

Privacy and Data Protection: Mitigating the Risks of Information Exposure

A Technical White Paper
July 2004



© 2004 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 USA

All rights reserved.

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

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

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

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

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

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



Please
Recycle



Adobe PostScript

Table of Contents

Introduction	1
Why Businesses Need Private Data	3
Defining Consent	4
Consumer Backlash	4
Mitigating the Risks — Personal Privacy and Data Protection	6
Gaining Consumer Confidence	6
Limiting Business Exposure	7
Building Competitive Advantage	7
Complying With Laws and Regulations	7
The Current State of Privacy Legislation Worldwide	8
EU Directive on Data Protection	8
United States Vertical and Regional Legislation	9
Sarbanes-Oxley Act	9
Gramm-Leach-Bliley (GLB)	9
Health Information Portability and Accountability Act (HIPAA)	9
21 CFR part 11	9
The Children’s Online Privacy Protection Act (COPPA)	10
State-Level Legislation	10
California Senate Bill 1386	10
Other Acts	10
How Can Identity Management Help?	11
User Provisioning	11
Profile Management	12
Access Management	12

Password Management	12
Directory Management	12
Audit and Reporting	13
The Solution — End-to-End Identity Management from Sun	14
Next Steps	15

Chapter 1

Introduction

Businesses and other organizations today are collecting and storing unprecedented amounts of personal data. They use this data to conduct daily business, deliver customized products and services to consumers/citizens, increase efficiencies, and build competitive advantage in quickly evolving markets. The pace of data collection continues to increase as organizations seek the ultimate “user profile.”

However, while pursuing this goal, organizations must also pursue a sometimes conflicting goal: Ensure that all personal data is used only in ways that consumers wish it to be used. Although consumers welcome the enhanced products and services made possible by extensive data collection, they also want some control over how their personal information will be accessed, used, and redistributed.

“According to a recent Accenture survey, 60 percent of the 223 business executives surveyed said that privacy policies are the least important of five factors that influence consumer trust. Yet 51 percent of the 347 consumers surveyed said that they have declined to do business with a company because they were uncomfortable with its privacy protection.”

– *Privacy is Your Issue*, CIO Magazine, June 1, 2004

Consumers’ concerns about their privacy are not entirely unfounded. As organizations have continued to collect and store greater amounts of personal data (including more data about each individual), breaches of personal data have been occurring with increasing frequency. The most frequent type of breach is identity theft. More than 27 million Americans have been victims of identity theft over the last five years, including 9.9 million people in just the last year. Losses attributed to identity theft totaled nearly \$48 billion for businesses in the last year while consumer victims reported \$5 billion in out-of-pocket expenses. The average business loss to identity theft was \$4800; the average consumer loss was \$500.¹

In addition to identity theft, other types of privacy breaches include incidents of sabotage against corporations, the negligent misuse of personal information, improper sale of personal information, and innocent errors such as the inadvertent transmission of personal information via e-mail.

The national media now reports stories of privacy breaches every week. As a result, consumers no longer feel very secure, and the growth of business-to-consumer (B2C) e-commerce will suffer as a result. When privacy breaches are so common and so visible, prudence dictates that businesses and other organizations take pains to ensure that personal information is protected effectively. No organization can plead ignorance today — especially organizations that conduct B2C business over the Web.

1. CIO Magazine, September 4, 2003

Consider the case of a manufacturer of upscale jeans. In June 2003, the company paid a fine and was required to deploy an effective information security program in response to repeated break-ins of its Web site that led to the disclosure of customer credit card information. Or consider the case of a major insurance firm. In early 2002, the firm was victimized by a disgruntled ex-employee who attempted to sell the names, social security numbers, and credit card records of 60,000 employees of the firm.

Obviously, prudent organizations are paying attention to these breaches and taking steps to reduce their organizations' risk profiles. But now there is another reason — in addition to prudence — for organizations to pay attention to the risk of privacy breaches: New laws and regulations that dictate what organizations must do and not do with regard to the collection, storage, and use of personal data.

