

A large, vertical, grey decorative shape on the left side of the page, with a curved right edge that tapers towards the top.

RISK, REACH, AND RETURN: EVERYTHING TODAY'S CISO NEEDS TO KNOW ABOUT USING SSO TO SUCCEED IN THE WEB 2.0 ERA

White Paper
September 2008

Table of Contents

| | |
|--|----|
| Executive Summary | 1 |
| The Evolution of SSO to Meet the Needs of the Open yet Secure Enterprise | 2 |
| Facing the Fears: Complexity, Time, Money, and Risk | 4 |
| What to Look for in a Solution to Meet Evolving SSO Challenges | 5 |
| How to Get Started | 7 |
| Sun OpenSSO Enterprise: The Complete Solution for SSO Challenges | 8 |
| Sun's Industry Leadership in Identity Management | 9 |
| OpenSSO Enterprise at Work in the Real World | 11 |
| Conclusion | 12 |

Chapter 1

Executive Summary

Open yet secure: It sounds like a contradiction, but it's the state to which every enterprise must aspire in order to succeed in the Web 2.0 era. Being open yet secure means extending the organization's *reach* to more partners, vendors, customers, and others outside the enterprise in more ways — while still controlling the amount of *risk* to which the organization is exposed as a result. Complicating the challenge further is the need to realize an acceptable *return* on the technology that is used to achieve the right risk:reach ratio for the enterprise.

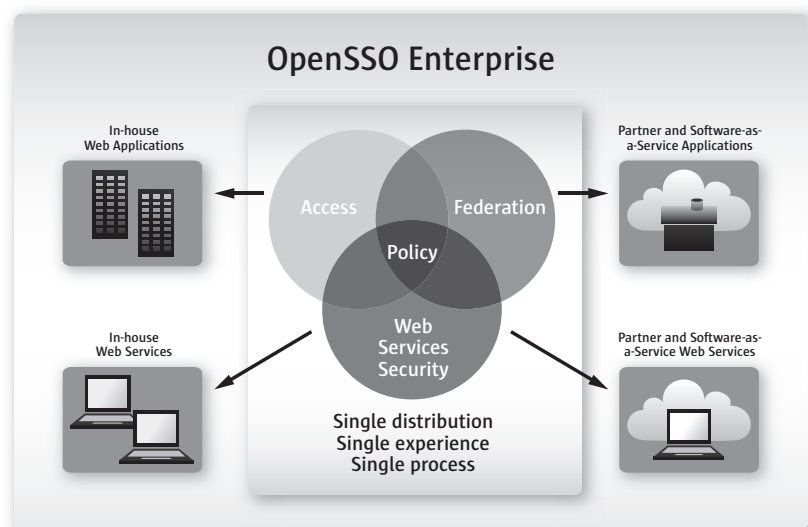
This paper is intended to arm the CISO with the knowledge to make informed choices to extend the enterprise's reach with minimal risk and maximum return on the technology employed in the effort. It will:

- Discuss how SSO has evolved from an internal tool for secure access to one that enables secure access from beyond the enterprise
- Deflate some of the common fears associated with taking SSO beyond the enterprise today
- Define the criteria for choosing the right identity-based technology approach and the ideal vendor for SSO initiatives
- Delineate practical steps to take to get started on an SSO initiative
- Describe Sun's comprehensive approach and industry leadership in addressing the challenges associated with creating an open yet secure enterprise

Chapter 2

The Evolution of SSO to Meet the Needs of the Open yet Secure Enterprise

Once upon a time, SSO was a tool for improving the way enterprises managed access to internal resources. Now with the growing trend toward Web 2.0 dynamic collaboration and the increasing involvement of partners in critical business process outsourcing, SSO has evolved to address the challenges associated with extending access to staggering numbers of external users.



Access, federation and Web service security, enables SSO across both in-house and partner applications and Web services to extend business reach and reduce security risk.

