Single Sign-on and Social Networks

Greg Goth

Call it what you will—single sign-on, federated identity, one-stop authentication—letting users sign on to the Internet once and securely access network resources anywhere has been one of the industry’s enduring quests.

While numerous standards efforts have steadily pursued this capability, most have been back-end technologies of which users are mostly unaware. Periodically, however, something brings these efforts to the foreground. Recent developments surrounding the open source OpenID federated-identity technology signal another high-profile period for single sign-on. But they also raise questions about how to achieve interoperability between disparate technologies meant for distinctly different user communities and which of these technologies might be worth investment.

“Large deployers who are cognizant of OpenID, [Microsoft’s] CardSpace, and the general information card arena are asking how all this stuff fits together?” says Roger Sullivan, president of the Liberty Alliance (www.projectliberty.org), a 150-member federated-identity standards body that’s been working on single sign-on since 2001. “They’ll say, ‘I understand what federation is all about and how to use it in a serious business application, but I also have an interest—a strategic interest—in being able to tap into this social community that’s using OpenID and figuring how I can then migrate that anonymous user into my more structured environment, to provide linked services that are more highly authenticated and secure to that more casual user.’”

OpenID Gains Momentum

OpenID (http://openid.net) was originally conceived as a convenient way for heavy blog users to traverse their Internet niche without having to sign on separately to each site. It has become the latest cause celebre of the single sign-on movement. Within a few days of each other in late October, both Microsoft (http://winliveid.spaces.live.com/Blog/cns!AEE1BB0D86E23AAC!1745.entry) and Google (http://google-code-updates.blogspot.com/2008/10/google-moves-towards-single-sign-on.html) announced their support of the OpenID 2.0 protocol.

Microsoft’s current OpenID release, included in its Live product suite of services including Hotmail and Windows Messenger, is for testing purposes only. The company expects its OpenID implementation to be ready for production “sometime in 2009.”

At first glance, the announcements appeared to signal that OpenID was ready to become the Internet-wide de facto standard for user-initiated single sign-on. However, even some of the technology’s most avid advocates admit there is much work to do, technologically and in shaping end-user perceptions.

Perhaps the most vexing problem is that the announced support of OpenID is a one-way proposition. The most popular email and identity providers—Yahoo as well as Google and Microsoft—currently serve as “issuing” OpenID providers, but they’ve hesitated to become “relying” providers, which accept logins from other OpenID sites. To many observers, this alone is adequate reason to wait until the OpenID community’s deeds match its words. After all, what’s the point of a single sign-on technology that won’t allow single sign-on?
In fact, representatives of Google and Microsoft don’t even agree as to why they’re delaying two-way implementation of the standard.

For example, Google security team member Eric Sachs blogged (http://google-code-updates.blogspot.com/2008/10/moving-another-step-closer-to-single.html) on 30 October, the day after Google announced its OpenID 2.0 availability, that only one problem stands in the way of becoming a relying party:

> Fortunately it is more of a technology problem than a usability issue. That problem is that rich-client apps (desktop apps and mobile apps) are hard-coded to ask a user for their username and password. As an example, all Google rich-client apps would break if we supported federated login for our consumer users, and in fact they do break for the large number of our enterprise E-mail outsourcing customers who run their own identity provider, and for which Google is a relying party today.

However, in an emailed statement, Microsoft representatives questioned whether other OpenID providers could maintain the levels of service availability and account protection that Windows Live ID provides for its users. If not, Live Service users might be “prevented from access their own data due to an inappropriate or unlucky choice of OpenID providers.” This raises two further questions. What is the worth of a community effort in which one of the most influential members holds forth the possibility other members could offer “inappropriate” or “unlucky” access to a trusting user? And what is that company’s true commitment to a legitimate two-way protocol instead of a low-resistance, one-way hook into more users.

**Transitions and Disconnects**

OpenID Foundation chairman Scott Kveton says the delay is indicative of a transitional period between centralized and decentralized architectures and business models.

“Sites are silos in and of themselves,” he says. “With system-centric design comes system-centric values—people asking, ‘How will this affect our user base? Will our users leave?’ But people are finding that instead of leaving, users are actually more rooted at that site if they can use OpenID. This occurs as we move to a more user-centric model.”

In fact, Kveton says niche sites might see a huge opportunity with smaller Web site operators from users of the big sites that now offer only one-way access via OpenID.

“You’re going to be able to implement OpenID on your site, and that will accept users from any one of those places. The big guys are still trying to get a feel for what this means, but in the next six to 12 months, I think there’s a huge opportunity for the smaller sites to take advantage of all these users who are now being exposed to it.”

Thus far, the exposure hasn’t translated to end-user popularity, however. Leah Culver, founder and lead developer of the San Francisco-based social networking and micro-blogging site Pownce, says, “None of our users are really asking for it. The truth is, when you go to sign up for a social network that uses OpenID, you still have to create all your profile information, and all it does is tie in your OpenID in as an alternative authentication, which is great if you like that. But right now, it’s not worth our time and effort to set up a second authentication service.”

Allen Tom, principal architect for Yahoo’s membership team, says the results of a recent company-run OpenID usability study (http://developer.yahoo.net/blog/archives/2008/10/open_id_research.html) showed users were frustrated not only with OpenID’s difficult multistep sign-on process but also had no idea what it really was.
"The most striking conclusion was that OpenID doesn’t really seem to have much brand recognition," Tom says.

According to Pownce’s Culver, the lack of recognition is a symptom of the disconnect between the developer and user communities.

"It’s one thing to be an advocate—as an independent developer, to say, ‘Hey, everyone should use OpenID.’ And it’s another thing to be a site owner, where you do have users, and you have to consider what they’re going to think of it, and most of them are not technical by far,” she says. “They’re used to password login and have never heard of OpenID. It’s really hard to break that pattern.”

**Japan Taking the Lead**

Although OpenID might appear to be spinning its wheels with the mass audience in the US, Liberty Alliance president Sullivan says the technology is being recognized as a potentially vital partner in other regions. The closing panel at the Alliance’s Asian board of directors’ November meeting was a joint presentation by Liberty, OpenID Japan, and Microsoft—three organizations which have been mutually antagonistic more often than not. The panel attracted 300 people.

Sullivan says the Japanese market will be the likely pioneer of melding social networking and transactionally oriented single sign-on technologies. He cites mobile phone services is Japan as an example. “Folks in Japan wave their phones over turnstiles in the metro, and that is the authentication device as well as the payment device. We’re nowhere near that in the US,” he says. In Japan, “OpenID represents one of many on-ramps onto the identity infrastructure highway. There are many ramps, some more secure than others. Everybody wants to get into the high-speed lane, and to do that you have to cross some barriers along the way.”

To some degree, Sullivan thinks the melding of federated identity technologies will be generationally driven. For instance, while many savvy midlife Internet users are quite satisfied with the increasing capabilities of interbank asset transfers using just one bank’s sign-on—one of federated identity’s signal applications—merchants targeting a younger demographic are still frustrated in capturing their user base online.

Sullivan says merchants that serve the younger demographic typically lament that their traditional way of asking to connect with the customer, an e-mail address, often results in the customer supplying a spoof address to avoid being solicited. Technologies such as OpenID, Sullivan says, can fill a key niche in the continuum of reaching those customers.

"Businesses are really starting to see the strategic importance of answering questions such as ‘How do I manage the progression from anonymity into a meaningful business interaction?’ Because at the end of the day, that’s what these technologies are all about—creating that seamless transition from anonymity to a highly secure environment and being able to use, at any point along the way, the technology that is appropriate for that transaction.”