In the United States, organizations must protect certain classes of personal information: Financial data under Gramm-Leach-Bliley (GLB), healthcare information under Health Information Portability and Accountability Act (HIPAA), and pharmaceutical information under 21 CFR part 11. Globally, the regimen varies; many countries have enacted sweeping privacy protections following the style of the European Union (EU) Directive on Data Protection.

Where does that leave the organization that collects and stores personal data? The organization, regardless of size, must gain better control over personal data. If it does not do so, it risks privacy breaches, including identity theft, sabotage, negligent misuse, and even inadvertent misuse. The repercussions can include loss of consumers' confidence, damage to the value of brands, reduction of shareholder value, lawsuits, fines, and even the imprisonment of corporate officers.

“The bottom line for each of these laws is accountability — accountability that goes beyond IT's responsibility to keep information systems and data secure. Management teams must formulate policies and procedures that comply with GLBA, HIPAA, and Sarbox, and ensure these policies are implemented. Otherwise, civil and criminal penalties may apply. Fines for ignoring a specific requirement under HIPAA can reach \$25,000 per violation, and a corporate officer who knowingly signs a false financial report can be fined up to \$1 million and/or face as many as 10 years in prison under Sarbox.”

– *Feds Reach Out and Touch IT*, Network Computing, July 10, 2003

Most people want some measure of control over their digital personae. Can technology help organizations ensure that their customers, citizens, clients, patients, or students will have that control? Today, in certain circumscribed environments, the answer is “Yes.” But in general, the answer for the foreseeable future is “No.”

The general solution to this problem lies in the discipline of identity management. Identity management is the comprehensive management and administration of user permissions, privileges, and individual profile data. Technologies to provide identity management are now maturing, yet most enterprises lack the organizational structure and process maturity to simply drop a product in place. Deploying identity management solutions requires a clear understanding of the problem and its implications.

How did we get into this situation? What exposures do we risk? What identity management solutions exist today? How can organizations implement them? This white paper will examine each of these questions as it attempts to address the problems of privacy and data protection.

Chapter 2

Why Businesses Need Private Data

Organizations — especially businesses — require information about individuals to carry out their missions. Retailers need to understand their customers' buying patterns, elected officials need to understand their constituencies' political interests, academic institutions need to understand their students' educational needs, and so on. In the Internet-enabled world, this need generates a set of parallel requirements:

- Gather as much data as possible about each customer.
- Preserve as much contextual information about the customer's actions and behavior as possible.
- Correlate customer data with other information (often residing in diverse data stores) that supports reasonably accurate forecasts about customer behavior.
- Don not break the law.

“Businesses demand the benefits of a technology-enabled world along with the relative anonymity, or privacy, that the pretechnology world provided.”

– *How to Meet Tomorrow's Privacy Rules Today*, CIO Magazine, November 1, 2002

Although these requirements enable the delivery of enhanced goods and services, they are also directly at odds with most consumers' concept of privacy. In an 1890 Harvard Law Review essay, Samuel D. Warren and Louis D. Brandeis expressed the concept of privacy such that each of us has the right to decide what others know about us, that we have the right to determine how that information is used and whether it can be redistributed, and that we have the right to be left alone.²

With each business transaction, a customer leaves a footprint — what was bought or loaned or asked or learned — in exchange for the convenience of using or gaining the permission to use an Internet-enabled capability. Retailers (interpreted broadly here to include governments, schools, hospitals, associations, and other providers of services) use this valuable information to fine-tune their products and services — including programs, classes, etc. — to better meet the needs of their markets.

2. The Right to Privacy, by Samuel D. Warren and Louis D. Brandeis, Harvard Law Review, Vol. IV, December 15, 1890, No. 5. (The full text of the article can be found at www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html.)

Defining Consent

The process of gathering information and maintaining its integrity requires two crucial components: The consent of the subjects and a considerable engineering effort. Increasingly, “consent” has been defined by legislation, such as privacy or “opt-in” legislation in the United States. Such legislation is usually applied within specific vertical markets or geographic regions (to be addressed in more detail later in this paper).

In Europe, under the provisions of the EU Directive on Data Protection, subjects must be informed in advance of any information that might be gathered about them, how it will be used, and where it will be kept. Furthermore, they must be allowed to opt-out entirely. Any organization that violates these provisions may face legal action from the subject’s government.

