VA Enterprise Design Patterns
Mobility

Staff-Facing Mobile Devices and Applications Security

OFFICE OF TECHNOLOGY STRATEGIES (TS)
OFFICE OF INFORMATION AND TECHNOLOGY (OI&T)

VERSION 1.0
DATE ISSUED: JANUARY 2017

APPROVAL COORDINATION

Gary E. Marshall 137891

Digitally signed by Gary E. Marshall 137891
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=gary.marshall@va.gov, cn=Gary E. Marshall 137891
Date: 2017.02.22 15:17:40 -05'00'

Gary Marshall
Director, Technology Strategies, ASD

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.gov, cn=PAUL A. TIBBITS 116858
Reason: I am approving this document.
Date: 2017.02.22 15:42:18 -05'00'

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

REVISION HISTORY

Version	Date	Approver	Notes
1.0	January 26, 2017	Aaron Ibarra	Final version for TS leadership approval and signature, including all applicable updates addressing stakeholder feedback and Section 508 Compliance.

CONTENTS

1 Introduction 5
1.1 Business Problem 5
1.2 Business Need 5
1.3 Business Case 6
1.4 Approach 6
2 Current Capabilities 7
2.1 Enterprise Mobility Management Gaps 7
2.2 Authentication Gaps 8
2.3 Mobile Device Data Backup 9
3 Future Capabilities 9
3.1 Centralized Enterprise Mobility Management 9
3.1.1 Hybrid Model 9
3.1.2 Data Management 10
3.2 Biometric Authentication 10
3.2.1 Server-Side Biometric Data Storage 10
3.2.2 Match-on-Card Biometrics 11
3.3 Derived Personal Identity Verification (PIV) 11
3.4 Mobile Data Backup 13
3.5 Summary of Guidance Recommendations 15
3.6 Alignment to the One-VA Technical Reference Model (TRM) 16
3.7 Alignment to Veteran-Focused Integration Process (VIP) 16
4 Use Cases 17
4.1 Use Case #1, Derived PIV Authentication on GFE Mobile Device 17
4.1.1 Purpose 17
4.1.2 Assumptions 17
4.1.3 Use Case Description 17
4.2 Use Case #2, Mobile Device Data Backup 18
4.2.1 Purpose 18
4.2.2 Assumptions 18
4.2.3 Use Case Description 18
Appendix A. Scope 20
Appendix B. Definitions 22
Appendix C. Acronyms 23
Appendix D. References, Standards, and Policies 25

Table 1: Native Key Store Pros and Cons 12
Table 2: Third Party Key Store Pros and Cons 13
Table 3: EMM Integration Pros and Cons 13
Table 4: Guidance Summary 15
Table 5: List of Approved Tools and Standards for Staff-Facing Mobile Devices and Applications 16

Figure 1: Mobile Data Backup Decision Tree 14
Figure 2: Use Case #1 18
Figure 3: Use Case #2 19

QUICK JUMP

Select an icon to skip to a section.

Current Capabilities

Future Capabilities

Use Cases

One-VA Technical Reference Model

The Veteran-Focused Integration Process

Enterprise Design Pattern Scope

1 INTRODUCTION

1.1 Business Problem

The continued growth in the use of mobile devices and enterprise applications by staff and contractors brings new security challenges to the Department of Veterans Affairs (VA). As of 2015, VA issued over 40,000 smartphones as Government Furnished Equipment (GFE) to its staff; VA expects to issue an additional 70,000 mobile devices over the next two years.

The following VA mobile security challenges were identified as the result of the use of staff-facing mobile devices and applications:

- The use of multiple Enterprise Mobility Management (EMM) solution segments to manage and secure mobile GFEs
- Authentication gaps, such as the inability of Personal Identity Verification (PIV)-Only Authenticated (POA) users to use MobilePASS for remote Citrix Access Gateway (CAG) access
- Lack of mobile device data backup

1.2 Business Need

With continued growth in demand for mobile devices among VA staff, VA needs to evaluate and modernize its mobile ecosystem. The current state of staff-facing mobile devices and applications use reveals opportunities to enhance security and efficiency. EMM is a holistic

approach to securing and managing mobile devices; EMM typically includes some combination of Mobile Device Management (MDM), Mobile Application Management (MAM), and data management capabilities.

At VA, there are multiple MDM solutions to managing GFE mobile devices that increase the number of complexity and configuration management issues and subsequent security vulnerabilities. For instance, a recent Federal directive mandated that all Federal systems use multi-factor authentication; the directive required VA to take action to enhance security. To meet this directive, VA introduced MobilePASS, a One-Time Password (OTP) that is valid for only one login session. Consequently, OTPs are inconvenient and labor-intensive. And since OTPs remain valid for several minutes, they can be intercepted or observed.

1.3 Business Case

The potential for data loss and intrusion to the larger infrastructure from mobile device use presents some of the greatest security risks to enterprises. The risks associated with portable computing at VA are not exceptions. In light of the tremendous growth of mobile device and application use in recent years at VA, this Enterprise Design Pattern (EDP) will enhance security for the use of staff-facing mobile devices and applications by mapping the capabilities of VAs current and future states.