Stage 1. SSO and internal access management

SSO was originally a means of simplifying how internal users gain secure access to resources as the number of resources grows. Rather than requiring a separate sign-on for every application or other resources — clearly an unsustainable approach as the number grows into the hundreds or thousands — the organization can instead enable users to use just one sign-on to access multiple resources.

Stage 2. SSO and extranet access management

The need to simplify how internal users gain access to resources has evolved into a need to do the same for external users. The problem is that most access management solutions today were designed for the enterprise and internal users, not the extranet and external users. The difficulty for the enterprise is in finding a way to address both internal and external needs without over-complicating the technology infrastructure or overtaxing the IT budget in the process.

Stage 3. SSO and federation

As the enterprise struggles to increase revenue without increasing costs, SSO has evolved to include federation, or the ability to make identity and entitlements portable across multiple domains. An increasingly important element in identity architectures, federation creates opportunities to expand business reach by building federated connections to SaaS applications, partner services, affiliate services, acquisitions/subsidiaries, business process outsourcing, and third-party hosted portals, among others. To make it work in the real world and in the long term requires standards-based technology. Only through standards can there be repeatable, scalable processes for easily accommodating growing numbers of external entities.

Stage 4. SSO and secure Web services

Attention is now shifting to the challenge of ensuring that Web services delivered by organizations are secure, requiring SSO to evolve once more, this time to accommodate sign-on for Web services just as it has evolved to accommodate Web application access and federation.

In reality, many enterprises are dealing with several of these stages at once. For example, an organization may be confident in the way it is handling internal access management, but still looking for the best approach to manage the challenges that have evolved as the enterprise further extends its reach.

Chapter 3

Facing the Fears: Complexity, Time, Money, and Risk

Addressing SSO at multiple levels, starting internally and then moving out to handle extranet access management, federation, and secure Web services, may seem a daunting prospect. As a result, the CISO may have understandable fears about the scope of the challenge, how long it's going to take, and what it's going to cost.

Fear: It's complicated.

Fact: It doesn't have to be. By choosing a technology approach that addresses every stage in the evolution of SSO, the enterprise can deal with immediate and future problems without the nightmare of also dealing with separate licenses, infrastructures, and products. The other reason to think holistically about a solution is to ensure that you purchase a solution that will grow incrementally with your business.

Fear: It's time-consuming.

Fact: One of the main reasons a technology deployment takes longer than expected is that too much time is spent adapting the existing IT environment to the new technology — or vice-versa. The key is having an open agnostic architecture that's designed to be easily integrated into existing environments and to interoperate with third-party identity products.

Fear: It's expensive.

Fact: A standards-based approach that scales as the number of external users grows will decrease operational costs by providing a repeatable, scalable approach to onboarding new applications, web services and partners. Simultaneously, being able to quickly integrate new partner services that directly enhance customer value can increase revenue and provide competitive differentiation. So it not only won't cost the enterprise an undue amount of money, it will contribute to *making* money for the enterprise. Standards and interoperability also help control costs by reducing the amount of work needed to integrate legacy applications.

Fear: It's too risky.

Fact: In most cases, organizations can federate with partner applications without ever having to share user credentials such as password and user ID. This is because standards-based federation allows both the identity provider and the service provider to choose the minimal set of attributes to share, rather than requiring the sharing of such sensitive attributes.

Chapter 4

What to Look for in a Solution to Meet Evolving SSO Challenges

Comprehensive capabilities

The ideal is to have one solution that addresses the multiple areas of extranet access management, federation, and secure Web services. Look for a solution that does not require multiple licenses, separate products, and separate infrastructure to address multiple requirements.

Flexible, modular architecture

While the ideal solution addresses all areas of SSO, it shouldn't *require* the enterprise to deploy every capability including those it's not yet ready to take advantage of. The architecture should be modular to roll out capabilities as they are needed. And it should have the flexibility to easily integrate with existing identity and access management solutions that may already be in place.

