

waters

APRIL 2003

Building Federated Identities

An alliance hopes its standardized systems for sharing identities will, among other things, clear one of the stumbling blocks to implementing Web services. **By Robert Daly**



Up until now, the issue of verifying trusted user identities kept most Web services deployments behind the corporate firewalls and limited their benefits. An industry consortium of 150 equipment, identity, infrastructure and service providers and financial service firms is aiming to solve that problem by creating a standard identity system run through a federated network model. The consortium, known as the Liberty Alliance, expects to release Version 2.0 of its standard this summer.

"This is a federated model, not a centralized model," says Simon Nicholson, the chairman of Liberty Alliance's business and marketing expert group. "Instead of using a hub-and-spoke architecture, each provider in the circle-of-trust maintains its own identity information. Our goal is to deliver technology in which those

identities can be federated and linked together."

On a very basic level, federated network identity means organizations and individuals can allow separate entities to manage different sets of identity information. Account federation enables associating or binding a user's multiple Internet accounts within a "circle-of-trust" among organizations that is governed by some legal agreement. Federated single sign-on enables users to sign on with one member of the circle-of-trust and subsequently use other sites within the group without having to sign on again.

The Liberty Alliance sees its standards having a major impact among financial institutions, and some of its early adopters hail from the sector, including Communicator Inc., whose products include a commingled investment research portal.

The alliance released its initial version of the standard last July. Version 1.0 enabled users to decide whether to link accounts with various identity providers and made it easier for companies and individuals to take advantage of Web services. In January, the group released Version 1.1, which provided maintenance updates to the first version, editorial changes to clarify the specification and other fixes primarily aimed at reducing barriers for implementing the technology by improving flexibility and clarifying ambiguities.

The planned 2.0 release this summer would keep the version updates on a regular pace. "We're aiming to have a six-to-nine-month window between the releases," says Nicholson. "That's the plan."

Communicator Inc. has adopted the technology and has retro-engineering its Hub ID system to meet the new standard and de-

ILLUSTRATION BY GETTY IMAGES

ployed it with Securities.Hub, a portal that uses a single sign-on to allow seamless integration between the fixed income sites of the eight investment banks that are its members. It also displays member firms' news, prices and research in a portal format.

The company's model for facilitating movement between competing firms' sites made it a perfect candidate to test the federated identity, company officials say.

"The benefits of the technical capabilities of Securities.Hub for the dealers are that their customers are able to have a single sign-on across multiple enterprises," says Serge Shinkar, a product manager with Communicator. "Remember, these aren't your regular multi-enterprise situations—they're serious competitors that would never share their respective customer information with each other, but do need to work together to provide mutual customers with easier access to commingled information."

"Securities.Hub acts as a facilitator that improves the electronic inefficiencies," adds Miko Eda, Securities.Hub's president. "Securities.Hub doesn't come between the customer and dealer, it enhances their relationship. It provides a single sign-on, aggregates content and also provides instant messaging capabilities."

The company found porting its once-proprietary solution to the infant standard relatively painless, explains Shinkar. "The specification fit naturally into our federated directory. When we first approached the Alliance and showed them what we had done with our proprietary API, they said to us, 'We're looking do this and you've already done it.' As a result, we needed to adjust our APIs, but we didn't need to make changes to the underlying system, and

The Hub ID platform runs in its own data center and the member companies integrate the Hub ID interface into their systems without changing how their systems work, explains Shinkar. "Companies don't want to change their existing workflow. Hub ID allows each company to control their own system. The customer information isn't shared over the boundaries. It uses enough information to identify a user as the same person and profile—all of the specific customer relationship information stays inside each respective company. The federated identity shares some information with Hub ID, but never account numbers and other proprietary information. The federated directory is a permissioning schema," he says.

Hub ID operates by searching the information provided by the defined circle-of-trust (in the case of Securities.Hub, it's the user information provided by its members, Credit Suisse First Boston, Goldman Sachs, JP Morgan Chase, Lehman Brothers, Merrill Lynch, Salomon Smith Barney, Morgan Stanley and USB Warburg) and enables connections based on matches.

"For example, if Hub ID finds a Nicholas_Adams from Goldman Sachs and an nadams at CSFB, it will look to match the addresses and e-mails to make sure that it's the same person," says Shinkar. "Once identified, Hub ID sets up a flag and a 'handshake' so that the customer experiences a seamless movement between the two sites."

Since the launch of the standard and the early successes, such as Securities.Hub, the Liberty Alliance has seen dramatic interest from the industry. In an internal poll of its members, 17 percent of the respondents said they already have or are working on



“Our goal is to deliver technology in which those identities can be federated and linked together,” says Nicholson.

the end-users saw no immediate differences.”

“And by adopting the standard,” continues Shinkar, “it makes integrating the appropriate systems simpler and easier and lowers the technical barriers of entry for companies looking to deploy single sign-on solutions. Before the standard, [implementing single sign-on solutions] required significant time and effort to integrate the necessary systems and have them understand the proprietary protocol. Many companies aren't willing to spend the time and resources in implementing single sign-on solutions because they were quite an adventure. The new standard solves that.”

federated identity solutions and 59 percent said they are implementing a federated identity solution in the next 12 months, says Nicholson.

“Moving forward, we'll be increasingly examining the business issues hindering adoption and working to remove the barriers,” says Nicholson. “Some of the issues that we are addressing include what are the business terms that companies need to consider when creating a circle-of-trust.” In the version 2.0, the standard will provide a framework for permissions-based attribute sharing that will allow circles-of-trust to link together. ■