# THE COMPLETE BUYER'S GUIDE for IDENTITY MANAGEMENT

August 2006

**Abstract**

If you are currently evaluating identity management solutions, this guide will provide the information and tools to help you make the right decision. In the first section of the guide, you will find a business primer that examines the role of identity management in addressing today's business opportunies and challenges as well as discusses the characteristics of an effective solution. In the second section of the guide, you will find helpful decision-making tools you can use to ensure that your selection is best suited to your business needs and technology environment.

# Table of Contents

**A New Business Paradigm**

For more and more users, the network is becoming the nexus of engagement. As the hunger for online services grows, a new set of requirements emerges for users and businesses alike:

- Users' expectations for more choices, along with better content and services, will only continue to increase.
- Businesses are eager to meet those expectations by making new applications and services available.
- Competitive pressures are pushing enterprises to generate new lines of revenue and new customers through rapid delivery of new services.
- Businesses must also focus on keeping the current customer base happy and loyal by enhancing existing service offerings and delivering an outstanding customer experience.

Chapter 1

# Executive Overview

The Participation Age is ushering in a new era of business growth and opportunity. All around us—in the enterprise, in the developer community, between businesses and consumers, and in the public sector—people are interacting and collaborating in ways that were impossible just a few years ago. These new capabilities have quickly created new expectations for today's enterprise.

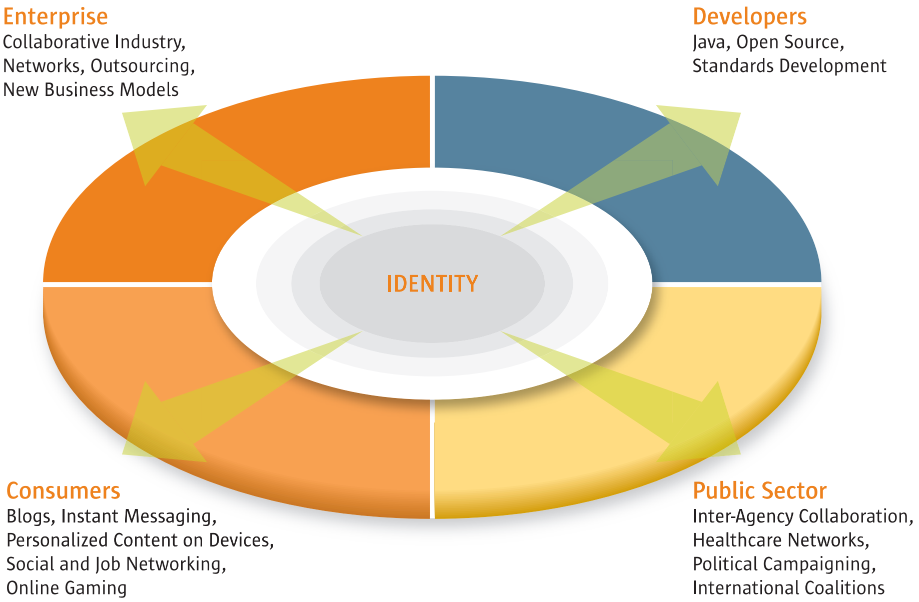
Enterprise
Collaborative Industry, Networks, Outsourcing, New Business Models
Developers
Java, Open Source, Standards Development
IDENTITY
Consumers
Blogs, Instant Messaging, Personalized Content on Devices, Social and Job Networking, Online Gaming
Public Sector
Inter-Agency Collaboration, Healthcare Networks, Political Campaigning, International Coalitions

Figure 1. The Participation Age

For more and more users, the network is becoming the nexus of engagement. As the hunger for online services grows, a new set of requirements emerges for users and businesses alike:

- Users' expectations for more choices, along with better content and services, will only continue to increase
- Businesses are eager to meet those expectations by making new applications and services available
- Competitive pressures are pushing enterprises to generate new lines of revenue and new customers through rapid delivery of new services
- Meanwhile, businesses must also focus on keeping the current customer base happy and loyal by enhancing existing service offerings and delivering an outstanding customer experience

All together, this Participation Age presents a new paradigm for the way people deploy, access, and use networked information, applications, and resources. Barriers

**What's Included**

- Business Primer
- Buyer's Checklist
- Industry Standards Fact Sheet
- Frequently Asked Questions
- Glossary

to access must fall away, freeing users and businesses to take the online experience to the known limits and beyond.

This shift brings about a tremendous opportunity for businesses, yet it also requires ubiquitous access in which user identity is an essential enabler. Participation, after all, requires trust. And trust requires identity. Today, there is an undeniable, urgent need for businesses and individuals to know who's on the other end of their transactions, to trust that entity and to be confident that the information they share is safe with them. Identity management holds the answers to these needs and becomes an enabler of the Participation Age.

By providing everything required to effectively manage identities, both within the enterprise and across traditional business boundaries, identity management makes it possible to securely deliver the right resources to the right people at the right time and in the right context. In this way, it can enable businesses to dramatically accelerate growth while leaving competitors far behind—and do so safely and securely.

## What's Included

- **Business Primer.** A look at identity management trends, opportunities and solutions.
- **Buyers Checklist**. What to look for when evaluating solutions.
- **Industry Standards Fact Sheet.** Reference information for key initiatives.
- **Frequently Asked Questions.** Answers to the questions that come up most often.
- **Glossary.** Definitions of industry terms.

**Priorities of Today's Executives**

- How do we increase business productivity and reduce costs while at the same time get to market faster?
- How do we securely provide access to information, applications and systems for our customers, partners, and employees and still comply with legal mandates and company policies?
- How do we improve the customer experience by providing secure access to information and services while also expanding selling opportunities?

Chapter 2

# Business Primer: Identity Management Trends, Opportunities and Solutions

## Increasing Business Value While Reducing Costs and Risks

In the Participation Age, identity management solutions must address multiple business goals and serve competing, changing requirements. Consider the priorities of today's executives:

- How do we increase business productivity and reduce costs while at the same time get to market faster?
- How do we securely provide access to information, applications and systems for our customers, partners, and employees and still comply with legal mandates and company policies?
- How do we improve the customer experience by providing secure access to information and services while also expanding selling opportunities?

These are just a few of the conflicting demands that companies must meet today.

Doing business electronically is a requirement for competing in today's business environment. The result is a significant increase in the number and variety of users who require access to critical information resources. Access takes many forms. It can mean providing customer access to self-help, information, and online services to improve revenue results at a lower cost. And access can create secure workplaces where employees and partners work together to get new products and services to market faster. These are just two examples. The challenge is to open up the enterprise to new ways of conducting business while at the same time ensuring that information assets remain secure and privacy is protected.

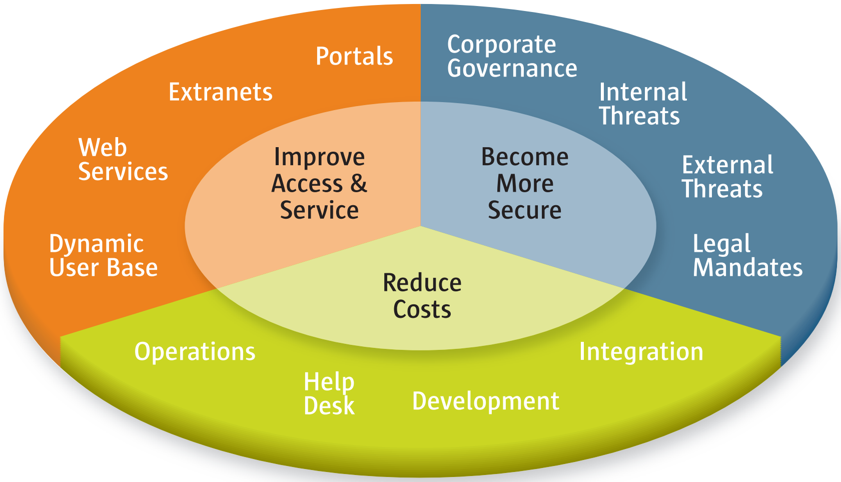

Figure 2. Participation means addressing multiple, conflicting business goals

**Cost Reduction vs. Risk Reduction**

- *Cost Reduction*
  Enterprises are looking for a solution that brings a higher degree of efficiency, leading to faster time-to-market, while also helping to reduce ever-increasing demands on help desks and IT staffs.

- *Risk Reduction*
  One of the most powerful drivers for identity management is to ensure that corporate information assets and privacy are well-protected while also providing greater access to internal employees and outside parties.

## Cost Reduction

Cost reduction has become a fact of life for business, but it cannot be achieved at the expense of business results. Enterprises are looking for a solution that brings a higher degree of efficiency, leading to faster time-to-market, while also helping to reduce ever-increasing demands on help desks and IT staffs.

The online business requires a cost-effective identity infrastructure that meets the needs of employees, partners, and customers. This infrastructure must support "anytime, anywhere" access with security, dynamic assembly and disassembly of teams, single sign-on, and easy integration with existing enterprise applications. And most importantly, it must be easily adaptable and scalable so the business can quickly take advantage of new opportunities.

