VA Enterprise Design Pattern:

1.0 Authentication, Authorization, and Audit

1.4 Mobile Veteran Facing Application Security

Office of Technology Strategies (TS)

Architecture, Strategy, and Design (ASD)

Office of Information and Technology (OI&T)

Version 1.0

Date Issued: November 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.gov, cn=TIMOTHY L MCGRAIL 111224
Date: 2015.11.23 13:59:32 -05'00'

Date: _____

Tim McGrail
Sr. 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.gov, cn=PAUL A. TIBBITS 116858
Reason: I am approving this document.
Date: 2015.12.03 12:55:58 -05'00'

Date: _____

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

REVISION HISTORY

Version Number	Date	Organization	Notes
0.1	3/11/2015	ASD TS	Initial Draft
0.2	4/6/2015	ASD TS	Delivered draft to vendors
0.3	5/6/2015	ASD TS	Incorporated best practices gleaned from vendor engagements.
0.4	5/12/2015	ASD TS	Incorporated further analysis of the issues and root cause analysis. Gap analysis of Federal guidelines for mobile security.
0.5	5/15/2015	ASD TS	Addressed feedback from Government Lead
0.6	5/20/2015	ASD TS	Incorporated O&M issue to problem statement and added further information on MDWS issue
0.7	5/22/2015	ASD TS	Incorporated stakeholder feedback
0.8	6/2/2015	ASD TS	Incorporate stakeholder feedback
1.0	6/22/2015	ASD TS	Incorporate formal staffing feedback

REVISION HISTORY APPROVALS

Version	Date	Approver	Role
0.1	3/11/2015	Nicholas Bogden	ASD TS Design Pattern Government Lead
0.2	4/6/2015	Nicholas Bogden	ASD TS Design Pattern Government Lead
0.3	5/6/2015	Nicholas Bogden	ASD TS Design Pattern Government Lead
0.4	5/12/2015	Nicholas Bogden	ASD TS Design Pattern Government Lead
0.5	5/15/2015	Nicholas Bogden	ASD TS Design Pattern Government Lead

0.6	5/20/2015	Nicholas Bogden	ASD TS Design Pattern Government Lead
0.7	5/22/2015	Nicholas Bogden	ASD TS Design Pattern Government Lead
0.8	5/22/2015	Nicholas Bogden	ASD TS Design Pattern Government Lead
1.0	6/22/2015	Nicholas Bogden	ASD TS Design Pattern Government Lead
1.0	November 2015	Tim McGrail	ASD TS Final Design Pattern Review

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Problem

Secretary Robert A. MacDonald observed in his 2014 MyVA Presentation that "Assessments informing the [2014-2020] strategic plan told us the VA often provides a fragmented, disjointed experience that results in poor customer service and frustrated Veterans and beneficiaries." The following issues stem from the current state of mobile security for Veteran Facing Mobile Applications. These issues will severely impact the Veteran's user experience if not addressed.

1. Limited enterprise security guidance for leveraging Enterprise Shared Services (ESS) within VA's IT infrastructure, currently there are no enterprise security policies for Mobile Veteran Facing Applications.
2. Lack of standardized methods to protect Veteran Protected Health Information (PHI) and Personally Identifiable Information (PII) data residing on the mobile device (i.e. data at rest) and data in transit, currently there are no enterprise security policies for Mobile Veteran Facing Applications.
3. Lack of a Single Sign On (SSO) capability for Veterans using public-facing mobile applications. The Identity and Access Management (IAM) services for SSOe were recently implemented. Existing mobile applications are lacking SSO capability.
4. Limited availability of enterprise capabilities to protect the VA IT infrastructure from unsecure mobile applications. The Mobile Applications Governance Board (MAGB) has been suspended with VHA releasing the majority of application development under the Connected Health Board. There is no centralized oversight of mobile applications development.
5. Once Mobile Veteran Facing Applications are released there is a three-month support period after which they become the responsibility of the business owner. There are no plans for operations and maintenance (O&M) of applications beyond the sustainment period which could lead to security vulnerabilities being.

1.2 Business Case

Implementing the mobile security guidelines established in this document for Veteran Facing Mobile Applications will allow VA to meet the Federal security guidelines established for mobile and wireless security. These guidelines provide the following benefits:

- Allows Veterans to enter their authentication credentials once and gain access to all Veteran Facing applications requiring authentication on a mobile device

- Provide protection to any Veteran PHI/PII data residing on the Veteran's mobile device beyond the mobile device's native security (if activated)
- Veteran Facing Mobile Applications have gone through standardized development and testing, reducing the risk of unsecured applications being deployed.
- Secures existing mobile applications without modifications
- Allows VA developers to focus on the Veteran's needs when building new applications instead of implementing security capabilities provided by containerization technologies, increasing cost savings to VA

2 CURRENT CAPABILITIES AND LIMITATIONS

2.1 VA Mobile Infrastructure

The VA Mobile Framework (VAMF) provides the infrastructure and common services to allow mobile applications to access the VA infrastructure and provide services for the Veteran. The following diagram depicts the VAMF Logical Architecture.