When a business is building contextual information, it wants to know a customer’s habits. For example, a service station might want to know that customer XYZ buys gas every other weekend. In addition, the business would like to correlate that set of information with additional information, for example, that the customer lives in a certain neighborhood, regularly uses the car wash, and always uses a debit card to pay for purchases.

Such correlated information helps businesses target specific buyers with special offers and conveniences tailored to their unique desires and needs. Most customers appreciate these targeted offers, and are more likely to respond to them than to mass-marketed offers. Analysis of correlated information can supplement existing marketing programs, as well as inspire new ones.

In the service station hypothetical case, the service station may have gathered some information from its own records, and collected other information from sources outside the business. To gather personal information from outside its own walls, an organization may query credit rating agencies, name and address lists, voter registration rolls, demographic surveys, and other public and private sources. This correlation of customer information is sometimes called “Customer Data Integration,” or CDI. The goal of CDI is twofold: First, to achieve as complete a picture of the customer as possible, and second, to maintain the accuracy of customer information.

Consumer Backlash

There is a drawback to CDI. When subjects learn or suspect that an organization is collecting information from multiple sources, even if the sources themselves are innocuous, they may interpret the collecting as a violation of their right to privacy. Too vigorous an initiative — one that runs too far ahead of the expectations and comfort level of the subjects — can create a backlash.

For example, in 2001, a large pharmaceutical company offered a novel service. On its Web site, patients who used a specific drug could subscribe to receive an automated e-mail to remind them to refill their prescriptions. Due to a programming error, the e-mail was sent with all 669 subscribers’ e-mail addresses visible; that is, each recipient was given information that could enable him to learn the identities of 668 other drug users.

The subsequent investigation resulted in a settlement that includes a required annual review of the company’s implementation of enhanced training, technology, incident response systems, and business processes. In addition, the company must maintain comprehensive audit records of these activities for the next five years. These sanctions may not appear to be burdensome to such a large organization, but most companies would rather avoid such sanctions if possible.

The pharmaceutical company clearly had no criminal intent. It simply wanted to provide a value-added service to its customers, who incidentally would refill their prescriptions on time if they used a specific drug according to the prescribed regimen.

Up to this point, the goals of any reputable business using information technology to better understand its customers, employees, and prospects are — oddly enough — identical to those of a professional identity thief. Both a business and a thief want access to personal data. However, the two sides part at the point where the information is used. The business wants to use the data for ethical and lawful purposes, complying with regulatory mandates and applicable laws. The identity thief does not.

Chapter 3

Mitigating the Risks — Personal Privacy and Data Protection

With few exceptions, the business processes detailed above involve major risks associated with maintaining personal privacy and data protection. As a result, today's organizations face significant pressures to:

- **Gain consumer confidence** by protecting personal data from risk of theft, fraud, and misuse
- **Limit business exposure** by providing access to personal data on a “need to know” basis only
- **Build competitive advantage** by developing a real-time method for maintaining data integrity, and by offering a secure, convenient way to validate and correct personal information
- **Comply with laws and regulations** by reporting on who had access to what information at any given time

Let's look at each of these four pressures, and at how organization can meet and overcome them.

Gaining Consumer Confidence

To be competitive, companies need to gain (or keep) consumer confidence in order to win (or keep) their business. Confidence includes the assurance that personal data will be protected effectively. Often, the biggest threat to personal data is an insider who is also a “keyholder” — a person who has access to internal systems because of contract or partnership arrangements with a company.

With employee turnover running at 100 percent in industries such as retail, it is not unusual for 20 percent of company accounts to belong to employees who haven't worked for the organization for five years or longer. These accounts never expire and allow former employees to roam freely inside the enterprise.

Companies that fail to shut the door on former employees and temporary employees who maintain valid company IDs and passwords run the risk of exposing sensitive business information, and thereby jeopardizing brand reputation, consumer confidence, and shareholder value. As an example, consider the harm suffered by the insurance firm previously mentioned in the introduction to this paper.

If an industry has many vendors, overcapacity will drive out the weak — including those perceived as taking unnecessary risks with private information. In certain industries, such as online stock market trading, the smallest breach of security can be fatal to customer confidence.

