

**VA Enterprise Design Patterns
Privacy and Security**

Non-Person Entity (NPE) Security

**OFFICE OF TECHNOLOGY STRATEGIES (TS)
OFFICE OF INFORMATION AND TECHNOLOGY (OI&T)**

**VERSION 1.0
DATE ISSUED: OCTOBER 2015**



APPROVAL COORDINATION

TIMOTHY L
MCGRAIL
111224

Digitally signed by TIMOTHY L MCGRAIL
DN: dc="us", dc=sw, o=adobe
c=us, 2.5.4.9. Date:
111224
o=us 2015.10.20 14:05:57-0400'

Tim McGrail
Senior Program Analyst
ASD Technology Strategies



Date: 20 Oct 15

Paul A. Tibbits, M.D.
DCIO Architecture, Strategy, and Design

REVISION HISTORY

Version	Date	Approver	Notes
1.0	10/20/15	Tim McGrail	Updated with problem statement and vendor input.

CONTENTS

1	Introduction	4
1.1	Business Need	4
1.2	Approach	5
2	Current Capabilities and Limitations.....	5
3	Future Capabilities	6
3.1	Non-Person Entity (NPE) Security Target State.....	6
3.2	Non-Person Entity (NPE) Security Constraining Principles	7
3.3	Alignment to the One-VA Technical Reference Model (TRM)	8
4	Use Cases	9
	Appendix A. Scope	11
	Appendix B. Definitions.....	12
	Appendix C. Acronyms	14
	Appendix D. References, Standards, and Policies.....	16
	Table 1: NPE Security Solution Constraining Principles.....	7
	Table 2: List of Approved Tools and Standards for Enterprise NPE.....	9
	Figure 1: Notional Application Interaction with NPEs	4
	Figure 2: Non-Person Entity Security Concept Target State.....	6
	Figure 3: VistA Application Authentication Workflow (As-is).....	9

1 INTRODUCTION

VA defines "Non-Person Entity (NPE)" as a non-human entity with a digital identity that acts in cyberspace. NPEs include organizations, hardware devices (e.g., servers and routers), software applications, and information artifacts. The following figure provides a generic application interaction involving NPEs.

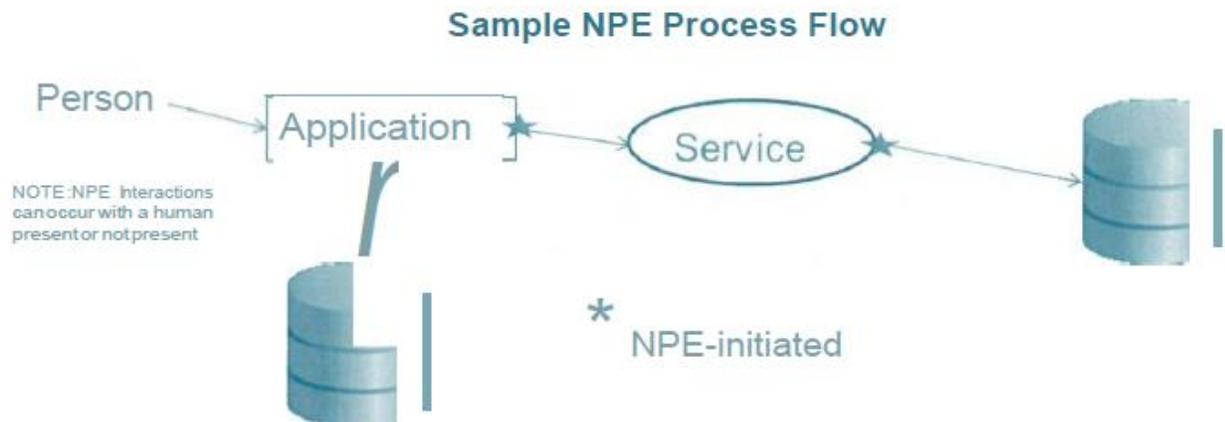


FIGURE 1: NOTIONAL APPLICATION INTERACTION WITH NPEs

VA has capabilities to validate person entity connections to enterprise resources, but these resources either consume shared credentials (either through instance proxy or service accounts) or do not use NPE credentials. This results in VA having little to no specific NPE access control or auditing abilities.

