
VA Enterprise Design Patterns:

5. Mobility

5.3 Staff-Facing Mobile Devices and Applications

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

Version 1.0

Date Issued: March 2016



THIS PAGE INTENTIONALLY LEFT BLANK FOR PRINTING PURPOSES

APPROVAL COORDINATION

Rodney Emery
Director, Technology Strategies and GEAC, ASD

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

REVISION HISTORY

Version	Date	Organization	Notes
0.1	11/13/2015	ASD TS	Initial Draft
0.3	12/10/2015	ASD TS	Updated draft to include business need and approach. Incorporated stakeholder input to develop current capabilities and limitations section.
0.5	2/12/2016	ASD TS	Updated draft to include best practices derived from vendor engagements.
0.7	3/2/2016	ASD TS	Updated to reflect comments received during the public forum.

REVISION HISTORY APPROVALS

Version	Date	Approver	Role
0.1	11/13/2015	Nick Bogden	ASD TS Mobile Architecture Design Pattern Lead
0.3	12/10/2015	Nick Bogden	ASD TS Mobile Architecture Design Pattern Lead
0.5	2/12/2016	Nick Bogden	ASD TS Mobile Architecture Design Pattern Lead
0.7	3/2/2016	Nick Bogden	ASD TS Mobile Architecture Design Pattern Lead

TABLE OF CONTENTS

1.0	INTRODUCTION	1
1.1	BUSINESS NEED.....	1
1.2	APPROACH.....	2
2.0	CURRENT CAPABILITIES AND LIMITATIONS	2
2.1	AS-IS MOBILE STRATEGY GAPS	3
2.1.1.	<i>Accessing Enterprise Resources</i>	3
2.1.2.	<i>Operations and Maintenance</i>	3
2.1.3.	<i>Mobile Device Management</i>	3
2.2	LACK OF MOBILE APPLICATIONS GOVERNANCE BOARD	4
2.3	AUTHENTICATION GAPS.....	4
2.3.1.	<i>Single Sign-On and PIV</i>	4
2.3.2.	<i>Two-factor Authentication</i>	4
2.4	MOBILE INFRASTRUCTURE RELIABILITY AND SCALABILITY ISSUES	5
3.0	FUTURE CAPABILITIES	5
3.1	TO-BE MOBILE STRATEGY	5
3.2	NEW AUTHENTICATION FACTORS	8
3.3	MOBILE ARCHITECTURE AND INFRASTRUCTURE	9
3.4	ALIGNMENT TO TRM	12
4.0	USE CASES	14
APPENDIX A.	DOCUMENT SCOPE	18
	SCOPE.....	18
	DOCUMENT DEVELOPMENT AND MAINTENANCE.....	18
APPENDIX B.	DEFINITIONS	19
APPENDIX C.	ACRONYMS	20
APPENDIX D.	REFERENCES, STANDARDS, AND POLICIES	22

FIGURES

Figure 1 – GFE Mobile Devices and BYOD Staff-Facing Application Access.....	8
Figure 2 – VA “To-Be” Mobile Architecture.....	10
Figure 3 – Use Cases #1 and #2	15
Figure 4 – Use Case #3.....	17

TABLES

Table 1 – Current Issues and Future State.....	11
Table 2 – TRM Approved Standards and Technologies	13
Table 3 – Definitions.....	19
Table 4 – Acronyms	20
Table 5 – References, Standards, and Policies.....	22

1.0 INTRODUCTION

The Department of Veterans Affairs (VA), Office of Architecture, Strategy, and Design (ASD) conducted an independent study in 2014 to identify mobile computing issues and found that “VA users and employees will not seek the approval of VA government hierarchy to use new commercial technology, nor will VA government hierarchy be able to stop or control the introduction of new commercial technology into the VA work environment¹”. VA staff and contractors are increasingly using mobile devices to access enterprise resources. VA requires standardized approaches to regulating staff and contractor access to these resources while permitting flexibility as new mobile technologies become available.

1.1 Business Need

The Veterans Health Administration’s (VHA) Office of Informatics and Analytics and Human Factors Engineering (HFE) group has found that clinicians will continue to leverage various forms of devices to access VA services. The Mobile and Security Technology office in Service Delivery and Engineering (SDE) Enterprise Systems Engineering (ESE) estimates up to 70,000 new mobile devices will be added to the VA network in the next two years. VA must continue to make investments in the mobile infrastructure to support this growing need. These investments help VA address IT infrastructure adaptability concerns that hinder a mobile workforce, in accordance with the Enterprise Technology Strategic Plan (ETSP). Secure connections with mobile infrastructure enhancements improve agility and responsiveness to customer demands. The following are four critical issues for staff-facing mobile devices and applications:

- Incomplete mobile strategy leaves gaps in policy and infrastructure decisions that adversely affect VA staff.
- Lack of a centralized mobile governance board creates inconsistencies between policies and policy enforcement between administrations, lines of business (LOB), and programs.
- Current available authentication factors do not take advantage of the latest mobile technologies and standards that provides enhanced security while simplifying authentication for VA staff.
- VA’s mobile infrastructure has reliability issues that prevent VA staff from performing their tasks.