Limiting Business Exposure

Unfortunately, most organizations have difficulty in managing employees' access to private information. However, organizations must learn to manage access so that each employee — or partner, supplier, or distributor — has access on a “need to know” basis only.

Often, current employees have unrestricted access to company systems and data unrelated to their job responsibilities. Security policy should restrict employee access to pertinent areas of the business. For example, why should a customer service representative be allowed to access company inventory data? Moreover, whenever employees attempt to gain access to areas unrelated to their jobs, the organization must be able to detect this activity and take appropriate action.

In one celebrated case, the traitor Robert Hanssen regularly scanned numerous databases across the FBI seeking any files about himself or his neighbors — to see if he might have been discovered. Had this activity been monitored, it might have alerted internal security personnel that something was amiss earlier, and limited the scope of Hanssen's activities.

Building Competitive Advantage

Companies that maintain the integrity of their data in real time enjoy a competitive advantage. For example, online travel services and online brokerages compete directly in three dimensions: Timeliness, breadth, and accuracy. A consumer looking for a room or a trip, or an investor intending to trade a stock, wants rapid access to comprehensive information and correct access to prices and opportunities. If consumers discover later that they could have obtained a better deal elsewhere, they are less likely to be repeat customers of the online service.

In fact, since the online value proposition is speed, low cost, and accuracy, consumers are apt to compare their experience with respect to these three service levels. Firms that are unable to meet these criteria must redefine their value to their potential customers in other terms. For instance, an online travel service might not be the least expensive service but may offer a guarantee that the reservation will be honored. An online brokerage might not be the quickest to execute a trade but may supplement its trading with access to more robust investor research.

Similarly, a company can enhance its competitive advantage by developing a real-time method for maintaining data integrity, and by offering a secure, convenient way to validate and correct personal information. For instance, a B2C site could offer customer self-service to update their home address and credit card information. The user would communicate with the site over a secure link (Secure Sockets Layer — SSL). This process must itself be strongly authenticated. For protected classes of information, companies must balance user convenience against robust authentication. In one case, a healthcare provider in the New England area will not allow password resets either over the phone or through the Web site. Instead, the subscriber may place a request but the changed password will be delivered by postal mail. In that organization's judgment, the risk of releasing personal health information — a protected category under HIPAA regulations — was greater than the risk associated with inconveniencing users.

Complying With Laws and Regulations

Every business, and especially every e-business, must maintain control over its IT environment. At a minimum, its security program should be auditable; that is, the business must be able to keep track of who had access to which data at any given time. Few jurisdictions today will permit personal information to be placed at risk of disclosure without more robust controls than those that are now in place. Only by knowing who has access to what data can businesses hope to conform to the myriad laws and regulations governing the acquisition and use of personal information.

Chapter 4

The Current State of Privacy Legislation Worldwide

Across different jurisdictions, various laws and regulations govern the privacy of personal data. These laws take various approaches to privacy protection. For convenience of discussion, privacy legislation can be broken down into four groups:

- Countries that conform to the broad and general EU Directive on Data Protection
- Countries, such as the United States, that protect specific vertical categories of information
- States within the United States that have introduced privacy legislation
- Countries that have not enacted protections specifically for digitized personal information

We will discuss the first three groups.

EU Directive on Data Protection

The EU Directive on Data Protection does not attempt to classify specific types of personal data. Rather, it establishes a set of rules that address the handling of all types of personal data. In essence, those countries that have enacted national legislation enabling the EU Directive on Data Protection generally impose the following obligations on enterprises conducting business within their jurisdictions:

- Personal data must be kept confidential.
- Individuals need to know in advance, and in detail, what information will be collected about them, who will use it, how it will be used, where it will be stored, what procedure to follow to verify and update it, and how to effectively remove it. These functions are key elements of identity management, mentioned above.

The Directive also states that the baseline controls appropriate to achieve the required level of confidentiality and identity management should be drawn from the industry in which the subject organization operates. So, if an industry is generally pursuing ISO 17799 as a security baseline, then ISO 17799 will be the standard against which compliance will be measured.