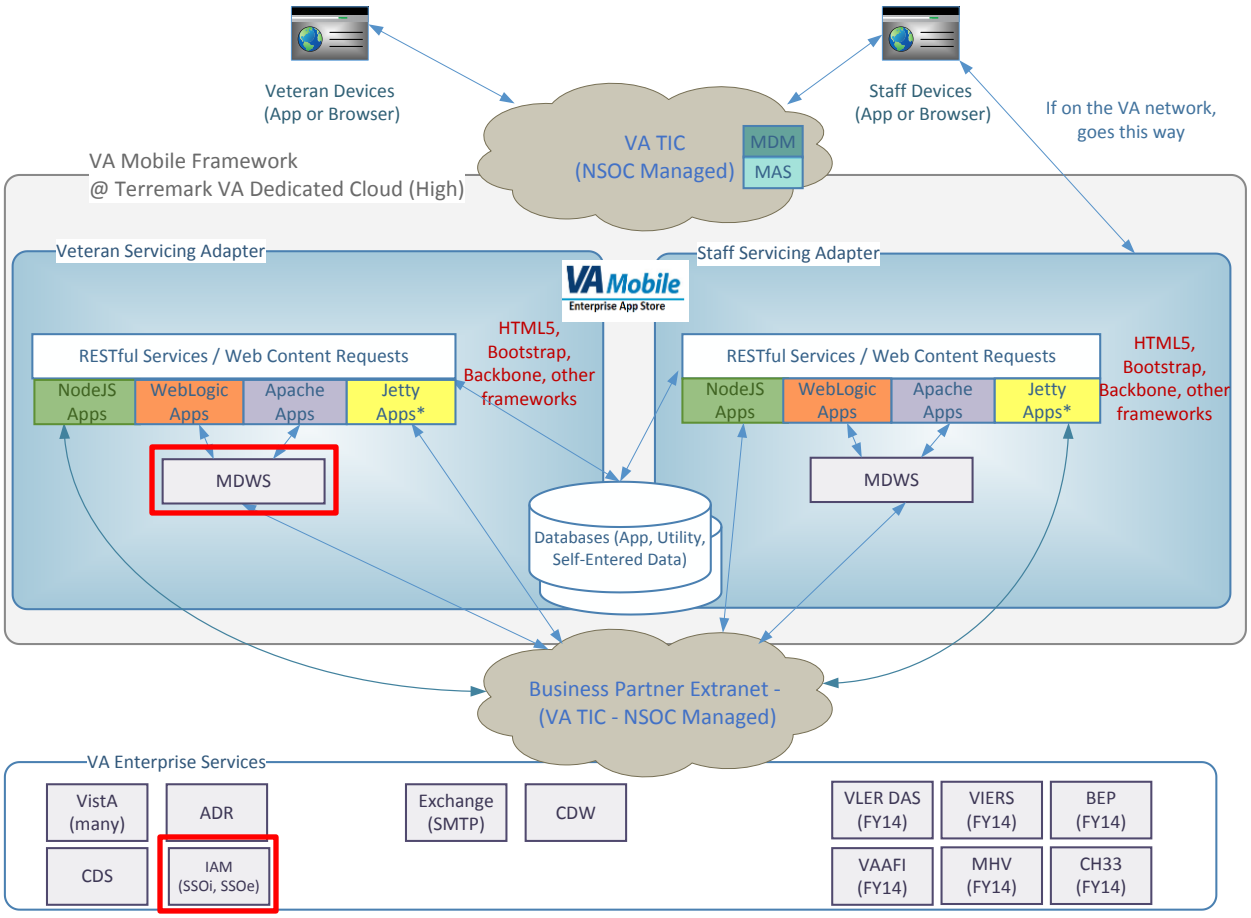

Figure 1: VAMF Logical Architecture

Transport Layer Security (TLS) is the preferred protocol used by VAMF to provide privacy and data integrity of information to other devices/applications. During the handshake between VAMF and clients, they will negotiate (sending the version of SSL/TLS and cipher suites supported) and use the most secure communication that both support. The VAMF supports TLS 1.0, 1.1, and 1.2. The VAMF is able to accept EXtensible Markup Language (XML) or JSON (JavaScript Object Notation) as a method of data transfer to Veteran mobile devices.