¹VA. (2014) *VA Mobile Computing Program Assessment*

1.2 Approach

The near-term approach to evolving enterprise capabilities for staff-facing mobile devices and applications is as follows:

- Continue support for existing government furnished equipment (GFE) mobile devices.
- Incorporate new GFE mobile devices and bring your own device (BYOD) requirements into existing mobility governance functions.
- Examine impact of enterprise mobile GFE and BYOD requirements on existing VA mobile infrastructure, and derive both functional requirements for infrastructure enhancements and non-functional requirements (e.g., security, availability, reliability).
- Transition existing GFE and BYOD devices to enhanced mobile infrastructure that addresses functional and non-functional requirements.

The current capability limitations identified in Section 2 must be examined to establish guiding principles and a centralized policy for VA staff-issued GFE mobile devices and BYOD. Section 3 provides an approach to evolving capabilities to achieve a mobile-ready workforce, based on industry best practices for managing staff-facing mobile devices and applications.

2.0 CURRENT CAPABILITIES AND LIMITATIONS

The following will address a set of issues in VA, while providing insight on the current capabilities for staff-facing mobile devices and applications:

- “As-Is” Mobile Strategy Gaps
 - No guidance on the use of Virtual Private Network (VPN) or Citrix Access Gateway (CAG). In some cases staff are directed to use both technologies
 - There is no plan for operations and maintenance of applications beyond the sustainment period
 - Multiple Mobile Device Management (MDMs) utilized to manage Mobile GFE
- Lack Of Mobile Applications Governance Board (MAGB)
 - No cohesiveness between LOBs and individual work streams for mobility
 - Lack of interest and participation from MAGB
- Authentication Gaps
 - SSOi is not being fully utilized by all staff-facing applications
 - Personal Identity Verification (PIV)-Only Authenticated (POA) users are unable to use MobilePASS for remote CAG
- Mobile Infrastructure Reliability and Scalability Issues
 - Data packets are being lost during transfer with GFE mobile devices accessing VA services

- Current VA Mobile Framework (VAMF) infrastructure will not support the scalability needed for the expected growth of staff-facing mobile devices accessing the VA network in the near future

2.1 As-Is Mobile Strategy Gaps

2.1.1. Accessing Enterprise Resources

Capabilities: Currently, VA's mobility strategy allows for remote access to enterprise resources only through the Citrix Access Gateway (CAG). Office of Information & Technology (OI&T) stakeholders have stated that this method has room for improvement to enable VA staff and contractors to access the VA network. As a result, VA is researching two usage models that use a native application as opposed to CAG. The first model would allow VA staff to use an additional mobile device to access information. The second usage model would allow VA staff to choose the device they want to use. In addition, VHA is developing a mobile and BYOD program through coordination with the VHA CTO. The program includes different options for BYOD mobile devices such as Secure Services BYOD, Comprehensive BYOD, and Mobile Deployment.

Limitation(s): While VA staff has access to the VA network through CAG, reliability issues often hinder staff from connecting to VA systems and services. Furthermore, a cost analysis performed by VA revealed that the CAG solution was significantly more expensive than alternative technologies such as VPN.

2.1.2. Operations and Maintenance

Capabilities: Staff-facing applications have a three-month sustainment period until they become the responsibility of the business owner. Maintaining applications to address security vulnerabilities and other software issues is a key factor in determining the success and usefulness of the application to staff. It will be crucial for any security vulnerabilities to be addressed in a timely manner to protect the VA network and data.

Limitation(s): There is no plan for operations and maintenance of applications beyond the sustainment period. It is critical to clearly assign responsibility and funding for maintenance of staff-facing applications beyond the sustainment period.

2.1.3. Mobile Device Management

Capabilities: Currently, there are multiple MDMs utilized to manage GFE mobile devices in VA. Blackberry Enterprise Server (BES) is the legacy system utilized to manage all Blackberry GFE mobile devices. AirWatch's MDM is utilized to manage all other types of GFE mobile devices. Existing MDM capabilities include enforcing password complexity requirements, delivering and

removing applications, reviewing which applications are installed on the device, and delivering and removing VPN profiles, VA Intranet and Wi-Fi access.

Limitation(s): Managing multiple MDMs for different operating systems raises the potential for configuration management issues whenever changes to the baseline security standards for mobile devices occur. Additionally, it cannot deliver a FIPS 140-2 vault in which all VA applications or data reside. VA requires Federal Information Processing Standard (FIPS) 140-2 encryption for all data that has to be encrypted.

2.2 Lack of Mobile Applications Governance Board

Capabilities: Currently, each LOB manages mobility activities for their business needs. VHA releases the majority of application development under the Connected Health Board.

Limitation(s): Insufficient IT standards, policies, and processes for mobile technologies have hindered VA, as explained in greater detail in the Mobile Architecture Enterprise Design Pattern. There is a lack of a centralized MAGB to create and enforce policies between administrations, LOBs, and programs.

2.3 Authentication Gaps

2.3.1. Single Sign-On and PIV

Capabilities: Office of Management and Budget (OMB) M 11-11 mandates that agencies “require the use of PIV credentials as the common means of authentication for access to that agency’s facilities, networks, and information systems.” In accordance with this mandate, VA implemented policies that require the use of Public Key Infrastructure (PKI) enabled PIV cards to enable internal user identity authentication to Active Directory (AD). VA’s Identity and Access Management (IAM) Single Sign-On Internal (SSOi) is available only to internal VA users and supports PKI, AD username/password, and Kerberos.

