

# VA ENTERPRISE DESIGN PATTERNS PRIVACY AND SECURITY ENTERPRISE AUTHORIZATION



Office of Technology Strategies (TS)  
Office of Information and Technology (OI&T)

Version 1.0  
Date Issued: June 2016

---

## EXECUTIVE SUMMARY

### Scope

The purpose of this document will be to provide strategic direction for VA to establish enterprise-wide authorization services using a common set of standards for attribute based and role-based access control (ABAC/RBAC). Such a service would allow the VA to define and edit authorizations that determine what resources (e.g., systems, services, and objects/data) can be executed or accessed by an authenticated user or process, ensuring that a user (or process) may only do what he or she has permission to do, thereby increasing data security and protection of sensitive information, including PHI and PII.

### Business Need

VA's responsibility for protecting access to a large amount of sensitive patient information includes moderating access by a number of external business partners as well as its own staff. VA requires an Enterprise Shared Service (ESS) for authorization of internal and external users. A service is needed to manage the availability, vocabulary and use of attributes from multiple sources to implement varying levels of access control. This includes guidance on the creation of a compliant architecture, recommendations for migration to new capabilities and instructions for application owners to integrate with enterprise Identity and Access Management (IAM) services.

VA OI&T provides multiple services that support authorization. This includes a portfolio of services to include RBAC and ABAC solutions as well as availability of a range of attributes through a Virtual Directory. However, VA projects have historically had limited insight into

these available solutions, resulting in challenges adopting an enterprise-wide approach to using a standard set of authorization services. Examples of current authorization services include IAM's Single Sign-On (SSO), Authorization Management Service (AMS), Specialized Access Control (SAC), and access controls set by Microsoft Active Directory domain controllers and middleware platforms such as the Enterprise Messaging Infrastructure (eMI). Although IAM provides several enterprise services, some of these are recently deployed and many VA applications have not yet adopted these newer capabilities and have no requirement to do so. A lack of centralization for authorization prevents integrated policy management and compliance. An evaluation of current authorization services reveals the following systemic barriers to adopting enterprise authorization services: 1) lack of a centralized policy store; 2) limited governance of standard authorization solutions and attributes; 3) lack of a flexible authorization standards profile that applies to all VA projects.

## **Approach**

The VA's target Enterprise Authorization solution will provide a consistent process for assessing and providing authorization services across applications. IAM and application owners will work together as described in Section 3 to assess the level of granularity needed by an application. IAM will then support the application owner in selecting the appropriate services to achieve the required level of technical controls by using an approach that leverages RBAC, ABAC or hybrid controls including those inherent to the application. Specifically, this design pattern identifies a centralized method for ensuring a consistent authorization process across all VA applications; identifies best practices for migrating to new authorization processes; and provides guidance on preparations required by application owners to integrate with the authorization service.

While IAM offers multiple authorization services now, the future state for VA enterprise authorization services will increase application owner engagement with IAM services to provide consistent authentication, authorization and auditing across VA. This informs the design of authorization services that will cover the following primary goals: 1) define standards for centralized services for RBAC, ABAC and hybrid controls beyond those inherent to the application and guidance for implementation; 2) a consistent methodology for assessing application requirements to match the security requirements for appropriate use of RBAC, ABAC and application technical controls; and 3) define security considerations for standards and protocols used to support authorization including RBAC, ABAC and others.

---

[Enterprise Design Patterns](#) (EDPs) are developed by TS in coordination with internal and external subject matter experts and stakeholders. An EDP is a reusable capability guidance document that identifies best practice approaches and resources for achieving VA IT strategic

objectives. The EDP Team uses industry trends and innovations; enterprise architectural standards; and guiding principles for capabilities and constraints to improve efficiency and effectiveness and define solutions to reoccurring technical problems. The EDP helps guide the design of IT systems and services by VA project teams.