

Network Identity: Unlocking the Value of Web Services

How Identity Management Can Make Web Services More
Useful to Your Users — and More Powerful for Your Business



Table of Contents

- Executive Summary**1
- The Identity Crisis**2
- Sun's Solution: An Open Approach to Identity-Enabled Web Services**4
 - Comprehensive Identity Management Capabilities 4
 - Standards-Based, End-to-End Identity Infrastructure 5
- The Enabling Technology**6
- The Sun Advantage**8
- Conclusion**10
 - For More Information10

Chapter 1

Executive Summary

Identity management has become a critical requirement for every enterprise with a Net presence. In fact, the quality of your network identity technology can determine the value of your Web services.

If you can monitor and control who is accessing your Web services, you can personalize the services delivered to consumers. You can authorize specific individuals to access specific resources at specific times. You can provide a convenient and consistent user experience across applications and Web sites. You can establish trust relationships with intermediaries and providers. Without identity management, the value of your Web services — to both end users and your business — is limited.

Yet implementing an effective identity management solution can be a complex challenge for most organizations today. The increasing use of Web services; the growing number and diversity of users; the need to provide network resources to suppliers and business partners as well as employees and customers; and the proliferation of access devices and technologies all make identity management more difficult.

By implementing a comprehensive identity management solution now, you can gain the upper hand in using Web services to create business advantages. You can position your organization to profit from better customer service and avoid the expense, risk, and complexity of piecemeal solutions.

This paper briefly summarizes the trends that are making identity management more critical than ever today. It describes Sun's approach to comprehensive, standards-based identity management; identifies the key products, solutions, and technologies that can deliver on the demands; and provides examples of how Sun has successfully deployed identity management solutions.

Chapter 2

The Identity Crisis

Identity is more than just a name and a face. Identity includes the vital information that enables you to create a user profile, tailor your Web services to specific consumers, and provide privacy and security. And because each user identity is in a constant state of flux, it must also be updated, managed, controlled, and protected — continuously. As more and more business is conducted over the Web, it becomes increasingly difficult to keep pace with the requirements of identity-based Web services, yet it is also increasingly important to do so.

Following are just a few of the trends that have increased the need for more effective identity management today.

- **Upward Spiral in Demand for Identity-based Web Services:** Today's end users — whether internal employees, customers, suppliers, or other business partners — expect to have the right network resources available to them at the right times, regardless of their physical location or the access device they are using. Identity management is the key requirement for delivering customized, anytime/anywhere access to Web services. In short, it is no longer who you know, but how well you know them.
- **Increasing Organizational and IT Complexity:** Growth, mergers and acquisitions, geographical expansion, new alliances, and changing supply relationships all increase the complexity of identity management. But organizational changes also exponentially increase the complexity of the IT environment, making the task of identity management almost unmanageable. The profusion of policies, platforms, systems, and controls can lead to:
 - Inefficient, incompatible “islands of information” with high support costs
 - Multiple passwords for multiple services, leading to end-user frustration
 - Poor IT asset management

- Lack of centralized management and reporting
- Limited flexibility and scalability
- Greater exposure to security risks
- **Tougher Regulatory Compliance Requirements:** Meeting the demands of regulatory agencies is more difficult than ever. With legislation such as HIPAA, the EU Data Protection Directive, the GLB Act, and the Sarbanes/Oxley Act, it is increasingly important to make sure that only authorized people have access to sensitive resources, and that the activities of those who have access are carefully administered, monitored, and controlled. Your organization's identity management technology is central to your ability to meet compliance requirements and determine which users can use which resources.
- **Growing Burden on End Users, Administrators, and Developers:** An inability to manage network identity adversely impacts three critical groups:
 - *End users* can experience frustration at not receiving the personalized services they require in an acceptable timeframe and may forego doing further business with the company.
 - *Administrators* can become overwhelmed with the challenge of manually satisfying user requests for resources, and help desks can become swamped with calls that cannot be answered in a timely basis.
 - *Developers* who are required to implement security policy as they write applications may find it too cumbersome to manually keep track of which users have access to which resources.

