VA ENTERPRISE DESIGN PATTERNS
PRIVACY AND SECURITY
USER IDENTITY AUTHENTICATION

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

Version 2.0
Date Issued: March 2016

EXECUTIVE SUMMARY

Scope

The Department of Veterans Affairs (VA) has a unified enterprise Identity and Access Management (IAM) program to coordinate the secure access to VA resources for both internal and external users. Office of Management and Budget (OMB) M 11-11 mandates that agencies "require the use of PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems" for internal users and contractors. External users such as other Government agencies, private sector parties, and citizens, including veterans, require varying levels of access to interact with VA services. This Enterprise Design Pattern describes the "to-be" state for VA internal (PIV-enabled VA employees, contractors, and volunteers) and external (business partners, veterans and others who access VA resources from outside the VA network) user identity authentication. In addition to describing the "static" rules for authentication, this document de-scribes "adaptive" authentication tools that will be implemented and the need for authentication proto-cols that can support role-, attribute-, and risk-based access controls.

Business Need

Information system owners perform proper authentication in a variety of ways. They use approved identity authentication procedures that consider the importance and sensitivity of the in-formation in a system. They recognize the threats and vulnerabilities to the system. They consider the level of confidence in any user's asserted identity. They understand the risks that are posed to the enterprise by the potential loss or exposure of information contained in the system. Assessment of the system and the information it processes is directly tied to the level of assurance (LOA) (per NIST SP 800-63) and authentication method required.

VA has implemented Enterprise Shared Services (ESS) for user authentication through the Identity and Access Management (IAM) program. Use of these services constrains project-specific solution designs to a standard set of enterprise security services, which improves manageability and reduces the attack surface. These services will help VA address cybersecurity goals and objectives for protecting federated identity credentials and support the shift to two-factor authentication (2FA) where possible, as de-scribed in the VA Enterprise Cybersecurity Strategy (Version 1.0 released in September 2015).

Approach

To support the move to enterprise authentication services, VA is adopting NIST SP 800-63 LOAs and aligning appropriate authentication protocols to the level of risk posed by those applications. Standardization of these authentication protocols and technologies used by these applications will simplify application design, increase network security, and allow for proper user management. Projects will coordinate with the IAM Business Program Management Office (BPMO) to integrate their system with IAM services based on the LOA determination.

User authentication for VA IT resources will be conducted in a manner that: provides confidentiality by preventing unauthorized access; provides integrity that protects against unintentional or malicious change; provides availability of data for users; and integrates with Enterprise Shared Services to support proper auditing and monitoring.

All VA projects shall coordinate with IAM to determine appropriate integration requirements for IAM services, including the specific type (s) of identity credentials based on the sensitivity of the information that can be accessed, the strength of the identity credential, and the environment where the identity credential is being presented. The following sections describe the core foundations of the IAM SSO service and the guidance for SSOi and SSOe services.

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.