



Case Study:

Aetna Enhances Secure Provider Portal with SSO and SAML 2.0

The Company

Aetna is one of the nation's leading diversified health care benefits companies, serving approximately 37.2 million people with information and resources to help them make better informed decisions about their health care. Aetna offers a broad range of traditional and consumer-directed health insurance products and related services, including medical, pharmacy, dental, behavioral health, group life and disability plans, and medical management capabilities and health care management services for Medicaid plans. Customers include employer groups, individuals, college students, part-time and hourly workers, health plans, governmental units, government-sponsored plans, labor groups and expatriates.

Key Objectives

Aetna sought to provide role-based access control to a portal that would offer healthcare providers access to Aetna-hosted applications and transactions through a single sign-on (SSO), and delegate office administration of this access to providers.

The Initial Drivers for Single Sign-On

Aetna conducted research to help identify and better understand what their healthcare providers needed. "Focus groups showed us that our providers wanted a portal that they could access for multiple payers," said Chere Parton, head of Aetna Provider eSolutions. "Then separately, we defined our internal needs which included having the capability of providing additional products and services to these providers in a highly secure way."

Aetna's Deployment Wins a 2008 IDDY Award



Aetna was recently honored by the Liberty Alliance with an IDDY Award (IDentity Deployment of the Year). The IDDY recognizes identity-based applications built using Liberty Federation (including SAML 2.0), Liberty Web Services, Liberty People Service and Liberty Advanced Client specifications.

Aetna's deployment is garnering raves throughout the industry. It stood out to the IDDY judges for the following reasons:

- Aetna and NaviMedix have successfully collaborated around the Liberty principles of party federation.
- They've established re-use through interoperability standards and avoided point-to-point solutions.
- Using SAML 2.0, they are also positioned for the circle of trust and ID assurance principles in their enterprise architecture continuum.
- From a business perspective, this collaboration has enhanced the experience between Aetna and its providers.
- Aetna's Secure Provider Web site via NaviNet offers a superior security model to support its strategic direction of offering important information only to the appropriate users in a provider's office.
- This model positions Aetna to support clinical decision tools, i.e., patient care alerts, and a host of upcoming clinical initiatives.

Moving Forward: Addressing Privacy and Security

Aetna made a strategic decision to convert a home-grown portal, internally designed and constructed at Aetna, to an externally hosted online provider portal that would not only include a variety of tools, transactions and content hosted by Aetna, but would also include interfaces with third-party Internet Application Service Providers and Content Service Providers.

"If you want a good challenge as an IT security strategist health care is the place to be," said Aetna's Head of Security Architecture Mark Coderre. "We have the ultimate need for accuracy and privacy given customer interests in online health information and privacy."

Beyond those industry-specific concerns, Coderre said, Aetna's challenges were similar to those any organization faces when seeking to share confidential information:

- Identifying the legal agreements that need to be in place to protect trusts
- Coordinating the technical and legal requirements of multiple parties
- Agreeing at an early stage about the definition of identity
- Avoiding the privacy risks of collusion

Aetna addressed these issues via SAML 2.0, a standard for exchanging authentication and authorization data between security domains.

"The question of what makes up an identity is critical because it forms the basis of the SAML assertion," said Coderre. "If that's ambiguous, then the sanctity of SAML doesn't mean anything."

This is a critical issue since the portal uses SAML 2.0 for single sign-on with an integrated Federated Identity Management process allowing providers seamless access to information across all systems.

"Strong deployments come from careful business analysis, which Aetna has certainly done well. Liberty's specifications follow the same process of first identifying needs and quantifying needs, with very careful attention paid to privacy and global policy considerations, and then creating technological solutions. We applaud Aetna for such a sound process, which is clearly reflected in a smooth, successful deployment. We are very pleased to award Aetna with a 2008 IDDY Award for this excellent work."

**-Britta Glade
Director of Marketing,
Liberty Alliance**

Aetna's Solution

Aetna was able to convert its existing proprietary portal to a more sophisticated, delegated access portal operated by a third-party provider, NaviMedix. Beginning in Fall 2007 and reaching completion in June 2008, Aetna deployed the portal to offices representing 300,000 providers and staff, scalable to 500,000. The portal supports 30 transactional functions, including Claim Status Inquiry, Referral, pre-certification, Eligibility and Benefits.

NaviMedix, a leading innovator in automating health care provider communications, had worked with Aetna previously, and Aetna chose NaviMedix for this project after a thorough search. NaviMedix's experience in role-based security systems was a major factor in Aetna's choice, as was its ability to give providers access to multiple payers while allowing each payer to offer differentiated products and services through the portal.

The solution puts the responsibility to oversee access to the portal in the hands of physicians and healthcare providers, rather than in Aetna's. "Previously, we would try to understand the structure of each [provider's] office," said Chere Parton. "Whether one person should have access to eligibility, or a pre-certification transaction, or a referral transaction. It's difficult to know that, as a health insurer. The new portal puts those decisions in the hands of the healthcare providers."

How It Works: Federation in Action

Federated ID Management aligns IDs and roles between NaviMedix as an IDP, and Aetna as an SP-IDP.

