

GCN

The
Technology
Authority for
Government

Government Computer News

TECH TRENDS



STOCK ILLUSTRATION SOURCE

Illinois crosses the bridge

BY WILLIAM JACKSON | GCN STAFF

Given the consolidation of the IT department, we were able to push that out to a more standardized environment.

— DOUG KASAMIS, ILLINOIS

Illinois was exploring new territory when it launched its public-key infrastructure program at the turn of the century. But it took an economic recession — and a statewide, belt-tightening information technology consolidation — to finally push PKI into use.

“In Illinois, the benefits of enabling digital signatures were recognized and proselytized in the late 1990s,” said the state’s acting chief information officer, Doug Kasamis. A contract was signed with Entrust in 2000 and the system was in production by 2001. But by 2005, only 7,000 certificates had been issued. “It didn’t really make a good business case four years into it,” Kasamis said.

Slowly but surely, however, state businesses and organizations are starting to use PKI, now that a standard infrastructure is in place. Illinois now has about 110,000 certificates in use and is issuing new ones at a rate of about 2,000 a month. Most of the state’s wastewater treatment facilities use the certificates to digitally sign and file monthly discharge reports to the state’s Environmental Protection Agency, which are passed along electronically to the federal EPA. The state claims savings of about \$12 million a year from having digitized 5,000 state and local forms that can either be printed and filled out or filed electronically.

Out in front

And Illinois is the first state to be certified with the Federal Bridge Certification Authority, a federal program to allow government agencies to recognize one another’s certificates. Judith Spencer, chairwoman of the Federal ID Credentialing Committee, hopes it will be the first of many.

“I think that over the next few years, you will see more” cross-certification between states and the federal bridge, Spencer said.

It was a budget crisis that helped to put the state’s PKI program on a solid footing. After the state’s economy took a nose dive in 2001 and 2002, Rep. Rod Blagojevich ran for gov-

ernor, successfully campaigning on a platform of eliminating the \$5 billion deficit without raising taxes.

“We had to consolidate and centralize a lot of services,” said Geoff Potter, deputy director of Central Management Services, which manages the state’s IT infrastructure and procurement. “A big piece of that was the IT and telecom arena.”

State IT systems had been created in silos, each going its own way, Potter said. “We had several dozen different desktop operating systems.”

CMS inherited the PKI program when it was charged with standardizing and centralizing the state’s IT, communications and acquisitions programs, Kasamis said. Standardized platforms made it simpler to enable applications for digital certificates, which act as electronic identifications that can be accepted online and used for authentication, encryption or digitally signing documents.

“Given the consolidation of the IT department, we were able to push that out to a more standardized environment,” he said. “We were able to leverage economies of scale.”

The state now is standardized on Microsoft’s Windows XP as its desktop operating system and on Outlook Exchange for e-mail.

“One of the best things that came out of consolidation was a standard e-mail platform,” said Mark Anderson, CMS PKI manager. And that paved the way for statewide acceptance of PKI.

Birth of a program

The state’s PKI program was born in the wake of the E-Sign law, the federal Electronic Signatures in Global and National Commerce Act of 2000 that gave electronic signatures the same status as ink-on-paper signatures.

Illinois already had enacted its own Electronic Commerce and Security Act in 1999, and CMS settled on PKI as the tool to enable the services these laws envisioned.

PKI uses pairs of mathematically related but distinct keys for encrypting data. By keeping one key private and making the

other key public, data can be exchanged securely and the identity of a person encrypting a message can be verified, creating digital signatures. Digital certificates that have been digitally signed by a trust-

ed party can be used as an online ID and can contain a private key with which the user can encrypt or sign messages.

“The Illinois act didn’t specify PKI, but it is the only technology that can meet the re-

quirements,” said Brent Crossland, head of Entrust’s state and local division.

Illinois had the option of outsourcing the job of issuing and managing its certificates to a trusted third party, or of

What’s so hard about PKI?

Applications that would benefit the most are complex, expensive

IN THE SEVEN YEARS since President Clinton swiped a smart card through a reader and signed the Electronic Signatures in Global and National Commerce Act into law, the response has been underwhelming.