2.2 Medical Domain Web Services (MDWS)

Systems/services highlighted in red in Figure 1 indicate areas having security ramifications from a non-staff external user perspective that need to be addressed. VAMF allows using system accounts through Medical Domain Web Services (MDWS) in violation of NIST and HIPAA requirements. These system accounts are used to represent human triggered system interactions from external 'consuming applications' to VA systems. There is no ability to track the specific system/individual accessing PII/PHI data. The Veterans Health Information Systems and Technology Architecture (VistA) office has provided guidance requiring all new applications are not allowed to use MDWS to access VistA. The Vista Access Enhancements (VAE) project is addressing this issue. As part of the interim solution, five major consumers of VistA systems will migrate from MDWS to VistA Integration Adapter (VIA). VistA will undergo kernel modifications to enable accurate recording and of new and existing users of remote systems/applications integrating with VistA. This topic is covered in the Non-Person Entity (NPE) Enterprise Design Pattern. The IAM SSOe service was recently completed providing a single sign on capability for external users of mobile devices. New Veteran Facing applications requiring access to the VA network will authenticate using this service.

2.3 VA Mobile Framework (VAMF)/Identity and Access Management (IAM) Integration

Within the VA Mobile Application Store for Veterans are two main types of applications –secure access to PII/PHI information and unsecure informational applications. All users may access applications not involving PII/PHI data. Single Sign-On External (SSOe) via Identity and Access Management's (IAM) is required for applications involving PII/PHI. IAM SSOe accepts Federal Identity, Credentialing, and Access Management (FICAM) approved government and commercial credentials.

The VAMF provides a set of common services for mobile applications called the HealthAdapter. The HealthAdapter protects these services by requiring users to authenticate using DoD Self-Service Logon (DS Logon) credentials when operating in "Veteran" mode (Veteran Environment). Authenticating and identifying the user is accomplished using DS Logon as an authentication provider and IAM's SSOe service offering to establish the session between the user and the HealthAdapter. The HealthAdapter is a middle-tier-component designed to

provide easy-to-consume, resource-oriented services when developing health care applications. IAM SSOe supports multiple authentication providers. For "Veteran" mode, DS Logon will be used as the authentication provider/user credentials.

DS Logon, by policy, does not allow credentials to use a proxy through another system. Veterans cannot enter their credentials into the mobile application directly, nor can the credentials be sent to the HealthAdapter and then forwarded to DS Logon. This approach augments the IAM SSOe offerings ensuring a mobile application and the HealthAdapter are never provided direct access to the credentials.

For further information regarding the HealthAdapter please refer to https://wiki.mobilehealth.va.gov/display/vaha3/Veteran+Authentication+and+Identification.

3 FUTURE CAPABILITIES TO ADDRESS LIMITATIONS

The Government Mobile and Wireless Security Baseline, a Digital Government Strategy (DGS) deliverable, was released by the Federal CIO Council and the Department of Homeland Security (DHS). This baseline is used to assist Federal Departments and Agencies (D/As) in the secure implementation of mobile solutions through agency enterprise architectures. Four key areas identified to “accelerate the secure adoption of mobile technologies into the Federal environment” are Mobile Device Management (MDM), Mobile Application Management (MAM), Identity and Access Management (IAM), and Data Management. The VA Enterprise System Engineering (ESE) office determined MDM was too intrusive for Veteran-owned devices, not used for non-staff devices and is beyond the scope of this document. The remaining three areas are outlined below and describe how Mobile Veteran Facing Applications address these areas.

3.1 Mobile Application Management (MAM)

Containerization solutions allow the enterprise to provide fine-grained application-level controls. Separating the Veteran’s personal data from VA applications and data is an industry best practice. Containerization allows VA data accessed by these applications to remain segregated from personal data regardless of the device on which mobile applications are being used.

There are two approaches to incorporating containerized mobile application security into Mobile Facing Veteran Applications. The first approach and preferred method is to use application wrapping. Application wrapping allows developers to secure their applications without additional development work. Existing applications can be secured by being wrapped without any modification to the code. This approach is quick and provides limited impact to current and future Veteran Facing Applications.

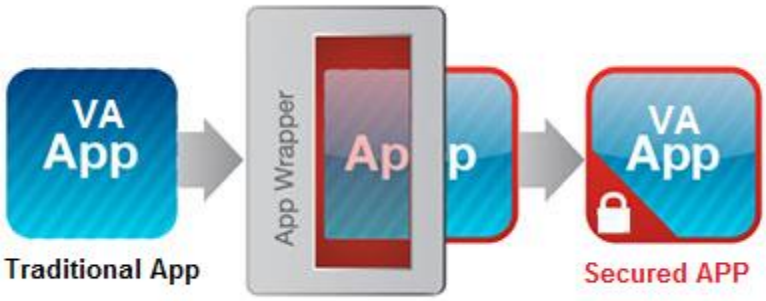

Figure 2: Application Wrapping

Code integration is the second approach where developers use customized application programming interfaces (APIs) and/or software development kits (SDKs). This approach provides advanced functionality not possible by application wrapping (e.g. secure inter-application communication, etc.). This approach should only be used when application wrapping does not provide the necessary capabilities.

