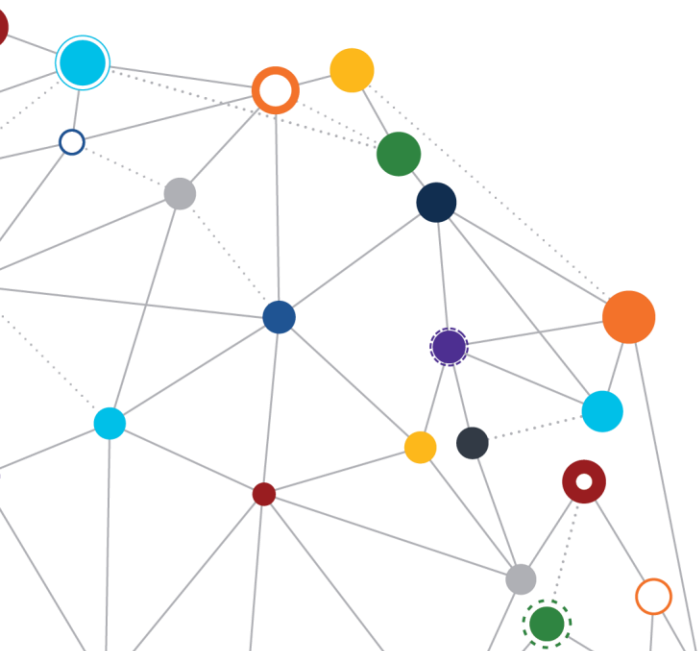OFFICE OF
INFORMATION
AND TECHNOLOGY

# Mobile Veteran-Facing Applications
# Enterprise Design Pattern

*Mobile Veteran-Facing Applications Development: Migrating and Developing Applications within the VAEC; Ensuring a Scalable and Secure Infrastructure*

August 2018 | Demand Management Division

**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 | Mobile Veteran-Facing Applications EDP Segment 2 document approved |

# 1   Context

The information technology (IT) project teams at the Department of Veterans Affairs (VA) are provided with standard approaches to transitioning to the cloud; including migrating existing mobile applications to the cloud, and initiating mobile application development within the cloud. The Cloud First Policy[1] at VA adopts a cloud computing environment for mobile computing as the basis for improved mission services and capabilities. The hybrid cloud for mobile computing hosts at least some of the data and services within VA's own infrastructure to protect sensitive workloads, while other workloads operate within shared cloud deployment models.

# 2   Problem

The current VA Mobile Framework (VAMF) is challenged to support rapid elasticity, since resources must be forecasted with the platform provider.[2] The VAMF provides an internet-accessible layer of services to isolate VA mobile applications from the VA infrastructure; and provide secure access to VA back end services.

# 3   Approach

VAMF and the Mobile Application Environment (MAE) will transition to the VA Enterprise Cloud (VAEC).[3] The MAE provides a development environment that incorporates tools and services for developers within the VA network.[4] The VAMF provides the infrastructure to allow VA applications to be hosted within a standard architectural mobile cloud services (MCS) framework.

## 3.1 Migrating existing applications to VAEC

All project teams developing Veteran-facing applications should comply with the business rules that follow.

- Perform a Cloud Readiness Review for applications by utilizing the Cloud Suitability Questionnaire, developed as part of the *Suitability Methodology & Assessment* deliverable.[5]

---

[1] Reference the *Cloud First* policy, articulated within VA Directive 6517*, Cloud Computing Services*, at http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=852&FType=2.

[2] Reference the VAMF at https://mobile.va.gov/content/mobile-app-environment-and-services.

[3] Reference the Department of Veterans Affairs *Cloud Strategy Roadmap*, FY18 & FY19.

[4] Reference the MAE at https://mobile.va.gov/content/mobile-app-environment-and-services.

[5] For information on cloud readiness for individual systems and applications, reference the *Suitability Methodology & Assessment of Sample Target Applications Deliverable*, Office of Information and Technology (OIT), December

- If Cloud Readiness Criteria are met, transition existing applications to the VAEC through the VA Enterprise Cloud Service (ECS) intake process.[6]
- Host applications on the VAEC in accordance with VA Cloud Policy, based on the Federal Risk and Authorization Management Program (FedRAMP) impact levels, as shown in the table below.[7]

*Table 2: Cloud Platform Hosting Guidance*

| FedRAMP Impact Level | Cloud Platform |
| --- | --- |
| **High** | VAEC<br>On-site Private Cloud |
| **Moderate** | Cloud.gov |
| **Low** | Cloud.gov |

- Perform end-to-end testing of the migrated application.