In the past, VA implemented solutions on an as-needed basis, without a centralized mobile strategy. This EDP, however, presents a mobility plan at VA that incorporates industry best practices to improve the overall security and end-user experience - in concert with VA's Mobile Architecture, Staff-Facing Mobile Devices and Applications, Veteran-Facing Mobile Applications, and Veteran-Facing Mobile Security Application EDPs.

1.4 Approach

The following steps define a near-term approach to enhancing the security and mobile infrastructure utilized to support VA staff-facing mobile devices and applications:

- Review the existing EMM tools
- Identify additional EMM capabilities required
- Review the One-VA Technical Reference Model (TRM) to search for a single EMM suite that provides the required capabilities; and if required, research EMM solutions not identified in the One-VA TRM
- Consolidate as many EMM tools into a single EMM suite while utilizing open standards to prevent vendor lock-in
- Develop a mobile device data backup plan

- Implement and incorporate new authentication capabilities in phases

2 CURRENT CAPABILITIES

A review of the current capabilities to manage and secure staff-facing mobile devices and applications revealed areas for improvement and capability gaps. Specific areas of focus included the existing EMM capabilities, authentication options to meet Two-Factor Authentication (2FA), and capabilities to backup data on GFE mobile devices.

2.1 Enterprise Mobility Management Gaps

Recently, VA established a mobile device security and management baseline for application to all GFE mobile devices.[1] The absence of a centralized cross platform EMM solution will challenge the goal of applying and maintaining this security and management baseline.

Currently, VA utilizes multiple MDMs to manage GFE mobile devices. *Blackberry Enterprise Server* (BES), a middleware program, is the legacy system that VA utilizes to manage all Blackberry GFE mobile devices. Simultaneously, VA utilizes VMware *AirWatch*, a provider of EMM software, to manage all other types of GFE mobile devices. VA also utilizes the Good Secure Collaboration Suite, now known as the BlackBerry Enterprise Mobility Suite, to allow staff to access corporate email from an array of operating systems; including the iPhone Operating System (iOS), Android, and Windows platforms. This diverse set of Commercial Off-The-Shelf (COTS) EMM tools raises the potential for configuration management issues whenever changes occur to the baseline security standards for 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 Virtual Private Network (VPN) profiles, VA Intranet, and Wi-Fi access. A centralized EMM that incorporates MDM capabilities can simplify the process of maintaining a security and management baseline.

Furthermore, VA currently does not have the ability to provide a Federal Information Processing Standard (FIPS) 140-2 vault for data to reside. VA requires FIPS 140-2 encryption for all data that requires encryption. Therefore, VA staff cannot store files and photographs that require encryption on a GFE mobile device.

[1] VA. (2015) Information Security Webinar Series – Mobile Device Security

2.2 Authentication Gaps

The Office of Management and Budget (OMB) Memorandum 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." VA implemented a 2FA solution in response to Memorandum M 11-11 directives and other Federal directives that mandate that all Federal systems use multi-factor authentication.

VA staff and contractors who use CAG to connect to the VA internal network must have a PIV card and Personal Identification Number (PIN) in order to comply with this directive. However, this is not feasible for most because their mobile devices are not PIV-enabled; this scenario resulted in the development of MobilePASS. MobilePASS provides 2FA for remote CAG users by generating an OTP. This method has proven inefficient for POA staff members who are unauthorized to use MobilePASS; therefore, they must utilize PIV card readers for direct use of PIV cards with their mobile devices. PIV card readers can interface with the mobile device over a wired or wireless interface. The use of wired PIV card readers is currently used sparingly, as it is a costly and inconvenient solution for VA staff.

Through the use of radio frequencies, Near Field Communication (NFC) can provide a wireless interface between a PIV card and a mobile device. VA does not, however, utilize this technology for a variety of reasons at this time. First, there is limited guidance from the National Institute of Standards and Technology (NIST) or the Defense Information Systems Agency's (DISA) Security Technical Implementation Guides (STIGs) for implementing the capability to use NFC to read PIV cards. Second, not all mobile device manufacturers have enabled their device's NFC capability to be available to third party developers.

Another limitation to MobilePASS is that it provides authentication for applications that are classified at Level of Assurance (LOA) 3, but not LOA 4. VA's Identity and Access Management (IAM) program offers a Single Sign-on Internal (SSOi) service for internal VA users. SSOi is the standardized enterprise-level authentication mechanism required for staff-facing system/application access at VA. However, in its current state, SSOi is not approved for use with LOA 4 applications; thus, there is no means to authenticate into a LOA 4 application with SSOi. For further information, refer to the User Identity Authentication EDP. Due to these constraints, VA needs to review newer methods of authentication, such as biometric authentication and derived PIV (Section 3), which offer enhanced security and a more usable authentication for VA staff.

