
VA Enterprise Design Patterns:

5. Mobility

5.1 Mobile Architecture

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

Version 2.0

Date Issued: December 2015



THIS PAGE INTENTIONALLY LEFT BLANK FOR PRINTING PURPOSES

APPROVAL COORDINATION

**TIMOTHY L
MCGRAIL 111224**

Digitally signed by TIMOTHY L MCGRAIL
111224
DN: dc=gov, dc=va, o=internal, ou=people,
0.9.2342.19200300.100.1.1=tim.mcgrail@va.g
ov, cn=TIMOTHY L MCGRAIL 111224
Date: 2015.12.14 11:35:54 -05'00'

Tim McGrail
Senior Program Analyst
ASD Technology Strategies

**PAUL A.
TIBBITS 116858**

Digitally signed by PAUL A. TIBBITS 116858
DN: dc=gov, dc=va, o=internal, ou=people,
0.9.2342.19200300.100.1.1=paul.tibbits@va.g
ov, cn=PAUL A. TIBBITS 116858
Reason: I am approving this document.
Date: 2015.12.22 14:25:17 -05'00'

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
1.7	9/30/15	Nicholas Bogden	ASD TS Mobile Architecture Design Pattern Lead
2.0	12/14/15	Tim McGrail	ASD TS Design Pattern Final Reviewer

TABLE OF CONTENTS

- 1 INTRODUCTION 1**
 - 1.1 BUSINESS NEED.....1
 - 1.2 APPROACH.....2

- 2 CURRENT CAPABILITIES AND LIMITATIONS..... 2**
 - 2.1 CURRENT MOBILE ARCHITECTURE.....2
 - 2.2 LIMITATIONS.....3

- 3 FUTURE CAPABILITIES..... 5**
 - 3.1 ENTERPRISE MOBILE STRATEGY6
 - 3.2 SCALABLE MOBILE ARCHITECTURE7
 - 3.3 MOBILE SECURITY10
 - 3.4 USER EXPERIENCE.....11
 - 3.5 AGILE MOBILE APPLICATION DEVELOPMENT.....11
 - 3.6 ENTERPRISE MOBILE APPLICATION MAINTENANCE SUPPORT12
 - 3.7 PREPARING FOR EMERGING TECHNOLOGIES.....13
 - 3.7.1 *Cloud Computing Impact*.....13
 - 3.8 ALIGNMENT TO THE TRM13

- 4 USE CASES 15**

- APPENDIX A. DOCUMENT SCOPE 20**
 - SCOPE.....20
 - INTENDED AUDIENCE20
 - DOCUMENT DEVELOPMENT AND MAINTENANCE.....20

- APPENDIX B. DEFINITIONS 21**

- APPENDIX C. ACRONYMS..... 23**

- APPENDIX D. REFERENCES, STANDARDS, AND POLICIES..... 25**

FIGURES

Figure 1: “As-Is” High Level Mobile Architecture Framework	3
Figure 2: “To-Be” Enterprise Mobile Architecture Design Pattern Concept.....	6
Figure 3: Key Drivers for Mobile Strategy	7
Figure 4: “To-Be” High Level Mobile Architecture Framework	8
Figure 5: Use Case #1	15
Figure 6: Use Cases #2 and #3.....	17
Figure 7: Use Case #4	19

TABLES

Table 1: TRM – Mobile Architecture	14
--	----

1 INTRODUCTION

The concept of mobility is quickly growing as an enterprise discipline within large organizations including VA. Mobility involves the collective set of people, processes, and technology associated with the increased availability of mobile devices, wireless networks, and information access services applicable to mobile computing within a business environment. The Department of Veterans Affairs (VA) has mobile computing platforms established, however the architecture is currently not extendible throughout the enterprise and limited in supplying the robust capabilities required to support the level of service Veterans and VA staff expect..

Secretary Robert A. MacDonald observed in his 2014 MyVA Presentation “assessments informing the [2014-2020] strategic plan told us VA often provides a fragmented, disjointed experience resulting in poor customer service and frustrated Veterans and beneficiaries.” The Secretary described how Servicemembers, Veterans, and beneficiaries take on the burden of serving as their own integration point for “multiple VAs.”

VA faces the following challenges embracing mobile computing:

- Absence of an enterprise-wide mobility strategy
- Constraints with the current mobile architecture
- Mobile device and application security
- Inconsistent user experience due to limitations in the mobile architecture
- Inconsistent governance processes encompassing the mobile application development lifecycle
- Non-standard mobile application maintenance
- Adaptability to emerging technologies

1.1 Business Need

VA’s future-state IT vision, as outlined in the Enterprise Technology Strategic Plan (ETSP), supports consistent implementation of mobile computing solutions throughout all lines of business (LOB). An architectural framework of required IT capabilities will make possible the seamless integration of enterprise resources deployed to devices not hardwired to VA’s internal network. This integration provides both internal and external users an access point to common, device-independent services at any time and at any location in accordance with VA’s IT vision. Enterprise mobile architecture must meet the following requirements:

- Accelerate mobile solution deployment by facilitating rapid decision-making using a repeatable process
- Facilitate the transition from a non-compliant mobile middleware solution to a scalable enterprise mobile platform

- Provide common access to data to improve business processes by reducing the time to retrieve information

1.2 Approach

Achieving the “To-Be” mobile architecture requires a multi-year initiative supported by both the Office of Information & Technology (OI&T) and Administration leadership encompassing strategy, governance, and technology investment. The focus of this design pattern is to:

- Identify the current capabilities and limitations with the existing mobile architecture
- Provide enterprise-level capability guidance identifying best practices for solving recurring technical problems within VA’s mobile IT environment
- Describe key components of the “To-Be” enterprise mobile architecture and supporting strategy and governance processes

This document aligns with VA enterprise mobile strategic guidance and ETSP goals for the “To-Be” VA IT infrastructure. The “To-Be” reference architecture will guide the development of the Mobile Application Reference Architecture (MARA), in addition to solution-level architectures and implementation guidelines.

2 CURRENT CAPABILITIES AND LIMITATIONS

2.1 Current Mobile Architecture

All mobile applications are deployed within the VA Mobile Framework (VAMF) architecture and Mobile Application Environment (MAE). Limitations with the VAMF raise security and scalability issues. The VAMF allows the use of system accounts through Medical Domain Web Services (MDWS) violating National Institute of Standards and Technology (NIST) and Health Information Portability and Accountability Act (HIPAA) requirements.