1.1 Business Need

This Enterprise Design Pattern (EDP) establishes the official enterprise guideline for enterprise-wide NPE security across all lines of business in accordance with NIST and VA security policies (see Appendix D). Enhancements to VA's operational model described in this document will also provide the ability to track user access to Personal Identity Information (PII) and Protected Health Information (PHI) via Identity and Access Management (IAM) services. An enterprise wide approach to NPE security provides the following benefits:

- Ensures compliance with VA's Personal Identity Verification (PIV)-only authentication and enterprise on-boarding and off-boarding (per Continuous Readiness in Security Program (CRISP) for NPEs).
- Validates accurate, unambiguous NPEs to enterprise resources (vice generic "application proxy" user accounts) through integration with Single Sign-On Internal and External (SSOi/SSOe).

- Simplifies the technology stack by using Enterprise Shared Services (ESS) and IAM, resulting in improved reliability and maintainability.

1.2 Approach

The near-term approach to resolving the issues outlined above starts with addressing recurring security challenges integrating IAM with VistA and applying lessons learned to establishing NPE security across all lines of business. The approach involves the following actions explained in Sections 3 and 4:

- Correlate the target VA New Person file to IAM Provisioning with some account management functions provided by the Provisioning engine.
- Manage direct user login to backend systems (terminal session, Computerized Patient Record System, etc.) with IAM SSOi/SSOe with SSOi/SSOe tokens.
- Enable external systems (distant VistA system, a middle tier service, etc.) that call a backend system to pass the end user's SSOi/SSOe Secure Assertion Markup Language (SAML) token to the backend system to perform authentication and logging at the user level.

2 CURRENT CAPABILITIES AND LIMITATIONS

NPEs act on a person's behalf, thereby creating issues with identifying users, applications, and system activities. This makes performing forensics more difficult, as indicated in the Use Cases in Section 4. VA is migrating legacy applications and enterprise integration middleware to the IAM platform and ESS, and this migration requires NPE considerations to improve the overall security posture. "Application proxy" entities are used strictly for machine-to-machine actions (e.g. batch processing, etc.) related to application processes and are not associated with specific human-triggered interactions. The "to-be" NPE architectural concept in Section 3 supports propagating user identities using a common set of communication standards. The enterprise NPE construct addresses the following limitations:

- Legacy applications or systems unable to authenticate a calling NPE, resulting in no auditability or trust for those transactions.
- Inadequate ability to check whether there is a valid, active system session.
- Limited ability to validate that the calling system has a right to connect to the service provider (trust relationship between systems).
- Limited ability to validate the application on the calling server. This especially applies to distant VA System instances where dozens of applications could be calling.

3 FUTURE CAPABILITIES

Enterprise-wide NPE security through ESS and IAM are based on the following planning assumptions:

- Authoritative Data Sources (ADS) require integration with ESS infrastructure platforms including the Enterprise Messaging Infrastructure (eMI).
- VA's IAM Provisioning solution is the official authoritative source for creation, activation, and deactivation of user accounts in ADS.
- All current and newly-created ADS user accounts are integrated with the IAM's enterprise user store and IAM Provisioning.

3.1 Non-Person Entity (NPE) Security Target State

The "to-be" architectural concept shown in Figure 2 includes both human application interaction and NPEs as a consolidated whole. It provides a method for current and future VA applications and systems to reduce generic application proxy system accounts in the ESS target environment.

