

# TRANSITIONING TO SECURE WEB-BASED STANDARDS AND PROTOCOLS

Dr. Elizabeth A. McDaniel, Dr. William R. Simpson,  
Coimbatore S. Chandersekaran and Dr. Kevin E. Foltz

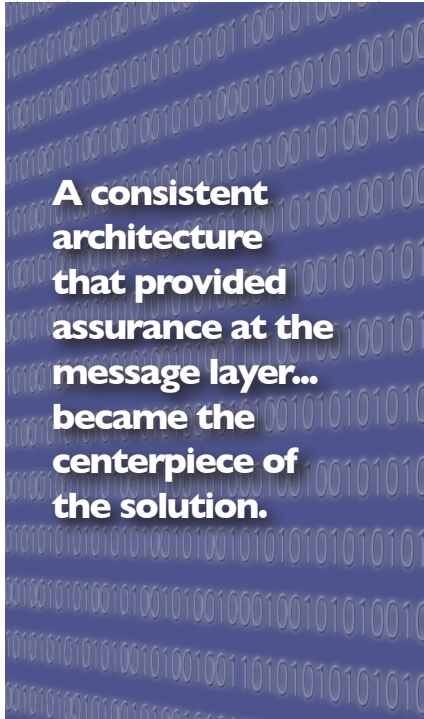
## The Problem

Across DoD, non-standard IT arrangements and complexities grew with every new system and application. For example, in response to many procurement solicitations, vendors implemented their own security and communications solutions. As a consequence DoD organizations have thousands of systems with unique characteristics and vulnerabilities. The complexities of a myriad customized systems and applications - with often repeated data and information saved on local servers and computers - make information sharing difficult and expensive, and reveal uneven security policies and practices that add to enterprise vulnerabilities.

## Our Approach to the Problem

IDA researchers are completing foundational work required to accomplish goals set in the DoD Information Enterprise Strategic Plan released in May 2010.<sup>1</sup> This has included designing and building a high assurance web-based approach to content sharing and information security. The research team designed a pilot system based on the evolving web service model that fosters net-centricity and information sharing, allows access from many devices, desktop and mobile, and conserves valuable DoD IT resources. The pilot solves the problems of interoperability and enterprise-wide security through the use of standard interfaces and protocols that guarantee interoperability and make the management of capabilities much simpler. The IDA team is currently collaborating with the Defense Information Systems Agency (DISA) and the Air Force on a pilot test in the Defense Enterprise Computing Centers.

In response to DoD CIO guidance, the Air Force Chief Information Officer committed to creating a web-based, net-centric solution. The challenge was to build a single consistent, net-centric information assurance architecture to support the key related elements of the DoD strategic plan, including integration of warfighter network and command and control



**A consistent architecture that provided assurance at the message layer... became the centerpiece of the solution.**

<sup>1</sup> Goal 1 in the plan is a “robust DoD Information Enterprise [that] provides the Department and mission partners access to discoverable, authoritative, relevant, trusted, and actionable information and services to enable effective and agile decisions for mission success.” Goal 2 calls for a “balanced suite of DoD Enterprise Services [to] be visible, accessible, understandable and trusted, enabling net-centric information sharing via a service-oriented information enterprise.” Goal 4 proposes a “unified and resilient DoD Information Enterprise where only authorized users (including mission partners) have ready access to their information; missions continue under any cybersecurity situation; and associated components perform as expected and act effectively in their own defense.”

---

capabilities, improving situational awareness, and optimizing transport of authoritative secure information. A consistent architecture that provided assurance at the message layer - using a claims-based paradigm for security based on Public Key Infrastructure and Security Assertion Markup Language-based authorization - became the centerpiece of the solution. The layered architecture in the pilot system takes advantage of greater usability, vendor flexibility through industry standards, and greater opportunity to improve or modify the overall implementation while allowing for legacy operations during adaptations to new approaches.

The system is designed to protect five primary security aspects of information: confidentiality, integrity, availability, authenticity, and non-repudiation. Design principles, for example extensibility and information hiding, are supplemented by security mechanisms, including strong two-way authentication using DoD Public Key Infrastructure. The layered architecture is critical to the security approach.

## Implications of the Research

Web-enabled information - made discoverable and accessible using open, standard protocols and techniques, via standard desktops or other edge devices from the field - facilitates information sharing and access to information for more informed decision making.

