



Enterprise Design Patterns: Non-Person Entity (NPE) Security

Design Pattern Scope: This Enterprise Design Pattern 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. This document will assist the VA in establishing policy and methodology related to 'user identity' propagation across all architectural tiers of system design.

Current State: NPEs act on a person's behalf, thereby creating issues with identifying users, applications, and system activities. This makes performing forensics more difficult. 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.

Design Pattern Solution: The NPE solution offered in this document 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. The NPE solution also leverages approved tools and standards catalogued in the Technical Reference Model (TRM).

VA defines an NPE as a non-human entity with a digital identity that acts in cyberspace. NPEs include organizations, hardware devices, software applications, and information artifacts.

This document 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.

The near-term approach to resolving NPE issues starts with addressing recurring security challenges to integrating IAM with VistA.

This approach involves applying lessons learned to establishing NPE security across all lines of business, and correlating the target VA New Person file to IAM Provisioning with some account management functions provided by the Provisioning engine. It also involves managing direct user login to backend systems with IAM SSOi/SSOe tokens, as well as enabling external systems 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.

The enterprise NPE construct outlined in this document 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

What are Design Patterns?

Reusable templates that guide the enterprise to implement a set of technologies in standard ways

How do Design Patterns relate to the Enterprise? Design Patterns translate OI&T's strategic goals, as documented in the Enterprise Technology Strategic Plan (ETSP), into "real world" direction to guide system design

How can I learn more? To learn more about Security Design Patterns, contact Joseph Brooks (Joseph.Brooks2@va.gov)

To read the full document, see the TS website: www.techstrategies.oit.va.gov

To ask questions about Design Patterns in general, reach out to AskTS@va.gov