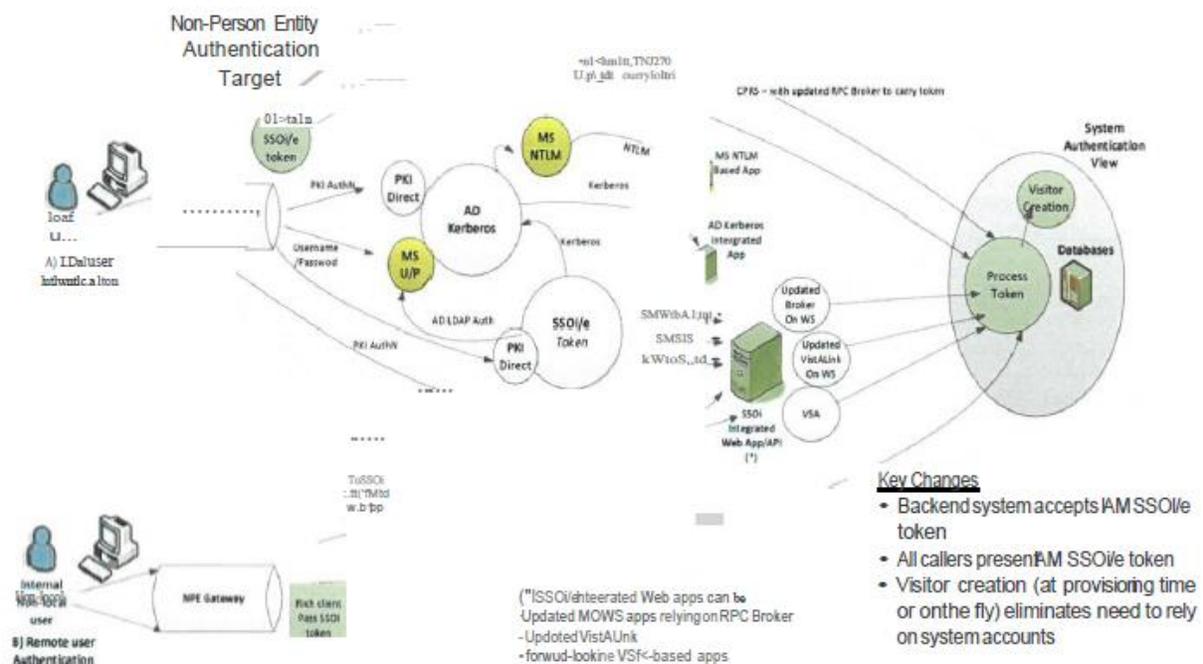


FIGURE 2: NON-PERSON ENTITY SECURITY CONCEPT TARGET STATE

Specifically for VistA, the target state requires the Kernel and IAM teams to align development with enterprise direction for integrating with IAM services. The Internal Authentication and External Authentication EDPs (Appendix D) provide additional details on these services. The NPE solution brings authoritative data sources (e.g., VistA user accounts) under the authority of

IAM Provisioning, enabling identities propagation to authenticate, authorize, and audit NPE transactions.

3.2 Non-Person Entity (NPE) Security Constraining Principles

Enterprise-wide NPE security incorporates the planning assumptions at the beginning of Section 3. The following list represents the constraining principles that guide NPE solution requirements analysis:

TABLE 1: NPE SECURITY SOLUTION CONSTRAINING PRINCIPLES

ID	Constraining Principle	Description
3.2.1	NPE Machine-to-Machine Connections and Provisioning	The target state of the NPE machine-to-machine connections and Provisioning (in the context of VistA) involves communication between VA's backend systems and IAM Provisioning through a "New Person" web service built by the Kernel team on the Virtual Server Assembler VSA platform.
3.2.2	Interface Specifications	IAM requires a VA Provisioning Service Provisioning Markup Language (SPML) interface specification to ensure that user provisioning interactions with VA's backend systems take place in a standards-based, vendor-independent fashion. This SPML specification is reusable for other legacy migration efforts and will provide an additional ESS service capability for systems to consume.
3.2.3	User Sponsorship	All NPE communications that are initiated from NPE devices need to be under the cognizance of humans (Sponsorship), who accept responsibly for NPEs transactions that were sponsored under their authorization.
3.2.4	Protocol Conversion	All VA systems and applications use the eMI for ESS protocol conversion needs.
3.2.5	Identity and Access Management	All systems using IAM's SSOe authentication framework enable use of e FICAM-certified Identity Providers (IdP) or Credential Service Providers (CSPs) that have been approved by VA.
3.2.6	Propagation Model	VA requires an enterprise-level identity propagation model. This identity model ensures that propagation of authenticated identities (user/machine) are propagated through all the steps in the NPE communication transaction, which may need to be propagated through multiple VA systems and recesses.
3.2.7	NPE Credential Renewal	Renewal of Public Key Infrastructure (PKI) certificates by NPE aligns to Federal Bridge guidelines. VA limits credentials to non-production or prohibits the use of self-signed