## Risk Reduction

One of the most powerful drivers for identity management is to ensure that corporate information assets and privacy are well-protected while also providing greater access to internal employees and outside parties.

Around the world, concern about security and privacy has resulted in the passage of numerous laws and regulations, including the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act, the Gramm-Leach-Bliley Act, the European Data Protection Directive, and the Canadian Privacy Act. Businesses are challenged to comply with these requirements while simultaneously speeding time-to-market, improving quality-of-service, and increasing profit.

Providing more and broader access and greater security while also achieving faster time-to-market with lower costs demands a unified identity management infrastructure.

## Building Value on a Secure and Compliant Identity Infrastructure

A secure and compliant identity infrastructure can help your business to:

- Simultaneously open and secure access to your information
- Expand and enhance partner networks by sharing services beyond business boundaries
- Reduce time and costs associated with security and compliance by automating relevant activities and processes
- Ensure regulatory compliance through centralized control, complete visibility into access privileges, and consistent enforcement of identity management policies
- Continually ensure that only authorized users have access by automatically detecting and reacting to potential risks
- Achieve cost savings and competitive advantages by streamlining operations and

automating business processes

- Create new revenue opportunities by using collaborative partner networks to efficiently and securely deliver services online

A comprehensive identity management solution provides everything required to create a secure and compliant identity infrastructure by addressing the 4 A's of identity management:

**Authentication—Quickly verify user identities**

- Authenticate and authorize all user requests for secure applications and services with one integrated solution, regardless of where the requests come from or where the applications and services reside

**Authorization—Control user access**

- Ensure that only authorized users may access protected resources based on specific conditions, and that they are granted access only after proper authentication
- Provide role- and rule-based authorization for centralized policy enforcement

**Administration—Manage users and assets**

- Provide a highly scalable deployment option for incorporating secure identity administration (e.g., registration, self-service, delegated administration) and federated provisioning capabilities into extranet-facing applications and portals
- Accelerate the introduction of new, revenue-generating applications and services without having to compromise on security or compliance controls

**Auditing—Automatically document what happened**

- Audit identities across enterprise applications and systems
- Eliminate manual effort and enable continuous compliance by automatically scanning for, identifying, and fixing policy violations
- Provide a clear trail of access requests so auditors can identify and correct potential regulatory violations
- Include packaged policies as a starting point to help achieve compliance faster

**The 4 A's of Identity Management**

- *Authentication*
  Quickly verify user identities
- *Authorization*
  Control user access
- *Administration*
  Manage users and assets
- *Auditing*
  Automatically document what happened

## Assessing Sun Identity Management

Sun identity management solutions are designed to meet the complex, demanding requirements of today's enterprise. They address the 4 A's of identity management —authentication, authorization, administration, and auditing—with capabilities for provisioning, access management, directory services, federation, and auditing. All Sun identity management solutions are easily integrated with heterogeneous IT environments, so they're quick and cost-effective to deploy and maintain.

**What Analysts and Community Leaders Say about Sun Identity Management**

- Forrester ranked Sun as #1 in both current offering and market presence.
- Gartner positioned Sun in the Leaders Quadrant of its "Magic Quadrant for User Provisioning."
- Ovum awarded Sun 21 out of 25 stars for its identity management solutions, 10 out of 10 stars for vision and directory and meta-directory services, and eight out of 10 stars for provisioning/identity administration and federation.

Here's what analysts and identity community leaders have said about Sun identity management:

**Forrester ranked Sun as #1 in both current offering and market presence.**
"Sun stands out as functionally superior and sets the gold standard for user account provisioning... Sun Microsystems is a market leader for a reason—its product delivers superior provisioning functionality with the highest ease of use."
*Forrester Wave: User Account Provisioning, Q1 2006*

**Gartner positioned Sun in the Leaders Quadrant of its "Magic Quadrant for User Provisioning."** Those in the Leaders Quadrant demonstrate balanced progress and effort in all execution and vision categories. "Sun's actions raise the competitive bar for all products in the market, and they change the course of the industry."
*Magic Quadrant for User Provisioning, 1H06—Roberta Witty, Ant Allan,*
*Ray Wagner, 25 April 2006*

**Ovum awarded Sun 21 out of 25 stars for its identity management solutions, 10 out of 10 stars for vision and directory and meta-directory services, and eight out of 10 stars for provisioning/identity administration and federation**. "Sun leads because of their comprehensive vision, which will enable them to grow with the market without fundamentally changing their concepts... Sun has proven ability to provide the foundation for mega-scale identity management projects."
*Ovum, Identity Management: Time for Action, July 2005*

These are some of the specific advantages of working with Sun:

**Comprehensive Sun IT Platform.**
Sun identity management is part of the Sun Java™ Enterprise System, a revolutionary, open-source, subscription-based approach to integrated infrastructure software systems that reduces IT costs and complexity. Sun Java Enterprise System runs as part of the Solaris Enterprise System, the only comprehensive and open infrastructure software platform available today.

**Freedom of Choice.**
Sun's partnerships with leading system integrators means that organizations can work with the deployment specialists of their choice to roll out Sun identity management solutions. Sun's commitment to open source software means that software integrators and their customers have complete access to Sun software for development. In addition, Sun offers product and suite pricing models to optimally match license pricing with specific needs.

**Technology Innovations.**
Sun identity management solutions are all based on open standards to make them easy to integrate with existing technology infrastructures, demonstrating Sun's leadership in developing and promoting technology standards. Sun was also the first to

**Advantages of Working with Sun**

- Comprehensive Sun IT Platform
- Freedom of Choice
- Technology Innovations
- Return on Investment

introduce an integrated provisioning and identity auditing solution; this innovative approach extends identity management-driven business improvements to automatically address key compliance issues.

**Return on Investment.**
The open architecture that characterizes Sun identity management makes the process of applying identity management to numerous networked resources faster and simpler. With deployment time reduced from months to weeks, ROI payback can be measured in months instead of years. Sun identity management solutions also deliver continuing financial improvement by reducing ongoing administration costs up to 30%.

**Identity Management Offerings**

- *Identity Lifecycle Management and Identity Auditing*
  Sun Java™ System Identity Manager
- *Authorization and Authentication*
  Sun Java™ System Access Manager
- *Federation*
  Sun Java™ System Federation Manager
- *Directory Services*
  Sun Java™ System Directory Server Enterprise Edition

## Exploring Sun's Identity Management Offerings

Sun's comprehensive set of identity management solutions enables organizations to securely manage, protect, store, verify, and share data both internally and across extranets. These products are designed to provide scalability that can enable organizations to accommodate more users and resources without requiring an entirely new investment in identity management capabilities.

**Identity Lifecycle Management and Identity Auditing: Sun Java™ System Identity Manager.** Identity Manager is the first identity management solution to combine identity lifecycle management and compliance automation in one solution. Within this solution, identity lifecycle management keeps track of what a user should have access to, while identity auditing keeps track of what the user does have access to —and makes sure that the two are aligned. This makes it possible to prevent many compliance violations and to quickly remediate violations when they do occur.

**Authorization and Authentication: Sun Java™ System Access Manager.** Access Manager delivers a single solution for authorizing and authenticating all user requests for secure applications and services—whether they come from within the organization or from an external partner or vendor through an extranet. By combining open, standards-based access control with secure access capabilities such as single sign-on, this solution minimizes the security and business risks associated with conducting business more openly in the Participation Age.

**Federation: Sun Java™ System Federation Manager.** Federation Manager makes the process of integrating with partners easily repeatable. Using features such as extranet single sign-on to authenticate users across domains, Federation Manager enables organizations to collaborate securely with a virtually infinite number of business partners without having to create a new secure infrastructure for collaboration every time.

**Directory Services: Sun Java™ System Directory Server Enterprise Edition.** Directory Server Enterprise Edition is a secure, highly available, easy-to-manage directory solution that streamlines the management of diverse identities from intranet and extranet sources. It delivers seamless integration with Microsoft Active Directory via on-demand password synchronization between Microsoft Windows environments and the Directory Server environment.

## Key Business Benefits

By reducing risk and increasing security, Sun identity management solutions:

- Protect sensitive information and resources from internal and external threats in the online global economy
- Make it easier to tackle today's tremendous regulatory compliance challenges with

**Delivering Measurable Results**

- Business Acceleration
- Revenue Generation
- Increased Productivity
- Improved Security and Compliance

robust auditing and reporting capabilities

- Empower organizations to deliver open, secure access to customers, suppliers, and partners through broad support for federated identity management and Web services

## Improving Real-World Results with Sun Identity Management

Sun identity management has delivered measurable results in key areas to a broad range of organizations in both the private and public sectors. Here are just a few examples:

### Business Acceleration

- Henkel: new-technology implementation in months instead of years
- Lake Superior State University: instant access to campus systems
- Western Michigan University: accelerated provisioning of new students

### Revenue Generation

- T-Mobile: Rapid access to new services for 20 million subscribers
- RouteOne: Acceleration of loan process for 40 million transactions annually

### Increased Productivity

- Caremark: 80% reduction in administrative staff

### Improved Security and Compliance

- ADP: integration of processes to streamline regulatory compliance efforts
- DaimlerChrysler: centralized directory to help meet requirements of privacy laws
- Athens International Airport: immediate access to secure applications

**Buyer's Checklist Contents**

Chapter 3

# Key Considerations for Evaluating Identity Management Solutions

## Buyer's Checklist for Identity Management

As you evaluate various identity management solutions, use this checklist to compare key architecture components and designs along with features and functions available in the solutions under review.