“Nothing much has come of E-Sign yet,” said Brent Crossland, head of the state and local government team at Entrust.

The law gives the same legal weight to digital signatures as to traditional pen-and-ink signatures, supposedly opening the way for electronic commerce and delivery of services. There is a lot of online commerce these days, but little of it uses digital certificates, public-key infrastructure and the other mechanics of digital signatures beyond device authentication to enable secure connections.

That is not to say e-signatures are not being used at all. One of the success stories of Illinois’ ambitious statewide PKI program is the use of electronic Discharge Monitoring Reports. Each of the state’s 2,400 waste-

water treatment facilities must file a DMR with the state Environmental Protection Agency each month. With

paper reports, data must be manually keyed into state systems, leaving lots of potential for error, said Geoff Potter, head of the Central Management Services Department.

“Now, more than half of them use the PKI environment” to file electronically, Potter said. That’s great, but “48 percent still submit the forms on paper.”

Why? It’s a comfort factor, he said. Some people are just more comfortable with computers and online transactions than others. Some reporting entities are as small as a mobile-home park, and the responsible official might not trust or understand digital certificates.

“Signed paper forms in government are not going away,” Crossland

said. There is a lot of potential for online government, but “we are just getting to the point where we are starting to implement some electronic signatures.”

What makes PKI so hard? There are two major hurdles, Crossland said. Illinois has pretty much overcome the first one: provisioning digital certificates on a large-enough scale to make it worthwhile to enable applications to use them, he said.

Illinois has set up an online registration system based on its driver’s license database. Online forms that use digital signatures have a link to the registration site, where a certificate can be downloaded.

“It’s really easy for anybody to link to that registration process,” Crossland said. “It’s a real-time registration” that takes minutes for a credential with a low or moderate level of assurance, which most individuals use. “That’s a big plus.”

The other hurdle is on the back end of the process. Every attempt so far to enable electronic forms has focused on some single, complex application, Crossland said. The Illinois EPA form is a good example. Because it is a complex, dynamic form on which information in one field affects subsequent fields, it is a good candidate for automation. It can simplify the filing process and produce a good return on investment.

“But this becomes very complex and expensive to build,” Crossland said, and the user base is small. “You can’t do that for 5,000 generic forms that people need to file every day.”

This creates a dilemma. Complex applications keep PKI programs small and expensive and do not drive general acceptance. Simpler processes — such as filing a change-of-address form — do not benefit from automation as much, producing less return for the people who process them and less convenience for those who file them. But there is at least some return on enabling lots of simple forms, and it can help make PKI familiar and raise the public comfort level.

Illinois started with the complex forms but has stuck with its PKI program long enough — and its certificates are becoming numerous enough — that it is beginning to gain popular acceptance. — William Jackson



doing the job itself. The state has opted to license the software from Entrust and be its own certificate authority.

"We're a self-signing CA," Anderson said.

Not every organization assumes the responsibility of being its own CA, preferring to pass a job that is not a core competency to a specialist such as Entrust. The choice ultimately comes down to a question of "personal management preferences," said Crossland, who worked for the state of Illinois when the program was implemented. For Illinois, it was a question of accountability.

"The CMS said, 'If we're going to rely on this service, I want to be able to get my hands around the throat of the guy responsible if anything goes wrong,'" he said.

As with any technology, PKI has a front and a back. On the back end, applications have to be enabled to accept and use digital certificates, signatures and encryption. On the front end, users have to have the certificates. From the beginning, Illinois was ambitious in its plans to put the certificates into the hands of as many users as possible. Rather than restrict their use to in-house applications the certificates were made available to all citizens so that agencies could use them with public-facing services.

"The idea was to make government more answerable to the citizen," Anderson said. A Web portal was set up where citizens could download certificates, and online applications using the certificates link to the portal. The idea was to not have to explain the technology to the user, Anderson said. "The technology is basically hidden from them."

