VA Enterprise Design Patterns
Enterprise Architecture

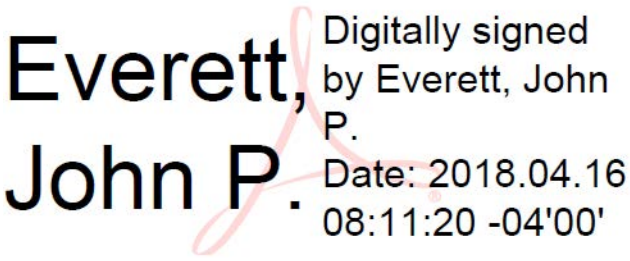
Enterprise Service Oriented Architecture (SOA)

OFFICE OF INFORMATION AND TECHNOLOGY (OIT)

VERSION 2.0

DATE ISSUED: APRIL 2018

APPROVAL COORDINATION



JOHN P. EVERETT

EXECUTIVE DIRECTOR, DEMAND MANAGEMENT DIVISION

DEENEEN AKEO

DIRECTOR, ARCHITECTURE AND ENGINEERING SERVICE

REVISION HISTORY

Version	Date	Approver	Notes
1.0	10/20/2015	Tim McGrail (ASD TS)	Final version for TS leadership approval and signature, including all applicable updates addressing stakeholder feedback and Section 508 Compliance
2.0	11/1/2017	Nicholas Bogden (ASD TS)	Updated format as well as content on business case and introduction, and revised document based on stakeholder feedback and comments

CONTENTS

QUICK JUMP

Select an icon to skip to a section.

Current Capabilities

Future Capabilities

Use Cases

One-VA Technical Reference Model

The Veteran-Focused Integration Process

Enterprise Design Pattern Scope

1 INTRODUCTION

The Department of Veterans Affairs (VA) uses Service Oriented Architecture (SOA) to incorporate repeatable, standardized information technology (IT) functions to help project teams avoid duplicating functionality that is used elsewhere in the enterprise. SOA is an architectural approach where applications use common, vendor-independent message formats to provide services that can be discovered by other applications. These services often contain one or more functions that are designed to fit within the SOA architecture[1], rather than using large, monolithic applications or systems.

SOA provides a uniform means to offer, discover, use, and interact with capabilities to produce desired effects that are consistent with measurable preconditions and expectations. SOA components typically publish a list of interface descriptions for applications or services to incorporate. Service contracts ensure that service providers meet agreed-upon levels of service.

[1] A formal definition of SOA is provided by The Open Group: "Service-Oriented Architecture (SOA) is an architectural style that supports service-orientation. Service-orientation is a way of thinking in terms of services and service-based development and the outcomes of services. A service: (1) is a logical representation of a repeatable business activity that has a specified outcome (e.g., check customer credit, provide weather data, consolidate drilling reports), (2) is self-contained, (3) may be composed of other services, (4) is a "black box" to consumers of the service.

There are several variants of SOA. VA uses Enterprise Shared Services (ESS) to enable applications to consistently consume SOA-based resources across VA and VA external partner organizations. Cloud computing implementations could be considered an extension of this concept since they are typically service-driven and use application programming interfaces (APIs).

Policies and processes often accompany SOA. This Enterprise Design Pattern (EDP) will help VA to define those for VA. It documents the current use of SOA, its current limitations, and a future architecture for expanding the use of SOA. The document provides links to lists of existing ESS, descriptions of existing services at VA, details on an API gateway, and a roadmap for further implementation.

1.1 Business Problem

VA projects that do not use ESS may duplicate enterprise functions, adding cost, time, and interoperability challenges to the overall VA IT enterprise. This EDP helps provide information and direction to address the following business problems:

- The creation of large, monolithic IT applications can add cost and development time, compared to reusing ESS.
- Changes and updates for large, monolithic IT applications can be time consuming, especially if updates need to be made.
- VA project teams may not be aware of ESS and related functions, such as the enterprise service bus, the API gateway, and microservices. A central repository of all relevant services and standards may not be well known to all project teams.
- VA project teams may not be aware of options for developing new ESS.
- VA project teams and other implementers do not have an enterprise roadmap of future steps for reuse of IT functions through SOA.
- When each project is responsible for many security controls, the project team needs a corresponding variety of expertise. Gaps in skills can cause inconsistent reporting of compliance and increase risk to VA.

1.2 Business Need

The following IT issues and capability gaps resolve the business needs addressed by this document:

- VA needs to reduce the complexity of projects that project managers (PM) must manage.
- VA needs to be more agile in adapting to changing business needs.

- VA needs to reduce the level of effort to manage risk for new projects.
- VA needs to reduce infrastructure costs and invest more in delivery of business services.
- VA needs a well-known, comprehensive, and easy-to-use centralized repository for ESS. This function can be used by project teams seeking to reuse an existing service and by those seeking to expose a service to VA project teams.
- VA would benefit from easy-to-deploy ESS functions in VA projects, including standardized SOA service contracts, interfaces, messaging standards, and related utilities to orchestrate data flows between projects and shared services. The setup and invocation of such services should be automated so that they are easy-to-deploy for project teams.
- VA needs to implement such services with in-transit encryption and authentication to ensure security.
- Organizations are often challenged in justifying, prioritizing, and measuring their SOA investments.[2]
- Design and implementation errors prevent organizations from realizing the true benefits of SOA.[2]
- Adoption of SOA requires significant changes to application delivery practices and mindsets.[2]

1.3 Business Case

The engagement of enterprise SOA offers the benefits that are highlighted in Table 1. By engaging ESS and promoting SOA, these benefits can be realized across relevant VA project teams.

TABLE 1: BUSINESS BENEFITS

Business Benefits	Description
Cost Savings	The use of reusable software and functions allow projects to be deployed with reduced cost.
Reduce Development Times	Project teams that reuse existing services can often benefit from quicker development times.
Improve Standardization	A common set of shared services can standardize the interfaces offered to VA project teams.
System Interoperability	ESS allows for system interoperability, which aids system integration

[2]References: Gartner, *The Most Common SOA Mistakes and How to Avoid Them*, May 15, 2017, and *Where to Start (or Restart) with Service-Oriented Architecture*, October 28, 2017.

Business Benefits	Description
Updates and Modernization of Services	• Enterprise services are maintained separately from individual projects. Updates to ESS can be phased in over time to provide security updates and modernization features to projects. • Disruption to individual projects can be minimized if interfaces do not change. Updates to components can be achieved without changing project elements.
Improve Security Compliance	Use of shared services improves compliance and reduces the burden on PMs to design security controls.

Substantial VA IT investments have focused on consolidating IT infrastructure and exposing legacy resources as reusable SOA services to enhance interoperability, improve security, and reduce operational costs. This document establishes an official enterprise direction for VA's migration to a SOA environment that uses ESS and common IT infrastructure platforms.

ESS will help VA achieve the following goals:

- Advance organizational interoperability and agility through reuse across internal and external organizational and program boundaries.
- Promote the standardization, reuse, interoperability, and composition of the best available capabilities developed under the auspices of any system, in order to meet business and mission requirements.
- Reduce the total lifecycle cost of IT.
- Improve information security.

1.4 Approach

This document provides overarching guidelines and a target future state to help ESS planning and road mapping. This EDP identifies current ESS that can help VA projects and lines of business (LOB) organizations to reuse existing capabilities. This is intended to allow VA project teams to make better use of ESS and for other efforts to offer ESS within VA.

The following is a summary of the approach for adopting ESS at VA for interoperable data sharing:

- Phase 1: Establish Standards
    - Establish project-level service design guidelines for ESS architecture, development, and support.
    - Populate and maintain a common repository for information via the Enterprise Data Layer.

    - Publish ESS implementation guidance and disseminate to project teams.
    - Conduct portfolio planning to determine needed ESS and avoid creation of duplicative functionality.
- Phase 2: ESS Execution
    - Deploy SOA infrastructure capabilities to support current and projected ESS.
    - Architect, deploy, and sustain ESS in accordance with VA intake and analysis of business needs, production planning, and detailed scheduling.
    - Support migration of legacy systems to ESS through VA's SOA infrastructure.
- Phase 3: Continual Improvement
    - Update standards and service design guidelines to account for lessons learned.
    - Evaluate the current and future state of SOA infrastructure and develop a roadmap for evolving the SOA infrastructure to accommodate emerging technologies.

2 CURRENT CAPABILITIES AND LIMITATIONS

VA currently implements a series of ESS and an API gateway. SOA basics, examples of these services,[3] and limitations are detailed in this section.

2.1 Overview of Enterprise SOA

This section differentiates enterprise SOA from other reusable techniques and concepts, such as microservices and cloud computing. Enterprise SOA includes applications that offer services to other components within the IT enterprise to help maximize reuse. Microservices are a form of SOA in which each application is composed of modular individual services. Each of these modular services can also be reused by other projects (See Microservices EDP for additional information[4]). Cloud services are internet-based computing services based on SOA principles. These services are offered through remote data centers to provide reusable components that can be invoked by project teams. In many cases, VA does not provide or manage the cloud services, but VA does own and manage the corresponding data.

[3] Additional information on VA ESS can be found in Appendix E.
[4] Additional information is available from https://www.oit.va.gov/library/programs/ts/edp/cloud/Microservices_V1.pdf.

The following table highlights differences between SOA and microservice approaches.

TABLE 2: COMPARISON OF SOA AND MICROSERVICES

Category	SOA	Microservices
Communications	Enterprise Service Bus	Lightweight, standard communication protocols
Organization	Decompose a monolithic application into services	Decompose a monolithic application into services
Modularity	Functions and services that encompass a wide range of features	Lightweight/'fine grained' services with a more narrow scope
Planning orientation	Oriented around services	Oriented around capabilities provided

2.1.1 Open Group SOA Reference Architecture

The Open Group's SOA Reference Architecture[5] guides the categorization of ESS and is used to inform ESS architecture guidance and governance processes. The following categories describe service functionality:

- Interaction: Client-centric services (e.g., portal services) tied to organizational roles and solution applications
- Process: Business process services (e.g., workflows) are tied to an organization's way of doing business
- Business Application: Stand-alone services that provide a discrete, business-related capability, specific to a narrow set of service domains
- Information: Services (e.g., data access services, data federation services) that provide information related to business entities. These are broadly used across processes and less specific than process services
- Utility: Stand-alone services that normally have a broad cross-section of stakeholders provide a discreet, business-related capability across a wide range of service domains
- Access: Services (e.g., adapters) that provide access to legacy systems and whose service interfaces are tightly coupled to the legacy system interface
- Partner: Services capturing interoperability with partners, isolating VA from changes

[5] Reference: The Open Group, *SOA Reference Architecture*, ISBN: 1-937218-01-0, November 2011.

The service layering and service categorization guidelines provide detailed implementation guidance on each abstraction layer and service category that informs solution architecture development. Future versions of this document will include links to these guidelines and additional details on the architecture modeling activities.

2.1.2 Open Group SOA Governance Framework

The Open Group SOA Governance Framework is now an international standard, having passed its six-month ratification vote in the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). According to Gartner, effective governance is a key success factor for SOA solutions today and in the future. This endorsement of The Open Group standard by ISO means that this vendor-neutral and proven SOA governance standard is now available to governments and enterprises world-wide. The SOA Governance Framework enables organizations—public, private, large and small—to rapidly develop their own robust governance regimens and use industry best practices. This substantially reduces the cost and risk of using SOA. As an international standard, the framework will now provide authoritative guidelines for organizations across the globe to implement sound SOA governance practices.

