
VA Enterprise Design Patterns: Mobile Architecture

Office of Technology Strategies (TS)
Architecture, Strategy, and Design (ASD)
Office of Information and Technology (OI&T)

Version 1.0

Date Issued: December 31, 2014



THIS PAGE INTENTIONALLY LEFT BLANK FOR PRINTING PURPOSES

APPROVAL COORDINATION

Date:

Tim McGrail
Deputy Director (Acting)
ASD Technology Strategies

Date:

Paul A. Tibbits, M.D.
DCIO Architecture, Strategy, and Design

REVISION HISTORY

| Version | Date | Organization | Notes |
|---------|----------|--------------|---|
| 0.70 | 11/26/14 | ASD TS | Initial Draft |
| 0.85 | 12/05/14 | ASD TS | Second draft document with updates made throughout document based upon initial internal/external stakeholder review and comment. |
| 0.95 | 12/11/14 | ASD TS | Third and final draft for stakeholder review prior to TS leadership approval/signature. Updates made following Public Forum collaborative feedback and working session. |
| 1.0 | 12/31/14 | ASD TS | Final version for TS leadership approval and signature, including all applicable updates addressing stakeholder feedback and Section 508 Compliance. |

REVISION HISTORY APPROVALS

| Version | Date | Approver | Role |
|---------|----------|---------------------------|--|
| 0.70 | 11/26/14 | Jacqueline Meadows-Stokes | ASD TS Mobile Architecture Design Pattern Lead |
| 0.85 | 12/05/14 | Jacqueline Meadows-Stokes | ASD TS Mobile Architecture Design Pattern Lead |
| 0.95 | 12/11/14 | Jacqueline Meadows-Stokes | ASD TS Mobile Architecture Design Pattern Lead |
| 1.0 | 12/31/14 | Jacqueline Meadows-Stokes | ASD TS Mobile Architecture Design Pattern Lead |

TABLE OF CONTENTS

| | | |
|-------------|--|----|
| 1. | Introduction | 1 |
| 1.1. | Background | 1 |
| 1.2. | Purpose | 2 |
| 1.3. | Scope..... | 3 |
| 1.4. | Intended Audience..... | 3 |
| 1.5. | Document Development and Maintenance | 3 |
| 2. | VA Mobile Architecture Key Components | 3 |
| 2.1. | Mobile Application Environment (MAE) | 4 |
| 2.2. | VA Mobile Framework (VAMF) | 4 |
| 3. | Design Pattern “To-Be” Architecture..... | 4 |
| 3.1. | VA “To-Be” Enterprise Mobile Architecture | 4 |
| 3.2. | Mobile Architecture Attributes..... | 6 |
| 3.2.1. | Mobile Device Management (MDM) | 6 |
| 3.2.2. | Mobile Security | 6 |
| 3.2.3. | Mobile Application Management (MAM)..... | 7 |
| 3.2.4. | Availability..... | 9 |
| 3.2.5. | Maintenance and Support | 10 |
| 3.3. | Mobile Architecture Constraining Principles & Strategic Guidance | 10 |
| Appendix A. | Use Cases | 14 |
| Appendix B. | Vocabulary | 17 |
| Appendix C. | Applicable References, Standards, and Policies..... | 19 |

TABLE OF FIGURES

| | |
|---|---|
| Figure 1 – VA Mobile Framework “As-Is” Logical Architecture | 2 |
| Figure 2 – “To-Be” Enterprise Mobile Architecture Design Pattern Concept..... | 5 |

TABLE OF TABLES

| | |
|--|----|
| Table 1 – Enterprise Mobile Architecture Constraining Principles and Strategic Guidance..... | 10 |
| Table 2 – Applicable “As-Is” and “To-Be” Enterprise Mobile Architecture Use Cases | 14 |
| Table 3 – Applicable Acronyms and Terms | 17 |
| Table 4 – Applicable References, Standards and Policies | 19 |

1. INTRODUCTION

1.1. Background

The concept of mobility is quickly growing as an enterprise discipline within large information technology (IT) organizations. It involves the collective set of people, technologies, processes and governance associated with the increased availability of mobile devices, wireless networks, and information access services applicable to mobile computing within a business environment. The number of organizational employees and stakeholders requiring support for the use of mobile computing devices to access information, tools and services on demand is growing at an accelerated rate.

Within VA there is a mobile infrastructure present, to a certain degree, but not at the enterprise-level and not fully capable of supplying the robust capabilities that have come to be expected in today's mobile landscape by both the user and the application developer. Some of the problems that VA faces include:

- Existence of domain-specific structures and processes, in addition to the utilization of existing structures and processes,
- Escalating numbers of varying mobile device, telecommunications, and operating license costs
- Insufficient IT standards, policies and processes in place for mobile technologies
- Insufficient support for mobile service development and implementation
- Multiple development, test and production environments
- Limited wireless infrastructure
- A lack of streamlined processes for application certification
- Bring Your Own Device (BYOD) use without appropriate/complete policy in place
- Unknown or not easily identifiable authoritative data and data sources for Veteran-facing applications
- Cross-administration of the Mobile Applications Governance Board (MAGB) and its subgroups.

VA is currently in the process of evolving aspects of its mobile platform and environment through development and implementation of key components, projects, capabilities and policies within certain lines of business (LOBs). This includes implementation of the VA Mobile Framework (VAMF) that resides within the Mobile Application Environment (MAE), both of which are described in greater detail as "Key Components" of the enterprise-level VA mobile environment in Section 2 of this document. It also includes efforts to prioritize development and deployment of internally and externally developed applications through the Mobile Development and Mobile Health External Development (MHED) efforts, respectively. Both efforts allow for the management of these applications in accordance with their priority and the Project Management Accountability System (PMAS) process to expedite turn around and release of applications without the cost of significant administrative overhead.