A bridge to the feds

Because the state issued the certificates, they could be trusted by any state agency, regardless of the application for which they were first issued, and they could be used by local governments, too. In 2004, they were expanded to the federal government when the state cross-certified with the federal bridge.

The bridge is an evolving solution to the challenge of ensuring that digital certificates

being used to access federal services are valid. Since the mid-1990s, the federal government's focus has shifted from issuing its own certificates to a federated system built on trusted relationships between certificate authorities.

When a digital certificate from another provider is submitted to an online application, it can be passed along to the federal bridge. The bridge can verify that the certificate was indeed issued by an organization whose policies have been accepted as trusted. The bridge also can check with the issuing authority to ensure that the certificate still is valid. The bridge opened for business in 2002, and Illinois was accepted as a trusted CA in 2004.

"Illinois saw early on the potential for a win-win situation in partnering with the federal PKI community," Spencer said. But the process was not a simple one. "We had to work long and hard with Illinois."

It was not that Illinois had done anything wrong, but the job of making the policies of various entities for issuing and managing certificates mesh is a complex one, and Illinois came to the table with a program already in place rather than building it from the ground up to federal specifications.

To date, Illinois remains the only state to be cross-certified.

"We saw some interest from other states prior to Sept. 11," when budget priorities dramatically changed, Spencer said. But post-Sept. 11 security programs, such as Homeland Security Presidential Directive 12, which mandates smart government ID cards, are spurring new interest in the bridge. The cards can carry digital certificates, and making state IDs interoperable with federal cards could make the bridge an attractive vehicle for exchanging certificates.

Illinois state police have a program to use biometric authentication with PKI to enable field access by first responders to sensitive resources.

"In 1999, that was something nobody had thought of," Anderson said. The certificates also are being used to enable data sharing between



Illinois saw early on the potential for a win-win situation in partnering with the federal PKI community.

— JUDITH SPENCER, FEDERAL ID CREDENTIALING COMMITTEE

After IT consolidation, Illinois becomes one of the first states to fully deploy a PKI and hook into the federal bridge

state and federal law enforcement agencies. “It does allow us to exchange secure information much more quickly.”

It is a
misperception
that you have to go
for a killer app.

— MARK ANDERSON, CMS

Bleeding edge

Illinois has enjoyed some successes with its groundbreaking program, and acceptance is on the rise. But you know what they say about pioneers: Those are the guys with the arrows in their backs. Did Illinois jump the gun in being the first with a statewide PKI program for citizens? At the very least, some mistakes were made.

“They probably went down some blind

alleys along the way,” said Crossland, who was there at the time. “Anybody could point out mistakes that were made. I think it was a smart thing to do. Maybe a little premature.”

“We were too decentralized to begin with to roll it out in the late 1990s,” when the project first began to take shape, Kasamis said. That problem was taken care of by fate, finances and a new administration. He also warns against looking for a single application that will justify the project and provide a return on its investment. “There is no single killer app,” he said.

Anderson agrees. Single sign-on was expected to be the driver for PKI and digital certificates, but after six years the system doesn’t have the critical mass to achieve this.

“It is a misperception that you have to go for a killer app, because it sets out an unobtainable goal,” he said. Go for the incremental improvements and savings instead.

Illinois has enabled about 30 state applications for PKI, and more are being enabled by local governments and universities. But it is the mass of users driving demand for

those applications that spell success for a program, Kasamis said.

“It’s not the number of applications, it’s the number of certificates that I get excited about,” he said.

But it now appears that going after the mass market at the beginning, as Illinois did, might not be the best idea. Crossland said there is a clearer idea today of how to go about implementing PKI, thanks in part to the ground Illinois has broken and some of its missteps along the way.

“There isn’t anything that was inherently wrong about what we thought about PKI,” he said.

Illinois began its implementation with a public deployment of certificates to enable user applications. Then it moved on to supplying state staff and administrators and finally looked at network security and device authentication. The consensus now is that is backward, Crossland said. “Now we talk about network security and device authentication first,” and deploy certificates out to individuals later.

Who knew? ■