Current state mobile apps use MDWS to perform queries against the VHA Corporate Data Warehouse (CDW) – a set of databases containing data replicated from VistA. OI&T has not identified an authoritative source for Veteran facing mobile apps to use to obtain Veteran data. Both the repository and the interface layer must be specified for this access, since it is unclear whether CDW can handle the performance load of the online mobile transactions. Additional requirements necessitate the source data be updated more frequently than the CDW working database. The updates to the datasets are daily, weekly, and monthly. Depending on the requirements of the mobile app, the frequency of the updates is not satisfactory to the Veteran or to the VA staff trying to serve the Veteran.

The following figure provides a visual depiction of the “As-Is” mobile architecture framework including current capabilities:

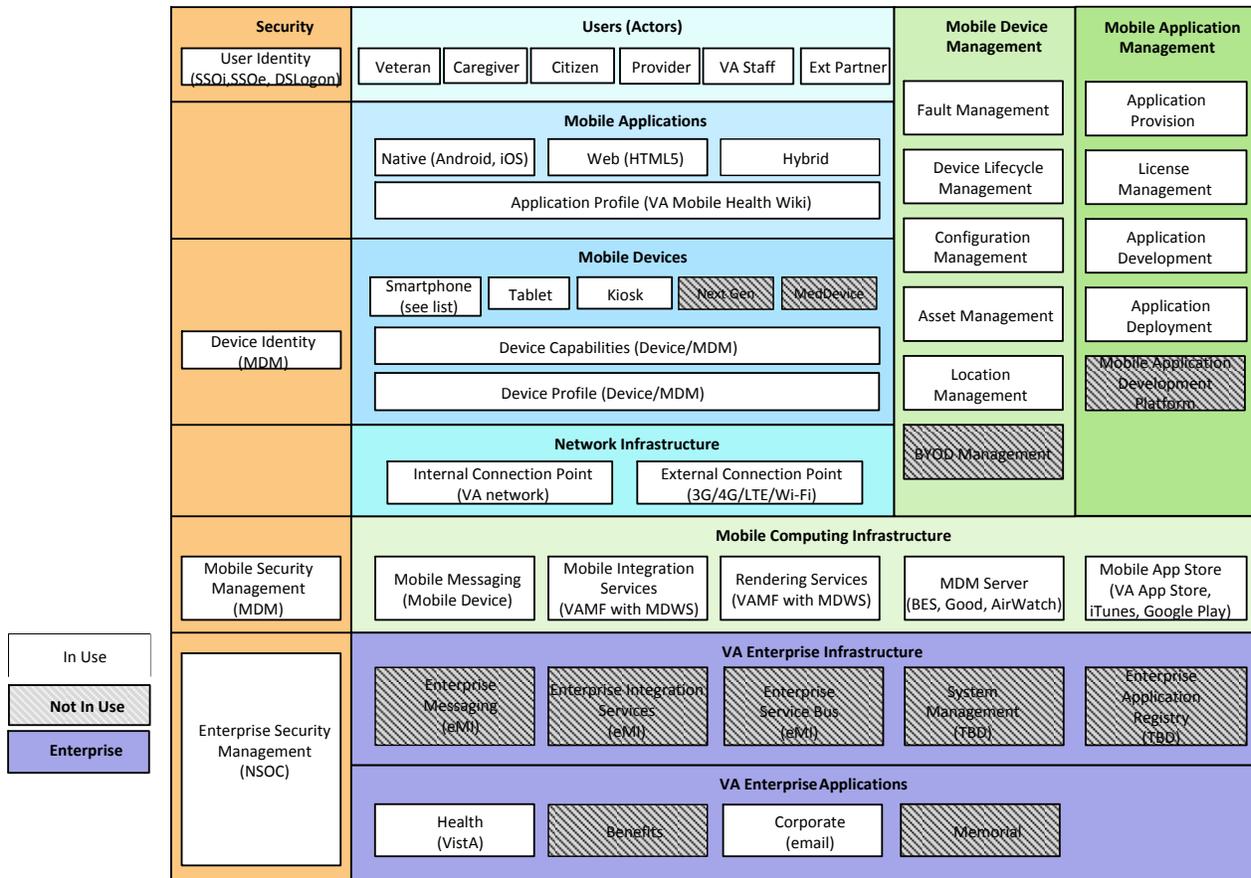


Figure 1: “As-Is” High Level Mobile Architecture Framework

The Veterans Health Administration’s (VHA) Web and Mobile Solutions Team (WMS) maintains the MAE, which is a development environment within VA networks. An approved application can be developed on the MAE, which allows users access to its tools and services. The business owner can also choose to develop the approved application in another environment, but the code must be uploaded to MAE before VHA can perform a compliance review. In addition, MAE offers a vendor service to allow a developer to test their code for security vulnerabilities.

2.2 Limitations

The “To-Be” mobile architecture framework addresses the following limitations:

- Enterprise Mobile Strategy:** While VA has engaged in mobile development efforts, it does not have a comprehensive enterprise mobile strategy. This strategy should encompass all aspects of an enterprise’s mobile network, services, devices, platforms, while also accommodating new technology trends (e.g. bring your own device [BYOD])

and the Internet of things [IoT]). The business impact of deployed applications or are under development require better metrics. Key Performance Indicators evaluating app usage and effectiveness need to be established. Current metrics for web apps developed by VA are not readily available.

- **Mobile Platforms:** VA has invested in redundant technology as departments are working in silos towards their mobile initiatives. OI&T has invested in technology not being leveraged by the mobile development team. VA owns licenses for IBM's Mobile First platform and an enterprise license for Oracle's Web Center Portal.
 - Lack of multi-platform availability: Over 50 percent of applications are iOS only, limiting the reach and availability to users running on other operating systems.
 - Insufficient IT standards, policies, and processes for mobile technologies: Centralized governance and oversight has not been established across the LOBs in VA. There is insufficient support for mobile service development and implementation.

- **Scalable Mobile Architecture:**
 - Lack of scalable infrastructure: Current systems can only support 3,500 concurrent users and require the ability to scale to support an increase in additional users accessing enterprise resources.
 - System memory limitations: The VAMF designed their runtime support services to be bundled into one web application archive (WAR) file. Development and testing issues occur due to the unpacking and packing of the entire WAR file for each build. In order to address this limitation, multiple instances of the same WAR file were deployed. This has introduced scalability challenges across all of the application services (WebLogic) that constitute the VAMF.