These are initial steps that form the beginning of the evolution of VA's overarching Enterprise Mobile Architecture, which will move the Department from sets of stove-piped systems and domain specific

structures and processes, to an agile mobile infrastructure integrated within a modern service oriented architecture (SOA) environment.

Figure 1, below, provides a logical representation of the “as-is” state of the VA mobile environment. It is meant to convey the current IT infrastructure and allow for a visual analysis of capability gaps that exist, current work being performed to address these gaps, and areas that still need to be considered in planning and executing a “to-be” enterprise mobile architecture framework.

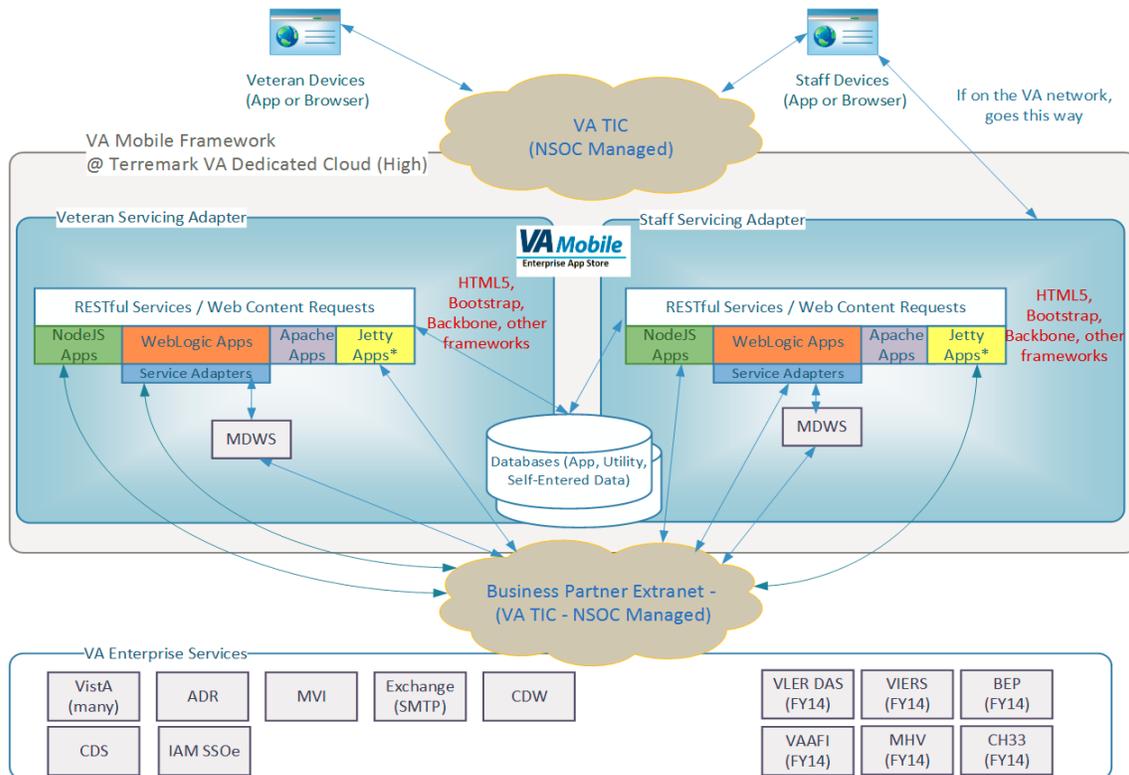


Figure 1 – VA Mobile Framework “As-Is” Logical Architecture

1.2. Purpose

The purpose of the Enterprise Mobile Architecture Design Pattern document is to provide enterprise-level capability guidance that identifies best-practices for solving recurring technical problems within VA’s mobile IT environment. It is meant to be limited enough to be usable and broad enough to be reusable as a formalized approach that projects within the VA mobile space will leverage in the establishment of their solution architectures. This design pattern, and subsequent follow-on mobile design patterns, will guide projects to appropriate implementation resources that aid in establishing design specifications for mobile system development and integration.

1.3. Scope

This design pattern document provides an enterprise-level view of the “to-be” mobile architecture environment within the VA IT infrastructure. It describes the vision for utilizing agreed upon common reusable capabilities, as validated by VA LOBs, to provide seamless mobile access to VA Enterprise Shared Services (ESS) through the VAMF and enterprise Messaging Infrastructure (eMI). The document will focus on a vendor-agnostic framework for an enterprise mobile architecture environment, and will refer to, rather than duplicate, lower-level solution guidance associated with these capabilities.

The Design Pattern document is generally applicable across all domains and describes:

- Background on the “As-Is” state of the VA mobile environment
- Descriptions of key components of the Enterprise Mobile Architecture environment
- Design Pattern “To-Be” Enterprise Mobile Architecture and associated attributes
- Table of enterprise-level mobile constraints and strategic guidance

This design pattern document **does not** address detailed technical solution architecture guidance for implementing specific mobile frameworks and tools. It will only provide the constraints to drive VA mobile programs towards development of solutions that effectively meet the specific goals of their initiatives.