The net results of inadequate identity management?

- Lower end-user satisfaction rates
- Lower return on investment (ROI) for IT assets
- Higher administrative and development costs for Web services
- Exposure to financial penalties for regulatory noncompliance
- Weaker security
- Inability to react quickly to new customer, employee, and partner requirements

Chapter 3

Sun's Solution: An Open Approach to Identity-Enabled Web Services

While the problems of inadequate identity management are easy to identify, unfortunately, solutions are not. Most companies today must deal with the realities of inconsistent business and security processes, disjointed applications and Web sites, heterogeneous IT environments, multiple user registries and directories, and incompatible security management technologies.

Sun's solution is to bring an end-to-end, standards-based approach to managing secure access to Web resources — within the enterprise or across business-to-business value chains.

Comprehensive Identity Management Capabilities

Sun has identified seven key capabilities that an identity management solution must deliver:

- **Access Management:** The identity management solution should provide a common, standards-based authentication and authorization infrastructure to replace ad hoc and application-specific methods. It should provide capabilities such as:
 - Authentication that challenges the users to provide credentials
 - Single-sign-on functionality so that users can authenticate once and access multiple authorized resources
 - Password management services
 - Accounts lockout for early intrusion detection
 - Public Key Infrastructure (PKI) support for stable, scalable security

- A policy framework for defining, evaluating, and managing security policies
- Detailed reporting capabilities so that administrators can analyze user activity, traffic patterns, violations, and attempts at tampering
- **Identity Administration:** The identity management solution should provide simple yet powerful tools for user management and administration of identities and policies, with browser-based administration of user identities, policies, and services. In addition, it should provide delegated administration capabilities that allow specific administrative tasks to be delegated to the authority who is closest to the user community (employees, customers, suppliers, or partners). This way, administrators can be broken out by organizational structure so that each department can manage its own users.
- **Federation Management:** Because the Internet has become a prime vehicle for business, community, and personal interactions, the identity management solution should provide a system to enable users to aggregate all of their various identities into one network identity. This system is called identity federation. It enables users to log in once at one service provider's site and then go to an affiliated site without having to reauthenticate or reestablish their identity.
- **Service Management:** The identity management solution should provide a way to customize and register management parameters for external applications, such as channels in a portal server or mail quotas on an e-mail server.
- **Directory Services:** An organization's directories (repositories of customer, employee, and supplier information) are the raw material for building an infinite variety of personalized, integrated services that can be made Web- or portal-accessible through single sign-on. An identity management solution should be based on directory services to provide a means for handling identity throughout the computing environment.
- **Identity Synchronization:** The identity management solution should provide bidirectional synchronization of directory information so that when changes to an identity are made to one application, other applications in the enterprise are automatically updated.
- **Identity Provisioning:** The identity management solution should include or integrate easily with identity provisioning solutions, which helps to automate the entire administrative process, dramatically cutting the time and cost of identity management.

Standards-Based, End-to-End Identity Infrastructure

Integration of systems, channels, business processes, applications, and solutions is one of the most difficult problems organizations face today, and lack of integration is one of the key obstacles to implementing an effective identity management solution. Sun's approach is to leverage industry standards in its products and industry best practices in its services. To facilitate "integratability" and interoperability, Sun leverages standards at every level — from the eXtensible Markup Language (XML), Simple Object Access Protocol (SOAP), and Java™ technology to Liberty Alliance standards for federated identity.

Chapter 4

The Enabling Technology

Sun offers the combination of standards-based hardware and software products, services, best practices, and expertise to help organizations implement sophisticated and effective identity management solutions. Core offerings include:

- **Sun™ ONE Identity Server:** The Sun ONE Identity Server 6.0 is a standards-based software product that can help your organization manage secure access to Web-based applications. It provides scalable access management services that help secure the delivery of business information, improve the user experience, and put a federated identity framework in place so that you can create new revenue opportunities through enhanced affinity relationships with business partners and customers. It is the ideal platform for consolidating authentication, authorization, and single sign-on capabilities, and provides the ability to administer user accounts and security policy for access control.
- **Sun ONE Directory Server:** The Sun ONE Directory Server provides a central repository for storing and managing identity profiles, access privileges, and application and network resource information. Information stored in the Sun ONE Directory Server can be used for the authentication and authorization of users to enable secure access to enterprise and Internet services and applications. The software helps improve security and protection of key corporate information assets by ensuring that appropriate access control policies are enforced across all communities, applications, and services on a global basis.
- **Sun ONE Meta-Directory:** Sun ONE Meta-Directory consolidates and integrates identity information spread throughout the enterprise into a single profile. In addition, Sun ONE Meta-Directory helps to improve the quality of information within the diverse applications through bidirectional synchronization.

- **Liberty Alliance Specifications:** The Liberty Alliance is a global industry alliance and the largest body to drive open, neutral standards for federated network identity management and services. The Liberty Alliance delivers technical interoperability through the development and maintenance of open technical specifications, partnerships to drive interoperability and convergence, and proven interoperability between implementations. It also delivers business interoperability through the development of business frameworks, guidelines, and best practices. The Liberty Alliance 1.1 specifications were released on January 15, 2003. For more information, visit projectliberty.org.
- **Sun Infrastructure Solution for Network Identity:** The Sun Infrastructure Solution for Network Identity integrates software, systems, storage, and services into comprehensive solutions that can enable your organization to quickly begin implementing an open, end-to-end secure network identity infrastructure today. It provides identity management, identity and service provisioning, and application security, and is sized for enterprise deployments scaling from 5000 to 250,000 user identities — all backed by a scalable reference architecture, network identity design and implementation methodologies, and Sun high-performance servers in integrated building-block start-up configurations. For more information, visit sun.com/software/sunone/whitepapers.html.
- **Lifecycle Service and Support:** Sun Services offers a variety of programs and expert consulting services that can help your company implement an end-to-end identity management solution. For example, the Sun ONE Services Suite helps you architect, implement, and manage a complete Sun ONE platform architecture. In addition, Sun Network Identity Services give you access to Sun consultants who can play a key role in the execution of your network identity strategy with technical expertise in Sun ONE software, Java technology, security technology, and architecture services.

Chapter 5

The Sun Advantage

Many vendors today provide identity management solutions and claim to deliver outstanding results. As the inventor of many of the technologies that power the network today, and the thought leader of the Internet era, Sun is uniquely qualified to deliver on the demands of identity management. Among the reasons:

- **Depth and Breadth of Technical Expertise:** With over 20 years of technical innovation and product excellence, Sun can provide direct access to some of the best and brightest technical professionals in the industry. Sun consultants have a combination of deep technical knowledge and broad industry experience that few vendors can match.
- **Partnership-oriented Business Model:** Since its inception, Sun has focused on providing industry-leading platform infrastructure and partnering with best-in-class solution providers whose products complement and add value to the Sun platform. Today, Sun works collaboratively with hundreds of established and up-and-coming independent software vendors (ISV) and systems integrators. Together, Sun and its best-of-breed partners can address your specific identity management needs and tailor a complete, cost-effective solution.
- **Integrated Infrastructure Solutions:** The Sun Infrastructure Solution for Network Identity helps cut the cost, risk, and deployment timeframes of your identity management solution. This integrated solution brings together the products, partnerships, and services you need to design, develop, and implement a complete solution. And you can test your solution before you invest in products at Sun's global network of iForceSM Solution Centers.

- **Successful Deployments:** Sun has an extensive track record of successful identity management solution implementations worldwide. Sun's own internal identity management projects provide excellent references. One example is the Sun Identity Management Service (SIMS), an internally facing, global employee information directory service. SIMS provides a centralized repository of information that can be used for authenticating or authorizing employee access to all enterprise services and applications. It aggregates information about more than 50,000 employees, interns, and contingent workers (name, employee ID, phone number, calendar URL, e-mail addresses, and more), drawing from Sun's HR implementation and other applications. Another example is the Sun Access Management Service (SAMS), an externally facing, global customer/partner information directory service. This service is intended to replace Sun's eCR (e-Business Customer Registry) and help eliminate the need for multiple customer/partner data repositories. When integrated with the My SunSM portal, SAMS will establish a single sign-on facility for customers and partners, along with one repository of user information. It will integrate 18–20 applications, representing approximately 30 percent of Sun's online business activity.