2.3 Mobile Device Data Backup

Unlike data that is stored on GFE desktops and laptops, data stored on GFE mobile devices are not backed up. As additional GFE mobile devices, particularly tablets, are issued to VA staff, more content that is not backed up exists. These mobile devices are also more prone to loss and theft.

The current option for staff to back up data on GFE mobile devices is not automated; it requires a great deal of manual steps. Staff can utilize the smartphone manufacturer's encrypted backup software on their GFE desktop or laptop computer to back up their mobile device data using a traditional backup infrastructure. Cloud backup services, sync, and file sharing are not permitted by current VA security policies. Staff also has the option of transferring files manually between GFE mobile devices via internal email or *Airdrop* (iOS). *Airdrop* is a service within Apple Inc.'s operating system that utilizes Wi-Fi to transfer the data between the two devices; it requires both mobile devices to be in the vicinity of each other.

The lack of automation requires a number of manual steps to back up data, making it unlikely that backups are completed by staff with any regularity, or at all. Therefore, the data created on mobile devices is at greater risk of permanent loss.

3 FUTURE CAPABILITIES

3.1 Centralized Enterprise Mobility Management

As device management matures for desktop, mobile, and connected devices, VA can merge the management of devices into a single unified endpoint management system in accordance with the IT Service Management (ITSM) EDPs and VA 6500 Handbook guidance. EMM is a key component to securing and managing GFEs and Bring-Your-Own-Device (BYOD) mobile devices. EMM consists of many components for investment.

3.1.1 Hybrid Model

A flexible EMM will manage devices and their applications in an efficient manner. To this end, this EDP recommends a hybrid approach to ensure device-level encryption and application wrapping; the approach provides additional security and management features. VA should consolidate all mobile devices under the management of one MDM. Managing multiple MDMs for different operating systems raises the potential for configuration management issues and increases complexity. In addition, application wrapping allows a mobile application

management administrator to set specific policy elements that can be applied to an application or group of applications. These policy elements can include such decisions as whether a user authentication is required for a specific app or if data associated with the app can be stored on the device.

3.1.2 Data Management

A data management security strategy will need to keep data encrypted, while only allowing approved applications to access and transmit data. GFE mobile devices will utilize encrypted containers that meet FIPS Publication 140-2 standards to protect data at rest. BYOD mobile devices do not have data stored in the device, so the issue is avoided. Both GFE and BYOD mobile devices need data encryption during transmission that also meets FIPS 140-2 encryption standards. VA follows guidance from OMB Memorandum M-04-04 and NIST Special Publication 800-63-2 to rate all existing mobile applications and categorize them to the appropriate LOA. Every staff-facing mobile application will perform a risk assessment to determine the minimum LOA, in accordance with the User Identity Authentication EDP.

3.2 Biometric Authentication

With the continued introduction of biometric reading capabilities of smart phones (e.g., fingerprint, voice pattern, iris scanning, facial recognition), biometrics can be used as authentication factors. Multiple authenticators in a layered approach can ensure a higher level of security. This approach would apply individual policies to a particular user, and layer those policies to ensure that authentication is completed as securely and conveniently as possible. For example, the user would pass a series of biometric tests, such as an eye scan, facial recognition, and a fingerprint analysis, before a determination is made to permit access to the network. Biometric authentication offers several advantages, such as the inability to access the mobile device if it is lost or stolen. There is no need to remember passwords or PIN numbers. There is no duplication of biometric identifiers because each individual has their own unique biometric features. It is also important to be flexible in determining the best biometric capability for a particular application. There is not always a biometric modality that is best suited for all conditions and implementations. Many factors must be considered when implementing a biometric device, including location, security, acceptability, and usability.

3.2.1 Server-Side Biometric Data Storage

In traditional biometric systems, users are prompted to create “identity templates,” which take an individual’s biometric data (fingerprints, eye veins or retina, etc.) and store them on a central server. This identity template is then used to cross-reference and validate a user’s identity when that user is authenticating into the network. Storing biometric data on the server

provides a fast computation time for comparing data and validating or rejecting a user, while also providing flexibility in running a rich variety of algorithms. Additional benefits include a higher random access memory (RAM) capacity, which is important for certain algorithms to access when verifying a user. While server-side storage has its benefits, there are also some concerns and risks. For example, if the user is traveling for work purposes and unable to connect to the server, the user has no way of authenticating into the network. Additionally, if biometric data on the server is compromised, that credential cannot be canceled because it is uniquely specific to the user.

3.2.2 Match-on-Card Biometrics

Match-on-card technology consolidates biometrics with smart cards. This enables users to carry their biometric data with them and match it on the card. The user executes the biometric scan in the same way as the traditional approach, only this time the reader extracts information from the biometric image in the form of minutiae points; those points are then bundled into data packets and sent to the card for matching. The card then executes a comparison algorithm and produces a score that reveals the similarities between the biometric image sent to the card and the one stored on the card; it then renders a decision. The fundamental difference between the match-on-card process and the traditional biometric process is that the match-on-card identity template is locked on the smart card and does not require internet connection or a back-end database to authenticate the user. Because match-on-card locks the data in the chip, lost or stolen cards pose minimal risks. Additionally, the biometric is never stored on a backend database, eliminating the risk of compromise at this level.

