White Paper

Services-Oriented Architecture (SOA) and Federated Identity Management (FIM)

By:

Jon Oltsik
Enterprise Strategy Group

November 2006

Table of Contents

20 Asylum Street, Milford, MA 01757 ● 508-482-0188 ● www.enterprisestrategygroup.com ● info@enterprisestrategygroup.com

Executive Summary

Business requirements seem to accelerate on a daily basis. Leading companies remain ready to respond to customer whims, outsource business processes, improve internal controls, and respond to changing regulations. Legacy IT infrastructure simply wasn't designed to fill today's business requirements but it is ludicrous to suggest "ripping and replacing" valuable assets.

Is there a solution to this paradox? ESG believes that the answer is yes. This paper concludes:

- **SOA can provide the necessary application services.** SOA essentially "wraps" existing systems and applications with web services interface. Yes, SOA can be a significant project but the investment can ease application integration, marry web-based delivery with mission-critical mainframe applications, and provide a platform for rapid development and extending applications to external constituencies.

- **SOA needs Federated Identity Management (FIM).** The often overlooked part of SOA is related to managing identity authentication, authorization, accounting, and security. Existing stovepiped identity management infrastructure wasn't built for these functions. What's needed is federated identity management (an architecture based upon open standards) as a complement to SOA.

- **IBM Tivoli Federated Identity Manager can make the federated identity management vision a reality.** IBM Tivoli Federated Identity Manager can bring FIM from concept to implementation. Tivoli FIM can act as a federated identity middleware bridge between external business partners and SOA security domains. In this role, Tivoli FIM, centralizes operations, enables rapid user provisioning, identity propagation, customizes business rules, and acts as a hub for token mediation, identity mapping, logging and reporting.

Business Agility Demands IT Agility

Ask any CEO if their business has changed over the last 10 years and you'll likely receive an incredulous glare in response. Regardless of industry type, company size, or geographic location, executives agree that business is becoming more demanding, competitive, and fast-paced each day. What is driving these unprecedented changes?

- **Globalization adds new competition and business model pressures**. The end of totalitarian governments, burgeoning capitalism, and decades of investment in developing nations has given rise to new global competitors based in areas like Eastern Europe, China, and India. Unlike any other time in history, these new players possess a combination of educated workers, low hourly wages, and advanced technology. These forces demand that established businesses examine their business models, cut costs, and try to out-innovate offshore upstarts.

- **Mergers and acquisitions demand rapid integration.** Globalization has also combined with industry deregulation to accelerate consolidation in multiple industries. M&A activity success or failure comes down to efficient and effective process and systems integration.

- **Specialization forces more internal scrutiny.** Even the largest businesses now realize that they can't be good at everything. In order to focus their firms business activities, many CEOs are examining their business operations looking for opportunities to outsource skills or entire business processes. Call center operations, human resources activities, and software development outsourcing alone account for a market of over $100 billion

20 Asylum Street, Milford, MA 01757 ● 508-482-0188 ● www.enterprisestrategygroup.com ● info@enterprisestrategygroup.com

(source: the Outsourcing Journal).

- **Regulations require more controls and oversight.** In the midst of rapid business trends, companies are also required to do a better job of instituting tight controls on IT systems and private information while maintaining up-to-date records on all activities. While the initial challenge is simply achieving compliance, smart firms are using the compliance requirement as a means to automate processes, improve efficiencies, and maximize productivity.

Each of the trends described above has a high dependency on corporate IT. Today's CIO is responsible for extending internal systems to outside constituents, developing new applications, managing outsourcers, and enabling users to dig through the haystacks of corporate data in order to find the valuable needles. As such, any limitations in IT flexibility or responsiveness can jeopardize the entire business itself.

SOA Meets Business Requirements

Real-time business demands are a mismatch for stovepiped IT systems or complex application integration initiatives. Given these pressing needs, many firms are building a Services-Oriented Architecture (SOA) as an IT backbone in order to provide the flexibility and agility needed to meet new business needs. SOA can be seen as a business-centric IT architectural approach for integrating business applications as linked, repeatable business tasks or services.

Unlike previous attempts at application interoperability, SOA is built on top of widely accepted technology standards like XML, SOAP, and HTTP. Enterprise companies report that SOA can:

- **Accelerate application development.** Rather than modify existing applications with hundreds of lines of new code, SOA allows developers to add business logic discretely as new web services. What's more, SOA is object-based allowing code to be reused over and over again. Want to enable an existing application service for a new partner? SOA makes this process far more efficient.