1.4. Intended Audience

The Design Pattern is meant to be used by VA Integrated Project Teams (IPTs) that have mobile requirements, are developing internal VA mobile applications, or are provisioning mobile applications and devices in support of VA business processes or initiatives.

1.5. Document Development and Maintenance

This document was developed collaboratively with internal stakeholders from across the Department and included participation from VA’s Office of Information and Technology (OI&T), Product Development (PD), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE). 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. Updates will be coordinated with the Government lead for this document, which will also facilitate stakeholder coordination and subsequent re-approval depending on the significance of the change.

2. VA MOBILE ARCHITECTURE KEY COMPONENTS

The Enterprise Mobile Architecture Design Pattern document will align with VA enterprise mobile strategic guidance and VA Enterprise Roadmap goals for the “to-be” VA IT infrastructure. It will drive the reference architecture guidance being developed within the Mobile Application Reference Architecture (MARA), as well as subsequent solution-level architectures and implementation guidelines.

This section provides high-level overviews of key components within the VA enterprise mobile infrastructure that are applicable to solving the recurring problems within the current state of the IT environment, as described in Section 1.1. These components make up the backbone that influences the “to-be” mobile architectural concepts and associated attributes outlined in Section 3, which will guide the establishment of design constraints applicable across all mobile programs in VA.

2.1. Mobile Application Environment (MAE)

The VA Mobile Application Environment (MAE) is an external production and testing environment that is located in the Terremark VA Dedicated Cloud. It consists of four separate environments: Development, Test [Federal Information Security Management Act (FISMA) low], Integration and Production (FISMA high), which provide tools and services for internal VA mobile applications to use for test and compliance reviews. These environments have the Mobile Application (MA) software installed and operational to support common services used by mobile applications.

Project management tools within the MAE are used to track the progress of each externally developed mobile application, to include defect tracking. The processes for changes to the project are described in the Mobile Application Program (MAP) Change Management Plan found with the MAP program-level documentation.

2.2. VA Mobile Framework (VAMF)

The VAMF, as shown in Figure 1, is a system developed initially through the VA Innovations program at the Veterans Health Administration (VHA) and provides the capabilities and common services that allow mobile applications to access the VA infrastructure to achieve the business needs of stakeholders. The VAMF is intended to support a wide variety of applications, both Veteran/caregiver focused as well as VA staff focused. VAMF provides an environment for achieving enterprise-level certification (testing, certification and release) of mobile application to meet the OI&T developed process for expeditious release of externally developed mobile applications. Internally developed mobile applications will also use VAMF resources and services and will follow the same processes as externally developed applications. For additional details on the design and specifications describing the VAMF, see the most current version of the *Mobile Application Program VA Mobile Framework (VAMF) System Design Document (SDD)*.

3. DESIGN PATTERN “TO-BE” ARCHITECTURE

3.1. VA “To-Be” Enterprise Mobile Architecture

The “to-be” vision for VA’s enterprise mobile architecture is the ability to provide a uniform, seamless network and data access experience across all Veteran and clinician facing applications regardless of interface platform (mobile vs. web), device, physical location or user role. It will provide a reliable and enjoyable digital interaction through conformance to collectively developed, maintained and enforced design standards (HL7, FHIR, etc.) applied to cross-platform services for developers to build to, regardless

of endpoint. This will create a consistent experience and ensure the agility to keep up with the fast paced growth of device technology.

Figure 2, below, is an enterprise representation of the VA “to-be” mobile environment. It depicts the high-level interactions between multiple users/devices on varying platforms accessing Enterprise Shared Services (ESS) through both internal and external applications. This is achieved through the respective LOB mobile environments contained within the VAMF and via the VA eMI. Section 3.2, to follow, will provide descriptions and enterprise guidance in alignment with appropriate federal standards and policy for an initial set of capability attributes associated with these interactions. Further detailed guidance will be made available through subsequent, capability specific, design patterns as well as through the implementation of the VA Mobile Application Reference Architecture (MARA) that is currently under development.

