Technology Strategies

Defining OI&T's "To Be" Technology Vision

Enterprise Design Patterns: Internal User Identity Authentication (Authentication, Authorization & Audit Increment 1)

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 askCTS@va.gov

- **Internal User Authentication Defined:** The process of determining whether someone is, in fact, who they are claiming to be. Internal users are: VA Employees, Contractors, and Volunteers who have access to VA resources from within the VA network.
- **Current State:** Designers can implement any sort of authentication protocol - as long as it meets established VA security standards.
- **Design Pattern Solution:** Project teams must move from building application-specific authentication functionalities to consuming VA's enterprise authentication services. This is simpler and cheaper for developers - and it boosts VA's security environment.

Currently, VA allows the use of non-standardized processes to conduct internal VA user identity authentication to the network and to applications

This lack of consistency in authentication patterns on the network **decreases security** by increasing system complexity. Moreover, when developers build application-specific authentication protocols, **overall costs to the enterprise rise**.

Developers must use enterprise services for internal user authentication, with Identity and Access Management (IAM) Single Sign-On Internal (SSOi) prioritized as the default protocol

Two additional approved authentication protocols will exist, which reflects the VA's complex environment. If an information system cannot use SSOi, then the team should work with IAM to determine which of the other two protocols is appropriate.

IAM services are in place and ready to be used. IAM services currently have scalability to support onboarding of additional information systems as needed. IAM also has detailed integration patterns available for use by developers. By leveraging these enterprise-level services, the VA will be able to achieve the authentication consistency needed to boost the security of its network.

When done correctly, identity authentication procedures take into account the following considerations:

1. The sensitivity of the **information** that can be accessed
2. The strength of the identity **credential**
3. The **environment** where the identity credential is being presented

Implemented authentication protocols can then (1) prevent unauthorized access, (2) protect against unauthorized changes, and (3) enable the availability of data for the proper users.

TechStrat Today Blog | TS Website | TS Yammer