Trusted identity management solutions for service oriented architectures
To support your IT objectives

Tivoli software

Increase business flexibility in your SOA by establishing trusted identity management as a service.

Highlights

- Understand which users can connect to services and how they are connecting to those services
- Increase flexibility to add new services or modify existing ones as needed, by deploying an "identity-aware" enterprise service bus
- Reduce the complexity of identity processing for new and existing services, by establishing trusted identity management as a service
- Help control access management costs, by reducing redundant application coding requirements
- Help meet compliance requirements, by auditing identity access end to end

In a world where globalization continually adds new competition and business model pressures, mergers and acquisitions require rapid integration, and new regulations require tighter controls and insight, IT agility has never been in greater demand. Service oriented architecture (SOA) has gained widespread appeal for its ability to both ease application integration and provide a platform for rapid development and extension of existing applications to external customers — by reusing applications without rewriting them. SOA can help make businesses more responsive, competitive and — ultimately — profitable. From an IT perspective, SOA delivers numerous benefits as well, by:

- Simplifying application interfaces.
- Introducing rich business abstractions, using Web Services Description Language (WSDL) to describe the application interfaces.
- Decoupling the interfaces from the business applications and connecting them with an enterprise service bus (ESB).

However, along with its many benefits in creating and connecting new services and helping to reduce complexities, the openness of an SOA also creates security and compliance challenges. For example, each application brings its own set of identities, and as the applications are repurposed and reused in a service, they are extended to new users not originally envisioned in previous

deployments. In addition, each application may have different identity attributes and access definitions. So repurposing requires not only extending services to new users but also allowing existing users to seamlessly transition from one service to the next. This creates a need to:

- Translate and map a diverse set of user identities across different services.
- Manage application-specific identities across organizational silos and firewalls.
- Enact proper access controls for each services application.

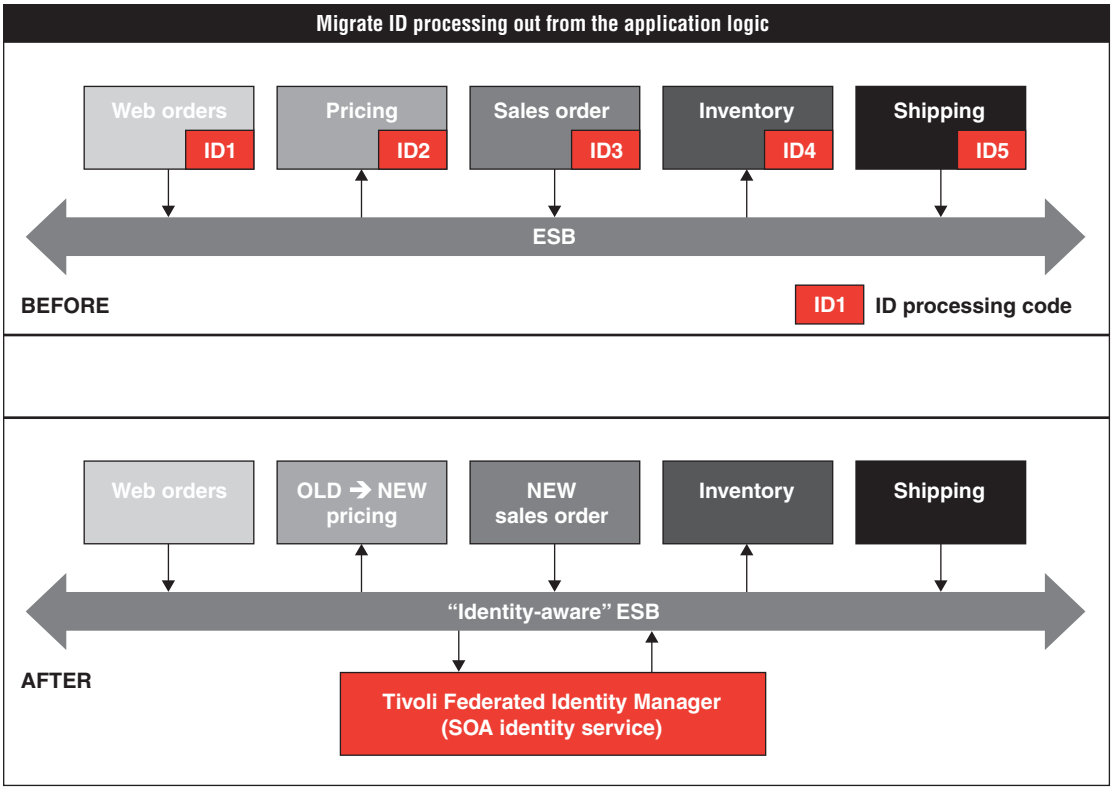
Beyond employing federated identity management to share and access services from other organizations, enterprise architects charged with managing user identities across composite business applications and business units — as well as thousands of internal and external end users — must support SOA by creating "trusted identity management as a service." Establishing this common identity broker service enables the business flexibility to add new services or connect existing services without having to recode identity processing as business needs change.

It also enables you to maintain high levels of security and privacy and allows line-of-business experts to focus on delivering the business logic that is required within the application — not on the security of the application itself. To accomplish application security goals, enterprise architects also need the ability to know which users are able to connect to these additional services — and how they are connecting to them.

Understand which users are connecting to services and how they are connecting

While your ESB connects multiple, disparate services, IBM Tivoli® Federated Identity Manager helps you establish an identity trust management framework you can use to determine which users are connecting to those services, what credentials are being used to connect them and propogate the required credentials end to end — from a point of contact, such as XML gateway through ESB to the back end such as an ERP or mainframe application. For example, you have an inventory service to connect to an ESB and integrate with the rest of the SOA implementation. The inventory service uses a set of mainframe identities to authenticate users, and the enterprise cannot expose those identities to the portal users for privacy and compliance reasons. In this scenario, the identity trust management framework is able to map and validate the portal identities to the mainframe identities using IBM RACF® PassTicket and allow seamless, secure, auditable access to the inventory service. This framework helps to ensure that the business has the reliability and assurance of knowing that the event or transaction is performed in a secure manner.