Limitation(s): VA’s GFE mobile devices and BYOD must use IAM’s SSOi for applications accessing PII/PHI data. Currently not all staff-facing applications use SSOi, thereby forcing users to perform multiple logons to individual applications. The Use Cases in Section 4 provide additional context regarding use of IAM services by mobile devices to access enterprise resources.

2.3.2. Two-factor Authentication (2FA)

Capabilities: In conjunction with M-11-11, VA implemented Two-Factor Authentication (2FA) as a result of federal directives mandating all federal systems use multi-factor authentication. To comply with this directive VA Staff/Contractors who use CAG to connect to the VA internal network must have a PIV card and PIN. As the majority of mobile devices (e.g. smart phones

and tablets) are not PIV-enabled devices, VA developed MobilePASS which provides Two-Factor Authentication for remote CAG users by generating a one-time password (OTP) code.

Limitation(s): VA has determined that a certain portion of staff members will be enforced to use their PIV cards for VA network access. These staff members will be designated PIV-Only Authentication (POA) and will not be able to use MobilePASS which would require them to have a PIV reader on their phone. In addition, despite the introduction of MobilePASS, there are new authentication factors that offer greater security and easier means for VA staff to authenticate themselves that need to be incorporated in VA.

2.4 Mobile Infrastructure Reliability and Scalability Issues

Capabilities: The VA Mobile Framework (VAMF) provides an internet accessible layer of services to isolate VA applications from VA infrastructure and provides secure access to VA back end services. Current systems can only support 3,500 concurrent users and need the ability to scale up to support many more users accessing enterprise resources.

Limitation(s): One issue is the ability to manage and support the increase of connections to back end services. There are already reliability issues with the VA mobile infrastructure as reported by VHA's application development team. Tests performed on staff-facing applications using GFE mobile devices accessing VA services have shown lost data packets during transfer. These issues will only be exacerbated with an increased network load.

Another challenge with the VAMF is that the implementation is not extensible. The VAMF was designed so that all runtime support services were bundled into one web application archive (WAR) file. This caused development and testing issues due to unpacking and packing of the entire WAR file for each build. To address this limitation, multiple instances of the same WAR file were deployed introducing scalability challenges across all of the application services (WebLogic) that constitute the VAMF introducing an issue with the WebLogic server running out of memory.

3.0 FUTURE CAPABILITIES

3.1 To-Be Mobile Strategy

The "to-be" mobile strategy requires stakeholder participation across all OI&T pillars and LOBs to establish consistent expectations and criteria for VA staff usage of mobile devices and applications. This includes secure access of enterprise resources through containerized applications and internal VA stores, using a rapidly elastic and robust enterprise mobility management platform, as explained in the Mobile Architecture Enterprise Design Pattern. The current information security policy listed in the VA Handbook 6500 states that all mobile

devices that store and transmit VA data must be GFE. All applications developed and used must store and transmit data using a FIPS 140-2 validated cryptographic module. This policy limits BYOD to “thin client” solutions where no VA data is stored on the mobile device itself, which is consistent with standards in VA’s Enterprise Technical Architecture (ETA).

- Thin Client Solution: The use of Virtual Desktop Infrastructure (VDI) combined with virtualization technology to provide a thin client solution for BYOD. VDI refers to the process of running a user desktop inside a virtual machine that lives on a server in the datacenter. VDI provides the means to connect to legacy VA applications such as VistA. The use of VDI would provide several benefits including reduced time to deploy applications and updates, central administration, and protection against loss and leaks of VA data. A thin client solution works well with a strong authentication mechanism, which VA has with the enforcement of 2FA. *Problem(s) Addressed: Mobile Strategy Gaps*
- Transition Legacy Systems: With VA looking into the development of a mobile version of the VistA application with complete encryption, VDI would provide a transitional step as more legacy VA systems are replaced or supplemented with newer mobile friendly technologies. *Problem(s) Addressed: Mobile Strategy Gaps, Mobile Infrastructure Reliability and Scalability Issues*
- Open Framework: VA GFE mobile devices that are managed by MDM and Mobile Application Management (MAM) need to be configured to ensure access to external systems relevant to VA (e.g. DoD health IT systems, third-party hospitals, commercial pharmacies, etc.). *Problem(s) Addressed: Mobile Strategy Gaps*
- Mobile Phone Docking: The continual increase in processing power of mobile devices along with its proliferation across VA presents new opportunities. To leverage this development, VA will implement mobile device docking stations connected to a video monitor, keyboard, and mouse at strategic locations (e.g. VA offices, VA hospitals). *Problem(s) Addressed: Mobile Strategy Gaps*
- Enterprise Mobility Management (EMM): EMM is a key component to securing and managing GFE and BYOD mobile devices. EMM itself consists of many components, not all of which will need to be implemented by VA. The following describes the components VA needs to continue investing in. *Problem(s) Addressed: Mobile Strategy Gaps*
 - MDM: VA should consolidate all mobile devices to be managed under one MDM. Managing multiple MDMs for different operating systems raises the potential for configuration management issues and increases complexity. GFE mobile devices should continue to be managed by an MDM solution. Discussions with VA stakeholders have led to the determination that VA staff would not want a BYOD

solution where they would have to enroll their mobile devices to a MDM solution.