United States Vertical and Regional Legislation

The United States Government has chosen to regulate privacy matters by region and industrial sector. Public companies must certify the integrity of their financial data to conform to the Sarbanes-Oxley Act. Financial data protection is described under the Financial Modernization Act, commonly known as Gramm-Leach-Bliley (GLB). Healthcare data is addressed by the Health Information Portability and Accountability Act (HIPAA) and 21 CFR part 11. Data concerning minors is addressed by the Children's Online Privacy Protection Act (COPPA).

Sarbanes-Oxley Act

The Sarbanes-Oxley Act introduces sweeping reform for financial reporting standards by publicly traded companies and requires that the CEO and CFO personally attest to the correctness and auditability of the systems that produce the organization's financial data. This requires that executives know who has access to what information. Specifically, the act requires attestation regarding financial data used to assemble the firm's financial reports. However, that statement can be seen as inadequate if the firm cannot account for the permissions granted to other employees regarding the processes from which the financial data is extracted. (For more information, see www.aicpa.org/info/sarbanes_oxley_summary.htm.)

Gramm-Leach-Bliley (GLB)

Gramm-Leach-Bliley dictates that organizations preserve the confidentiality of personal financial data. Violations are investigated by the Federal Trade Commission, which recently added a number of attorneys to its staff to support prosecutions. Depending on how the courts handle prosecutions, this statute could be narrowly constructed to address only the activities of specific organizations in the financial industry, or it could be more broadly interpreted to encompass any organization that acts as a custodian of any personal financial information — including any employer that permits online access to employee salary or benefits information. (For more information, see www.ftc.gov/os/2000/05/65fr33645.pdf.)

Health Information Portability and Accountability Act (HIPAA)

The Health Information Portability and Accountability Act directs healthcare providers to preserve the confidentiality of individual medical records. As with Gramm-Leach-Bliley, the courts have yet to determine the breadth of applicability of the statute. However, the penalties for violations are severe. Any hospital, doctor's office, dental clinic, HMO, health insurer, or similar organization found guilty of intentional violation of healthcare privacy "for commercial advantage, personal gain, or malicious harm," may face fines of up to \$250,000 — and the principals may face prison terms of up to ten years. In addition, *any* organization that maintains personal health records must establish an auditable process for granting and revoking permission to view and distribute those records. (For more information, see aspe.hhs.gov/admsimp/pl104191.htm#1176.)

21 CFR part 11

In the pharmaceutical industry, the Federal Drug Administration (FDA) has established guidelines for any individuals or organizations governed by the FDA who use electronic recordkeeping and electronic signatures (any digitized representation of a signature, including digital certificates and holographic images). These guidelines establish requirements for electronic recordkeeping, specifically requiring auditable procedures governing electronic records, to ensure the integrity of that data. As with Gramm-Leach-Bliley, sufficient controls over the processing of electronic records require robust and auditable controls over the provisioning of access to those systems. (For more information, see www.fda.gov/ora/compliance_ref/part11/FRs/updates/cpg-esig-enf.pdf and www.fda.gov/ora/compliance_ref/part11/FRs/updates/cpg-esig-enfnoa.htm.)

The Children’s Online Privacy Protection Act (COPPA)

The Children’s Online Privacy Protection Act establishes privacy protections for any organization holding information about children. If an organization releases personal data about a child (such as a home address), and that information is used to support a crime involving that child, the organization can be prosecuted as though it had committed the crime itself. (For more information, see www.ftc.gov/os/1999/10/64fr59888.htm.)

State-Level Legislation

California Senate Bill 1386

California Senate Bill 1386 requires any organization that loses a California citizen’s personal data to alert its California customers via “notification to major statewide media.” Personal data includes last name, first initial, and any of a number of items such as a driver’s license number, social security number, credit card number, or bank account number. Most U.S.-based organizations have customers who are citizens of California. These organizations need to understand their exposure and prepare to deliver this notification in the worst case scenario. (For more information, see info.sen.ca.gov/pub/01-02/bill/sen/sb_1351_1400/sb_1386_bill_20020926_chaptered.html.)

Other Acts

The National Conference of State Legislatures maintains a Web site that tracks legislation related to privacy protection and identity theft.

For a current list of pending and signed bills, see www.ncsl.org/programs/lis/privacy/idt-01legis.htm.