The framework includes a standard governance reference model and a mechanism for enterprises to customize and implement the compliance, dispensation, and communication processes that are appropriate for them. Long term vitality is an essential part of the framework. In light of changing business and technical circumstances, the framework gives guidance on evolving these processes over time, ensuring the on-going alignment of business and IT.[6]

2.1.3 Interoperability

Interoperability among IT systems is often a recurring challenge that has never been easy to resolve despite the development of data exchange protocols, standards, and platforms. In health care, data exchange standards and protocols are at the root of all interoperability and Health Information Exchange (HIE) initiatives, and are fundamental to their success. Data exchange standards define how patient health information is acquired, assembled, packaged, and transmitted. Vocabularies and taxonomies ensure that the data conforms to healthcare industry domain concepts and classification schemes, and enforces a level of semantic

[6] Reference: http://www.opengroup.org.

normalization. These messaging standards, in turn, rely on underlying wire, transport, connection, and security protocols for safe and reliable sharing and exchange.[7]

The following figure details standards, initiatives, and networks used across healthcare systems to help illustrate the complexity involved in health system interoperability.

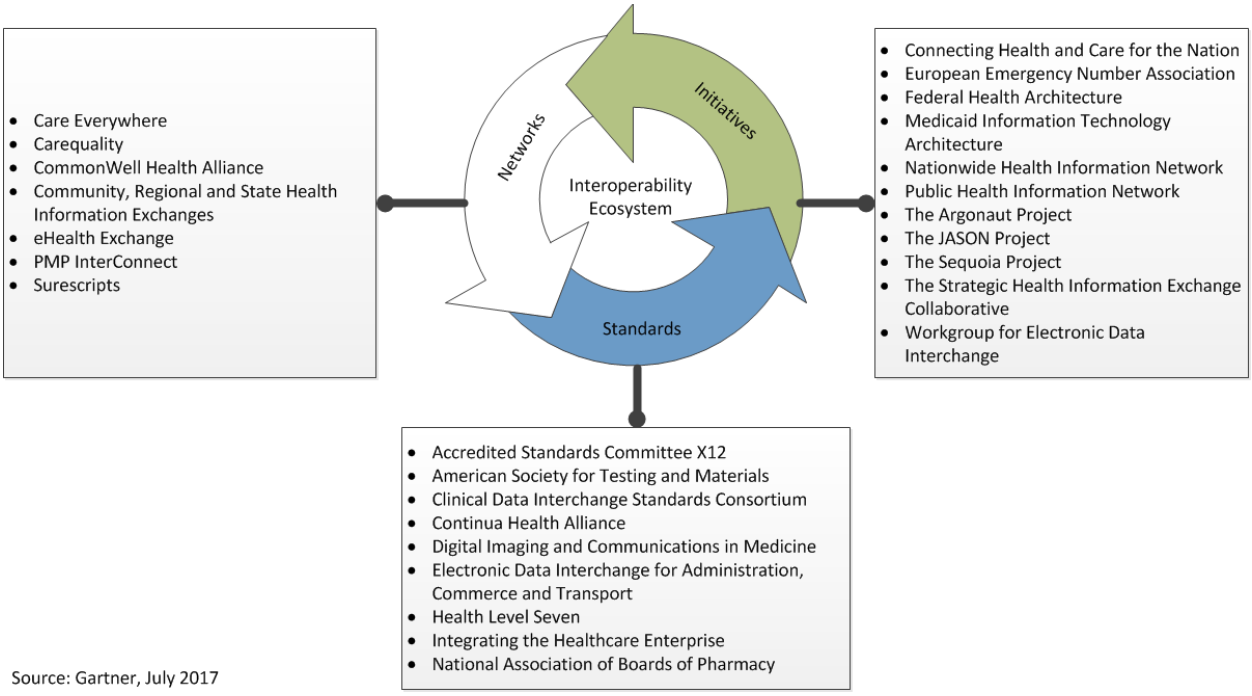


FIGURE 1: HEALTH INTEROPERABILITY NETWORKS, INITIATIVES AND STANDARDS

Key Findings include the following:

- The healthcare industry's "interoperability problem" has been described as an electronic health record (EHR) data-blocking problem. Since patient data has become the currency of our healthcare system, this will remain a valid concern. However, the interoperability problem is more about the formidable industry and technical challenges of sharing patient information safely at scale.
- Health data exchange standards continue to evolve and modernize, and are more aligned with industry information-sharing challenges, but their adoption will not ensure success. Effective and pervasive interoperability depends more on genuine cooperation among industry stakeholders and vendors than on technological innovation and advancement.

[7] Reference: Gartner, *The Road to Healthcare Interoperability Goes Through the National Health Information Network*, July 5, 2017.

- Community, regional, and state-sponsored HIEs and industry interoperability networks are the most practical vehicles for promoting healthcare interoperability. Collectively, they form the basis for a national health information network (NHIN), envisioned by the Office of the National Coordinator for Health Information Technology (ONC) over a decade ago.

2.2 Catalog of Existing Shared Services

This section provides examples of selected ESS and ESS in development at VA. VA sites also list ESS with accompanying information. Such sites include the Enterprise Service Collaboration Portal (ESCP),[8] the WebSphere Service Registry and Repository (WSRR),[9] and the Veteran's Information System and Technology Architecture (VistA) Integration Adapter[10] API. These resources provide repositories of enterprise data and data services available for VA project teams and system developers. Without one common site, stakeholders can be challenged in identifying ESS that may be applicable to their projects.

Additional information on existing ESS is found in Appendix E. This section will include references to existing materials on VA ESS. The VA Enterprise Cloud also offers General Support Services (GSS), which are reusable cloud computing resources that may benefit VA projects.[11] The US General Services Administration (GSA) offers Unified Shared Services Management (USSM), which may be helpful to VA projects.[12]

2.2.1 Corporate Data Warehouse

The Office of Information and Technology (OIT) built the Corporate Data Warehouse (CDW) and four regional data warehouses (RDW1-4) to store and query data. The CDW program is central to business management, clinical and administrative research, and healthcare system innovation. Through efforts such as CDW, OIT and the VA Data Governance Council (DGC) seek to provide a high-performance business intelligence infrastructure through standardization, consolidation, and streamlining of clinical data systems.

---

[8] The ESCP can be found at https://escp.aac.va.gov/.
[9] The WSRR dashboard can be found at https://vaausemiihtwgdev12.aac.va.gov/ServiceRegistryDashboard/Administrators and Information on the WSRR Studio can be found at https://vaausemiihtwgdev12.aac.va.gov/ServiceRegistry/ClassificationDetailButtonHandler.do.
[10] VIA contains Web Services Description Language (WSDL) files for service usage at https://vaww.viapreprod.va.gov/via-webservices/.
[11] Additional information on cloud computing GSS can be found at https://vaww.portal.va.gov/sites/ECS/SitePages/What%20is%20the%20VA%20Enterprise%20Cloud%20%28VAEC%29.aspx.
[12] Information on the GSA USSM, stipulated by OMB Memorandum 16-11, can be found at https://www.ussm.gov/.

Figure 2 provides a system diagram of CDW.

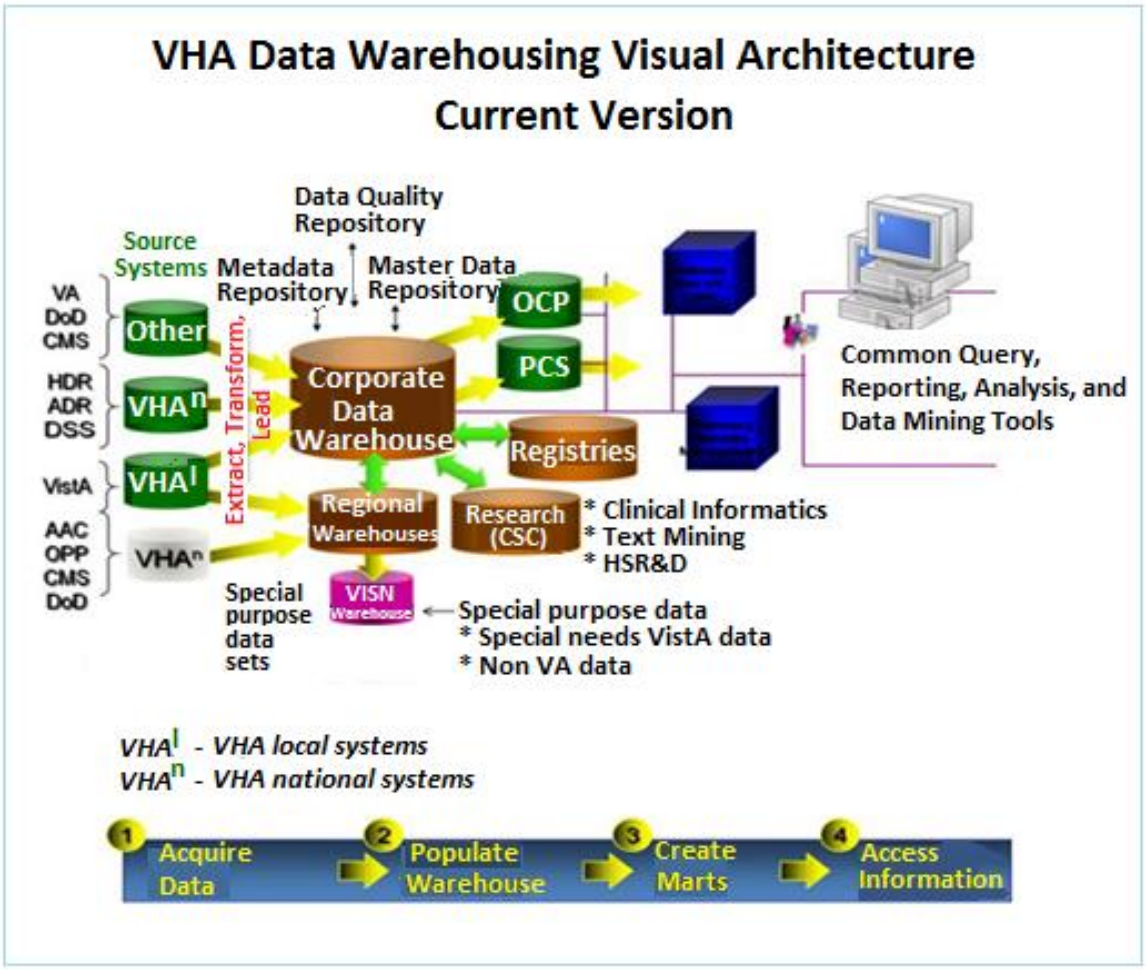


FIGURE 2: CORPORATE DATA WAREHOUSE VISION

The mission of CDW includes delivery of better visibility and higher availability across departments, leveraging existing IT infrastructure investment, and providing repeatable database read and large scale data warehouse capabilities. CDW functions as an ESS that provides common services (e.g., querying, reporting, analytics) using data from all regional data warehouses.

Efforts related to CDW are on-going. A working group currently exists to address and develop common interfaces and terminology. The developmental changes (e.g., changes due to interfaces, integrating services, program names, and organizational structures for programs) can present a management challenge.[13] Eventually, it will be possible to integrate data from multiple sources.

2.2.2 Enterprise Program Management Office (EPMO) Messaging Platform

The Enterprise Program Management Office (EPMO) Messaging Platform is the current VA enterprise messaging service. This replaces the prior Enterprise Messaging Infrastructure (eMI) service. eMI was intended to minimize point-to-point connections and support a SOA infrastructure in support of VA distributed applications. Messaging flows used by VA include: (1) messages to DoD, (2) messages to vendor independent messaging (VIM), and (3) pharmacy message flows. Other services that aid messaging include the Virtual Lifetime Electronic Record (VLER) Data Access Services (DAS) and Veteran Information/Eligibility Record Services (VIERS).

Although EPMO Messaging Platform is the enterprise service, there are multiple competing messaging platforms in use. Currently, there is not one single platform that can meet all messaging requirements. Table 3 provides details of other messaging and information sharing systems, many of which exchange medical or health information.[14] This represents an opportunity for greater consolidation and simplification of the architecture.