- MAM: An alternative yet also secure method is the use of application wrapping. This approach provides security and management capabilities to already-developed staff-facing applications.
- Data Management: A data management security strategy will need to cover keeping data encrypted while only allowing approved applications to access and transmit data. GFE mobile devices will utilize encrypted containers that meet FIPS 140-2 standards to protect data at rest. BYOD would not have any data stored in the device so this would not be an issue. Both GFE and BYOD mobile devices would need to have data encrypted during transmission that also meets FIPS 140-2 encryption standards. VA follows guidance from Office of Management and Budget (OMB) 04-04 and National Institute of Standards and Technology (NIST) SP 800-63-2 to rate all existing mobile applications and categorize them to the appropriate Levels of Assurance (LOA). Every staff-facing mobile application will perform a risk assessment to determine the minimum LOA In accordance with the User Identity Authentication Enterprise Design Pattern.
- Unified Endpoint Management: As device management (e.g. PCs, mobile devices, and connected devices) matures, VA will want to merge the management of all these devices into a single unified endpoint management, in accordance with IT Service Management (ITSM) Enterprise Design Patterns and VA 6500 Handbook guidance. *Problem(s) Addressed: Mobile Strategy Gaps*
- Policy Compliance: VA will need to adhere to new policies issued to Government agencies. This includes the new open source software policy included in the Second Open Government National Action Plan (NAP). This policy requires that: (1) new custom code whose development is paid for by the Federal Government be made available for re-use across Federal agencies; and (2) a portion of that new custom code is released to the public as Open Source Software (OSS). *Problem(s) Addressed: Mobile Strategy Gaps*

Figure 1 below depicts how VA staff and contractors will download staff-facing applications via GFE devices and BYOD.

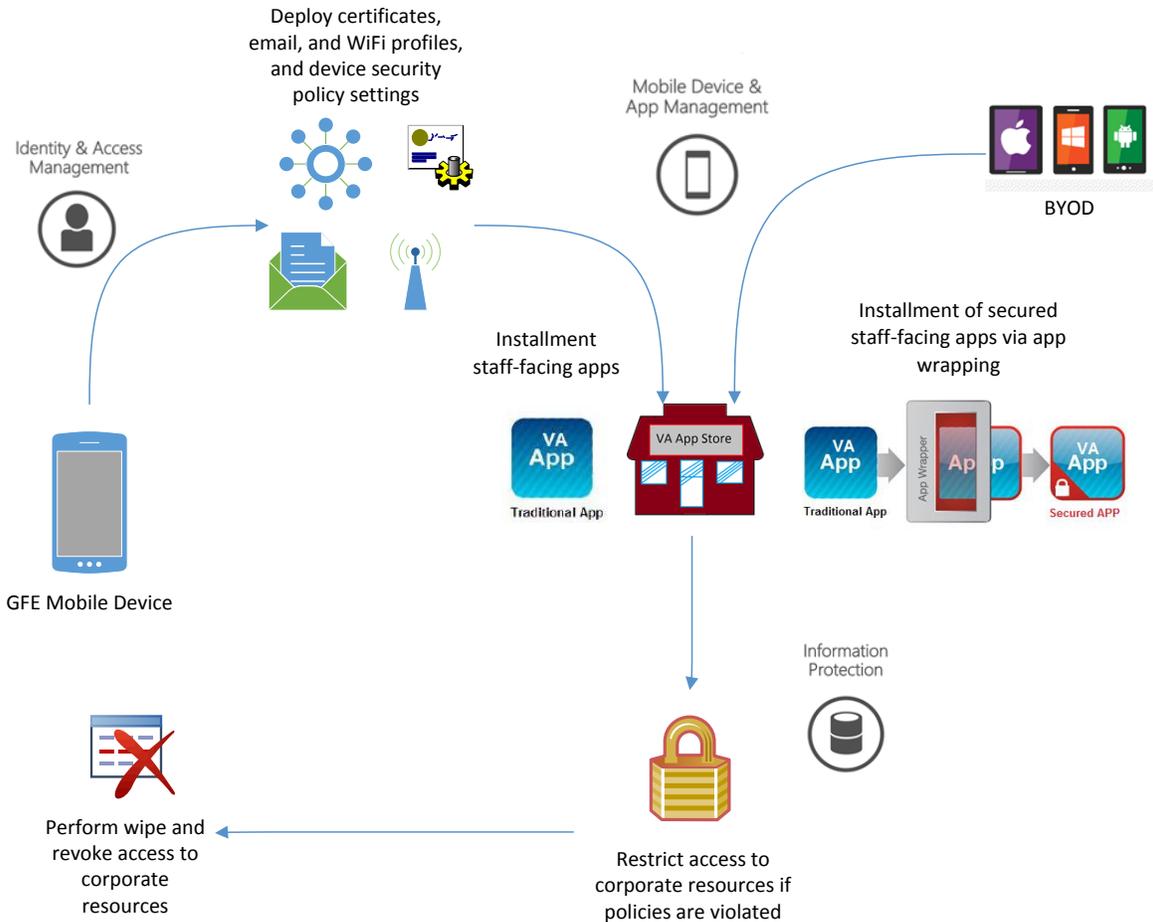


Figure 1 – GFE Mobile Devices and BYOD Staff-Facing Application Access

GFE devices will have MDM installed providing VA with device management capabilities such as configuring device security policies, deliver and remove: VPN profiles, VA Intranet, and Wi-Fi access. Staff will download staff-facing apps via the internal VA application store which serves as the authoritative source for all staff-facing applications. BYOD devices will not have MDM installed and instead will download staff-facing applications via the internal VA application store that are secured through application wrapping. Access to corporate data will be restricted if the mobile device falls out of compliance with GFE/BYOD guidelines. VA will have the capability to remove applications from the GFE/BYOD devices if a device falls out of compliance or is lost.