The VA's Web and Mobile Solutions (WMS) Team manages a Mobile Application Development Life Cycle that includes: planning, development, compliance, preproduction simulation, Initial Operating Capability (IOC) field testing, release, and sustainment. Further information on the Mobile Application Development Life Cycle can be found here. Updates can come on a monthly basis, but take a minimum of three months to be released, due to the processes the development, security, operations, and compliance teams currently use. Agile methodologies will facilitate more frequent deliveries.

A key aspect to addressing unsecure software is maintaining existing applications. An application management policy to ensure applications are up-to-date must be employed and incorporated into a mobile applications O&M plan. Additionally the use of application whitelisting (only allowing installation of mobile applications from an authorized enterprise app store) will further protect the Veteran from downloading malicious and or vulnerable applications. Veterans can download VA branded applications from the VA App Store and other sources including the Apple App Store and Android App Store. VA needs to ensure all VA branded applications have gone through the VA's Mobile Application Development Life Cycle. VA must also develop a process for vetting mobile applications to check for vulnerabilities and malware, and digitally sign applications that have been approved through the Mobile Application Development Life Cycle.

Mobile Veteran Facing Application Problems Addressed: #1, #2, #4, #5

3.1.1 Security Policies

For the security of the VA enterprise, the ability to perform compliance monitoring on Veteran's mobile devices is mandatory. This compliance monitoring encompasses operating system versions and jail broken/root detection. There must be the capability to respond when there is a compliance issue or if a device has been reported lost or stolen by remote locking, and/or wiping (only the containerized segment) the Veteran's mobile device. Application wrapping provides the capability to perform a remote wipe of the wrapped application and/or the data contained within the application. The Veteran will not lose any data residing outside of the application.

Mobile Veteran Facing Application Problems Addressed: #1, #2

3.2 Identity and Access Management (IAM)

Mobile Veteran Facing Applications will be designed to leverage IAM's SSOe authentication framework. This framework will allow these applications to use FICAM certified Identity Providers (IdP[1]) or Credential Service Providers (CSPs) approved by VA. This will eliminate the need for applications to support application-issued credentials. SSOe has solutions supporting both native client and HTML. IAM solutions are designed to work in environments using SOAP and REST based architecture. They will work with project teams to identify and provide solutions.

3.2.1 VA Secure Mobile User Identity Authentication to VA Resources

Figure 3 depicts the "To-Be" Veteran Secure Mobile Authentication, reflecting the consolidated Single Sign-on approach VA is implementing. This approach allows application designers to perform a single integration with IAM SSOe, avoiding the need to integrate with many different CSPs. This allows external users to authenticate once to VA and gain access to multiple resources.

[1] List of IdPs can be found at: http://www.idmanagement.gov/approved-identity-services

