

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

# **THE ROLE OF IDENTITY MANAGEMENT IN MEETING THE CHALLENGES OF FINANCIAL SERVICES ORGANIZATIONS**

White Paper  
November 2007

## Table of Contents

<b>Executive Summary</b> .....	<b>1</b>
The role of identity management .....	2
<b>Financial Services Challenges and the Identity Management Response</b> .....	<b>3</b>
The challenge: Compliance .....	3
The identity management response: Improved internal controls .....	3
The challenge: Risk reduction .....	4
The identity management response: Limiting the potential for breaches .....	5
The challenge: Quality of service .....	5
The identity management response: Improved QoS through automation and federation .....	6
<b>Sun Identity Management for Financial Services</b> .....	<b>7</b>
A step-by-step approach to implementation .....	7
<b>Key Capabilities of Sun Identity Management for Financial Services</b> .....	<b>8</b>
Robust auditing and reporting .....	8
Secure control over sensitive information .....	8
Key enablers for improved QoS and increased growth .....	9
<b>Financial Services Challenges and Sun Identity Management: Case Studies</b> .....	<b>10</b>
Compliance in investment banking .....	10
Risk reduction in international banking .....	10
Quality of service in retail banking .....	11
<b>Conclusion</b> .....	<b>13</b>

## Chapter 1

# Executive Summary

From banks and investment brokerages to financial services professionals and insurance companies, financial services organizations of all kinds face a unique set of interdependent challenges today.

As part of one of the most highly regulated industries in the world, companies in the financial services sector are increasingly driven by the growing need to comply with regulatory and legal requirements governing the integrity, security, and privacy of the data they manage. And as companies that routinely handle extremely sensitive and private information for individuals and businesses, they are also front and center when it comes to the challenge of finding ways to reduce operational risks associated with keeping such data secure.

Meeting these challenges — regulatory compliance and risk reduction — can be a costly proposition if it's not approached with the right planning, strategy, and tactics. And that can create a third challenge. Because as long as companies have their hands full and their budgets tied up with these internal challenges, they will be hard-pressed to turn their focus toward opportunities to improve quality of service (QoS) and successfully pursue new growth and revenue.

Consider this: Even with the challenges in front of it today, the financial services industry faces unprecedented opportunity. The Internet opened the door for financial services companies to deliver more services to more customers than ever before. But they need to be ready. They must have plans and processes already in place for dealing with the fundamentals of compliance and risk reduction — so they can move on with the challenge of delivering QoS that will allow them to accelerate growth. And they must also put into place the infrastructure that will enable them to pursue growth efficiently and cost-effectively.

Identity management is a key component of the IT infrastructure to address all these challenges.

## The role of identity management

Identity management can make it possible for financial services companies to meet complex challenges. By providing them with the tools to closely control and manage access to sensitive information and valuable resources online, identity management enables financial services companies to address the issues on which their success or failure rides.

- **Compliance.** Identity management provides automated access tracking and reporting capabilities, which are essential to meeting audit requirements accurately and cost-effectively.
- **Risk reduction.** By allowing complete visibility into users' identities and access activities, and the ability to manage them centrally, identity management increases the security of sensitive online information and resources.
- **Quality of service.** Automation and federation are key principles to pursuing new levels of QoS. Automation eliminates slow, costly, error-prone manual processes for managing identities. Federation enables rapid roll out of customer services by enabling companies to efficiently share resources across traditional business boundaries.

The following pages contain detailed information about how identity management works within the financial services IT infrastructure to deliver on these points.

