Public Key Infrastructure (PKI) Starts To Deliver

By *Anne Chen*, eWEEK
April 1, 2001 9:00 PM PT

On June 30, 2000, president Clinton made history when he signed the Electronic Signatures in Global and National Commerce Act—federal legislation legalizing digital signatures—into law. He also helped Chuck Chamberlain breathe a whole lot easier.

Ten years ago, Chamberlain, manager of the U.S. Postal Service's NetPost Certified and e-Government programs, recommended that the USPS invest in PKI (public-key infrastructure) technologies. Until June, he was still anxiously waiting for that investment to pay off. Clinton's signature on the E-SIGN Act meant the Postal Service could officially use PKI to launch programs that include authentication of users so they can purchase postage over the Internet.

"I've probably been waiting the longest for the digital signature act to be signed," Chamberlain said. "It gives credibility to the idea of empowering our users to conduct secure and authenticated transactions over the Internet."

Chamberlain certainly hasn't been the only one waiting for the promise of PKI to be fulfilled. For years now, the IT industry has eagerly anticipated the widespread adoption of PKI, once touted as a panacea for securing e-business that would, in one fell swoop, solve the problems associated with authentication, confidentiality and single sign-on.

While the need for such an all- encompassing answer to e-business security problems is still undeniable, the reality is that, so far, most enterprises have either stayed away from PKI or limited it to pilot and small-scale deployments. That's because, for many enterprises, PKI technology has proved to be too expensive and too fraught with management and interoperability problems to be deployed on a large scale.

But that's beginning to change. While many of the cost and management problems inherent in the technology still remain, IT managers like Chamberlain are finally enjoying some success in their efforts to justify PKI investments. Indeed, annual PKI product sales are expected to top $1.2 billion by 2003, up from a mere $125 million in 1998, according to International Data Corp., in Framingham, Mass.

Much of that increased spending on PKI is due to the E-SIGN bill and new privacy regulations—such as the HIPAA (Health Insurance Portability and Accountability Act) requirements in health care—looming in many industries. And much of it is a result of a more pragmatic approach to PKI deployment being taken by many enterprises. Rather than contemplating large, enterprise wide PKI projects, early adopters such as the USPS, Visa International and PersonalPath Systems Inc. are using PKI much more selectively, and only where it can be shown to enable specific new e-business opportunities.

The lesson to be learned from such PKI pioneers, say experts: Don't get so carried away by

PKI's promise that you let the technology drive the business model rather than the other way around.

"The fundamental question is how much better are we going to be able to run the business if we have PKI," said Bill Jaeger, an analyst at Meta Secur e-Com Solutions Inc., in Atlanta. "While there is progress to be made, when we get to PKI-enabled applications, centralized directory services, integrated certificate authorities and client-support certificates, the idea of PKI will be a very sensible one. Then, we'll certainly have the ROI [return on investment] made."

While all the pieces needed to justify broad, enterprise wide deployments are not yet in place, they're getting closer. Next week, at the RSA Conference show in San Francisco, vendors such as Certicom Corp., of Hayward, Calif., are expected to announce new PKI products for enabling wireless PKI, improved interoperability and easier management.

Delivering PKI

PKI is essentially an encryption system that uses keys to identify and authenticate users. Commercial PKI products typically control which users can get access to enterprise applications such as e-commerce systems. They also provide a variety of related management capabilities such as passing out keys or certificates to users, keeping track of their use and revocation, and integrating with other enterprise applications.

Besides licensing and deploying the PKI software, user organizations must often create new policies and processes to support it. All of that, experts say, can be expensive, especially in large-scale deployments. (See chart, Page 53.) The three-year cost of owning and operating a PKI system from a vendor such as Entrust Technologies Inc., which manages 500,000 digital certificates, would be more than $11 million, according to Aberdeen Group Inc., of Boston.

That kind of cost and complexity has led organizations like the USPS to deploy PKI only where it can clearly be shown to enable new business opportunities or significantly reduce costs.

In March, the Postal Service began to reap the benefits of PKI when it announced NetPost Certified, a program that allows customers to register their public keys and get postal certificates to support online transactions, securing and authenticating electronic correspondence between government agencies.

The Postal Service plans to deploy the program at 10,000 post offices this summer. The Postal Service will act as the certificate authority and distribute certificates, but it will not actually issue keys. Those must be generated by customers themselves on their Internet browsers or placed on smart cards, said Bob Krause, vice president of e-commerce for the USPS.

NetPost Certified augments a program already in place under which the USPS issued hundreds of thousands of digital certificates to validate users purchasing postage online via their PCs last year.

