Secure SOA environments for banking.

June 2006
Executive summary

Today, banks face complex competitive and regulatory challenges. In order to meet the challenges of today and the future, institutions must create flexible frameworks to simplify the integration between applications, processes and technologies – both internally and across business partners.

By addressing this need, service oriented architecture (SOA) helps banks improve customer service, reduce costs and leverage legacy applications to deliver more value-added services to customers and partners.

The seamlessness implicit in an SOA environment – integrating formerly separate domains of authorization and control – requires new security technology to manage and protect customer data. Security issues are particularly pressing for banks, based on the nature of banking itself as well as the increased burden of compliance with U.S. and international regulations.

IBM Tivoli® products and services enable banks to secure SOA applications, provide comprehensive identity management, improve compliance reporting, reduce administration costs and deliver an enhanced user experience based on single sign-on access to multiple services.

SOA for banking addresses today’s challenges

The banking sector today faces lower margins, increased consolidations, new regulations and rapidly changing customer demands.

Clearly, the challenges facing banks have never been greater. As a result, banks have developed a number of innovative strategies – many of them supported by advances in information technology (IT) – to lower costs, improve customer offerings and ensure their continued competitiveness in the marketplace.
To take full advantage of today’s technology, a bank needs new ways to evolve its IT infrastructure beyond traditional silos of information and functionality. More specifically, it needs an IT infrastructure where systems, databases and applications can work together efficiently, reliably and cost-effectively.

To meet these needs, many banks have adopted an IT strategy based on SOA. SOA provides an enterprise-wide, standards-based integration architecture that effectively overcomes differences in platforms, software architecture, languages and network protocols.

For banks, SOA-based applications can provide seamless integration across the enterprise and among business partners, helping to improve services, reduce costs and leverage legacy environments.

**SOA introduces new security requirements**

The openness introduced by SOA-based applications requires a new approach for the management of security within the company and across partners. The need for SOA security is particularly pressing for banks, based on several factors.

First, the nature of banking itself both drives and is driven by sensitive information regarding everything from third-party assets to customer data. Banks must provide the highest levels of confidentiality, backed by strong protection for account, asset and transaction information.

Secondly, banks must comply with a growing number of regulatory acts and standards, such as Sarbanes-Oxley and Basel II, which involve rigorous requirements for security, auditing and reporting.
As a result of the critical needs for confidentiality, information protection and compliance, a bank implementing a secure SOA environment must fully address the following issues:

- **Authentication** — A common identity management solution across the infrastructure is needed to successfully authenticate and manage user identity.
- **Authorization** — An automated system for access and privileges is required to identify the user once and then automatically map the user’s identity across multiple systems, services and infrastructure components.
- **Security for legacy applications** — SOA supports the valuable reuse of legacy applications. However, reuse also requires added functionality for proper security management—for example, the ability to integrate IBM CICS®-based environments and Web applications.
- **Compliance** — Proper compliance involves all the issues raised by authentication, authorization and application reuse. Security controls as well as reporting and audit capabilities must form an integral part of an SOA environment.
- **Real-time security monitoring** — No technology infrastructure is ever 100 percent secure, and complex infrastructures change daily. SOA environments must be consistently monitored for security attacks, malware, misconfigurations and internal misuse.
- **User experience** — Users must be able to navigate easily across SOA and Web services with a minimum of password and identity verification procedures.

Address security requirements with IBM solutions for SOA security management

For the banking industry, IBM offers a comprehensive, tightly integrated family of solutions to support security-rich SOA environments:

- **IBM Tivoli Federated Identity Manager** supports the management of federated identities and access to SOA-based Web services that span the security domains of banks and partners.
IBM Tivoli Identity Manager delivers a security-rich, automated and policy-based user management solution that helps effectively manage identities, passwords and access to both Web services and legacy applications.

IBM Tivoli Access Manager for e-business provides run-time authorization, centralized policy-based user management in conjunction with policy enforcement points and auditing for single sign-on to Web applications in an SOA implementation.

IBM Tivoli Security Operations Manager provides a centralized platform for monitoring, analyzing and investigating security incidents and policy violations in real time. The platform analyzes and correlates logs from throughout the entire IT infrastructure – including intrusion detection systems, firewalls, hosts and servers – as well as the application layer where most SOA attacks will take place.

View secured SOA environments in three banking scenarios

To better understand the real-world benefits of a security-rich SOA environment for banking, we can consider three scenarios in which banks use SOA and IBM Tivoli solutions to deliver services to their customers in a protected, cost-effective way that supports compliance efforts.
1. Channels management

Banks are increasing their focus on managing their sales channels as a means to improve the quality and depth of the information they collect about their customers. This enables banks to better serve their customers and build marketing programs to more effectively identify cross-selling opportunities and offer complementary services.

Need:

A customer deposits a $70,000 check into her savings account, but she does not have any investment products through the bank. A financial planner at the bank needs controlled access to her account profile so he can recommend appropriate investments from the bank’s portfolio of products.

Process:

Preconfigured customer relationship management (CRM) software alerts the bank’s Investment Services department that a large deposit from the customer has been made. An e-mail notification is sent automatically to the financial planner at the local bank.