- **Mobile Security:** Mobile applications historically relied on web services that used anonymous accounts to interact with Veterans Health Information and Systems Architecture (VistA). Not integrating with enterprise Identity and Access Management (IAM) services poses risks to ensuring proper identity propagation to the back-end systems that make up system accounts to perform VistA transactions.

- **User Experience:** Mobile analytics needed to investigate and optimize the user experience are only available for iOS applications and are not available for other platforms.

- **Inefficient Mobile Application Development Lifecycle:** The complexity of systems and the lack of a robust testing capability impact current compliance turn-around times. The

Mobile Application Program (MAP) office has defined and implemented an initial set of processes focused on completing the initial release process (Verification & Validation, Compliance Reviews, Operational Readiness Review, etc.) for the purpose of initiating the Field Testing/Initial Operating Capability for a new mobile application. The target release time is 40 days, but actual durations are significantly higher. The current goal is to produce workable code, released to a production environment, within 120 days. Compliance reviews are taking longer than expected due to the number of defects in the code delivered to the MAP office.

- **Non-standard Mobile Application Maintenance:** Released mobile applications have a three-month support period after which they become the responsibility of the business owner. There is no plan for operations and maintenance of applications beyond the sustainment period.
- **Preparation for Emerging Technologies:** The current VA mobile infrastructure is constrained to a set of specific technologies, and it is not extensible to accommodate emerging technologies such as cloud computing and IoT.

3 FUTURE CAPABILITIES

Figure 2 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 Enterprise Mobility Management (EMM) and via the VA Enterprise Messaging Infrastructure (eMI). The EMM will encompass cross-platform capabilities including Mobile Device Management (MDM), Mobile Application Management (MAM), and mobile security. Further detailed guidance will be made available through subsequent capability-specific Enterprise Design Patterns.

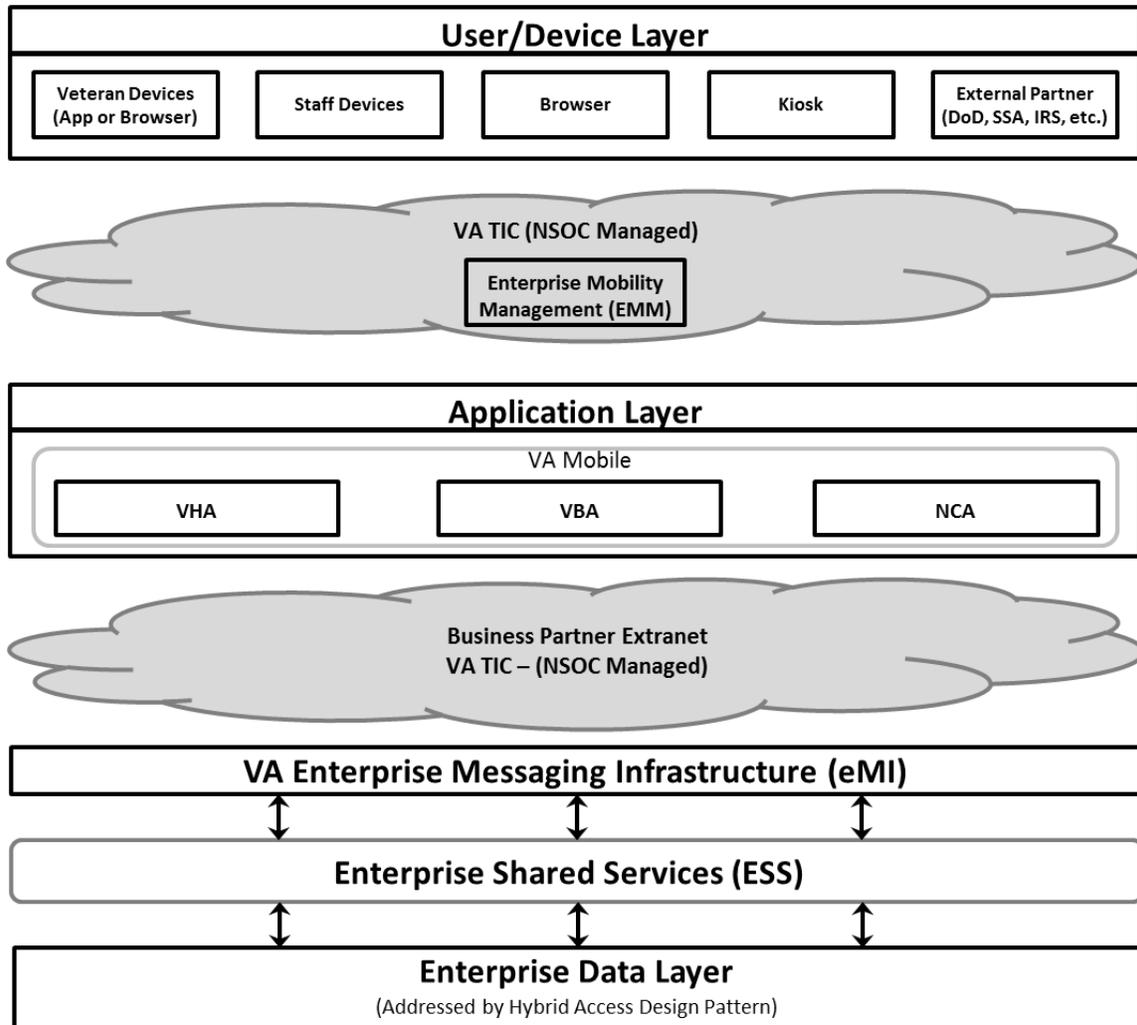


Figure 2: “To-Be” Enterprise Mobile Architecture Design Pattern Concept

3.1 Enterprise Mobile Strategy

An enterprise mobile strategy, as illustrated in Figure 3, will be developed to ensure:

- **Scalable Mobile Application Platform:** The platform will have the ability and flexibility to connect into existing services, serving as middleware by retrieving key data from existing information stores. This platform will make it easier to scale mobile application offerings to meet the complex needs of the user base.
- **Well-defined Mobile User Experience:** Mobile applications set expectations for usability, appearance, and behavior. When developing mobile applications, the design should consider "touch first" simplicity and mobile contextual services (i.e., location and voice). Usage behavior analysis—how users access information and transition from mobile to traditional laptops or desktops—should play a key role in how services are developed.
- **Multi-device and Multi-channel Support:** With a multi-channel and multi-device strategy, VA will be able to reach a greater cross section of Veterans. Cross-platform

development tools and an integration infrastructure will support a multichannel environment.

