Employ user-centric federated identity management to increase customer satisfaction and business collaboration

IBM Tivoli Federated Identity Manager

 Highlights

■ Simplify application integration using many forms of user credentials, and facilitate secure information sharing between trusted business partners and divisions within an enterprise

■ Improve the user experience with user-centric, federated SSO identity management

■ Implement a stand-alone identity service tool for establishing identity awareness in SOA and Web services environments

■ Use open standards and specifications to enable greater collaboration across the business ecosystem

■ Employ advanced operational features to ease application security integration, including support for multiple types of point-of-contact servers

■ Use modular software that supports z/OS environments as well as entry-level software that enables collaboration with small-to-midsize business partners

Exchanging critical information across company boundaries—among customers, suppliers and partners—is a necessity in today’s fast-paced world. End users expect to access all your services via a single interface, user name and password. Yet the proliferation of the more flexible and open service oriented architecture (SOA) and Web 2.0 environments creates its own set of identity management and compliance challenges. Collaborating and managing user and services identities across a business ecosystem places substantial demand on enterprise IT infrastructures. With an ever-increasing amount of vital information contained in different security domains, using federated single sign-on (SSO) techniques to help integrate this information can provide quick benefits and savings.
IBM Tivoli® Federated Identity Manager helps you establish an identity trust management framework to know which users are connecting to your services and what credentials are being used to connect to them. Tivoli Federated Identity Manager will propagate the required credentials end to end, from a point-of-contact server through an enterprise service bus (ESB) to the back-end mainframe. The software provides concurrent support for leading federated SSO protocols, including Security Assertion Markup Language (SAML) 1.0/1.1/2.0, Liberty Identity Federation Framework (ID-FF) 1.1/1.2 and Web Services (WS)-Federation, enabling users to connect to multiple business sites, while helping to preserve the confidentiality of user data.

Tivoli Federated Identity Manager delivers two key capabilities:

- **Federated SSO**—to enhance user productivity and facilitate trust by delivering SSO across separately managed infrastructure domains.
- **SOA identity service**—to reduce administrative costs, establish trust and facilitate compliance by managing, mapping and propagating user identities.

Through these two powerful and modular capabilities, Tivoli Federated Identity Manager enables partner interactions that are trusted, convenient, auditable and address key compliance concerns related to partner access from other domains. Designed to minimize impact on business applications, Tivoli Federated Identity Manager can help you reduce costs and speed deployment timeframes for integrating applications within your collaboration infrastructure. Use it to:

- Support broad federation functionality by enabling SSO, rich security customization and Web services security.
- Provide identity awareness across your SOA and Web services.
- Simplify the integration of identity and security.
- Communicate authentication and identification information about business partners through support for multiple security tokens.
- Automate the enrollment of user accounts and entitlements.

Transition to user-centric identity management

Trust between parties in a transaction is paramount, yet today this trust is increasingly threatened with the continued rise in identity thefts and other fraudulent activities. Identity managers must move from enterprise-centric identity management to a user-centric approach that puts customers, partners and suppliers in control of asserting trust, determining where sign-on is occurring and which specific user attributes they want to share between an identity provider and a relying party or service provider.

Tivoli Federated Identity Manager goes beyond traditional identity management offerings by supporting user-centric identity management through integration with open standards frameworks, such as OpenID and Information Card Profile, using identity selectors from Microsoft® Windows® CardSpace and the Higgins Trust Framework that do not require sharing of metadata between identity and service providers. These open identity frameworks encourage collaboration between companies and business partners, and help provide a greater level of service to end users.

A transition to federated, user-centric identity management can help you:

- Drive down identity management and maintenance costs (for consumers, employees and contractors).
- Increase authentication strength.
- Enhance compliance reporting and auditability.
Remove the complexity of application identity management

Tivoli Federated Identity Manager helps organizations provide customers, partners and employees with greater flexibility to access multiple business applications while reducing the complexity of managing multiple identities. For instance, you can integrate Tivoli Federated Identity Manager with an organization’s Web applications without using proprietary application programming interfaces (APIs).

