NetworkWorld
THE NEWSWEEKLY OF ENTERPRISE NETWORK COMPUTING

Certificates merit a look

By Ellen Messmer

Banks, universities, government agencies and even churches have begun handing out public-key certificates to employees, enabling individuals to digitally sign and encrypt e-mail and files.

And while early adopters are raving about improvements in internal and external communications security, they also are running into interoperability problems and seeing regulatory

See Certificate, page 16

Certificate

Continued from page 1

hassles on the horizon.

While public-key infrastructure (PKI) products and services are available from a host of companies, organizations that have experimented with the technology say customers may find themselves getting locked into a particular vendor's offerings.

"Most [of this] equipment is not interoperable," said Paul Ma, program manager for the IT security development group at the National Aeronautics and Space Administration.

Setting up shop

Most companies adopting PKI technology are doing so in one of two ways: They are setting up shop as certificate authorities (CA) or outsourcing the job to PKI service firms such as VeriSign, Inc. and Digital Signature Trust Co.

Setting up shop as a CA basically involves installing certificate management and directory servers and complementary desktop software, such as Web browser plug-ins. Certificate management servers generate certificates, revoke them and perform other tasks. Certificates are stored in the directory server. According to product vendor Entrust Technologies, Inc., companies can expect to pay at least $10,000 per server and anywhere from $1 to $75 per user.

Organizations such as NASA, which plans to become its own CA, have found a lack of interoperability among PKI components, such as CA servers, and directory servers based on Lightweight Directory Access Protocol technology. Ma said these pieces are not as standardized as vendors would lead customers to believe.

The interoperability problems mean that a certificate based on one vendor's technology often can't go through a routine online validation check at a CA server from another vendor to ascertain whether the certificate has been revoked.

"There's fighting between the CAs to get market share," said Ma, who has spent years testing software from Entrust, VeriSign, GTE CyberTrust Solutions, Inc., Microsoft Corp., and others.

"Entrust and VeriSign have loaded up their certificates to work only with their CA," Ma claimed.

Work at the Internet Engineering Task Force on a standard called the Public-Key Infrastructure Exchange-3 is supposed to take interoperability between CA servers to a higher level. But the commercial sector, particularly banks, will be the driving force in getting the situation straightened out, Ma predicted.

Despite interoperability headaches, early adopters said public-key technology is still attractive.

"There's nothing else like it — it has no competition," said Roger White, MIS director at NationsBank, which intends this summer to hand out digital certificates based on VeriSign technology to 30,000 employees.

But White admitted there are kinks to work out with PKI. NationsBank last Friday joined dozens of other financial institutions, industry vendors and government agencies in Washington, D.C. for a private meeting of the Bankers Roundtable, a financial industry trade group, on the subject of public-key technology.

One issue that vendors need to address is how to handle PKI end users who over time are issued more than one certificate, White said. It isn't easy for client software to search a directory to find the right public-key certificate, he added.

"I'm telling my technical people — make room for a key ring for multiple certs," White said.

Ma concurred. "A major issue is multiple certificates," he said.

PKI believers

But when PKI works, it works.

The Church of Jesus Christ of Latter-day Saints, based in Salt Lake City, has handed out public-key certificates to church administrators in its offices in Australia and the U.K. This lets administrators send digitally signed Novell, Inc. GroupWise messages asking to open new bank accounts or make funds transfers.

The electronically signed messages replace a fax-based system. "With fax, we'd want to know if the request was legitimate and we'd call them to confirm it," said Ray Anderson, director of treasury services at the church.

This wasn't very convenient, particularly in far-flung areas of the world. The church plans to have 11 more international offices up with digital certificates by year-end, with a total of 58 next year. Digital Signature Trust is operating the CA server for the church, which is using Entrust's desktop suite for GroupWise.

In Massachusetts, the state's Online Government Task Force two weeks ago issued a report calling for the use of public-key certificates, according to Daniel Greenwood, deputy general counsel for the state's technology services division. But that doesn't mean the state will be handing out certificates to all its residents and businesses any time soon.

"Public-key technology should be viewed as one among many ways to authenticate a transaction," said Greenwood, who served as chairman of the task force. The state has taken pains to conduct a cost-benefit study to gauge where certificates might fit in, and the answer so far has been that many applications don't really need them.

"In some cases, the overhead of building a huge PKI is unnecessary," Greenwood said.

Still, the Massachusetts Division of Banks — the agency that handles a huge regulatory paperflow between banks and the state — has begun using certificates to exchange secure, authenticated bank filings electronically in a pilot program with GTE CyberTrust.

One thing Greenwood does not want to see is state or federal licensing of CAs. But he is in favor of developing industry guidelines on CA operations.

This work has just begun in the CA Ratings and Trust Task Force, set up under the National Automated Clearinghouse Association (NACHA).

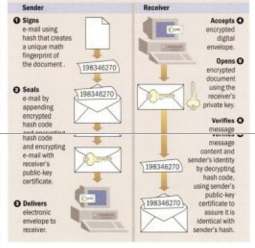
A somewhat similar effort is underway within the American Bar Association's Information Security Committee, according to Michael Baum, the committee's chairman and VeriSign's policy advisor.

At the committee's next gathering, which starts April 5 at the Patent & Trademark Office in Crystal City, Va., the group will spend three days working on proposed "Guidelines for Certificate Policies and Accreditation Criteria."

Citibank N.A., Visa U.S.A., Inc. and groups such as the Bankers Roundtable are leading the charge against CA licensing. ■

Keeping documents safe with public-key encryption

Groupware, file transfer, e-mail and even database servers can all use public-key encryption technology. Here's how to use the technology with e-mail:



Get more information online at www.nwfusion.com
DocFinder: 6338