Standards-based

Scalability is essential to securely and successfully extending enterprise reach over the long term, and standards are essential to scalability. Look for a standards-based solution that supports leading industry standards such as SAML, WS-Federation, and WS-Trust.

Minimal customization

As the enterprise extends its reach to include increasing numbers of external partners and their resources, it becomes increasingly important that any SSO solution be designed to work seamlessly with those partner applications. It should not require substantial customization or programmatic development to work with external applications.

Depth of vendor expertise

Choose a vendor who understands the interrelationships between core identity challenges — not just the SSO challenges of extranet access management, federation, and secure Web services, but also provisioning, role management, directory services, and compliance management. Your vendor should also serve as a strong architecture and design resource who can guide you in building an identity infrastructure that can scale and evolve to extend your reach and manage your risk over the long term.

Open source over proprietary

Open source products that provide support and indemnification offer many advantages over proprietary products. Open source products tend to be more secure, due to the open nature of the source code and the continual beta that occurs throughout the product's lifetime. They also provide greater access to information, along with the ability to participate in community forums and collaborate closely with community members. Finally, open source communities are likely to innovate more quickly, and they tend to have a shorter time-to-market.

A pricing model that supports growth

After working hard to incorporate the right features and reduce risk, the last thing a business needs to worry about is making sure licenses are in compliance every time more partners or applications are added. Purchase a solution that provides a subscription model that is all-inclusive, and beware of solutions that have hidden costs in the form of additional agents or modules that are necessary for business growth. Finally, companies in start-up mode or those who need to prove the concept in order to get funding will benefit by starting with an open source solution. This model makes it possible to start with minimal investment, get buy-in from key business leaders, and then secure the funding to make the business or project a success.

Chapter 5

How to Get Started

Now that you know how to select the right solution, here are some practical guidelines for planning an SSO project.

Extranet access management

Identify how many times internal employees have to sign on to internal applications and how many times customers have to sign on to extranet-facing applications. Quantify the dollars spent on fielding login and password reset support calls. Use this metric as a baseline to show how an SSO solution can reduce costs.

Federation

Don't attack too much at once; small, quick wins make it easier to sell larger federation projects later. Start by identifying a federation use case that can be completed quickly. Once you have one partner onboard, start to ramp up and engage multiple partners at once. Show the CISO a holistic view of your federation vision: onboarding subsidiary applications, partner applications, acquisition applications, business process outsourcing, and so forth. Describe the benefits in terms of the end user experience, and discuss economies of scale (i.e., the more applications you onboard, the more you save).

SaaS

Target a single SaaS application to demonstrate the value of outsourcing Web 2.0 services (for example, Google Calendar, Salesforce.com, Facebook). Compare this to the cost of hosting your own version of these applications internally. Evaluate the reach of the SaaS application compared to the reach of an internally hosted version. Do a simple proof of concept with a SaaS application to demonstrate its value and simplicity. Federation with a SaaS application can often be implemented in less than a day and is a visually impressive example of federation to show your CISO.

Web services security

Evaluate how many Web services are exposed in your organization. Try to identify how many, if any, are secured. Use these statistics to make a strong business case to your CISO about reducing risk and providing transparency around Web services security.

Chapter 6

Sun OpenSSO Enterprise: The Complete Solution for SSO Challenges

Sun OpenSSO Enterprise was designed to help today's enterprise address every aspect of the SSO challenge, both immediately and as the organization's needs evolve. Solution highlights include:

One solution for access management, federation, and Web services security

OpenSSO Enterprise is the only access management solution to provide internal and extranet access management, support federation, and enable Web services security — all as part of a single, self-contained Java application, without the need for separate products or licenses. Organizations with existing internal access management solutions will find it easy to integrate OpenSSO Enterprise with them; those looking for a complete solution for internal and external users will find all the capabilities they need in this solution.