ID	Constraining Principle	Description
		certificates.
3.2.8	Identity Attributes	NPE transactions require a "minimum 4" set of attributes (M4A) for IAM Secure Assertion Markup Language (SAML) tokens accompanying all NPE service requests. The M4A elements include Subject Organization, Subject Organization ID, Unique User ID and Subject ID.
3.2.9	Auditing	The NPE auditing process will require systems and applications to enable detailed logging capabilities and to utilize messaging.
3.2.10	API Gateway	The NPE solution uses the API Gateway to manage the unmanned authentication of sponsors. The API Gateway will manage the entire NPE Sponsorship process and ensure that the NPE Sponsorship requirements for processing NPE communication according to VA policies are met.
3.2.11	Service Accounts and Application Proxies	All NPE transactions will review a human representative to "bless" the NPE actions. The sponsor is responsible for the transaction on the NPE device that they authorize through the sponsorship process.
3.2.12	NPE Certificates	VA requires an NPE attestation capability to verify critical cyber-metrics. NPEs required Trusted Platform Modules (TPM) for secured, measured boot for system integrity (including remote measurement verification) for all NPEs.
3.2.13	NPE Termination	VA requires security procedures for NPE termination for full closure of all NPE credentials through proper system and application tracking, and NPE sponsorship accountability.
3.2.14	Levels of Assurance	<p>NPEs follow established levels of assurance (LoA) explained in Appendix D. Per FICAM, any NPE that has been engaged in handling VA sensitive information at level 2, 3 or 4 needs to have their records preserved:</p> <ul style="list-style-type: none"> • For Levels 2, and 3, seven years and six months beyond the expiration. • For Level 4, ten years and six months beyond the expiration.

3.3 Alignment to the One-VA Technical Reference Model (TRM)

The NPE solution leverages approved tools and standards catalogued in the One-VA Technical Reference Model (TRM). The following table includes a mapping of technology categories to approved technologies and standards, and mandated ESS required by all VA projects.

TABLE 2: LIST OF APPROVED TOOLS AND STANDARDS FOR ENTERPRISE NPE

Category	Example Technologies	Example Standards	Mandated ESS
Authentication	SiteMinder	X.509, OAuth/OpenID Connect, Kerberos, SAML	IAM Access Services
Authorization	Axiomatics, Active Directory	XACML, LDAP	IAM Access Services
Messaging	WebSphere SOA Suite	SOAP (legacy interfaces), HTIPS (REST), JMS	eMI
Encryption	FIPS 140-2 Compliant Cryptographic Modules	WS-*, TLS per FIPS 140-2 requirements	IAM Access Services
Security Gateway	SecureSpan, DataPower	HTIPS	API Gateway
Auditing	DataPower, Splunk	NIST SP 800-53, VA Handbook 6500	TBD

4 USE CASES

The NPE Security EDP use case focuses on VistA machine-to-machine interactions, which supported development of the constraining principles in Section 3. The following figure shows the workflow with a Local System Administrator:

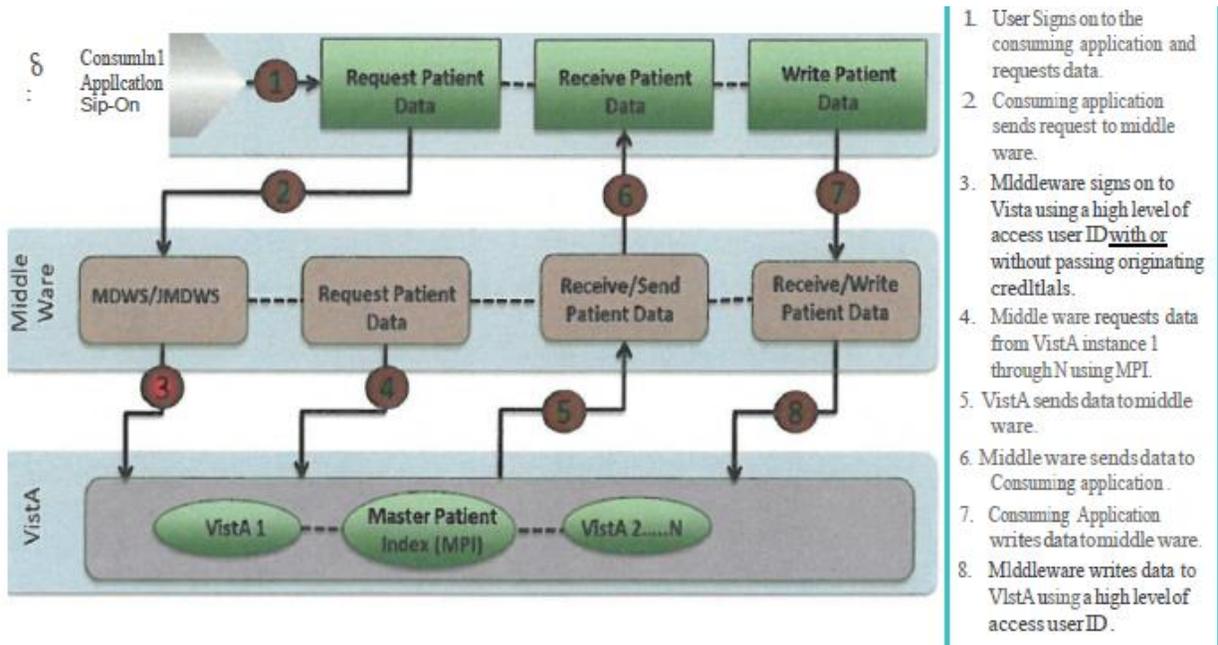


FIGURE 3: VISTA APPLICATION AUTHENTICATION WORKFLOW (AS-IS)

Local VA machine-to-machine authentication has the following aspects:

- The terminal session that is established from the local user to the target VistA application conducts a "roll and scroll" accessed through a terminal emulator.
- Computerized Patient Record System (CPRS) and other rich client applications running on the user's workstation are connecting to local VistA with RPC Broker.
- Web applications connecting to VistA with VistA Link - Kernel Authentication and Authorization for Java 2 Enterprise Edition (KAAJEE) web module handles the user login flow and hands user information from Kernel to the other needed VA web applications.
- Medical Domain Web Services (MOWS) client applications maintains an RPC Broker connection to all VistA systems, and offers a web service to its clients that takes a VistA station number and a user's Access and Verify code.

A Remote System Administrator user has authenticated to some other system, which could be a distant VA system or partner application. Key aspects of remote machine-to-machine authentication are as follows:

- The user may or not be known to the VistA systems or the user may be known to only one VistA system, and used one of the methods listed in the above section to sign in.
- An RPC Broker-based rich client application that has authenticated the user to the distant VistA may wish to run an RPC on a local VistA instance.
- A VistA Link-based application has RPCs that can be run by a user representing the application in the local VistA. Typically these would be run when a user who has logged in via KAAJEE to a distant VistA starts working with a patient who has records in the local VistA.
- A VA system process wants access to a local VistA and there is "No User" present. Example: Corporate Data Warehouse {CDW} pulls MyHealthVet {MHV} data nightly to stage data.

A VA middleware application may also access local VistA data. A user is present for the application that is calling the middleware. In this use case the middleware application {e.g., MDWS} is going to rely solely on trust and allow the system to authenticate to the network without presenting any user credentials using an application proxy accounts credential. There are several variations to this use case including the following:

- A user has signed into a distant VistA system {e.g. Suicide Hotline}.
- Self-service sign-in (e.g., MHV running RPCs to show its users prescription information).
- Unknown Department of Defense (DoD) user.

APPENDIX A. SCOPE

This EDP describes the "to-be" state for VA NPE security. It describes "adaptive" authentication tools that need to be implemented and the need for authentication protocols that can support attribute- and risk-based access controls. The scope of this document is as follows:

- Ensure enterprise mandate for Personal Identity Verification (PIV) compliance is met for VA backend system access
- Ensure Continuous Readiness in Information Security Program (CRISP) on-boarding and off-boarding enterprise mandate is met for VA backend system access
- Automate and improve accuracy in creation of VA backend system visitor accounts as a path to moving away from reliance on "anonymous" VA backend system accounts that represent systems rather than people
- Integrate VA backend system user management within the IAM context and provide mapping from the VA backend system user identifier and enterprise user identifiers (Active Directory (AD), PIV)
- Integrate all forms of user access to VA backend system ("roll and scroll" terminal session, Computerized Patient Record System (CPRS), calls from remote systems, etc.) with the IAM Single Sign-On - Internal (SSOi) user session

This EDP will assist the VA in establishing policy and methodology related to 'user identity' propagation across all architectural tiers of system design.

