**White Paper: System Interoperability and Standards Compliance**

Architecting Integration Across Modern Digital Ecosystems (VA Context)

White Paper: System Interoperability and Standards Compliance – Architecting Integration Across Modern Digital Ecosystems (VA Context)

## Executive Summary

As the Department of Veterans Affairs (VA) advances modernization across its benefits, healthcare, and identity platforms, system interoperability becomes not just a technical feature but a core architectural mandate. Secure data exchanges across platforms like Salesforce, AWS, Oracle, and VA Profile must adhere to rigorous compliance frameworks (e.g., HL7, FHIR, MISMO), utilize standardized APIs, and operate through middleware that enables resilient and event-driven architecture. This white paper provides detailed explanations for each integration approach and outlines how standards compliance can be maintained throughout VA’s ecosystem.

1. System Integration Overview

## 1.1 Salesforce Integration

- REST APIs: Enable secure, standards-based Create, Read, Update, Delete (CRUD) operations for Veteran records and case management. REST is ideal for synchronous calls such as real-time claim status checks or updating contact details.

- Platform Events: Allow asynchronous communication for processes that do not require immediate responses, such as queuing background workflows (e.g., sending email confirmations or updating third-party logs).

- Salesforce Connect: Facilitates federated access to VA external data systems like MPI (Master Person Index) or VA Profile, without data replication. It supports data virtualization, ensuring users can query remote data as if it were native to Salesforce.

- Middleware Options:

- Mulesoft: Natively integrates with Salesforce and supports complex transformations.

- AWS AppFlow: Provides point-to-point syncs between Salesforce and AWS services.

- Informatica and Boomi: Support broader enterprise integration, offering drag-and-drop interfaces for mapping and data flow orchestration.

## 1.2 AWS Integration

- EventBridge/SNS/SQS: EventBridge provides centralized event routing for system events (e.g., benefit eligibility decisions). SNS and SQS allow decoupled messaging between producers and consumers.

- Glue & Lambda: Glue serves as the ETL platform, transforming data from source to target formats. Lambda functions offer serverless compute to process events, transform payloads, or orchestrate calls between systems.

- IAM + Cognito: Provide secure access control and federated identity integration, commonly tied with Azure AD or other enterprise identity providers.

- Data Lakes (S3 to Redshift/Athena): Serve analytical needs by capturing structured and unstructured data, enabling SQL-like querying through Athena or data warehousing via Redshift.

## 1.3 Oracle Integration

- Legacy Systems: Claims and benefits logic reside in legacy Oracle databases accessed via PL/SQL APIs. These often use VA’s Enterprise Service Bus (ESB) or older middleware for communication.

- Modernization Strategy:

- Oracle Integration Cloud (OIC): Offers REST-based adapters for modern API exposure.

- JDBC Access: Used within containerized microservices to abstract and modularize data access.

- JSON Mapping: Enables easier transformation from relational data models to modern API schemas.

2. Integration Middleware and Patterns

## 2.1 Middleware Platforms

- Mulesoft: Powers VA’s API-led strategy, encouraging reuse of connectors and pre-built modules. Centralizes logging, enforces governance, and facilitates schema enforcement.

- AWS Glue: Manages ETL workflows with job versioning and schema cataloging. Useful for synchronizing analytics or archiving data from production systems.

- Informatica/Boomi/SnapLogic: Offer low-code interfaces to accelerate integration with less engineering effort, suitable for rapid MVP or POC deployments.

## 2.2 Architecture Patterns

- Canonical Data Model: Promotes standard definitions (e.g., "Veteran," "Claim") across systems, reducing coupling and easing translation between formats.

- Event-Driven Messaging: Enables real-time responsiveness. Kafka or EventBridge serve as brokers that notify downstream systems (e.g., Corp DB updates, case changes).

- ETL vs ELT:

- ETL: Traditional method—transform data before storage, used in compliance-heavy workflows.

- ELT: Stores raw data and transforms on demand, ideal for data lake and analytics use cases.

3. Industry Standards for Interoperability

## 3.1 MISMO

- Used primarily in mortgage and lending domains, MISMO provides XML and JSON schemas for data sharing.

- VA Usage: Essential for Loan Guaranty workflows, allowing compatibility with underwriters and banking institutions.

- Key Tools: Schema validators and transformation templates (XSDs) help verify compliance before submission.

## 3.2 HL7

- HL7 v2.x is a legacy format used in healthcare (e.g., VistA, lab interfaces). Messages are pipe-delimited and require middleware to parse and route.

- Challenge: HL7 formats must often be translated into more modern REST APIs or JSON payloads, especially for integration with newer systems like Cerner.

## 3.3 FHIR

- A modern standard (RESTful) built under HL7, used extensively in Cerner and CMS integrations.

- Resources: SMART on FHIR enables patient-facing apps; Bulk FHIR supports population health.

- VA Usage: Supports patient record access, clinical API use cases, and integration with third-party apps.

4. Example Architecture: Integrated Benefits Platform

## Scenario:

- A Veteran submits a claim through Salesforce.

- Eligibility is verified in an AWS-hosted microservice.

- Claim validation occurs in an Oracle system.

- Health status is retrieved from a FHIR-compliant Cerner instance.

## Components:

- API Gateway: Secures and routes API traffic to appropriate backend services.

- Mulesoft: Performs transformations (e.g., HL7 to JSON, MISMO XML to canonical model).

- Kafka: Broadcasts claim updates to subscribers (e.g., notification services, audit logs).

- AWS Glue: Tags and stores data for reporting and analysis in S3.

## Security Considerations:

- OAuth2 and OpenID Connect enforce authentication/authorization.

- All tools and protocols must be VA TRM-approved.

- Audit trails and data flows are logged and validated for FISMA compliance.

## 5. Resources and Tools

| Area | Resource |

|------|----------|

| Mortgage | https://www.mismo.org |

| Healthcare | https://www.hl7.org, https://smarthealthit.org |

| Cloud Integration | https://docs.aws.amazon.com/glue |

| Salesforce APIs | https://developer.salesforce.com/docs |

| Middleware | https://www.mulesoft.com, https://boomi.com, https://www.informatica.com |

| VA Integration Specs | Internal VA ESB documentation, VA Profile, MPI, and Corp DB APIs |

## Conclusion

VA’s goal of seamless digital service delivery hinges on resilient and standards-compliant system integration. This requires careful alignment of middleware, APIs, schemas, and security protocols across diverse platforms. By leveraging canonical models, asynchronous patterns, and interoperability standards like MISMO and FHIR, the VA can offer Veteran-centric services that are secure, maintainable, and future-ready.

## Next Steps:

- Formalize and publish canonical entity definitions across domains.

- Enhance VA ESB to support event-based messaging patterns.

- Deploy conformance test harnesses (e.g., MISMO XML validators, FHIR reference servers).

- Align all data and API pipelines with FedRAMP and VA TRM-compliant tooling.