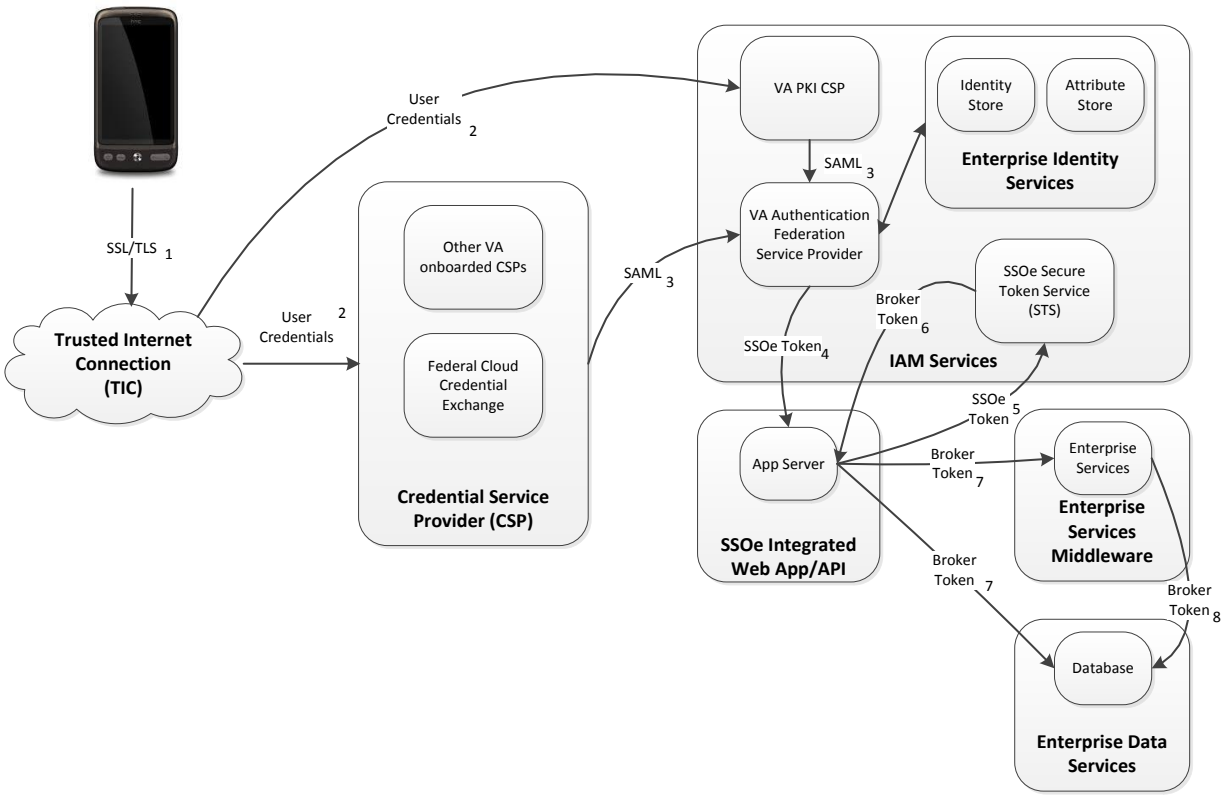

Figure 3: To- Be Veteran Secure Mobile Authentication Design Pattern

The IAM SSOe platform is integrated with a number of CSPs, either externally or internally managed. The CSPs provide identity assertions in the form of SAML tokens to the VA Authentication Federation Service Provider within the SSOe infrastructure. Once received by the Federation Service Provider, the token is validated and the service provider brokers the connection from the user to the application. User information is passed to SSOe integrated applications in HTTP headers, called SSOe Tokens in the diagram above.

Detailed architecture for SSOe infrastructure is provided in the Identity and Access Management VA Authentication Federation Infrastructure (VAAFI) System Design Document.

3.2.2 Application Integration with SSOe

The design of the SSOe Infrastructure requires application owners to integrate once with the SSOe to enable the full suite of authentication services. This simplifies application design, allowing applications to take advantage of SSOe capabilities. By allowing SSOe to manage the authentication process, application security is assured through the adoption of a common enterprise approved authentication standard. The use of SSOe Services by applications allows external users to obtain VA services with a variety of existing credentials and credential service providers (CSP). This reduces the need for VA to maintain a diverse set of user stores

supporting individual applications. In alignment with policies of federated CSPs, credentials are not stored on the Veteran's mobile device.

Additional information is provided in the AA&A Design Pattern: External User Authentication document.

Mobile Veteran Facing Application Problems Addressed: #1, #3

3.3 Data Management

There are two aspects to data management:

1. The categorization and tagging of data to enable information sharing and safeguarding
2. Encrypting sensitive information (e.g. PII/PHI) stored on a mobile device and transmitted across unsecured networks to protect against unauthorized access or disclosure.

VA follows guidance from OMB 04-04 and NIST SP 800-63-2 to rate all existing mobile applications and categorize them to the appropriate Levels of Assurance (LOA). Every mobile application will perform a risk assessment to determine the minimum LOA. While there are no standard rules encompassing all data sets, the following provides general guidance for application developers. LOA1 allows for submission of forms or data and return status to verify a user submitted data. LOA2 allows users access to their own PII/PHI data VA has about them. All LOA2 applications must integrate with VA's IAM SSOe for authentication. This information is further detailed in the AA&A External User Authentication Design Pattern.

Application level encryption must be utilized so the container does not rely on the native device's encryption or on the developer writing to native encryption APIs. This encryption provides strong protection against data leaks between Veteran personal data and VA applications and data. Data at rest is protected within the encrypted container. The data will be encrypted during transmission from the enterprise, to the Veteran's mobile device. This encryption level will is required to meet Federal Information Processing Standard (FIPS) 140-2 certified cryptography per VA HandBook 6500.

Mobile Veteran Facing Application Problems Addressed: #1, #2

The security recommendations highlighted in this design pattern are referenced in the Government Mobile and Wireless Security Baseline and Mobile Security Reference Architecture (MSRA) documents issued by the DGS. To secure Mobile Facing Veteran Applications, developers will focus on the containerization, application management, IAM, and data management issues described in Section 3.

3.4 HTML5 Applications

HTML 5 based web applications will be used for informational Veteran Facing applications and not transactional ones. As a result HTML 5 based applications will follow the same security protocols as VA websites utilizing SSL/TLS.