Document Development and Maintenance

This EDP was developed collaboratively with stakeholders from the ESS Security Group and included participation from VA's Office of Information and Technology (OIT), Product Development (PD), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE). In addition, the Technology Strategies team engaged industry, external government agencies, and academic experts to review, provide input, and comment on the document. This document contains a revision history and revision approval logs to track all changes. Updates need to be coordinated with the Office of Technology Strategies' lead for this document; they will facilitate stakeholder coordination and subsequent re-approval depending on the significance of the change.

APPENDIX B. DEFINITIONS

This appendix provides definitions for terms used in this document, particularly those related to databases, database management, and data integration.

Key Term	Definition
Access	Interaction with a computer system for instance Vista. Such interaction includes data retrieval, editing (create, update, delete) and may result from a variety of technical mechanisms including traditional user log on, consuming applications exercising middleware based connectivity, SOA service requests, etc.
Accurate, Unambiguous User Identity	Information that represents the actual human that is interacting with a computer system, including the initiation of that interaction.
Application Proxy	Construct involving the use of a generic, non-human "user" entity to represent "machine-to-machine" interaction where appropriate for interactions that do not involve a specific end user.
Consuming Application	The application consuming services from a provider system. Generally used when discussing a front-end application supporting a user, but even service providers can themselves be a consumer of other services.
Enterprise Service Bus (ESB)	An SOA infrastructure device which manages message traffic, routing and a variety of other functions for instance orchestration, mediation, etc. The primary ESB at VA is the Enterprise Messaging Infrastructure (eMI).
Enterprise Shared Service (ESS)	A SOA service that is visible across the enterprise and can be accessed by users across the enterprise, subject to appropriate security and privacy restrictions.
Identity Attributes	Characteristics which describe the user (e.g. name, National Provider Identifier, organization, etc.). Establishment of reasonably reliable "unique identity" is generally based on a combination of multiple identity attributes. Specific user identifiers include employee number and email address; may vary from organization to organization but identifier types ought to remain constant for all transactions from a specific organization.

Key Term	Definition
Machine-to-Machine Interaction	In some cases, application processes resulting from workflow (not human interaction) will result in interaction with provider systems to download data, initiate background processing, etc. These actions are not directly initiated by a specific human and the interaction would be attributed to an NPE, possibly via a service account.
Provider System	A system (e.g. VistA) which <i>provides</i> service at the request of a consuming application.
SAML	An XML-based open standard data format for exchanging authentication and authorization data between parties.
Service Oriented Architecture	A paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations
User	A person that interacts with a computer system application. In this context, a "user" is not limited to VA staff members and may include persons from external organizations, patients, beneficiaries, designees, etc.
SSO and User Provisioning	A services provided by Identity and Access Management (IAM) for authenticating users and providing user provisioning information to other systems.
User Types	Traditional types including VA staff, staff of non-VA agencies (e.g. DoD), staff of private sector organizations (e.g. Walgreens); nontraditional, non-staff types including patients, beneficiaries, designees, sponsors, caregivers, etc.
VistA 'Visitor' Record	In conjunction with VistA Kernel, CPRS established an approach for recording "local" users on "remote" VistA systems so that had not previously had a user record (File 200, New Person file) record on file for that person. These records facilitate VistA auditing and role-based access logic as intended. However they do not have access/verify codes that would allow remote users to log on independently of the external application (e.g. CPRS) or exercise functionality that is not allowed by that application.

APPENDIX C. ACRONYMS

The following table provides a list of acronyms that are applicable to and used within this document.

Acronym	Description
AD	Active Directory
API	Application Program Interface
ASD	Architecture, Strategy and Design
CDW	Corporate Data Warehouse
CPRS	Computerized Patient Record System
CSP	Credential Service Provider
eMI	Enterprise Messaging Infrastructure
ESB	Enterprise Service Bus
ESS	Enterprise Shared Service
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
HTTPS	Hypertext Transfer Protocol over TLS
IAM	Identity and Access Management
MHV	MyHealtheVet
IdP	Identity Provider
JMS	Java Messaging Service
KAJJE	Kernel Authentication and Authorization for Java 2 Enterprise Edition
LDAP	Lightweight Directory Access Protocol
LoA	Level of Assurance
M4A	Minimum 4 Attributes
MDWS	Medical Domain Web Services
NIST	National Institute of Standards and Technology
NPE	Non-person Entity
PKI	Public Key Infrastructure
PIV	Personal Identity Verification
REST	Representational State Transfer
RPC	Remote Procedure Call
SAML	Security Assertion Markup Language
SDD	System Design Document
SPML	Service Provisioning Markup Language
SOA	Service-Oriented Architecture
SSOe/SSOi	Single Sign-On External/Internal
TLS	Transport Layer Security
TPM	Trusted Platform Module
TRM	Technical Reference Model