The financial planner is given controlled access to the account profile of the customer. To access the required customer account information and profiles, financial planners must submit their credentials to a secured application. Once the credentials have been verified and approved, financial planners are free to view and revise the status and portfolio information of their clients. Tivoli Access
Manager for e-business authenticates the identity of the financial planner and authorizes him to access a selection of the customer’s information based on the bank’s service offerings and the customer’s possible needs.

The financial planner can now begin to prepare an investment recommendation. He reviews the customer’s profile and creates a list of appropriate products. The financial planner also logs on to the bank’s intranet to collect information about the mortgage services offered by the bank. Finally, he accesses the Web site of a brokerage company, one of the bank’s channel partners, to collect investment options that meet the customer’s risk and age profile. With Tivoli Federated Identity Manager, his authenticated identity is automatically extended to the brokerage company’s Web services, thereby allowing seamless access to its investment planning engines. The financial planner then selects and prepackages a set of financial products.

At this point, the financial planner is well prepared to contact the customer and propose financial services and products based on her particular circumstances.

Services integrated through SOA:

- CRM
- Portfolio planning
- Real-time financial data
- Protection against identity theft and fraud
- E-mail

2. Account services

Need:

A customer wants to open a new account online and subscribe to a variety of services. The bank must be able to address his needs quickly and effectively, helping to establish a strong, long-lasting relationship.
Secure SOA environments for banking.

**Process:**

The customer visits the bank’s Web site and goes to the appropriate page to open an account. He submits his personal information and other biographical data. Next, he is asked to provide a personal password and ID information, which is then verified against his customer profile to match the password information with previously supplied identification records. With Tivoli Federated Identity Manager, this information is collected through the bank’s Web services and securely stored on the bank’s mainframe system.

The customer also selects automatic deposit to his account for his paychecks. Tivoli Federated Identity Manager is used to federate his identity with the Automated Clearing House (ACH) network, and an auto-deposit is established with his employer.

As the customer is setting up his new account and services, Tivoli Identity Manager automatically creates a customer profile through its CRM software. Once the customer has selected services to access, this information is used by Tivoli Access Manager for e-business to audit and control his interactions with the bank.

With the account and its related services set up, the customer is able to view account balance information online, use ATM services for transactions and visit branch offices to deposit or withdraw cash.

Services integrated through SOA:

- Credit checking
- CRM
- Portfolio or customer account management
- Records management
- Web infrastructure housing online account management services
3. Records management for compliance

Need:

For compliance, banks need a cost-effective way to maintain audit trails, preserve access logs and archive business records in an accurate, up-to-date and comprehensive manner.

Process:

A customer makes a large deposit to her savings account. This prompts an automatic notification to a financial planner at the bank, identifying her as a prospect for additional banking products.

The financial planner uses his identification credentials to log on to the account profile database. Tivoli Access Manager for e-business authenticates the financial planner and authorizes him to access only those applications he needs to put together a detailed sales proposal.

In developing his proposal, the financial planner navigates across several different Web applications for customer accounts and services. He also visits the Web site of a business partner to access information about their investment products.

Each of these applications requires credentials for access. Tivoli Federated Identity Manager, in conjunction with Tivoli Access Manager for e-business, provides security-rich, single sign-on for the financial planner, both within the bank’s security domain and at the partner Web site.

The financial planner is now ready to contact the customer with a customized proposal. Each transaction in this sales process must be digitally stored and maintained for records-keeping purposes. Tivoli Access Manager for e-business records each access to the Web applications. These records are
used to generate reports for verifying compliance with various corporate and regulatory requirements. Also, Tivoli Access Manager for e-business generates a complete list of users with access to each Web application along with a cross-referenced list of SOA services that have been granted to each user.

Services integrated through SOA:

- Business line applications such as loan originations and investment products through business partners
- CRM
- Account management

**Summary**

With IBM Tivoli solutions, a bank can establish and maintain an effective SOA environment that maximizes security and facilitates compliance.

Tivoli Identity Manager, Tivoli Access Manager for e-business, Tivoli Federated Identity Manager and Tivoli Security Operations Manager provide a comprehensive and integrated solution that helps banks:

- Simplify integration between systems and applications across the enterprise and with other organizations across the Internet.
- Facilitate security and compliance initiatives by helping to reduce exposure and providing audit and tracking reports.
- Enhance end-user experience through single sign-on and seamless access to multiple services.
- Create revenue-generating opportunities by enabling controlled access to customer information and supporting partnerships with financial service providers.
- Reduce administration overhead, including help-desk costs, by providing self-care password and personal profile management.
About Tivoli software from IBM

Tivoli software from IBM helps organizations efficiently and effectively manage information technology (IT) resources, tasks and processes in order to meet ever-shifting business requirements and deliver flexible and responsive IT service management, while helping to reduce costs. The Tivoli portfolio spans software for security, compliance, storage, performance, availability, configuration, operations and IT lifecycle management, and is backed by world-class IBM services, support and research.

For more information

To learn more about IBM Tivoli solutions and maximizing the security of SOA environments for banking, contact an IBM representative or IBM Business Partner, or visit ibm.com/tivoli