TABLE 3: VA TRUSTED INFORMATION SHARING SYSTEMS

Acronym	Name	Description
DAS	Data Access Services	Provides a system of middleware responsible for transport of Veteran health, benefits, or administrative data between consumers and producers
EXS	Exchange	Provides Microsoft Exchange E-mail Environment
DVP	Digital Veterans Platform	Enables interoperability between VA and commercial applications by providing: (1) electronic health records, (2) operation management, (3) customer relationship management, (4) API gateway, and (5) analytics services
VIA	VistA Integration Adapter	Provides web services for applications to derive data and execute methods on VistA systems
MDWS	Medical Domain Web Services	Provides suite of middle-tier SOA web services that can virtualize any legacy VistA remote procedure call

[13] For example, there may be changes from an effort related to CDW known as the Enterprise Data Warehouse (EDW).

[14] Many of these trusted information sharing systems are listed in the VA Systems Inventory (VASI).

Acronym		
eHX	eHealth Exchange	Provides functions to exchange VA and partner electronic health records
BHIE	Bidirectional Health Information Exchange	Provides primary health information exchange (HIE) between VA and Department of Defense (DoD)
DSM	Direct Secure Messaging	Enables sharing of medical information between VA and non-VA care providers
FHIE	Federal Health Information Exchange	Enables secure, one-way transmission of protected electronic health information from DoD to VA
VAP	Veterans Authorizations and Preferences	Enables Veterans to set and manage health information sharing preferences with federal and private partners
VIERS	Veteran Identity / Eligibility Reporting System	Provides consuming business applications with access to a standard, enterprise view of personnel information (e.g., demographic, benefit, history information)
VIE	Vitria Interface Engine	Receives data from a VistA site, uploads to Austin Information Technology Center (AITC), receives acknowledgements from AITC, and downloads to the VistA site

2.2.3 Enterprise Identity and Access Management (IAM)

VA implemented ESS for user authentication through the Identity and Access Management (IAM) program. Use of these services constrains project-specific solution designs to a standard set of enterprise security services, which improves manageability and reduces the attack surface. These services will help VA address cybersecurity goals and objectives for protecting federated identity credentials and support the shift to two-factor authentication (2FA), where possible, as described in the VA Enterprise Cybersecurity Strategy.[15] Figure 3 shows the use of these IAM services from both the single sign on (internal) and federated (external) user perspectives.[16]

[15] Reference: VA OI&T Enterprise Cybersecurity Strategy, September 2015, https://www.oit.va.gov/library/strategy/VA_Enterprise_Cybersecurity_Strategy_final_09222015.pdf.

[16] In this diagram, authorization is provided by the IAM integration layer. Additional information can be found at the User Identity Authentication EDP at https://www.oit.va.gov/library/programs/ts/edp/privacy/UserIdentityAuthentication_V2.pdf.

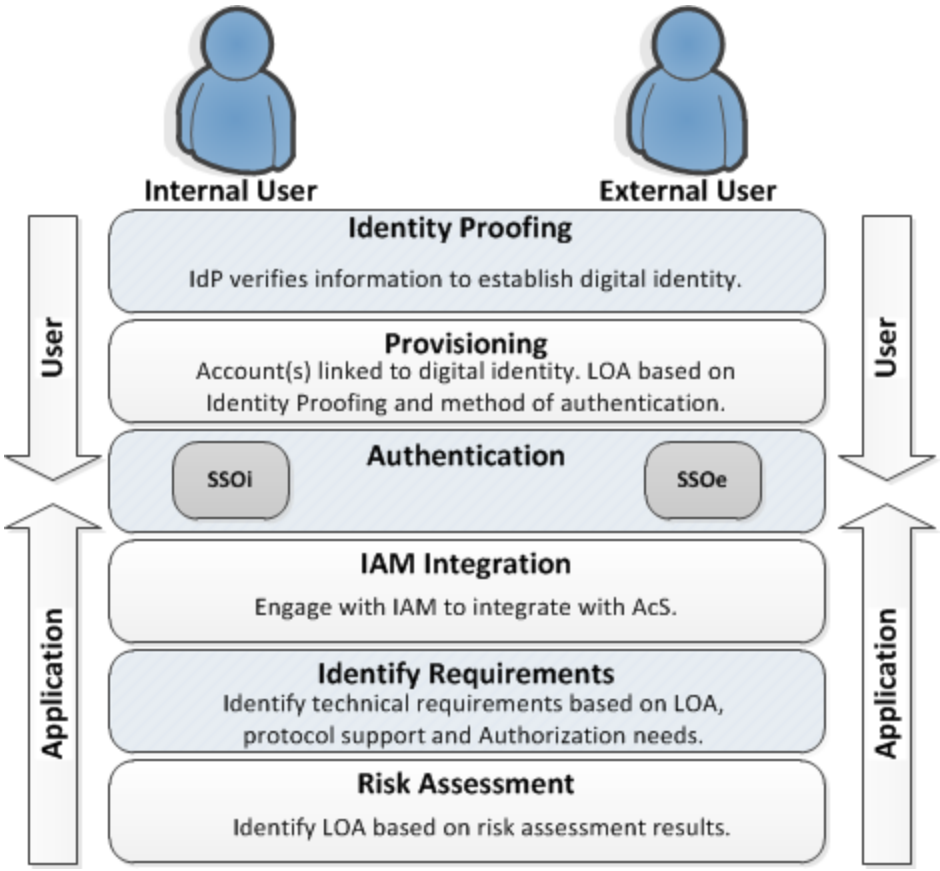


FIGURE 3: IDENTITY AND ACCESS MANAGEMENT

VA has a unified enterprise IAM program to coordinate secure access to VA resources for both internal and external users. The authentication services are also designed to be supportive of VA's current and future enterprise authorization and auditing policies and guidelines. These include VA Directive 6510, which specifies identity and access management policy for VA staff and programs. Additionally, Office of Management and Budget (OMB) Memorandum M-11-11 mandates that agencies "require the use of Personal Identity Verification (PIV) credentials as the common means of authentication for access to that agency's facilities, networks, and information systems" for internal users and contractors. OMB Memorandum M-04-04 also provides policy for assurance of electronic transactions requiring authentication. This can be used to determine assurance level and validate that implemented systems meet it. External users, such as other government agencies, private sector parties, and citizens, including

Veterans, require varying levels of access to interact with VA services. For additional information on user identity authentication, please see the User Identity Authentication EDP.[17]

IAM Provisioning

IAM provisioning is the authoritative source for user identity. By leveraging IAM provisioning, VA applications can centrally manage user information, attributes, roles, and accounts, using data from authoritative identity sources.

The provisioning service uses automated and centralized workflows to enhance security and bolster efficiency. As a result, application administrators, who previously had to manually manage user administration, now have services available to automate the process. Provisioning assigns the Security Identifier (SecID) as a unique user identifier for integrated applications to use for user authorization and audit.

Identity Store (Master Veteran Index (MVI))

IAM provides the MVI, VA's authoritative source for identity data.[18] MVI correlates the multiple VA person types within VA and DoD to assign a unique identifier to each person. This identifier is used for all patients with a record in VistA.

SecID is the enterprise identifier for user identity. It remains the same even if the user status changes (e.g., changes from Veteran to contractor to employee). SecID is the identifier used to correlate provisioning records to MVI's integration control number (ICN), which is the unique person identifier. These two identifiers are correlated.[19]

MVI, based on the enhanced Master Patient Index (MPI), is the authoritative federated identity service within VA, establishing, maintaining, and synchronizing identities for VA clients, Veterans and beneficiaries. The MVI includes authoritative sources for health identity data and contains over 17 million patient entries populated from all Veterans Health Administration (VHA) facilities nationwide. The MVI provides the access point mechanism for linking patient information to enable an enterprise-wide view of patient information, uniquely identifies all active patients who have been admitted, treated, or registered in any VHA facility, and assigns a unique identifier to the patient. The MVI correlates a patient identity across the enterprise,

[17] Reference: User Identity Authentication EDP, version 2.0, March 2016, https://www.oit.va.gov/library/programs/ts/edp/privacy/UserIdentityAuthentication_V2.pdf.
[18] Reference: Veteran and Eligible Beneficiary Identity Authoritative Data Source Selection Memorandum, November 4, 2016, https://www.vapulse.net/docs/DOC-121923.
[19] Additional information can be found at http://vaww.oed.portal.va.gov/sites/vrm/IAM/playbooks/Pages/Prov/Prov.aspx.

including all VistA systems and external systems, such as DoD and the NHIN. The MVI facilitates sharing health information, resulting in coordinated and integrated health care for Veterans. New IT systems must be interoperable with the MVI and legacy systems. The Healthcare Identity Management (HC IdM) Team, within the VHA Data Quality Program, is the steward of patient identity data, performing maintenance and support activities.[20]

2.2.4 Benefit Gateway Services

VA implemented Benefits Gateway Services (BGS) to reuse existing benefits data for other initiatives. Six years later, BGS is processing up to 30 million transactions each day across the enterprise to allow Veterans and other stakeholders to securely access their benefit claims. Use of BGS has also made it possible to deploy a new claims processing system in half the time of its predecessor.

BGS is still in development. Accordingly, VA projects should seek the latest interface information when developing to use BGS services.

2.3 Limitations

In summary, the current state of SOA has the following limitations:

- Lack of one single catalog of ESS
- Single platform is not used for messaging
- Future direction is pending, pursuant to the implementation of the new EHR system
- ESS are evolving and not all candidates for ESS are fully matured
- Developmental changes are on-going, making management challenging

VA's adoption of ESS to achieve an enterprise SOA is still a work in progress. Several VA projects listed in this section are expected to continue to offer ESS within VA. Expansion of more of these services will lead to a better migration to an enterprise SOA environment. This will also align with VA's innovation key principal[21] and the forward-looking guiding principal.[22]

[20] Reference: https://catalog.data.gov/dataset/master-veteran-index-mvi.
[21] Source: Office of Information and Technology, Year End Review, 2017, page 11.
[22] Source: Department of Veteran Affairs, FY 2014-2020 Strategic Plan, Page 5.

3 FUTURE CAPABILITIES

Shared Services need to be identified and used more often by project teams. All VIP projects should use approved ESS and shared platforms. This may require use of mechanisms and services to help recommend appropriate ESS.

Future updates of this EDP will include references to detailed implementation guidance and ESS roadmap content for each approved ESS, through coordination with EPMO Demand Management and their Planning Analysis Document (PAD) efforts.

3.1 SOA Infrastructure Guidelines

The following guidelines help project teams to determine when to use VA SOA capabilities from the EPMO Messaging Platform. Many EPMO Messaging Platform capabilities come from the HealthShare Enterprise Platform (HSE), Digital Veteran Platform (DVP), and the DAS SOA Gateway. These guidelines help identity appropriate functions (e.g., endpoint management, orchestration, communication, even handling, data transformation) for projects. They provide business rules to help consolidate and simplify the overall architecture.

1. HealthShare Enterprise Platform (HSE Platform): Use the HSE Platform for integration in the Health domain and specifically with VistA. Veteran Health Information Exchange (VHIE) VA external partners (e.g., Walgreens Pharmacies, Allegheny Health Network, University of Wisconsin Health) shall integrate with the HSE Platform.[23]
2. Digital Veteran Platform (DVP): Use DVP for integration in the Benefits, Memorial, Corporate, and Enterprise domains. Additionally, use DVP for integration across multiple domains.
3. DAS SOA Gateway: Use DAS SOA Gateway for integration with DoD and integration with the DAS persistent data store. Also use DAS SOA gateway for integration with other external private sector service consumers and government agencies (e.g., DoD, Centers For Medicare/Medicaid (CMS), Internal Revenue Service (IRS), Social Security Administration (SSA)).[24]

[23] VHIE integrations with the HAS platform are being architected now.

[24] The primary mission for DAS is to provide persistent Data as a Service (DaaS). Other capabilities of DAS align with the EPMO Messaging Platform functions.

