ARCHITECTURE DECISION RECORD (ADR)

Decision Summary: VA.gov to Phase Out the Use of IBM-based SSOe for External and Veteran-facing authentications

Approved by the VA Chief Architect (OIT/OCTO) on Nov 5th, 2025.

Context

VA.gov is currently utilizing IBM's SSOe (Single Sign-On External) for Credential Service Provider (CSP) and Master Person Index (MPI) communications. However, VA.gov also has its own integrations with VA's CSPs through Login.gov and ID.me, as well as MPI, enabling it to authenticate external users directly without relying on SSOe.

The IBM SSOe implementation has not met the evolving needs and performance expectations of the VA, resulting in a suboptimal experience for Veterans, with numerous errors and delays during the sign-in process. Additionally, the contract with IBM is set to expire in September 2026. The VA intends not to renew this contract and instead plans to transition all its digital authentication tools away from IBM's infrastructure before the contract's expiration.

Decision

VA.gov will remove its dependency on IBM-based implementations of Single Sign-On External (SSOe), specifically IBM Security Access Manager (ISAM) and IBM Security Verify Access (ISVA), and will transition to the VA.gov-managed single sign-on implementation currently supporting authentication across VA.gov and the VA Health & Benefits mobile app. Long-term enterprise alignment for external authentication will be addressed through future architectural decisions.

Rationale

The primary reasons driving this decision are the poor Veteran experience and performance issues associated with the current system. As most Veteran-facing features and transactions now occur on VA.gov and it is rare for Veterans to move between VA applications, sharing sessions with non-VA.gov and VA applications is no longer necessary.

This action will:

- Significantly reduce the errors Veterans encounter during sign-in (or provide them with clear paths to resolve these errors),
- Enhance sign-in performance,
- And offer a better overall experience for Veterans engaging with the VA online.
- Poor performance has added an average of 16 seconds per sign-in, resulting in an estimated 507,000 hours of Veteran time lost during the sign-in process over the past year.
- To eliminate silent failures, OCTO must be able to monitor the complete sign-in flow. Currently, Veterans experiencing these SSOe errors are not returned to VA.gov, and VA.gov is not notified of the event or its cause.
- The inability to configure and customize identity policies hinders OCTO's efforts to increase the adoption of NIST Identity Assurance Level 2 and support unique use cases such as the Accredited Representative Portal, which requires specific user attributes and session management policies.
- There are limitations on OCTO's ability to support new features and use cases, such as caregiver and delegate access, business partner features, production test cases, fraud discovery and mitigation, and exploration of emerging sign-in technologies like passkeys.
- Authentication brokering through SSOe is not a requirement for sign in on VA.gov. The VA Health & Benefits mobile app, used by about 1.5 million Veterans monthly, performs about 3 million authentications a month without SSOe today (the app uses a VA.gov web view for sign in, which is common for mobile applications).

Risks and Mitigations

- **Risk:** Loss of session continuity between VA.gov and legacy AccessVA applications.
  Mitigation: VA.gov will continue to recognize active SSOe sessions if present and offer contextual messaging for reauthentication when needed.
- **Risk:** Confusion for users accustomed to seamless navigation across SSOe-backed VA systems.
  Mitigation: VA.gov will deliver clear sign-in guidance and messaging to set expectations and minimize user frustration. This will affect a very small percentage of Veterans that leave VA.gov and navigate to an AccessVA application. For the 1% of users that access the Oracle Health portal, VA.gov will create an SSOe session so that they may be

redirected without needing to sign in again. This will be in place while the portal functionality is being moved to VA.gov and the SSOe IBM contract is still active.

- **Risk:** Internal applications or business units dependent on shared sessions may need minor architectural changes.
  Mitigation: OCTO is engaging with impacted stakeholders to support transition planning and offer integration guidance where required.

- **Risk:** Potential perception that SSOe retirement reduces security assurance.
  Mitigation: All supported Credential Service Providers (e.g., Login.gov, ID.me) meet federal IAL2/AAL2 standards, ensuring no loss in authentication strength or assurance.

- **Risk:** Load and performance testing for the new authentication path is limited due to the inability to fully simulate MPI behavior in a non-production environment. Previous attempts to test MPI at scale have caused outages, creating constraints on proactive testing.
  Mitigation: The VA.gov sign-in system has already been exposed to peak production traffic during past SSOe outages and has demonstrated stable performance under load. To further minimize risk, the rollout will be executed gradually—ramping from 0% to 100% over a period of several weeks. This phased approach allows for real-time monitoring and the ability to pause or rollback and reassess if issues are identified.

Impact(s)

User Experience: Since this is a modification to backend services, users will not see a change when signing in, other than the improvements detailed above (e.g. elimination of silent failures within SSOe, reduced time to sign-in, etc.).

Application Architecture: The change will utilize existing VA.gov integrations and sign-in flows, so minimal changes are needed, except for the removal of SSOe in the flow. This architecture is already in place for the VA Health & Benefits mobile application, where SSOe is not used for user authentication.

Security and Compliance: Since this functionality and integrations exist within VA.gov itself (VASI ID #2103), the ATO controls and external connections are already accounted for at the system level. OCTO is already the authorizing official of Login.gov and ID.me, and security and compliance is managed by the office. The credential providers, Login.gov and ID.me, are responsible for complying with NIST Digital Identity Guidelines (SP 800-63), and OCTO ensures the appropriate identity assurance levels and other policies are in place.

Monitoring and Support: VA.gov already has comprehensive monitoring in place for the 13 million sign-in events across 3 million users each month (this includes the VA Health & Benefits mobile app where SSOe is not used). Existing tools used by VA.gov teams, like Datadog and PagerDuty, will continue to be leveraged for monitoring and escalation of issues and on call support. Additionally, OCTO today provides technical and user support for Login.gov and ID.me.

Stakeholder and Platform Interoperability: VA.gov will leverage existing Login.gov, ID.me, and MPI integrations to perform user authentication. These connections and agreements are already in place.

Technical Debt: No new software or integrations are needing to be developed, so maintenance will be entirely for existing integrations and sign-in flows. Reduced use (and eventual removal) of SSOe from VA.gov simplifies overall system architecture.

For questions or further clarification, contact the Enterprise Architecture team at ea@va.gov.

BASSAM KALDAWI

Digitally signed by BASSAM KALDAWI
Date: 2025.11.05 09:55:03 -08'00'

Sam Kaldawi
Chief Architect
Office of the Chief Technology Officer (OCTO)

**Disclaimer:* This ADR provides architectural guidance only and does not imply AES (Architecture and Engineering Services) ownership of operational, licensing, or funding responsibilities associated with tool usage. Alternative solutions that meet VA's technical and policy standards may continue to be considered under VA's enterprise architecture framework.