



## Enterprise Design Patterns: Mobile Veteran-Facing Application Security

### What are Enterprise Design Patterns?

Reusable templates that guide the enterprise to implement a set of technologies in standard ways

### How do Enterprise Design Patterns relate to the Enterprise?

Enterprise Design Patterns translate OI&T's strategic goals, as documented in the Enterprise Technology Strategic Plan (ETSP), into "real world" direction to guide system design

### How can I learn more?

To learn more about Mobile Enterprise Design Patterns, contact Nicholas Bogden  
([Nicholas.bogden@va.gov](mailto:Nicholas.bogden@va.gov))

To read the full document, see the TS website:  
[www.techstrategies.oit.va.gov](http://www.techstrategies.oit.va.gov)

To ask questions about Enterprise Design Patterns in general, reach out to  
[AskTS@va.gov](mailto:AskTS@va.gov)

- **Enterprise Design Pattern Scope:** The Enterprise Mobile Veteran-Facing Application Security Enterprise 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.
- **Current State:** 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
- **Design Pattern Solution:** 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