For further reference, the following figure provides an architectural view for the EPMO messaging platform and the interactions it facilitates:[25]

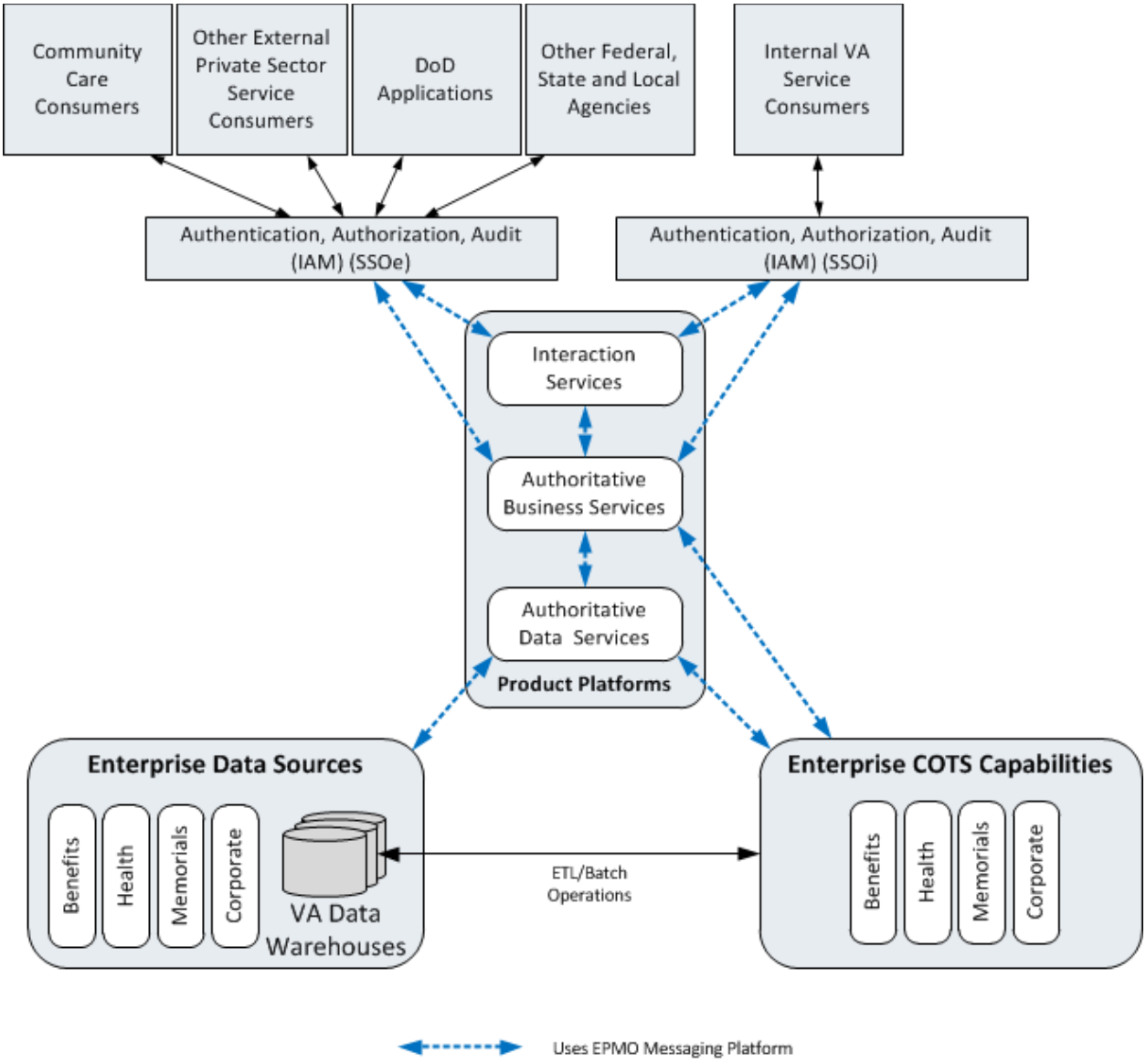


FIGURE 4: HIGH-LEVEL CONTEXT DIAGRAM FOR HEALTHCARE ESS INTERACTION

Additionally, Figure 5 diagrams the capabilities of the EPMO Messaging Platform by type.

[25] The systems shown in this diagram do not yet reflect the forthcoming new EHR system. As of the date of publication, the contracts for this system have not been finalized.

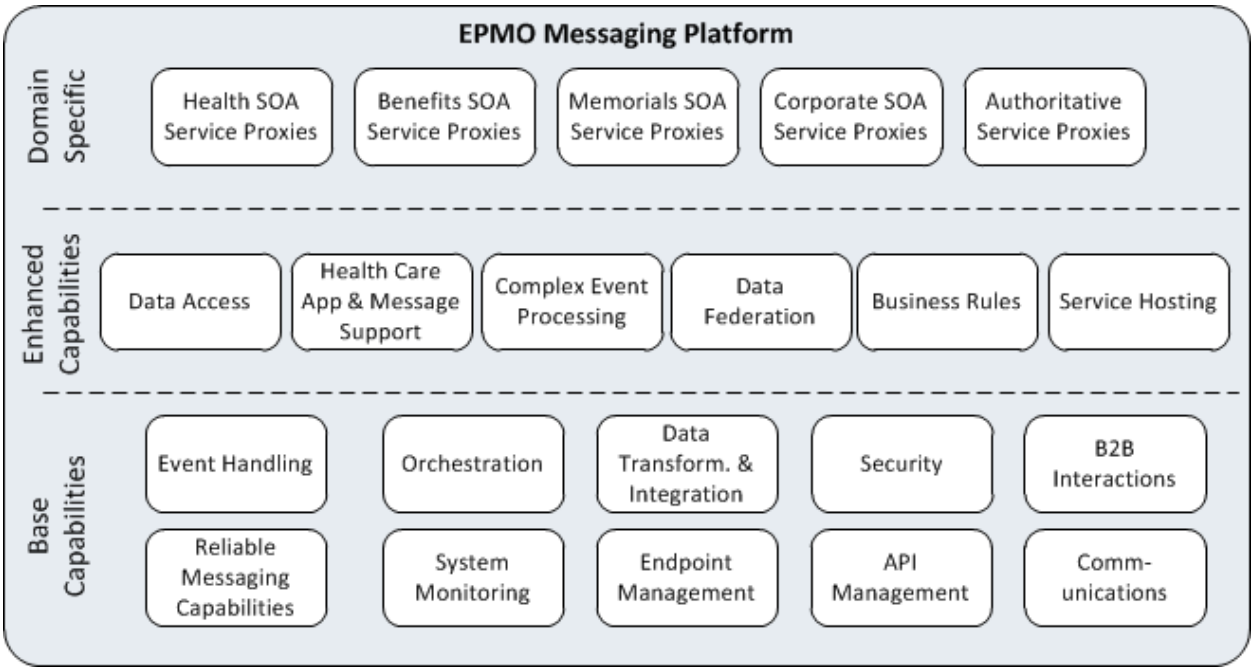


FIGURE 5: EPMO MESSAGING PLATFORM CAPABILITIES

Services provided by the EPMO Messaging Platform will include those listed in Table 4.[26]

TABLE 4: EPMO MESSAGING PLATFORM SERVICES

Service	Description
Domain Specific	
Health SOA Service Proxies	Translates service calls between various client service protocols and those used by the Health SOA services
Benefits SOA Service Proxies	Translates service calls between various client service protocols and those used by the Benefits SOA services
Memorials SOA Service Proxies	Translates service calls between various client service protocols and those used by the Memorials SOA services
Corporate SOA Service Proxies	Translates service calls between various client service protocols and those used by the Corporate SOA services
Authoritative Service Proxies	Translates service calls between various client service protocols and those used by an Authoritative Service
Enhanced Capabilities	

[26] Veteran Affairs EDPs cover many of these topics. The most current versions of these EDPs can be found at https://www.oit.va.gov/programs/techstrategies/edp.cfm.

Service	Description
Data Access	Provides ability to access data through various means (e.g., databases, Node.js, MUMPS, etc.)
Health Care Application and Messaging Support	Supports integration of health care applications including VistA and the integrated electronic health record (iEHR) system
Complex Event Processing	Evaluates and summaries messages as events, providing information on business conditions
Data Federation	Provides ability to aggregate data from various sources across DoD, VA, and partner systems
Business Rules	Provides rules within SOA infrastructure and methods to capture and expose rules
Service Hosting	Provides server resources to handle requests, allowing projects to provide services to VA and external users
Base Capabilities	
Event Handling	Provides a system processing workflow with event handling
Orchestration	Supports process logic to implement a composite service or automated system-to-system interactions
Data Transformation and Integration	Supports translation of data between formats, structures, and semantics to allow use by native applications
Security	Provides security services including IAM, authentication, encryption, and decryption
B2B Interactions	Supports protocols such as Applicability Statement 2 (AS2) or web services to communicate with external business partners or internal autonomous units
Reliable Messaging Capabilities	Provides messaging, message storage, and routing features to ensure high availability and reliable communications
System Monitoring	Provides health monitoring for SOA infrastructure components
Endpoint Management	Provides a run time registry to manage and support governance of end point devices
API Management	Enforces access control and traffic management for client programs at runtime
Communications	Supports interactions among applications and system components using a variety of protocols

3.2 Enhancements to SOA Infrastructure

In line with the VA Strategic Plan, enhancements to VA's overall SOA infrastructure can improve capital expenses and aid efficiencies.[27] Enhancements to VA's Service Provisioning Markup Language (SPML) infrastructure can aid authentication and authorization between users, projects, service providers, and identity provider/management.

Future efforts to synchronize between ESS repository functions (e.g., VIA, ESCP, WSRR) and reusable cloud computing services will help VA project teams to effectively discover and reuse ESS. These functions need to also synchronize with the EPMO Messaging Platform. In the near future, these efforts will need to include synchronization with the forthcoming electronic health record system and any related working groups.[28] VA project teams should make use of existing ESS where possible.

Continuing to analyze the relationship between SOA and cloud services will help VA understand the importance of SOA when introducing cloud-based services. The SOA integration platform plays a key role in integrating the existing application into cloud services and between clouds. Canonical data models combined with ontology and semantics establish the basis for linking data and processes across systems and clouds in the future.[29] SOA governance is the foundation for cloud governance. Future considerations should include the formalization of services and contracts in the SOA architecture which will serve as a template for formalizing cloud services.

3.3 Migration of Health Record System

Future VA health record management will use a new electronic health record system.[28] The new system environments are expected to be rolled out to VistA sites, one at a time. Non-EHR components such as benefits, administrative, financial, and logistics data will remain in VistA until replaced by other systems. These changes will likely require a reworking of those existing ESS that are affected by this migration. This system is expected to work closely with the DoD health record system, which may help improve Veteran access to VA benefits and services.[30]

---

[27] Source: Objective 3.3, Department of Veterans Affairs, FY 2014-2020 Strategic Plan.

[28] This is planned to be an implementation of Cerner systems (e.g., HealtheIntent, HealthShare Information Exchange, and Millennium) that will work with the system used by the DoD. Details of these deployments are still being finalized at the time of publication of this document.

[29] Source: Oracle, SOA and Cloud Computing, http://www.oracle.com/technetwork/articles/soa/ind-soa-cloud-2190513.html.

[30] This is in line with FY2014-2020 Strategic Plan objective on page 18 to "Improve Veteran Access to VA Benefits and Services."

The anticipated initial operating capability of this new system is provided by Figure 6. The HSE Platform will unify and modernize access to all VistA-based health and non-health data currently maintained in the 130+ local VistA instances, as well as consolidate and modernize legacy message-oriented integration mechanisms (e.g., Vitria Interface Engine [VIE] used to provide Health Level Seven (HL7) messaging at local Vista sites, between VistA sites, and with National systems). The HSE Platform will allow VA to transition from legacy, non-standard VistA-integration methods to a single VistA integration platform that will support key functionality:

- Improve access to VistA data with reduced impact on VistA systems;
- Federate patient record data at a national level across all Vista instances;
- Cache federated patient data to speed response times for consuming systems;
- Transform VistA data to standard formats required by consuming systems; (e.g., HL7, Consolidated-Clinical Document Architecture (C-CDA), Fast Healthcare Interoperability Resources (FHIR))
- Support message-oriented, service-oriented and Representational State Transfer (REST)-style interoperability; and
- Orchestrate and execute business processes and business rules.