Chapter 6

Conclusion

Network identity is the heart and soul of Web services. With the right network identity technology, you can personalize content and services, control access to resources, provide a consistent user experience across applications and Web sites, and establish trust relationships with intermediaries and providers. Without the right solution, you risk:

- End-user frustration
- Poor utilization of IT assets
- Higher administrative and development costs
- Inability to meet regulatory compliance requirements
- Ineffective security
- A diminished reputation for quality of service

By implementing Sun's comprehensive identity management solution now, you can transform identity management from a challenge and a problem into a business advantage.

For More Information

For additional details about any of the products or services mentioned in this document, please call your local Sun sales representative or visit Sun's Web site at sun.com.

SUN™ Copyright 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054 U.S.A. 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. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, iForce, Java, and My Sun are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. 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's 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 252.227-7015(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.

SUN™ Copyright 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, Californie 95054 Etats-Unis. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, iForce, Java, et My Sun sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REpondre A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



Please
Recycle



Adobe PostScript

Learn More

Get the inside story on the trends and technologies shaping the future of computing by signing up for the Sun Inner Circle program. You'll receive a monthly newsletter packed with information on the latest innovations, plus access to a wealth of resources. Register today to join the Sun Inner Circle Program at sun.com/joinic.

To receive additional information on Sun software, products, programs, and solutions, visit sun.com/software.

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 800 786-7638 or +1 512 434-1577 Web sun.com



Sun Worldwide Sales Offices: Africa (North, West and Central) +33-13-067-4680, Argentina +5411-4317-5600, Australia +61-2-9844-5000, Austria +43-1-60563-0, Belgium +32-2-704-8000, Brazil +55-11-5187-2100, Canada +905-477-6745, Chile +56-2-3724500, Colombia +571-629-2323, Commonwealth of Independent States +7-502-935-8411, Czech Republic +420-2-3300-9311, Denmark +45 4556 5000, Egypt +202-570-9442, Estonia +372-6-308-900, Finland +358-9-525-561, France +33-134-03-00-00, Germany +49-89-46008-0, Greece +30-1-618-8111, Hungary +36-1-489-8900, Iceland +354-563-3010, India-Bangalore +91-80-2298989/2295454; New Delhi +91-11-6106000; Mumbai +91-22-697-8111, Ireland +353-1-8055-666, Israel +972-9-9710500, Italy +39-02-641511, Japan +81-3-5717-5000, Kazakhstan +7-3272-466774, Korea +822-2193-5114, Latvia +371-750-3700, Lithuania +370-729-8468, Luxembourg +352-49 11 33 1, Malaysia +603-21161888, Mexico +52-5-258-6100, The Netherlands +00-31-33-45-15-000, New Zealand-Auckland +64-9-976-6800; Wellington +64-4-462-0780, Norway +47 23 36 96 00, People's Republic of China-Beijing +86-10-6803-5588; Chengdu +86-28-619-9333; Guangzhou +86-20-8755-5900; Shanghai +86-21-6466-1228; Hong Kong +852-2202-6688, Poland +48-22-8747800, Portugal +351-21-4134000, Russia +7-502-935-8411, Singapore +65-6438-1888, Slovak Republic +421-2-4342-9485, South Africa +27 11 256-6300, Spain +34-91-596-9900, Sweden +46-8-631-10-00, Switzerland-German 41-1-908-90-00; French 41-22-999-0444, Taiwan +886-2-8732-9933, Thailand +662-344-6888, Turkey +90-212-335-22-00, United Arab Emirates +9714-3366333, United Kingdom +44 0 1252 420000, United States +1-800-555-9SUN or +1-650-960-1300, Venezuela +58-2-905-3800 7/03 R1.0