### Identity Lifecycle Management and Auditing

| AUTOMATED PROVISIONING | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution create, update, and delete user accounts across the enterprise environment, including Web-based and legacy systems and apps? | ✓ | |
| Is the solution Web-based and available to administrators from any Web browser? | ✓ | |
| Is the solution designed to support users both inside (employees) and outside (partners, suppliers, contractors) the enterprise? | ✓ | |
| Can you easily and quickly find a user (or a group of users) and view their access privileges? | ✓ | |
| Does the solution allow you to instantly revoke all of a user's access privileges? | ✓ | |
| Does the solution leverage existing infrastructure (e-mail, browsers) to facilitate automated approvals for account creation? | ✓ | |
| Does the solution offer an automated approval mechanism with zero client footprint? | ✓ | |
| Does the solution provide the flexibility to map to your existing business processes? | ✓ | |

**Buyer's Checklist Contents**

| AUTOMATED PROVISIONING | SUN | OTHER VENDOR |
|---|---|---|
| If you answered yes to the previous question:<br>Are serial approval processes supported?<br>Are parallel approval processes supported? | <br>✓<br>✓ | |
| Does the solution provide automatic approval routing to persons appropriate to the system access requested (e.g., system owners) and organizational structure (e.g., managers)? | ✓ | |
| Can the solution dynamically determine routing of approvals based on defined organizational information (for example, real-time look up in Microsoft Active Directory to determine who the user's manager is and route approval to the manager)? | ✓ | |
| Does the solution allow delegation of approval authority to another approver (or multiple approvers)? | ✓ | |
| Can the solution automatically escalate a request to an alternative approver if allotted time elapses? | ✓ | |
| Can the solution request information from applications or data stores during the approval process? | ✓ | |
| Can the solution support rule-based routing of approvals? | ✓ | |
| Can the solution require automated approvals for deleting or disabling accounts? | ✓ | |
| Can the solution require automated approvals for changing account values? | ✓ | |
| Does the solution provide the ability to request information from approval participants to define account-specific information during the process? | ✓ | |
| Does the solution support creating custom approval screens and keeping them compatible in the upgrade process? | ✓ | |
| Can the solution fully automate the routine identity management processes in your environment? | ✓ | |

### Buyer's Checklist Contents

| AUTOMATED PROVISIONING | SUN | OTHER VENDOR |
|---|---|---|
| Can added accounts for new users in an authoritative source (e.g., HR database, directory) drive automated approvals and account creation? | ✓ | |
| Can changes in user status (e.g., job promotion captured in HR system) automatically drive changes in user access privileges? | ✓ | |
| Can information in an HR database on employees departing the organization be used to completely and automatically delete all access privileges on the day of departure? | ✓ | |
| Can the above processes be fully automated for large groups of users in addition to individuals (e.g., when an acquisition closes or a layoff occurs and a large group of users requires automated action)? | ✓ | |
| Will the solution detect manual changes made in managed systems and automatically respond? | ✓ | |
| When changes are detected, can the solution alert/notify designated personnel of access rights changes made outside the provisioning system to verify if changes are legitimate? | ✓ | |
| Once detected changes are approved, will the solution automatically update itself to include those changes? | ✓ | |
| Can the solution filter manual changes made on target systems so that only relevant identity changes trigger alerts? | ✓ | |
| If a detected account is not legitimate, can the solution automatically suspend the account? | ✓ | |
| Can the solution be used to enforce privacy policy? | ✓ | |
| Does the solution support role-based access control? | ✓ | |
| Does the solution support assignment of users to multiple roles? | ✓ | |
| Does the solution support the assignment of users to hierarchical or inherited roles? | ✓ | |

| AUTOMATED PROVISIONING | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution provide the ability to specify exclusionary roles that prevent certain roles from being assigned a conflicting role? | ✓ | |
| Can the solution assign resource account attribute values with the role? | ✓ | |
| Does the solution allow roles to be defined at any time, or not at all, rather than requiring role definitions prior to implementation? | ✓ | |
| Does the solution enable you to leverage key information systems in your environment as a source of authority on identity information to drive automated provisioning (e.g., detect new employees added to PeopleSoft and automate provisioning based on that change)? | ✓ | |
| Can the solution assign users to more than one role? | ✓ | |
| Can the solution assign users' individual access rights in addition to a role? | ✓ | |
| Does the solution dynamically and automatically change access rights based on changes in user roles? | ✓ | |
| Can the solution generate unique user IDs consistent with corporate policies? | ✓ | |
| Does the solution support rule-based access control that allows provisioning rules to be set and enforced on roles, users, organizations, and resources as needed in order to align with business needs? | ✓ | |
| Is the solution easy to use for both end-users and administrators? | ✓ | |
| Is the solution highly scalable to adapt to growth in users, applications, and access methods? | ✓ | |
| Does the solution work securely over WANs and across firewalls? | ✓ | |

**Buyer's Checklist Contents**

| AUTOMATED PROVISIONING | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution provide an interface to third-party workflow management applications? | ✓ | |
| Does the solution allow resource groups (such as an NT group) to be created from the interface? | ✓ | |
| Does the solution provide directory management capabilities, specifically the ability to create, update, and delete organizational units and directory groups? | ✓ | |
| Does the solution support pass-through authentication where a user can be validated by a managed user account? | ✓ | |
| Does the solution support all of the leading database servers and application servers? | ✓ | |
| Does the solution support provisioning to Mainframe security managers such as Top Secret, RACF, and ACF2? | ✓ | |
| Does the solution support provisioning to heterogeneous ERP environments including SAP and Oracle Applications? | ✓ | |
| Does the solution support provisioning to non-digital assets (e.g., mobile phones, badges, etc.)? | ✓ | |

| PASSWORD MANAGEMENT | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution provide password strength enforcement? | ✓ | |
| **If you answered yes to the previous question:**<br>Does the solution provide a password exclusion dictionary?<br>Does the solution provide a password history store to prevent re-use of old passwords? | <br>✓<br>✓ | |
| Does the solution allow users to manage their own passwords, including resetting passwords? | ✓ | |
| Can policy be set on challenge authentication questions (e.g., how many responses are required based on a user's organization)? | ✓ | |

**Buyer's Checklist Contents**

| PASSWORD MANAGEMENT | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution support customers providing their own self-service challenge authentication questions? | ✓ | |
| Does the solution allow end users to synchronize their passwords across multiple accounts? | ✓ | |
| When users change or synchronize passwords, does the solution enforce password strength policy? | ✓ | |
| Does the solution include a success/failure notification for password reset and synchronization? | ✓ | |
| Does the solution allow end users to request new accounts/ access to new services or applications? | ✓ | |
| **If you answered yes to the previous question**:<br>Are required approvals enforced when users request new accounts or access to new resources? | ✓ | |
| Can users update personal attribute information (address, cell phone number, etc.) and have that information automatically propagated to the appropriate resources? | ✓ | |
| Can the solution support accessing the Web-based user self-service functions without requiring network log-in? | ✓ | |
| Does the solution integrate with interactive voice response (IVR) for password reset functions? | ✓ | |
| Can the user view the status of the request from a Web interface? | ✓ | |
| Does the solution support a kiosk mode to be configured for users to change passwords from any terminal? | ✓ | |

| IDENTITY SYNCHRONIZATION SERVICES | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution provide a Web-based interface for individuals to view and edit their personal profile information (such as legal name, mailing address, cell phone, and emergency contact)? | ✓ | |

| IDENTITY SYNCHRONIZATION SERVICES | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution provide integration with authoritative systems to detect profile changes and synchronize them where needed (for example, detect title and salary change in the payroll system and update those attributes in the CRM system and LDAP directory)? | ✓ | |
| Does the solution provide enterprise-wide identity data synchronization, ensuring that profiles are accurate and consistent? | ✓ | |
| Does the solution provide one interface to view all identity profile data? | ✓ | |
| **If you answered yes to the previous question:**<br>Does the ability to view all identity profile data in one interface require the building of another identity repository? | | |
| Does the solution provide a fast scheduling capability to execute time-sensitive actions? | ✓ | |
| Is the solution agentless, or does it require installing software on each managed resource? | ✓ | |
| Does the solution provide an incremental synch capability to increase performance? | ✓ | |
| Does the solution provide data transformation and validation rules during synchronization? | ✓ | |
| Does the solution support business rules by automatically completing access privilege or profile data changes according to corporate policies? | ✓ | |
| Does the solution support a large number of connectors to synch between many systems? | ✓ | |
| Does the solution have an attribute mapping interface? | ✓ | |
| Can the solution accommodate bi-directional synchronization via any method as determined by target resource capabilities (e.g., event-driven, polling, and reconciliation)? | ✓ | |