Tivoli Federated Identity Manager software helps expand the capabilities of your ESB, by helping you efficiently and effectively manage and provision user identities across your SOA. The combination of the software with your ESB provides an "identity-aware" ESB — solving critical security requirements. The software helps ensure that users have access to applications, data and information based on their security credentials and access level, regardless of which application they are accessing. In addition, Tivoli Federated Identity Manager provides the ability to migrate identity processing out from the applications and into reusable, trusted identity management services. The integration of Tivoli Federated Identity Manager with your ESB results in an increased flexibility to connect new services or modify existing ones as needed, and reduce the complexity of identity processing for the new or modified services (see diagram on the next page).



Tivoli Federated Identity Manager simplifies identity processing in an SOA by creating identity "abstraction" — migrating identity processing out from the application logic.

Reinforce compliance by auditing identity access end to end

As your SOA infrastructure grows in complexity, user identification must be checked along each step of a transaction. You must know at each point along the way which user is accessing the information — not only to ensure a secure environment, but also to meet strict audit requirements for compliance.

Tivoli Federated Identity Manager enables you to conduct "identity validations and translations," by checking identity from the point of login to data access to completing transactions — credentials are verified in the beginning and then passed along during each step. So while you are able to quickly deploy new services or repurpose existing services to support business goals, Tivoli Federated Identity Manager simultaneously enables you to maintain accountability and meet strict compliance requirements by helping you maintain a clean, consistent source of user identities.

Built-in reporting and integration with IBM Tivoli Compliance Insight Manager help you meet requirements for the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, Sarbanes-Oxley, ISO 17799 and other security regulations.

Increase business flexibility to add services or modify existing ones as needed

Often the challenge in adding new services or modifying existing ones is the identity processing that is required at the application level as each service is added. Tivoli Federated Identity Manager helps IT organizations provide more business flexibility by eliminating the need to manage identity processing from each individual service and application. It streamlines identity management by centralizing and externalizing the identity processing from the individual application, so siloed and legacy applications are no longer a barrier to adding new services, and allows line-of-business application developers to focus on what they do best within the business — rather than focusing on IT security.

Help control access management costs by reducing application coding requirements

Because Tivoli Federated Identity Manager helps centralize and simplify user access management across your SOA, it helps to reduce the labor required to maintain different identities for different applications, improving consistency in support of accuracy and compliance. It also helps you gain better overall enforcement and reduce development costs, since developers are no longer required to perform the same function and application coding repeatedly. In addition, with Tivoli Federated Identity Manager:

- Application developers no longer need to write their own complex access control rules.
- Operations and security burdens are lifted, since all federated identity management for administration and access control policy management can be centralized.
- Your staff no longer needs to piece together activities by scouring distributed audit logs, since the software aggregates identity logs to supply you with rich reports.

Reduce the complexity of trusted identity management

Tivoli Federated Identity Manager can help you extend the value of your ESB to make it "identity aware," by removing the need to manage multiple identities from multiple, heterogeneous locations. By using the software with your ESB, your organization can:

- Federate user identity credentials transparently across all required applications.
- Eliminate the need for users to log in multiple times to different applications.
- Deliver an improved and simplified access experience.

Enhance trusted identity management in your SOA with these products

Tivoli Federated Identity Manager is designed to work seamlessly with:

IBM WebSphere® Enterprise Service Bus — helps quickly build a flexible integration infrastructure. Supports interactions between service end points via standards-based connectivity, a spectrum of interaction models and quality-of-interaction service and mediation capabilities. Offers role-based administration support, prebuilt mediation functions and requires minimal programming skills.

IBM WebSphere Message Broker — acts as a universal adapter by delivering universal connectivity, data format support and transformation to connect from anything, to anything. Provides a powerful, integration-based ESB for standards-based, custom, complex and legacy systems and is optimized to accommodate any IT environment with various application and middleware technologies.

IBM WebSphere DataPower® SOA Appliances — purpose-built, easy-to-deploy network devices that simplify, help secure and accelerate your XML and Web services deployments while extending your SOA infrastructure. You can use the appliances to deliver integrated, standards-based access control to address Web users and Web services needs.

IBM Tivoli Composite Application Manager for SOA — monitors, manages and controls the Web services layer of your IT architecture. The software helps you identify the source of bottlenecks or failures and pinpoint services that use the most resources. Use it to help monitor service levels and visualize the flow of Web services without operator intervention via an easy-to-use console.

IBM Tivoli Compliance Insight Manager — automates user activity monitoring across heterogeneous systems, with dashboard and reporting to measure your security posture and respond to auditors' requests.

For more information

For more information about how Tivoli Federated Identity Manager can help you establish trusted identity management as a service within your SOA, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli

About Tivoli software from IBM

Tivoli software provides a set of offerings and capabilities in support of IBM Service Management, a scalable, modular approach used to deliver more efficient and effective services to your business. Helping meet the needs of any size business, Tivoli software enables you to deliver service excellence in support of your business objectives through integration and automation of processes, workflows and tasks. The security-rich, open standards–based Tivoli service management platform is complemented by proactive operational management solutions that provide end-to-end visibility and control. It is also backed by world-class IBM Services, IBM Support and an active ecosystem of IBM Business Partners. Tivoli customers and business partners can also leverage each other's best practices by participating in independently run IBM Tivoli User Groups around the world — visit www.tivoli-ug.org

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
9-07

TIS10442-USEN-00