

A large, abstract graphic on the left side of the page, consisting of overlapping, semi-transparent, curved shapes in shades of gray, creating a sense of depth and movement.

IDENTITY FEDERATION: TRANSCENDING THE BOUNDARIES OF BUSINESS FOR SECURE COLLABORATION

White Paper
October 2005

Table of Contents

Executive Summary	3
What Is Driving Federation	4
The Virtual Enterprise	4
The Challenges of Securely Sharing Information Across Traditional Boundaries	6
Interoperability	6
Information Security	6
Cost Control	6
Quality of Service	7
The Requirements of a Federated Solution	8
Automation	8
Federation Standards	8
Circles of Trust	8
Federation and Sun Identity Management Solutions	9
Standards Leadership	9
Integrated and Integratable Solutions	9
Complete Portfolio of Identity Management Solutions	10
Federation at Work in the Real World: Three Examples	12
Telecommunication: Multiple Services, Millions of Subscribers	12
Financial Services: A Robust Solution for Streamlined Vehicle Financing	12
Automotive Manufacturing: Driving Simplified, Secure Relationships with Multiple Partners	13
Conclusion	14

Chapter 1

Executive Summary

*Federation: The agreements, standards, and technologies that make identity and entitlements portable across autonomous domains.*¹

As organizations increasingly share applications and information with external partners online, the prospect of enabling secure user access to resources across security domains can seem at the very least daunting — and at the very worst impossible. In fact, it is virtually impossible for organizations that are working with a complex and dynamic universe of users spanning multiple domains to efficiently and reliably manage and authenticate identities across those domains. Short of maintaining a virtually unlimited amount of information about other organizations' users in its own data stores, what can an organization do? Identity federation is the answer.

Federation makes identities portable across domains so that they can be efficiently shared with and leveraged by trusted partners. It provides the mechanism whereby an organization can accept that external users have already been authenticated by a trusted partner and can grant them access — without having to be responsible for managing all their identity information. Within this framework, users enjoy seamless, secure access to partners' services via a single sign-on (SSO) to multiple applications. This not only radically simplifies the process of granting access, it also makes it possible to maintain the high levels of security necessary to protect the integrity of that access.

This white paper will:

- Explore trends in online collaboration, among businesses and other types of organizations, that are driving the shift toward federation
- Examine the business and technology challenges associated with these trends — challenges that federation can address
- Define and describe the requirements of federation-based solutions for large-scale online collaboration, and address the challenges inherent in meeting these requirements
- Demonstrate how Sun incorporates support for federation in its identity management solutions, and provide real-world examples of Sun solutions at work today

1. Definition from Burton Group, Identity and Privacy Strategies Research Report, "Toward Federated Identity Management: The Journey Continues," August 19, 2003.

Chapter 2

What Is Driving Federation?

The pace of today's business environment requires companies to constantly reevaluate how they:

- Share information with users beyond their boundaries
- Efficiently deliver new services to internal users
- Collaborate with partners to broaden their market reach

What's more, they must do all this without compromising security and without sacrificing visibility into key business processes. The pressure to maintain user privacy is growing, as demonstrated by legislation such as the Health Insurance Portability and Accountability Act (HIPAA), to name just one of the many new laws related to this issue. As a result, organizations are increasingly challenged to prove accountability for activities that are highly distributed and exploding in scale.

This need to securely share resources beyond traditional boundaries — especially as a means of creating new business opportunities, outsourcing operations outside the enterprise's core competency, or enriching the experience of existing users — drives the need for identity federation.

The Virtual Enterprise

From Web-based, joint business ventures such as wireless services, to collaborative corporate vendor portals, to sites where government agencies, schools, and other institutions deliver information and services, the virtual enterprise is defining new opportunities for organizations to work together online. In order to share information across multiple boundaries with the growing number of consumers, vendors, partners, and others, organizations in virtual enterprises must have a mechanism in place for authenticating external identities from multiple sources. Federation can play this role in any of a number of scenarios, as illustrated in the following.