**Buyer's Checklist Contents**

| IDENTITY SYNCHRONIZATION SERVICES | SUN | OTHER VENDOR |
|---|---|---|
| Can you completely configure data flow into and out of the provisioning system (including attribute mapping, transformations, etc.) via a Web-based interface (for example, the ability to configure detection of a telephone attribute change on Directory A, transformation of telephone attribute, propagation of telephone attribute to Directory B and Directory C without having to resort to coding or scripting)? | ✓ | |

| ENTERPRISE ARCHITECTURE CONSIDERATIONS | SUN | OTHER VENDOR |
|---|---|---|
| Is the solution specifically architected for rapid deployment? | ✓ | |
| Does the solution have a proven track record of rapid deployments? | ✓ | |
| Does the solution offer agentless connections to managed resources in order to reduce deployment time and simplify operations and maintenance? | ✓ | |
| Does the solution leverage an intelligent indexing system to manage user identities and access privileges, leaving account information with the information owner and thus avoiding the time-consuming effort of building and maintaining another user repository? | ✓ | |
| Does the solution provide an automated way to discover and correlate all accounts associated with an individual to speed the account mapping process? | ✓ | |
| **If you answered yes to the previous question:**<br>Does the solution provide a way to engage end-users in the discovery process for their own accounts? | ✓ | |
| Does the solution support managing accounts for a user who has multiple accounts on the same resource (for example, a user  who has an administrative account and a development account both on "Resource A")? | ✓ | |

| ENTERPRISE ARCHITECTURE CONSIDERATIONS | SUN | OTHER VENDOR |
|---|---|---|
| Does the vendor offer a wizard-style toolkit to extend coverage of managed platforms to custom and proprietary applications? | ✓ | |
| Does the solution include the ability to connect to resources using existing custom UNIX or Windows scripts? Can customers create new resource adapters by only using operating system scripts? | ✓ | |
| Does the solution include an Integrated Development Environment (IDE) and debugger built on an industry-accepted standard such as NetBeans? | ✓ | |
| Does the solution support SPML 2.0? | ✓ | |
| Does the solution support deploying on all the major database products, including Oracle, UDB DB2, Microsoft SQL Server, and MySQL? | ✓ | |
| Can the solution be deployed in heterogeneous Web application servers, including BEA Weblogic, IBM Websphere, Apache Tomcat, and Sun Java System Application Server? | ✓ | |
| Does the solution run on all the major operating systems including: Solaris, AIX, Microsoft Windows, and Linux? | ✓ | |

| EXTRANET ARCHITECTURE CONSIDERATIONS | SUN | OTHER VENDOR |
|---|---|---|
| Can the solution scale to meet the needs of the extranet, including peak load registration and self-service (e.g., thousands of updates per minute)? | ✓ | |
| Does the solution provide built-in transactional integrity for extranet use cases that require guaranteed delivery of high volumes of provisioning transactions? | ✓ | |
| Does the solution enable non-invasive integration with extranet infrastructure components (e.g., no requirement for directory schema or tree changes; provides agentless connectivity to back-end systems)? | ✓ | |

**Buyer’s Checklist Contents**

| EXTRANET ARCHITECTURE CONSIDERATIONS | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution deliver service-level visibility into the performance and throughput characteristics of the extranet identity administration system? | ✓ | |
| Can the solution facilitate automated account linking and correlation across multiple back-end repositories to provide a single view of an external customer? | ✓ | |
| Does the solution include pluggable auditing for integrating with different auditing data formats, storage locations, and reporting facilities that may already exist in the extranet environment (e.g., merging with existing access logs and reporting systems)? | ✓ | |

| IDENTITY AUDIT | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution provide object-level security and auditing to track system change configuration? | ✓ | |
| Does the solution provide a comprehensive set of predefined reports? | ✓ | |
| Can the solution be configured to audit and report any and every provisioning action that occurs (e.g., new accounts created, provisioning requests by approver, account changes, failed administrator access attempts, failed user access attempts, password changes, password resets, accounts disabled, accounts deleted, rejected provisioning requests, etc.)? | ✓ | |
| Does the solution provide a comprehensive view into who has access to which resources? | ✓ | |
| Does the solution report on who had access to what on a given date? | ✓ | |
| Does the solution provide the ability to quickly find and report on a user’s (or a user group’s) access privileges? | ✓ | |
| Can reports be run on demand? | ✓ | |
| Can reports be scheduled to run on a regular basis? | ✓ | |

| IDENTITY AUDIT | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution report by administrator (accounts created, accounts modified, accounts deleted, password changes, complete audit history per administrator, administrative capabilities per administrator)? | ✓ | |
| Does the solution report by platform or application (users per platform, provisioning history per platform, who performed the provisioning actions on target platform)? | ✓ | |
| Does the solution report on workflow (requests made by user, requests approved by approver, requests denied by approver, requests escalated, delegation of approvals including to whom and for what period of time)? | ✓ | |
| Does the solution report on roles (users per role, resources per role, approvers per role, changes to roles)? | ✓ | |
| Does the solution report on delegated administration (delegated administrators, what their administrative privileges are, and over what user groups and what managed platforms)? | ✓ | |
| Does the solution provide a comprehensive audit log of all actions/modifications carried out through the system? | ✓ | |
| Does the solution easily integrate with corporate reporting tools (e.g., Crystal Reports, Actuate)? | ✓ | |
| Can the reports be easily exported into Microsoft Excel, Microsoft Word, or databases directly from the user interface? | ✓ | |
| Does the solution report by user (audit history per user, accounts/privileges by user, self-service activity by user, role membership)? | ✓ | |
| Can the solution proactively detect risks such as dormant accounts across all managed platforms? | ✓ | |
| **If you answered yes to the previous question:**<br>Can automated action be taken when certain results are found (e.g., automatically disable dormant accounts, send alert to administrator)? | ✓ | |

| IDENTITY AUDIT | SUN | OTHER VENDOR |
|---|---|---|
| Can the solution easily report on account-related security risks in the environment? | ✓ | |
| Can the solution check for these risks on demand? | ✓ | |
| Can the solution check for account risks on a regularly scheduled basis? | ✓ | |
| Does the solution provide performance tracking and performance tools like provisioning-time metrics, and tracing? | ✓ | |
| Does the solution provide a graphical interface for creating and managing provisioning workflows, rules, and interface screens? | ✓ | |
| Does the solution provide the ability for a user to certify that a given set of users has the correct entitlements? | ✓ | |
| Can the approval process be done through a custom workflow with multiple approvers? | ✓ | |
| Are the approvals logged in an audit log that satisfies the requirements of external auditors? | ✓ | |
| Does the solution support the creation and enforcement of policies? | ✓ | |
| Does the solution support scanning for policy violations? | ✓ | |
| Does the solution provide a compliance dashboard listing policy violations? | ✓ | |
| Does the solution reconcile logical and actual access across applications? | ✓ | |
| Does the solution allow multiple approvers and dynamic approvers? | ✓ | |
| Does the solution allow multiple levels of remediators? | ✓ | |
| Does the solution allow remediations with escalation and configurable timeout? | ✓ | |

| IDENTITY AUDIT | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution provide for flexibility to mature the access review process? | ✓ | |
| Does the solution scan, detect, and fix violations on a regular schedule? | ✓ | |
| Does the solution allow access review based on exception? | ✓ | |
| Does the solution allow access review to be done by multiple indices, orgs, managers, and applications? | ✓ | |
| Does the solution allow creation of audit rules that are cross-platform? | ✓ | |
| Can the solution allow entitlements to be changed during the review process? | ✓ | |
| Does the solution provide for manager attestation? | ✓ | |
| Does the solution provide for policy-based periodic access review? | ✓ | |
| Does the solution address erroneous aggregation of privileges? | ✓ | |
| Does the solution provide for automated remediation or "Actionable Audits"? | ✓ | |
| Does the solution reconcile logical and physical access? | ✓ | |
| Does the solution allow preventive compliance whenever a user is changed? | ✓ | |
| Does the solution allow you to capture Separation of Duties conflicts? | ✓ | |
| Does the solution capture policy exceptions and revoke them on expiration? | ✓ | |
| Does the solution allow audit policies to be imported from a spreadsheet or file formats? | ✓ | |

## Access Management

| ACCESS MANAGEMENT | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution include federation and support for open standards? | ✓ | |
| Does the solution provide off-the-shelf agents for Web servers/ app servers, Web apps, and portals? | ✓ | |
| Is the solution based on the J2EE architecture for high levels of integration and customization? | ✓ | |
| Does the solution provide centralized security policy enforcement of user entitlements by leveraging role- and rule-based access control? | ✓ | |
| Does the solution provide high availability and failover capabilities to eliminate any single point of failure? | ✓ | |
| Does the product use multiple load-balanced policy servers, policy agents, and directory instances to do so? | ✓ | |
| Does the solution provide up-to-the-minute auditing of all authentication attempts, authorizations, and changes made to access activity and privileges? | ✓ | |
| Is the solution able to offer true single sign-on (SSO) in Microsoft Windows environments beginning with the sign-on event at a Windows user's desktop? | ✓ | |
| Does the solution allow enterprise applications and platforms to integrate into the centralized authentication/authorization framework seamlessly? | ✓ | |
| Does the solution integrate easily with other SSO products? | ✓ | |
| Does the solution require a specific directory be used as the repository? Is that directory ubiquitous? | ✓ | |

