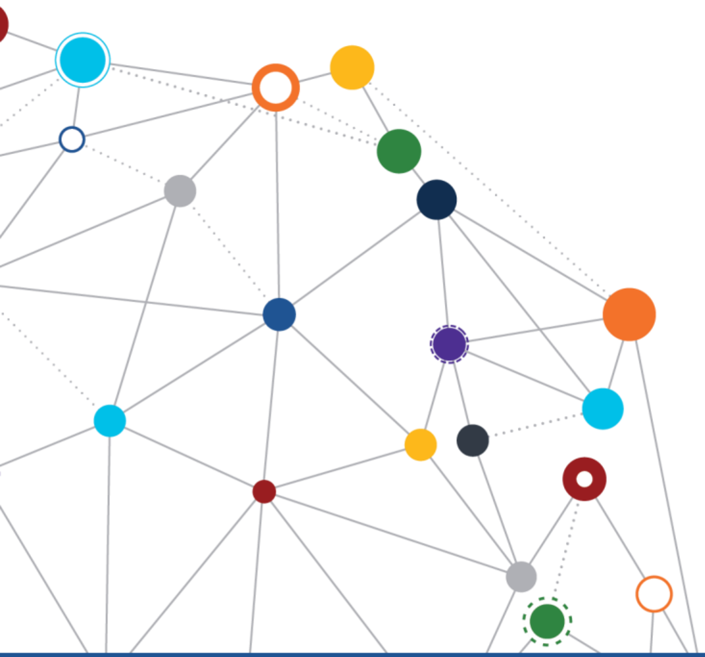
OFFICE OF
INFORMATION
AND TECHNOLOGY

Identity and Access Management (IAM) Enterprise Design Pattern

Single Sign-On (SSO)

March 2019 | Enterprise Program Management Office



U.S. Department of Veterans Affairs
Office of Information and Technology

Table of Contents

Table 1: Change Matrix

Version	Date	Description of Updates
1.0	3/4/2019	IAM Segment: Single Sign On (SSO) document approved

1 Context

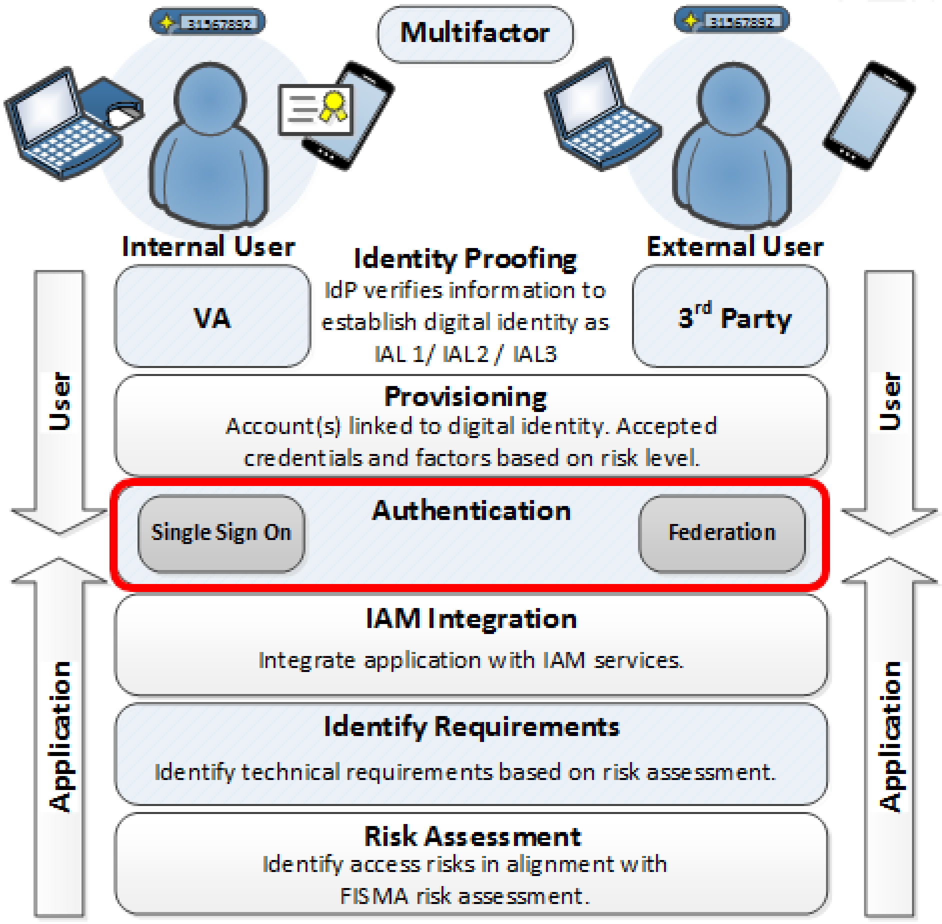
The Department of Veterans Affairs (VA) has a unified enterprise Identity and Access Management (IAM) program to coordinate secure access to VA resources for both internal and external users. IAM services are guided by the Office of Management and Budget (OMB) M 11-11,[1] the Federal Information Processing Standard (FIPS) 200, the National Institute of Standards and Technology (NIST) Guidelines (800-63 and 800-53 per Appendix D), and the Federal Identity, Credential, and Access Management (FICAM) initiative.