## 3.2 Developing new mobile applications within the VAEC

- Use Enterprise Shared Services (ESS) for new applications. Examples of ESS include shared services from eight provider organizations that are located at the Enterprise Service Collaboration Portal (ESCP)[8]; and the VistA Integration Adapter (VIA) Web Services Description Language (WSDL) files.[9] Additional examples are provided in Appendix B.
- Develop applications within the VAEC.

---

20, 2017 and VA Directive 6517, *Cloud Computing Services*, at http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=852&FType=2.

[6] Refer to the *VA Cloud Strategy Roadmap* at https://vaww.portal.va.gov/sites/ECS/_layouts/15/WopiFrame.aspx?sourcedoc=/sites/ECS/Shared%20Documents. /ECSO%20Team%20Information/Welcome%20Kit/10.%20VA-OIT-EPMO-Cloud%20Strategy%20Roadmap%200- %20v6-2.docx&action=default&DefaultItemOpen=1. The intake process is also subject to *the Unified OIT Intake Process Guide*, August 1, 2018, focused on solution planning before project requirements are addressed through the Veteran-focused Integration Process (VIP), at https://vaww.vashare.oit.va.gov/sites/dmo/dmdocsite/DM%20External%20Government/OIT%20Intake%20Proces s%203.0%20Job%20Aids%20and%20Supporting%20Documents/Guide_Unified%20OIT%20Intake%20Process.docx. It is focused on solution planning before project requirements are addressed through the Veteran-focused Integration Process (VIP).

[7] Reference FedRAMP impact levels at https://www.fedramp.gov/search-results/?search=fedramp+impact+levels.

[8] The Enterprise Service Collaboration Portal (ESCP) is accessed at https://escp.aac.va.gov/. The ESCP portal includes eight provider organizations; within these organizations are 190 shared services to date. Provider organizations include Orchestration Services, formerly Customer Gateway Services (CGS); Non-VistA Health Services (includes Tooling and Data Management); Architecture Support Group; Benefit Gateway Services; Identity and Security Services; Interagency Services, and Vet360.

[9] The VistA Integration Adapter (VIA) is referenced at https://vaww.viapreprod.va.gov/via-webservices/.

- Host applications on the VAEC, in accordance with VA Cloud Policy and based on FedRAMP defined impact levels, as referenced in Table 2.
- Application designers: Utilize the General Support System (GSS) Services provided by the VAEC,[10] in accordance with VA Native Cloud Technology Policy.[11] GSS Services include both common services (e.g. active directory, disaster recovery, monitoring) and common security and scanning tools (e.g. BigFix, Splunk).
- Perform project end-to-end testing.

## 3.3 Ensuring scalability and a secure infrastructure

- Ensure that projects utilize the Identity and Access Management (IAM) Federated Identity Management (FIM) System.[12]
- Apply Mobile Application Management (MAM) to Veteran-facing applications.[13]
- Transition the application architecture from monolithic to microservices architecture, according to the Microservices Enterprise Design Pattern (EDP)[14] and a future microservices strategy document.[15]

---

[10] Reference *General Support Services V1.0* at https://vaww.portal.va.gov/sites/ECS/SitePages/VA-Enterprise-Cloud-VAEC.aspx.

[11] Source: VA Memorandum *Use of Software as a Service, Managed Services, and Cloud-Based Native Technologies and Approaches,* April 10, 2018, Deputy Assistant Secretary Bill James, Enterprise Program Management Office (EPMO), Office of Information and Technology (OIT).

[12] Reference the VA policy on Identity and Access Management (IAM) at www.va.gov/vapubs/viewPublication.asp?Pub_ID=823&FType=2.

[13] Reference the *Mobile Veteran-Facing Application Security* EDP at https://www.oit.va.gov/library/programs/ts/edp/privacy/MobileVeteranFacingApplicationSecurity_v1.pdf.

[14] Reference the *Microservices* EDP at http://vaww.ea.oit.va.gov/enterprise-design-patterns-reports/.