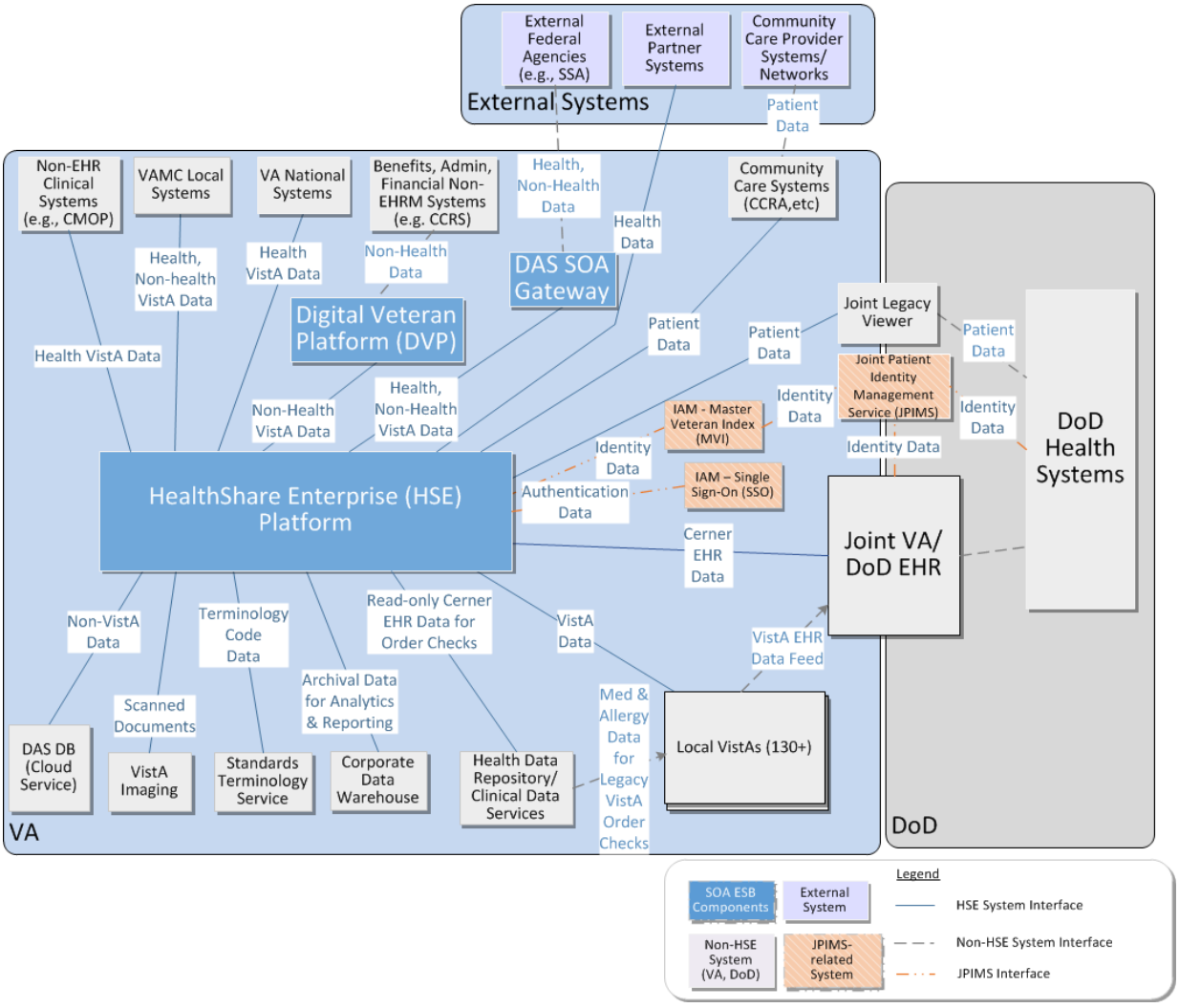


FIGURE 6: PROPOSED INITIAL OPERATING CAPABILITY OF NEW EHR SYSTEM

Health information exchanges and industry interoperability networks are trust and technology arrangements for facilitating patient information sharing. Given their increasing importance, VA executives and project teams may benefit from actively engaging and participating in these alliances (e.g., Strategic Health Information Exchange Collaborative (SHIEC))[31]. This effort to evolve VA systems will help meet customer service based on the VA FY2014-2020 Strategic Plan.[32]

[31] Additional information can be found in Figure 1.
[32] Source: FY2014-2020 Strategic Plan, Pages 32 - 34.

3.4 API Gateway

The use of an API gateway can help to publicize services, ensure security, and verify authentication of users. Planned VA project efforts include installation and use of an API Gateway to manage APIs. This will be followed by build out and testing of APIs through this service.[33]

VA will leverage enterprise-grade API gateways (often referred to as SOA gateways) to act as an intermediary guarding VA's internal web services from untrusted access. For further details, please see the Microservices,[34] Mobile Architecture,[35] Secure Messaging,[36] and User Identity Authentication EDPs.[37]

Future API gateway features that will benefit VA IT efforts include:

- **Service Contracts**: The API gateway should offer service contracts that specify performance of shared services, with minimums and maximums listed, where possible.
- **Focus on Developers**: The API gateway should focus on developer (consumer) enablement to encourage reuse.
- **Mediation of Services**: API management technologies have three core components. At the heart of the solution is an API gateway that can be deployed in a number of ways, including cloud-hosted services, physical or virtual appliances, or installed software. A single API management deployment can include multiple gateways under common control. The other two core components are an API administration capability and an API developer portal. The administration capability is used by API providers to define, manage, and monitor the publication of API endpoints and access policies associated with them. The API developer portal is used to provide self-service to API consumers, allowing them to discover APIs and documentation, access support and usage metrics, and request and manage API keys for their applications.

---

[33] Additional information can be found from Gartner, *Choosing Application Integration Technology*, October 28, 2016 and *Choosing an Architecture for Managing APIs and Services*, June 20, 2017.
[34] Reference: Office of Technology Strategies (TS), Microservices Enterprise Design Pattern, Version 1.0, July 2016, https://www.oit.va.gov/library/programs/ts/edp/cloud/Microservices_V1.pdf.
[35] Reference: Office of Technology Strategies, Mobile Architecture, Version 3.0, July 2017, https://www.oit.va.gov/library/programs/ts/edp/mobile/MobileArchitecture_V3.pdf.
[36] Reference: Office of Technology Strategies, Secure Messaging Enterprise Design Pattern, Version 2.0, September 2016, https://www.oit.va.gov/library/programs/ts/edp/privacy/SecureMessaging_V2.pdf.
[37] Reference: Office of Technology Strategies (TS), User Identity Authentication, Version 2.0, March 2016, https://www.oit.va.gov/library/programs/ts/edp/privacy/UserIdentityAuthentication_V2.pdf.

- **Publication of Services**: The API gateway should manage the publication and consumption of services via APIs, using web-based protocols. The technology also supports and promotes the service utilization, with integrated support for developer discovery and self-service through API developer portals. Using an API management solution to publish service capabilities can also provide valuable traceability of service dependencies and consumption. Most solutions also provide developer and administration portals to encourage self-service and to support the tracking and analysis of API utilization.
- **Policy Enforcement**: The API gateway should manage and enforce policies to standardize and control the use of distinct service implementations. Policies can include security, authentication, authorization, traffic management, and monetization. API management is complementary to other application integration technologies and application service implementation architectures (e.g., microservices and coarse-grained services using traditional application servers and frameworks). This is because the gateway deployment model is independent of the service implementation architecture and platform.
- **Decouple Specification from Implementation**: The API gateway should decouple API specification from service implementation. This is done by supporting basic payload and protocol mediation, including payload transformation, mapping and filtering (e.g., between SOAP and REST and between XML and JavaScript Object Notation (JSON)).
- **Flexible Deployment Model**: VA API gateway services should support a flexible and distributed deployment model. This model is supported by API management products, allowing hybrid cloud and on-premises deployment architectures. Some products support consumption-based pricing, rather than licensing deployed software instances.
- **Full Lifecycle API Management**: The implementation of an API gateway should consider full life cycle API management. This should cover planning, design, implementation, publication, operation, consumption, maintenance and retirement of APIs. It includes a developer's portal to target, assist, and govern the communities of developers who embed the APIs, as well as the runtime management and analytics.
- **Standardized Interfaces or API Management**: The API gateway should offer standardized interfaces for projects (where possible) and API management to decouple API specification from service implementation. This can include payload and protocol mediation, translation, and transformation.

VA API gateway implementation should note:

- API gateways should not be used to orchestrate complex integration requirements. Most API management products lack support for complex orchestration, sophisticated data transformation, and application adapters. The features are required to aggregate application services and data into coarse-grained composite APIs. Most products rely on protocol-level connectors, since no application or Software as a Service (SaaS)-specific connector support is available. Using integration capabilities in the API management platform dilutes the decoupling and separation of concerns between policy enforcement and service logic. When orchestration capability is available in the API gateway component, it should be used with caution.
- API gateways should not have a predominant focus on HTTP-based web services (REST, SOAP and XML-Remote Procedure Call (RPC)). Current products provide limited support for message-oriented or event-based protocols and patterns. Some products support WebSockets and/or integration with Java Messaging Service (JMS) providers.
- Most API gateways are not suitable for integration scenarios that require polling or monitoring for changes. These scenarios are best addressed by other integration technologies. Note that some API gateways support file-based interaction.

Governance of APIs and application services is no longer just about control; it's also about agile delivery and productivity. Technical professionals delivering APIs, SOA and microservices need a governance architecture to help an organization define, promote, secure and support their use.[38]

3.5 Roadmap

This roadmap section contains content on the background of SOA/shared services, SOA considerations, migration to SOA, and project selection. These considerations are helpful for expanding the use of SOA within VA.

3.5.1 Background

Pursuant to the Enterprise Roadmap (FY2016-2018),[39] reuse is foundational to digitization concepts. “Shared” services used across an organization will lower costs and accelerate delivery. VA began to adopt shared services and open architecture concepts in 2011.

[38] This use of flexible platforms is in line with VA Strategic Outcome 1B from the Office of Information & Technology Strategic Plan, December 2016.
[39] Reference: https://www.ea.oit.va.gov/EAOIT/docs/FY-2016-2018-Enterprise-Roadmap.pdf.

Until recently, the use of shared services was not enforced or managed at VA. However, in 2016, the VA Chief Information Officer (CIO) established an ESS portfolio within the EPMO to centralize shared service management in the areas of benefits, health, corporate, inter-agency, and enterprise services, such as messaging and IAM.[40] Use of shared services is one of many leading practices that OI&T leadership is adopting to better manage its resources, provide faster service to its customers, and satisfy the needs of Veterans.

3.5.2 Considerations

As indicated by Gartner research in 2016, many surveyed organizations have adopted SOA as an integration and modernization strategy.[40] While SOA can certainly help modernize integration, a focus solely on integration is not as mature as a focus on capabilities. The focus of a SOA adoption plan should be to modernize application architecture to achieve agility, manageability, and scale, and to enable systems to support digital business. An organization's SOA maturity increases as it moves from an integration-centric to a capability-centric approach. This is because the capability-centric approach is adding more value than the approach to merely integrate functionality. An illustration of this maturity is shown in Figure 7.