Privacy Legislation	Summary Overview
EU Directive on Data Protection	Establishes a set of rules that address the handling of all types of personal data
U.S. Sarbanes-Oxley Act (SOX)	Requires that the CEO and CFO of publicly traded companies personally attest to the correctness and auditability of the systems that produce the organization’s financial data
U.S. Gramm-Leach-Bliley (GLB)	Dictates that organizations preserve the confidentiality of personal financial data
U.S. Health Information Portability and Accountability Act (HIPAA)	Directs healthcare providers to preserve the confidentiality of individual medical records
U.S. 21 CFR part 11	Establishes electronic recordkeeping guidelines for any individuals or organizations governed by the FDA
U.S. The Children’s Online Privacy Protection Act (COPPA)	Establishes privacy protections for any organization holding information about children
California Senate Bill 1386	Requires that any organization that loses a California citizen’s personal data must alert its California customers via “notification to major statewide media”

Chapter 5

How Can Identity Management Help?

Identity management includes all aspects of obtaining, maintaining, securing, and controlling access privileges to, and the content of, personal data. This personal data can include contextual, enterprise-specific individual information, such as permissions and rules governing access to certain corporate resources, an individual's hire date, or a customer's purchase history, as well as global, nonenterprise personal data, such as birth date, home address, or emergency contact information. Both types of data present enterprise risks. Organizations must manage these risks according to accepted business practice and legislative mandate.

Identity management can help meet this goal. A comprehensive identity management solution offers user provisioning, profile management and data synchronization, access management, password management, directory services, and audit and reporting. Let's take a brief look at each of these capabilities.

User Provisioning

User provisioning is the set of activities within the broad scope of identity management that addresses the administration and management of contextual, enterprise-specific identity information. An effective provisioning solution gives the enterprise a single interface to correctly and completely grant an individual the appropriate permissions to access enterprise resources. For instance, a bank teller should be allowed to access the demand deposit application for a certain segment of the bank's customer population, while a customer should only be allowed to access the demand deposit application for his own accounts.

A comprehensive provisioning solution should be broad and flexible enough to cover all applications, platforms, and interfaces that a company might need to manage, or that an individual might need to use. An effective provisioning solution should also provide the equally crucial function of *deprovisioning*. That is, when an individual's relationship to an organization changes, the solution must allow the appropriate form of disconnect (rule-based, simple deletion, suspension, or transfer to another individual for audit or evaluation) for each relevant application and/or platform across the enterprise.

Increasingly, enterprises are focusing their resources on delivering specific value-added activities while outsourcing noncritical operations to third parties. This approach naturally generates a federation of (possibly competing) enterprises contributing to the creation of a set of products and/or services. As a result, a provisioning solution should permit grants and revocations of access privileges not only within an enterprise but also across enterprise boundaries, ideally using an open, standards-based approach to cross-enterprise integration, collaboration, and management.

Sarbanes-Oxley has significant meaning for corporations that must ensure security, reliability, and efficiency to consumers and investors. In an age when bad publicity erodes consumer and investor confidence, the risk of not moving aggressively will likely translate into reduced profitability and an expensive public relations recovery program. ...Provisioning is one IT solution which can make compliance with Sarbanes-Oxley easier, faster, and more reliable. Provisioning manages user access, simplifies processes, and improves internal quality.

– DMReview.com, May 2004

Profile Management

Beyond defining enterprise-specific (or federation-specific) contextual attributes, the enterprise needs to effectively manage other global personal data. A brokering approach should be used to enforce the accuracy and consistency of profile data across an enterprise and provide self-service functionality to individuals who want to maintain control over sensitive personal information. It should also automate the synchronization of this data across an enterprise's resources, further ensuring that all data is up to date and relevant. And since an individual might occupy multiple roles across a set of federated enterprises, the brokering solution should accommodate the policies in force within each enterprise.

Access Management

To protect the privacy of user information, standards-based access control mechanisms must be in place to manage appropriate levels of access based on roles and relationships with the organization. Access management helps organizations manage secure access to Web-based resources within the enterprise or across business-to-business (B2B) value chains. It should provide a comprehensive set of capabilities for managing identities and for enforcing authorized access to network services and resources.