3.5 Technical Reference Model (TRM)

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

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

To view the full range of technologies provided by the TRM, please visit the following link: http://www.va.gov/TRM/ReportVACategoryMapping.asp

3.6 Summary of Security Strategy

The following is a summary of the strategy for Mobile Veteran Facing Applications:

- Containerization must be performed via application wrapping when possible otherwise code integration is to be used whenever application wrapping does not provide the required functionality
- Security policy compliance monitoring with ability to remote lock and/or wipe the device
- Application management policy to keep Veteran Facing application up-to-date

- Central VA Application Store with digitally signed applications
- All Veteran Facing applications must authenticate using IAM's SSOe service
- All Veteran Facing applications must perform a risk assessment to determine their minimum LOA
- Application level encryption must meet FIPS 140-2 standards

4 USE CASE

The Veteran Facing Application Security use cases demonstrate how a Veteran's application will work with the SOA architecture, enterprise shared services and the VA enterprise architecture.

Use Case	Use	Data Sensitivity	Security Aspects
Veteran accesses, creates, or modifies personal non-public data	Veteran/caregiver accessing medical and patient data using a mobile device for medication and related care information, preventative care. This could also be a Veteran accessing CH 33 or other non-health benefits Right information at the right time for the proper care.	VA Sensitive Data (SPI)/Personal Health Information (PHI) Administratively Confidential Information (ACI) (aka. PGD/IAM–DS/Logon/SSOe/Oauth)	Authentication: SSOe Authorization: Role Based Access Control (RBAC) Data Transport: TLS

Use Case # 1

User Experience: Veteran makes a single change securely and is updated across all VA systems

- A Veteran initiates a change of address through a mobile application to reflect the Veteran's move from the Washington, DC area to the San Francisco, CA area.
- The Veteran can login using existing credentials established on VA systems or using an external approved Credential Service Provider.
- Veteran's token is validated and the CSP brokers the connection between the Veteran and the application.
- In the brokered connection, user information is passed to SSOe integrated applications in HTTP headers, called SSOe Tokens.

- A data message is sent from the application through authoritative information services to the data layer.
- The message is processed by the Enterprise Create, Read, Update, Delete (eCRUD) service, which writes the address change to the data lake and to the ADS for Veteran addresses