Although the match-on-card process addresses certain issues faced by the traditional server-side approach, there are still key differences that can favor the biometric approach, such as processing power and speed. Since the processing power on the card is far less than that of a server, the speed to establish the identity is reduced. Servers operate 10-to-100 times faster than a smart card. Also, from a role-based access control (RBAC) perspective, there is no central authority to dictate permissions. Match-on-card would verify the person is who they say they are, but without tapping into a central authority, such as IAM's SSO service, it would not be able to say whether the person was allowed to be there. A card would be able to hold permissions, but it cannot revoke the information. Another challenge is that once the card architecture and algorithm have been designed and manufactured, there is no easy way to change or upgrade that architecture.

3.3 Derived Personal Identity Verification (PIV)

Derived PIV credentials leverage the identity proofing and vetting results of the current and valid PIV credentials of VA staff. This saves VA time and effort by using existing valid PIV cards

to generate a separate Derived PIV credential. Derived PIV credentials are stored on the GFE mobile device as either a software certificate, such as a software token, or on a hardware component that is removable or embedded within the GFE mobile device, such as hardware token.

The LOA required for the systems and applications that the staff access through their GFE mobile device will determine which type of token is needed. Software tokens provide LOA 3 security, while hardware-based tokens provide LOA 4 security. Staff with a need for LOA 3 system and application access should be able to apply for a Derived PIV remotely through a self-enrollment and management portal. This not only reduces the burden on the help desk and badging offices, but it makes the process quick and simple for users. Hardware tokens will require in-person issuance as ID proofing and biometric data needs to be collected. In addition, no mobile devices on the market can support LOA 4 credentials without a third party adapter that has FIPS Publication 140-2 level 2 cryptographic modules. VA should monitor the developments of mobile device manufacturers, as many are moving towards supporting LOA 4 credentials and it will be easier and less costly to support LOA 4 credentials on GFE mobile devices. Until then, it is recommended that staff utilize a PIV card reader to avoid extra complexity of a third party adapter.

An important consideration for software tokens is where to store the Derived PIV certificate on the GFE mobile device. The three possible storage options for the software token include the native key store, the third party key store, and EMM integration. Each option offers a different set of advantages and challenges, as described below.

TABLE 1: NATIVE KEY STORE PROS AND CONS

Pros	Cons
Public Key Infrastructure (PKI) authentication to native applications of mobile devices (e.g., email, contacts, calendar, web browser)	No additional security for the Derived PIV certificate other than phone unlock security measures only some MDM applications can leverage the native key store
	No third party applications managed by the MDM can utilize the native key store
	Private key is made available to applications
	No automated key services (e.g., key history recovery, certificate renewal)

TABLE 2: THIRD PARTY KEY STORE PROS AND CONS

Pros	Cons
Applications never see the Derived PIV certificate, so it cannot be stolen	Added layer of complexity over native key store
Multiple levels of security provide greater security to keys compared to native key stores	
Encryption key history recovery is automatic and synchronized with all PIV cards possessed by the owner	
Automatic certificate renewal prior to expiration	

TABLE 3: EMM INTEGRATION PROS AND CONS

Pros	Cons
PKI based authentication for native MDM applications (e.g., email, web browser, VPN, File Share)	Added layer of complexity over native key store
Third party applications protected by MDM can use PKI authentication	
MDM protection and control of mobile devices	

3.4 Mobile Data Backup

Unlike the desktop computers issued by VA, GFE mobile devices do not have their data backed up. To back up and protect the valuable data generated from mobile devices, decision makers need to weigh the impact of several considerations. The first consideration is the efficiency of the backup. The following diagram depicts a decision tree that lists the options available.