Business-to-Employee or Organization-to-Employee Collaboration

The opportunity: Moving some aspects of employees' communications and services online — such as human resources (HR)-related services, for example — can dramatically increase operational efficiency. Examples include:

- Organizations providing their employees with the means to access benefits information on insurers' or other suppliers' sites
- Employees accessing outsourced applications as well as help desk and other services

Business-to-Consumer and Other Consumer-Facing Collaboration

The opportunity: Giving consumers the convenience of "one-stop" shopping and other activities creates new revenue opportunities for enterprises and increases satisfaction among users. Examples include:

- Customers simultaneously purchasing or receiving services from multiple businesses representing a general area — for example, airline, hotel, and car rental; or bank, brokerage, and lender
- Students using a single education site to register for classes, buy books, communicate with professors and advisors, engage in e-learning with other institutions, join alumni groups, and participate in other activities both inside and outside their university

Business-to-Business and Other Interorganizational Collaboration

The opportunity: Unprecedented economies result when organizations that previously could barely share information at all due to geographical or other barriers can now collaborate instantly and effortlessly online. Examples include:

- Related companies in the same industry — such as health care organizations, other health care providers, and payors — that need to share information with each other to deliver services to consumers
- Government agencies that must work together as part of a larger entity — such as the 22 groups that make up the U.S. Department of Homeland Security
- Manufacturers, service providers, and other kinds of businesses that work with multiple companies for the goods and services they need to create their own products — such as a wireless telecommunication provider delivering numerous personalized services
- Channel partners such as brokers, agents, or independent sales associations that need to be able to access the company's resources

Chapter 3

The Challenges of Securely Sharing Information Across Traditional Boundaries

Interoperability

The challenges:

- For users — Remembering separate passwords for every single application
- For administrators — Authenticating users' identities across organizational boundaries (and often having to deal with multiple types of identity information for a single user in the process)

The federated solution:

- An SSO that provides access across applications in multiple domains
- Portability of identity information across security domains
- Leveraging of trust relationships to accept that a user has already been authenticated by a trusted partner

Information Security

The challenges:

- Applying security policies across multiple organizations
- Keeping private information private when exchanging data about many users from a multitude of sources

The federated solution:

- A framework for cross-organizational interoperability in which a user must be authenticated only once, but can be authorized as appropriate at the enterprise providing the service
- Implementation of the latest standards and technologies to provide sound security policies and strengthen authentication credentials, such as digital certificates or stronger composition policy for passwords
- Clear user control over which external partners can link to a company's identities, and what personal attributes are provided across organizational boundaries

Cost Control

The challenges:

- Managing identities on an unprecedented scale without incurring untenable infrastructure costs
- Reducing costs by making authentication and authorization portable and reusable across large provider networks in which identities may be owned by external partners

The federated solution:

- The ability to accept a trusted partner's authentication of a user's credentials, while efficiently mapping authorizations to those trusted credentials
- Automation of identity management tasks to eliminate costs for manual processes

Quality of Service

The challenges:

- Streamlining navigation between internal applications and those hosted by partners
- Securely delivering new services to internal and external users

The federated solution:

- SSO for multiple applications hosted in multiple domains
- Management and authentication of identities where they are owned, enabling new services to be introduced at an accelerated pace

Chapter 4

The Requirements of a Federated Solution

Automation

Identity federation automates the process of sharing identity information across traditional organizational boundaries. Without it, every organization involved in a collaboration must manually create lists of users who need access to resources, a costly and time-consuming process. Or an organization can use the same Web access management tools employed by other participating organizations, and rely on those proprietary mechanisms for sharing information. However, the proprietary nature of this approach soon makes it impractical to go very far beyond collaborating with one or two partners. Federation sidesteps all of these problems by using standardized, automated mechanisms to widely and securely share user identity information.