[15] A microservices strategy is scheduled to be developed by VHA and ITAMs by 4QFY19.
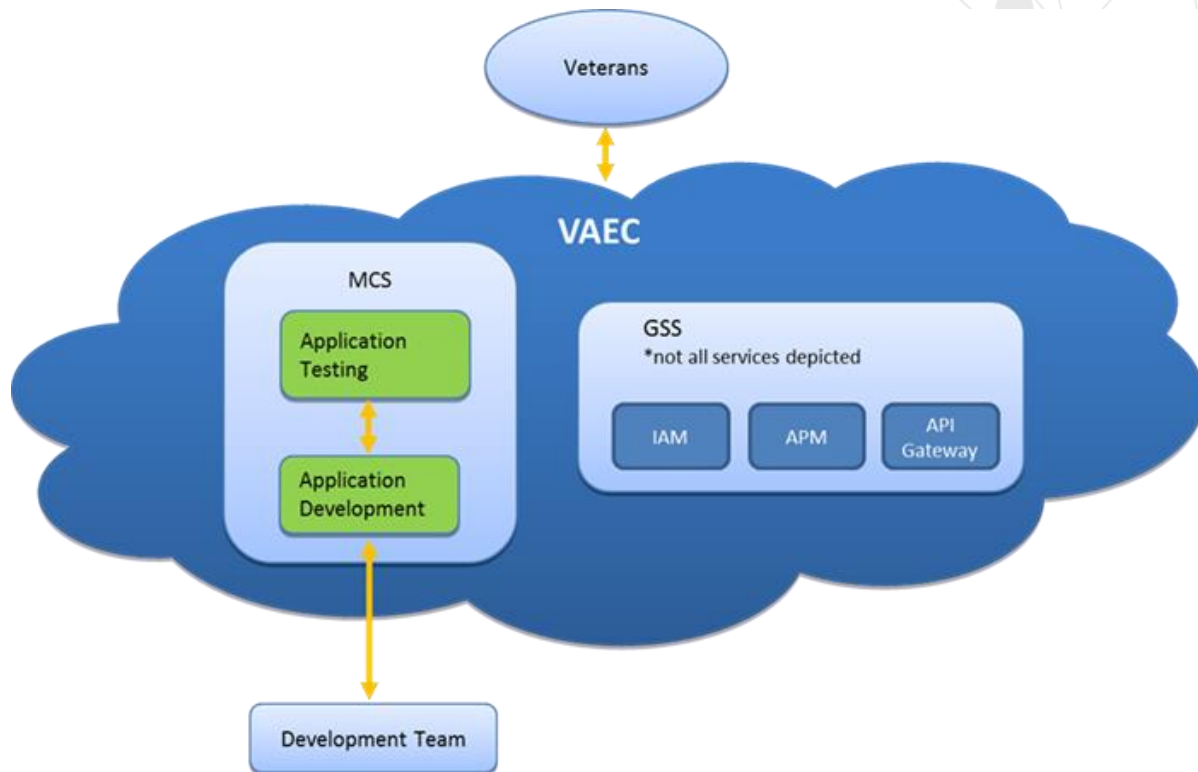
*Figure 1: Mobile Cloud Services (MCS) and General Support System (GSS) Services provided by the VAEC*

## 4  Application

The Design, Engineering, and Architecture (DEA) User Stories have a standard for VistA Integration Control Registrations (ICR), software source code scans, and conceptual and detailed system design models. The Veteran-focused Integration Process (VIP) requires project teams to comply with the approved standards in the One-VA Technical Reference Model (TRM);[16] and map to the Design, Engineering, and Architecture (DEA) User Stories.

*Table 3: DEA User Stories*

| DEA User Story | Title | User Story Text |
|---|---|---|
| **DEA 04.14.01** | COTS Products | All Commercial-off-the-Shelf (COTS) products used in the solution shall be from mature companies large enough to support those products over the expected life of the product; at all locations at which they may be installed. |

---

[16] Reference the One-VA Technical Reference Model (TRM) on the VA internal network at http://trm.oit.va.gov/.

| DEA User Story | Title | User Story Text |
|---|---|---|
| **DEA 04.14.02** | Open Source | Open Source Software (OSS) shall be thoroughly evaluated when VA acquires software; and OSS development practices shall be considered when VA develops software. |
| **DEA 04.14.03** | One-VA Technical Reference Model (TRM) | All technologies and standards and their respective versions used by the solution shall be listed and identified as permissible for usage in the VA Technical Reference Model (TRM); or complete the Strategic Technology Alignment Team (STAT) waiver process to acquire the appropriate waivers issued by the STAT Governance Council (GC).[17] |
| **DEA 04.16.01** | Data Access Service (DAS) | All VA software projects that establish or change external interfaces shall use Data Access Service (DAS) infrastructure capabilities and services, if available and applicable. |
| **DEA 04.21.01** | Compute Capacity | Compute resource requirements will be based on simulated workload testing, application performance models, and system instrumentation and analysis. System design will support scalability of compute capacity. |
| **DEA 04.21.02** | Infrastructure Capacity | Supporting infrastructure requirements (compute, storage and network) will be based on simulated workload testing, application performance models, and/or ongoing production performance monitoring and analysis. System design will support scalability of capacity for each of the infrastructure resources. |
| **DEA 04.23.01** | Cloud Computing | Cloud computing provides access to a shared pool of configurable, on-demand computing resources (e.g. servers, VMs, storage, network, applications, or services) that can be rapidly deployed and re-provisioned with reduced management effort or service provider interaction. |