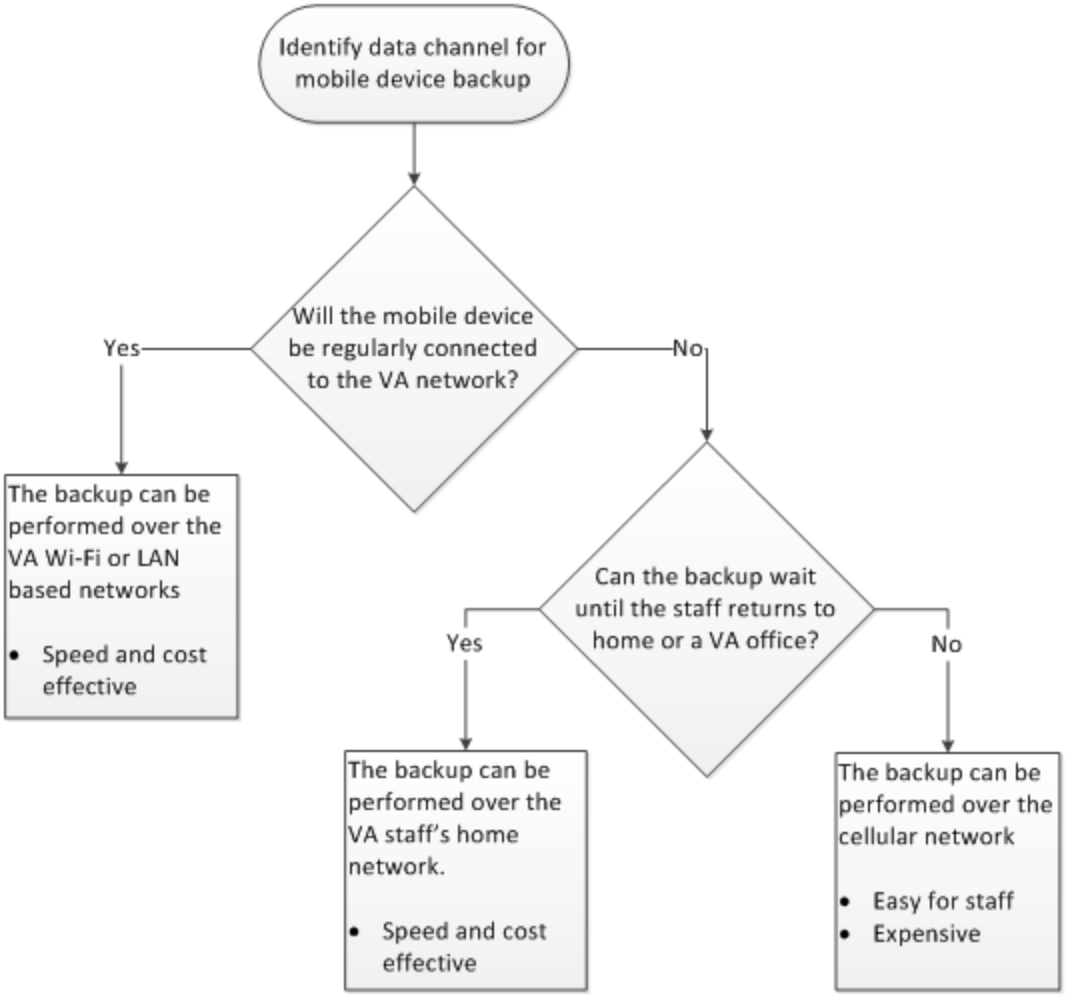

FIGURE 1: MOBILE DATA BACKUP DECISION TREE

The next set of criteria to consider includes data retention, data encryption, and data discovery. Data retention must adhere to federal guidelines. A minimum record retention period for registration data is:[2]

- For LOA 2 and 3, seven years and six months beyond the expiration;
- And for LOA 4, ten years and six months beyond the expiration.

For backed up encrypted data, the backup system must also save its associated keys for the life span of the data. In addition, the backup system staff must store key management structure to maintain key correlation to the data. VA needs to consider data discovery for information that is backed up and how it fits within VA's data integration efforts, including adoption of standards

[2] NIST. (2011) Electronic Authentication Guidelines

for Semantic Web Technology. The Enterprise Data Analytics EDP describes the current and planned future state for VA's business intelligence and data analytics capabilities.

Finally, VA needs to consider where to store all of this data, whether through a public cloud or internal storage. Data temperature takes into consideration latency, volume, item size, request rate, and durability of the data and is useful in deciding what type of data storage to use. The Data Storage EDP discusses data temperature in-depth. Public cloud storage providers have become so efficient at such low costs, that individual organizations cannot match. For these reasons, this EDP recommends that cold data is stored in a public cloud, while hot and warm data can utilize VA internal storage.

Currently, EMM solutions do not offer multi-platform mobile device backup capabilities, so VA should utilize a separate mobile device backup solution. However, VA should continue to monitor this area, as EMM suites continue to expand their capabilities including data backup.

3.5 Summary of Guidance Recommendations

The following table provides a summary of the near term and long term security and capabilities guidance for staff-facing mobile devices and applications.

TABLE 4: GUIDANCE SUMMARY

Guidance Summary
Near Term Guidance
Centralized EMM solution that includes MDM, MAM, and data management
Implementation of new authentication factors to achieve 2FA ▪ Biometrics and/or ▪ Derived PIV o Self-enrollment and management portal of software tokens for LOA 3 security access o Hardware tokens issued for LOA 4 security access
Development of a mobile device backup plan
Provide a data backup capability for GFE mobile devices
Long Term Guidance
Adoption of a unified endpoint management solution of desktops, laptops, mobile devices, Internet of Things (IoT) devices, etc.
Monitor the trend of NFC as a viable and secure PIV reader option for mobile devices in the Federal sector

3.6 Alignment to the One-VA Technical Reference Model (TRM)

All projects will leverage the approved tools and standards located in the One-VA TRM[3] to comply with the architectural guidance provided in this document. Table 5 lists the approved tools for this EDP. This document establishes the technical standards that inform the decisions about mobile technologies that are included in the One-VA TRM. Future updates of this EDP will reflect forecasted standards and subsequent changes in approved products in the One-VA TRM.