VA has two general populations of users who require access: (1) internal users include employees, contractors, trainees, and volunteers, and (2) external users, comprised of Veterans, beneficiaries, and health partners, including employees and contractors from other Government agencies. All require varying levels of access to interact with VA services.

2 Challenge

VA continues to innovate to make services more accessible for Veterans. To provide many services, the user must be identified and authenticated to be presented user-specific information, protect privacy, and prevent fraud. Users are often burdened with tracking multiple usernames and passwords that are used repeatedly to login and gain access to services. Single sign-on (SSO) is one method to relieve this type of user fatigue. The user is asked to authenticate once and is then able to access multiple applications. The progression of how IAM services are engaged by users and system owners is shown in Figure 1. This Enterprise Design Pattern (EDP) focuses on the area highlighted in red.

[1] Note that M 11-11 is a pending rescission. Refer to a draft OMB policy aligned with NIST 800-63 at https://policy.cio.gov/identity-draft/.


Multifactor
Internal User
Identity Proofing
IdP verifies information to establish digital identity as IAL 1/ IAL2 / IAL3
External User
VA
3rd Party
User
User
Provisioning
Account(s) linked to digital identity. Accepted credentials and factors based on risk level.
Authentication
Single Sign On
Federation
IAM Integration
Integrate application with IAM services.
Identify Requirements
Identify technical requirements based on risk assessment.
Risk Assessment
Identify access risks in alignment with FISMA risk assessment.
Application
Application

[2]

Figure 1: Overview of IAM Progression

3 Approach

Authentication establishes that a user attempting to access a service can control the methods used to authenticate (authenticators).[3] It should be noted that authentication does not validate the identity of the user. Validation of user identity is accomplished during identity proofing, where the authenticator is connected to the user.[4] As authentication only verifies control of the authenticator, it is important to properly protect each area of the identity lifecycle according to the acceptable risk level of the service accessed. Projects that are required to use the Veteran-

[2] Figure 1 was created by the VA Office of Information and Technology (OIT) Architecture and Engineering Service (AES) EDP Team from information obtained from VA OIT IAM Subject Matter Experts (SMEs) and the National Institute of Standards and Technology (NIST) Publication 800-63A at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.
[3] Refer to the *IAM Authenticators and MFA* EDP at https://www.oit.va.gov/library/recurring/edp/.
[4] Refer to *IAM Identity Proofing* EDP at https://www.oit.va.gov/library/recurring/edp/.

Focused Integration Process (VIP)[5] are subject to the VA Assessment and Authorization (A&A) Process,[6] which is based on the Risk Management Framework (RMF).[7] The associated risk assessment will result in a projected authentication assurance level (AAL) that will drive authentication requirements.[8] This document will discuss SSO and requirements related to AAL.

