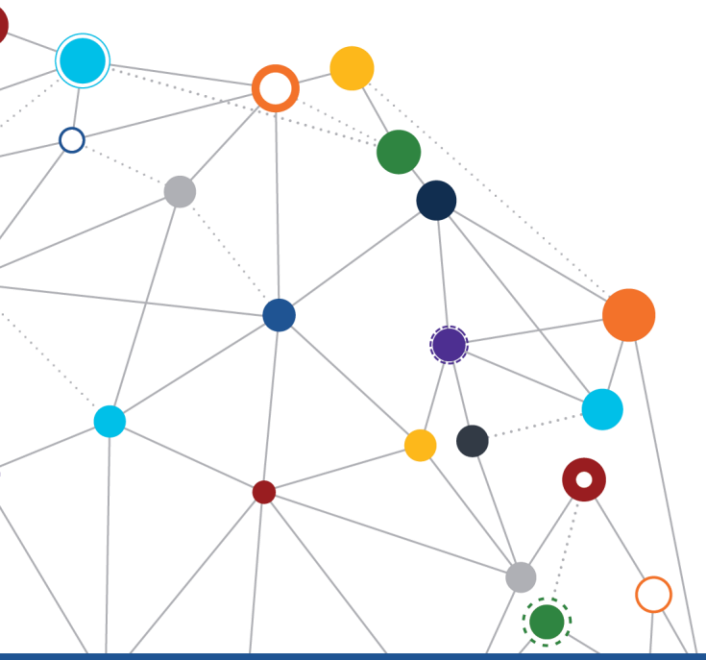
OFFICE OF
INFORMATION
AND TECHNOLOGY

Application Programming Interface (API) Enterprise Design Pattern

API Management

August 2018 | Demand Management Division



VA | U.S. Department of Veterans Affairs
Office of Information and Technology

Table of Contents

Table 1: Change Matrix

Version	Date	Description of Updates
1.0	08/03/2018	API EDP Segment 3 document approved

1 Context

The Department of Veterans Affairs (VA) implements numerous information technology (IT) projects with Application Programming Interfaces (APIs) that expose underlying services. This document provides recommendations to project teams for discovery, configuration management, data management, API gateways, and analytics, promoting greater use and reuse of APIs and services.

2 Problem

The technical management of APIs within VA span multiple management platforms. The absence of a common approach, platform, and resources for managing APIs can lead to inefficiencies and difficulties in centralization. Frequent updates of APIs can break backward compatibility and lead to rework for applications that consume APIs.

3 Approach

This document seeks to resolve API management issues by providing actionable steps and planning recommendations for project teams in the areas of discovery, configuration, data management, gateway services, and analytics.

3.1 Discovery

To ensure APIs are discoverable by automated platforms, project teams should:

- Discover APIs through VA Enterprise Architecture Repository (VEAR) and developer.va.gov (when available). Adhere to the documentation standards found in the API Documentation Standard Enterprise Design Pattern (EDP).[1]
- Where possible, ensure that all APIs share a common schema or structure (e.g., common date time format, common image format, common record format) to reduce the number of service response structures that must be managed.[2]
- Design APIs and data representations with focus on a subject area (e.g., clinical, research, supply chain, logistics).

[1] Reference the VA *API Documentation Standard EDP*, June 2018, at https://www.oit.va.gov/library/files/edp/apis/APIEDP_DocumentationStandard_v1.pdf.

[2] More information on data formats will be made available in the VEAR at https://vaausdarapp41.aac.dva.va.gov/ee/. If additional information is needed, project teams may choose to contact the Data Governance Council (DGC) Secretariat at *VADataGovernanceCouncil@va.gov*. Open Data should be machine-readable and follow *Office of Management and Budget Memorandum 13-13* at https://digital.gov/open-data-policy-m-13-13/.

3.2 Configuration Management

To ensure successful API configuration management and governance, project teams should:

- Where possible, retain the same API version so that existing VA projects can continue to interface with the corresponding, underlying service. Avoid changes to the API that will break compatibility with existing VA consuming applications.
    - Design for backward compatibility to the maximum extent possible. If compatibility is broken, keep the frequency of such major API changes to a minimum.
    - Employ techniques such as continuous release and automated deployment for the underlying service software, while maintaining the same API version. The versioning of the API should not be tied to the service software versioning.
- When API deprecation is necessary, mark older versions of APIs for retirement to address API version management.
    - Alert the application owners 180 days ahead of deprecation and work with them to enable applications to use the new API version.
    - When an API version is identified as deprecated, developers should be alerted through deprecation warnings. For example, provide a warning that the API is deprecated as an output parameter that will show in system logs.
    - With appropriate notification, retire and remove deprecated APIs from the platform to avoid maintenance overhead.
- Define an API testing strategy to ensure that APIs have the necessary levels of security, reliability, and governance.[3]
- Ensure that the metrics and responsibilities of the Service Level Agreement (SLA) are implemented by the API and service provider.
- Validate and document legacy APIs when the legacy API is incorporated into a project.[4] After a legacy API is documented and tested, publish and maintain the API documentation in the VEAR. Retain copies of this documentation with the system operating the API.[5]
    - Software code and APIs that VA previously funded are available for use, but need to be validated by project teams. This will ensure that legacy APIs still in use are properly documented and managed.