- **Rapid Application Lifecycle:** Establish a bi-weekly or monthly release schedule for mobile operating systems (OS). Major OS updates will cause Application Programming Interface (API) changes to time devoted to planned application enhancements. Changing phone sizes and form factors pose an additional challenge. The ability to develop applications quickly and inexpensively is a key component of VA's enterprise mobile strategy.

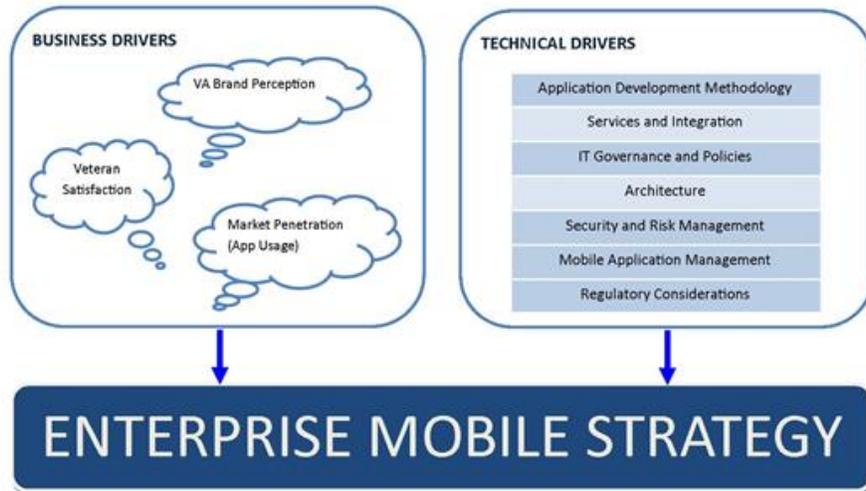


Figure 3: Key Drivers for Mobile Strategy

3.2 Scalable Mobile Architecture

The “To-Be” mobile architecture framework in Figure 4 defines the full stack of functional components required to support mobile application development. This framework addresses the future state of an enterprise-wide mobile development platform and MAM, along with a scalable mobile computing infrastructure compliant with VA policy.

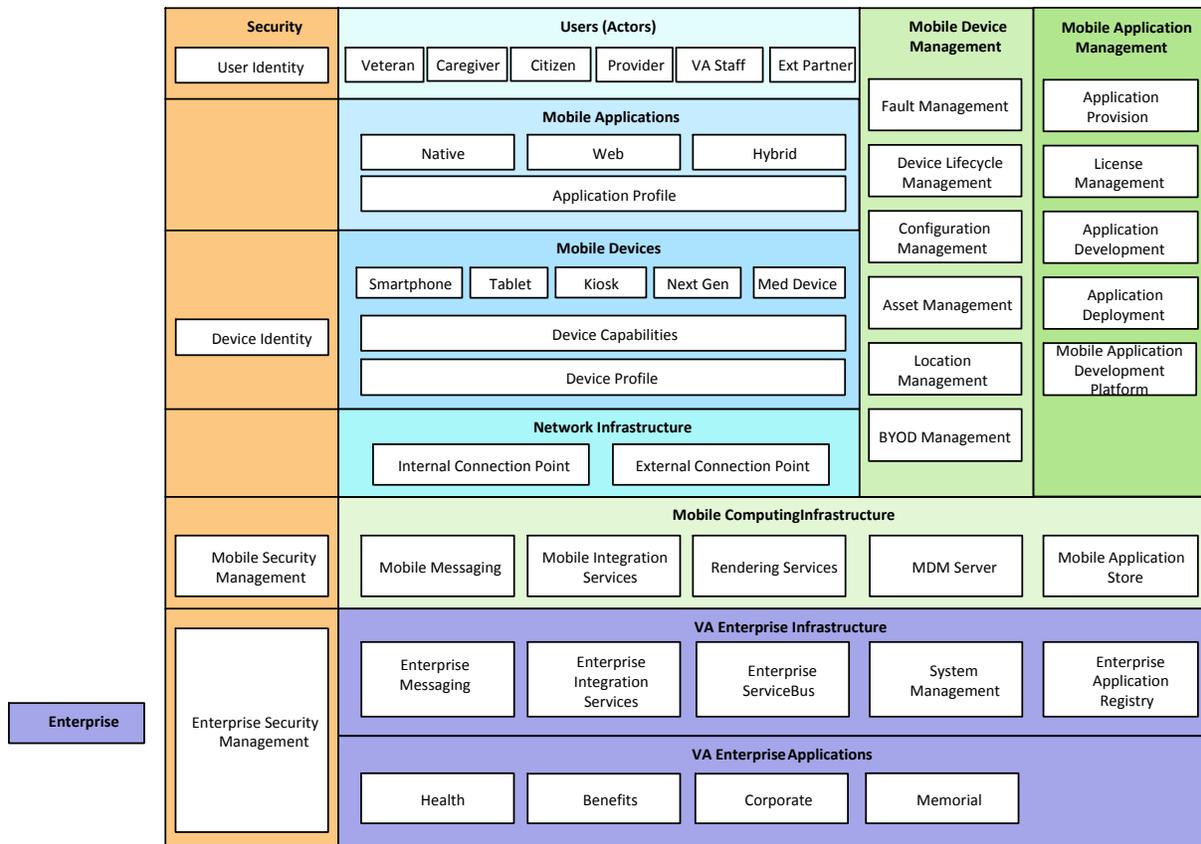


Figure 4: "To-Be" High Level Mobile Architecture Framework

The future capabilities will provide robust MDM to support enterprise-wide BYOD, application containerization, standardized development, and testing environments. The MDM will also support a standard Mobile Application Store (MAS) for internal and external users, standardized security controls, and seamless connections with network access points provided by the National Systems Operating Center (NSOC). The following is a summary of the high-level IT capabilities needed to address limitations cited in Section 2:

- **Mobile Middleware:** Scalable mobile middleware will be implemented to leverage backend Service Oriented Architecture (SOA) services and security capabilities. Transactional systems will need to be prepared to handle a very high volume of concurrent users. Current systems can only support 3,500 concurrent Veterans logging in. An EMM platform will the scability needed to meet the needs of more Veterans.
- **MDM:** MDM will provide the capability to manage both government furnished equipment (GFE) and employee-owned devices (BYOD) across the enterprise. As the demand for VA staff to be able to utilize their own mobile devices to access services on the VA enterprise grows, the need to manage BYOD devices increases.

