



Manage by Fact, not Fantasy



PKI set to safeguard B2B transactions

Michael MacMillan

IT World Canada

For years it has tempted financial institutions with the promise of airtight online transaction security, but experts say public key infrastructure technology, although progressing steadily, is also moving slowly.

Take New York-based Identrus LLC, a for-profit company founded in 1997 by several of the world's largest banks, and dedicated to overcoming the "final obstacle" preventing companies from conducting business-to-business Internet commerce from thriving — namely, concerns over passing sensitive information over public networks.

It has since developed an open, multivendor PKI infrastructure network that facilitates digital signatures and certificates. By using it, Identrus says large, corporate trading partners can certifiably identify each other during e-commerce transactions, and make those transactions binding at the click of a button. As well, it has prescribed specifications and standards that its partner vendors must adhere to in order to do business with its member banks.

"It's always been hard to say that the basic technology Identrus provides, which is really PKI...plugs a hole somewhere. It's more of an enabling technology to let you do the stuff that you probably wouldn't have done before," said Dave Oshman, senior vice-president of technology at Identrus.

Consumers have long since enjoyed freedom to do banking via the Web with nothing more than a username and password. In the event of identity theft or some other criminal activity, those funds are often covered. But organizations that engage in B2B transactions are often responsible for their own losses. And breaches do little for a bank's reputation. As a result, they and their corporate customers are looking to PKI as a way to make such transactions as safe as possible.

But that isn't as easy as it sounds, said Robert Lendvai, vice-president of marketing at Ottawa-based security specialist Cyberpass Corp. "PKI is a complex technology. There are challenges of integrating it with existing applications, Web applications and legacy applications, and then there are all kinds of policy and registration issues...So it's not a simple technology, and the cost of implementing it has been quite high," he said.

Toni Marshall, senior manager of Deloitte & Touche's secure e-business group in Toronto, who has been involved in financial PKI projects in Australia and the United Kingdom, said three main obstacles face PKI adoption in financial institutions — an inability to successfully argue the business case at the outset, trouble with implementation and problems with deployment once it's installed.

"The interesting thing is there's no reason for them to be struggling, and as I work around the globe I notice the clients all making very similar mistakes or dealing with similar issues," she said. "I'm not sure people are going up the learning curve."

Marshall said PKI should be looked at as part of a company's core infrastructure, not just technology to be applied on a case-by-case basis — a common error among financial institutions, she said. But a shortage of people with the skills and smarts to run PKI systems from an operational perspective is also hampering efforts.

"That's where a lot of them struggle, they get someone in, they get implemented and configured, and then they say how to we make this work for 100,000 users. So they're two very different issues," Marshall said.

Kyberpass is among a growing number of companies which are trying to address the implementation and integration issue by offering middleware to make it easier for bank IT staff to tie together PKI systems with legacy applications. It's a growth market — IBM Corp. recently rolled out a suite of middleware products, the WebSphere Financial Network Integrator, to help banks better secure their electronic payments system (and aimed, in part, at helping banks take advantage of the Identrus standard).

"The intent here is to...exploit every bit of capability they have, and then on top of that to provide a thin layer of services needed for any financial services hub to do high-quality transaction processing," said Melanie Rose, director of solutions technologies development for IBM software group in Somers, N.Y., at the time of the Financial Network launch.

Microsoft Corp., meanwhile, has included an integrated set of tools for creating, deploying, and managing public key-based applications in its Windows 2000 platform (and, along with several partners, is also working with Identrus).

Oshman said a previous lack of applications geared for PKI platforms was partly responsible for slow adoption rates. Still, he said the limited success of PKI thus far wasn't something the security industry predicted. "To be brutally honest, it's not quite been disappointing, but it's been much slower than expected." Currently 60 banks are partners in the Identrus network, including Bank of Montreal, Canadian Imperial Bank of Commerce, Royal Bank of Canada and the Bank of Nova Scotia. Of those, 14 are live and in production.

"Ten years ago, we would have expected to have 50 banks running live," he said.

However, that sluggishness is somewhat limited to North America. Experts point out that banks in Europe and the Asia/Pacific region, particularly Japan, have embraced the technology much more readily. Lendvai attributes this to a "paranoia" of government found on this side of the ocean, less political willingness to sacrifice privacy or trust banks or government.

Marshall also pointed to North American geography — where Canadian and U.S. banks do a big chunk of their business with each other, eliminating the trans-border security concerns that are more pressing in Europe and Asia, as another reason large scale PKI hasn't yet been adopted here.

Still, Lendvai said banks are unlikely to allow the benefits of full-blown PKI to escape them. "The banks are trying to ensure that they're not left behind on what's expected to be a multibillion opportunity to manage high value transactions over the Web."