3.2 New Authentication Factors

- Derived Personal Identity Verification (PIV): NIST SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials provides guidelines for implementing

derived PIV credentials for mobile devices. A derived PIV credential provides an alternative token, which can be implemented and deployed directly on the mobile device. This makes it a practical alternative for mobile devices that do not have PIV card readers or Near-Field Communication (NFC) to communicate with a PIV card directly.

Problem(s) Addressed: Authentication Gaps

- **Biometrics:** The use of biometrics as an authentication factor will be utilized with the continued introduction of biometric reading capabilities of smart phones (e.g. fingerprint, voice pattern, iris scanning, facial recognition, etc.). Biometric authentication offers several advantages such as never being lost or stolen, cannot be forgotten, and unique to each individual. VA Connected Health is working on developing biometric authentication for VA Staff. *Problem(s) Addressed: Authentication Gaps*

3.3 Mobile Architecture and Infrastructure

Figure 2 shows 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) via the Enterprise Messaging Infrastructure (eMI) through staff-facing applications.

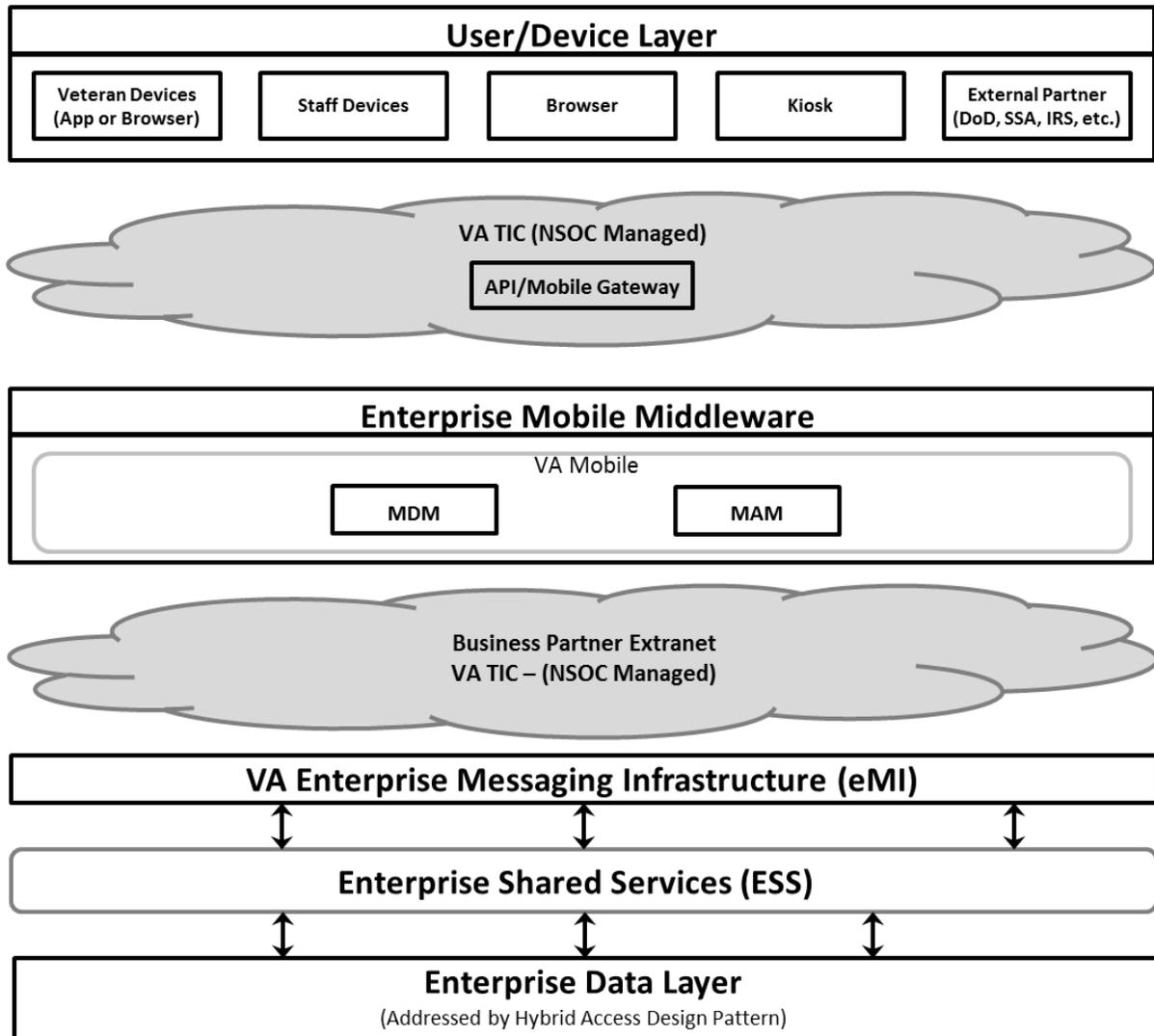


Figure 2 – VA “To-Be” Mobile Architecture

The “To-Be” VA mobile architecture framework needs to be designed in a manner that is open and scalable.

