Will PIV-I be the identity standard of the future?

Monday, August 29, 2011

Or is it already?

BY ZACK MARTIN, EDITOR, AVISIAN PUBLICATIONS

It didn't take long after the Personal Identification Verification (PIV) standard was unveiled and government employees were being issued credentials for someone to come up with PIV-Interoperable.

The idea was a bit amorphous at first, most seemed to think it would be used for government contractors and first responders. But that's changed. Government contractors are rolling out enterprise identity management systems using the PIV-I standard, and corporations that do little to no business with the government are considering deployment to comply with regulatory issues such as Sarbanes-Oxley and Payment Card Industry Data Security Standards.

"What we find in working with industry is that there are tremendous incentives to use PIV-I from a governance, risk management and compliance perspective," says Sal D'Agostino, CEO at IDmachines. "You can leverage best practices to meet any compliance regime out there. Consolidation of all these compliance issues has a real economic benefit and can help keep a company safe from situations where they could be liable for penalties of up to $1 million a day."

And while corporate America considers using the identity standard, state and local governments as well as contractors are already rolling it out. Over the last few months CertiPath, Verisign, Entrust and Verizon have announced cross-certification with the Federal Bridge Certification Authority at the new PIV-I assurance level. Any organization that wants to issue PIV-I credentials and use them to communicate with the federal government can contract with these companies.

Why PIV-I?

The original scope of PIV-I was just for non-federal issuers and contractors who need to communicate frequently with the federal government, says Anna Fernezian, identity management program manager at CSC. "Many organizations have daily requirements for acknowledging documents or acknowledging reporting structures that need to be signed and trusted by the federal government," she says.

The spec is meant for government contractors who will be working on a job for six months or less, says Gary Moore, chief architect for global governments at Entrust. Anything more than six months and contractors are required to undergo a background check from the government.

Government contractors are still the primary audience for PIV-I, but the scope has grown to include health care workers, first responders and possibly even everyday citizens wanting to secure their identity online.

The standard has grown more popular because of its stability and options with certification, says D'Agostino. "There are multiple options you can take … cross certify yourself, create your own

certificate authority, get certificates or get the entire thing as a service," he says. "PIV-I is pretty clear on how to go about and do it and there are options in the marketplace."

And there may be more options coming soon, D'Agostino says. FIPS 201 is being revised and the first draft has been released. While PIV-I is considered a smart card standard now that may not be the case in a few years. "Look at this as more than just a smart card," he says. "It gives people options on how to do it. Having the entire specification built on standards-based technology and protocols are signs of a very mature offering that makes it very attractive."

When choosing a smart card system there are two routes an organization can go: standards-based or proprietary. Proprietary systems sometimes perform better than standards-based systems but they lock an organization to a specific vendor or product set.

Standards-based systems, like PIV-I, give organizations options. Smart cards can be purchased from one organization, readers from another and software from another still. There are also economies of scale with standards-based technologies.

"Certainly with standardization, costs are reduced because you have more providers, more vendors, more opportunity to purchase products … so prices become more competitive," says Fernezian.

Tapping into the 'civilian CAC'

Sam Strickland, Booz Allen Hamilton's Executive Vice President and Chief Financial Officer, goes through the security process to get his PIV-I card

Booz Allen Hamilton had been having the discussion around PIV-I for some time, says Frank Smith, chief technology officer at the consulting firm. "But it wasn't until NIST published a standard three-years ago that VeriSign started thinking about building capability around it," he says. VeriSign is the contractor for the Booz Allen program.
Two years ago the company started preparing for its issuance of PIV-I, what Smith calls, a "civilian Common Access Card." The process wasn't necessarily easy. "There are policy issues you have to work through and those will be living as the implementation passes," he says. "It's a fundamental change to how an organization deploys security."

Previously, Booz Allen had a corporate ID with proximity technology that was mainly used for physical access control, Smith says. For logical access and digital signatures employees used software certificates.

In order to issue a PIV-I credential, the company had to collect fingerprint data from employees, something not all were comfortable with, Smith explains. There are also legal issues governing the collection of biometrics from employees at private companies. If they do not work directly with a federal client, Booz Allen gives employees the option of opting out of the biometric collection.

The change in the physical appearance of the badge can cause problems too, Smith says. “Anytime you change the layout it requires work so the current employees know what the badge looks like,” he explains. “The time it takes to do that becomes fairly significant.”

There has also been change in how the ID is issued. Employees must be physically present to enroll for the credential and then pick it up. The employee’s identity also must be confirmed with the one stored on the card before it is activated.

This has added time to the process. It’s not always practical for the employee to wait for the card to be issued as it can take 15 to 30 minutes for printing and encoding. The time adds up when issuing credentials to 28,000 employees across the country.