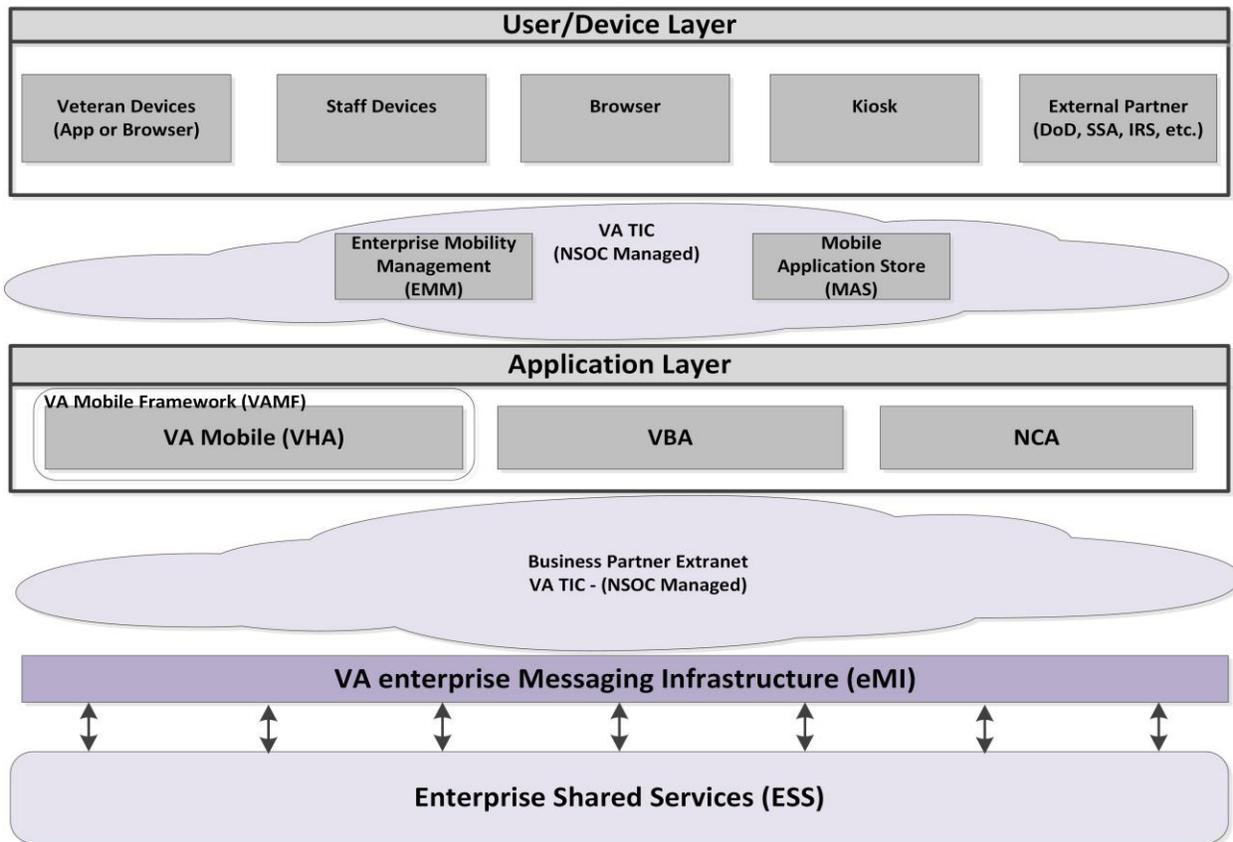


Figure 2 – “To-Be” Enterprise Mobile Architecture Design Pattern Concept

3.2. Mobile Architecture Attributes

This section describes the “to-be,” vendor-agnostic attributes of the VA Enterprise Mobile Architecture. The included attributes have been identified as an initial set of key concepts involved in ensuring an effective VA enterprise mobile architecture. The content associated with each of these attributes combines an understanding of the “as-is” VA IT infrastructure, knowledge of required internal VA and external government policy, and the application of industry best practices to create the enterprise-level capability guidance that will drive the realization of the “to-be” vision for VA’s mobile environment. This descriptive language and constraining guidance was developed through collaboration with both internal and external government and industry stakeholders.

3.2.1. Mobile Device Management (MDM)

As the number of mobile device models, platforms and operating system versions available continues to grow at an exponential rate, VA will continually face increased and complex mobility management challenges. The Department’s MDM capability and tools will provide the ability to manage both government furnished equipment (GFE) and employee-owned devices (Bring Your Own Device – BYOD) across the enterprise. It will provide the largest external network throughput possible within budgetary guidelines, and a full, multi-site high availability and disaster recovery environment with automatic failover and load balancing, including network and database components. The MDM will leverage highly-integrated mobile monitoring tools that watch devices, connections, data sources, protocols, and compliancy, across cloud or on-premises installations.

The VA “to-be” MDM environment will also include a robust, centralized, dedicated administration server environment that provides the ability to administer ALL devices, build policies, publish applications, perform updates/upgrades, etc. While this centralized management approach will be established across the enterprise IT infrastructure, the MDM should not create too rigid of an administrative environment. It will need to fully support any regional, departmental, regulatory, or other administration requirements.

3.2.2. Mobile Security

The federal government has moved towards federated credentials as a method for securing single sign-on (SSO) authentication and authorization across enterprise and personal devices, user accounts, and applications. In order to meet VA standards for ensuring the security of sensitive information, the “to-be” mobile infrastructure, in combination with VA’s Identity and Access Management (IAM) SSO solutions, will provide government approved and Federal Information Processing Standards (FIPS) certified encryption for all data at rest and in transit. Encryption and security of content, credentials and configurations will be more critical than device security (i.e. no reliance on native solutions to protect actual data). Security associated with mobile devices and applications will adhere to policy and standards identified within the most current version of the Mobile Security Design Pattern document, which is planned for initial development Q2 FY15. At the level of patient generated data (PGD) (i.e., PII/PHI), all information from mobile applications will be normalized and adhere to standardized processes for

encryption of data-at-rest and in transit in compliance with HIPAA controls in addition to these security policies. These constraints will be met during the development and execution of solution level architectures and implementation guidance in adherence with all applicable security and Enterprise Information Management policy and controls. To comply with these standards, the mobile environment will provide the ability to integrate advanced security capabilities and solutions for:

- Single Sign-On (SSO)
- Rights management
- Containerization of applications to prevent digital leaks and unauthorized information access
- Derived credentials that are federated across all applications
- Digital signatures
- Physical tokens (PIV cards, sleds, etc.)
- Biometric technology used for two factor authentication (fingerprints, etc.)
- Mobile communications discovery through audit trails.

A subsequent design pattern specifically focused on VA Mobile Security is planned for development and completion during FY15. For more information and specifics on applicable Department and Federal security standards and policies, as well as “to-be” VA security capabilities, refer to the currently available Authentication, Authorization and Audit (AA&A) design pattern documents.