**Buyer’s Checklist Contents**

## Federation Services

| FEDERATION SERVICES | SUN | OTHER VENDOR |
|---|---|---|
| Has the solution been proven to be interoperable with other products based on SAML? | ✓ | |
| Has the solution been certified as “Liberty Interoperable”? | ✓ | |
| Does the solution support the latest specifications (ID-FF 1.2. ID-WSF)? | ✓ | |
| Does the solution enable you to deploy standards-based Liberty Web services? | ✓ | |
| Does the solution allow partners to enable federation and manage their own user information? | ✓ | |
| Do you need to limit sharing of identity and attributes to partners on a need-to-know basis? | ✓ | |

## Directory Services

| DIRECTORY SERVICES | SUN | OTHER VENDOR |
|---|---|---|
| Is the solution a complete directory service solution (e.g., also includes directory proxy, distribution and virtualization capabilities, synchronization with Microsoft Active Directory, and Web-based access to directory data)? | ✓ | |
| Does the solution provide proxy services for high-availability, enhanced security and client interoperability? | ✓ | |
| Does the solution provide Microsoft Active Directory synchronization? | ✓ | |
| Does the solution provide a Web-based viewer/editor for the directory data? | ✓ | |
| Does the solution provide a set of tools to tune and optimize directory service deployments? | ✓ | |
| Does the solution provide a comprehensive Web-based administration framework for the service? | ✓ | |

**Buyer's Checklist Contents**

| LDAP DIRECTORY SERVICES | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution install easily? | ✓ | |
| Does the solution allow bulk loading? | ✓ | |
| **If you answered yes to the previous question:**<br>Can the solution load more than 1,000 entries per second? | ✓ | |
| Does the solution's bulk load ensure data conformance and schema compliance? | ✓ | |
| Does the solution support multiple platforms, including: Solaris 9/10 SPARC and x86, HP-UX, Redhat Linux, Windows 2000/2003? | ✓ | |
| Does the solution support DSML? | ✓ | |
| **If you answered yes to the previous question:**<br>Does the solution support DSML natively, e.g., not as a separate gateway? | ✓ | |
| Does the solution provide a complete command-line interface (CLI) (e.g., all functions can be performed via the CLI without using the console)? | ✓ | |
| Does the solution provide the ability to change the configuration using a CLI and a GUI? | ✓ | |
| Does the solution provide the ability to make most configuration changes to the service while online? | ✓ | |
| Does the solution provide the ability to make most configuration changes using LDAP commands? | ✓ | |
| Does the solution allow you to do fast data backups using file system copy commands? | ✓ | |
| Does the solution allow you to backup the data while online? | ✓ | |
| Does the solution allow you to recreate indexes while online? | ✓ | |

**Buyer's Checklist Contents**

| LDAP DIRECTORY SERVICES | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution allow you to reinitialize a replica while online? | ✓ | |
| Does the solution allow you to change the schema while online? | ✓ | |
| Does the schema replicate automatically? | ✓ | |
| Does the solution allow online access control changes? | ✓ | |
| Does the solution support access control determination dynamically based on the bind DN and target entries (e.g., dynamic access controls)? | ✓ | |
| Does the solution include attribute encryption to protect sensitive data? | ✓ | |
| Does the solution include fractional replication? | ✓ | |
| Does the solution support an unlimited number of password policies? | ✓ | |
| Does the solution provide both roles and class of service (dynamic attribute assignment)? | ✓ | |
| Does the solution provide high availability for write operations? | ✓ | |
| Does the solution have extensive documentation? | ✓ | |
| **If you answered yes to the previous question**:<br>Is the documentation easy to read and does it cover all capabilities? | ✓ | |
| Does the documentation include detailed examples of deployment configurations? | ✓ | |
| Does the documentation include online help? | ✓ | |
| Does the solution include localized versions of the administration console? | ✓ | |

**Buyer's Checklist Contents**

| LDAP DIRECTORY SERVICES | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution include utilities for tuning and performance testing? | ✓ | |
| Does the solution include complete Application Programming Interfaces (APIs) and Software Development Kits (SDKs) for creating applications? | ✓ | |
| Is the solution supported by most major System Integrators? | ✓ | |
| Is the solution supported by most Independent Sofware Vendors (ISVs) in the identity management market? | ✓ | |
| Does the solution provide a plug-in architecture with a fully documented SDK to extend server capabilities? | ✓ | |
| Does the solution provide fast initialization through binary copy of another replica? | ✓ | |
| Does the solution provide dynamic attribute capabilities? [KLL1] | ✓ | |
| Does the solution support vertical scalability (e.g., enable usage of higher-end machines with many CPUs and more memory capacity)? | ✓ | |
| Does the solution have performance that scales up to 18 CPUs? | ✓ | |
| Does the solution support 64-bit hardware to take full advantage of large quantities of fast memory? | ✓ | |
| Does the solution support horizontal scalability (e.g., adding more machines to improve search performance)? | ✓ | |
| Can the solution support tens of thousands of search requests per second to the same data set? | ✓ | |

| DIRECTORY PROXY SERVICES | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution provide transparent server failover and failback? | ✓ | |

**Buyer's Checklist Contents**

| DIRECTORY PROXY SERVICES | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution automatically load-balance traffic? | ✓ | |
| Does the solution provide automatic referral following? | ✓ | |
| Does the solution provide detection of denial of service attacks? | ✓ | |
| Does the solution detect and prevent malformed LDAP requests? | ✓ | |
| Does the solution allow you to limit the number of connections? | ✓ | |
| Does the solution allow you to limit the amount of data per client connection? | ✓ | |
| Does the solution allow you to limit the number of simultaneous operations per connection? | ✓ | |
| Does the solution allow you to timeout inactive sessions/clients? | ✓ | |
| Does the solution allow you to configure SSL from clients? | ✓ | |
| Does the solution allow you to configure SSL to LDAP servers? | ✓ | |
| Does the solution allow you to create access control groups based on IP address or authentication? | ✓ | |
| Does the solution support dynamic query and response filtering? | ✓ | |
| Does the solution support disallowing specific query filters? | ✓ | |
| Does the solution support dynamic schema mapping? | ✓ | |
| Does the solution allow you to hide parts of the DIT? | ✓ | |
| Does the solution allow you to hide attributes? | ✓ | |

**Buyer's Checklist Contents**

| DIRECTORY PROXY SERVICES | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution allow you to distribute a flat name space across multiple sets of servers? | ✓ | |
| Does the solution provide multiple distribution algorithms out of the box? | ✓ | |
| Does the solution include an API to create specific distribution algorithms? | ✓ | |
| Does the solution allow configuration changes to be made using the LDAP protocol? | ✓ | |
| Does the solution support centralized configuration? | ✓ | |
| Does the solution support load-balancing based on LDAP operation type? | ✓ | |
| Does the solution support routing based on LDAP operation type? | ✓ | |
| Does the solution provide activity tracking between proxy and directory servers? | ✓ | |
| Does the solution provide a powerful GUI to manage multiple proxy instances and multiple Directory Server instances through a common console? | ✓ | |
| Does the solution provide an advanced CLI that can be used to script all proxy management operations? | ✓ | |
| Does the solution support operation-based affinity so that LDAP reads after LDAP writes are not impacted by any potential replication delay? | ✓ | |
| Does the solution provide tailored views of directory data to applications? | ✓ | |
| Does the solution have capabilities to send alerts by email? | ✓ | |
| Does the solution have capabilities to execute scripts on alerts? | ✓ | |

**Buyer's Checklist Contents**

| DIRECTORY PROXY SERVICES | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution provide LDAP views of RDBMS systems? | ✓ | |
| Does the solution have capabilities to aggregate entries from multiple data sources including LDAP, LDIF, or JDBC sources? | ✓ | |
| Does the solution support schema- and ACI-checking on virtual views? | ✓ | |
| Does the solution provide DN and attribute renaming? | ✓ | |
| Does the solution provide attribution transformation capabilities (e.g., merge two attributes into one, split one attribute into two, etc.)? | ✓ | |

| ACTIVE DIRECTORY SYNCHRONIZATION | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution do synchronization with Microsoft Active Directory (2000 & 2003)? | ✓ | |
| Does the solution provide a non-intrusive, zero-install footprint on Windows Server (e.g., no files are required to be installed on any Windows systems)? | ✓ | |
| **If you answered yes to the previous question:**<br>Can users still change their passwords using Ctrl-Alt-Delete? | ✓ | |
| Does the solution do bi-directional synchronization? | ✓ | |
| **If you answered yes to the previous question:**<br>Does the solution do bi-directional synchronization for passwords?<br>For entry creation?<br>For entry deletion?<br>For account activation/inactivation?<br>For group synchronization? | ✓<br>✓<br>✓<br>✓<br>✓ | |
| Does the solution support existing entry populations? | ✓ | |
| Does the solution support custom schema in both Microsoft Active Directory and Sun's Directory Server? | ✓ | |