- The MDM will leverage highly integrated mobile monitoring tools to monitor devices, connections, data sources, protocols, and compliance, across cloud or on premise installations.
- The “To-Be” MDM environment will include a robust, centralized, dedicated administration server environment providing the ability to administer all devices, build policies, publish applications, and perform updates/upgrades, etc. This approach will fully support any regional, departmental, regulatory, or other Administration requirements.
- VA Application Catalog: The VA application catalog will accommodate a hybrid application environment, catering to both applications developed for mobile web browsers and applications integrating more specific functionality (e.g., phone cameras). The catalog will be designed with minimal administrative overhead (i.e., simply controlled and maintained). The application catalog will have the capability to retrieve an app from a commercial app store, place it in a container, and certify the application for use within the VA network (standard suite of tools). This will require coordination with vendors to avoid re-licensing issues and enable containerization of applications from respective commercial app stores.
- Network Reliability: The “To-Be” infrastructure will provide the largest external network throughput possible within budgetary guidelines, providing a full, multi-site high availability and disaster recovery environment with automatic failover and load balancing.
- Mobile Application Management (MAM): The “To-Be” mobile infrastructure will include a scalable MAM capability providing the available throughput for support of an increasing number of cross-platform mobile applications allowing both VA and non-VA users to access ESS through those applications. MAM will provide scalable enterprise-level processes and structures capable of supporting both a “build-as” or a “buy” decision process promoting the re-use of commercial off the shelf (COTS) applications, available open source applications, and internal development of VA specific applications. MAM will be established to ensure application security and remote application management.
- API Gateway: A robust API gateway is required for securing and managing VA’s APIs. This will ensure protection between untrusted and trusted zones providing demilitarized zone (DMZ) class security and a threat defense system at the perimeter to SOA and cloud environments.
- Mobile Back end as a Service (MBaaS): MBaaS combines programmatic and design tools, preconfigured client libraries, connectors, and preconfigured cloud infrastructure, making it easier and more cost-effective for developers to create mobile applications with a cloud back end.

- IPv6 Support: VA has an established IPv6 transition program, which has already met all Office of Management and Budget milestones as of 2012. The mobile architecture supports IPv6 addresses and VA's network infrastructure.
- Geolocation and Geofencing: EMM will enable access to device-specific geolocation features in accordance with NIST guidelines (Appendix D). Future capabilities for MDM may provide support for geofencing and other geospatial capabilities (e.g., remote wiping) dependent on business or other mission requirements.

The mobile architecture includes integration with the eMI for connections to ESS allowing for integration with on-premises resources including Active Directory. Additional attributes include:

- Seamless network/data access regardless of physical location or user roles
- Scalable processes and structures (e.g., development, deployment)
- Support for open source development
- A streamlined application certification process
- All approved internal applications exist in VA Application Catalog
- Authoritative data source for Veteran-facing applications
- Federated credentials across all applications (including mobile)
- Ensured patient information security (e.g., personally identifiable information [PII], protected health information [PHI])

3.3 Mobile Security

In order to meet VA standards for ensuring the security of sensitive information, the "To-Be" mobile infrastructure will integrate with VA's IAM single sign-on (SSO) solutions to ensure Federal Information Processing Standards (FIPS) certified encryption for all data-at-rest and data-in-transit. Encryption and security of content, credentials, and configurations is more critical than device security (i.e., no reliance on native solutions to protect actual data). Mobile users and devices will consume and generate data through ESS via a standardized, authoritative data source for Veteran-facing applications and a specific repository for patient generated data (PGD) ensuring patient information security (e.g., PII, PHI). For PGD, all information from mobile applications will be normalized and adhere to standardized processes for encryption of data-at-rest and data-in-transit in compliance with FIPS 140-2.

To comply with these standards, the mobile environment will provide the ability to integrate advanced security capabilities and solutions for:

- Single Sign On (SSO)
- Access rights management
- Containerization of applications to prevent digital leaks and unauthorized access

- Application wrapping
- Digital signatures
- Derived PIV credentials based on NIST guidance
- Biometric technology used for two-factor authentication (fingerprints, etc.)
- Audit logging

3.4 User Experience

User experience comprises information architecture and visual design. Information architecture addresses business requirements and key performance indicators. Identifying user requirements is a key performance indicator. The following guidelines encompass user experience:

- Service Request Capability: A user should be able to issue a “service request” for the information requested. With this model, the impact to existing systems is minimal. Instead, a service request for information is made to the existing database and presented to the user in a format to be displayed in a mobile application.
- Offline Data Access: The ability to access information or have a temporary cache of data will enhance user experience. Having an encrypted database for short-lived data inside the application will address the security concerns due to data-at-rest on a mobile device.
- Always-ON Virtual Private Network (VPN): A user currently has to resubmit credentials whenever switching networks or whenever the device goes into a sleep mode. Users need the security of an always-ON VPN.
- User Analytics: To demonstrate application adoption, VA will identify application performance metrics to track how an application is performing across various devices and device versions. This data will help optimize the applications to the most popular devices and platforms used by Veterans and VA staff. Metrics including slow web service calls, network performance, and API request performance will help assess the continual ability of the infrastructure to support mobile applications.

3.5 Agile Mobile Application Development

- Centralized Code Repository: All project phases will share a centralized code repository and be governed by a document and change management process.
- Standardized Labs: Alpha labs need to be separated and a centralized beta lab will allow external users to test application code. This allows enforcement of standards and establishes proper controls for consistent results.
- Agile Change Management: Develop a streamlined change management process to address backlogs. Every mobile change management submission will have an approver and a backup approver.