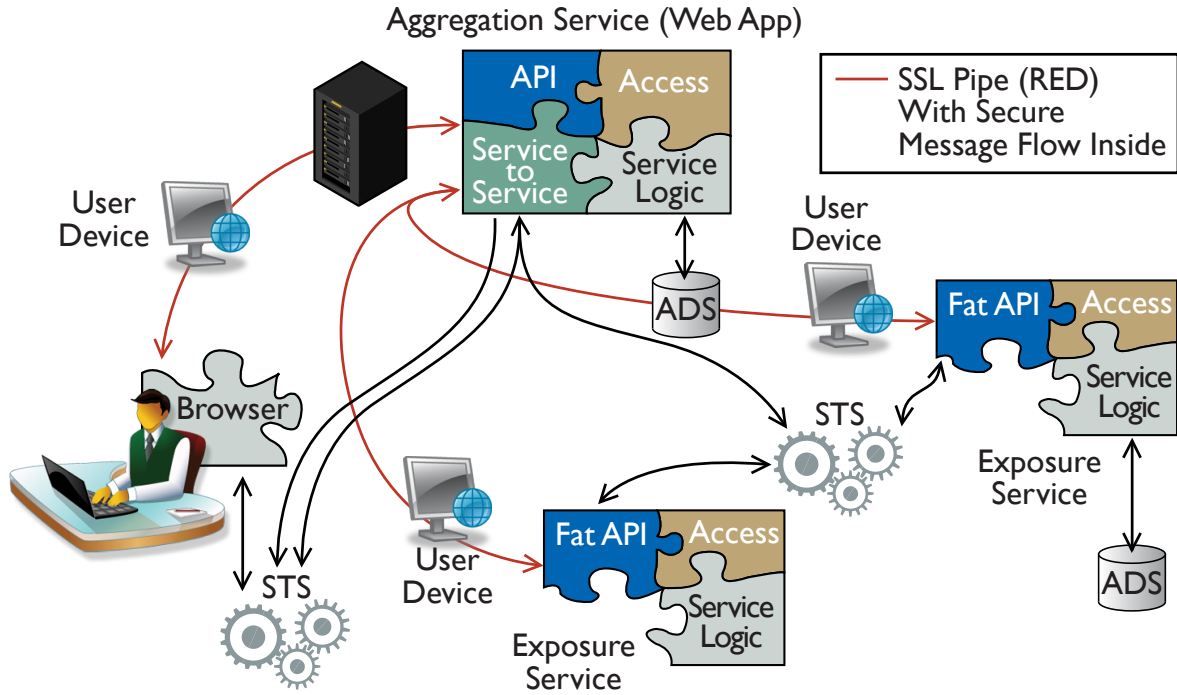
The model relies upon a layered architecture, in which each layer below the mission services can and should be implemented by industry-standard

COTS products, rather than custom software. Taking advantage of such standards will enable DoD to focus on developing higher level capabilities to fulfill its mission, rather than spending time on lower level integration tasks.

DISA currently has responsibility for centralized hosting, management, and deployment that includes end-to-end testing and performance monitoring capability. The Air Force and DISA will collaborate on bounded user requirements described through detailed business re-engineering and generating Quality of Service, performance, and access rules consistent with associated architecture products, support plans, and Service Level Agreements. Though this project focused on the Air Force's particular environment and net-centricity goals, IDA's research has potentially wide ranging implications for DoD. As a model for enterprise solutions, it can enable net-centric operations, foster information sharing, address security concerns, and create standards that will enhance DoD efficiency and cost saving. In describing this work to other DoD CIOs, our sponsor indicated that "the Air Force has been diligently working to move to a net-centric environment while improving our IT development and delivery processes. Our goal is to greatly improve the IT acquisition cycle time and build our capabilities in accordance with a well defined, standard engineering baseline."

## CLAIMS BASED SECURITY

Based on verifiable credentials containing claims to identify or privilege



## CLAIMS BASED IDENTIFICATION AND AUTHORIZATION

Authentication Using Verifiable DoD Certificate Credential and Authorization Using Verifiable Security Token Server SAML Credentials

*Dr. McDaniel is a National Defense University Fellow in IDA's Information Technology and Systems Division - on detail from her position as Dean of Faculty and Academic Programs at the National Defense University iCollege.*

*Dr. Simpson is a research staff member in IDA's Information Technology and Systems Division. His analyses have focused on such diverse topics as integrated diagnostics, Internet scale distributed systems and artificial intelligence.*

*Mr. Chandrasekaran is a research staff member in IDA's Information Technology and Systems Division. He has conducted extensive research in such fields as identity management, distributed systems security, and cognitive systems.*

*Dr. Foltz is a research staff member in IDA's Information Technology and Systems Division. He has conducted research in networks, security, and testing.*