**Buyer's Checklist Contents**

| ACTIVE DIRECTORY SYNCHRONIZATION | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution support mapping between hierarchical and flat name spaces? | ✓ | |
| Can the solution target subsets of users in either Microsoft Active Directory or Sun's Directory Server? | ✓ | |
| Is the filtering capability fine-grained and configurable? | ✓ | |
| Does the solution support auxiliary object classes? | ✓ | |
| Does the solution allow default attribute values to be specified? | ✓ | |
| Can the solution's default values be parameterized? | ✓ | |
| Can the solution be configured centrally, but deployed in a distributed fashion? | ✓ | |
| Does the solution support centralized logging of all synchronization activity? | ✓ | |
| Does the solution support persistence of password changes even in the case of network failure? | ✓ | |
| Does the solution provide for failover of Microsoft Active Directory? | ✓ | |
| Does the solution provide for failover of Directory Server? | ✓ | |
| Is the solution highly secure with SSL connections between all elements? | ✓ | |

| WEB-BASED VIEWER/EDITOR | SUN | OTHER VENDOR |
|---|---|---|
| Can access be done over and optionally limited to SSL? | ✓ | |
| Can forms for editing objects be created and modified without writing code? | ✓ | |
| Can the interface be easily and completely branded? | ✓ | |

**Buyer's Checklist Contents**

| WEB-BASED VIEWER/EDITOR | SUN | OTHER VENDOR |
|---|---|---|
| Is the interface J2EE-based and does it support all major Web-containers? | ✓ | |
| Does the interface include an SDK to extend the functionality beyond what is provided out of the box? | ✓ | |
| Does the interface make full use of Directory Server access controls to control viewing and access to data? | ✓ | |
| Does the interface utilize existing Directory Server access controls or groups to control functionality within the solution (e.g., only show certain functions to users in a specific group)? | ✓ | |

| DIRECTORY SERVER RESOURCE KIT | SUN | OTHER VENDOR |
|---|---|---|
| Does the solution include a supported C and Java SDK to create LDAP client applications? | ✓ | |
| Does the solution provide a collection of tools to evaluate Directory Server configuration and deployment performances? | ✓ | |
| Does the solution include an out-of-the-box white pages application? | ✓ | |
| Does the solution include other sample applications? | ✓ | |

## Chapter 4
# Industry Standards Fact Sheet

Sun continues to be an active member in and leading contributor to a number of industry standards organizations—especially in the identity management space. With 20-plus years of experience in network computing innovation and open standards development, Sun has a legacy of delivering cross-platform interoperability.

You may not know what systems and solutions your company will implement in the future; therefore it's critical that your identity management vendor adheres to current technology standards and plays a strong role in helping to create future standards. Sun continues to fully support the adoption of open standards and is fully committed to producing ground breaking solutions that push the boundaries of innovation. At the same time, Sun strives to ensure that our technology is built upon and fully integrated with established and emerging standards.

Sun participates and is committed to the following industry standards bodies:

| INDUSTRY STANDARD BODY | SUN'S PARTICIPATION |
|---|---|
| **Lightweight Directory Access Protocol** | • Major contributor to and co-author of the LDAP V3 Technical Specifications<br>• First vendor to ship reference LDAP implementations |
| **Liberty Alliance—Identity Web Services Framework (ID-WSF)**<br>www.projectliberty.org | • Management Board Member<br>• First vendor to earn "Liberty Alliance Interoperable" logo for Sun Java System Access Manager<br>• Access Manager is the first productized solution supporting the latest Liberty Alliance Phase 2 (ID-WSF) |
| **OASIS—Service Provisioning Markup Language (SPML)**<br>www. oasis-open.org | • Chair of the OASIS Provisioning Services Technical Committee<br>• Major contributor to the SPML specification<br>• First to release an open source SPML toolkit |

| INDUSTRY STANDARD BODY | SUN'S PARTICIPATION |
|---|---|
| OASIS—Security Assertion Markup Language (SAML)<br>www.oasis-open.org | • Member of the Board of Directors and a Foundational Sponsor<br>• Active participation in numerous technical committees including Security, SOA, and Web Services<br>• Leader in defining SAML<br>• Access Manager is one of the first access management products to support the latest SAML 1.1 specifications |
| OASIS—eXtensible Access Control Markup Language (XACML)<br>www.oasis-open.org | • Secretary of the OASIS XACML Technical Committee<br>• First to release an open source version of XACML 1.0 |
| OASIS Directory Services Markup Language 2.0 (DSML)<br>www.oasis-open.org | • Contributor to the DSML technical specification<br>• One of the first vendors to productize DSML 2.0 |
| W3C<br>www.w3.org | • Active member of W3C with strong involvement in XML and related security standards |
| WS Interoperability Organization (WS-I) | • Member of the board of directors, contributing member<br>• Working directly with Microsoft on emerging standards in the WS-* stack like WS-Addressing and WS-Federation |

**Take the Next Step**

- See the savings
- Sign up for Identity Insights
- Contact Sun

Chapter 5

# End-to-End Identity Management from Sun

## Take the Next Step

1. **See the savings.** Sun's ROI calculator shows just how much Sun identity management could cut costs and reduce complexity for a specific organization. Visit www.sun.com/identity/resources to use the calculator.

2. **Sign up for Identity Insights.** As a member, you will receive an eNewsletter, exclusive invitations, and information on upcoming special offers and events. Go to www.sun.com/identityinsights to join the program.

3. **Contact Sun.** We're ready to put identity management to work on addressing your security, compliance, and outsourcing opportunities. Go to www.sun.com/identity/getstarted.

**FAQ Contents**

- Identity Management in General
- Provisioning and Auditing
- Access Management
- Federation
- Directory Services

Chapter 6

# FAQs

## Identity Management in General

**What specific capabilities does Sun identity management offer my business?**

Sun takes a comprehensive approach to identity management, with automated solutions that address provisioning of users for access to enterprise resources, as well as auditing of usage (Sun Java System Identity Manager), access management for enterprise resources (Sun Java System Access Manager), federated identity for open yet secure access across domains (Sun Java System Federation Manager), and directory services (Sun Java System Directory Server Enterprise Edition). These products can be implemented individually, in concert, or phased in over time.

**Can Sun identity management help with compliance?**

Sun identity management solutions feature capabilities to ensure compliance with national and international regulations governing privacy, security, and financial integrity. They provide enterprise-wide identity auditing and reporting capabilities and a role-/rule-based approach to support repeatable, auditable, and enforceable security processes. They also provide the ability to review the status of access privileges at any time to meet audit requirements.

**Will Sun identity management help our company reduce IT costs?**

Sun solutions are fully automated, which eliminates costly manual processes associated with provisioning users, managing access, and doing auditing/reporting. Automation also simplifies everyday tasks such as password resets to reduce help desk costs. Sun identity management is designed to integrate easily with existing IT infrastructures, speeding deployment and reducing implementation costs.

**How can Sun identity management help us increase revenue?**

Sun identity management solutions support collaboration among companies to develop revenue-enhancing products and services and bring them to market faster. These products support collaboration by delivering key capabilities such as single sign-on (SSO) across diverse systems and by extending security and other policies to multiple domains. In this way, companies can openly yet securely share access to their resources with an infinite number of other companies.

**Will we have to rework our business processes to accommodate identity management?**

No. A good identity management solution will be flexible enough to work with your current business processes. Through commitment to standards and open interfaces,

**FAQ Contents**

Sun identity management solutions make interoperability with existing systems and third-party technologies simple and affordable. This decreases integration costs, reducing deployment times and maximizing the value of prior technology investments. In addition, Sun solutions pave a smooth path to future technology investment with a highly modular design that enables you to implement one or more Sun products now and then phase in others over time.

**What would be a good starting point for implementing identity management?**
Most organizations will be best served by first prioritizing the problems they are trying to solve. Is the key driver efficiency of account management? Secure yet easy access? Faster deployment of identity-consuming applications? Or just providing a higher quality of service to your user base? Once you prioritize the business issues, you can prioritize the systems that you want to match to identity management. Applications that hold secure information, have large user populations, and that are often accessed by temporary or contract workers are key targets for automated identity management.

**How does Sun identity management measure up to others, according to the analysts?**
Forrester ranked Sun #1 in current offering and market presence and said “Sun Microsystems is a market leader for a reason—its product delivers superior provisioning functionality with the highest ease of use” *(Forrester Wave: User Account Provisioning, A1 2006)*. Gartner positioned Sun in the Leaders Quadrant in its Magic Quadrant for User Provisioning and said “Sun’s actions raise the competitive bar for all products in the market, and they change the course of the industry” *(Garter Magic Quadrant for User Provisioning, 1H06, Roberta Witty et al., 25 April 2006)*. Ovum awarded Sun 21 out of 25 stars for its identity management solutions and said “Sun leads because of their comprehensive vision, which will enable them to grow with the market without fundamentally changing their concepts” *(Ovum, Identity Management: Time for Action, July 2005)*.

