ARCHITECTURE DECISION RECORD (ADR)

Decision Summary: Designate AWS Secrets Manager, Azure Key Vault, and CyberArk Conjur as Enterprise Standard Utilities within the Software Factory (SWF) category Secrets Management.

Approved by the VA Chief Architect (OIT/OCTO) on March 2024

Context

Secrets management is a critical component of modern application security and platform operations. Applications across VA environments require secure storage, rotation, and controlled access to credentials, encryption keys, API tokens, and other sensitive configuration data.

Without standardized secrets-management practices, programs may introduce inconsistent tools and ad-hoc mechanisms for storing and managing credentials. This increases operational risk, complicates automation pipelines, and weakens the enterprise security posture.

The Software Factory (SWF) category for Secrets Management was established to support secure and consistent handling of application secrets across cloud environments and DevOps workflows. Several tools were previously evaluated by OIT leadership and platform teams to support these needs.

This ADR formalizes the designation of enterprise standard utilities for secrets management to ensure consistent architectural alignment, improve security practices, and reduce duplication of tooling across VA environments.

Decision

AWS Secrets Manager, Azure Key Vault, and CyberArk Conjur are designated as Enterprise Standard Utilities within the Software Factory (SWF) category Secrets Management.

Platform alignment:

- **AWS Secrets Manager** will serve as the default secrets-management capability for AWS-native applications and environments.
- **Azure Key Vault** will serve as the default secrets-management capability for Azure-native applications and environments.
- **CyberArk Conjur** will serve as the default solution for DevOps automation and cross-platform secrets management scenarios.

This designation supports consistent enterprise practices, reduces duplication of tooling, and strengthens alignment across VA's secrets-management architecture.

Rationale

Designating AWS Secrets Manager, Azure Key Vault, and CyberArk Conjur as Enterprise Standard Utilities aligns with VA's architectural principles of secure reuse, platform alignment, and standardized enterprise capabilities.

These utilities are already integrated into VA cloud environments and DevSecOps pipelines, providing native mechanisms for secure storage, access control, and automated rotation of application secrets.

Leveraging these established capabilities:

- Promotes consistent handling and protection of credentials and sensitive configuration data
- Improves integration with cloud-native security services and automation pipelines
- Reduces the introduction of ad-hoc or duplicative secrets-management solutions
- Strengthens VA's overall application security posture
- Simplifies architectural governance during solution intake and design review

Formal designation within the SWF ensures that platform-appropriate secrets management capabilities are consistently reused while maintaining flexibility for justified exceptions.

Impact(s)

Operational Impacts

- Standardizes secrets-management practices across AWS, Azure, and DevOps automation environments.
- Reinforces use of existing enterprise-supported utilities, reducing variation in tool adoption.

- Streamlines onboarding and operational support by clearly identifying the default secrets management solutions for each platform.
- Helps reduce security and operational risk by promoting consistent handling of credentials and sensitive application secrets.

Architectural Impacts

- Establishes a unified secrets-management standard within the SWF category.
- Reduces introduction of duplicative or non-aligned secrets-management technologies.
- Strengthens architectural governance during solution intake and review, ensuring alignment with enterprise patterns.
- Improves interoperability, maintainability, and security posture across VA systems through consistent application of platform-appropriate utilities.
- Supports reuse of existing enterprise architectures, integrations, and automation patterns.

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

BASSAM KALDAWI Digitally signed by BASSAM KALDAWI
Date: 2026.03.06 12:57:35 -08'00'

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 architectural guidance and does not imply AES ownership of operational, licensing, or cost responsibilities associated with the adoption of the referenced technology or standard.

This ADR does not establish the referenced technology or standard as the exclusive solution for the defined use case. Other solutions 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 technology remain the responsibility of the respective program offices and stakeholders.

Designation of a product, utility, or technology as an "Enterprise Standard" is for technical alignment and reuse purposes only. Such designations do not constitute procurement direction, vendor preference, or endorsement. Any resulting acquisitions or license expansions must comply with all VA acquisition policies, including brand name justification requirements when applicable.