Enterprise Design Pattern: Secure Messaging (Authentication, Authorization & Audit)

- **Secure Messaging Defined:** An approach to ensure messages can traverse the network in a manner that provides authentication, authorization, message confidentiality, and message integrity.

- **Current State:** The VA is deploying new applications that consume services cutting across the traditional lines of business (LOB). A set of standards need to be developed between the LOBs to prevent interoperability issues. Current guidance for secure messaging within VA is limited and will lead to data sharing risks if not updated.

- **Design Pattern Solution:** To implement the standards and protocols required for message-level security.

This document expounds on the message-level security standards needed to integrate the enterprise IT infrastructure and Enterprise Shared Services (ESS).

It outlines the capabilities and standards achievable through the use of enterprise middleware solutions such as Enterprise Messaging Infrastructure (eMI) and XML/API Gateways. This guidance applies to SOAP message exchanges with systems internal and external to VA.

**Current VA guidance for secure messaging requires the use of Point to Point Encryption (P2PE) methods including TLS/SSL.**

There are significant limitations to managing P2PE security for systems that require multiple system hops. VA’s existing common web services security framework does not account for multi-hop messaging. The move towards a SOA based enterprise infrastructure requires enhancements to VA’s message-level security policies. VA must develop guidance on establishing proof of origin of messages, and building a SOA web services trust framework.

VA applications that integrate with enterprise resources must adhere to the following constraints:

- Use of message-level security for service-to-service communication.
- Adherence to WS-Security and associated specifications (e.g. WS-SecureConversation, WS-Trust, WS-Policy) for SOAP-based messages.
- Use of XML security standards including XML signatures and XML encryption. Integration with VA enterprise middleware and IAM, while also leveraging the use of API gateways.
- Adherence to NIST SP 800-95 guidelines.

In order to avoid security risks, the document describes the common set of standards used to protect web service messages, and refers to implementation guidance associated with the eMI.