- **Reusable Backend Services:** A key to achieving an open and scalable architecture framework is to adjust the way staff-facing mobile applications are developed. Backend services should be developed as a set of server-side functions that are optimized for a mobile environment. These server side functions can be published as application programming interfaces (APIs) and should be discoverable to developers through a service catalogue. The frontend developer will then be able to focus on the development of client side applications and simply utilize the backend service to connect with VA ESS and the Enterprise Data Layer. VA will be able to control which

frontend developers will have access to certain backend services. Problem(s) Addressed: *Mobile Infrastructure Reliability and Scalability Issues*

- Backend Service Catalogue: Backend services will be accredited and registered in an enterprise service registry, thereby centralizing security, policy management, and access control. This also provides the potential to modify the back-end service calls in a loosely coupled manner without modifying the front-end of the application. Problem(s) Addressed: *Mobile Infrastructure Reliability and Scalability Issues*

The following table provides a summary of the current state issues and how they will be addressed in the future state.

Table 1 – Current Issues and Future State

Area	Current State	Future State
Governance	Lack of centralized oversight across the multiple LOBs in VA and insufficient support for mobile service development and implementation.	The MAGB with full participation from all LOBs to strictly manage the VAMF and enforce mobile policies.
MDM	There are currently two MDMs in place; BES manages all Mobile GFE Blackberrys, while Airwatch manages all other types of Mobile GFE.	A hybrid solution which incorporates an MDM and containerization solution.
Logon	Multiple logons to individual apps are required.	Use of SSOi solution for VA staff and contractors to use multiple staff-facing apps.
Operations and Maintenance	There is no plan for operations and maintenance of applications beyond the three-month sustainment period.	An O&M plan which defines tasks, activities, and responsible parties and will be updated as changes occur.

Area	Current State	Future State
Mobile Infrastructure	There are reliability issues with the VA mobile infrastructure as data is lost between staff mobile devices and VA systems.	Reusable back-end services discoverable through a service catalogue.
BYOD	There are currently no policies in place for BYOD. CAG is the only approved method but is limited in accessing the VA network.	Use of a thin client solution, such as VDI in conjunction with application wrapping, will keep data off the device and provide data encryption.
Security	2FA for mobile devices with MobilePass	More robust authentication factors including derived PIV credentials and the use of biometrics.

3.4 Alignment to TRM

All components of VA’s “to-be” mobile architecture will use approved technologies and standards located in the VA Technical Reference Model (TRM) to comply with the architectural guidance provided in this document. VA will evaluate new technologies, particularly those provided by commercial cloud service providers, and those approved for enterprise consumption will be catalogued in the TRM. Mobile application developers are constrained by the approved mobile devices and development and testing tools supporting an agile system development lifecycle (SDLC).The following table highlights the standards profile and approved technologies for staff-facing mobile applications and devices.

Table 2 – TRM Approved Standards and Technologies

Tool Category	Example Approved Standards and Technologies
Static Code Analysis	HP Fortify
User Interface	HTML5, AngularJS
Authorization	XACML, OAuth (delegated access)
Authentication	SAML, OpenID Connect
Development Tools	Eclipse Android SDK, Apache Cordova, Apple Xcode, RAD Studio XE, Reflector, TestFlight

4.0 USE CASES

The following use cases are examples that demonstrate the application of the capabilities and recommendations described in this document.

Use Case #1 & #2, depicted in Figure 3, per the Mobile Architecture Enterprise Design Pattern.

Use Case	Use	Data Sensitivity
1. 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)
2. 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 performs 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)