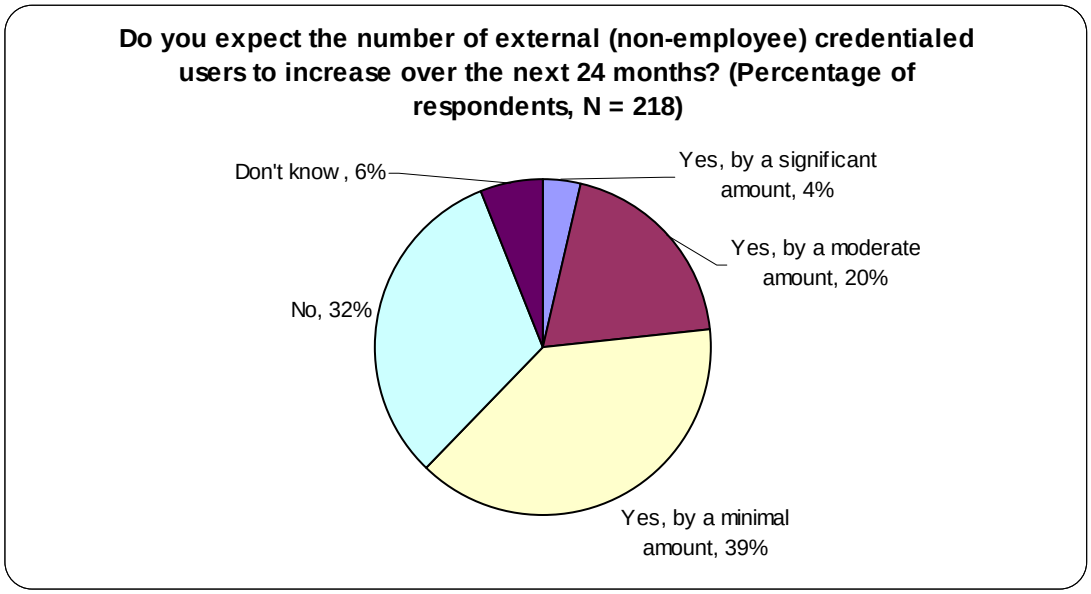
- **Ease application integration.** With standards like SOAP, UDDI, and WSDL, SOA can take existing business application silos and present them as services. With SOA, integration tasks that once took months of laborious customer coding can now be accomplished in a fraction of the time.

- **Open internal assets to outsiders.** The combination of rapid application development and simplified application integration provides enterprises with a way to extend and customize valuable internal applications and present them over the web for business partners, suppliers, and customers – a growing requirement in most large organizations (see Figure 1). In this way, SOA is especially useful for mainframe shops as it streamlines the process for opening mission-critical mainframe applications and data to web-connected outsiders.

With these technology underpinnings, SOA holds the promise of a new level of IT responsiveness. SOA can provide more efficient ways to enable user collaboration, re-engineer business processes, and share data.

20 Asylum Street, Milford, MA 01757 ● 508-482-0188 ● www.enterprisestrategygroup.com ● info@enterprisestrategygroup.com

Figure 1. Enterprise Plan to Extend Internal Systems to Outside Constituents



Identity Remains a Weak Link in the SOA Chain

SOA creates a new standards-based dynamic infrastructure for inter-enterprise collaboration and data exchange. This is a great enabling technology, but for SOA to work, it must be complemented by identity and trust. In an SOA context, identity and trust could encompass individual users, organizational units, corporations, or even web services themselves. Before utilizing SOA to provide a supplier with forecast information, a manufacturer must be certain that the requesting party is actually the supplier in question (as opposed to a competitor or spy) and that the "rules of engagement" for data exchange are established and enforced.

Establishing identity and trust relationships depends upon a combination of factors including contractual terms, privacy laws, and liabilities. While cumbersome, motivated business attorneys have always had the wherewithal to plow through this process. On the other hand, the technology infrastructure around identity and trust has been a far greater challenge for several reasons:

- **Users need accounts on multiple systems.** In order to get their jobs done, users were required to log on to a multitude of networks, business applications, and enterprise systems. Providing access to outsiders meant the same tedious account creation process, role definition, and user administration for network, application, and system access. Business partner employees will be less than enthusiastic when a new web services-based application claiming to automate order processing requires 5 new user name/password combinations. This may be acceptable in limited numbers but does not map well with an SOA model designed for high volume and massive scale.

- **B2B can demand a complex identity infrastructure.** Conducting e-business across multiple companies demands some type of cross-site identity infrastructure based upon things like X.509 digital certificates, PKI, and Certificate Authorities. If two business partners use two different authentication schemes, will the business benefit of SOA outweigh the technology burden of managing multiple identity infrastructures? Again, this process is manageable in small controlled industry communities but may be too

restrictive for more dynamic business processes and SOA.