[3] Reference the VA *API Release Standard* EDP segment at https://www.oit.va.gov/library/files/edp/apis/APIEDP_ReleaseStandard_v1.pdf. For more information, consult the VA *API* Security Pattern, when available.
[4] For additional information, reference the VA *API Documentation Standard* EDP segment, June 2018, at https://www.oit.va.gov/library/files/edp/apis/APIEDP_DocumentationStandard_v1.pdf.
[5] Reference the VA *API Documentation Standard* EDP segment, June 2018, at https://www.oit.va.gov/library/files/edp/apis/APIEDP_DocumentationStandard_v1.pdf.

    - Use existing VA API capabilities before creating new APIs and services.[6]
- Ensure that APIs and the underlying services align to VA strategic and business requirements.[7]
    - For example, APIs and their exposed services should align to the Systems and Application Domain of the VA EA and be consistent with the VA Digital Modernization Strategy of April 2018.[8]
    - Consult developer.va.gov (when available) for additional information on strategy and business requirements.

3.3 Data Management

APIs are often used to create, read, update, and delete data and are sometimes solely used in a data access and management capacity. Where APIs are used to interact with data sets, project teams should undertake data management steps.

When providing an API and the underlying service:

- Document the intended API purpose, required data, and data quality expectations.[9]
- In designing a new API, review a catalog of Authoritative Data Sources (ADS) to determine ADS for each data element.[10]
- Gather relevant API or data source artifacts (e.g., API documentation, data dictionaries, data models, reference data, business rules) to understand the candidate data, its associated requirements, and limitations. Consult the VA EA Data and Information Domain found in the VEAR to use consistent information classes.[11]
- Examine high-level descriptive statistics in coordination with the business owner to determine if there are data quality concerns to remediate.
- Define data quality requirements and dimensions based on the desired use of the API. This information should be provided with the API documentation to inform consumers of the API's quality and limitations.[12]

---

[6] Reference the VA *API Release Standard* EDP segment, June 2018, at https://www.oit.va.gov/library/files/edp/apis/APIEDP_ReleaseStandard_v1.pdf.
[7] Reference the VA Enterprise Architecture at https://www.ea.oit.va.gov/.
[8] Reference the VA Digital Modernization Strategy, April 2018, at http://vaww.ea.oit.va.gov/wp-content/uploads/2018/08/DigitalModernizationStrategy_080118.pdf.
[9] Data fields, quality, functionality, and definitions should be provided with the API documentation. For more information, reference the VA *API Documentation Standard* EDP segment at https://www.oit.va.gov/library/files/edp/apis/APIEDP_DocumentationStandard_v1.pdf.
[10] The VEAR may include relevant data source information at https://vaausdarapp41.aac.dva.va.gov/ee/. Work with the Data Governance Council (DGC) if an approved data source cannot be identified or does not exist.
[11] VEAR is available at https://vaausdarapp41.aac.dva.va.gov/ee/.
[12] These should be based on the DGC data quality dimensions: accuracy, completeness, consistency, timeliness, traceability, uniqueness, and validity. Also reference the VA *API Documentation Standard* EDP segment, June 2016, at https://www.oit.va.gov/library/files/edp/apis/APIEDP_DocumentationStandard_v1.pdf.

- Review data quality analysis results. Create reports which support review of anomalous data. Participate in iterative discussions with the data source partner on actions necessary to address data defects.
- Establish a Memorandum of Understanding (MOU) with the data source partner that specifies the type of data access and frequency of access that is permitted via the API.
- Document, publish, and maintain information about the API data specification.[13]

When consuming an API:

- Document the intended business use of known API consumers, including required data and data quality expectation.[14]
- Discover, understand, and implement an API data agreement (i.e., API data specification).