TABLE 5: LIST OF APPROVED TOOLS AND STANDARDS FOR STAFF-FACING MOBILE DEVICES AND APPLICATIONS

Category	Example Approved Tools and Standards
Application Development Tools	HP Fortify Runtime
Enterprise Service Bus (ESB)	IBM WebSphere
E-mail and Calendaring	BES, Good For Enterprise
Data in Motion	Health Level 7 Clinical Document Architecture (CDA)
Wireless Networks	Wi-Fi Protected Access (WPA)
Authentication	MobilePASS
Encryption	Transport Layer Security (TLS) Protocol
Mobile Device Management	Airwatch MDM, BlackBerry Enterprise Server

3.7 Alignment to Veteran-Focused Integration Process (VIP)

All mobile solutions that are subject to the Veteran-Focused Integration Process (VIP) will use approved products from the One-VA TRM; following VIP guidelines, all mobile devices will leverage the approved EMM solution. VIP is a Lean-Agile framework that unifies and streamlines information technology (IT) delivery oversight; VIP will deliver IT products more efficiently, securely, and predictably. VIP is the follow-on framework from Project Management Accountability System (PMAS) for the development and management of IT projects. VIP will propel the Department with even more rigor toward Veteran-focused delivery of IT capabilities.

More information can be found here (https://vaww.oit.va.gov/veteran-focused-integration-process-vip-guide/).

[3] http://trm.oit.va.gov/

4 USE CASES

4.1 Use Case #1, Derived PIV Authentication on GFE Mobile Device

4.1.1 Purpose

This use case describes the high level architecture in a scenario where a VA employee uses his or her GFE mobile device to access a 3rd party application that requires LOA 3 credentials.

4.1.2 Assumptions

- The user has a valid Derived PIV credential in the form of a software token
- The VA selects an enterprise wide 3rd party key store that is used for the storage of the Derived PIV credential on the GFE mobile devices
- An MDM solution manages the GFE mobile device
- The user utilizes a 3rd party application that is protected by the MDM to access VA enterprise data that requires LOA 3 credentials

4.1.3 Use Case Description

The high level architecture for Use Case #1 is displayed in the figure below. The steps for the Derived PIV use case are as follows:

1. A VA employee enters their PIN to accesses the 3rd party application
2. The container holding the Derived PIV credential (i.e., certificate) is unlocked by the system with the verification of the PIN
3. The user credential is transmitted across a TLS connection through a Trusted Internet Connection (TIC) to the Enterprise Mobile Middleware
4. The user credentials are forwarded to the IAM service
5. Certificate-based authentication is done via IAM's SSOi
6. Once the user is authenticated the 3rd party application that is protected by the MDM will interact with the Enterprise Messaging Infrastructure (eMI)
7. The eMI provides a connection with the ESS which in turn accesses the VA data layer
8. The GFE mobile device displays the information