A reverse proxy included with Tivoli Federated Identity Manager helps you integrate with a Web application via an HTTP/HTTPS connection. This provides loose coupling between the federated SSO middleware and the application layer, so a wide variety of Web applications can be connected into a federated environment with little or no application changes. In addition, applications and their associated middleware and servers can be upgraded without changes to the integration with the federated SSO services, and you can easily add new federation relationships and protocols. This federation deployment capability can dramatically reduce time to value and maintenance costs, compared with more intrusive API- or plug-in-based approaches.

Advanced operational management features ease identity management tasks

Your identity management team can leverage a vast range of operational capabilities and ease-of-use features built into Tivoli Federated Identity Manager, including:

- **Multiple point-of-contact servers**, including IBM Tivoli Access Manager for e-business, third-party access management offerings, IBM WebSphere® 6.1, third-party Web servers via a customized Web server and custom point-of-contact server plug-ins.
- **An advanced command line infrastructure and trust chain editor for quick deployments of identity service in SOA and Web 2.0 environments.**
- **The latest auditing and reporting capabilities**, including the Business Intelligence Reporting Tool (BIRT), integration with IBM Tivoli Compliance Insight Manager and built-in reports via console or the command line infrastructure.
- **Advanced key management through a console**, to easily change key store passwords and manage certificates during operation.
- **The ability to make run-time services reload configuration changes without requiring server restarts.**

Support compliance with unique Web services and SOA identity service capabilities

Many benefits of an SOA come from the reuse of existing application assets by dividing them into discrete business services and then combining these services in various combinations to implement business processes. Many existing applications are developed independently and have different representations of user identity and different ways in which identities can be exchanged. For example, many enterprises use a generic identity to allow access to business-critical data residing on the mainframe. Successfully managing different user identities and improving visibility of true identity exchange are critical to the success of your SOA.

Tivoli Federated Identity Manager offers a robust, stand-alone identity service tool, providing identity awareness—in SOA and Web services environments to IBM WebSphere DataPower® SOA Appliances, your ESB or IBM Customer Information Control System (CICS®)—to any organization.
Numerous features help enrich your SOA environment and improve visibility across multiple security domains and the enterprise IT infrastructure:

- **A secure transaction service (STS)** offers identity mediation services for your SOA and Web Services deployments by managing, mapping and propagating auditable identities. The Tivoli Federated Identity Manager identity service can be accessed from leading XML firewall gateways, ESBs and/or a mainframe CICS environment to provide identity mediation services for interactions across multiple security domains and with external organizations and services.

- **Support for multiple security tokens**—including SAML assertions, IBM RACF® PassTicket, x.509 certificate and Kerberos tickets, as well as customizable token types—to communicate authentication information about a business partner or service all the way to the back-end, mainframe or legacy applications.

- The STS can transform and exchange the identity credentials of one partner or domain with the identity infrastructure of another partner or domain, enabling reusable services deployments and faster adoption of a federated ESB solution.

- **Administrators can link Web services transaction access to an actual user identity using RACF PassTicket to improve transparency of IBM z/OS® or other legacy applications in an SOA.**

### Employ a federated ESB

Many ESB deployments today cannot efficiently connect and track identities across separately managed domains. By using the Tivoli Federated Identity Manager SOA identity service with your ESB, you can simplify administration and support compliance by making your ESB “identity aware,” removing the need to manage multiple identities from heterogeneous locations and helping to 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.

Integrating the Tivoli Federated Identity Manager SOA identity service with your ESB helps increase your flexibility to connect new services or modify existing ones as needed, and reduce the complexity of identity processing for new or modified services (see diagram). This identity awareness capability also enables organizations to provide proof of identity management compliance to auditors.

As a result, the Tivoli Federated Identity Manager SOA identity service is a critical component of IBM WebSphere Enterprise Service Bus, IBM WebSphere Message Broker, WebSphere DataPower and third-party ESB deployments with support for a standards-based interface for identity assertions.