- **End-to-end transaction auditing was difficult if not impossible.** Government regulations require firms to capture information about user access, behavior, and transaction activity. This information can be difficult to come by when users access multi-tiered application from web servers all the way back to mainframe data centers. When the compliance auditors demand to know which external users accessed the customer database, IT administrators will be forced to sort through multiple system and application logs to try and find all of the right puzzle pieces.

These are more than minor glitches. Lacking a scaleable infrastructure for identity, the SOA effort could suffer (see Table 1). To avoid this issue, the identity infrastructure must provide the same types of services as SOA itself. In other words, legacy identity infrastructure must be presented as secure identity services and provide the ability for the dynamic and accurate exchange of commonly understood identity information.

Table 1. Today's Identity Infrastructure Could Hamper SOA

SOA Requirement	Identity Infrastructure Limitation
Rapid user account provisioning	Stovepiped identity infrastructure means provisioning and managing multiple accounts for each user.
Organizational identity and identity propagation	Many different methods for authentication. Distributed identity infrastructure would also require access control rules on a system-by-system basis. Propagation of identities across service requests spanning security domains becomes much more important in the context of SOA.
End-to-end auditing	System-based log files make it difficult or impossible to understand user activities on a transaction-by-transaction basis.

Federated Identity Management and SOA

Fortunately, the technology industry recognized the problems around exchanging identity information over the web several years ago. Over the past 5 years, industry groups like the Liberty Alliance and OASIS developed a number of web-based identity standards that work together in providing a distributed model known as federated identity management. Federated identity management can be defined as an industry framework built on top of industry standards that let subscribers from disparate organizations use their internal identification data to obtain access to the networks of all enterprises in the group.

Like SOA, the beauty of federated identity management is that the framework, protocols, and standards extend existing identity management tools. Using standards like Liberty Alliance, SAML, and WS*, federated identity management enables (see Figure 2):

- **Common rules for information exchange.** Federated identity management is like SOA in that it defines a set of technology standards and protocols regardless of an organization's location, size, or technology infrastructure. In this way, federated identity management mirrors the dynamic scalable nature of SOA. Through SOA and federated identity management, multiple parties can now form ad-hoc relationships, provision users, exchange information, and integrate business applications -- without jumping through

20 Asylum Street, Milford, MA 01757 ● 508-482-0188 ● www.enterprisestrategygroup.com ● info@enterprisestrategygroup.com

technology integration hoops.

- **Authentication and authorization clarity.** Federated identity management provides a common way for individuals, web services, or organizations to identify who they are and what they are allowed to do. When Alice the purchasing manager wants to order supplies from Bob's Supplies, federated identity management will issue a standard security token or SAML assertion that describes Alice's user, role, and organization. Based upon this information exchange, Bob can be sure that the user and order are in fact legitimate.

- **Confidentiality and integrity communications and data exchange.** The WS-Security and WS-Trust specifications protect SOAP envelope headers and content as it is exchanged between organizations. In this way, federated identity management information cannot be compromised or tampered with by a man-in-the-middle attack. WS-Security can also match identity and time-stamped transactions for non-repudiation. When Alice tells her boss that she did not order 500 widgets from Bob, WS-Security can provide an indisputable record of the order containing Alice's security token, order information and time stamp as proof.

- **Federated Single-Sign-On (SSO) and provisioning.** Federated identity management extends the conveniences of SSO beyond the borders of the enterprise through SAML, Liberty and WS-Federation standards. Once Alice logs on to the network in the morning, she is free to access her account at Bob's supplies without the bother of separate user names and passwords. This cross-site expediency also pertains to user provisioning and de-provisioning. If Alice quits her job and is de-provisioned, her account will also disappear from Bob's Supplies using the WS-Provisioning standard.

IBM Tivoli Federated Identity Manager (FIM) Maps SOA and Identity in the Real World

Conceptually, SOA and federated identity management seem like a match made in heaven. Each extends existing IT investments, leverages standards, and enables cross-enterprise business processes.

