Securely Exchanging Data across the private and public information highway

Department of Human Services

Nominating Category

Enterprise IT Management

Nominator

Clifton Van Scyoc
Chief Technology Officer
Department of Human Services, Insurance and Aging

Project Initiation and Completion Dates

Jan 2014 – Dec 2015

pennsylvania
DEPARTMENT OF HUMAN SERVICES

Executive Summary

Pennsylvania's Department of Human Services (DHS) offers benefit and assistance programs to the Commonwealth's most vulnerable residents. In order to expedite delivery of the services, the DHS programs are constantly automating manual processes and improving efficiency through real time data exchanges between the federal, state and county government entities. Additionally, legacy DHS applications and mainframe systems are also undergoing modernization and being integrated with enterprise interfaces to improve data sharing, user experience and overall system capabilities. To enable data exchange, DHS envisioned an Enterprise Web Services Security framework to provide a standardized and consistent model of implementing security for data exchanges between DHS and other government entities including federal agencies, commonwealth agencies, counties and business partners. The following are the high level business objectives of Enterprise Web Service Security and Governance framework:

- Enable secure transmission of data exchange between DHS and external entities
- Implement consistent and centralized web services security based on open standards
- Establish web services virtualization to prevent the need to provide physical end-point level access to consumers
- Promote reuse of DHS enterprise web services to expedite adoption and reduce implementation cost
- Reduce operational and administrative cost of managing web services security

DHS implemented a comprehensive an advanced Enterprise Web Services Security and Governance solution in order to meet these objectives. The solution has streamlined the overall web services security management process and made it easier to meet advanced security controls for interfacing with federal and state Information Technology (IT) systems. The DHS Web Services Security Governance solution can serve as an example for other agencies and states that are currently facing the security, integration, standardization and governance challenges surrounding web services security.

pennsylvania
DEPARTMENT OF HUMAN SERVICES

Project Narrative: Concept

The Business Problem

The following business requirements highlights a need for DHS to implement a system that can enable secure exchange of data between the various government entities.

- As part of the Patient Protection and Affordable Care Act (ACA), the Centers for Medicaid and Medicare Services (CMS) established a Federal Data Services Hub (FDSH) for verification of citizen data with trusted data sources (TDS), including the Internal Revenue Service (IRS) and Social Security Administration (SSA).
    - ❖ **Cybersecurity requirement:** DHS systems were required to implement an advanced security layer (mutual client authentication or 2-way SSL) to ensure that information was transmitted over the internet securely, reducing the risk malicious of web services security exploits.
- The Internal Revenue System (IRS) required all states to share 1095B forms via web service.
    - ❖ **Cybersecurity requirement**: DHS needed to connect with IRS web services via open standards (WS-Security) requiring digital signature of timestamp and specific payload elements as enforced by the IRS.
- The Department desired a solution that would integrate the state and county level systems via standardized data exchanges and allow transmission of abuse referrals and outcomes between state and county systems.
    - ❖ **Cybersecurity requirement**: DHS needed to provide a secure and standardized way for PA counties to connect to its Child Welfare Information Solution (CWIS) for information exchange.
- Many DHS Systems undergoing modernization needed to decommission antiquated technologies or migrate legacy interfaces to allow integration with modern enterprise functionalities.
    - ❖ **Cybersecurity requirement**: DHS needed to provide a solution that allowed legacy interfaces to be reused, recycled, and leveraged with modern enterprise functionality with minimal developmental effort.
- DHS realized the benefits of developing standardized web services and application program interfaces (APIs) for exchanging data - thus enhancing standardization and interoperability between its systems. It also saw a growth in the number of disparate consumers accessing DHS web services and APIs, including internal applications, other commonwealth agencies, business partners, and the federal government.
    - ❖ **Cybersecurity requirement**: The scale of development and use of web services within DHS created a need for establishing a standardized, secure, efficient and effective web services security solution for handling the growing security demands.
    - The U.S. Department of Agriculture (USDA) Food and Nutrition Service (FNS) planned to discontinue a monthly batch file process for obtaining disqualified recipient data for other states, thus requiring states to connect using web services for real time data exchange.

- **Cybersecurity requirement**: This integration required DHS systems to digitally sign information payloads sent to FNS.

These business requirements, coupled with the department's commitment to keep citizen data communication between its systems and data exchanges secure, created an immediate need for an Enterprise Web Services Security and Governance solution.

The Solution

DHS envisioned a security and governance solution that meets its current and forthcoming web services security requirements. With this aim, DHS evaluated different technologies in the marketplace, and decided to build its web services security solution around a market leading commercial off-the-shelf (COTS) API Gateway technology. The innovative Enterprise Web Services Security and Governance solution provided streamlined management, standardized security and regulatory compliance for DHS web services. It also supported open standards of web services security - thus fostering interoperability within the ecosystem. This implementation helped DHS address its major web services security challenges, as described below.

- Provided security for the sensitive Personally Identifiable Information (PII) and Protected Health Information (PHI) being exchanged between the federal, state and county agencies and departments – promoting security fundamentals of confidentiality, integrity and availability for web services.
- Enhanced communication between disparate consumers and their systems by implementing open standards based web services security
- Facilitated implementation of complex and leading-edge web services security requirements in a cost-effective, reusable and interoperable manner – outside of application logic.