Designed for rapid deployment and configuration

Having all installation and configuration capabilities contained within one application speeds deployment. In addition, agent configuration, server configuration, and other tasks have been simplified to make them repeatable and scalable, so multiple instances of the solution can be deployed without additional effort. An embedded directory server eliminates the need to configure a separate directory to support the configuration store.

Standards-based for interoperability and scalability

Because OpenSSO Enterprise is a 100% Java™ solution, it can be quickly deployed on any OS platform, and it runs in any container platform. The solution supports all major federation protocols, and it enables organizations using different protocols to communicate despite these differences.

Open source innovation

Sun offers a complete strategy for delivering an open source identity suite that leverages community innovation to improve software development and delivery. OpenSSO Enterprise represents this new class of software development that is guided by a large, highly active community and supported by a world-class organization, Sun.

Chapter 7

Sun's Industry Leadership in Identity Management

Sun is widely recognized as a leader in identity management, with millions of identities under management. The company's complete portfolio of solutions also includes the following capabilities.

Converged provisioning and identity auditing

Sun™ Identity Manager software provides the comprehensive functions to apply and enforce security policy and meet compliance and audit requirements. Key features include:

- Integrated capabilities for preventative and detective compliance
- Identity controls consistently applied across provisioning and auditing
- Automated reviews, proactive scanning, and consistent enforcement
- Policy violation tracking and expiration capabilities to handle exceptions

Role management

Sun™ Role Manager software dramatically simplifies access control by applying enterprise access policies based on user roles rather than individual access privileges. Key features include:

- Role engineering and ongoing role maintenance
- Ongoing role certification by business unit managers or role owners
- Enterprise-level monitoring of access for policy conflicts
- Dashboard view of certification status and policy exceptions

Directory services

Sun™ Directory Server Enterprise Edition and Sun OpenDS™ Standard Edition provide an easy-to-manage directory infrastructure that consolidates and manages identity information from multiple sources. Key features include:

- High performance including sustained search performance and near-relational database write performance
- Robust security — including encryption, password protection, and multilevel ACLs — to protect data stores
- Advanced backup and restore to help ensure high availability and reliability

Services

Sun Services offers integrated and broad portfolios of that encompass the full lifecycle of identity management projects — from evaluation, through architecture and integration, to long-term solution management. These services include:

- Support services
- Professional services
- Managed services
- Learning services
- Partner services ranging from consulting to deployment to support

Chapter 8

OpenSSO Enterprise at Work in the Real World

Read these success stories to learn more about how OpenSSO Enterprise is helping enterprises worldwide extend their reach while controlling risk and maximizing technology investment returns.

BC Hydro

sun.com/customers/software/bc_hydro.xml

Business Industry Political Action Committee (BIPAC)

sun.com/customers/servers/bipac.xml

Government of Norway

sun.com/customers/software/norway.xml

Grant McEwan College

sun.com/customers/servers/grant_macewan.xml

Insurance Corporation of British Columbia

sun.com/customers/software/icbc.xml

ITOCHU Techno-Science Corporation Ltd.

sun.com/customers/software/itochu.xml

Robur

sun.com/customers/servers/robur.xml

Swisscom Mobile AG

sun.com/customers/software/swisscom1.xml

sun.com/customers/software/swisscom2.xml

Universidad Complutense de Madrid

sun.com/customers/software/complutense.xml

Western Michigan University

sun.com/customers/software/wmu.xml

For a complete list of all Sun identity management customer success stories, visit sun.com/identity/customers.

Chapter 9

Conclusion

In the Web 2.0 era, SSO has evolved from a tool for managing internal resource access to one that enables the enterprise to manage extranet access, federate with other organizations, and secure Web services. But using SSO to extend enterprise reach while reducing business risk can be challenging. Success comes from making informed choices of SSO projects to undertake and technology to rely on in the effort.

To learn more about Sun OpenSSO and Sun's comprehensive identity management portfolio, visit sun.com/identity.