### Choose a comprehensive SOA and Web services security solution

You can deploy the Tivoli Federated Identity Manager identity service with WebSphere DataPower SOA Appliances to leverage a powerful, integrated SOA and Web services security solution. The Tivoli Federated Identity Manager identity service provides:

- **General-purpose trust management.**
- **Reusable authentication services to diverse enforcement agents.**
- **The ability to add Java™ components for token translation or proprietary authentication.**
WebSphere DataPower SOA Appliances provide:

- **Firewall and threat protection.**
- **IBM WebSphere proxy processing.**
- **Increased security assurance.**

**Audit identity access into the mainframe environment**

The Tivoli Federated Identity Manager identity service enables you to conduct “identity validations and translations” by checking identity from the point of login, to data access, to transaction completion. 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, the unique ability of Tivoli Federated Identity Manager to simultaneously flow auditable identities from the distributed environment to the back-end mainframe environment enables you to maintain accountability and meet growing compliance requirements by helping you maintain a central, consistent source of user identities.

**Choose the federation solution that’s right for your organization**

In addition to using Tivoli Federated Identity Manager on distributed systems, you can use Tivoli Federated Identity Manager on z/OS for a high-availability identity management solution that also supports SSO and identity service natively on your IBM System z™ mainframe environment.

Also, enterprises that want to establish federated identity management with a small-to-midsize business partner can leverage IBM Tivoli Federated Identity Manager Business Gateway, an entry-level version that enables partner organizations to connect to your enterprise for a comprehensive identity management solution that supports advanced protocols such as SAML 2.0. Tivoli Federated Identity Manager Business Gateway can support your collaboration efforts throughout your supply chain or industry ecosystem.

---

**Tivoli Federated Identity Manager at a glance**

**Supported platforms:**

- IBM AIX® 5.2, 5.3, 6.1
- Sun Solaris 9, 10 (SPARC)
- Red Hat Linux Advanced Server 3.0 and 4.0 for IBM System x™
- Red Hat Linux Advanced Server and Enterprise Server 5.0 for System x
- Red Hat Linux Advanced Server 4.0 and 5.0 for IBM System p™
- Red Hat Linux Advanced Server 4.0 and 5.0 for System z
- SUSE Linux Enterprise Server 9 and 10 for System p, System x and System z
- HP-UX 11i V2 and V3 on Integrity

**Web Server plug-in component supports the following:**

- Apache Web Server 2.0 and 2.2
- IBM HTTP Server 6.1
- Microsoft Windows Internet Information Server 6.0
For more information
To learn more about how Tivoli Federated Identity Manager can help your organization employ new user-centric, trusted identity management and Web services identity awareness, contact your IBM representative or IBM Business Partner, or visit ibm.com/tivoli/solutions/security

About IBM Tivoli service management software
Tivoli software offers a service management platform for organizations to deliver quality service by providing visibility, control and automation—visibility to see and understand the workings of their business; control to effectively manage their business, minimize risk and protect their brand; and automation to optimize their business, reduce the cost of operations and deliver new services more rapidly. Unlike IT-centric service management, Tivoli software delivers a common foundation for managing, integrating and aligning both business and technology requirements. Tivoli software is designed to quickly address an organization’s most pressing service management needs and help proactively respond to changing business demands. The Tivoli portfolio is backed by world-class IBM Services, IBM Support and an active ecosystem of IBM Business Partners. Tivoli clients 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

© Copyright IBM Corporation 2008
IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.
Produced in the United States of America
June 2008
All Rights Reserved
IBM, the IBM logo, ibm.com, AIX, CICS, DataPower, RACF, System p, System x, System z, Tivoli, WebSphere and z/OS are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks owned by IBM in other countries. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml
Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries or both.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries or both.
Other company, product and service names may be trademarks or service marks of others.
Disclaimer: The customer is responsible for ensuring compliance with legal requirements. It is the customer’s sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer’s business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.