3.2.3. Mobile Application Management (MAM)

Application use for access to services and information are becoming the primary driver of mobility. VA has the responsibility to ensure that all applications that touch the network, read, or write data meet all of the requirements and guidelines established by the Office of Information and Technology (OI&T). The “to-be” VA enterprise mobile infrastructure will include a robust mobile application management capability. This capability must be scalable, having the available throughput for support of an ever increasing number of cross-platform mobile applications and allowing for both VA and non-VA users to access enterprise shared services and data through those applications. It will also need to include scalable enterprise-level processes and structures capable of supporting both a build as well as a buy decision process that promote the use and re-use of commercial off the shelf (COTS) applications, available open source applications, and internal development of VA specific applications. These processes and structures should focus on standardized development, testing, fielding, certification and governance, and maintenance and support across the enterprise network.

Application Development

VA’s target mobile application development environment will be aligned with the Department’s software development lifecycle (SDLC) process, as defined within the OneVA Enterprise Architecture (EA), and will be managed in accordance with the current Project Management Accountability System (PMAS) methodology. The development environment will allow for the safe but rapid creation and/or fully automated testing of internal and external mobile applications through formal, centralized governance

processes for mobile application requests, development, testing, and fielding. Development of internal VA mobile applications will be performed using tools available within the MAE and that are approved for use by the OneVA Technical Reference Model (TRM). This will ensure minimized administrative strains on development resource, while providing enterprise visibility of applications, proposed and under development, to VA stakeholders.

Application Deployment

The “to-be” VA mobile application deployment environment will be capable of supporting the release and maintenance of both commercially available applications (COTS) and internally developed VA specific applications. It will allow for the safe but rapid release of these internal and external mobile applications from a centralized point and through formal, standardized governance processes for mobile application requests, testing, and fielding. Applications will be tested, reviewed and approved through a standardized certification process before being made available as resources that connect to the VA network. Deployment for all mobile applications within the VA IT infrastructure will leverage the MDM’s app store capability as well as approved commercially available app stores, as appropriate.

VA Application Catalog

The existence of an enterprise mobile application catalog will require the flexibility to change frequently in order to keep up with the fast-paced growth of mobile technology and development. In order to accommodate this dynamic environment, the VA application catalog will be designed for the least amount of administrative overhead (i.e. simply controlled and maintained). It will be capable of accommodating a hybrid application environment, catering to both applications developed for mobile web browsers and applications integrating deeper/more specific functionality (using camera, etc.). The app catalog will also need to have the capability to retrieve an app from a commercial app store, place it in a container, and certify that application for use within the network (standard suite of tools). This will require coordination with the vendors to avoid re-licensing issues and enable containerization of applications from respective commercial app stores.

Application Certification and Governance

All mobile applications developed for use in the VA will be subject to a streamlined certification process, and OI&T will be responsible for ensuring that the application satisfies certification requirements prior to release into the production environment. OI&T will follow an Authority to Operate (ATO) certification process that expedites testing and release of applications developed using agile development methodologies, and coordinate with Line of Business stakeholders to ensure that applications satisfy business needs and rules without duplication application development efforts.

Certification testing is part of the overarching mobile governance process established for mobile applications required for Line of Business needs and supported by OI&T development. Mobile applications will be subject to the Mobile Application Governance Board (MAGB) and follow the streamlined system development lifecycle in accordance with PMAS guidelines. It will also aid in the

prevention of redundant and overlapping mobile application development and duplicative code development. Mobile application governance will be divided into business and technical groups:

Business: Ensure that customer needs and priorities accurately capture the “voice of the customer,” prioritize applications, gathering business requirements, identifying funding sources.

Technical: Ensure that apps are developed following standardized development environment and interfacing with enterprise infrastructure support services; configure app to meet operational support requirements using approved technologies from the TRM.

OI&T will be responsible for guiding application developers to consume ESS and IT infrastructure investments provided by the eMI, including device-independent FIPS 140-2 encryption and end-to-end application performance monitoring.

3.2.4. Availability

Cloud

The VA currently uses Cloud Infrastructure-as-a-Service (IaaS) at the Terremark Facility for its MAE, housing the hardware and software for the following services:

- Mobile Device Management
- App Lifecycle Management – development, testing, release, and sustainment

Cloud availability within the VA IT infrastructure will be driven by Service Level Agreements (SLAs) established through contracts by OI&T and other VA IT project offices. As the Department plans and executes the increased extension of resources to the cloud, a cohesive strategy and architecture for viewing and managing those resources will be established across the enterprise IT infrastructure, including mobile. Focus will need to be placed on aspects such as service orchestration, service management, business support, provisioning and configuration, and portability and interoperability. From a mobile perspective, the IT infrastructure will provide a unified management capability that allows for identification, viewing and managing devices, applications and servers that are both on-premises and in the cloud.

A cloud security approach will also be established, as security requirements such as authentication, authorization, availability, confidentiality, identity management, integrity, audit, security monitoring, incident response, and security policy management are cross-cutting and of critical importance in ensuring the protection of sensitive data (e.g. PII/PHI).

While this design pattern does not go into the specific capability guidance for these aspects of cloud computing, more detailed guidance is planned for subsequent Mobile, IaaS and AA&A design pattern document development efforts.

Data

Mobile users and devices will consume and generate data through enterprise share services via standardized, authoritative data source for Veteran facing applications and a specific repository for Patient Generated Data (PGD) that ensures patient information security (e.g., PII, PHI). This will be accomplished in awareness of the full complement of mobile and enterprise technology within VA and associated standards and policies.