3.1 SSO Overview

SSO is a centralized user authentication and session management service. It allows a user to sign on once to access multiple integrated, yet independent applications that use the original sign-on credentials. Once the user authenticates, the SSO creates a token. This token is provided to applications that are integrated with the service to manage the session. Session management includes policy compliance, such as timeouts. When application access is attempted, the application checks with the SSO service to determine if the user has a valid session. If the user has an active session, the user is authenticated. If the user is prompted for credentials when already having an active session with the SSO service, the action does not represent a SSO function, but instead, a credential reuse. The coverage of SSO is limited by the number of applications that are integrated with the SSO service. All VA services must use single sign-on (SSO) when the integrating application can support the technical standards. VA has two services related to authentication and SSO. Single sign-on internal (SSOi) provides single sign-on for internal users. Single sign-on external (SSOe) provides single sign-on for federation with external credentials.

3.2 Session Binding

When a user authenticates to a service, a login session is created. The session is used to ensure that the same user is continuing to use the service for the duration of time between login and logout. To protect the session, a session secret must be used to establish a secure communication channel for the duration of the session. For example, a connection could not fall back from the Hypertext Transfer Protocol Secure (https) to http after authentication and remain compliant. The list below describes the constraints for session binding.

- A session must not be considered at a higher AAL rating than the authentication event.

[5] Refer to the Veteran-Focused Integration Process (VIP) 3.2 Guide, December 2018, at https://vaww.vaco.portal.va.gov/sites/OIT/epmo/vip/Policy%20%20Guidance/VIP%20Guide%203.2.pdf.

[6] Refer to the VIP Security Guide at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=27; it provides details about the A&A process and how it reflects an implementation of NIST guidance and VA security policies. For additional information on VA Assessment and Authorization, refer to https://www.va.gov/PROPATH/map_library/process_AAA_ext.pdf.

[7] Refer to the NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems,* at https://pages.nist.gov/800-63-3/sp800-63-3.html. In addition, the VA Handbook 6500, *Risk Management Framework for VA Information Systems*, can be referenced at https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=793&FType=2.

[8] Refer to the *IAM Risk Assessment* EDP at https://www.oit.va.gov/library/recurring/edp/.

- The session secret must be presented directly by the subscriber’s software, or possession of the secret must be proven using a cryptographic mechanism.
- The session secret used for session binding must be generated by the session host in direct response to an authentication event.
- The session secret must be generated by an approved random bit generator that is compliant with SP 800-90Ar1 and must contain at least 64 bits of entropy.
- The session secret must be erased or invalidated by the session subject when the subscriber logs out or is logged off automatically.
- The session secret should not be placed in insecure locations. For example, Hypertext Markup Language (HTML)5 Local Storage is insecure.
- Transmission of the session secret must use an authenticated protected channel.
- The session secret must have an expiration that is based on the session expiration that is defined for the AAL.

There are different mechanisms that can be used to manage a session to meet these requirements.

3.2.1Browser Cookies

Browser cookies represent a common method for creating a session and tracking a user. If a cookie is used, there are several constraints:

- Cookies must be tagged to be accessible only in secure sessions (e.g., https).
- Cookies must be accessible to the minimum practical set of hostnames and paths.
- Session timeouts must not be dependent on cookie expiration.

It is recommended to tag cookies as inaccessible via JavaScript and to expire at the same time as the session. The expiration can be used to limit the accumulation of cookies, but expiration must not be used for session timeout.

3.2.2URLs and POST Content

A uniform resource locator (URL) can contain the name and value of a session token. POST[9] data can be used to send the session token name and value in the request. When these methods are used, it is important to validate the session information matches. This is used to protect the session from actions taken outside the session, as with Representational State

[9] Web services, including APIs, often use HTTP operations to read and write data, such as GET, PUT, POST, DELETE. Data, such as search words for a query and fields in a fill-in-form, are commonly transferred with the POST command, which requests to write data to the web server. POST carries request parameters in the message of the body, which makes it a secure way of transferring data.

Transfer (REST) Application Program Interfaces (APIs). URLs or POST content must contain a session identifier that must be verified by the Relying Party (RP).

