ARCHITECTURE DECISION RECORD (ADR)

Decision Summary: Designate Okta Customer Identity Services (CIS) as the standard enterprise platform supporting external Single Sign-On (SSOe).

Approved by the VA Chief Architect (OIT/OCTO) on 4/03/2026

Context

VA supports a growing portfolio of external-facing digital services, including VA.gov, that require secure, scalable, and user-friendly authentication for Veterans, beneficiaries, partners, and other non-workforce users. These external users have fundamentally different identity, security, and lifecycle requirements than VA workforce users and should not be authenticated through internal identity platforms designed for employee access.

Historically, external Single Sign-On (SSOe) capabilities across VA have been implemented using a combination of custom solutions and platform-specific integrations, resulting in inconsistent user experiences, duplicated capabilities, and increased security and operational risk. As demand for digital services continues to grow, this fragmented approach does not scale and complicates alignment with Federal Identity, Credential, and Access Management (FICAM) guidance and Zero Trust principles.

VA requires an enterprise-level external Customer Identity and Access Management (CIAM) capability that provides consistent authentication, federation, and identity governance for external users while maintaining clear separation from workforce identity systems. Establishing a standard external SSOe platform enables reuse, improves security posture, simplifies application onboarding, and reduces long-term operational complexity.

This Architecture Decision Record evaluates external SSOe technology options and establishes an enterprise architectural direction for external user authentication that aligns with VA security, privacy, and digital experience objectives.

Decision

Designate Okta Customer Identity Services (CIS) as the enterprise external identity control plane supporting Single Sign-On (SSOe) for VA.gov and other external-facing applications.

Okta CIS will serve as the enterprise identity broker for external applications and will federate with approved credential service providers (CSPs), such as login.gov and ID.me, in alignment with VA ICAM strategy and FICAM guidance. CSP-backed authentication is the default model for Veteran and public user access.

Direct Okta-managed identities may be used only for designated external user populations that are not appropriate for CSP-backed authentication (e.g., developers, certain partners, or sandbox environments) and must follow established enterprise governance and approval processes.

This decision:

- Establishes a clear architectural separation between external (consumer) identity and internal (workforce) identity systems.
- Designates Okta CIS as the enterprise platform for authentication, federation, and identity management for external users.
- Enables reuse of an existing enterprise CIAM capability to reduce duplication, complexity, and migration risk.
- Provides a consistent foundation for onboarding new external applications requiring SSOe.
- Supports phased transition from legacy external SSO implementations in alignment with enterprise modernization efforts.

This decision applies to external users only and does not alter the enterprise workforce identity strategy. Additionally, this decision aligns with and does not supersede VA's ICAM Next-Generation strategy.

This decision establishes architectural direction only and does not change existing organizational ownership of identity services, credential service provider (CSP) relationships, or operational responsibilities.

Rationale

Establishing Okta Customer Identity Services (CIS) as the enterprise external SSO platform aligns with VA's architectural principles of separation of concerns, reuse of enterprise capabilities, risk reduction, and standardization.

Okta CIS provides a mature Customer Identity and Access Management (CIAM) capability designed specifically for large-scale public user authentication and federation with credential service providers. This aligns with FICAM guidance and Zero Trust principles while supporting high availability and scalability requirements for VA.gov and other external platforms.

From an enterprise perspective, leveraging an already deployed and operational CIAM platform reduces duplication, minimizes integration risk, and avoids unnecessary procurement and migration disruption. Okta is currently in use within the Lighthouse Developer environment and has demonstrated technical feasibility through proof-of-concept integration with VA.gov's Sign-in Service. Expanding an existing enterprise capability provides a lower-risk path to modernization than introducing a new identity platform.

This decision supports:

- Existing enterprise CIAM capability already in use within VA environments
- A consistent external authentication foundation across VA digital services
- Improved onboarding of new external-facing applications
- Reduction of application-specific identity implementations
- A phased transition from legacy SSOe infrastructure
- Alignment with VA's broader ICAM modernization strategy

Finally, this approach enables modernization without service disruption, allowing VA to incrementally evolve its external authentication architecture while maintaining continuity of access for Veterans and other users.

Impact

This decision aligns with the previously approved decision record (AESADR-50) to utilize the Sign-in Service for traffic on VA.gov and establishes a clear operational path for external SSO modernization. Adoption and migration sequencing will be determined through coordinated program-level planning and are not prescribed by this ADR.

Immediate Operational Impacts

- Phasing out legacy IBVM ISVA infrastructure in alignment with migration planning.
- Establishment of Okta CIS as the onboarding standard for all new external SSO integrations.
- Alignment of existing external SSO integrations to a unified enterprise platform to avoid future double-migration scenarios.

- VA.gov integration with Sign-in Service to support development and validation of components required for direct credential service provider (CSP) integration through Okta.

Modernization and Transition Impacts

- Legacy and next-generation SSO capabilities will operate in parallel during transition to ensure continuity of service.
- The availability window for the legacy SSOe platform will be minimized through phased migration.
- Migration sequencing and interim hybrid states will be managed through program-level roadmaps and implementation planning artifacts.

Architectural Impacts

- Reinforces separation between workforce and external identity domains.
- Strengthens reuse and reduces application-specific identity implementations.
- Establishes a consistent enterprise external authentication foundation for VA digital services.
- Improves governance clarity during architecture intake and review.

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

BASSAM KALDAWI Digitally signed by BASSAM KALDAWI
Date: 2026.04.03 13:24:13 -07'00'

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

**Disclaimer: The Architecture and Engineering Services (AES) team's recommendation in this ADR is provided solely as an architectural guidance and does not imply AES ownership of operational, licensing, or cost responsibilities associated with the adoption of the recommended tool.*

This ADR does not establish the recommended tool as the exclusive solution for the defined use case. Other tools that meet VA requirements may continue to be used or evaluated as part of VA's enterprise technology strategy. Cost considerations, licensing agreements, and operational support for any tool remain the responsibility of the respective program offices and stakeholders.