For more information detailing the VA Enterprise Data-as-a-Service (DaaS) capability, associated data security architecture, standards and policy, refer to the DaaS Design Pattern document(s).

3.2.5. Maintenance and Support

Once VA has standardized its mobile environment on a flexible, secure, and scalable platform, maintaining and supporting its effectiveness in delivering high-availability is critical. Looking to the future, when supporting medical devices and Veterans across the country/world with hundreds of thousands of disparate devices, VA needs to ensure it can extract the complexity and maintain an enhanced user experience and capability offering. This includes the ability to scale the mobile platform to more than 100,000 users without incurring excessive associated costs. It also includes the availability of a lifecycle management capability for tracking, logging, and maintaining applications after they are deployed and available.

3.3. Mobile Architecture Constraining Principles & Strategic Guidance

The following table summarizes the constraining principles associated with enterprise mobile concepts and architectural attributes. These principles will be used to drive implementation guidance to programs involved with designing and implementing current and future VA mobile solutions.

Table 1 – Enterprise Mobile Architecture Constraining Principles and Strategic Guidance

| # | Mobile Concept/Attribute | Principles & Strategic Guidance |
|---|--------------------------------|---|
| 1 | Mobile Device Management (MDM) | MDM will provide the ability to manage both government furnished equipment (GFE) and employee-owned devices (Bring Your Own Device – BYOD) across the enterprise |
| 2 | Mobile Device Management (MDM) | MDM will provide the largest external network throughput possible within budgetary guidelines, and a full, multi-site high availability and disaster recovery environment with automatic failover and load balancing, including network and database components |
| 3 | Mobile Device Management (MDM) | MDM will leverage highly-integrated mobile monitoring tools that watch devices, connections, data sources, protocols, and compliancy, across cloud or on-premises installations |

| # | Mobile Concept/Attribute | Principles & Strategic Guidance |
|----|-------------------------------------|---|
| 4 | Mobile Device Management (MDM) | MDM will include a robust, centralized, dedicated administration server environment that provides the ability to administer ALL devices, build policies, publish applications, perform updates/upgrades, etc. |
| 5 | Mobile Device Management (MDM) | MDM will fully support any regional, departmental, regulatory, or other administration requirements |
| 6 | Mobile Security | The “to-be” mobile infrastructure, in combination with VA’s Identity and Access Management (IAM) SSO solutions, will provide government approved and Federal Information Processing Standards (FIPS) certified encryption for all data at rest and in transit |
| 7 | Mobile Security | Security associated with mobile devices and applications will adhere to policy and standards identified within the most current version of the Mobile Security Design Pattern document, which is planned for initial development in Q2 FY15. |
| 9 | Mobile Security | <p>The “to-be” VA mobile environment will provide the ability to integrate advanced security capabilities and solutions for:</p> <ul style="list-style-type: none"> • Single Sign-On (SSO) • Rights management • Containerization of applications to prevent digital leaks and unauthorized information access • Derived credentials that are federated across all applications • Digital signatures • Physical tokens (PIV cards, sleds, etc.) • Mobile communications discovery through audit trails |
| 10 | Mobile Security | At the level of patient generated data (PGD) (i.e., PII/PHI), all information from mobile applications will be normalized and adhere to standardized processes for encryption of data-at-rest and in transit in compliance with HIPAA controls in addition to these security policies |
| 11 | Mobile Application Management (MAM) | The “to-be” VA enterprise mobile infrastructure will include a scalable MAM capability that has the available throughput for support of an ever increasing number of cross-platform mobile applications and allows for both VA and non-VA users to access enterprise shared services and data through those applications. |
| 12 | Mobile Application Management (MAM) | MAM will provide scalable enterprise-level processes and structures capable of supporting both a build as well as a buy decision process that promote the use and re-use of commercial off the shelf (COTS) applications, available open source applications, and internal development of VA specific applications |

| # | Mobile Concept/Attribute | Principles & Strategic Guidance |
|----|---|---|
| 13 | Mobile Application Management (MAM): Development | The mobile application development environment will be aligned with the Department's software development lifecycle (SDLC) process, as defined within the OneVA Enterprise Architecture (EA) |
| 14 | Mobile Application Management (MAM): Development | Application development will be managed in accordance with current Project Management Accountability System (PMAS) methodology |
| 15 | Mobile Application Management (MAM): Development | The development environment will allow for the safe but rapid creation and/or fully automated testing of internal and external mobile applications through formal, centralized governance processes for mobile application requests, development, testing, and fielding |
| 16 | Mobile Application Management (MAM): Development | Development of internal VA mobile applications will be performed using tools available within the MAE and that are approved for use by the OneVA Technical Reference Model (TRM) |
| 17 | Mobile Application Management (MAM): Deployment | The "to-be" VA mobile application deployment environment will be capable of supporting the release and maintenance of both commercially available applications (COTS) and internally developed VA specific applications |
| 18 | Mobile Application Management (MAM): Deployment | Application deployment will allow for the safe but rapid release of these internal and external mobile applications from a centralized point and through formal, standardized governance processes for mobile application requests, testing, and fielding. |
| 19 | Mobile Application Management (MAM): Deployment | Applications will be tested, reviewed and approved through a standardized certification process before being made available as resources that connect to the VA network |
| 20 | Mobile Application Management (MAM): Deployment | Deployment for all mobile applications within the VA IT infrastructure will leverage the MDM's app store capability as well as approved commercially available app stores, as appropriate |
| 21 | Mobile Application Management (MAM): Deployment – App Catalog | The VA application catalog will be designed for the least amount of administrative overhead (i.e. simply controlled & maintained) |
| 22 | Mobile Application Management (MAM): Deployment – App Catalog | The app catalog will be capable of accommodating a hybrid application environment, catering to both applications developed for mobile web browsers and applications integrating deeper/more specific functionality (using camera, etc |
| 23 | Mobile Application Management (MAM): Deployment – App Catalog | The app catalog will also have the capability to retrieve an app from a commercial app store, place it in a container, and certify that application for use within the network (standard suite of tools) |