## Chapter 2

# Financial Services Challenges and the Identity Management Response

## The challenge: Compliance

The Financial Services industry is governed by some of the most rigorous regulatory mandates today. Companies in the sector are subject not only to the laws such as the Sarbanes-Oxley Act of 2002 which mandates the way publicly owned companies of all kinds maintain their financial data, but also to industry-specific legislation such as the Gramm-Leach-Bliley (GLB) Act in the US which includes provisions to protect consumers' personal financial information held by financial institutions. Not only that, but financial services companies which work in partnership with other companies around the world may be subject to international regulatory rules such as the European Union Data Protection Directive and Basel II which addresses capital adequacy. The Markets in Financial Instruments Directive (MiFID) which comes into effect in November 2007 has a number of requirements on client take-on which need to be addressed concerning profiling, classification and record keeping. With so many different regulations in play, the risk of compliance failure is significant and the cost can be high, whether it's a large fine for an audit failure or a tarnished reputation associated with a compliance failure becoming public.

The Know Your Customer regulations are also impacting the banks and especially the private client sections. Recent fines for AML compliance breaches have focused the minds in some of the banks to increase the priority of compliance efforts. Banks need to look into the areas of common impact on processes and systems to ensure that there is not duplication of effort and that those investments are made optimally. The banking industry as a whole is being faced with a huge regulatory burden at the moment, which is necessitating significant investment in new processes and accompanying IT.

## The identity management response: Improved internal controls

Identity management solutions that deliver comprehensive capabilities for monitoring, tracking, reporting on, and auditing access to relevant information and resources can help limit the risk of noncompliance. Within this context, to be an effective tool for financial services companies, identity management technology should specifically address essential capabilities such as:

- **Establishing and maintaining policies such as segregation of duties.** Establishing such policies is critical to complying both with broadly applied regulations such as Sarbanes-Oxley and industry-specific laws such as Gramm-Leach-Bliley, because it enables companies to delineate and demonstrate clear lines of demarcation for access to sensitive information. For example, consultants who architect business processes to enable compliance should not have the same levels of access as the financial auditors who audit those processes.
- **Providing instant knowledge of who has access to what.** The ability to know who has access to what information and resources at any time is another critical component for complying with laws that govern data integrity and privacy. An effective identity management solution should couple this ability with historical reporting on access activities, so that it's possible to determine and report on not only who has access in the present, but also who had access in the past within a specified time frame. This is especially critical in today's environment of frequent change due to company mergers and acquisitions, contracted and outsourced operations, and mobile workforces.
- **Automating audit procedures.** Automation is an important aspect of effective identity management because it makes compliance and auditing processes repeatable and sustainable over the long term. This has two important implications. One, it limits the risk that compliance and auditing will be compromised by manual error. Two, it reduces the administrative burden and associated costs of these ad hoc processes.

### The challenge: Risk reduction

At a time when identity theft and fraud continue to dominate headlines worldwide, no other industry has been as squarely in the hot seat as financial services. Public scrutiny of its policies and experiences with protecting customers and their sensitive information has known no limits. This is understandable, given that the financial arena is one in which people are at great risk for seeing sensitive data compromised. Consumers live in constant fear about unauthorized persons gaining access to their bank account data, credit card numbers, and other financial information. Some have begun to limit their online financial services activity as a result. Companies that can demonstrate their ability to guard against breaches will reap the benefits of engendering customer goodwill and loyalty and avoiding negative press.

## The identity management response: Limiting the potential for breaches

Identity management solutions that feature controls such as centralized management and visibility, rule- and role-based access, and strong authentication can allow appropriate exchanges of data and transactions while still protecting the privacy and security of sensitive information. An effective approach to identity management should place a demonstrable premium on guarding critical information by:

- **Providing a single point of control for managing identities.** A single point of control lowers the risk of a security breach by making it easier to support security policy across a financial services organization's divisions or departments. This becomes increasingly critical as more users from more points outside traditional organizational boundaries, such as contracted external insurance adjusters or auditors, have access to sensitive information and resources. There must be one authoritative point of control for managing all these users.
- **Enabling complete visibility into access and events.** When administrators can instantly see who has access to what information at any time, they can respond immediately to any violations or other issues that may arise. A complete identity management system for a financial services environment should not only show administrators who has access, it should also alert them to policy violations and automatically initiate remedial actions to limit potential damage. Centralized administration can also have the added benefit of reducing the costs of overseeing multiple systems.
- **Implementing rule- and role-based access control policies.** Among financial services organizations and their partners, access depends on a wide variety of factors — such as a user's role within an organization or an external party's relationship to it. Not only that, the status of these factors is subject to change. A mid-level manager may be promoted to a higher position, for example, necessitating a change in access privileges. Rule- and role-based policies offer the flexibility for financial services organizations to set rules for access control based on a variety of criteria, including users, organizations, resources, roles, or groups, and to instantly and easily change access privileges when a user's roles or relationships change.

## The challenge: Quality of service

Winning new customers and keeping existing ones presents a tough set of challenges for financial services organizations that seek to achieve new levels of growth and revenue. These companies must find ways to cost-effectively provide the increasingly high levels of service that are required to drive customer satisfaction and loyalty. One way to significantly improve the QoS is to go beyond the financial services organization's own capabilities to collaborate with other companies, both within and outside the financial services arena — such as health care providers, travel services, and entertainment companies. This can make it possible to offer more and better services than ever, to more customers than ever.

## The identity management response: Improved QoS through automation and federation

Identity management that combines high levels of automation with new capabilities for federation can help raise QoS and pave the way for new growth at a reasonable cost, and without making undue demands on organizational resources. The right identity management solutions can help financial services organizations achieve this goal by:

- **Providing extensive self-service capabilities.** Allowing customers and other users to handle everyday identity management tasks on their own, at their convenience, increases satisfaction levels. By setting up and managing their own passwords and accounts with minimal help desk involvement, they can get up and running faster and easily enjoy more services. Automated identity management systems make high levels of self-service available to growing numbers of users both within and outside the financial services organization, and at an extremely low cost. Savings are found in reduced help desk and administrative costs, while productivity gains are realized through reduced time to access.
- **Extending identity management services to partners.** Collaborating with other companies to deliver more extensive financial services offerings requires a technology infrastructure that makes it easy to extend identity management across traditional boundaries. Financial services organizations that want to work with multiple partners should seek an identity management solution specifically designed for repeatable integration of provisioning and other services with multiple entities. This will ensure a higher QoS, both among partners and to the end customer. Combining loans, savings, credit cards, and checking services, whether internal or cross-partner offerings, can improve customer satisfaction.
- **Enabling large-scale partnerships through federation.** One of the biggest obstacles to successful collaboration with other companies to offer more services has been the time, expense, and resources required to establish common security and identity infrastructures among partners. Federation creates a secure, repeatable framework for easily extending these infrastructures with multiple partners across traditional boundaries — instead of reinventing the wheel each time. Identity management solutions with effective federation capabilities can help reduce the risk associated with taking on new partners to deliver more services. It may also meet the demands of trading partners dealing in securities between companies, which are seeking more seamless yet secure methods of collaboration.

## Chapter 3

# Sun Identity Management for Financial Services

Sun identity management for financial services delivers all the capabilities that companies in this sector require to operate compliantly and securely, and at the same time deliver QoS that can drive successful business growth.

- **Sun Java System Identity Manager**

Identity Manager provides complete and scalable capabilities for user provisioning and identity auditing for preventative and detective compliance. Identity Manager enhances the security of private financial and other customer information, and improves compliance and audit performance.

- **Sun Java System Access Manager**

Access Manager enables Web Single Sign-on (SSO), secure access control, and federation services. A standard-based solution for secure access, it enables interoperability across multiple technology platforms within a financial services organization, as well as across extranets. It also uses role- and rule-based access control to enhance security.

- **Sun Java System Federation Manager**

Federation Manager improves financial services organizations' partnering capabilities by focusing on quickly establishing Trusted Domains and extending them to multiple partners. Federation Manager simplifies deployment into existing IT infrastructures, leverages existing authentication and authorization policies, and enables rapid, repeatable integration with multiple partners.

