

VA ENTERPRISE DESIGN PATTERNS PRIVACY AND SECURITY SECURE MESSAGING



Office of Technology Strategies (TS)
Office of Information and Technology (OI&T)

Version 2.0
Date Issued: September 2016

EXECUTIVE SUMMARY

Scope

Current systems at the Department of Veterans Affairs (VA) cannot ensure full end-to-end security, and therefore compromise the security and privacy of sensitive Veteran data. Hypertext Transfer Protocol Secure (HTTPS), now required for all VA websites, uses transport-level security. Transport-level security only ensures security for point-to-point connections; messages are only protected in transit. Therefore, security ends at intermediary points in the Information Technology (IT) infrastructure; messages become unencrypted at these locations. Attackers can intercept unencrypted messages or alter a user's identity credentials as it traverses the network.

Business Need

At present, VA guidance for secure messaging requires the use of transport-level security, which provides only point-to-point security, using methods that include transport layer security (TLS). With significant limitations to managing point-to-point security for systems that require multiple system hops, communication is only secure at the transport level and not the message level. Once the message reaches an intermediary hop, it is no longer secure. VA's common web services security framework does not account for multi-hop messaging. The move towards a SOA-based enterprise infrastructure requires the addition of message-level security. VA will develop guidance on establishing proof of origin of messages, and building a SOA web services trust framework.

Approach

The following steps define a near-term path toward strengthening the security of messages traveling within the VA network. This is particularly relevant for existing production systems that cannot guarantee end-to-end transport security. In the long run, VA will adopt cloud services that enable end-to-end transport security (both for data at rest and data in transit). Cloud services will include built-in functionality to support message-level security. Steps include: Gain agreement on standards for incorporating message-level security to VA; Review the existing capabilities of the API gateway incorporated into eMI; Determine whether this API gateway can be extended to an enterprise wide API gateway or if we need to introduce one to the VA network; And incorporate the enterprise-wide API gateway that includes all required capabilities.

[Enterprise Design Patterns](#) (EDPs) are developed by TS in coordination with internal and external subject matter experts and stakeholders. An EDP is a reusable capability guidance document that identifies best practice approaches and resources for achieving VA IT strategic objectives. The EDP Team uses industry trends and innovations; enterprise architectural standards; and guiding principles for capabilities and constraints to improve efficiency and effectiveness and define solutions to reoccurring technical problems. The EDP helps guide the design of IT systems and services by VA project teams.