| # | Mobile Concept/Attribute | Principles & Strategic Guidance |
|----|--|--|
| 24 | Application Certification & Governance | OI&T will follow an Authority to Operate (ATO) certification process that expedites testing and release of applications developed using agile development methodologies, and coordinate with Line of Business stakeholders to ensure that applications satisfy business needs and rules without duplication application development efforts. |
| 25 | Application Certification & Governance | Mobile applications will be subject to the Mobile Application Governance Board (MAGB) and follow the streamlined system development lifecycle in accordance with PMAS guidelines |
| 26 | Application Certification & Governance | Mobile application governance will be divided into business and technical groups |
| 27 | Application Certification & Governance | OI&T will be responsible for guiding application developers to consume Enterprise Shared Services (ESS) and IT infrastructure investments provided by the eMI, including device-independent FIPS 140-2 encryption and end-to-end application performance monitoring |
| 28 | Availability: Cloud | Cloud availability within the VA IT infrastructure will be driven by SLAs established through contracts by OI&T and other VA IT project offices |
| 29 | Availability: Cloud | VA cloud strategy and architecture will focus on infrastructure aspects such as service orchestration, service management, business support, provisioning and configuration, and portability and interoperability |
| 30 | Availability: Cloud | The IT infrastructure will provide a unified management capability that allows for identification, viewing and managing devices, applications and servers that are both on-premises and in the cloud |
| 31 | Availability: Cloud | A cloud security approach will be established to ensure the protection of sensitive data (e.g. PII/PHI) |
| 32 | Availability: Data | Mobile users and devices will consume and generate data through enterprise share services via standardized, authoritative data source for Veteran facing applications and a specific repository for Patient Generated Data (PGD) that ensures patient information security (e.g., PII, PHI) |
| 33 | Availability: Data | Data availability will be accomplished in awareness of the full complement of mobile and enterprise technology within VA and associated standards and policies |
| 34 | Maintenance and Support | The VA mobile platform will have the ability to scale to more than 100,000 users without incurring excessive associated costs |
| 35 | Maintenance and Support | The VA mobile platform will have the availability of a lifecycle management and monitoring capability for tracking, logging, and maintaining applications after they are deployed and available |

Appendix A. USE CASES

The following table provides the current set of mobile use cases developed by the Mobile Application Reference Architecture (MARA) Team. They were created to aid in identifying best practices and lessons learned, both in industry and VA implementations, as well as to help define the scope of the overall design pattern document and topics for future mobile design pattern increments.

Table 2 – Applicable “As-Is” and “To-Be” Enterprise Mobile Architecture Use Cases

| # | Use Case | Scenario Description | Data Sensitivity | Applicability |
|---|--|---|--|----------------------|
| 1 | Veterans consumes public Information and other public data | Veteran/citizen seeking information on TBI, PTSD, GI Bill, Burial, home loans, etc. using a mobile device | Public Information | External As-Is/To-Be |
| 2 | Veteran accesses, creates, or modifies personal non-public data | Veteran/caregiver accessing medical and patient data using a mobile device for medication and related care information, preventative care. This could also be a vet accessing CH 33 or other non-health benefits Right information at the right time for the proper care. | VA Sensitive Data (SPI)/Personal Health Information (PHI) Administratively Confidential Information (ACI) (i.e. PGD/IAM–DS/Logon/SSOe/Oauth) | External As-Is/To-Be |
| 3 | VA Staff uses corporate information services, e.g., email, messaging | VA staff exchanging email, messaging, etc., via approved mobile devices. Staff using web access to research medical information, benefit claims, SharePoint to share, etc. Clinical data without PII | SPI/PHI ACI Public (i.e. VA ata/FOUO/PII/ Acquisition Sensitivity IAM SSOi or PIV) | Internal As-Is/To-Be |

| # | Use Case | Scenario Description | Data Sensitivity | Applicability |
|---|--|--|--|----------------------|
| 4 | VA staff access Veterans' HIPAA/PGD/PII/HER data | VA staff using and exchanging medical or benefit data using approved devices to treat a Veteran. Even VA staff performing a housing inspection for a VA loan. Right information at the right time for the proper care. | SPI/PHI ACI (aka. VA ata/PGD/EHR/IAM SSOi or PIV) | Internal As-Is/To-Be |
| 5 | VA Staff and DoD health IT systems | VA staff access DoD medical systems using approved mobile devices. VA doctor can view DoD healthcare to determine future care for an OEF Veteran. This could also be extended to other areas of DoD for service verification. Right information at the right time for the proper care. | SPI/PHI ACI (aka VA data/PHI/PGD/EHR/DoD /IAM–user id/password/PIV/SAML) | Internal To-Be |
| 6 | DoD Staff accessing VA Records | DoD clinician using a DoD Approved mobile device with a VA approved app and proper authorization allowed to retrieve Veteran clinical and related data. | DoD credentials SPI/PHI ACI (aka VA data/PHI/PGD/EHR/DoD /IAM–user id/password | External To-Be |

| # | Use Case | Scenario Description | Data Sensitivity | Applicability |
|---|---|--|--|----------------|
| 7 | Veteran using third Party Application leveraging Enterprise Shared Services (ESS) | Veteran/patient using personal device and commercial developed applications leveraging RESTful interfaces to access/provide their self-entered data and VA health information – Requirements for view, download and transmit | VA Sensitive Data (SPI)/Personal Health Information (PHI) Administratively Confidential Information (ACI) (i.e. PGD/IAM–DS/Logon/SSOe/Oauth) | External To-Be |

Appendix B. VOCABULARY

The following table, Table 3, provides a list of acronyms, terms, and their associated descriptions that are applicable to and used within this design pattern document.