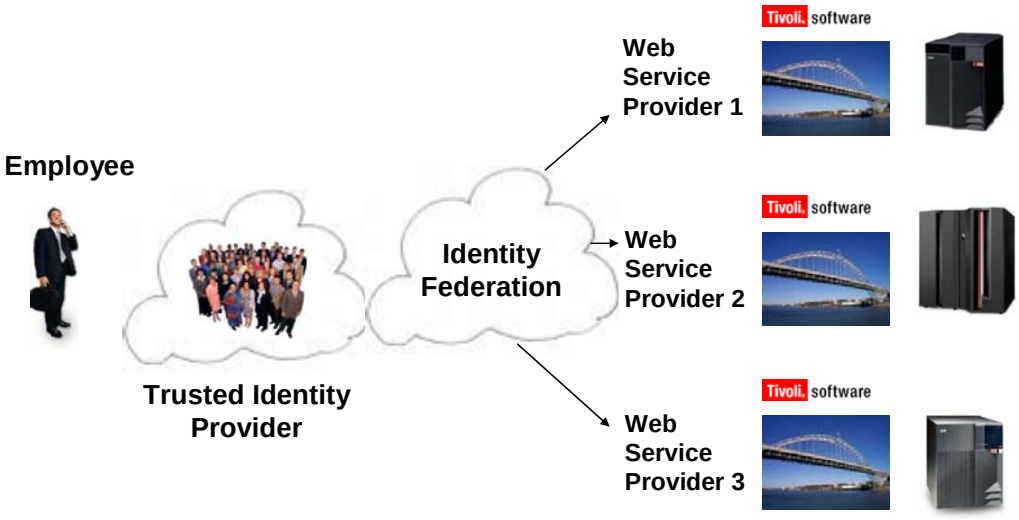
This is clearly a giant step forward and provides a perfect foundation for current and future business needs. Since SOA and federated identity management are still moving targets however, CIOs still face major product decisions and implementation challenges. For federated identity management to truly provide business value, it must morph from a theoretical concept to an enterprise-class set of services -- ASAP.

This transition requires a flexible federated identity management product like IBM Tivoli Federated Identity Manager (FIM). Tivoli FIM acts as an identity hub and adds real business ROI to SOA by (see Figure 2):

- **Acting as an identity proxy and policy manager.** Rather than add federated identity capabilities to various applications, appliances, and middleware, Tivoli FIM can act as an enterprise token mediation and identity mapping service for multiple control points within an SOA environment. IBM products like Datapower appliances, WebSphere Process Server, WebSphere ESB, and WebSphere Message Broker leverage FIM for enforcing identity policies. Tivoli FIM also takes advantage of IBM Tivoli Access Manager (TAM) enterprise authorization policies and auditing capabilities. In this way, Tivoli FIM acts as a kind of web-based customs agent by inspecting credentials, enforcing any restrictions.

- **Translating federated identity standards and business rules.** Tivoli FIM can act as a translator between organizations. For example, disparate business partners may use a multitude of different security tokens such as PassTickets, x.509 certificates Kerberos tickets, or customized authentication types. Tivoli FIM can evaluate business rules that

Figure 2. Tivoli FIM Architecture



run the identity management infrastructure. In this way, firms can modify business relationships and policies at the identity services tier without having to sink time and resources into rewriting or recompiling applications.

- **Integrating with mainframe identity facilities.** CIOs want to provide external access to mainframe applications but are leery of using federated identity management as a substitute for enterprise-class mainframe access control facilities like IBM's RACF. Why? RACF provides extensive reporting and auditing features that capture valuable information about user activities down to the transaction level. Recognizing this requirement, Tivoli FIM is tightly integrated into RACF. Tivoli FIM can map external user identities to RACF PassTickets (i.e. one-time passwords) and has the ability to create a RACF token for each user. This integration provides web to mainframe monitoring, auditing, and security.

- **Providing advanced reporting and auditing.** Given the emphasis that businesses place on regulatory compliance, Tivoli FIM provides an abundant array of reports around general authorization events as well as specific event details. For example, Tivoli FIM provides reports for events like failed authentication history, locked account history, authorization history by action, user administration event history, and security server audit history out of the box. Most users will find that Tivoli FIM "canned" reports provide audit information necessary for regulations like GLBA, HIPAA, and Sarbanes-Oxley or security

governance models like ISO17799, the CISSP CBK, or the NIST-800 series.

IBM Tivoli FIM Delivers Business ROI

Like IBM predecessors such as CICS and MQ Series, Tivoli FIM acts as a middleware bridge between external identities and internal assets. In this way, FIM can deliver real measurable ROI. CIOs will see near-term financial benefits from (see Table 2):

- **Identity-specific business logic development.** First, application developers no longer need to write their own complex access control rules. Rather, since Tivoli FIM already offers sophisticated authentication, authorization, and audit capabilities, they can simply call Tivoli FIM identity services. With Tivoli FIM, business units can modify business rules for specific individuals or groups negating the need to write and compile new code.

- **Central operations.** With Tivoli FIM, all identity operations for account creation, administration, and policy management can be centralized easing operations and improving security. For example, individual users or large business partners can be provisioned easily through FIM support for various WS* standards.