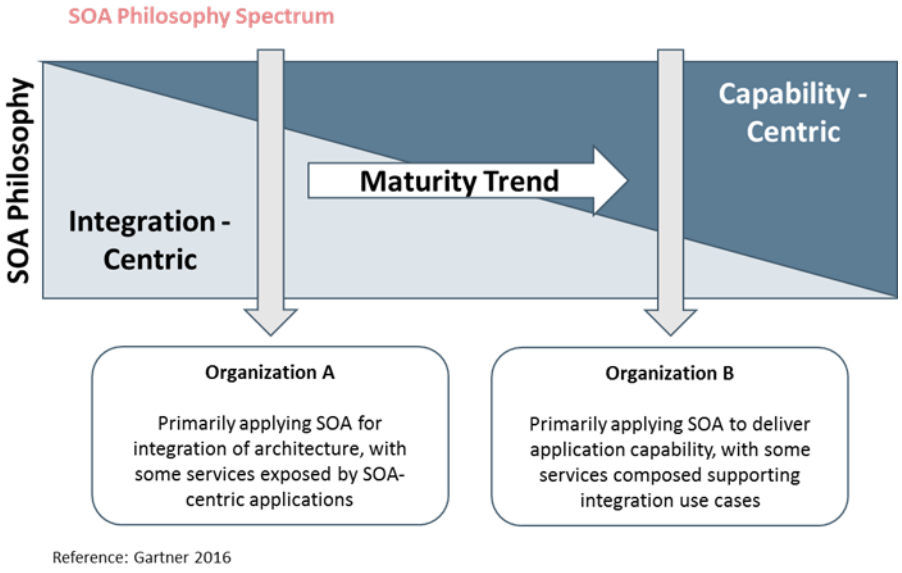


FIGURE 7: SOA MATURITY TRENDS

[40] Additional information is available from Gartner, *Where to Start (or Restart) With Service-Oriented Architecture*, October 28, 2016.

3.5.3 Migration to SOA

Recommendations for application leaders, when starting or restarting an SOA adoption plan include:

- Conduct pilot projects to enable teams to gain expertise in adopting SOA principles.
- Measure success on agility, rather than reuse.
- When needed, select commercial off-the-shelf (COTS) products that support open standards.
- Look beyond integration and concentrate on modernizing application architecture to support digital business imperatives.
- Application leaders responsible for modernizing their application architecture should:
    - From an organizational perspective — Define clear objectives and success criteria for SOA. Take an incremental approach to SOA adoption.
    - From a conceptual perspective — Apply different types of SOA appropriately, while avoiding confusion of SOA with technology.
    - From an implementation perspective — Choose API and service design patterns that ensure flexibility and usability.[41]

Pursuant to Gartner research in 2016, the path shown in Figure 8 lays the SOA foundation and moves to modern miniservice and microservice architecture. However, there is no architecture that can deliver complete agility and scalability. The architecture needs to be combined with the appropriate supporting infrastructure (outer architecture) and processes (such as the development operations software development and delivery process, DevOps) to make the systems truly agile.

SOA provides the foundations for a decision space to enable other modern architectures, such as microservices and miniservices, and other possible future considerations and next steps.

[41] References: Gartner,*The Most Common SOA Mistakes and How to Avoid Them*, May 15, 2017, and *Where to Start (or Restart) with Service-Oriented Architecture*, October 28, 2017.

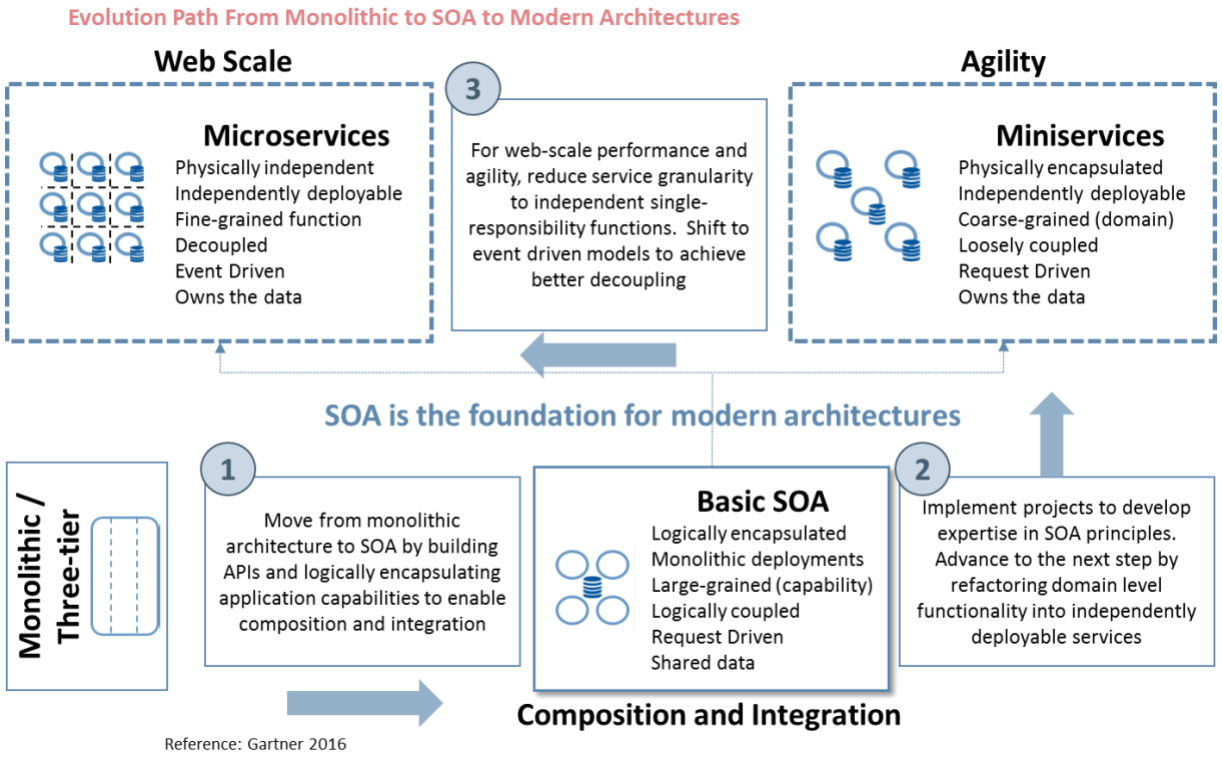


FIGURE 8: EVOLUTION PATH TO SOA

The goal of microservices architecture (MSA) is to improve development agility with deployment flexibility, scalability, and portability of application features; however, it is more costly and complex than delivering a well-structured non-distributed application. Achieving the benefits of MSA requires a high degree of development and operational maturity and automation. MSA is not based on all-new architectural principles; it combines SOA best practices with modern application delivery tooling and organizational disciplines. "Micro" is a concept of scope rather than size. A microservice should have a single purpose and be loosely coupled in design and deployed independently of other microservices. Microservices simplify the implementation (the "inner architecture") of each service, but their distributed nature requires a more complex operational environment (the "outer architecture").[42]

[42] References: Gartner, *Assessing Microservices for Cloud-Native Application Architecture and Delivery*, May 24, 2016 and 2017 *Planning Guide for Application Platform Strategies*, October 13, 2016; and Office of Technology Strategies, Microservices EDP, July 2016.

3.5.4 Value Determination and Project Selection

Gap analysis from current VA projects and from the existing library of EDP documents can help inform decisions about potential ESS that should be created. An analysis of these gaps and any newly determined gaps can be used to help identify and rank candidate ESS for development.

For each selected project, the demonstration of value is critical to gaining and maintaining momentum in the SOA adoption plan. Therefore, each project should clearly identify the metrics by which its success will be measured, both in terms of the solution's outcome and the approach used to deliver the solution.

The ability to deliver value in the first few pilot projects is especially important. If there is resistance within the organization, the implementers must carefully select pilot projects and build a business case to ensure future funding. Success can be achieved by finding projects that are small in scope and that demonstrate recognizable business value. If a team selects a large project, the risk of failure is higher, and skeptical sponsors may lose patience. On the other hand, if a team selects a project that is too small, there may not appear to be any measurable impact.

Effective SOA pilot projects have two characteristics:

- High visibility — The project addresses a recognizable business problem that clearly needs to be resolved. The project needs a business sponsor. If possible, the team should avoid technology-led projects.
- Low risk — The project does not significantly modify, extend, or enable mission-critical business processes. The use of new technology should be limited. An expensive, full-featured SOA suite is not necessary in order to deliver value.

There is a "sweet spot" for SOA pilot project candidates, where the IT complexity is lower than average, but the business value is higher. The ability to identify an appropriate project is challenging, but can result in high rewards. This is illustrated by Figure 9, which explains complexity compared to business value for different types of SOA pilot projects.[43]

[43] For a more detailed view and explanation of this diagram, refer to Gartner, *Where to Start (or Restart) With Service-Oriented Architecture*, October 28, 2016.

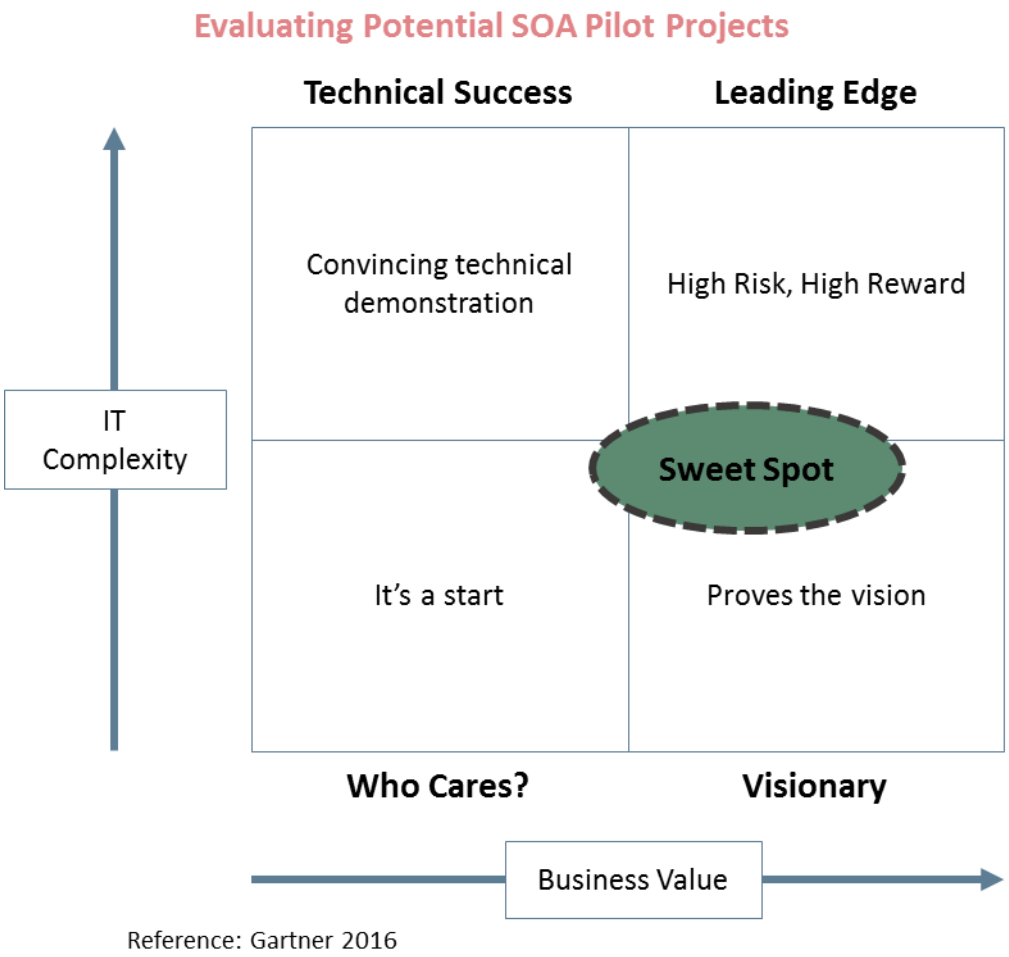


FIGURE 9: SOA PROJECT EVALUATION CONSIDERATIONS

3.6 Alignment to the One-VA Technical Reference Model (TRM)

All projects require approved technologies and standards. At VA, these are provided by the authoritative source, the One-VA Technical Reference Model (TRM), in order to ensure that VA stakeholders comply with VA and federal mandates.

Table 5 lists a selection of some of the categories of tools relevant to topics discussed in this EDP.[44]

[44] More focused future efforts will determine example standards and related ESS.