- Automation: Automating key components of the application development process significantly improves the efficiency with which an application or an update can be completed. Automated testing, workflow automation, application vetting, and a rules engine are key components driving efficiency.
- One Code Base: Require a single code base environment to be able to produce multi-platform applications.
- Application Vetting: Application vetting will be enforced to ensure that software is free of exploitable vulnerabilities. This allows rapid identification and resolution of software vulnerabilities across the entire security development life cycle.
- Application Certification and Governance: Certification testing is part of the overarching mobile governance process established for mobile applications required for LOB 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 according to PMAS guidelines. Participation from all VA LOBs on the MAGB is critical to ensuring centralized certification and governance of mobile applications. This review will prevent redundant and overlapping mobile application development and duplicative code development. Mobile application governance is divided into the following groups:

Business: Ensure customer needs and priorities are accurately captured as the “voice of the customer,” prioritize applications, gather business requirements, and identify funding sources.

Technical: Ensure applications are developed following the standard development environment and interfacing with enterprise infrastructure support services. Configure applications to meet operational support requirements using approved technologies from the Technical Reference Model (TRM).

OI&T will guide 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.

- Enterprise Application Store: The VA mobile application store will allow secure management, distribution, and maintenance of VA mobile applications for both Veterans and VA staff.

3.6 Enterprise Mobile Application Maintenance Support

Once VA has A standard mobile environment based on a flexible, secure, and scalable platform will ensure the critical high availability needed to support VA 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 and monitoring capability for tracking, logging, and maintaining applications after they are deployed and available.

3.7 Preparing for Emerging Technologies

3.7.1 Cloud Computing Impact

VA currently uses an outsourced private cloud at the Terremark Facility for its MAE, housing the hardware and software for the following services:

- Mobile Device Management
- Application Lifecycle Management: development, testing, release, and sustainment

Cloud availability within the VA IT infrastructure will be driven by service level agreements established through contracts by OI&T and other VA IT project offices. From a mobile perspective, the IT infrastructure will provide a unified management capability that allows for identifying, viewing, and managing devices, applications, and servers both on premise and in the cloud.

While this Enterprise Design Pattern does not go into the specific capability guidance for these aspects of cloud computing, more guidance is forthcoming in subsequent mobile, cloud computing, and privacy and security Enterprise Design Pattern development efforts.

3.8 Alignment to the TRM

All projects require approved technologies and standards provided by the TRM to comply with the guidance provided in this document. The “To-Be” mobile architecture drives the selection of approved mobility products that go into the TRM.

- Near-Term: Obtain joint recognition/approval of tools and frameworks (e.g., Backbone.js) used by all VA mobile development teams by adding them permanently to the TRM. Begin providing access to non-TRM tools on an evaluation basis allowing developers to test new tools.
- Mid-Term: Continue evaluating and prioritizing tools analyses to support standardized development and management of mobile applications.
- Long-Term: All mobile applications are developed using a streamlined set of approved tools to support:
 - Application Technology: Development tools, application testing, user interface
 - Systems Management: MDM, application performance monitoring, asset management, network performance optimization

- Network Security: Network auditing, encryption, intrusion detection, and prevention

All projects will leverage the approved tools and technologies located in the TRM to comply with the architectural guidance provided in this document. The following tools include:

Table 1: TRM – Mobile Architecture

Tool Category	Example Approved Technologies
Application Security	HP Fortify
Application Development Tools	HTML
Authentication	XACML, OAuth 2.0
Encryption	SAML, WS- Security, S-HTTP, TLS
Mobile App Development Tools	Adobe Edge Inspect, Adobe Edge PhoneGap Build, Android SDK, Apache Cordova, Apple Xcode, CSS-Mobile, ColdFusion Builder, LawnChair, jQuery Mobile, RAD Studio XE, Reflector, TestFlight
Web Browsers	Google Chrome, MS Internet Explorer, Safari

4 USE CASES

Use Case #1

Use Case	Use	Data Sensitivity
Veteran consumes public Information and other public data	Veteran/citizen seeks information on TBI, PTSD, GI Bill, Burial, home loans, etc., using a mobile device	Public Information

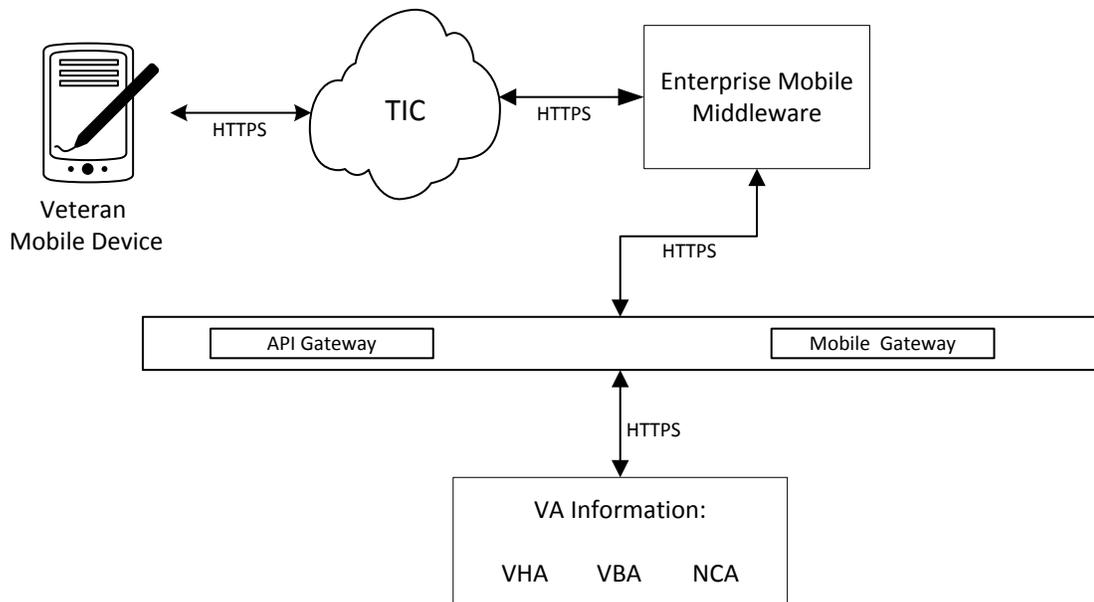


Figure 5: Use Case #1

Steps for Use Case #1

- 1) Mobile device establishes a connection with the Enterprise Mobile Middleware via HTTPS
- 2) The middleware connects with the Mobile Gateway, which then interacts with the API Gateway
- 3) The API Gateway retrieves the information from VA back end services (VHA, VBA, or NCA) the user is looking for
- 4) The data is then sent back to the user and rendered in the mobile application as a response