3.2.3 Access Tokens

An access token is used to allow an application to access a set of services after an authentication event. An example is OAuth[10] which enables delegated authorization. OAuth tokens must not be used for authentication.

3.2.4 Device Identification

Other forms of device identification may be used to establish a session if they meet the session binding constraints. For example, Transport Layer Security (TLS) mutual authentication, using X.509 certificates, is recommended for identity provisioning.[11]

3.3 Adaptive Authentication

NIST 800-53 control IA-10: Adaptive identification and authentication allows organizations to employ adaptive authentication controls that require users to provide additional authentication information. The authentication information is based on the AAL level of the application accessed. This applies to two areas: Step-Up Authentication and Adaptive Authentication.

- Step-Up Authentication - Authentication protocols must have functionality in place to allow a user to re-authenticate at an appropriate AAL to access requested resources that have appropriate access rights. This “step-up” functionality allows the issuance of a new authentication challenge at any point in a user session when an increase in AAL authentication is necessary. For example, if a user authenticated at AAL2, attempts to access an application that requires AAL3 will be prompted to authenticate again using multifactor authentication (MFA). While this is unlikely for VA users who use personal identity verification (PIV) cards for all authentication, it would apply to external users whose initial authentication could start with a lower level authentication.
- Adaptive Authentication - VA authentication protocols must be designed to allow the network to issue occasional re-authentication challenges to users, pursuant to established policy. This functionality allows VA to re-authenticate users at their current or higher AAL, based on perceived or established risks associated with a user’s session, behavior, or other established policy.

[10] Refer to *OAuth Security Primer* EDP at https://www.oit.va.gov/library/recurring/edp/index.cfm.

[11] Refer to *Identity Provisioning* EDP at https://www.oit.va.gov/library/recurring/edp/index.cfm.

3.4 Reauthentication

A user must be reauthenticated periodically. Continuity of an ongoing session must be based on possession of a session secret. The session secret is issued by the verifier or SSO service at the time of authentication and may be optionally refreshed. This could be a web browser session cookie or a session secret retained by an application. Session secrets must be non-persistent. This means that the session secret must not be retained if the service is restarted or the system is rebooted.

Session Reauthentication

When SSO is established, a session must not be extended indefinitely, based on the session secret alone. The information below describes NIST 800-63B limits for reauthentication:

- AAL1 - 30 Days maximum
- AAL2 - 12 hours maximum and after 30 minutes of inactivity
- AAL3 - 12 hours maximum and after 15 minutes of inactivity

Reauthentication using Federation

When SSO is established through federation to connect the identity provider (IdP) and RP, additional considerations may apply. Although the federation protocol supports authentication between the IdP and the RP, it does not establish a session. It is possible that the session expires for the RP, but has not expired for the IdP. In this case, the RP requests reauthentication from the IdP. The IdP generates a new assertion, without requiring the user to reauthenticate. The RP then appears to be compliant, while the user has not reauthenticated. The following ensures reauthentication policy compliance:

- The RP must specify a maximum authentication age and confirm that it can be supported by the IdP supporting federation.
- The IdP must communicate any information it has regarding the time of the most recent authentication event at the IdP.
- The RP must not assume that the subscriber has an active session at the IdP that is past the establishment of the federated login.
- The IdP must not assume that termination of the subscriber’s session at the IdP will propagate to the federated RP.

If the Security Assertion Markup Language (SAML) is used as the authentication protocol, the forceAuthN option must be used to force reauthentication. If OpenID Connect (OIDC) Protocol is used as the authentication protocol, the prompt:login option must be used to force reauthentication.