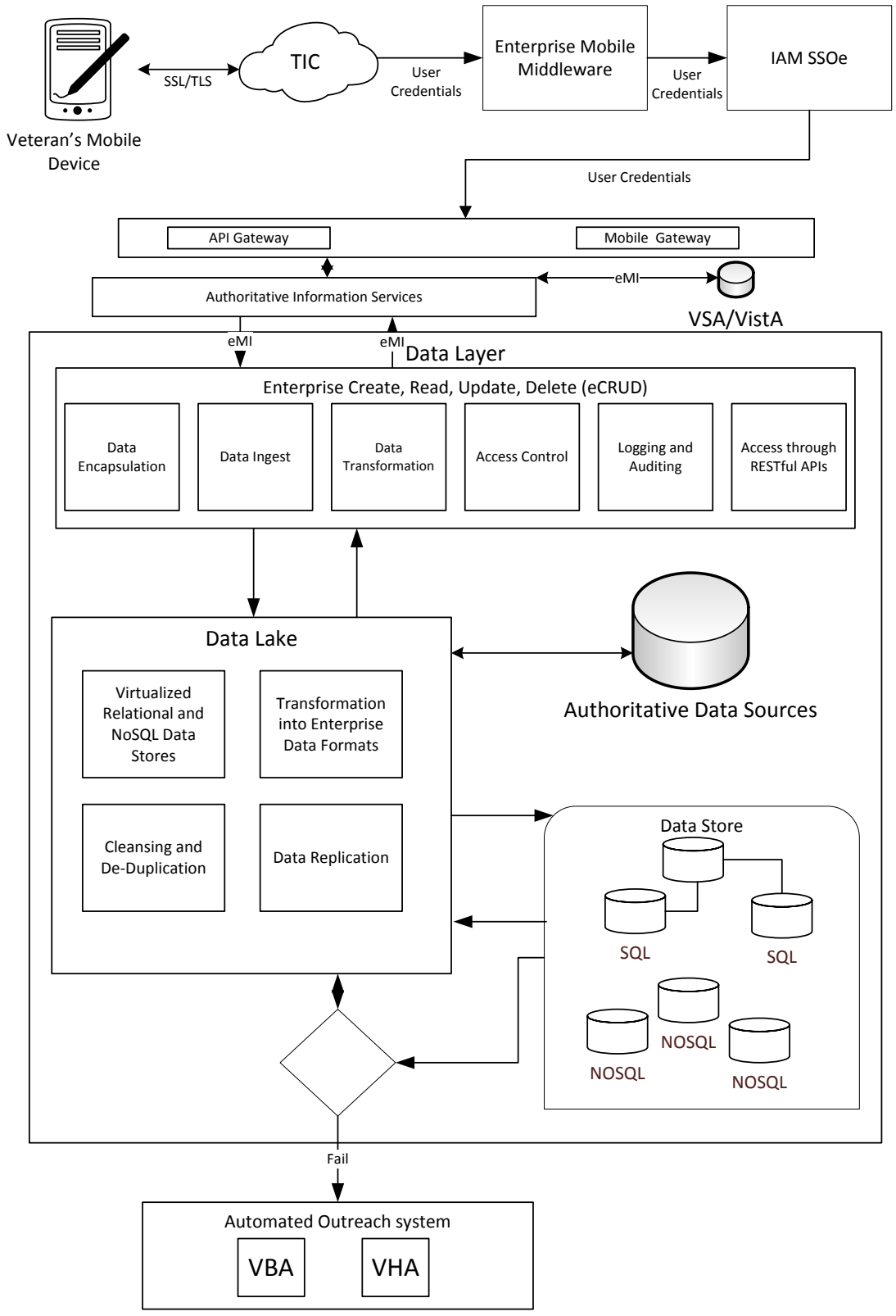

Figure 4: Use Case #1 - Veteran updates address

Use Case # 2

User Experience: Veteran accesses a single application to access all critical information pertinent to the Veteran. Veteran securely logs on using credentials previously established on an existing VA system.

- A Veteran accesses his or her medical prescription and then looks for benefits information through a mobile application
- The Veteran can login using existing credentials established on VA systems or using an external approved Credential Service Provider.
- Veteran's token is validated and the CSP brokers the connection between the Veteran and the application.
- In the brokered connection, user information is passed to SSOe integrated applications in HTTP headers, called SSOe Tokens.
- Veteran selects option to view list of his or her prescriptions. Applications calls on authoritative information services to access VistA for prescription records associated with Veteran's VHA patient ID. Veteran can now view the information.
- Veteran now selects an option to view current benefits. Application calls on shared services to retrieve Veteran's benefit information. Information is displayed on the mobile device