Use Cases #2 & #3

Use Case	Use	Data Sensitivity
VA staff uses corporate information services, e.g., email, messaging	VA staff exchange email, messaging, etc., via approved mobile devices. Staff use web access to research medical information, benefit claims, SharePoint to share, etc. Clinical data without PII	SPI/PHI ACI Public (i.e., VA data/FOUO/PII/ Acquisition Sensitivity IAM SSOi or PIV)
VA staff access Veteran's HIPAA/PGD/PII/EHR data	VA staff use and exchange medical or benefits data using approved devices to treat a Veteran. VA staff perform a housing inspection for a VA loan. Right information at the right time for the proper care.	SPI/PHI ACI (i.e., VA data/PGD/EHR/IAM SSOi or PIV)

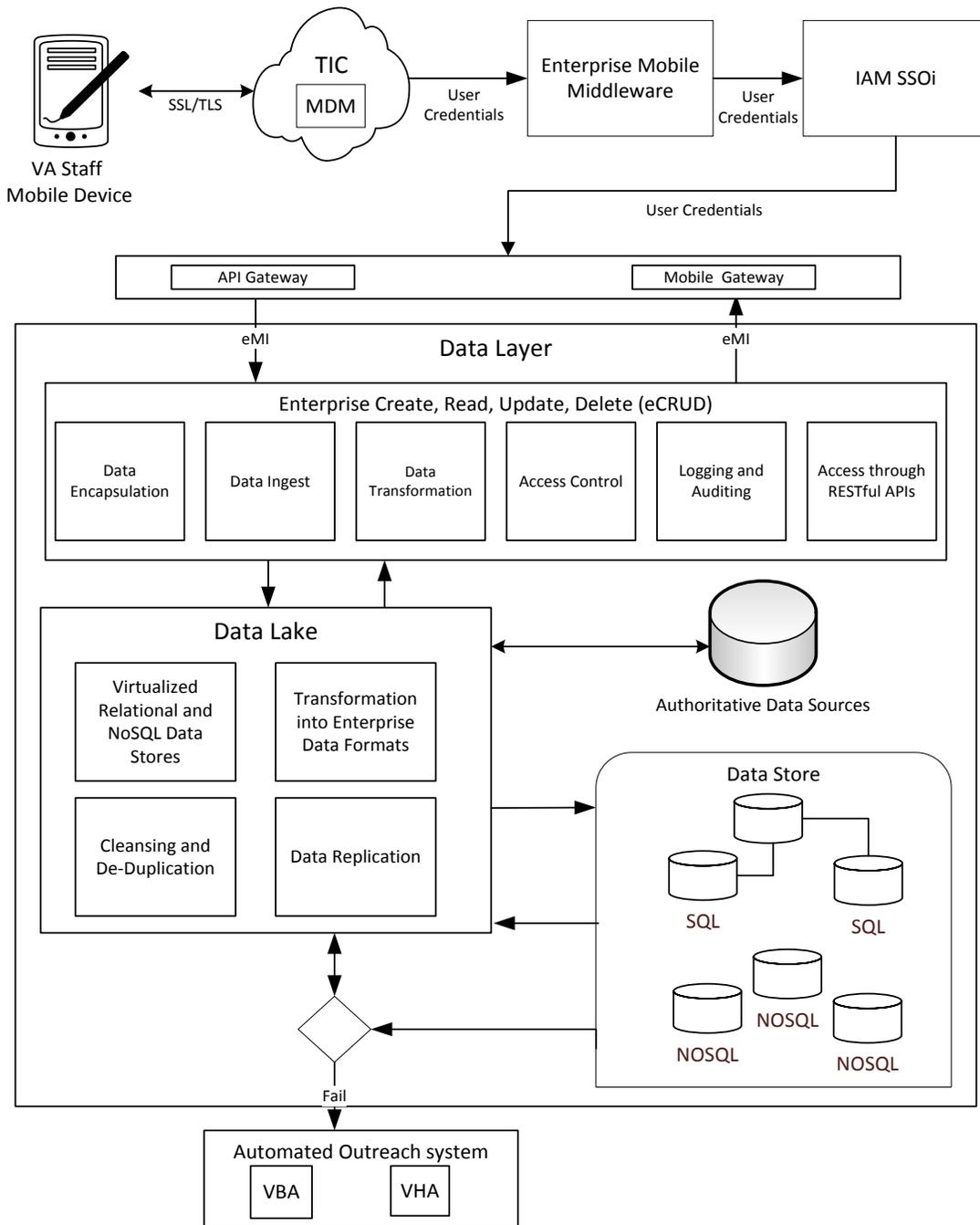


Figure 6: Use Cases #2 and #3

Steps for Use Case #2

- 1) Mobile device utilizes SSL/TLS to secure data being sent across the network, through a trusted Internet connection (TIC) to the Enterprise Mobile Middleware

- 2) User credentials are forwarded to the IAM
- 3) IAM SSOi authenticates the user and interacts with the Mobile Gateway, which then connects with the API Gateway
- 4) API Gateway utilizes eMI to connect with shared services (e.g., email, messaging)
- 5) Information is retrieved and displayed on the mobile device

Steps for Use Case #3

- 1) Mobile device utilizes SSL/TLS to secure data being sent across the network, through a TIC to the Enterprise Mobile Middleware
- 2) User credentials are forwarded to the IAM
- 3) IAM SSOi authenticates the user and interacts with the Mobile Gateway, which then connects with the API Gateway
- 4) API Gateway utilizes eMI to connect with the Data Layer
- 5) Application calls on authoritative information services to access VistA for Veteran patient information
- 6) VA staff selects an option to view current Veteran data. Application calls on shared services to retrieve Veteran's information. Information is displayed on the mobile device.

