Extend the value of System z investments through federated identity management solutions from Tivoli software.

July 2006
Extend the value of System z investments through federated identity management solutions from Tivoli software.

## Overview

As the global marketplace becomes more interconnected, enterprises are rapidly reorganizing into extended value nets of partners, suppliers, customers and competitors in an effort to help drive innovation and lower the costs of doing business. Many companies are adopting Web services and service oriented architectures (SOAs) as they participate in external interactions with other trading partners. An SOA leverages open standards to represent software assets as services; in turn, organizations use standardized Web protocols to communicate across boundaries to provide access to these services.

Existing IBM System z™ software—which often represents significant investments of time and money—can fully participate in SOAs. When it does, an organization can unlock the potential of high-value resources that reside on IBM z/OS® platforms and extend services internally and externally. As with any cross-enterprise initiative, however, expanding the reach of legacy mainframe applications and processes requires an approach that takes into account the need to manage authorization and access control, enforce enterprise-wide security policies and comply with expanding regulatory demands.

IBM Tivoli® identity management solutions can help an organization create the trust necessary to provide security for transactions across mainframe and distributed environments that use SOA and Web services technology. IBM Tivoli Federated Identity Manager, coupled with IBM Tivoli Access Manager
Extend the value of System z investments through federated identity management solutions from Tivoli software.

for e-business, provides centralized management of role-based access control and identity policies, plus built-in compliance tools. Consequently, the software helps simplify efforts to provide the secured connectivity between SOA-based business processes.

This white paper examines how Tivoli Federated Identity Manager and Tivoli Access Manager for e-business can help an organization optimize its System z investments by providing the security needed to integrate and extend business processes across and beyond the organization. Specifically, this white paper addresses how Tivoli identity and access management solutions can help:

- Integrate security between new distributed applications and legacy mainframe applications, such as IBM CICS®.
- Enable support for Web Services Security management with support for a rich set of security tokens, including PassTicket-based tokens and custom tokens unique to individual environments.
- Improve audit controls for legacy data and transactions that utilize Web services.
- Streamline identity transfer and sign-on at all levels of an organization, including the mapping of Internet sign-on identities to legacy/RACF identities with PassTickets.
- Provide audit controls for the identity transfer/exchange that are consistent with the audit controls provided within a mainframe environment.

Look more closely at Web services–oriented technology

The evolution to Web services–based transactions has occurred at a startlingly rapid pace. Just a decade ago, many companies still relied on large staffs of customer service representatives to receive and process orders and requests from customers, suppliers and trading partners. Today, these interactions are largely handled through HTTP-based communications. Customers, suppliers and trading partners now log in, check the status of and make modifications to orders that are entered and processed entirely by an organization’s IT infrastructure.

At an increasing rate, these communications are being transformed into Web services using standards-based messaging formats such as Simple Object
Extend the value of System z investments through federated identity management solutions from Tivoli software.

Access Protocol (SOAP). By combining a set of services that are offered by separate organizations, new applications and services can quickly be constructed to generate additional value.

This transformation is part of adopting an SOA strategy. To support efforts to enable services to be executed consistently across an organization, SOA provides a standard method of invoking the business logic and functionality of Web services across disparate organizations and network boundaries. In such an environment, an organization’s computing environment is viewed as a set of services – accessible from both inside and outside the organization.

Major vendors including IBM and Microsoft® have agreed to develop standards and standards-based technologies to enable interenterprise interactions. Included in this effort are standards and specifications such as Web Services Federation Language (WS-Federation), Web Services Security (WS-Security) and Web Services Trust (WS-Trust). Just as Web browser-based user interactions were revolutionized through the standardized use of HTML and Java™-based technologies, these open Web services standards and protocols are a key enabler for the move to an SOA.

Enable Web services security through federated identity management

In a dynamic environment that relies in part on interenterprise exchange, businesses must leverage their trust relationships with partners to implement federated business models. Federating businesses enables interenterprise exchanges. Federating identities through the sharing of identity data with trusted partners is the basis on which trusted interenterprise exchanges take place.

Sharing identity data enables a partner organization to obtain information about a third-party identity, such as a supplier, from that user’s home organization – without requiring the partner organization to create and manage identity data for the third-party user. As a result, entities can sign on to one organization and utilize resources provided by multiple partner enterprises across the Internet. Organizations can share information and invoke resources among one another precisely as far as their trust model allows.
As requests flow through the system, access control checks must be in place to properly authenticate the requestor and track information for auditing purposes. The challenge is that many existing applications have multiple representations of user identity and varying methods of exchanging identity data. Successfully dealing with these different user identities and identity exchange formats is critical to the success of an SOA. User credential mapping—transforming user identity information from one credential format to another—is a crucial step toward secure transactions among entities.

Although System z software is fully capable of becoming an integrated participant in a multiplatform SOA, this software has until now typically been configured to use application-based and other approximate mapping models—a less than ideal situation. Without full-service identity mapping, it can be difficult to determine who is making the request, because it can appear to come from the application rather than the user. Consequently, there is no way to ensure that the right people have access to the right resources—and therefore no means to deliver the tracking capabilities that are critical to meeting auditing requirements.