Future updates of this document will reflect updates to the DEA compliance criteria to reflect the guiding principles for application release.[18] Compliance with these standards apply to the following major project scenarios:

---

[17] Reference the Strategic Technology Alignment Team (STAT) waiver information at https://www.ea.oit.va.gov/EAOIT/VA_EA/STRATEGIC_TECHNOLOGY_ALIGNMENT_TEAM_STAT_WAIVERS.asp.

[18] Reference the Enterprise Architecture (EA) Guiding Principles at https://www.ea.oit.va.gov/EAOIT/VA_EA/Global-Principles.asp.

- All new development efforts leveraging the VAEC
- Application transitioning to the VAEC

# 5 Impact

If the Application Development and Deployment Guidelines are not implemented for mobile Veteran-facing applications, VA can expect the following outcomes:

- Projects will not be in alignment with the VA Cloud First Policy.
- Services expected by Veterans and their beneficiaries will be negatively impacted.
- The expected increase in Veteran mobile access, engagement, and interoperability will not be realized.

# Appendix A: References

**References:**

- VEAR: https://vaausdarapp82.aac.dva.va.gov/ee/request/home
- VA Digital Modernization Strategy, April 11, 2018: http://vaww.ea.oit.va.gov/wp-content/uploads/2018/08/DigitalModernizationStrategy_080118.pdf
- 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

## Appendix B: Enterprise Shared Services

This appendix describes a sampling of various ESS available within VA.

*Table 4: Various ESS Available within VA*

| # | Project | Service | Description |
|---|---------|---------|-------------|
| 1 | CDW | VA Corporate Data Warehouse | 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 | The Enterprise Message Broker enables message exchanges between VA systems and service messaging engine. |
| 3 | IAM | Master Veteran Index (MVI) | MVI is the authoritative source for person identity data; MVI 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; and 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 authorized user. In addition, eSig provides a mechanism for VA applications to verify the authenticity of user documents and data integrity on user forms. |

| # | 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 | Directory Services efficiently stores and manages user information; and provides a comprehensive view of predefined authoritative data managed by Identity and Access Management (IAM) for all users across the VA enterprise. |
| 7 | IAM | IP | Identity Proofing is 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) | 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). CSP is linked with the SSOi and SSOe programs. |
| 9 | IAM | Single Sign On External (SSOe) | SSOe allows a user that is authenticated at a federated CSP (IdP) to seamlessly access integrated applications. SSOe provides a single sign-on solution for internal facing VA applications; and authenticates users with CSP credentials and other externally-issued credentials (including mapping of credential to VA identity; and IBM tools). |

| # | Project | Service | Description |
|---|---------|---------|-------------|
| 10 | IAM | Single Sign On Internal (SSOi) | SSOi provides a single sign-on solution for internal facing VA applications. It 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). SSOi supports application implementation of PIV requirement. |
| 11 | IAM | Compliance Audit and Reporting (CAR) | 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. |
| 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. This may include the creation, modification, deletion, suspension, or restoration of such accounts and synchronizing user data. |
| 13 | Legacy VistA | VistA Instances | VistA Instances represent an installed copy of the VistA software at a particular location. |
| 14 | VLER DAS | DAS (Data Access Service) | DAS is a VLER Gateway – Authentication, Authorization, Audit & Access Control; many aggregators, transformers, splitters, routers, etc. |
| 15 | VLER DAS | eCRUD Wrapper | An eCRUD Wrapper provides designated common enterprise services, including enterprise Create/Read/Update/Delete (CRUD) services for enterprise data stores. |

| # | Project | Service | Description |
|---|---------|---------|-------------|
| 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. It connects providers, consumers, and others involved in supporting health and health care. |
| 18 | VistA Integration Adapter (VIA) API | VistA Integration via WSDL | VistA Integration is an 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 for all appropriate longitudinal health record data. |