Already, the Postal Service has begun to see returns on its PKI investments. The USPS, which jumped into the technology in 1991 in response to a request for it to act as a certificate authority for the Department of Defense, until recently lost about $80 million a year from meter tampering. Moving postage purchases online and using PKI, said Krause, has allowed the Postal Service to cut fraud losses significantly while also reducing costs.

The USPS, using PKI software from Cylink Corp., of Santa Clara, Calif., is also using PKI-based digital certificates to authenticate nonprofit mailers for mailing materials online.

"The upfront costs of the technology were high, but in the end, we are leveraging our PKI structure to provide real solutions to our customers," Krause said. "The opportunities for us to provide authenticated postal transactions override the initial investments."

Although the USPS is initially using PKI to enable some limited online applications, over time, Chamberlain said, the organization's PKI infrastructure will scale to manage tens of millions of certificates.

Experts say the USPS is one of the best examples of how to deploy PKI and quantify its costs.

"By taking it one project at a time, and by hiding all the technology details from the user, the USPS certainly has one of the most successful PKI deployments," said Jaeger with MetaSeS. "The key is being patient and understanding that the technology has to mature before it can solve all your security problems."

Experts like Jaeger say vendors must improve interoperability before users will be able to deploy PKI on an enterprisewide basis. Legacy and enterprise application vendors also need to support PKI. Revocation and validation models need to be supported by browsers and other applications on the client side, Jaeger said. These limitations, he said, account for why it is important for IT managers to explain to their executives that a PKI deployment cannot happen overnight and must happen in stages (see chart, right).

A healthy approach to PKI

Another organization that started its PKI deployment in a small and focused fashion, where it could deliver the most value, was PersonalPath, in Upper Saddle River, N.J., an application service provider serving health insurance companies.

Last year, PersonalPath deployed PKI over its intranet on a small scale. It chose to enable field nurses working out of home offices to access corporate documents over the Internet. Using TruePass from Entrust Technologies Inc., in Plano, Texas, the company authenticates users via digital certificates.

By allowing nurses secure, authenticated access over the Internet rather than using leased lines, Personal Path is now seeing savings of more than $1.5 million annually.

But PersonalPath, like the USPS, has much larger plans for PKI. The company began studying PKI two years ago in preparation for HIPAA regulations. Long term, PersonalPath officials see PKI as a key to satisfying comprehensive HIPAA requirements.

"The idea of the HIPAA regulations really jump-started our interest in PKI," said Tom Hagan, CIO and chief privacy officer of PersonalP ath. "But we are not just making a commitment to comply with HIPAA—we are making an investment based on the idea that PKI will be the security model of the future."

After the success of the internal rollout, executives at PersonalPath decided to begin to deploy a PKI infrastructure that would allow stronger authentication, digital signing and non-repudiation for one customer, Blue Cross Blue Shield Association of Michigan, based in Detroit.

Beginning April 30, patients using Blue Cross Blue Shield's Web portal will be able to start registering for digital certificates that will allow them to access health care information but not medical records. Over time, Blue Cross Blue Shield expects to issue up to 4.8 million digital certificates using the PersonalPath infrastructure.

"This is really just the initial infrastructure deployment," Hagan said. "In the future, we will continue to add more applications to our infrastructure."

Experts say taking PKI one step at a time is the best strategy. Indeed, many PKI implementations fail because companies succumb to the temptation to integrate too many systems with PKI at once. Because PKI can safeguard all communication transmitted on networks, extranets and intranets and provide single-sign-on authentication and digital signatures, many security managers overreach and find themselves unable to meet corporate expectations, experts say.

Even strong early supporters of PKI are coming to that conclusion. Visa International, in Foster City, Calif., for example, was an early adopter of PKI three years ago, building its SET (Secure Electronic Transaction) online financial transaction standard initiative around it.

Today, however, while the company continues to consider SET a way to reduce credit card fraud, Visa officials said they've concluded that PKI doesn't fit every type of online financial transaction.

Visa has moved away from SET and PKI for many home banking applications, for example, because it's not reasonable to assume that all consumers will have enabled digital certificates, said Tom Menessis, vice president of e-commerce authentication.

"We believe in PKI, but ... it needs to solve a technology problem or a business problem," Menessis said. "It is not necessarily PKI that is giving us the ROI, but the solutions we are able to provide because of the technology that are valuable."

While PKI isn't yet ready to fill the role of a ubiquitous, enterprise wide platform for guaranteeing secure online transactions, early backers such as Visa and the Postal Service can finally take some comfort that the technology is beginning to pay dividends. And, at least in the case of the Postal Service's Chamberlain, all it took was 10 years of anxious waiting.