Flexible identity and access management solutions from Tivoli software provide the crucial identity-mapping and tracking functionality needed to extend mainframe applications without sacrificing security. By participating in next-generation interenterprise collaboration, an organization can continue to derive mission-critical benefits from legacy applications.

**Explore the capabilities of Tivoli Federated Identity Manager**

Because it offers a services-based approach to single sign-on (SSO) and advanced credential transform, Tivoli Federated Identity Manager can help organizations use Web services standards to help maximize the security of transactions across mainframe and distributed environments. Tivoli Federated Identity Manager provides policy-based, integrated security management for federated Web services. It enables organizations to efficiently and cost-effectively share identity information in a trusted fashion.
The latest release of Tivoli Federated Identity Manager enables an organization to:

**Broaden its reach by facilitating cross-vendor federated SSO interoperability.** Support for federated SSO protocols, including Security Assertion Markup Language (SAML) 1.0/1.1/2.0, Liberty ID-FF 1.1/1.2 and WS-Federation, enables users to authenticate once to an identity provider and have service providers handle credential transformation. Users can interact with and use resources from multiple, distinct businesses across the trust boundary—simply and seamlessly. Tivoli Federated Identity Manager helps organizations provide customers, business partners and employees with greater flexibility in the ways they interact—while helping to reduce the complexity of managing multiple logon information.

**Provide increased support for multiple security tokens, including SAML assertions, PassTicket, x.509 certificate and Kerberos tickets, as well as PassTickets and customizable token types, to communicate authentication information about a business partner.** Tivoli Federated Identity Manager security token services (STS) can transform and exchange the security credentials of one partner or domain with the identity infrastructure of another partner or domain—in real time.

**Promote consistent, secured transactions through one-to-one identity mapping.** Tivoli Federated Identity Manager STS also enable the mapping of distributed user identities to IBM Remote Access Control Facility (RACF®) user identities along with generation and verification of RACF PassTickets (which are one-time-use passwords used for RACF authentication). The RACF user identity and PassTicket can then be used to connect to z/OS-hosted resources. An organization can establish predefined settings and/or use run-time calculations to consistently invoke transactions protected by z/OS Security Server RACF under the correct user identity.
Extend the value of System z investments through federated identity management solutions from Tivoli software.

Improve end-user accountability and transparency of z/OS applications in SOA environments by enabling administrators to link Web services transaction access to an actual user identity. By enabling the correlation of z/OS transactions with user identities that initiate the transactions, Tivoli Federated Identity Manager helps companies verify that the right information is delivered to the right people. That is a critical element for efforts to comply with relevant regulations and standards such as Sarbanes-Oxley, the Health Insurance Portability and Accountability Act (HIPAA) and Control Objectives for Information and related Technology (COBIT), along with other regulations and industry best practices. In addition, Tivoli Federated Identity Manager now provides support for the IBM Common Auditing and Reporting Service (CARS), with more than 30 “out-of-the-box,” preformatted reports to help track auditing data.

Invoke Web Services Security Management (WSSM) to support access control checks at the services invocation level. WSSM is critical to delivering legacy data and applications in an SOA. WSSM provides additional layers of security management over existing WS-Security functionality, such as added authentication, identification and authorization in the context of a federation relationship.

Leverage the intuitive IBM Integrated Solutions Console. Tivoli Federated Identity Manager includes a robust administrative console that enables an organization to configure predefined policies for authentication and authorization credentials, and enroll partners — all from one location.

Through these extensive functions, Tivoli Federated Identity Manager can help simplify the process of delivering mainframe applications within SOA environments — and greatly enhances opportunities to more quickly expand an organization’s customer base. For example, a financial services provider can potentially drive both organic and acquisitive growth by federating its services with large identity providers. Administrators of these sites, in turn, do not have to replicate expensive identity infrastructure investments to provide secure access for these users.
Extend the value of System z investments through federated identity management solutions from Tivoli software.

Leverage the combined strength of Tivoli Access Manager for e-business and Tivoli Federated Identity Manager

Together, Tivoli Federated Identity Manager and Tivoli Access Manager for e-business can enable a consistent, centralized approach to role-based access control, offering streamlined identity transfer and sign-on capabilities at all levels of an organization. While the WSSM functions of Tivoli Federated Identity Manager provide access control checks at the Web services invocation level, Tivoli Access Manager for e-business layers multiple authentication and authorization steps at the HTTP and URL level. Just as Tivoli Federated Identity Manager provides the federated SSO function at the services level, Tivoli Access Manager software establishes a session state once a user is authenticated at the URL level. It then transfers appropriate credentials to additional sites that operate under different authentication models as needed — without requiring the user to log on multiple times.

Administrators control access based on users’ roles in the organization, such as IT managers or customer service representatives. By evaluating business rules at run time, an organization can modify access-related parameters without having to rewrite or recompile applications — and thereby quickly respond to changes in business requirements.