Table 3 – Applicable Acronyms and Terms

| Acronym | Description |
|---------|---|
| AA&A | Authentication, Authorization and Audit |
| ACI | Administratively Confidential Information |
| ASD | Architecture, Strategy and Design |
| ATO | Authority to Operate |
| BYOD | Bring Your Own Device |
| COTS | Commercial Off the Shelf |
| DaaS | Data-as-a-Service |
| EA | Enterprise Architecture |
| EAA | Enterprise Application Architecture |
| EHR | Electronic Health Record |
| eMI | Enterprise Messaging Infrastructure |
| EMM | Enterprise Mobility Management |
| ESS | Enterprise Shared Services |
| ETA | Enterprise Technical Architecture |
| FHIR | Fast Healthcare Interoperability Resource |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Management Act |
| FOUO | For Official Use Only |
| GFE | Government Furnished Equipment |
| HL7 | Health Level Seven International |
| IaaS | Infrastructure-as-a-Service |
| IAM | Identity and Access Management |
| IPT | Integrated Project Team |
| IT | Information Technology |
| LOB | Line of Business |
| MA | Mobile Application |
| MAGB | Mobile Application Governance Board |
| MAE | Mobile Application Environment |
| MAM | Mobile Application Management |
| MAP | Mobile Application Program |
| MARA | Mobile Application Reference Architecture |
| MAS | Mobile Application Store |
| MDM | Mobile Device Management |
| MHED | Mobile Health External Development |
| NCA | National Cemetery Administration |

| Acronym | Description |
|---------|--|
| OIS | Office of Information Security |
| OI&T | Office of Information and Technology |
| OEF | Operation Enduring Freedom |
| PGD | Patient Generated Data |
| PHI | Protected Health Information |
| PII | Personally Identifiable Information |
| PIV | Personal Identity Verification |
| PMAS | Project Management Accountability System |
| SAML | Security Assertion Markup Language |
| SDD | System Design Document |
| SDE | Service Delivery and Engineering |
| SDLC | Software Development Lifecycle |
| SLA | Service Level Agreement |
| SOA | Service-Oriented Architecture |
| SPI | Sensitive Personal Information |
| SSO | Single Sign-On – SSOe/SSOi: External and Internal designations |
| TRM | Technical Reference Model |
| VAMF | VA Mobile Framework |
| VBA | Veteran Benefits Association |
| VHA | Veteran Health Administration |

Appendix C. APPLICABLE REFERENCES, STANDARDS, AND POLICIES

The Enterprise Mobile Architecture design pattern is aligned to the pertinent standards, policies directives and procedures referenced in Table 4, below. These references include guidance that is currently incorporated into the OneVA Enterprise Technical Architecture (ETA):

Table 4 – Applicable References, Standards and Policies

| # | Issuing Agency | Policy, Directive, or Procedure | Purpose |
|---|-------------------------|---|--|
| 1 | VA | VA 6500 Handbook | <ul style="list-style-type: none"> Defines the overall security framework for VA including data storage, retrieval, and exchange. |
| 2 | VA | VA Enterprise Design Patterns – Office of Technology Strategies | <ul style="list-style-type: none"> Defines the enterprise SOA capabilities that are supported ESS. ESS will be deployed for use by all VA applications regardless of the end-user device. |
| 3 | NIST | FIPS 140-2 | <ul style="list-style-type: none"> Federal Information Processing standard for encryption of data at rest and in motion in a mobile computing environment |
| 4 | VA | Enterprise Application Architecture (EAA) | <ul style="list-style-type: none"> Provides the “building codes” for the application architecture of the VA, this document is part of the OneVA ETA and referenced in the ETA Compliance Criteria |
| 5 | Federal CIO Council/DHS | DHS Mobile Security Reference Architecture | <ul style="list-style-type: none"> Provides detailed guidance on the use of enterprise mobile securities to ensure secure usage of mobile devices and applications, applicable throughout the US Government |
| 6 | VA | ESS Directive | <ul style="list-style-type: none"> Establishes policy regarding the development, deployment, and management of ESS in the VA |
| 7 | VA | VA Enterprise Roadmap | <ul style="list-style-type: none"> The Enterprise Mobile Architecture design pattern will help projects develop applications in alignment with the following IT Vision attributes found within the Roadmap’s IT Infrastructure chapter [formerly the Enterprise Technology Strategic Plan (ETSP) document]: Device Freedom, Temporal Freedom, Location Freedom, UI Freedom, Secure Authentication |
| 8 | VA | MAP VAMF System Design Document (SDD) | <ul style="list-style-type: none"> Detailed specifications regarding the VAMF |
| 9 | NIST | NIST SP 800-124 | <ul style="list-style-type: none"> Defines guidelines for the management of the security of mobile devices in an enterprise environment, including theVA |