TABLE 5: TRM – ENTERPRISE SOA

Technology Category	Example Technologies
Integration Software	Enterprise Service Bus, Service Registry, Messaging-Oriented Middleware, Device Integration
Data Integration	Data at Rest, Data in Motion (Common Message Terminology and Semantics), Database Replication and Clustering (e.g., Extract, Transform, Load)

The SOA EDP serves as a gateway to other EDPs that refer to applicable ESS, as discussed in Appendix E. Each EDP contains a reference to applicable One-VA TRM categories. This information will help projects guide their technology selection and plan for future technologies. All projects that leverage enterprise SOA capabilities to achieve interoperability objectives will execute the following:

- Adhere to the profile of information exchange standards
- Use only approved standard profiles that are documented in the One-VA TRM. Standards not included in the One-VA TRM require a waiver that is approved by the Veteran-centric Integrated Process (VIP).
- For healthcare information exchange, comply with the standard profile that is enforced by the Interagency Program Office (IPO) and described in the IPO Information Interoperability Technical Package (IT2P) and DoD/VA Health Standards Profile (HSP).

3.7 Alignment to VIP

VIP is a lean-agile framework that services the interests of Veterans through the efficient streamlining of activities that occur within the enterprise. The VIP framework unifies IT delivery oversight and will deliver IT products more efficiently, securely, and predictably. VIP is the follow-on framework from the Project Management Accountability System (PMAS) for the development and management of IT projects, which propel the Department with even more rigor toward Veteran-focused delivery of IT capabilities.

3.8 Summary Considerations for Project Managers and Planners

To help further VA's SOA vision and balance innovation with governance, VA project managers and planners review the key considerations found in Table 6.

TABLE 6: VA PROJECT RECOMMENDATIONS

Section #	Consideration
3.1	• Use the HSE platform for integration in the Health domain and specifically with VistA. • VHIE external partners (e.g., Walgreens Pharmacies) shall integrate with the HSE platform. • Use DVP for integration in the Benefits, Memorial, Corporate, and Enterprise domains. Use DVP for integration across multiple domains. • Use DAS SOA gateway for integration with DoD and integration with DAS persistent data store. • Use DAS SOA gateway for integration with other external private sector service consumers (e.g., eHX) and government agencies (e.g., DoD, CMS).
3.2	• Consider using ESS where possible. The following sites document available services: ESCP at https://escp.aac.va.gov/, WSRR at https://vaausemiihtwgdev12.aac.va.gov/ServiceRegistryDashboard/, and VIA at https://vaww.viapreprod.va.gov/via-webservices/. • Consider using cloud computing GSS. Information on GSS can be found at https://vaww.portal.va.gov/sites/ECS/SitePages/What%20is%20the%20VA%20Enterprise%20Cloud%20%28VAEC%29.aspx. • Consider using GSA USSM at https://www.ussm.gov/. • Consider ways of developing project components and functionality as new ESS that can be used across VA. References to these ESS should be provided to a VA enterprise ESS repository. [45]

[45] Ideally, in a future state, the ESS repositories will be consolidated to one repository for all VA

These recommendations will address the limitations from section 2 of this document, as described in Table 7.

TABLE 7: RESOLUTION OF CURRENT STATE LIMITATIONS

Limitation	Resolution
Lack of single catalog of ESS	• Use existing catalogs of ESS (e.g., WSRR, ESCP, VIA) and shared services (cloud computing GSS, GSA USSM) until single consolidated catalog is available.
Single platform is not used for messaging (Section 2.2.2 and Table 4 detail other information sharing)	• Plan for future use of the EPMO messaging platform including its components from the HSE platform, DVP, and DAS SOA gateway
Future direction is pending, pursuant to the implementation of the new EHR system	• Follow this section of this EDP towards the future state. • Future EDPs will further address the new EHR system, once it has matured.
ESS are evolving and not all candidates for ESS are fully matured	• Use existing catalogs of ESS (e.g., WSRR, ESCP, VIA) and shared services (cloud computing GSS, GSA USSM) until single consolidated catalog is available. • Register new services as ESS.
Developmental changes are on-going, making management challenging	• Use Table 6, which provides near term recommendations. Future EDP documents will provide more clarity to deal with future developmental changes.

4 USE CASES

The following use cases are examples that demonstrate the application of the capabilities and recommendations that are described in this document. Earlier in this document, Figure 4 and Figure 5 provide the architectural blueprint for the use cases.

4.1 Use Case #1: User Consumption of Public Data

The following use case refers to a generic service interaction involving DoD, VA, or other external partner consumers (e.g., Walgreens Pharmacy), with the goal of retrieving healthcare information (e.g., official patient records, prescription information, patient- generated data), subject to appropriate security and privacy restrictions.

4.1.1 Assumptions

- Pre-Conditions
    - Requestor authenticated to an application through security services platform (currently provided by IAM services).
    - Example VA applications (portals, web applications, mobile applications, kiosks) include the following:
        - Veterans Point of Service (VPS) application
        - Mobile Patient-generated Data (PGD) (Data Access Services) application
        - External non-VA client (e.g., DoD healthcare application)

4.1.2 Use Case Description

- Inputs
    - VA user invokes a service request to access VA healthcare information
        - This may occur through a mobile application, in accordance with the Mobile Architecture EDP guidance.[46]
        - IAM services authenticate the service consumer and support access control decisions, pursuant to the Privacy and Security EDPs.[47]
- Behaviors
    - External service consumers use an external gateway (also known as a SOA gateway service) capability to access services.
        - The external gateway refers to the eHealth Exchange for commercial consumers, such as the Walgreens Pharmacies.
        - DoD consumers leverage services, as outlined in the VistA Evolution Interoperability Plan. Currently, DoD consumers may also use the eHealth Exchange, if they do not use the Bi-directional Health Information Exchange (BHIE) DoD Adaptor (per the eHMP/VX architecture). In the long-term, the Defense Health Management Systems Modernization (DHMSM) data services will continue to leverage these services.
    - Request goes to the service provider.
        - The EPMO Messaging Platform provides integration middleware for a service provider that is part of the VistA Evolution Program.

[46] Reference: Office of Information Technology, Mobile Architecture Design Pattern, Version 3.0, July 2017, https://www.oit.va.gov/library/programs/ts/edp/mobile/MobileArchitecture_V3.pdf.
[47] Reference: https://www.oit.va.gov/programs/techstrategies/edp.cfm.

        - Invalid service requests will produce error messages to users through exception handling. Failed attempts are to be logged. This is in accordance with guidance from Privacy and Security EDPs.[48]
    - Service providers are exposed through service proxies and service entries.
        - Service interfaces are to be defined in accordance with the ESS Message Exchange Guide.
        - Enterprise service registry is needed to document the services.
    - Service provider processes request through a "wrapper" data access service (per the Enterprise Data Access EDP)[49] and prepares response in accordance with requestor's expectations.
    - VistA instances generate a response through data federation platforms (currently VIA).[50]
- Outputs
    - Response is routed back to requestor.
- Post Conditions
    - Requestor obtains application response, based on initial expectations.
    - A data warehouse capability (e.g., the Corporate Data Warehouse) collects data from authoritative data stores for business intelligence and analytics purposes. VistA will continue to provide batch feeds to the data warehouses, as indicated by the solid arrow.

4.2 Use Case #2: Benefits, Memorials, and Corporate ESS Interaction

The following use case refers to a generic interaction between an internal or external service consumer and a VA application, allowing the consumer to retrieve benefits information (including memorials information).

4.2.1 Assumptions

- Pre-Conditions
    - Requestor authenticated to an application through the security services platform and is authorized to access information. Currently, these are provided by IAM services.
        - The Privacy and Security EDPs[51] provide detailed architectural guidance for these capabilities.

[48] Reference: https://www.oit.va.gov/programs/techstrategies/edp.cfm.
[49] Reference: https://www.oit.va.gov/library/programs/ts/edp/dataSharing/EnterpriseDataAccess_V2.pdf.
[50] In the long term, a new system that is based on the new EHR is expected to be used here. At the time of publication, that the system is expected to be HealthShare Enterprise (HSE).

- Example VA applications (portals, web applications, mobile applications, kiosks) include the following:
  - Enterprise Veterans Self-Service (eBenefits)
  - National Gravesite Locator (NGL) application
  - Vets.gov at https://www.vets.gov/
  - VRM Customer Relationship Management (CRM) client

4.2.2 Use Case Description

- Inputs
  - VA user sends in a service request to access VA information.
    - This may occur through a mobile application, in accordance with the Mobile Architecture EDP guidance;[52] or it may leverage a user interaction capability, per the User Interaction Capabilities EDP guidance.[53]
    - IAM services authenticate the service consumer and support access control decisions, pursuant to Privacy and Security EDP guidance.[51]
- Behaviors
  - External service consumers use an external gateway capability to access enterprise services.
    - In this context, the external gateway may refer to a web server proxy that is located in a perimeter network.
  - Service request goes to service provider.
    - Invalid service requests will produce error messages to users through exception handling. Failed attempts are logged, in accordance with the Privacy and Security EDP guidance.[51]
    - Service request may either be brokered or go directly to the service provider (details found in implementation guidance).
  - Service providers are exposed through service proxies and service entries.
    - Service interfaces are to be defined in accordance with the ESS Message Exchange Guide.
    - Enterprise service registry is needed to document the services.
    - Services expose authoritative data sources in accordance with the Enterprise Data Access EDP.[54]

---

[51] Reference: https://www.oit.va.gov/programs/techstrategies/edp.cfm.
[52] Reference: https://www.oit.va.gov/library/programs/ts/edp/mobile/MobileArchitecture_V3.pdf.
[53] Reference: https://www.oit.va.gov/library/programs/ts/edp/ea/UserInteractionCapabilities_V2.pdf.
[54] Reference: https://www.oit.va.gov/library/programs/ts/edp/dataSharing/EnterpriseDataAccess_V2.pdf.

    - Service provider processes request and prepare response in accordance with requestor's expectations. Example services include:
        - Services offered through the Data Access Service (DAS)
        - Authoritative Information Services, pursuant to the Enterprise Data Access EDP[54] (exposes authoritative data sources, including Veterans Benefits Management System (VBMS))
    - Information services equate to a VA data layer (as discussed in the Enterprise Data Access EDP) and may include VBMS, Chapter 33, Customer Relationship (CRM), DAS, corporate email, and gravesite location data (BOSS Enterprise).
        - Offline data are imported into VA data warehouses.
        - Details on VA administration data concerns are provided in the Enterprise Data Access EDP.[54]
- Outputs
    - Response is routed back to requestor.
- Post Conditions
    - The requestor obtains application response, based on initial expectations.
    - A data warehouse capability (e.g., the Corporate Data Warehouse) collects data from authoritative data stores for business intelligence and analytics purposes.

More information about benefits, memorials, and corporate ESS considerations may be found in segment-level architectural models that are under development by EPMO Demand Management.

APPENDIX A. SCOPE

This EDP document provides an enterprise-level view of the "As-Is" and "To-Be" SOA capabilities within the VA IT infrastructure. The document focuses on a vendor-independent framework for an enterprise SOA environment. It references, rather than duplicates, lower-level solution guidance.

The focus of this EDP is on the:

- Background of the "As-Is" state of the VA SOA environment
- Descriptions of key components of the Enterprise SOA environment
- "To-Be" Enterprise SOA and associated attributes
- Table of enterprise-level mobile constraints and strategic guidance

This EDP is an update to the 2015 Enterprise SOA EDP. This document is generally applicable across all VA LOBs and describes the:

- "As-Is" VA ESS and SOA capabilities
- Processes to be used by the developer and Veteran
- Enterprise-level constraints, strategic guidance, and terminology

This EDP document *does not* address detailed technical solution architecture guidance for implementation. Rather, it provides the constraints to mature VA SOA.

Document Development and Maintenance

This EDP was developed collaboratively with internal stakeholders from across the Department, including participation from VA's OI&T, the EPMO, the Office of Information Security (OIS), ASD, and Information Technology Operations and Services (ITOPS). In addition, the development effort included engagements with industry experts to review, provide input, and comment on the proposed pattern. This document contains a revision history and revision approval logs to track all changes. Significant updates will be coordinated with the Government lead for this document; the Government lead will also facilitate stakeholder coordination and subsequent re-approval.