- **Sun Java System Directory Server Enterprise Edition**

Directory Server Enterprise Edition improves operational efficiency with secure and reliable directory services. DSEE is a secure, highly available, scalable and easy-to-manage directory infrastructure that effectively manages identities in growing and dynamic environments.

## A step-by-step approach to implementation

Open and integratable, Sun identity management products are designed expressly to reduce integration cost and complexity in existing environments. And because the portfolio is modular, financial services companies can take a multistep, phased approach to roll out, starting small and then building toward a comprehensive implementation. For example, you could start with capabilities to improve compliance, then move into increasing the security of sensitive information and resources, and ultimately implement service provider and federation functionalities to increase QoS and take advantage of growth opportunities.

## Chapter 4

# Key Capabilities of Sun Identity Management for Financial Services

## Robust auditing and reporting

To help ensure compliance with legislative requirements, Sun identity management solutions feature:

- Automated processes for compliance with regulations governing privacy, security, and financial integrity and affecting operational controls, personal financial information, and credit transactions
- Role- and rule-based approach to support repeatable, auditable, enforceable processes, which may be applied to financial account management, credit maintenance, and fraud prevention
- Fractional replication for protecting sensitive attributes and meeting compliance requirements while protecting financial privacy
- Enterprise-wide identity auditing and reporting across accounts, records, branches, and contractors operating in geographically separate divisions or projects
- Ability to review the status of access privileges at any time to meet audit requirements and governmental mandates, as well as to help prevent internal identity fraud

## Secure control over sensitive information

Sun identity management solutions employ a variety of capabilities, features, and tools to ensure that access to sensitive information is subject to the most secure control possible. These include:

- Compatibility with Liberty Alliance specifications for easier management of personal privacy issues when handling customer financial information and transaction records
- Conformance to global standards such as the BS 7799 security specification and others affecting control of capital, insurance liabilities, and customer privacy
- Centralized visibility and control over access to critical systems and information for auditing that access, monitoring separation of financial duties, and taking remedial action
- Real-time insight into who has access to what resources and data at any given time, which is particularly important when contracting financial services from multiple, changing, outsourced providers

- Automatic detection of and response to potential risks, such as dormant accounts which might be accessed for fraudulent purposes as a result of identity theft
- Role-based access control and centralized authentication to protect widespread financial resources from inappropriate access or human error in manual financial controls
- Two-factor authentication technology for increased protection of high-value financial data that is accessed online from many locations or devices
- Consistent enforcement of corporate security policies securing personal financial records

### **Key enablers for improved QoS and increased growth**

Sun identity management solutions help win new customers and engender loyalty in existing ones by enabling higher QoS. Key capabilities include:

- Self-service password management and other everyday tasks to improve the user experience when customers access their accounts and records
- Reduced costs for higher QoS through automation of previously manual tasks — such as help desk, claim processing, and credit card clearing — where secure personal information is maintained
- Ability to leverage existing authentication, authorization and security policies with partners when creating online markets, exchanges, or contract services
- Support for major federation protocols so financial partners can collaborate across their business domains for increased economies
- Repeatable integration for low-cost, rapid roll out of services across multiple financial service partners, branches, or markets

## Chapter 5

# Financial Services Challenges and Sun Identity Management: Case Studies

Several large financial services organizations are using Sun identity management to address specific challenges in their industry.

## Compliance in investment banking

**The challenge:** A worldwide investment banking firm was faced with the challenge of ensuring that all of the many financial applications it manages were in compliance with a multitude of regulations. To accomplish this, the firm needed a solution that would work across all of its applications to automate policies, check discrepancies, and report exceptions.

**The solution:** Sun identity management for financial services automatically checks access policies, instigates access policy reviews, and reports exceptions to administrators so that they can take appropriate action. The solution also simplifies reporting by aggregating it into an automated, workflow-driven policy that drives remediation.