In this model, Aetna is positioned as its own hub, between upstream portals and downstream service-providers, with an insulated method to reassert IDs and entitlements in a transitive manner.

The Federated Identity Management process keeps identification information in both systems synchronized. This ensures that access to information is regulated consistently irrespective of the point of entry of the user. This helps in meeting HIPAA PHI (Protected Health Information) requirements.

"Aetna has been a leading force and early adopter in the federation space," said Matthew Gardiner, Principal at CA, a longtime Aetna solutions provider. "They've been matching technology to real business requirements. They've continued to adapt early and often. They are recognized market leaders."

New Features

The new portal offers several attractive new features for healthcare providers:

- Providers can set access within Aetna's Secure Provider Web site for different users, with increased, HIPAA-compliant security options. For example, health care providers can give staff, those responsible for appointments and check-in, access to eligibility information only, while accounting staff may have additional access to claim and payment information. Providers' security officers can also set up customized access to important messages from Aetna according to users' roles.
- Free real-time transactions are available with Aetna as well as other payers, including major health plans and the Medicare program.
- Enhanced administrative options provide one-stop service. Only one username and password is needed to interact with Aetna or other health plans.
- Improved functionality provides customized transactions with more detail and easier navigation. Health care providers can check eligibility and benefits in real time, submit or inquire about claims, review claim payment policies, view and print explanations of payments online within 24 hours of claims processing, obtain electronic remittance advices, access Aetna's education site and conduct many other activities.
- Easy-to-use support tools help providers use the site and manage transactions.

New Services: Care Considerations and the Personal Health Record (PHR)

Aetna sends Care Considerations—alerts about patients' health care—to physicians through a NaviMedix platform called NaviNet®. Care Considerations identify possible gaps in care, drug-to-drug or drug-to-disease interactions, and more; they are derived through the MedQuery® program, developed by ActiveHealth Management, an independent subsidiary of Aetna. Aetna had previously sent these Care Considerations by phone, fax or mail, but NaviNet® allows them to also arrive by e-mail or as electronic alerts when a provider conducts any transaction involving the patient.

For example, Parton explained, when a provider makes an eligibility benefit verification—the most common portal transaction—a Care Consideration, which is based on Aetna's data including claims history, current medical, lab and pharmacy claims and patient demographics, pops up to alert the physician of an issue that requires attention. Electronic delivery offers the advantage of efficiency, timeliness, and no paper to file or lose, as well as the security of all NaviNet® transactions.

Separately, Aetna has also given members the capability to make their personal health records (PHRs) available to treating physicians through NaviNet®. These PHRs include information from Aetna's claims system as well as non-claims medical information entered by Aetna's members (the patients) themselves; patients have the opportunity to review, change and retract access to this information at any time.

The Benefits

The NaviNet® site allows providers to make their own decisions about access to benefits information, and makes that information available in a clear, timely manner. “More information about patients improves patient health; members get better care,” Parton said, “and improved health outcomes.”

“Feedback has been very positive,” said Parton, who also explained that the transition to the new portal has been smooth. “If anything, I’ve been surprised at how smoothly it’s gone.”

ROI of Federation

Single sign-on (SSO) was designed between NaviMedix and Aetna applications minimizing redevelopment and giving a common portal presentation to providers.

Enablement of web service transactions with federation is also having impact. “As a result of this implementation, we expect savings in a number of areas,” said Parton. “There’s reduction in calls to service centers, elimination of paper-based communications and increased utilization of electronic administrative tools.”

Looking Forward

For Aetna, the future of information sharing is now. “Federation point-to-point is one thing, but where this will lead is web federation with multiple parties, and Aetna’s already got those scenarios,” said Coderre. “The legal and technical logistics get more complicated as you put more parties together to satisfy a common transaction.”

Organizations such as Liberty Alliance are essential to navigate this process. Coderre said that Aetna’s work with Liberty, the Healthcare Information Technology Standards Panel (HITSP), and the Institute for Information Infrastructure Protection (I3P) has been extremely helpful, and will be even more so going forward.

“Being able to prove that you can safely link this data is going to be key to a higher adoption of new products such as the Personal Health Record,” Coderre said. “The cumulative efforts of Project Liberty, HITSP and I3P should be able to provide that safe linking of information without increasing the threat.

“Liberty’s Identity Assurance Framework (IAF) is especially important,” he added, “Because not every registration is going to be based on in person vetting.”

About Liberty Alliance

Liberty Alliance is the only global identity community with a membership base that includes technology vendors, consumer service providers and educational and government organizations working together to build a more trust-worthy internet by addressing the technology, policy and privacy aspects of digital identity management. Liberty Alliance is also the only identity organization with a history of testing vendor products for true interoperability of identity specifications. Nearly 80 products and identity solutions from vendors around the world have now passed Liberty Interoperable™ testing. Liberty Alliance works with identity organizations worldwide to ensure all voices are included in the global identity discussion and regularly holds and participates in public events designed to advance the harmonization and interoperability of CardSpace, Liberty SAML 2.0 Federation, Liberty Web Services, OpenID and WS-* specifications. More information about Liberty Alliance as well as information about how to join many of its public groups and mail lists is available at www.projectliberty.org.