

PRIMER

Federated Identity Management

BY DAVID F. CARR

What is it?

A system that allows individuals to use the same user name, password or other personal identification to sign on to the networks of more than one enterprise in order to conduct transactions.

How is it used?

Partners in a Federated Identity Management (FIM) system depend on each other to authenticate their respective users and vouch for their access to services. That allows, for example, a sales representative to update an internal forecast by pulling information from a supplier's database, hosted on the supplier's network.

Why is it necessary?

So that companies can share applications without needing to adopt the same technologies for directory services, security and authentication.

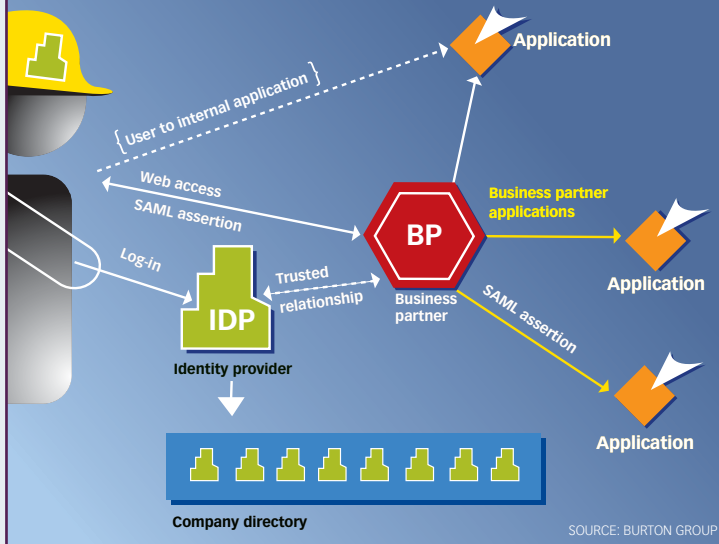
Within companies, directory services such as Microsoft's Active Directory or products using the Lightweight Directory Access Protocol have allowed companies to recognize their users through a single identity. But asking multiple companies to match up technologies or maintain full user accounts for their partners' employees is unwieldy. FIM allows companies to keep their own directories and securely exchange information from them.

How does it work?

A company must trust its partners to vouch for their users. Each participant must rely on each partner to say, in effect, "This user is OK; let them access this application." Partners also need a standard way to send that message, such as one that uses the conventions of the Security Assertion Markup Language (SAML). SAML allows instant recognition of whether the prospective user is a person or a machine, and what that person or machine can access. SAML documents can be wrapped in a Simple Object Access Protocol

REFERENCE: IDENTITY MANAGEMENT IN ACTION

In this business-to-business example, a user logs in and is authenticated by his company, which provides him with his identity and maintains his information locally in the company directory. The user can access applications within his company or use the Web to access applications on a federated partner's network. Behind the scenes, SAML statements are exchanged to authenticate the user and determine his privileges.



SOURCE: BURTON GROUP

message for the computer-to-computer communications needed for Web services. Or they may be passed between Web servers of federated organizations that share live services.

Who is using it?

Early adopters include American Express, Boeing, General Motors and Nokia. Another, Proctor & Gamble, had improvised its own federated-identity system using the more generic eXtensible Markup Language but is now moving to adopt SAML.

Are the standards solid?

They're getting there. SAML is backed by the Organization for the Advancement of Structured Information Standards (OASIS). The Liberty Alliance, an industry group formed to promote federated-identity standards, has adopted SAML 1.1 as part of its application framework. Microsoft and IBM have proposed an alternative specification called WS-Security. But Dan Blum, a technology analyst with the Burton Group of Midvale, Utah, believes that OASIS may try to make these two approaches converge in SAML 2.0.

What are the challenges?

Trusting a partner to authenticate its own users is a good thing only if that partner has solid security and user-management practices. Also, while some Web access-management products now support SAML, implementing the technology still commonly requires customization to integrate applications and develop user interfaces. ◀

QUIZ: Should Your Company Share Identities?

	TRUE	FALSE
We contract out employee services, and we want providers to appear as if they are part of our company.	<input type="checkbox"/>	<input type="checkbox"/>
We provide consumer services with partners, and we want to give users a common log-in system.	<input type="checkbox"/>	<input type="checkbox"/>
Our company has authorized a number of customers or suppliers to access applications on our network.	<input type="checkbox"/>	<input type="checkbox"/>
Customers or suppliers have offered us access to their applications.	<input type="checkbox"/>	<input type="checkbox"/>
Some business partners have expressed active interest in federated identity technology.	<input type="checkbox"/>	<input type="checkbox"/>
We are comfortable being an early adopter of technologies that are still being refined.	<input type="checkbox"/>	<input type="checkbox"/>

Score: 6 Trues Join the federation.
4-5 Get some experience with the technology and use it more aggressively as it matures.
3-0 Avoid the leading edge for now.