**The technology:** The access management capabilities of the Sun solution enable the firm to create policies to control employee access privileges based on the employee's role within the organization, including making changes to privileges any time that role changes. In addition, the audit component of the solution automatically checks privileges against policies and generates periodic access reviews to report exceptions, eliminating manual, error-prone processes. Administrators can also initiate checks to review reports at any time.

**The benefits:** By automating compliance-related processes, the firm significantly reduced the risk of regulatory violations, while at the same time, it relieved compliance-associated administrative burdens. Timely review of account access against live resources, for example, saves time in remediation and ensures information is current. In addition, the aggregation of reports with automated workflow makes remediation a systematic, repeatable process.

## Risk reduction in international banking

**The challenge:** An international, interbanking group needed to facilitate collaborative interactions among 11 member banks, while protecting the integrity of its data systems. As the guarantor of rules defining functions such as credit card issuance, cash withdrawal management, and payment acceptance, the group was responsible for ensuring that its systems were reliable and secure.

**The solution:** The group chose Sun identity management to address the security requirements of an access environment involving multiple organizations and high user turnover, specifically:

- Ability to immediately suspend access privileges when a user's association with the group ends
- Accurate, up-to-date visibility into user access
- Ongoing detection and reporting of potential security risks and security policy exceptions

**The technology:** Automation is the key to enabling the group to achieve its goals. The Sun identity management solution automates user provisioning and deprovisioning processes, eliminating the security risks associated with delays in changing user privileges when users' roles change. The Sun solution also enables immediate visibility into who has access to what resources at any given time, and automatically detects and reports on potential problems.

**The benefits:** Sun identity management provides reliable, repeatable processes for provisioning and deprovisioning a large, diverse, and constantly changing set of users, reducing the risk of security breaches. Centralized visibility into access and ongoing risk detection further secure the environment, as well as helping to ensure compliance with regulatory requirements.

## Quality of service in retail banking

**The challenge:** A nationwide retail banking organization wanted to create a more satisfying customer experience by integrating services from external partners into its online offering. By improving QoS in this way, the company hoped to attract new customers and engender loyalty in existing ones. The technology to support the integration of services would therefore have to ensure a good customer experience no matter how many customers would ultimately be served or how many services would be offered to them.

**The solution:** Sun identity management for financial services enables federation across the company's partners, streamlining the process of delivering externally provided services on the company Web site. Sun identity management also allows a convenient single sign-on for customers using multiple services, meaning that they can easily access multiple applications without multiple logins.

**The technology:** Sun federation services enable seamless transitions from application to application online, through an information-gathering and indexing process that is entirely transparent to the customer. Here's how it works. When a user logs on, Sun identity management technology:

- Logs identity information, such as attribute or authorization
- Creates an index to that information
- Redirects the user's browser to the requested application
- Provides the application with the index to the identity

However, all the user knows is that the appropriate content instantly appears in the browser. One of the keys to enabling this entire process is compliance with the Security Assertions Markup Language (SAML) 1.1 specification. In fact, Sun's leadership in driving identity management and federation standards was central to the selection of Sun.

**The benefits:** Allowing customers to access more services without logging into multiple sites with different passwords provides a distinct competitive advantage. In addition, because Sun identity management is standards-based, it supports growth by making it easy to ramp up business relationships with new partners. It also scales to accommodate growing user populations.

## Chapter 6

# Conclusion

Financial services organizations today must cope with unique and unprecedented challenges in the realms of regulatory compliance, risk reduction, and quality of service. Sun identity management for financial services provides a complete portfolio of products to help them address these issues, efficiently and cost-effectively.

To learn more about identity management and its role in meeting the challenges faced by today's financial services organizations, or to request additional information about Sun identity management solutions, visit [www.sun.com/identity](http://www.sun.com/identity).