Password Management

The more systems and applications that users have access to, the more important password policies become. Enforcing consistent, strong password policies across the enterprise is essential to providing high levels of security. Password management should be a centralized and highly secure function. Ideally, it should be automated and provide an easy-to-use self-service interface to the individual, in order to reduce the burden on the help desk (password problems are the #1 reason for calls to help desks).

Directory Management

Directory management is a key underpinning to providing an enterprise identity infrastructure that enables regulatory compliance. Enterprises that use intranets or the Internet to provide services to customers, employees, and business partners face the challenge of managing identity information for a multitude of users. LDAP directory architectures are the best practice for simplifying deployment of secure applications, customer/partner portals, and e-commerce operations.

Audit and Reporting

For the purposes of regulatory compliance and audit, the enterprise should have access to a forensically durable logging and auditing component. Some identity management solutions take no measures to preserve the integrity of log records; as a result, any individual with database administrator skills can alter or destroy log records. We are not suggesting a transaction log record, but rather a log indicating which authority granted or revoked each individual's right to access certain classes of information, how rules were developed or altered, and what delegation or recall of administrative capabilities is required within the enterprise or across the federation. Without this capability, the organization will be unable to verify the auditability of its critical IT systems.

All of the above capabilities should be standards-compliant to the extent that such standards are viable. A few examples include the Secure Assertion Markup Language (SAML), the Service Provisioning Markup Language (SPML), and the Liberty Alliance Project initiative supporting a federated identity management model.

Chapter 6

The Solution — End-to-End Identity Management from Sun

Sun offers a full suite of products designed to meet the identity management requirements described in this paper.

- **Sun Java™ System Identity Manager** lets the enterprise automate processes to guarantee that individuals have access only to those systems they need, and that once that access is no longer needed, it is withdrawn. It also provides a secure, centralized system for password management. Through automation and self-service, Java System Identity Manager eliminates the #1 source of costly help desk calls and, at the same time, enhances service and security.
- **Sun Java System Access Manager** is a security foundation that helps organizations manage secure access to an enterprises' Web applications both within the enterprise and across business-to-business (B2B) value chains. It provides open, standards-based authentication and policy-based authentication and authorization with a unified framework.
- **Sun Java System Directory Server Enterprise Edition** provides secure, highly available, scalable directory services for storing and managing accurate and reliable identity data. It increases security by serving as a front end to prevent denial of service (DoS) attacks and access by unauthorized users. Security is further improved through the ability to deny or allow access based on IP address, group membership, and other criteria.
- **Identity audit and reporting capabilities are available in both Java System Identity Manager and Java System Access Manager.** These capabilities maintain a forensically durable record of who has access to what. Deployed in the correct context of policy, these products can reinforce the integrity and auditability of each enterprise's business processes dealing with personal data.

Chapter 7

Next Steps

1. Double-check the obvious. Make sure that your organization has designated a compliance officer, that this person is up to date on all laws and regulations relevant to your business, and that a process is in place to monitor privacy legislation in all jurisdictions in which your organization operates.
2. Survey all instances of personal data and access privilege information acquired by or stored within the organization. The survey should include the nature of the information, the business process that requires it, and the mechanism for maintaining the confidentiality and accuracy of that information.
3. Develop an accurate assessment of which, if any, of the various types of personal data may present a risk to the organization, and what sanctions the organization might face if that information is lost, stolen, altered, or inadvertently disclosed.
4. Develop an approach to manage that risk, incorporating appropriate technology to amplify and preserve the integrity of the risk-management processes.
5. Automate those risk-management processes with the appropriate technology.

To learn more, please contact your Sun sales representative or visit www.sun.com/identity_mgmt.

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



Sun Worldwide Sales Offices: 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, Saudi Arabia +9661 273 4567, Singapore +65-6438-1888, Slovak Republic +421-2-4342-94-85, 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 +44-1-276-20444, United States +1-800-555-9SUN or +1-650-960-1300, Venezuela +58-2-905-3800, or online at sun.com/store

SUN © 2004 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, the Sun logo, Java, and The Network Is The Computer are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States 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. UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd. Information subject to change without notice. 07/04 R1.0