- **Consolidated logging, reporting, and auditing for compliance.** Many companies struggle with compliance in two areas: 1) lengthy audit cycles and 2) redundant processes. Tivoli FIM helps address both of these issues. By aggregating identity logs and offering rich reports, Tivoli FIM alleviates the needs to piece together activities by combing through multiple distributed audit logs.

Clearly, Tivoli FIM can make it easier to manage a complex federated identity management implementation and thus lower operating costs. Aside from this IT benefit, Tivoli FIM also delivers true business benefits. By streamlining the provisioning process, companies can dynamically extend their systems to new business partners accelerating their ability to boost productivity or drive new revenue. Since Tivoli FIM also can be used to define and enforce business rules, it can be used to customize business processes on a user-by-user basis. This can help firms maintain a competitive edge while bolstering customer care.

Table 2. Tivoli FIM ROI Benefits

Tivoli FIM Function	What it Does	ROI Benefit
Identity-specific business logic development	Accommodates business rules in the identity tier alleviating the need to write or compile new application code	Accelerates projects. Enables granular customization. Lowers application development and maintenance costs.
Central operations	Aggregates federated identity management, administration, and operations	Streamlines operations and lowers operating costs. Also improves security.
Consolidated logging and reporting	Acts as a hub for all federated identity logging information.	Decreases the time needed for compliance audits. Helps eliminate redundant processes.

20 Asylum Street, Milford, MA 01757 ● 508-482-0188 ● www.enterprisestrategygroup.com ● info@enterprisestrategygroup.com

The Future:

Digital Identity: User centricity, Meta system and Project Higgins

A new wave of individual and enterprise productivity will be driven through the integration of people with business processes. Information about people in the enterprise is abundant and growing, both in richness and in volume. However, it is scattered in many disparate databases and lacks integration. Also, given the trends towards social networking, collaborative computing, and people as core part of processes, users need to be empowered to better manage their identity information, and control access to the same.

To address these trends and requirements, a federated, digital representation of people in the enterprise will emerge, that dynamically and automatically captures increasingly rich information about individuals. To facilitate this, it is necessary to have access to identity information irrespective of where it resides. . This can create an identity meta system where federated, digital representation of people (identity data, metadata, relationships, profiles, etc.) is achieved which in turn enables higher levels of automation and optimization.

Given the user is at the center of collaboration, social networks and people oriented processes, empowering users to actively manage their identity information is crucial. This is also important because privacy of user information is a key requirement, letting users control who can access their personal information is scalable, preferable and evolving approach. Such an approach leads to user centric identity management that empowers users to manage, control and share their information within constraints imposed by laws and regulations.

To address these key concepts around identity meta system and user centric identity management, IBM has joined and making significant contributions towards an open source project, thus building the key ecosystem. Project Higgins, under the Eclipse organization, defines a component architecture and framework to address these requirements, and allows for different identity systems to interoperate.

IBM Tivoli products plan to leverage the framework provided by Project Higgins and provide capabilities to address the market around – user centric identity management and identity metasystem.

The Bottom Line

Like time, global business waits for no one. Success demands flexibility, customization, and rapid execution. These requirements simply weren't possible in an IT architecture of application silos and stovepiped identity management.

SOA and federated identity management promise an appropriate technology solution. Each of these efforts use established web protocols and widely supported web services to wrap existing application and identity infrastructure thus extending them to external customers, suppliers, and business partners over the web. The problem isn't with the model or the vision; it is with real world problems like implementation and execution.

Tivoli FIM is one of the most effective products for bridging the potential of federated identity management with implementation realities. Tivoli FIM interoperates with existing identity infrastructure (including mission-critical RACF) and thus bridges external and internal identity policies and management. Tivoli FIM also centralizes identity operations which increases security while lowering cost. From a partnering perspective, FIM frees organizations from the cost and

operational overhead of managing 3rd party users and identities. Finally, Tivoli FIM user provisioning and user-centric business rules can help deliver real business value.

Aside from keeping costs low, Tivoli FIM is also a great way for enterprises to achieve secure and rapid business integration. Tivoli FIM supports of broad out-of-the-box integration, streamlines the development of user/group-specific business rules, and simplifies security management of web services between heterogeneous platforms. In total, the FIM platform's business flexibility can help enable business – not just IT – benefits.

As enterprises embrace SOA, business-savvy CIOs should also consider IBM Tivoli Federated Identity Manager for identity management. At the very least, Tivoli FIM should be on every enterprise short list.

20 Asylum Street, Milford, MA 01757 ● 508-482-0188 ● www.enterprisestrategygroup.com ● info@enterprisestrategygroup.com