Federation Standards

Standards are essential to the exchange of identity information across disparate systems. Burton Group CEO Jamie Lewis explains how it works: “If one domain uses Kerberos to authenticate users, for example, and another uses ID/password authentication, the two systems can still exchange information regarding authentication operations if they share a common method for exchanging that information. That’s precisely what the Security Assertions Markup Language (SAML) does.”²

SAML is the eXtensible Markup Language (XML)-based specification supported by the Organization for the Advancement of Structured Information Standards (OASIS). It has been adopted by the Liberty Alliance, an industry organization consisting of 160 member companies that have joined together to promote federation standards. The alliance’s Identity Federation Framework extended SAML to offer higher-level capabilities that have now been incorporated back into the latest SAML specification.

Circles of Trust

An organization can have all the technology and standards in place for federation, but the framework will work only if there is one more essential element: trust. Organizations that share information must ultimately trust each other for federation to succeed. Neil McAlister, writing in *InfoWorld*, says that organizations must establish what he calls “an identity network, where if A trusts B and B trusts C, A knows it can also trust C. To create such a network, however, partner organizations have to establish both a shared set of rules and some idea of accountability.”³

A shared set of rules is a defining element of the identity networks operated by leading service providers today. These “circles of trust” represent a business model in which information-sharing and collaboration are governed by agreements about responsibility for various aspects of the information-exchange infrastructure and by agreements about:

- Mutual confidence (trusted authentications and authorizations)
- Service management (remote payments, geolocation, mobile data services)
- Billing (enabling event- and subscription-based models)
- Risk management
- Liability management
- Compliance (such as the Trusted Transaction Roaming platform, or T2R)

2. Burton Group, *Federation: Separating Hype from Reality*, Latest Insight column, Jamie Lewis, November 7, 2002.

3. *InfoWorld*, *Identity's Federated Future*, Neil McAlister, September 3, 2004.

Chapter 5

Federation and Sun Identity Management Solutions

Sun enthusiastically supports identity federation through its:

- Industry leadership in developing federation standards
- Demonstrated commitment to creating products based on standards
- Integrated and integratable philosophy of product and service development
- Complete family of identity management solutions — in particular, Sun Java™ System Access Manager, Sun Java System Federation Manager, and Sun Java System Identity Manager Service Provider Edition

Standards Leadership

As a leading member of both OASIS and the Liberty Alliance, Sun has played a major role in the evolution of key federation standards. The company was first to market with fully supported versions of these specifications in commercially available solutions. Sun customers are currently using these standards successfully in Sun products. Sun solutions specifically support:

- The SAML standard for SSO to multiple resources
- Liberty Alliance specifications for open, federated, SSO identity solutions
- The Service Provisioning Markup Language (SPML) industry standard for exchanging and administering user access rights and resource information across heterogeneous environments
- Leading Web services standards such as XML, Simple Object Access Protocol (SOAP), XML digital signatures, XML encryption, and Java technology
- The Lightweight Directory Access Protocol (LDAP) standard for accessing information directories

Integrated and Integratable Solutions

Sun™ identity management solutions are designed to help organizations share information and resources securely and efficiently. They are highly integrated solutions that are also highly integratable. Sun solutions are designed to reduce integration cost and complexity across organizational boundaries through:

- Support for federation and other industry standards, as described above
- An open architecture that emphasizes interoperability among heterogeneous technology environments

This integrated and integratable approach to identity management in general delivers the flexibility that federation demands, while helping organizations control the cost of managing identities across traditional boundaries.

Complete Portfolio of Identity Management Solutions

Sun Java System Access Manager

Sun Java System Access Manager provides a secure, federated framework and authentication-sharing mechanism for organizations that need to streamline the management of identities across multiple applications and organizations. Its built-in federated identity framework allows an authenticated identity to be recognized, and enables the user associated with that identity to access information and services across domains. This, in turn, enables users to seamlessly and securely access multiple applications and services, creating unprecedented revenue growth, cost savings, and other opportunities for enterprises, while enhancing the user experience and improving operational efficiencies.