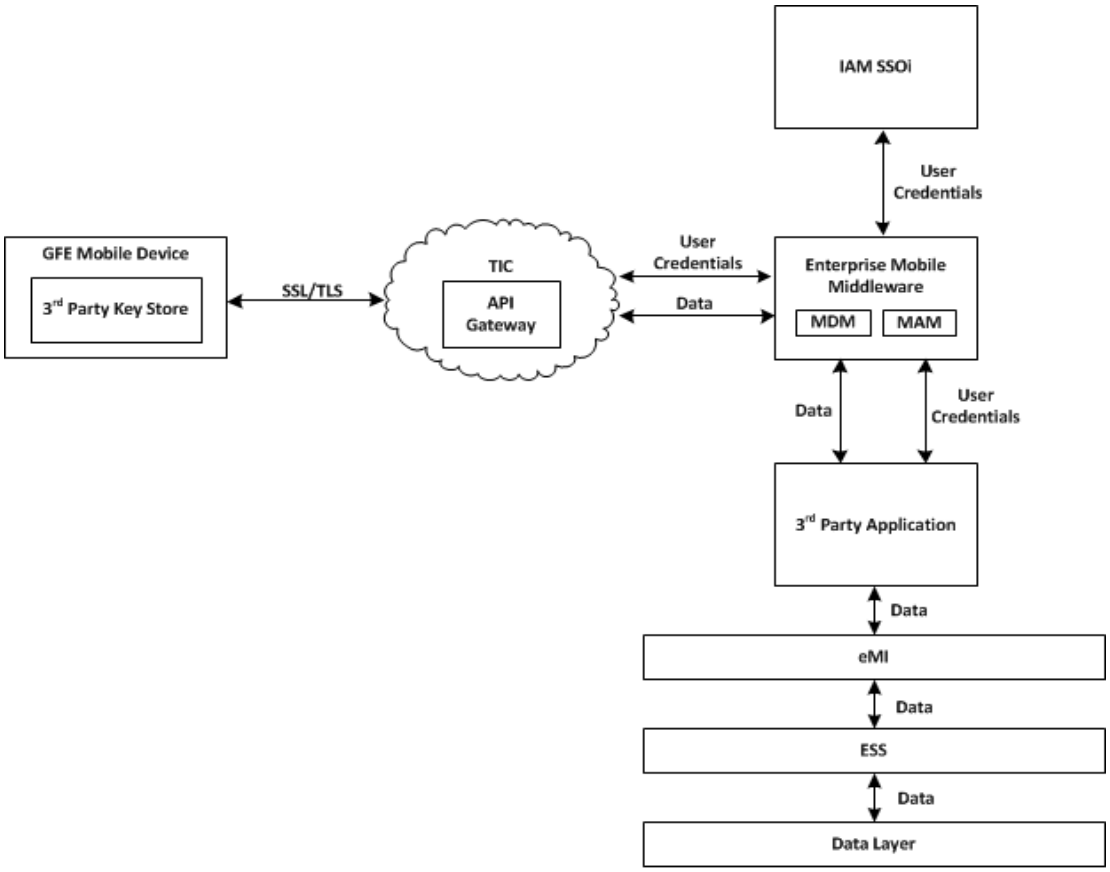

FIGURE 2: USE CASE #1

4.2 Use Case #2, Mobile Device Data Backup

4.2.1 Purpose

This use case describes the high level architecture in a scenario where a VA employee backs up a GFE mobile device in a VA hospital.

4.2.2 Assumptions

- The GFE mobile device has a mobile device backup client installed
- The GFE mobile device user has valid credentials
- The VA employee is located in a VA hospital and has an established Wi-Fi connection to the VA network

4.2.3 Use Case Description

The figure below displays the high level architecture for Use Case #2.

1. The backup client initiates a scheduled backup of the data on the GFE mobile device

2. The data is routed through the Enterprise Mobile Middleware
3. The Enterprise Mobile Middleware interacts with the eMI
4. The eMI provides a connection with the ESS which in turn accesses the VA data layer
5. The VA Analytic Ecosystem ingests the data from the VA data layer and will determine data temperature and whether data should be stored within VA internal storage or external cloud storage[4]

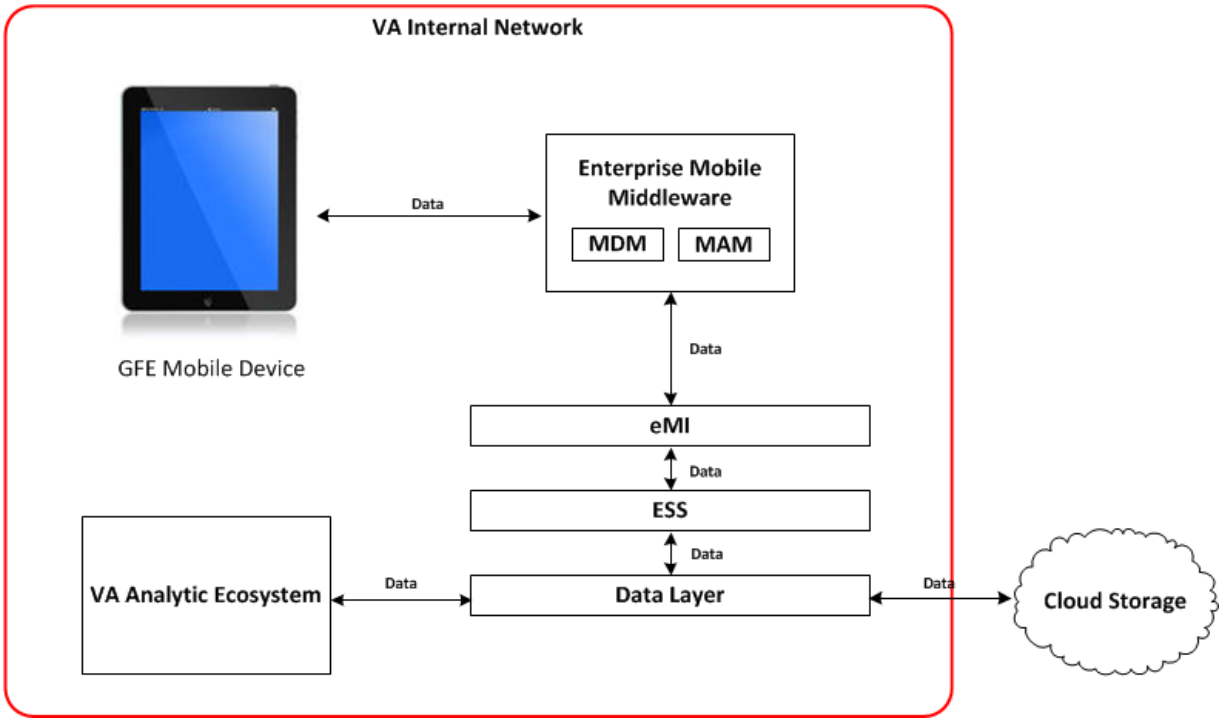

FIGURE 3: USE CASE #2

[4] VA (2015) Interoperability and Data Sharing Design Pattern Enterprise Data Analytics

APPENDIX A. SCOPE

The Staff-Facing Mobile Devices and Applications Security EDP focuses on best practices for enterprise security on GFE issued devices and staff-facing applications.