3.5 Rate Limiting

Although MFA limits the ability to perform guessing attacks, some services provided to external users may still use credentials that are single factor and more susceptible to brute force attacks. The verifier must implement controls to protect against credential guessing attacks. The verifier must limit consecutive failed authentication attempts on a single account to no more than 100. Other practices may be used to reduce the ability to perform these types of attacks, such as the following:

- Requiring a Completely Automated Public Turing Test to tell Computers and Humans Apart (CAPTCHA) to be completed after a set number of failed attempts
- Requiring a wait time between a set number of failed attempts and the next authentication attempt; this increases the time cost of each attempt, making many guesses too time consuming
- Whitelisting Internet Protocol (IP) addresses; while this method may be difficult to manage manually, risk-based authentication includes device information as part of granting access and fulfills this basic concept
- Performing behavior-based analysis of authentication attempts to identify anomalies

3.6 SSOi Exception Criteria

General Technical Exceptions

During the feasibility assessment for integration with SSOi, it may become apparent that integration is not yet feasible. This may occur with legacy applications or other technical incompatibilities. In these cases, a proxy must be used that will be compliant with VA policy and AAL requirements. A proxy presents the proper AAL between the user and the proxy, while a lower AAL may be used between the proxy and the application. If the proxy were to be circumvented, this lower AAL would be accessible. Due to this weakness, all applications that use a proxy as part of an SSOi exception must be protected by a device isolation architecture (DIA) that is in compliance with VA enterprise security architecture requirements. DIA is a network security architecture design that restricts a device from communicating with the rest of the network except through a designated proxy which enforces required security controls that may not be met by the device itself.

Exceptions Related to NTLMv2 Support

When NT Local Area Network Manager (NTLM)v2 is enabled for SSO, using a smart card or PIV is similar to using a password. The hash of the smart card credentials is independent of the personal identification number (PIN). Windows creates a hash of the result to facilitate SSO so that the user is not prompted repeatedly for credentials. The end result is that the attacker could use the hash of the smart card until its lifetime expires, which is considerably longer than the time for a password to expire, in most cases. Due to this weakness, all applications that enable NTLMv2 must be protected by a device isolation architecture (DIA), in compliance with VA enterprise security architecture requirements.

3.7 Records Retention

The VA IAM service retains all audit logs related to authentication, in compliance with VA policy. In compliance with NIST 800-63B, the IdP must comply with its respective records retention policies, in accordance with applicable laws, regulations, and policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply. NIST indicates that the IdP is responsible for risk assessment to determine record retention. To support proper record retention, the project team must inform the VA IAM service of any record retention requirements that may exceed normal retention that is identified as part of the service level agreement (SLA).

4 Application of Practices

The following use case represents application of the SSO practices described in this document.

4.1 Integration with Single Sign-On (SSO)

4.1.1 Purpose

Updated Federal policy has been released with new requirements for single sign-on (SSO). VA has many IT services that require authentication by both internal and external users. SSO improves the user experience.

4.1.2 Assumptions

- The application has completed authorization planning to determine the level of access that is granted based on the assertions provided via SSO.
- The collection of any required assertions about the subscriber that are required for authorization have been completed as part of planning for identity proofing.
- A risk assessment has been completed to determine the appropriate AAL of the application that will use SSO.

4.1.3 Use Case Description

- The system owner has submitted the business case for a solution as a VIP Request (VIPR). The system requires integration with VA IAM for internal user access.
- The system owner contacts VA IAM to identify available services.
- Integration with SSOi is required for internal VA applications by VA IAM policy.
- The project team reviews the integration patterns provided by VA IAM, which explain the session binding methods available.

- The project team selects an integration pattern and coordinates with VA IAM to complete the deployment with SSOi.

4.2 Key Practices

Table 2 highlights key practices identified in this EDP.