In addition to identity federation, Access Manager includes other capabilities for streamlining identity management:

- **Web SSO** allows users to sign on once to access information and resources across heterogeneous applications, platforms, and domains. This enhances security by streamlining the authorization process, improves the user experience by making it easier for users to access information and resources, and reduces support requirements for password resets and other password management services.
- **Centralized authorization services** provide centralized security policy enforcement, enabling organizations to consistently apply security policies across applications and domains.

Sun Java System Federation Manager

Sun Java System Federation Manager provides the capabilities to quickly and efficiently establish and extend trust. Sun's federation solution helps businesses view security as a way to increase revenue, ensure user privacy, and quickly integrate partners into business offerings without impacting the user experience or compromising the security and integrity of those offerings.

Federation Manager is deployed at a service provider site to provide users with more secure, private access to applications and services. It employs standard protocols, including SAML and Liberty, to create interoperability across many partner sites. Sun's federated solution brings a fresh approach to delivering federation services by helping service providers more efficiently leverage the core security and identity infrastructures of hub partners. Because it makes trusted domains easily extensible across vast networks of partners, Federation Manager can be used to create infinitely reusable application security mechanisms that enable diverse authentication and access solutions to work together seamlessly.

In this way, Federation Manager enables low-cost, secure federation solutions that can scale infinitely and be deployed easily by spoke partners.

- **Partner SSO** authenticates users and exchanges credentials and security tokens across partners in trusted domains. It leverages recognized authorities to identify users and determine which applications and services they may access, even across partners in different domains.
- **Account linking** connects user accounts across multiple security domains to create a seamless, yet highly secure, user experience in multiprovider service offerings.
- **Global logout** manages sessions across many partners to define when user interactions must be terminated. Federation Manager bases control on how sensitive an application is, and matches that control to the trust agreements deployed by partners.

Sun Java System Identity Manager Service Provider Edition

Sun Java System Identity Manager Service Provider Edition makes it possible for organizations to speed the development of new applications and services on a broad scale by using identity services as the basis for development. It applies a service-oriented architecture to identity management, replacing disparate identity administration schemes with consistent and reusable identity services. Scalable to millions of users, the solution also integrates easily with existing Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and Supply Chain Management (SCM) applications, as well as with existing identity and access management infrastructures.

In addition, Identity Manager Service Provider Edition includes a number of capabilities for streamlining identity administration in federated solutions:

- **Federated provisioning and synchronization services** help expedite the rollout and expansion of federated identity management capabilities by enabling companies to federate accounts and other data necessary to personalize the relationship across trusted partner networks. These services automate initial setup and ongoing management of federated accounts, including termination when the relationship ends.
- **Registration and self-administration services** speed time to market for portal applications by providing the Web service interfaces needed to quickly provision users and allow them to perform their own password resets, profile updates, and other everyday administrative tasks. These services support multiple languages including SPML and Java. Using these services not only reduces application development time, it cuts development and maintenance costs.

All Part of a Comprehensive Approach to Identity Management

Java System Access Manager, Federation Manager, and Identity Manager Service Provider Edition are part of a complete portfolio of identity management solutions that addresses every aspect of identity management, from provisioning users to auditing and reporting on access activities. Other components of Sun identity management are:

- **Sun Java System Identity Manager**
Java System Identity Manager provides complete capabilities for user provisioning and deprovisioning, password management, and identity data synchronization. A comprehensive solution for managing identity profiles and permissions, Identity Manager lowers risk on multiple levels, improving security, audit performance, and legislative compliance.
- **Sun Java System Directory Server Enterprise Edition**
Java System Directory Server Enterprise Edition delivers directory services, security/failover capabilities, and synchronization with Microsoft Active Directory, all in one directory solution. It provides the foundation for the entire enterprise identity infrastructure, using features such as fractional replication, multiple password policies, and flexible deployment to improve security.
- **Sun Java System Identity Auditor**
Java System Identity Auditor allows organizations to monitor and verify key identity controls, detect violations of those controls, and fully report on events. Through these capabilities, it enables repeatable, sustainable, and cost-effective compliance with internal and external regulatory requirements across applications.