APPENDIX B. DEFINITIONS

This appendix provides definitions for terms used in this document.

Key Term	Definition
Application Program Interface	A set of definitions of the ways one piece of computer software communicates with another; it is a method of achieving abstraction, usually (but not necessarily) between higher-level and lower-level software[55]
Application proxy	Construct involving the use of a generic, non-human "user" entity to represent "machine-to-machine" interaction, where it is appropriate for interactions that do not involve a specific end user
Auditing	The inspection or examination of an activity based on available information; in the case of computer systems, this is based on the review of the events generated by the system or application
Consuming Application	The application consuming services from a provider system; generally used when discussing a front-end application supporting a user, but even service providers can themselves be a consumer of other services
Delegated Access	When an owner authorizes another to serve as his or her representative for access to a particular resource
Enterprise Shared Service	A SOA service that is visible across the enterprise and can be accessed by users across the enterprise, subject to appropriate security and privacy restrictions
Service	A mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised, consistent with constraints and policies, as specified by the service description
Service Oriented Architecture	A paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains; it provides a uniform means to offer, discover, interact with, and use capabilities to produce desired effects that are consistent with measurable preconditions and expectations

[55] Source: https://project-open-data.cio.gov/glossary/.

APPENDIX C. ACRONYMS AND ABBREVIATIONS

The following table provides a list of acronyms and abbreviations that are applicable to and used within this document.

Acronym	Description
2FA	Two Factor Authentication
AcS	Access Services
AITC	Austin Information Technology Center
API	Application Programming Interface
AS2	Applicability Statement 2
ASD	Architecture, Strategy, and Design
BHIE	Bi-Directional Health Information Exchange
BGS	Benefits Gateway Service
CAR	Compliance Audit and Reporting
C-CDA	Consolidated Clinical Document Architecture
CCRA	Community Care Referral and Authorization
CDW	Corporate Data Warehouse
CIO	Chief Information Officer
CMS	Centers for Medicare/Medicaid
COTS	Commercial off-the-shelf
CPE	Clinical Presentation Experience
CRM	Customer Relationship Management
CSP	Credential Service Provider
DaaS	Data as a Service
DAS	Data Access Service
DGC	Data Governance Council
DHMSM	Defense Health Management Systems Modernization
DoD	Department of Defense
DSM	Direct Secure Messaging
DVP	Digital Veterans Platform
EDP	Enterprise Design Pattern
eHMP / VX	Enterprise Health Management Platform / VistA Exchange
EHR	Electronic Health Record
eHX	eHealth Exchange
eMI	Enterprise Messaging Infrastructure
EPMO	Enterprise Program Management Office

Acronym	Description
ESB	Enterprise Service Bus
ESCP	Enterprise Services Collaboration Portal
eSig	Electronic Signature
ESS	Enterprise Shared Services
ETSP	Enterprise Technology Strategic Plan
EXS	Exchange
FHIE	Federal Health Information Exchange
FHIR	Fast Healthcare Interoperability Resources
GSS	General Support Services
GSA	General Services Administration
HC IdM	Healthcare Identity Management
HIE	Health Information Exchange
HL7	Health Level 7
HSE	HealthShare Enterprise
HSP	Health Standards Profile
HTTPS	Hypertext Transport Protocol Secure
IAM	Identity and Access Management
ICN	Incident Control Number
IEC	International Electrotechnical Commission
iEHR	Integrated Electronic Health Record
IPO	Interagency Program Office
IRS	Internal Revenue Service
ISO	International Organization for Standardization
IT	Information Technology
IT2P	Interoperability Technical Package
ITOPS	Information Technology Operations and Services
JMS	Javascript Message Service
JSON	JavaScript Object Notation
LOA	Level of Assurance
LOB	Lines of Business
MDWS	Medical Domain Web Services
MHV	MyHealtheVet
MPI	Master Patient Index
MSA	Microservices Architecture
MUMPS	Massachusetts General Hospital Utility Multi-Programming System

Acronym	Description
MVI	Master Veteran Index
NGL	National Gravesite Locator
NHIN	Nationwide Health Information Network
OIS	Office of Information Security
OI&T	Office of Information and Technology
OMB	Office of Management and Budget
ONC	Office of the National Coordinator
PAD	Planning Analysis Document
PE	Product Engineering
PGD	Patient Generated Data
PIV	Personal Identity Verification
PM	Project Manager
PMAS	Project Management Accountability System
RDW	Regional Data Warehouse
REST	Representational State Transfer
RPC	Remote Procedure Call
SaaS	Software as a Service
SAC	Specialized Access Control
SecID	Security Identifier
SHIEC	Strategic Health Information Exchange Collaborative
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
SPML	Service Provisioning Markup Language
SSA	Social Security Administration
SSOe	Single Sign On External
SSOi	Single Sign On Internal
STS	Secure Token Service
TRM	Technical Reference Model
TS	Technology Strategies
USSM	Unified Shared Services Management
VA	Veterans Affairs
VAMC	VA Medical Center
VAP	Veterans Authorizations and Preferences
VBMS	Veterans Benefits Management System
VHA	Veterans Health Administration
VIA	VistA Integration Adapter

Acronym	Description
VIE	Vitria Interface Engine
VIERS	Veteran Information Eligibility Record Services
VIM	Vendor Independent Messaging
VIP	Veteran-Centric Integration Process
VistA	Veterans Health Information Systems and Technology Architecture
VLER	Virtual Lifetime Electronic Record
VPS	Veterans Point of Service
WS	Web Services
WSRR	WebSphere Service Registry and Repository
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language

APPENDIX D. REFERENCES, STANDARDS, AND POLICIES

VA project teams and stakeholders may benefit from reviewing the content in the following references and standards. These cover many topics related to this area.

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
1	VA	VA 6500 Handbook	Defines the overall security framework for VA, including data storage, retrieval, and exchange
2	VA	VA EDPs – Office of Technology Strategies	Defines the enterprise IT capabilities that are provided through ESS; ESS will be deployed for use by all VA applications, regardless of the end-user device
3	VA	ESS Directive	Establishes policy regarding the development, deployment, and management of ESS in VA
4	VA	VA Enterprise Technology Strategic Plan (ETSP)	Helps projects develop applications in alignment with the SOA attributes of the ETSP's IT Vision
5	VA	VA Directive 6551, http://www.techstrategies.oit.va.gov/docs/designpatterns/6551dir16.pdf	Establishes a mandatory policy for establishing and utilizing EDPs by all VA projects developing IT systems, in accordance with VA's OI&T VIP, the integrated development and release management process
6	VA	Enterprise Service Collaboration Portal (ESCP), https://escp.aac.va.gov/	Lists authoritative enterprise data and essential enterprise data services to help VA system and application developers to search, view, request, and consume
7	VA	VistA Integration Adapter (VIA) web services, https://vaww.viapreprod.va.gov/via-webservices/	Lists VistA Integration Adapter (VIA) API services, available for consumption with link to Web Service Description Language (WSDL) for each service
8	VA	VA Identity and Access Management, https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=823&FType=2	Provides identity and access management policies for VA
9	OMB	OMB Memorandum M-11-11, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-11.pdf	Mandates use of PIV as common means of authentication for personnel

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
10	The Open Group	http://www.opengroup.org	Provides a reference SOA architecture
11	OMB	OMB M-04-04, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2004/m04-04.pdf	Provides policy for assurance of electronic transactions that require authentication
12	OMB	OMB M 16-11, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-11.pdf	Provides policy on a federal IT shared service model

APPENDIX E. ENTERPRISE SHARED SERVICES

This appendix describes a sampling of various ESS available within VA. Readers may also wish to reference the ESCP Service Catalog, WSRR, and VIA for further descriptions and details.[56] These online resources list more services than the table in this section.

#	Project	Service	Description
1	CDW	VA Corporate Data Warehouse	Organizes clinical data into a logical data domain (e.g., pharmacy, lab chemistry, etc.)
2	EPMO Messaging Platform	Enterprise Message Broker	Enables message exchanges between VA systems and service messaging engine
3	IAM	Master Veteran Index (MVI)	The authoritative source for personal identity data; maintains identity data for persons across VA systems; provides a unique universal identifier for each person; stores identity data as correlations for each system where a person is known; provides a probabilistic matching algorithm; (Includes MPI, PSIM, and IdM TK); maintains a gold copy, known as a Primary View, of the person's identity data; broadcasts identity trait updates to systems of interest; maintains a record locator service
4	IAM	Electronic Signature (eSig)	eSig enables Veterans and their surrogates to digitally sign forms that require a high level of verification that the user signing the document is a legitimate and an authorized user; in addition, eSig provides a mechanism for VA applications to verify the authenticity of user documents and data integrity on user forms

[56] References: ESCP at https://escp.aac.va.gov/; WSRR at https://vaausemiihtwgdev12.aac.va.gov/ServiceRegistryDashboard/; and VIA at https://vaww.viapreprod.va.gov/via-webservices/.

#	Project	Service	Description
5	IAM	Specialized Access Control (SAC)	SAC will enable an application to authorize and control access down to the transaction, field or object levels if needed; provides an Extensible Access Control Markup Language (XACML) based web-service interface for fine grain authorizations; leverages attributes; such as digital identity, credentials, user attributes, contextual or environmental attributes, from a variety of sources, in conjunction with resource policies, to make real-time access control decisions
6	IAM	Directory Services	Efficiently stores and manages user information and provides a comprehensive view of predefined authoritative data managed by IAM for all users across the VA enterprise
7	IAM	Identity Proofing	The step in the IAM process where an end-user initially establishes their identity with a registration agent or authority
8	IAM	Credential Service Provider (CSP)	Provides a VA operated Level 1 and Level 2 credential for individuals who require access to VA applications, yet cannot obtain a credential from another VA accepted credential service provider (i.e. DS Logon); linked with the SSOi and SSOe programs
9	IAM	Single Sign On External (SSOe)	Allows a user that is authenticated at a federated CSP (IdP) to seamlessly access integrated applications; provides single sign-on solution for internal facing VA applications; authenticates users with CSP credentials and other externally-issued credentials (including mapping of credential to VA identity) (IBM tools)
10	IAM	Single Sign On Internal (SSOi)	Provides single sign-on solution for internal facing VA applications; allows internal users access to a variety of VA systems and applications using a reduced set of login credentials, including VA-issued PIV cards (LOA 4) and credentials generated by the VA Active Directory (LOA 2); supports application implementation of PIV requirement
11	IAM	Compliance Audit and Reporting (CAR)	Provides the capability to monitor integrated applications and services to produce reports and generate alerts triggered by events or breach of predetermined event thresholds

#	Project	Service	Description
12	IAM	Provisioning	User provisioning is the process of associating a digital identity with one or more resource access accounts, which may serve as records for user data and permissions; may include the creation, modification, deletion, suspension, or restoration of such accounts and also synchronizing user data
13	Legacy VistA	VistA Instances	An installed copy of the VistA software at a particular location
14	VLER DAS	DAS	VLER Gateway – Authentication, Authorization, Audit & Access Control; many aggregators, transformers, splitters, routers, etc.
15	VLER DAS	eCRUD Wrapper	Provides designated common enterprise services, including enterprise Create/Read/Update/Delete (CRUD) services for enterprise data stores
16	VLER DAS	Persistence as a Service	The VLER Data Access Service (DAS) is responsible for transfer of structured and non-structured storage of VLER data between internal and external consumers and producers
17	VLER eHealth Exchange	External Gateway	The eHealth Exchange Service's (formerly the NHIN) technology and standards provide a secure, nationwide, interoperable, health information infrastructure; connects providers, consumers, and others involved in supporting health and health care
18	VistA Integration Adapter (VIA) API	VistA Integration via WSDL	Interface with VistA for patient records, patient lookup, order management, scheduling, lab data, hospital locations, and other services
19	VistA Exchange / eHMP	Data Federation	VistA Exchange will provide 'native federation' to all appropriate longitudinal health record data