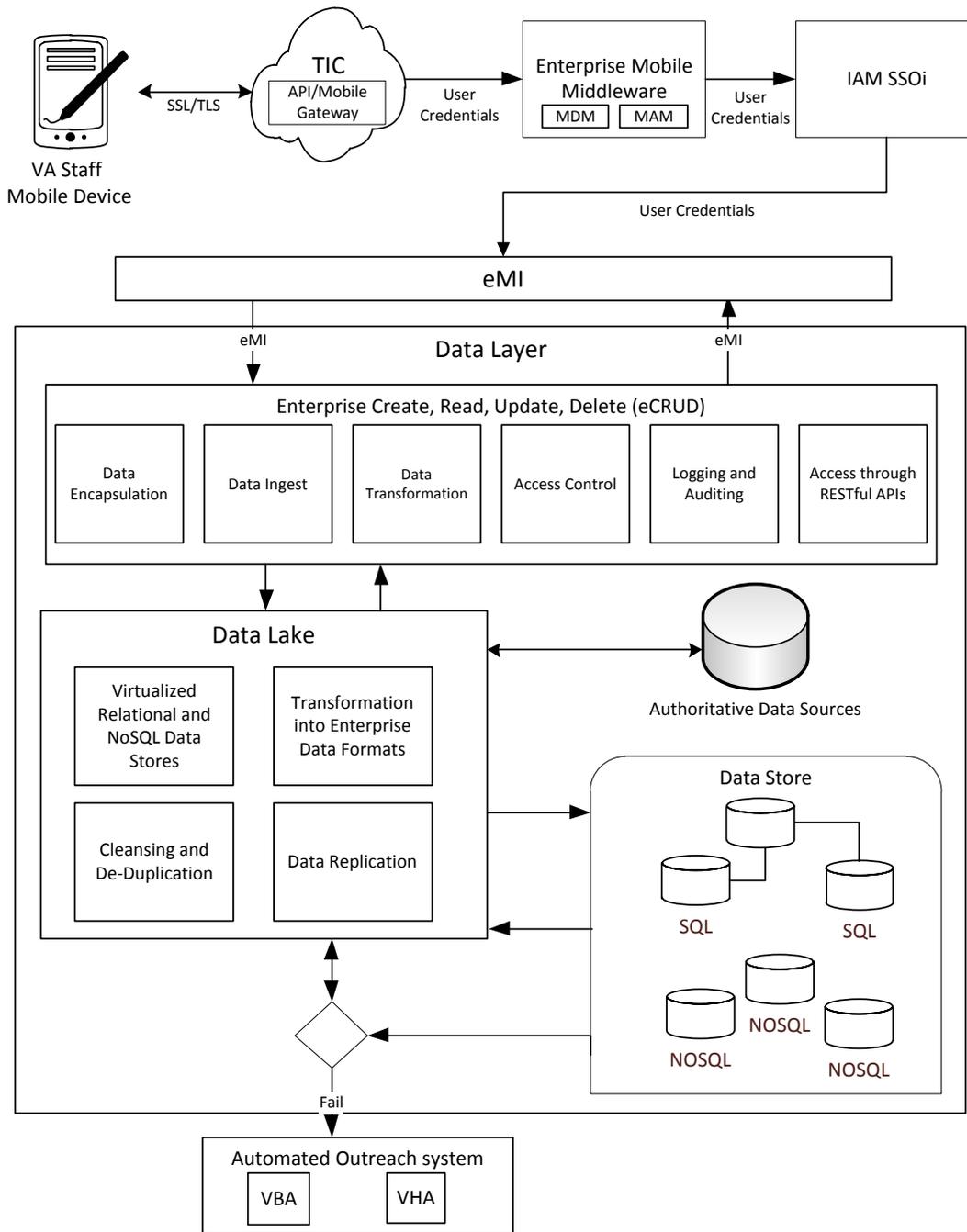


Figure 3 – Use Cases #1 and #2

Steps for Use Case #1

- 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 eMI
- 4) eMI provides the connection with shared services (e.g., email, messaging)
- 5) Information is retrieved and displayed on the mobile device

Steps for Use Case #2

- 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 eMI
- 4) eMI provides the connection 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 #3 per the Mobile Architecture Enterprise Design Pattern

Use Case	Use	Data Sensitivity
3. 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)

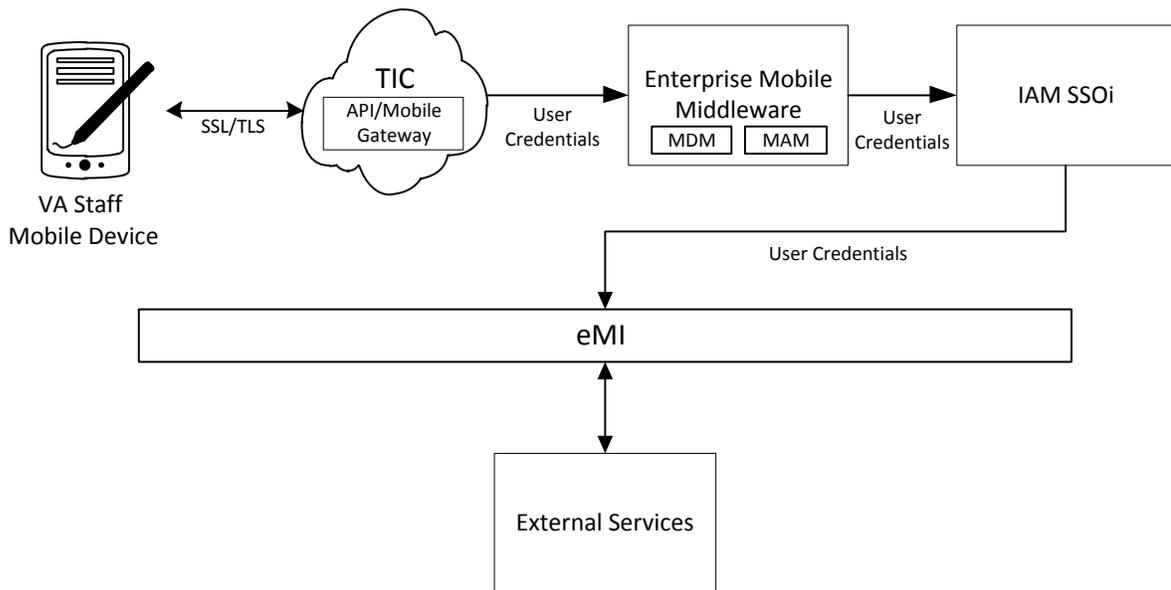


Figure 4 – Use Case #3

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 eMI
- 4) eMI provides access to the DoD medical system and other external services