Chapter 6

Federation at Work in the Real World: Three Examples

Three companies in very different industries rely on Sun identity management solutions for identity federation capabilities to enable the virtual enterprise.

Telecommunication: Multiple Services, Millions of Subscribers

The challenge: A large, international telecommunication provider hoped to drive revenue growth by expanding its portfolio of key revenue-generating services. By offering more services, the company could expand its user base and increase loyalty among existing users. However, meeting this challenge would require the company to deploy an identity management solution to unify the identities of several disparate business units and trusted service providers. Such a solution would have to deliver:

- High performance and scalability
- Open standards and protocols
- Rapid deployment
- Identity federation
- Reusability across many partners

The solution: The company chose Sun federated identity management to enable:

- Federation of accounts between identity provider and service provider
- A single, seamless sign-on to services with secure protection against identity theft and fraud
- Termination federation

The benefits: Subscribers can now quickly and easily leverage multiple services without being challenged to present authentication credentials over and over again. They can also leverage additional services that the provider is able to offer via trusted partners. The company is therefore now able to:

- Launch new offerings to an audience that is eager to consume them
- Enhance ease of use to attract new customers and increase satisfaction among existing ones
- Create perceived switching costs from the value of the combined services
- Improve customer service to reduce the risk of subscriber churn

Financial Services: A Robust Solution for Streamlined Vehicle Financing

The challenge: An aggregation management company saw an opportunity to collaborate with vehicle dealers and manufacturers to streamline the vehicle financing process. The company envisioned replacing a process that had historically been time-consuming and inconvenient for vehicle buyers with one that would be fast and simple. To make it work, the company needed a system that would link all parties, so they could share loan-related information in real time.

The solution: The aggregator used Sun federated identity management to provide federated SSO to their portal for vehicle dealers. Through this portal, dealers can exchange credit application data with manufacturers' finance operations.

The benefits: Support for Liberty Alliance standards means that partners can seamlessly link to increase interoperability and lower the cost of collaborating in the virtual enterprise. The solution provides the aggregator with 99.999 percent (five nines) availability, and scales to process 40 million transactions a year.

Automotive Manufacturing: Driving Simplified, Secure Relationships with Multiple Partners

The challenge: One of the largest automotive manufacturers in the world wanted to pave the way for more productive business relationships by streamlining its approach to identity management — specifically by eliminating its reliance on proprietary systems, improving its management of identity information from multiple directories, and reducing authentication requirements for access to applications within and outside the enterprise. As the first step in the process, the company sought out a solution that would simplify the way its employees access the services of its business partners.

The solution: The company initially deployed Sun federated identity management to enable employees to enjoy secure access to services from multiple business partners without having to use different passwords for different partner services. Specifically, more than 70,000 employees are now able to directly access 401(k) benefit information that resides behind a partner's firewall without having to log onto a separate Web site. The Sun solutions underlying this secure SSO capability provide the foundation for large-scale sharing of applications and resources with partners without having to adopt new authentication, directory services, or security technologies.

The benefits: The advantages of federated identity go beyond simplified business processes and improved service to employees. By adopting a proven, standards-based approach to federated identity management, the company gained the power and flexibility to infinitely expand its partner relationships and use them to pursue new opportunities — all without having to devote undue time and resources to managing identities in multiple directories.

Chapter 7

Conclusion

Identity federation dramatically streamlines and simplifies the process of sharing with trusted partners the identity data associated with users who share electronic access to information and resources across domains. By making it possible to extend user credentials and authorizations across traditional organizational boundaries, federation eliminates major logistic and economic obstacles to online collaboration. Federation enables today's virtual enterprise, providing a vehicle for unprecedented opportunities to deliver information, goods, and services online.

To learn more about identity federation, or to request additional information about Sun identity management solutions, visit www.sun.com/identity.

© 2005 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 USA

All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun Suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California.

Sun, Sun Microsystems, the Sun logo, Java, and the Network is the Computer are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun written license agreements.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.277-7015(b)(6/95) and DFAR 227.7202-3(a). DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.