Booz Allen uses both fixed issuance stations and portable versions that go out to smaller offices, Smith says. The company is now one-third of the way through its issuance process.

The credentials that have been issued are being used internally for logical access, Smith says. Booz Allen was the first contractor to be cross certified with the Federal PKI Policy Authority. Still before the IDs can be used at a government site, the agency must enroll it in its specific security system.

Booz Allen’s customers are happy with the system, Smith says. “They don’t have to issue an ID card, they just have to recognize ours,” he says. “It keeps down their cost and is more efficient.”

The company is working to have the credential recognized by all the federal agencies it works with, but it’s a piecemeal effort. The credential is cross certified with the Federal Bridge, which means it’s a recognized ID, but agencies decide whether or not to accept it. “Each single client has to make the decision to cross certify the credential,” Smith says.

Booz Allen has had more luck having its credential accepted for logical access than physical access. “But I’m sure that will change,” Smith adds, “as more physical access control systems roll out.”

The physical access control piece of the system is still moving into place at Booz Allen facilities, Smith says. Because prox had been used previously and the new credentials haven’t been issued to everyone, employees must temporarily carry two IDs. The plan is to replace all the legacy prox readers and use contactless for all physical access control.

The project overall has been well received from clients, employees and executives at the firm, Smith says. “By consolidating logical and physical access we now have a one stop shop,” he says. “Everything happens with one process.”

Smith still warns that the project is not for the faint of heart. “PIV-I is no trivial undertaking,” he says. “Make sure you know the time and effort that goes into deployment. But it’s a significant improvement in our ability to provide end-to-end identification.”

First responders take to PIV-I

PIV-I has also been touted as a standard for first responder credentials, and a few jurisdictions across the country have started to issue new IDs. Virginia, with it’s location close to the capital, was one of the first states to start issuing PIV-I, says W. Duane Stafford, statewide credentialing coordinator for the Commonwealth of Virginia.

FEMA started the effort to push an interoperable credential to firefighters, paramedics, police and other first responders. The Sept. 11 attacks showed it was difficult to keep track of first responders reporting to a scene. A secure credential that stored the individual’s qualifications emerged as a tool to help solve the problem.

The Virginia ID contains a verified identity, listing of the cardholder’s specific skill set and biometrics that comply with the PIV-I standard. “We wanted to deploy an interoperable credential that we could recognize and that others could as well,” says Stafford.

At the close of 2010, nearly 13,000 credentials had been issued and 39 handheld scanners purchased for on-scene validation, Stafford says. There are also eight enrollment and issuance stations hosted by local jurisdictions around the state. Verizon Business set up the system for the commonwealth.

To keep costs in line, Virginia is only issuing the IDs to first responders who could be deployed across state lines, Stafford says.

The state has also been working with private industry, phone, gas and electric companies, so they could possibly use a PIV-I credential as well when responding to scenes, Stafford says.

Entrust sees an opportunity to provide PIV-I credentials to first responders across the country, says Entrust's Moore. "Many states don't have the ability to gear up the infrastructure to issue cards to first responders," he says.

The company announced a new service extending its Non-Federal Identity SSP service to include PIV-I compliance for state governments, the private sector and entities that wish to securely communicate and interoperate with the U.S. federal government.

Health care is taking a hard look at PIV-I as well. The National Institute of Health is using PIV-I credentials for login to PubMed, Moore says. PubMed is made up of more than 20 million citations for biomedical literature from MEDLINE, life science journals and online books.

CertiPath is also hearing from the health care market, says Steve Howard, vice president of credentials at CertiPath. The main interest has been from those working with regional health information networks for access to systems.

But CertiPath is also issuing PIV-I credentials in little thought of places, such as the janitorial staff at secure government facilities, Howard says. The U.S. Army Reserve is requiring that contractors have PIV-I credentials for access to facilities, and this includes vendors and janitors.

Vendors can use the credential to electronically sign and deliver contracts and then those employees who are working at a site can use the ID for access to facilities, Howard says.

Physical access may have been the main use case for PIV-I, but a stronger case for online identity may be in the works. With the National Strategy for Trusted Identities in Cyberspace released in April, some are making a case for PIV-I to be a credential standard.

The strategy would offer consumers options in order to secure identities and conduct transactions online. There would be levels of assurance, identity proofing attribute sharing all included in a possible identity scheme. Exactly how this would be done and what technologies would be used have yet to be determined.

But Howard says PIV-I will be a player in the market due to its stability, and by the time the strategy is finalized, the number of credentials that will already be in circulation. "It is the only standard that works," Howard says. "For non-federal parties, the only game in town is PIV-I."