## Provisioning and Auditing

**Can Sun identity management help with both our day-to-day resource provisioning needs and all the compliance requirements we have now?**
Sun Java System Identity Manager is the first solution to offer cost-effective provisioning and compliance in one solution. It delivers a single solution to handle:

1. user provisioning and synchronization of user identity information across applications, directories and data stores and
2. identity-based compliance-related auditing and reporting, including early detection of potential security problems and automatic notification of policy violations.

Because the provisioning and auditing capabilities are integrated in one solution, the process of detection and remediation is seamless: A violation can be detected, the account disabled pending investigation, and the entire incident documented and reported—all with the same solution.

**Can Identity Manager provision all of our resources—not just digital IT systems, but also non-digital assets like phones, PDAs, badges, and so on?**
Yes. Identity Manager can provision digital systems automatically, creating the accounts as soon as a request is made from your authoritative source. Identity Manager can also provision your non-digital resources via workflow and email requests. For example, when you need to issue a new badge for physical access to facilities, Identity Manager can email the owner of the badge system to request the badge and relay all the relevant information such as user's name, start date, and location.

**How will Identity Manager address our concerns about identity theft and data privacy?**
Identity Manager delivers the combined capabilities to detect violations of policy related to identity theft and privacy protection. For example, if an employee violates policy by taking home a laptop computer with detailed customer information on it, Identity Manager will instantly detect the violation, alert the employee's manager, and disable the account to eliminate any possibility of the information being compromised by unauthorized users while the laptop is in an unauthorized location outside the company.

**Can Identity Manager prevent regulatory violations involving segregation of duties?**
Yes. For example, if you have an employee who changes jobs within the company, you don't have to worry that the employee will continue to have access to the resources appropriate to his or her old job as well as access to conflicting resources that are related to the new position. This eliminates the possibility of inadvertently violating regulatory requirements for segregation of duties.

**Will the capabilities of Identity Manager extend to our customized proprietary applications?**
Yes. Most companies need to extend coverage to custom or highly verticalized applications, and Identity Manager is specifically designed to support that. The Sun Resource Adapter Wizard provides a complete development toolkit that includes capabilities for developing fully functional custom resources adapters for systems that are not supported out-of-the-box. This toolkit is available free-of-charge to customers and partners. Systems integrators, including PricewaterhouseCoopers and Deloitte & Touche, are also trained and certified by Sun to develop resource adapters. The average development time for a new adapter is just three to five days.

**FAQ Contents**

**How long will it take to start seeing a return on our investment in Identity Manager?**

Unlike typical identity management solutions that take about 18 months to deploy, Identity Manager can be implemented in a fraction of that time—speeding the time to ROI as well. At Burlington Northern Santa Fe Railway, for example, Identity Manager was deployed in 45 days to cover 40,000 users on five platforms. Once Identity Manager has been implemented, most enterprises can expect to see a return on investment within a year.

**Can Identity Manager scale to support hundreds of thousands of users as we step up online partnerships with other organizations?**

Yes. Identity Manager extends identity controls to unlimited extended environments, and it has been proven to deliver provisioning and auditing to environments with tens of millions of users. Identity data in extended environments is stored locally to maximize efficiency but managed centrally to maintain security.

## Access Management

**Is there a way to avoid having to use different solutions to manage access to our Web, Java, federated, and Web services environments?**

Access Manager provides a single, integrated solution for securing access to web and Java-based applications, federated partner networks, and Web services. In each case, Access Manager simplifies how users gain access to applications, providing single sign-on (SSO) capabilities to web applications, portals, Windows desktop environments, Java applications, and loosely coupled Web services based on a centralized set of authentication mechanisms and secure-access policies.

**How can we be sure that Access Manager will work with systems and solutions we implement in the future—or with solutions that we develop with partners?**

Access Manager is standards-based and Sun is a leader in standards development, ensuring support for current and future standards-driven applications. To facilitate collaboration among partners, Access Manager specifically supports the latest federation standards, allowing for broad interoperability—including single sign-on—across multiple systems.

**Can we use multiple directories with Access Manager?**

Yes. Access Manager can be configured to authenticate users against any LDAP-compliant directory, ensuring full leverage of existing application investments.

**Does Access Manager include any auditing capabilities?**

Access Manager provides real-time auditing of all authentication attempts, authorizations, and administration activity. The solution also maintains a history of all event data to meet specific requirements for auditabilty and to help ensure regulatory

**FAQ Contents**

compliance.

**What is the difference between role-based and rule-based access control?**

Roles provide a grouping mechanism for authorization and can be implemented in a variety of ways; static groups and dynamic groups (based on attribute values in user entries) are the most popular. Rules provide a flexible means of protecting applications based on conditions that can modify how and when resources are accessible. For example, you can use rules to limit access based on IP address, time of day, authentication credential, and other specific conditions. Combining roles with rules provides a robust and flexible framework for meeting business and security requirements while allowing access to protected resources.

## Federation

**As the number of partners we collaborate with online keeps growing, can Sun identity management help us reduce the complexity of maintaining so many partnerships?**

Yes. Federation Manager is designed to make the process of integrating with a partner repeatable with an infinite number of other partners. So instead of having to recreate the integration process every time you add a new partner, you can apply the same framework over and over again to as many partners as you have. This simplifies and speeds integration with new partners, helping you develop new revenue streams more rapidly and at a lower cost.

**How can Federation Manager simplify access to our networked resources, but still keep them secure?**

Extranet single sign-on (ESSO) authenticates users and exchanges credentials across partners. This makes it easy for partners to access your resources, and, at the same time, leverages established authorities to identify the partners and determine which applications and services they may access.

**How can Federation Manager help us to ensure that our security policies are enforced when we're in collaboration with other companies?**

Federation Manager leverages your existing authentications and authorizations so that these capabilities are implemented consistently across an unlimited number of partner domains. Using existing capabilities and mechanisms this way not only allows you to extend security policy to partners, it also allows you to reduce the cost and complexity of creating federated service offerings, because you don't have to reestablish security every time you establish a new business partnership.

**FAQ Contents**

## Directory Services

**Can Sun provide us with a directory solution that works with Microsoft Active Directory?**

Yes. Directory Server Enterprise Edition provides seamless integration with Active Directory via on-demand password synchronization between Windows environments and Sun's directory server environment.

**Does the phrase "Enterprise Edition" mean that there's a limit to the size of user community we can support with Directory Server Enterprise Edition?**

No. Directory Server Enterprise Edition has broad market scope and applies to any organization that needs to manage any number of identities and users securely and efficiently. This directory solution is designed to scale from hundreds or thousands of users within an enterprise to the tens of millions of users that have become so common in service provider environments today.

**Is Directory Server Enterprise Edition supported by third-party software products that we might use, such as CA/Netegrity or Plumtree?**

Sun's Directory Server has for years been the de facto standard LDAP directory to which most software companies have tested and developed their LDAP-enabled products. This makes Directory Server Enterprise Edition the most widely supported directory on the market.

**Will Sun provide the tools to help our IT staff write cross-platform, directory-enabled applications?**

Yes. Directory Server Enterprise Edition includes LDAP Software Development Kits (SDKs) for C and Java programming languages to help streamline the process of writing client applications for the directory. These APIs expose all of the functions for connecting to an LDAP directory and accessing or modifying its entries. They can be used to design and integrate directory functionality into applications at the programmatic level.

**What other tools are available for performance optimization, benchmarking, tuning, and troubleshooting?**

Directory Server Enterprise Edition comes standard with the Directory Server Resource Kit, which provides tools for optimizing performance, creating and performing benchmarks, tuning for high performance, and troubleshooting directory problems. Sun has also developed one of the most powerful load-generation testing applications on the market. Freely available at slamd.com, SLAMD includes all the tests needed to thoroughly performance-test deployment of Directory Server Enterprise Edition.

**Glossary Note**
Terms in *italics* are also defined in the glossary.

Chapter 7

# Glossary of Terms

## A

**Access Management**: management of secure access to an enterprise's network resources both within the enterprise and across business-to-business value chains.
**Active Directory**: see Microsoft Active Directory.
**Administration**: the ongoing management of network resources and *users*.
**Audit**: an intensive examination of records, such as audit trails, either to ensure that policy is being followed or to track events and violations back to the source.
**Authentication**: process by which a computer, computer program, or another *user* attempts to confirm that the computer, computer program, or user from whom the second party has received some communication is, or is not, the claimed first party.
**Authorization**: the process by which an entity attempts to confirm that another entity is allowed to access a resource. Authorization always includes *authentication*.

## B

**Breach**: the successful defeat of *security* controls, which could result in a penetration of the system; a violation of controls of a particular system such that information assets or system components are unduly exposed.