This document will cover:

- Mobile security best practices in alignment with the Government Mobile and Wireless Security Baseline
- New authentication factors to achieve two-factor authentication
- Mobile device data backup

Topics outside the scope of this EDP but are covered in other EDPs are:

- Veteran-Facing Application Security
- Bring Your Own Device
- Mobile governance processes
- IoT Devices

Intended Audience

This document is meant for use by all project teams that are developing new applications that are deployed into production within the VA's IT infrastructure. These applications are device-independent and encompass the acquisition of COTS software (including open-source solutions) to meet data sharing requirements. They utilize message-level security standards that are provided by enterprise messaging middleware to make calls to Enterprise Shared Services (ESS).

Document Development and Maintenance

The Staff-Facing Mobile Devices and Application Security EDP team developed this EDP collaboratively with internal stakeholders from across the Department, including participants from VA's Office of Information and Technology (OI&T), Enterprise Program Management Office (EPMO), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE). The Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and the National Cemetery Administration (NCA) contributed extensive input and participation. 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 in order to track all changes. The EDP team will coordinate updates with the Government Lead for this

document and will also facilitate stakeholder coordination and subsequent re-approval, depending on the significance of the changes.

APPENDIX B. DEFINITIONS

This appendix provides definitions for terms used in this document, particularly those related to databases, database management, and data integration.

Key Term	Definition
Derived PIV	A derived PIV is a new credential (a digital certificate) stored on a mobile device that is derived from the trust of a valid PIV card.
Enterprise Shared Service	A Service Oriented Architecture (SOA) service that is visible across the enterprise and can be accessed by users across the enterprise, subject to appropriate security and privacy restrictions.
Secure Socket Layer (SSL)	A standard security technology for establishing an encrypted links between a server and a client—typically a web server (website) and a browser; or a mail server and a mail client (e.g., Outlook).
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 (SOA)	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
Transport Layer Security (TLS)	A protocol that ensures privacy between communicating applications and their users on the Internet

APPENDIX C. ACRONYMS

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

Acronym	Description
2FA	Two-Factor Authentication
ASD	Architecture, Strategy and Design
BES	Blackberry Enterprise Server
BYOD	Bring Your Own Device
CAG	Citrix Access Gateway
CDA	Clinical Document Architecture
COTS	Commercial Off-the-Shelf
DISA	Defense Information Systems Agency
EDP	Enterprise Design Pattern
eMI	Enterprise Messaging Infrastructure
EMM	Enterprise Mobility Management
EPMO	Enterprise Program Management Office
eMI	Enterprise Messaging Infrastructure
ESB	Enterprise Service Bus
ESS	Enterprise Shared Services
FIPS	Federal Information Processing Standard
GFE	Government Furnished Equipment
IAM	Identity and Access Management
iOS	iPhone Operating System
IoT	Internet of Things
IT	Information Technology
ITSM	IT Service Management
LOA	Level of Assurance
MAM	Mobile Application Management
MDM	Mobile Device Management
NCA	National Cemetery Administration
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
OI&T	Office of Information and Technology
OIS	Office of Information Security
OMB	Office of Management and Budget
OTP	One-Time Password
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PMAS	Project Management Accountability System

Acronym	Description
POA	PIV-Only Authenticated
RAM	Random Access Memory
SDE	Service Delivery and Engineering
SOA	Service Oriented Architecture
SSL	Secure Socket Layer
SSOi	Single Sign-on Internal
STIGs	Security Technical Implementation Guides
TIC	Trusted Internet Connection
TLS	Transport Layer Security
TRM	One-VA Technical Reference Model
VA	Department of Veterans Affairs
VBA	Veterans Benefits Administration
VHA	Veterans Health Administration
VIP	Veteran-Focused Integration Process
VPN	Virtual Private Network
WPA	Wi-Fi Protected Access

APPENDIX D. REFERENCES, STANDARDS, AND POLICIES

This EDP 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 Enterprise Technical Architecture (ETA):

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
1	OMB	M-04-04 "E-Authentication Guidance for Federal Agencies"	Description of Level of Assurance for Federal agencies.
2	NIST	NIST Special Publication 800-157	Guidelines for Derived Personal Identity Verification (PIV) Credentials
3	NIST	NIST Special Publication 800-63-1	Electronic Authentication Guideline
4	CIO Council	Government Mobile and Wireless Security Baseline	Baseline of standard security requirements for mobile computing issued by the Federal CIO

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