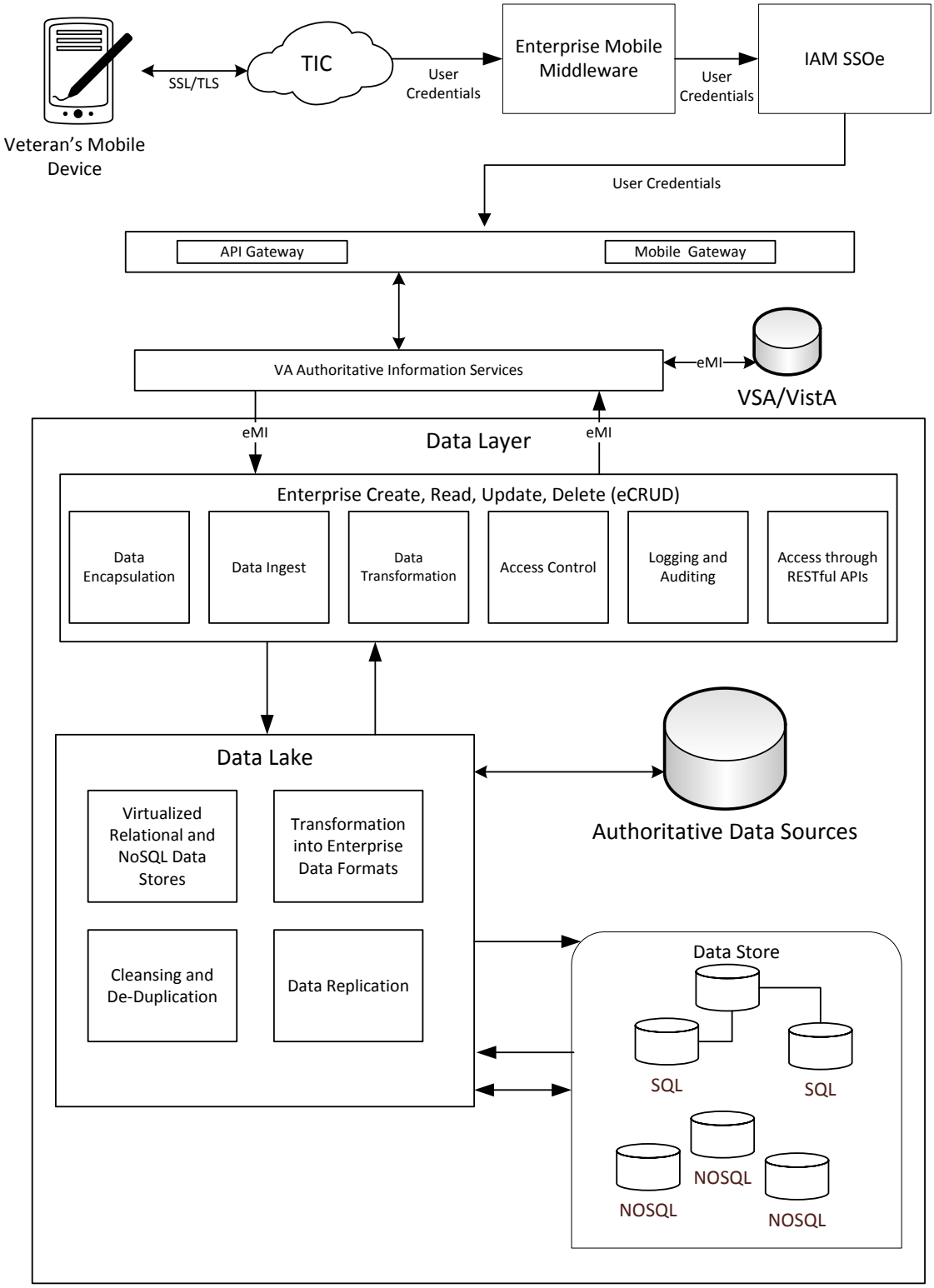

Figure 5: Use Case #2 - Veteran access data across Lines of Business

Appendix A. SCOPE

Purpose

The Enterprise Mobile Veteran Facing Application Security Design Pattern document provides enterprise-level capability guidance that identifies security best practices for Veteran-facing mobile applications accessing VA IT resources. It is meant to be limited enough to be usable and broad enough to be reusable as a formalized approach for Veteran-facing mobile application projects that leverage enterprise security capabilities. This document and the corresponding Mobile Veteran Facing Application Design Pattern will guide projects to implementation resources that will support detailed design specifications.

Scope

The Veteran Facing Mobile Applications considered in this Design Pattern are device agnostic, and will be able to perform on a wide variety of mobile devices that are commonly used by Veterans.

This document will cover:

- Best practices to achieve mobile security based on the Government Mobile and Wireless Security Baseline
- Security methods to protect PHI and PII data residing on the Veteran's mobile device
- Preventing data leakage between VA Veteran data and Veteran personal data on the Veteran's mobile device
- Methods to protect the VA IT infrastructure
- Utilizing the VA's IAM Single Sign On External (SSOe) service to authenticate to the VA network

The following content is beyond the scope of this document, but may be referenced in appropriate locations to guide further technical planning:

- Securing mobile applications used by anyone other than Veterans and their beneficiaries
- Securing interactions between wearable devices that produce patient generated data
- Non-Person Entity (NPE) authentication of external users, this is covered in the NPE Design Pattern

Intended Audience

The Design Pattern is meant to be used by VA Integrated Project Teams (IPTs) that have mobile Veteran Facing requirements, or are provisioning mobile Veteran Facing applications.

Document Development and Maintenance

This document was developed collaboratively with stakeholders from offices throughout VA, including 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). The effort included engagements with industry experts to review, provide input, and comment on this Enterprise Design Pattern. This document contains a revision history and revision approval logs. Updates will be coordinated with the Government lead for this document, who will also facilitate stakeholder engagements and subsequent re-approval.

Appendix B. DEFINITIONS

Key Term	Definition
Application Wrapping	Applying additional security features, such as encryption, to a mobile application or group of applications to add layers of protection to mobile application(s) requiring additional security.
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 Device	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.
Personally Identifiable Information (PII)	Any information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Information does not have to be retrieved by any specific individual or unique identifier (i.e., covered by the Privacy Act) to be PII.

Key Term	Definition
Protected Health Information (PHI)	Individually identifiable health information held by a covered entity or by a business associate acting on its behalf. PHI excludes education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g, records described at 20 U.S.C. §§ 1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer. Within VA, VHA is the only covered entity. Certain other VA components, such as OI&T, are business associates of VHA.
Sensitive Personal Information (SPI)	The term, with respect to an individual, means any information about the individual maintained by VA, including the following: (i) education, financial transactions, medical history, and criminal or employment history; (ii) information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records.
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.

Appendix C. ACRONYMS

Acronym	Description
ASD	Architecture, Strategy and Design
DHS	Department of Homeland Security
DoD	Department of Defense
eMI	Enterprise Messaging Infrastructure
ESB	Enterprise Service Bus
IPT	Integrated Product Team
MARA	Mobile Application Reference Architecture
MDM	Mobile Device Management
NIST	National Institute of Standards and Technology
OI&T	Office of Information and Technology
PD	Product Development
PHI	Protected Health Information
PII	Personally Identifiable Information
SDE	Service Delivery and Engineering
TRM	Technical Reference Model
VA	Veterans Affairs
XML	Extensible Markup Language

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:

#	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 the VA, which applies to all applications that leverage ESS.
2	CIO Council	Government Mobile and Wireless Security Baseline	Provides a baseline of standard security requirements for mobile computing
4	CIO Council	Mobile Security Reference Architecture	Provides guidance to Federal agencies implementing mobile security
5	VA MAP	VA Mobile Framework System Design Document	