## C

**Canadian Privacy Act**: legislation enacted to extend Canadian laws that protect the privacy of individuals to personal information held by a government institution that provides a right of access to such information.
**Compliance**: a state or act of accordance with established standards, specifications, regulations, or laws. More often connotes a very specific following of a particular compliance standard and is usually the term used for the adherence to government regulations and laws.
**Computer Security**: technological and managerial procedures applied to computer systems to ensure the availability, integrity, and confidentiality of information managed by the computer system.

## D

**Delegated Administration**: the assignment of day-to-day *user* administration responsibilities to someone other than a central administrative authority. Improves operational efficiency by distributing the administrative burden to multiple authorized parties who are overseen by the central administrative authority.
**Directory Services**: a network layer that identifies network *users* and other resources as well as the policies that are assigned to them.
**Directory Services Consolidation**: consolidation of disparate directories to eliminate redundancy. Increases efficiencies when adding or deleting information and reduces

**Glossary Note**
Terms in *italics* are also defined in the glossary.

management costs.
**DSML (Directory Services Markup Language)**: a new standard for representing directory information as *XML*.

## E

**European Data Protection Directive**: legislation concerning the protection of individuals with regard to the processing of personal data and the free movement of such data.
**Extranet**: an extension of a Web site or *intranet*, accessible only by authorized *users* who are non-employees, such as contractors, suppliers, partners, etc.

## F

**Federated Identity**: the agreements, standards, and technologies that make identity and entitlements portable across autonomous domains.
**Federated Identity Management (FIM)**: the management of identities between corporate boundaries. Refers to the amalgamation of the account information from all service providers that are accessed by one *user* (personal data, *authentication* information, buying habits and history, shopping preferences, etc.).

## G

**Gramm-Leach-Bliley Act**: federal legislation enacted in the United States to control the ways that financial institutions deal with the private information of individuals. Also requires financial institutions to give customers written privacy notices that explain information-sharing practices.

## H

**HIPAA (Health Insurance Portability and Accountability Act)**: federal legislation enacted in the United States to establish standardized mechanisms for electronic data interchange (EDI), *security*, and confidentiality of all healthcare-related data. Mandates security mechanisms to ensure confidentiality and data integrity of any information that personally identifies an individual.

## I

**ID-WSF (Identity Web Services Framework)**: *Liberty Alliance* framework for identity-based *Web services*.
**Identity Auditing**: comprehensive auditing and reporting of *user* profile data, change history, and permissions enterprise-wide. Ensures that *security* risks are detected so administrators can respond proactively and comply with legislative mandates.
**Identity Management**: a category of interrelated solutions that are employed to administer *user authentication*, access rights, access restrictions, account profiles, *passwords*, and other attributes supportive of *users'* roles/profiles on one or more applications or systems.
**Identity Profile**: a collection of information about an individual, including personal

**Glossary Note**
Terms in *italics* are also defined in the glossary.

information (i.e., name and contact information), legal information (i.e., social security number and compensation), and *authentication* information (i.e., *user ID* and *password*).

**Identity Provisioning**: the automation of previously fragmented, manual processes for managing the full *user* lifecycle. Greatly reduces the time it takes to grant access to *users* and to change or revoke their access privileges based on role changes.

**Identity Synchronization**: synchronization of identity data across a wide range of heterogeneous applications, directories, databases, and other data stores. Improves operational efficiencies by eliminating the need for data to be synchronized manually.

**Information Security**: the result of any system of policies and/or procedures for identifying, controlling, and protecting from unauthorized disclosure information which is authorized to be protected by executive order or statute.

**Intranet**: a private network protected by a firewall and accessible only by authorized *users*.

**Intrusion**: any set of actions that attempts to compromise the integrity, confidentiality, or availability of a resource.

**Intrusion Detection**: pertaining to techniques that attempt to detect intrusion into a computer or network by observation of actions, *security* logs, or *audit* data. Detection of break-ins or attempts, either manually or via software expert systems, that operate on logs or other information available on the network.

**IPSec (Internet Protocol Security)**: standard *protocols* for securing IP traffic, developed by the IETF (Internet Engineering Task Force).

## L

**LDAP (Lightweight Directory Access Protocol)**: a protocol for accessing online directory services.

**Liberty Alliance**: an organization developing and deploying the *Project Liberty* suite of standards, which defines *protocols* for *FIM* and Web services communication between organizations.

## M

**Meta-Directory**: set of software tools that synchronize the contents of multiple *user* directories. Typically reads a list of user and user-attribute data from multiple directories, builds a master directory of users and their attributes, and pushes new or changed data from the master directory back to some or all of the managed directories.

**Microsoft Active Directory**: the directory service used in the Microsoft Windows 2000 architecture.

## O

**OASIS (Organization for the Advancement of Structured Information Standards)**: a non-profit, international consortium that creates interoperable industry specifica-

**Glossary Note**
Terms in *italics* are also defined in the glossary.

tions based on public standards such as *XML* and *SGML* as well as others that are related to structured information processing.

## P

**Password**: a secret string of characters attached to a specific *user name*. A *user* must enter the correct *password* to be allowed access into a system.

**Password Management**: the setting, resetting, and synchronization of *passwords* across enterprise systems. Can be automated to streamline administrative requirements and improve service to *users.*

**Policy Management**: a workflow process to enforce policy for access and rights to employees, partners, and customers.

**Project Liberty**: defines *protocols* for *FIM* and Web services communication between organizations, initially for *SSO (single sign-on)* based on *SAML.*

**Protocols**: agreed-upon methods of communication used by computers.

**Provisioning**: the maintenance of records corresponding to employees, customers, or other recipients of a service (such as email) in a directory service or similar database for use by *identity management* software.

## R

**Risk Assessment**: a study of vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of *security* measures. The process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations.

**Role-based Access Control**: the identification, *authentication*, and authorization of *users* based on the jobs they perform within an organization.

**Rule-based Access Control**: the granting of access to secure networked resources based on the presence of certain specific conditions.

## S

**SAML (Security Assertions Markup Language)**: the Extensible Markup Language *(XML)*-based specification supported by *OASIS*. Adopted by the *Liberty Alliance*, an industry organization consisting of 160 member companies that have joined together to promote federation standards.

**Sarbanes-Oxley Act**: legislation enacted in the United States in response to the high-profile Enron and WorldCom financial scandals to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise. Administered by the Securities and Exchange Commission (SEC), which sets deadlines for *compliance* and publishes rules on requirements.

**Security**: a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.

**Security Audit**: a search through a computer system for *security* problems and vulnerabilities.

**Glossary Note**
Terms in *italics* are also defined in the glossary.

**Security Policy**: an established and constantly updated list of rules for secure network usage.
**SPML (Service Provisioning Markup Language)**: the *XML*-based language that facilitates the exchange of *provisioning* information among applications and organizations.
**SSL (Secure Sockets Layer)**: a session layer protocol that provides *authentication* and confidentiality to applications.
**SSO (Single Sign-on)**: *authentication* process in a client/server relationship where the *user* can enter one name and *password* and have access to more than one application or access to a number of resources within an enterprise. Eliminates the need for the *user* to enter further authentications when switching from one application to another.
**Synchronize Active Directory**: bi-directional synchronization between *LDAP* and *Microsoft Active Directory*, an essential function for almost every networked business or other organization.

## T

**TCP/IP (Transmission Control Protocol/Internetwork Protocol)**: the suite of *protocols* upon which the Internet is based.
**Token**: an *authentication* tool; a device utilized to send and receive challenges and responses during the *user* authentication process.

## U

**User**: any person who interacts directly with a computer system.
**User Identification (User ID)**: the process by which a *user* identifies himself or herself to the system as a valid user (as opposed to *authentication*, which is the process of establishing that the *user* is indeed that user and has a right to use the system).
**User Name**: a unique handle assigned to an authorized user upon system registration.

## V

**Virtual Identity Services**: a single Virtual ID that identifies *users* across all applications and assets in an enterprise. Provides for quick, cost-effective *provisioning* of employees, partners, and customers to enterprise resources.
**Vulnerability Detection**: the process of identifying threats and vulnerabilities and prioritizing the greatest risks.

## W

**W3C**: the World Wide Web Consortium, created in 1994 to lead the World Wide Web to its full potential by developing common *protocols* that promote its evolution and ensure its interoperability.
**Web Access Management**: see Web SSO.
Web Services: a collection of *protocols* and standards used for exchanging data be-

**Glossary Note**
Terms in *italics* are also defined in the glossary.

tween applications. Can be used by software applications written in various programming languages and running on various platforms to exchange data over computer networks like the Internet.

**Web SSO**: a simplified *SSO* that works strictly with applications and resources that are accessed with a Web browser. Also called *Web access management*.

**WS-I (Web Services Interoperability Organization)**: organization chartered to promote Web services interoperability across platforms, operating systems, and programming languages.

## X

**XACML (Extensible Access Control Markup Language)**: an *OASIS* standard for managing access control policy.

**XML (Extensible Markup Language)**: a *W3C* initiative that allows information to be encoded in a way that facilitates its easy exchange on the Web.

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN (9786) Web sun.com