



Karen Wendel

Karen Wendel has more than 20 years of experience in financial services, applications development and business management. Her expertise includes international banking, payments, treasury management and transaction processing. Before joining IdenTrust, she was the CEO of eFinance Corporation, an applications development company that provides risk and credit decision solutions. She was also previously a partner at Belgium-based consulting firm, The Capital Markets Company (CAPCO), where she led its e-finance practice. Prior to that, she led the US Financial Services Practice of Gemini Consulting.

Set up in the 1990s to put banks at the centre of building trust in B2B e-commerce, IdenTrust has enjoyed mixed fortunes. But as identity theft becomes more sophisticated and corporates struggle with proprietary security tokens, PKI and IdenTrust are enjoying a renaissance, says CEO Karen Wendel.

Long live PKI

In the last few months there has been significant market traction behind digital identity management. Why is it such a hot topic now?

The main reason is that the market has started to evolve. There are more electronic forms of communication, while the amount of activity associated with hacking and the sophistication of criminals has increased. Solutions that were sufficient are no longer adequate and banks are having to find ways to deal with this.

There are also other factors that have contributed to the industry's increased focus on digital identity management. The results of 9/11, combined with the fallout from Enron and Sarbanes-Oxley has created a 'perfect storm'. Corporates have auditors breathing down their necks and there is an increasing need to demonstrate that someone is who they say they are.

IdenTrust was created back in the 1990s at the height of the internet boom. Why is it only gaining wider market acceptance now?

IdenTrust (formerly Identrus) was ahead of its time. We were thinking about problems that everybody hoped were never going to happen. Also at that time IdenTrust was still very bank-centric, but it is corporates that are feeling the pain. Corporates started running into problems: they were receiving digital identities based on bilateral agreements, but they needed someone independent that could serve as a source of identity verification vouching for the corporate.

When we talk about identity authentication, we are talking about being absolutely positive someone is who they say they are. When companies use a digital identity based on the IdenTrust rule set, there is this chain of trust so that they know the identity is vouched for. From an IdenTrust perspective, that identity is key to activating a whole variety of capabilities and functions.

You need to feel certain that, whatever mechanism you have for storing that identity, it is the most secure and robust mechanism you can find. It needs to be something that is separated from you as a physical being. IdenTrust credentials can be stored on a smart card or USB token. We also support soft certificates. We don't support biometrics because there are so many privacy issues associated with that. Also, most of what we do is cross-border, and as soon as you start going cross-border you run into legal issues, which presents problems for solutions based on biometrics.

Yet IdenTrust uses Public Key Infrastructure (PKI), a relatively old and expensive technology to deploy.

PKI has gone through many different periods of adoption. In 1999 when IdenTrust was getting started, PKI was the thing. But it was very expensive and complicated to implement and it was more concerned with cryptography and less interested in the business implications. From 2001 to 2005, everyone started saying PKI is dead. Pin and password increased in popularity. But by the end of 2006, criminal activity and identity theft was on the increase and now PKI is enjoying something of a renaissance.

Different kinds of encryption mechanisms are used to support PKI. None of them have been successfully hacked into in a commercial setting. PKI is also less expensive to implement now. A bank that wanted to be a Certificate Authority (CA), previously would have had to spend USD 7 million to USD 10 million just to get started. Now we are talking about an investment of less than USD 500,000.

How has that translated in terms of market support for IdenTrust digital identity credentials?

Our digital certificate volume is doubling year-on-year,

“ The issue with SWIFTNet connectivity for corporates is that there is only authentication at the corporate level.

and we expect to see significant uptake in 2008. One of the problems we had historically is that we were expecting the banks to create applications that had IdenTrust identity credentials embedded in them. That didn't happen. We are now looking to develop applications such as bank account mandate management, changing account signatories and bank account opening and closing, which incorporate IdenTrust credentials.



the distribution channel for IdenTrust-based credentials, which is similar to the credit card model. We are starting with the major corporates like Shell, Danone and Merck, which have multiple banking relationships and want a single security and ID mechanism that is interoperable between all their banks. Once companies like Shell start doing it, then other people will learn from what they do.

Are you also in discussions with SWIFT regarding authenticating corporates for SWIFT corporate access?

In terms of bank account mandate management, there are examples of companies that have asked their banks for a list of account signatories only to find that 25% of them were wrong. Some people had died or left the company, but the account signatory list had not been updated. Corporates also have desk drawers full of security tokens for accessing electronic banking systems. The more access mechanisms they have, the more opportunities for someone to hack into them. It is a major problem.

How can companies get rid of this desk drawer full of proprietary banking security tokens?

Each and every bank has their own variation on how they secure their electronic banking applications, but corporates are asking for just one standard so they can interface with any bank. Some banks like Citi are saying that all of their corporate banking infrastructure is going to be PKI-based and standardised on a single platform, IdenTrust. If more banks start doing that, then all of the other application providers that service these markets are likely to follow suit.

We are not going to re-invent the wheel every time. Banks need to leverage their existing investment. Member banks in IdenTrust spent \$170 million developing a comprehensive framework for issuing trusted identities that combine policies, a legal framework, trusted operations and technology (P.L.O.T.). The IdenTrust rule set is the 'crown jewels' of the company and it is unique in the market place.

IdenTrust has historically been bank-focused. How do you envisage gaining traction amongst corporates?

Although we are starting to target corporates, banks are still

Yes. We are hearing directly from the corporates that they want to be able to use IdenTrust identity authentication with their corporate access to SWIFT. The issue with SWIFTNet connectivity for corporates is that there is only authentication at the corporate level. There is no authentication at the personal level, yet some of the major corporates are asking for 'double signing' at both the corporate and individual level.

Companies like Merck and Shell want to secure end-to-end processing linking ERP and treasury management system interfaces to SWIFT's SCORE model and using IdenTrust digital identities from start to finish. This provides them with accountability down to each individual touching the transaction. Corporates are increasingly aware of the liability associated with the information that they create and retain. Requiring individual signatures provides both non-repudiation and liability limitation.

Corporates also want to streamline their interactions with financial institutions. Using SWIFT, and having a globally interoperable standard, increases straight-through processing (STP) for corporates and their banks. It also enables a standard to be used across all financial services. This increases productivity and reduces costs. Beyond these benefits, corporates will also be able to use the same digital signature for multiple applications within the financial services provider rather than having a different authentication mechanism for each service within the same institution. Standardising identity authentication in this realm makes it easier to bring more automation to small- and medium-sized enterprises who do not have fully implemented ERP systems. //