture, Increment 1, Version 1.1, Final*, 16 November 2006 (Unclassified//For Official Use Only)

NSA3 NSA, *XML Schema Guidance for Cross Domain Security Policy Enforcement, version 0.9.0*, 24 July 2006

National Institute of Standards and Technology (NIST)

NIST1 NIST, Federal Information Processing Standard (FIPS) PUB 140-2, *Security Requirements for Cryptographic Modules*, 3 December 2002 http://csrc.nist.gov/cryptval/140-2.htm

NIST2 NIST Special Publication 800-95, *Guide to Secure Web Services*, August 2007

Organization for the Advancement of Structured Information Standards (OASIS)

OASIS1 OASIS, *XACML Profile for Role Based Access Control (RBAC) Committee Draft 01*, 13 February 2004

OASIS2 OASIS, *eXtensible Access Control Markup Language (XACML) Version 2.0*, 1 February 2005

OASIS3	OASIS, *SOAP Message Security 1.1 (WS-Security 2004)*, 1 November 2006
Authors	
COST1	Costello, R. "RSS," undated
COST2	Costello, Roger "Building Web Services the REST Way"
NEWC1	Newcomer, Eric, *Understanding Web Services, XML, WSDL, SOAP, and UDDI*, Addison Wesley, 2002
ONEIL1	O'Neil, Mark et. Al. *Web Service Security*, Osborne, 2003
Web Page	
SRCH1	SearchSOA.com Definitions , SOAP, 13 November 2007, http://searchsoa.techtarget.com/sDefinition/0,,sid26_gci214295,00.html