



Enterprise Design Patterns: External User Identity Authentication (Authentication, Authorization & Audit Increment 2)

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 this Design Pattern, contact Dusty Jackson
(Dusty.Jackson@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

- **External User Authentication Defined:** The process of determining whether someone is actually who they claim to be. External users include other government agencies and their employees, external private sector partners and their employees, and citizens.
- **Current State:** VA has adopted a federated approach that allows the use of many different credential types to access VA resources.
- **Design Pattern Solution:** VA is moving towards the implementation of enterprise shared security services through the Identity and Access Management (IAM) program.



This design pattern provides an overview of external user identity authentication processes and capabilities that VA will implement. It supports the VA's goals of increasing security, decreasing total cost of ownership (TCO) and increasing information re-use/agility.

Defined as users who access VA resources from outside of the VA 'network,' external users include those accessing information from any type of device, mobile or not. In addition to describing the "static" rules for authentication, the design pattern describes the response to the need for authentication protocols that can support attribute- and risk-based access controls.

User authentication to VA resources: applications, systems, and networks within VA, must be conducted in a manner that:

- Provides confidentiality by preventing unauthorized access;
- Provides integrity that protects against unintentional or malicious change;
- Provides non-repudiation of identity, integrity, and origin of data;
- Provides availability of data for users;
- And provides auditability for the enterprise.

VA's future authentication and authorization environment will require that a 'rich' user profile (one that contains required user attributes) be provided to allow for proper implementation of access control services.

Additionally, VA will implement a consolidated Single Sign-on (SSO) approach integrated with a Levels of Assurance (LOA) framework. This approach will allow application designers to perform a single integration with IAM SSO External (SSOe), eliminating the need to integrate with many different Credential Service Providers (CSPs).

This architecture will also allow external users to authenticate once to VA and gain access to many different resources, without requiring separate authentication for each one. This achieves the goal of increasing access to VA resources while eliminating complexity for external users.