Use Case #4

Use Case	Use	Data Sensitivity
VA staff and DoD health IT systems	VA staff access DoD medical systems using approved mobile devices. VA doctor can view DoD health information 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 (i.e., VA data / PHI / PGD / EHR/ DoD / IAM–user id / password / PIV / SAML)

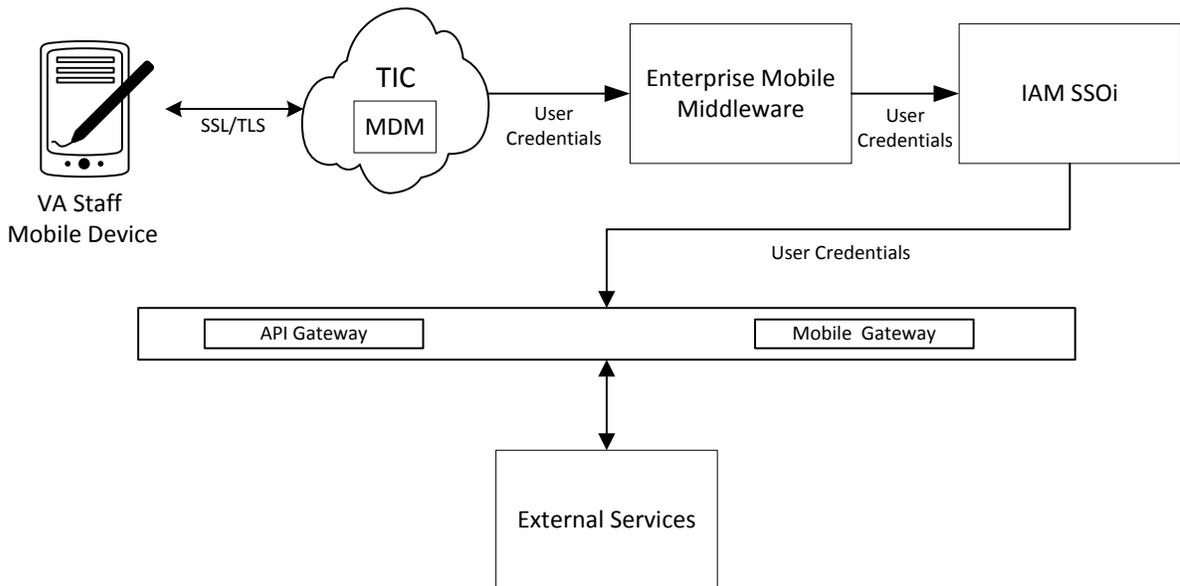


Figure 7: Use Case #4

Steps for Use Case #4

- 1) Mobile device utilizes SSL/TLS to secure data being sent across the network, through a TIC to the Enterprise Mobile Middleware
- 2) User credentials are forwarded to the IAM
- 3) IAM SSOi authenticates the user and interacts with the Mobile Gateway, which then connects with the API Gateway
- 4) The API Gateway provides access to the DoD medical system and other external services

Appendix A. DOCUMENT SCOPE

Scope

This Enterprise 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 re-usable capabilities, as validated by VA LOBs, to provide seamless mobile access to VA ESS through the VAMF and 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.

This 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 Enterprise 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.

Intended Audience

This Enterprise Design Pattern is meant to be used by VA Integrated Project Teams (IPT) 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.

Document Development and Maintenance

This document was developed collaboratively with internal stakeholders from across the Department and included participation from VA’s 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, who will also facilitate stakeholder coordination and subsequent re-approval depending on the significance of the change.

Appendix B. DEFINITIONS

Key Term	Definition
Enterprise Shared Service	<p>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.</p> <p>http://vaww.ea.oit.va.gov/enterprise-shared-services-service-oriented-architecture/</p>
Mobile Application	<p>A mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer. Mobile applications frequently serve to provide users with similar services to those accessed on PCs. Apps are generally small, individual software units with limited function.</p>
Mobile Application Management	<p>The delivery and administration of enterprise software to end users' corporate and personal smartphones and tablets.</p>
Mobile Device	<p>A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smartphones, tablets, and E-readers.</p>
Mobile Device Management	<p>Software that secures, monitors, manages and supports mobile devices deployed across mobile operators, service providers and enterprises. MDM functionality includes over-the-air distribution of applications, data and configuration settings for all types of mobile devices, including mobile phones and smartphones and tablet devices.</p>
Service	<p>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.</p>

Key Term	Definition
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 consistent with measurable preconditions and expectations.

Appendix C. ACRONYMS

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

Acronym	Description
AA&A	Authentication, Authorization and Audit
ACI	Administratively Confidential Information
API	Application Programming Interface
ASD	Architecture, Strategy and Design
ATO	Authority to Operate
BPE	Business Partner Extranet
BYOD	Bring Your Own Device
CDW	Corporate Data Warehouse
COTS	Commercial Off the Shelf
EA	Enterprise Architecture
EAA	Enterprise Application Architecture
EHR	Electronic Health Record
eMI	Enterprise Messaging Infrastructure
EMM	Enterprise Mobility Management
ESCCB	Enterprise Security Change Control Board
ESS	Enterprise Shared Services
ETA	Enterprise Technical Architecture
ETSP	Enterprise Technology Strategic Plan
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
IoT	Internet of Things
IPT	Integrated Project Team
IT	Information Technology
LOB	Line of Business
MA	Mobile Application
MADP	Mobile Application Development Platform
MAGB	Mobile Application Governance Board
MAE	Mobile Application Environment

Acronym	Description
MAM	Mobile Application Management
MAP	Mobile Application Program
MARA	Mobile Application Reference Architecture
MAS	Mobile Application Store
MBaaS	Mobile Back end as a Service
MDM	Mobile Device Management
MHED	Mobile Health External Development
MVI	Master Veteran Index
NCA	National Cemetery Administration
NIST	National Institute of Standards and Technologies
NSOC	Network Security Operations Center
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
TIC	Trusted Internet Connection
TRM	Technical Reference Model
VAMF	VA Mobile Framework
VBA	Veteran Benefits Association
VHA	Veteran Health Administration
VistA	Veterans Health Information Systems and Technology Architecture
WAR	Web Application Archive

Appendix D. REFERENCES, STANDARDS, AND POLICIES

This Enterprise Design Pattern is aligned to the following VA OI&T references and standards applicable to all new applications being developed in the VA, and are aligned to the VA ETA:

#	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 IT capabilities that are provided through Enterprise Shared Services (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	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
5	VA	ESS Directive	<ul style="list-style-type: none"> Establishes policy regarding the development, deployment, and management of ESS in the VA
6	VA	VA Enterprise Technology Strategic Plan (ETSP)	<ul style="list-style-type: none"> The Enterprise Mobile Architecture design pattern will help projects develop applications in alignment with the Mobility attributes of the ETSP’s IT Vision
7	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 the VA