DHS Enterprise Web Services Security and Governance solution introduces a next-gen "security tier" between the consuming application and the physical web services. This tier provides secure virtualized end-points for application consumption, thus masking the backend web service and data layer. In addition, it establishes a trusted security zone architecture where different types of security are enforced - ranging from basic http authentication, to multifactor authentication and IP address filtering – based on the consumer's assurance level.

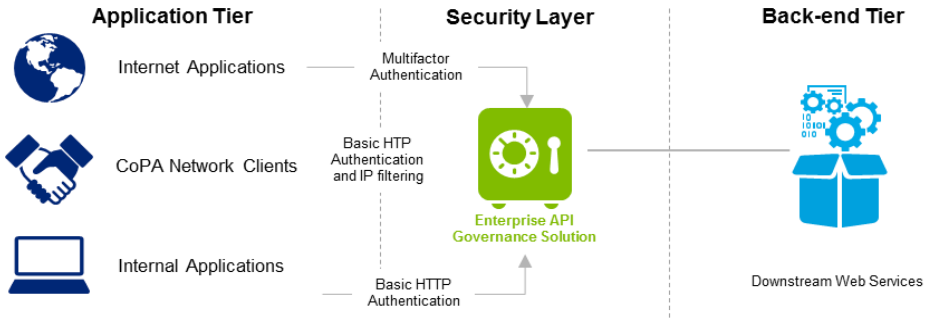

Figure 1. DHS Enterprise Web Services Security and Governance solution protects DHS web service communication

Significance

Through this initiative, DHS implemented a mature, reusable and centralized Enterprise Web Services Security and Governance solution to facilitate digital information sharing with citizens, business partners and federal agencies. The solution allowed DHS to provide online services to Pennsylvania residents in a speedy, secure and consistent way, thereby enhancing citizen trust in governmental services. It has also proved monumental in improving the cross-agency communication between the commonwealth agencies and business partners, with the establishment of industry accepted and open standards for securely sharing data. Furthermore, this standardized and industry leading implementation of web services security controls helped reduce the need for developing complex security within web service code and helped realize the associated cost savings.

DHS migrated its existing web services from legacy security to the new solution, therefore enhancing its security posture and providing consistent security controls. As a result of this initiative, applications are now authenticated and only consume web services through a single interface.

The following table summarizes the key benefits realized through this initiative.

DHS Enterprise Web Services Security and Governance Significance	
Security	• Confidentiality, Integrity and Availability for data exchanges
Reusability	• Provision for multiple access points, with specialized security, for same physical service • Promotes recycle and reuse of existing web services; resulted in cost saving during modernization efforts within DHS.
Virtualization	• Enhanced security through service virtualization • Eliminates the need to expose internal services and routes to external consumers.
Advanced Monitoring	• Centralized audit and logging and Fine-grained logging capability (specific payload elements) • Service performance monitoring to maintain desired Quality-of-service levels.
Reduced Developmental Effort	• Implements transformation between web services formats, protocols and binding – promoting reuse and recycle of existing code. • Faster time-to-delivery for business requirements.

Table 1. DHS Enterprise Web Services Security and Governance Benefits.

pennsylvania
DEPARTMENT OF HUMAN SERVICES

Impact

Through the implementation of the Enterprise Web Services Security and Governance solution, DHS has established a centralized gateway to secure data exchange – resulting in significant time and associated labor cost savings for the agency. Some of the most significant impacts of this initiative are described below.

Quantitative	• **Secures and monitors more than 50 million transactions per month**, protecting critical information of over 3 million Pennsylvania citizens that interact with DHS. • Governs **more than 220 web services** in a consistent, simplified and secure manner. • Support **more than 10 complex security cases**. This allows DHS application teams to focus their efforts on the business logic development while complex integrations with external systems are done through the solution.
Qualitative	• **Standardized** web services security for DHS web services utilizing the gateway. Over 40 DHS applications, over 5 business partners and several commonwealth agencies now transmit data with DHS in a secure and effective manner. • **Reuse and recycle** of legacy interfaces, through the use of Web Services Security and mediation layer, thus **reducing cost** related to modernization efforts • **Reduction of administration and maintenance overhead** through the use of a single point of management to install and renew more than 50 client and SSL certificates.
Innovative	• **Reusable web services** reduce development effort and provide standardization across applications. This promotes reusability of code without affecting existing interfaces. • **Web service mediation** is used to expose a physical web service under different protocols and formats. For example, DHS services that were designed as Net.TCP are now be exposed as HTTPS enabling legacy enterprise assets to remain relevant. • **Enables integration** of inflexible web services, like those offered by COTS products, in application desired format which otherwise is cost-intensive task.

The following graphic illustrates how the solution has provided a secured and integrated platform to enable data exchanges with various government entities.

Figure 2. Impact of DHS Enterprise Web Services Security and Governance Solution

This initiative has allowed DHS to better serve its constituents by providing a secure, effective means to transmit citizen's data in real-time. The DHS Web Services Security and Governance solution serves as an example for other agencies and states dealing with similar challenges regarding web service security, governance, expansion and adoption.