Used in combination with Tivoli Access Manager for e-business, Tivoli Federated Identity Manager can help:

- Manage access controls across services-based process flows both within an organization and between business partner organizations.
- Establish a centralized access policy for multiple domains.
- Provide centralized auditing functions to help determine the number of failed authorizations, the effectiveness of security policies and whether or not administrators are abusing access privileges.
- Leverage extended authentication methods, which are frequently required by financial services organizations such as the FDIC and the Federal Reserve in the United States.

### Highlights

<table>
<thead>
<tr>
<th>Enable consistent, centralized and role-based access control</th>
<th>Leverage the combined strength of Tivoli Access Manager for e-business and Tivoli Federated Identity Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Together, Tivoli Federated Identity Manager and Tivoli Access Manager for e-business can enable a consistent, centralized approach to role-based access control, offering streamlined identity transfer and sign-on capabilities at all levels of an organization. While the WSSM functions of Tivoli Federated Identity Manager provide access control checks at the Web services invocation level, Tivoli Access Manager for e-business layers multiple authentication and authorization steps at the HTTP and URL level. Just as Tivoli Federated Identity Manager provides the federated SSO function at the services level, Tivoli Access Manager software establishes a session state once a user is authenticated at the URL level. It then transfers appropriate credentials to additional sites that operate under different authentication models as needed — without requiring the user to log on multiple times.</td>
</tr>
<tr>
<td></td>
<td>Administrators control access based on users’ roles in the organization, such as IT managers or customer service representatives. By evaluating business rules at run time, an organization can modify access-related parameters without having to rewrite or recompile applications — and thereby quickly respond to changes in business requirements.</td>
</tr>
<tr>
<td></td>
<td>Used in combination with Tivoli Access Manager for e-business, Tivoli Federated Identity Manager can help:</td>
</tr>
<tr>
<td></td>
<td>• Manage access controls across services-based process flows both within an organization and between business partner organizations.</td>
</tr>
<tr>
<td></td>
<td>• Establish a centralized access policy for multiple domains.</td>
</tr>
<tr>
<td></td>
<td>• Provide centralized auditing functions to help determine the number of failed authorizations, the effectiveness of security policies and whether or not administrators are abusing access privileges.</td>
</tr>
<tr>
<td></td>
<td>• Leverage extended authentication methods, which are frequently required by financial services organizations such as the FDIC and the Federal Reserve in the United States.</td>
</tr>
</tbody>
</table>
Extend the value of System z investments through federated identity management solutions from Tivoli software.

To better understand how the identity management chain is secured and made available at each stage of the application request process, consider a typical scenario, as illustrated in the following diagram:

In this diagram, a customer requests a service with a credential based on SAML or Liberty using a browser-based interface (HTTP). This credential is known externally to the organization and needs to be transformed into an identity or credential that is known internally. In this example, the resource being used is built on top of a set of CICS transactions. The same resource is accessed from both a browser-based, user-interactive application and a Web service that partner applications can utilize.

The user-interactive access path utilizes the IBM WebSphere® Application Server run-time environment, for which Tivoli Access Manager for e-business helps protect a browser-based application on the front side. The user contacts
the application through an HTTP request for authentication that is sent to the reverse proxy server provided by Tivoli Access Manager for e-business. After the logon verification is complete and the user’s access is confirmed, the request passes to WebSphere Application Server.

Once the request arrives at the application running on WebSphere Application Server, the application can employ a Java Connection Architecture (JCA) connector. JCA connectors are used to communicate with other enterprise information systems (EIS), such as CICS running on z/OS. The JCA connector, using a customized Java Authentication and Authorization Service (JAAS) logon module, can contact the Tivoli Federated Identity Manager STS to establish a credential that can be presented to the EIS.

In the bottom part of the diagram, a similar access model is shown that enables the same application to be used as a Web service by partner organizations. For protecting Web services, either a Web Services Gateway or the IBM DataPower® XS40 XML Security Gateway – one of the most widely deployed XML security gateways in the industry – can be used. These gateways or firewalls perform the corresponding functions of the Tivoli Access Manager for e-business HTTP reverse proxy server in the top part of the diagram (see page 9).

As part of processing the Web services request, the Web services gateway and Web services implementation (which are also often built on WebSphere Application Server) can utilize Tivoli Federated Identity Manager STS capabilities to transform the external credential and obtain a corresponding, internally known credential. In turn, this credential can be used by the CICS transaction and security services on z/OS. Once processing is invoked on the z/OS system, the operation runs under the identity of the specified entity, and the access checking and audit records are logged as appropriate. If access controls permit the transaction to run, the information is returned and the Web service invocation is complete.
Extend the value of System z investments through federated identity management solutions from Tivoli software.

Summary
As SOA technologies enable organizations to open z/OS applications to business partners, suppliers and employees, Tivoli Federated Identity Manager and Tivoli Access Manager for e-business provide a simple, loosely coupled model for delivering access to information and services in a trusted fashion. Built on open federated SSO and Web services standards, this centralized, integrated approach provides an optimized and cost-effective way to manage complex credential transform and permissions checks while simplifying the user experience.

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 how Tivoli Federated Identity Manager and Tivoli Access Manager for e-business can help you leverage your System z investments, contact your IBM representative or IBM Business Partner, or visit ibm.com/tivoli/solutions/security