Acronym	Description
VHA	Veteran Health Administration
VistA	Veterans Health Information Systems and Technology Architecture Extensible Markup Language
XML	Veterans Health Information Systems and Technology Architecture Extensible Markup Language

APPENDIX D. REFERENCES, STANDARDS, AND POLICIES

This EDP is aligned to the following VA OI&T references and standards applicable to all new applications being developed in the VA, and are aligned to the VA Enterprise Technical Architecture (ETA):

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
1	VA OIS	VA 6500 Handbook	Directive from the OI&T OIS for establishment of an information security program in the VA, which applies to all applications that leverage ESS.
2	U.S. Army	U.S. Army -Identity and Access Management (IdAM) Reference Architecture (RA) v2.0	Provides guidance on NPE from an Army perspective http://ciog6.army.mil/Portals/1/Architecture/ArmyIdentityandAccessManagement(IdAM)ReferenceArchitectureV2.pdf
4	DOD	DoD IdAM Strategy	Provides guidance on NPE http://csrc.nist.gov/projects/abac/july2013_workshop/july2013_abac_workshop_howard.pdf
5	NIST	NIST Special Publication 800-162 Guide to Attribute Based Access Control (ABAC) Definition and Considerations	Provides guidance on NPE http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf
6	OMB	Federal Information Security Management Act (FISMA) of 2002 they needs to implement a foundational level of security controls outlined in the Federal Information Processing Standard (FIPS) 200	For information systems to ensure compliance with the Federal Information Security Management Act (FISMA) of 2002 they needs to implement a foundational level of security controls outlined in the. FIPS 200 states that, "Organizations needs to identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
7	OMB	Federal Information Processing Standard (FIPS) 200 and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53	Special Publication 800-53, Revision 4, provides a more holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate-contributing to systems that are more resilient in the face of cyber-attacks and other threats. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
8	NIST	NIST 800-63-2: Electronic Authentication Guideline standards	VA has adopted NIST risk management framework, NIST 800-63-2: Electronic Authentication Guideline standards for rating application Levels of Assurance (LOA) and aligning appropriate authentication protocols to the level of risk posed by those applications.
9	OMB	Approved Identity Services in US Government	http://www.idmanagement.gov/approved-identityservices
10	VA ASD	VA EDPs, Office of Technology Strategies	Provides references to the use of enterprise capabilities as part of the integration with IAM services. These documents are intended to standardize and constrain the solution architecture of all applications in VA. http://www.techstrategies.oit.va.gov/docs_design_patterns.asp
11	VA ASD	Full range of technologies provided by the TRM	http://www.va.gov/TRM/ReportVACategoryMapping.asp
12	VA ASD	Enterprise Technology Strategic Plan (ETSP)	http://www.techstrategies.oit.va.gov/docs_ent_tech_strat_plan.asp

NPE Levels of Assurance

Levels of Assurance (LoA) are critical for the NPE solution. In order for the solution to be secure LOAs governance needs to be established that follows a similar model to person entities. This Entity Authentication Assurance Framework (EAAF) defines four LoA for entity Authentication. Each LoA describes the degree of confidence in the processes leading up to and including the

authentication process itself, thus providing assurance that the entity claiming a particular identity (i.e. The entity) is in fact the entity to which that identity was assigned. To determine the level of credential required to validate a sponsor's identity, the VA needs to identify the requirements for each step in the authentication and authorization process. This includes the following steps:

- Sponsor/Application Initial enrollment
- Verification of the sponsors identity credentials
- NPE Transaction management
- Long term NPE communications transaction records management
- Sponsor/ Application Suspension, revocation, re-issuance
- NPE communication transaction Audit

LoA1 is the lowest level of assurance, and LoA4 is the highest level of assurance. Determining which LoA is appropriate for the given application is critical to the NPE solution. The LoA of the credential that the Sponsor presents needs to be correlated to the LoA of the respective system. The systems access rights must be equivalent to their respective sponsor.

Disclaimer: This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.