Appendix A. DOCUMENT SCOPE

Scope

This Enterprise Design Pattern is a supporting guidance document of the overarching Mobile Architecture Enterprise Design Pattern with a focus on VA staff (including contractor personnel) use of mobile devices. This document provides an enterprise-level view of the “As-Is” and “To-Be” mobile capabilities relevant to Staff-Facing Mobile Devices and Applications and the standard processes in use. This document focuses on the guiding principles for establishing enterprise capabilities that enable staff-facing mobile devices and applications. These capabilities (e.g., MDM and MAM) address reoccurring challenges associated with VA staff using GFE mobile devices or their own personal mobile devices configured for VA use (BYOD). This document will serve as a starting point for establishing centralized policy for VA staff GFE mobile devices and BYOD applicable to all lines of businesses. The growing demand for accessing VA services and external systems relevant to VA (e.g. Defense Health Management System Modernization (DHMSM) in DoD) among VA staff on mobile devices makes standardization of staff-facing applications a priority.

Topics that are out of scope for this Enterprise Design Pattern, but may be referenced, are:

- Mobile applications used by Veterans
- Interactions between wearable devices that produce patient generated data
- Mobile security, including Single Sign-On (SSO)

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). Extensive input and participation was also received from VHA, VBA and NCA. 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.

Appendix B. DEFINITIONS

Table 3 – Definitions

Key Term	Definition
Enterprise Mobility Management	An all-encompassing approach to securing and enabling employee’s use of smartphones and tablets. Typically involves some combination of MDM, MAM, and data management.
Enterprise Shared Service	A SOA service that is visible across the enterprise and can be accessed by users across the enterprise, subject to appropriate security and privacy restrictions. http://vaww.ea.oit.va.gov/enterprise-shared-services-service-oriented-architecture/
Mobile Application Management	The delivery and administration of enterprise software to end users’ corporate and personal smartphones and tablets. It assists with software delivery, software licensing, configuration, application life cycle management and usage tracking.
Mobile Device Management	The administrative area dealing with deploying, securing, monitoring, integrating, and managing mobile devices, such as smartphones, tablets, and laptops in the workplace. It allows the distribution of applications, data and configuration settings and patches for such devices.
Service	A mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description.
Service Oriented Architecture	A paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations.

Appendix C. ACRONYMS

The following table, Table 4, provides a list of acronyms that are applicable to and used within this Enterprise Design Pattern document.

Table 4 – Acronyms

Acronym	Description
ACI	Administratively Confidential Information
AD	Active Directory
ASD	Architecture, Strategy and Design
BES	Blackberry Enterprise Server
BYOD	Bring Your Own Device
CAG	Citrix Access
DHMSM	Defense Health Management System Modernization
EHR	Electronic Health Record
eMI	Enterprise Messaging Infrastructure
EMM	Enterprise Mobility Management
ESS	Enterprise Shared Services
ETA	Enterprise Technical Architecture
ETSP	Enterprise Technology Strategic Plan
FIPS	Federal Information Processing Standards
FOUO	For Official Use Only
GFE	Government Furnished Equipment
IAM	Identity and Access Management
IoT	Internet of Things
IT	Information Technology
LOB	Line of Business
MAGB	Mobile Application Governance Board
MAM	Mobile Application Management
MAP	Mobile Application Program
MARA	Mobile Application Reference Architecture
MDM	Mobile Device Management
MVI	Master Veteran Index
NCA	National Cemetery Administration
NFC	Near Field Communication
OIS	Office of Information Security
OI&T	Office of Information and Technology
OMB	Office of Management & Budget
OTP	One-Time Password

Acronym	Description
PGD	Patient Generated Data
PHI	Protected Health Information
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
SAML	Security Assertion Markup Language
SDE	Service Delivery and Engineering
SDLC	Software Development Lifecycle
SOA	Service-Oriented Architecture
SPI	Sensitive Personal Information
SSL	Secure Socket Layer
SSO	Single Sign-On – SSOe/SSOi: External and Internal designations
TIC	Trusted Internet Connection
TLS	Transport Layer Security
TRM	Technical Reference Model
VAMF	VA Mobile Framework
VBA	Veteran Benefits Association
VDI	Virtual Desktop Infrastructure
VHA	Veteran Health Administration
VistA	Veterans Health Information Systems and Technology Architecture
VPN	Virtual Private Network
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 VA, and are aligned to the VA ETA:

Table 5 – References, Standards, and Policies

#	Issuing Agency	Applicable Reference/Standard	Purpose
1	VA OIS	VA 6500 Handbook	Directive from the OI&T OIS for establishment of an information security program in VA, which applies to all applications that leverage ESS.
2	CIO Council	Bring Your Own Device	A toolkit to support Federal Agencies implementing Bring Your Own Device (BYOD) programs
3	CIO Council	Mobile Security Reference Architecture	Provides detailed guidance on the use of enterprise mobile securities to ensure secure usage of mobile device and applications, applicable throughout the US Government
4	VA MAP	VA Mobile Framework System Design Document	Detailed specifications regarding the VAMF
5	NIST	NIST SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials	Defines guidelines for implementing derived PIV credentials
6	VA	https://vacloud.us/groups/ipobyodwikihomepage/	Information on VA's Mobile and BYOD Program