

Getting to know you

By: Tim Wilson

Network World Canada (06 Dec 2007)

Identity management (ID management or “IDM”) identifies individuals in an IT system, and controls access to resources by connecting that identity to a combination of user rights and restrictions. Within organizations – either public or private – these identities can be roles-based, as opposed to being identified with a specific function. This is true also for external access to the varying roles played by private sector customers and users of government services.

“In Canada, by and large most firms haven’t taken the time to classify their data,” says Dave Senf, director of Canadian security and software research for IDC. “And it’s really in its infancy for firms to be able to talk to each other in a meaningful way from a user-based perspective.”

It is also early going for simple roles-based IDM within organizations, but that’s about to change, and not just because potential customers get it, or because the vendors are wowing them with revolutionary technology: it is the regulatory and compliance requirements that are largely driving demand.

Francois Daigle, director of professional services for [Okiok Inc.](#), a security and authentication software development company in Laval, Que., says that although Canada is in the early stages, larger companies are getting there.

“Most of our large customers are driven by compliance issues. If they are financial firms with U.S. exposure then there is Sarbanes-Oxley (SOX) to think of, and in Canada there is Bill C-198,” says Daigle. “And this can move out of finance and to large retail or pharmaceutical companies.”

Certainly, although the regulatory environment may affect different vertical market sectors in unique ways, those independent software vendors (ISVs) selling into the market see IDM as a cross-industry, horizontal solution.

Idan Shoham, chief technology officer for Calgary-headquartered M-Tech Inc., which publishes a suite of IDM software, agrees that IDM is driven more by scale than industry.

“We typically see customers having about 10,000 and up users,” says Shoham. “But where we do see a bit of variability is in that threshold. For example, companies in heavily regulated industries or with very deep pockets will typically have a lower threshold before this kind of technology makes sense.”

In effect, for some industries the benefits justify the costs. It's getting easier, too, because companies like M-Tech and Okiok (partnered with Siemens) are adding capabilities all the time, as are some big players, among them IBM (Tivoli), Microsoft, Oracle, Sun (iPlanet), and Novell.

M-Tech's Shoham points out that a subtle but important industry trend is the desire to rein in deployment costs. Right now, if a company purchases a user provisioning system, they can expect to spend up to 10 times the purchase price on professional services for installation, configuration, testing and roll out.

"That's just crazy," says Shoham. "The vendor community has to work harder to bring it down."

This means that for vendors a main focus should be product engineering to find ways for deployment to be faster and easier.

Richard Reiner, chief security and technology officer for [Telus](#) Security Solutions, says that only a few years ago the market was represented mostly by small companies selling roles-based engines, but "now the big IDM vendors like Sun and Novell are partnering with the engine companies to make it part and parcel of their architecture." One example: at the end of November Oracle Corporation announced that Intercede's MyID identity credential management software would integrate with Oracle Identity Manager, functioning as a single solution.

This makes sense to IDC's Senf. "Although vendors have their own technology, the Holy Grail is to have more commonality," he says, adding that though there have been efforts to get agreements among vendors, it is a slow process.

Integration issues are only partly a matter of will. Some vendors have unstable APIs that can change radically between patch level releases, and often have stability problems. According to Shoham this is mostly an issue with large ERP systems. "What this means to customers," he says, "is that they need careful change control when upgrading or patching their ERP applications, to allow time to find and work around new bugs and API changes."

Conceptually, old and new applications are pretty much the same: they have users, users have attributes, and there are security groups with users attached. Given the uniformity of the model, the challenge is in large part a matter of building the linkages. A company like M-Tech, for example, ships with over 70 connectors for all kinds of systems, including IBM mainframes and ERP software from the major vendors.

However, although some IDM vendors are selling a compelling integration message, Senf thinks it's important to back up the discussion, and to assess the challenges that a company faces simply in terms of preparation and assessment. "There are also a lot of cultural issues within an organization," he says. "Money has to be spent to classify information."

And time, too. Reiner from Telus is often hearing that there is fear of IDM in the marketplace due to stories of huge and unwieldy solutions. “People get tied in knots with the approval process,” he says. “For one role there can be dozens, or even hundreds of criteria for a user to get fully provisioned. If we’re just trying to get Bob or Sue to work then, yes, a lot of it is automated, but there is still a real need to simplify this.”

Okiok’s Daigle tells a cautionary tale of how lining up too early with a big vendor can create headaches, recounting his experience of being in a large organization that wanted to deploy IDM. “They’d chosen the vendor before doing the analysis,” he says. “We told them they were doing it backwards. They took our advice: we started from the bottom and met with managers of the business units and the users. The vendor was overselling – in the end the company spent \$500,000 and not \$1 million.”

It seems like fair advice not to bring a big vendor in at the start of a project. And if one goes first to a company with a heavy services component, it makes sense to see who they’re aligned with (although Okiok is a strong Siemens partner, the company claims vendor neutrality). As a rule of thumb, the more specialized the company, the more likely it is that the advice will not bleed into inappropriate areas.

To get a sense of ROI, organizations need to balance the timelines and investments against savings based on speedier provisioning, as well as – and this is near impossible to calculate – the potential cost of having the wrong people access sensitive data.

When all is said and done, a working system should save on labour costs. “This is more efficient change management,” says Shoham. “It means effective lifecycle management and the efficient onboarding of new users, as well as more prompt and reliable access termination to reduce security exposures.”

The security argument is a common one, and often tied in with the other drivers of IDM adoption, compliance and privacy. However, even the best IDM system cannot eliminate data leakage. This is particularly true if network segmentation issues are not properly dealt with. This isn’t just a software issue, but requires an organizational understanding of how the network is built. “It’s the only way to properly ensure that the right people have the right access,” says Senf, “and the wrong people don’t.”