3.4 API Gateway

The capabilities of an API Gateway are a critical part of an API-driven business strategy. This capability will be hosted at api.va.gov (when available). Project teams should work to ensure their APIs and underlying services are configured as follows:

- Register APIs on api.va.gov (when available) so that external partners can authenticate and use the service.
- Use API gateway, which will monitor traffic, prioritize traffic, and throttle traffic where needed. The gateway can help to ensure that spikes of traffic will not overload backend services.[15]
- Where available, use VA API gateway functions for consuming/invoking APIs to streamline development efforts, orchestrate calls, validate data, and ensure consistent security practices are followed.
- When implementing microservices for an API, consult section 3 of the Microservices EDP for additional recommendations.[16]

[13] For more information on documentation and publishing, reference the VA *API Documentation Standard* EDP segment, June 2016, at https://www.oit.va.gov/library/files/edp/apis/APIEDP_DocumentationStandard_v1.pdf.
[14] Consult common use cases documented by 18-F at https://github.com/18F/api-standards.
[15] Additional content on API gateways can be found in the VA *Secure Messaging* EDP, September 2016, at https://www.oit.va.gov/library/programs/ts/edp/privacy/SecureMessaging_V2.pdf.
[16] Refer to the VA *Microservices* EDP, July 2016, at https://www.oit.va.gov/library/programs/ts/edp/cloud/Microservices_V1.pdf.

3.5 Analytics

Analytics help API developers and the underlying service providers to understand usage and performance. Developers of APIs and related service developers are required to:

- Use analytics to monitor API and service performance, including response time, uptime, number of API calls, errors, latency, and backend service performance. DevOps staff should use this information as a feedback loop to adapt and adjust the API and underlying service, using scalability.[17] Publish API performance information and data as a scorecard for API consumers to reference.
- Develop business metrics for each API on a case-by-case basis. Use analytics to understand API usage and plan for improvements. Determine key metrics (e.g., number of developers using the API, usage and adoption trends, user sources).[18]
- Monitor and log API traffic and performance to aid security posture.[19] Enterprise services are available from the Enterprise Cloud Solutions Office (ECSO).[20]
- Guarantee API runtime quality through analyzing certain features, such as API monitoring, deployment, and dynamic provisioning.

4 Application

The Design, Engineering, and Architecture (DEA) user stories have a standard for service access and documentation, VistA Integration Control Registrations (ICRs), and web traffic and performance analytics. Project teams using the Veteran-focused Integration Process (VIP), or developing or retaining APIs, must comply with the approved standards in the One-VA TRM; and map to the DEA user stories below. Future changes in the standard will be reflected in the One-VA TRM; and in pertinent DEA user stories that are related to both API consumption and provisioning.

[17] For more information on application and service performance monitoring, refer to the VA *End-to-End Application Performance Management* (APM) EDP, August 2017, at https://www.oit.va.gov/library/programs/ts/edp/ea/ApplicationPerformanceManagement_v3.pdf.
[18] For web-based services or applications, the API is available through the Digital Analytics Program (DAP), which provides Google Analytics for federal government web sites. More information is available at https://digital.gov/dap/.
[19] More information on enterprise audit is available in the VA *Enterprise Auditing* EDP, February 2015, https://www.oit.va.gov/library/programs/ts/edp/privacy/EnterpriseAuditing_v1.pdf.
[20] More information on General Support Services (GSS) that can support traffic monitoring can be found at https://vaww.portal.va.gov/sites/ECS/SitePages/VA-Enterprise-Cloud-VAEC.aspx.

Table 2: DEA User Stories

DEA User Story	Title	User Story Text	Relevant User Story Acceptance Criterion
DEA.04.17.01	Service Access	As an Enterprise Architect, I need exposed and published interfaces so that systems are loosely coupled, with uniform behavior, and have defined and limited interaction.	(1/1) 100% of enterprise-level services have exposed and published interfaces.
DEA.04.17.02	Service Enabled Information Sharing	As an Enterprise Architect, I need Service Enabled Information Sharing so that services can be reused across the enterprise, reducing costs and resource requirements, while improving quality.	(1/1) Analysis to identify the available Shared Enterprise Services required for the solution in the VA Service Registry has been conducted and results documented.
DEA.04.18.02	Web Analytics	As an Enterprise Architect, I need Web Analytics so that web performance and customer satisfaction tools are implemented on all Department of Veterans Affairs (VA) government websites, providing objective performance analytics to improve the development and delivery of effective digital government services.	(1/3) Per Milestone 8.2 of the Digital Government Strategy, product must adhere to the implementation guidance of the GSA federally funded Tier 2 implementation of Google Analytics. (2/3) Product must not expose, or make vulnerable, any personally identifiable information (PII) or protected data and be operated in accordance with all Federal and Department Privacy and Security Policies.
DEA.04.24.01	Service Design and Documentation	As an Enterprise Architect, I need consistent and reusable service design	(1/2) 100% of Enterprise Shared Services are reviewed for compliance with published guidelines, including publication in