Table 2: Key Practices IAM SSO EDP

Category	Area	Description
Identity and Access Management	Single Sign-On	To protect the session, a session secret must be used and a secure communication channel must be used for the duration of the session.
Identity and Access Management	Single Sign-On	A session must not be considered at a higher AAL rating than the authentication event.
Identity and Access Management	Single Sign-On	The session secret must be presented directly by the subscriber's software, or possession of the secret must be proven using a cryptographic mechanism.
Identity and Access Management	Single Sign-On	The session secret used for session binding must be generated by the session host in direct response to an authentication event.
Identity and Access Management	Single Sign-On	The session secret must be generated by an approved random bit generator, that is compliant with SP 800-90Ar1 and contains at least 64 bits of entropy.
Identity and Access Management	Single Sign-On	The session secret must be erased or invalidated by the session subject when the subscriber logs out or is logged off automatically.
Identity and Access Management	Single Sign-On	The session secret should not be placed in insecure locations. For example, HTML5 Local Storage is insecure.
Identity and Access Management	Single Sign-On	Transmission of the session secret must use an authenticated protected channel.
Identity and Access Management	Single Sign-On	The session secret must have an expiration that is based on the session expiration defined for the AAL.
Identity and Access Management	Single Sign-On	If a cookie is used for session security, there are several constraints: • Cookies must be tagged to be accessible only on secure sessions (e.g., https). • Cookies must be accessible to the minimum practical set of hostnames and paths.

Category	Area	Description
		• Session timeouts must not be dependent on cookie expiration.
Identity and Access Management	Single Sign-On	URLs or POST content must contain a session identifier that must be verified by the relying party (RP).
Identity and Access Management	Single Sign-On	OAuth tokens must not be used for authentication.
Identity and Access Management	Single Sign-On	Authentication protocols must have functionality in place to allow a user with appropriate access rights to re-authenticate at an appropriate AAL to access requested resources.
Identity and Access Management	Single Sign-On	VA authentication protocols must be designed to allow the network to issue occasional re-authentication challenges to users, per established policy.
Identity and Access Management	Single Sign-On	Session Reauthentication: When SSO is established internally, a session must not be extended indefinitely, based on the session secret alone. The information below describes NIST 800-63B limits for reauthentication: • AAL1 - 30 Days maximum • AAL2 - 12 hours maximum and after 30 minutes of inactivity • AAL3 - 12 hours maximum and after 15 minutes of inactivity
Identity and Access Management	Single Sign-On	Federated Reauthentication: • The RP must specify a maximum authentication age and confirm that it can be supported by the IdP supporting federation. • The IdP must communicate any information it has regarding the time of the latest authentication event at the IdP. • The RP must not assume that the subscriber has an active session at the IdP that is past the establishment of the federated login. • The IdP must not assume that termination of the subscriber’s session at the IdP will propagate to the federated RP.

Category	Area	Description
		• If SAML is used as the authentication protocol, the forceAuthN option must be used to force reauthentication. • If OpenID Connect (OIDC) Protocol is used as the authentication protocol; the prompt:login option must be used to force reauthentication.
Identity and Access Management	Single Sign-On	The verifier must implement controls to protect against credential guessing attacks. The verifier must limit consecutive failed authentication attempts on a single account to no more than 100.
Identity and Access Management	Single Sign-On	All applications that use a proxy as part of an SSOi exception must be protected by a device isolation architecture (DIA) that is in compliance with VA enterprise security architecture requirements.
Identity and Access Management	Single Sign-On	All applications that enable NTLMv2 must be protected by a device isolation architecture (DIA) that is in compliance with VA enterprise security architecture requirements.
Identity and Access Management	Single Sign-On	To support proper record retention, the project team must inform the VA IAM service of any record retention requirements that may exceed normal retention, which is identified as part of the service level agreement (SLA).

5 Impacts

If risk management is not used to define the technical requirements for the IAM components of VA solutions, the following risks are increased:

- FISMA non-compliance, contributing to a material weakness or other audit findings by external agencies with oversight
- Inadequate technical protections for sensitive data that may contribute to unauthorized access, data breach, or fraud

Appendix A: References

- DEA User Stories: https://vaww.portal2.va.gov/sites/asd/TechStrat/IPTS/SitePages/Home.aspx
- FISMA User Stories: https://vaww.portal2.va.gov/sites/asd/AERB/FISMASecurityCompliance/SitePages/Home.aspx
- TRM: http://trm.oit.va.gov/
- NIST 800-63-3: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
- VA 6500.3: http://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=733&FType=2
- VA 6510 (under revision): http://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=823&FType=2

Disclaimer: This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.

Statement of Endorsement: Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, and shall not be used for advertising or product endorsement purposes.