DEA User Story	Title	User Story Text	Relevant User Story Acceptance Criterion
		and documentation so that interactions between systems are known, and costs can be lowered through reuse and consumer discovery	the VA Service Registry, if applicable. (2/2) 100% of APIs that meet the OpenAPI specification standard must be documented according to the API EDP Documentation. Template and published in the VEAR.
DEA.04.24.03	Conceptual Design Documentation	As an Enterprise Architect, I need standardized architecture and engineering conceptual design so that stakeholders can determine whether the product concept meets real customer needs and is technically feasible. Standard conceptual diagrams provide consistent, reusable, and modifiable documentation, which supports compliance reviews, maintainability, and the security of the VA Enterprise	(3/5) The product architecture and design documentation includes a Conceptual Software Design Component Diagram that depicts the high-level software components of the product.
DEA.04.24.02	Detailed Design Documentation	As an Enterprise Architect, I need standardized architecture and engineering detailed design so that stakeholders have consistent, reusable, and modifiable	(4/5) The product architecture and design documentation includes an Application Design Component Diagram that depicts the software components of the product, their attributes and operations, and their public and private interfaces.

DEA User Story	Title	User Story Text	Relevant User Story Acceptance Criterion
		documentation, which supports compliance reviews, maintainability, and the security of the VA Enterprise.	
DEA.04.25.02	Integration Control Registrations (ICRs)	As an Enterprise Architect, I need Integration Control Registrations (ICRs) so that I have a mechanism for identifying and documenting integration points with VistA, including application logic available for reuse by consuming applications, while reducing the risk to custodial and consuming applications.	(1/2) ICRs are in an active status prior to application installation into a production system. (2/2) Updates to ICRs are successfully completed without a negative impact to consuming applications.
DEA.04.26.01	Enterprise Design Patterns	As an Enterprise Architect, I need Enterprise Design Patterns so that system design at VA is systematic, reusable, and compliant with VA Directive 6551.	Conduct an analysis of Enterprise Design Patterns (EDPs) to determine which are applicable and can be implemented by the product solution.

Future updates of this document will reflect updates to the DEA compliance criteria to reflect the guiding principles for API release. Compliance with these standards apply to the following major project scenarios:

- All new development efforts leveraging the VAEC
- All new and existing APIs that expose ADS
- All new and existing APIs that provide endpoints for approved Enterprise Shared Services (ESS)

5 Impacts

If standard API management approaches are not followed, the following negative impacts may be realized across the VA enterprise and projects:

- VA will not capitalize on reuse possibilities if APIs are not discoverable by developers and easy to use
- Lower efficiency and security risks if there is no API gateway to serve as a single point of entry
- Limited or isolated visibility into API usage and enterprise performance without common approaches to analytics

Appendix: References

- Office of Management and Budget Memorandum 13-13, https://digital.gov/open-data-policy-m-13-13/
- VA Digital Modernization Strategy, April 2018, http://vaww.ea.oit.va.gov/wp-content/uploads/2018/08/DigitalModernizationStrategy_080118.pdf
- VEAR, https://vaausdarapp41.aac.dva.va.gov/ee/
- API Documentation Standard, June 2016, https://www.oit.va.gov/library/files/edp/apis/APIEDP_DocumentationStandard_v1.pdf
- Microservices EDP, July 2016, https://www.oit.va.gov/library/programs/ts/edp/cloud/Microservices_V1.pdf
- Secure Messaging EDP, September 2016, https://www.oit.va.gov/library/programs/ts/edp/privacy/SecureMessaging_V2.pdf
- VA Enterprise Cloud General Support Services, https://vaww.portal.va.gov/sites/ECS/SitePages/VA-Enterprise-Cloud-VAEC.aspx
- Digital Analytics Program (DAP), https://digital.gov/dap/
- End-to-End Application Performance Management (APM) EDP, August 2017, https://www.oit.va.gov/library/programs/ts/edp/ea/ApplicationPerformanceManagement_v3.pdf
- Enterprise Auditing EDP, February 2015, https://www.oit.va.gov/library/programs/ts/edp/privacy/EnterpriseAuditing_v1.pdf
- 18F GSA API Standards: https://github.com/18F/api-standards
- VA DEA Assessment Guidance: https://vaww.portal2.va.gov/sites/asd/AERB/DEA_Assessment/DEA%20User%20Story%20Alignment/Home.aspx
- VA Directive 6551: https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=829&FType=2

Disclaimer: This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.

Statement of Endorsement: Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, and shall not be used for advertising or product endorsement purposes.