

PKI picks up the pace

Government allows for broader participation by contractors

BY ALICE LIPOWICZ

The federal public-key infrastructure has seen a quickening pace of activity in recent months as the government has begun allowing more options for contractors and state and local agencies to participate in the system.

PKI is a system of identity management and information security developed during the past two decades. Organizations that participate in a PKI pact agree to trust one another's credentials.

Several developments at the Defense Department and federal PKI authorities have spurred acceptance in recent months.

In September, DOD authorized its first non-DOD provider for digital certificates that can be used to access the department's computer systems. It is the first time a commercial provider, Exostar LLC, of Herndon, Va., can sell a credential that can directly access DOD systems at a medium level of security.

Exostar's emergence as an officially sanctioned purveyor of digital certificates follows a DOD policy change initiated a year ago to expand use of external PKI vendors, said Paul Grant, special assistant for federated identity management and external partnering at DOD.

"This is a great step," Grant added. "We want more organizations to be credential service providers."

Exostar is selling the digital certificates primarily to aerospace and defense companies and their suppliers. "We have seen a lot of interest, especially given the cybersecurity threats that exist and the requirements of the DOD," said Vijay Takanti, vice president of security and collaborative services at Exostar.

NEW MOMENTUM

In February, VeriSign Inc. became the first vendor authorized to sell a managed PKI service with digital certificates trusted by the

federal government at the medium hardware level. Colorado, Kansas, Pennsylvania and several commercial companies have signed on for the service, VeriSign officials said.

VeriSign's service can be used for physical or logical access and with or without a smart card for identification. VeriSign is targeting contractors, companies and public agencies that need to communicate with federal agen-



cies via secure e-mail, secure Web sites and digital signatures.

"I'm asserting there is a new wave of momentum for PKI that started this year driven by the need for interoperability with the federal government," said Nicholas Piazzola, vice president of government programs at VeriSign. "Not only is PKI not dead, but it is revitalized."

As of June, more than 20 companies are participating in a trust network between the federal government and pharmaceutical industry through the nonprofit Safe-BioPharma

Association's PKI system. The drug companies use PKI to securely submit and sign applications with the Food and Drug Administration. They also use it for research documents, applications and other forms at the National Institutes of Health, DOD, the Veterans Affairs Department and other agencies.

"We are seeing some significantly increased activity among our members," said Mollie Shields-Uehling, president of Safe-BioPharma. "It is critical to be interoperable with the federal government agencies."

The federal PKI system allows for interoperability through the Federal Bridge Certification Authority and works with vendors, government agencies and cross-bridging organizations, such as Safe-BioPharma for health care and Certipath for aerospace and defense.

Although PKI encryption technology has been in use for decades — originally in national security applications, such as secure phone calls, in the 1980s — it has had limited use because of its complexity and cost. However, the technology got a significant boost this decade through Homeland Security Presidential Directive 12 and Personal Identity Verification card programs for federal employees. Those programs, which are not yet fully deployed, include use of digital certificates to verify identity for physical and logical access to federal systems.

At Certipath, interest in federal PKI has been expanding throughout the supply chain to nonaerospace companies. Some are using it to ensure interoperability with DOD and other federal departments, and others use it for their own internal purposes, including uses such as tagging equipment and securely approving maintenance tasks, said Jeff Nigriny, Certipath's president. "There is a viral effect happening," he said.

Although PKI is most commonly used online for Web sites and secure e-mail, Certipath recently built and began operating a

SAMPLE

model architecture for PKI use in physical access systems, too, he said. Such a system has advantages such as being able to immediately revoke access when an employee leaves a company.

"When an employee leaves, we do not want them to be able to log in and access the company computers or to have physical access to the buildings," Nigriny said.

At Safe-BioPharma, the drug companies, which are highly regulated, developed a digital certificate standard that is interoperable with federal systems. Shields-Uehling said other catalysts for adopting PKI are cost and ease of use as the technology evolves to replace large quantities of paperwork — not only for applications and materials submitted to federal authorities but also for human resources and contracting.

"We are seeing all kinds of uses for the digital certificates, such as digitally signing for pay, for contracts, and for things like conflict-of-interest forms," she said.

FDA relies on PKI systems for ensuring the security and identity of applications and other multiple forms, and the National Institutes of Health has been testing the use of PKI for federal drug investigations, she said.

"NOT ONLY IS PKI NOT DEAD, BUT IT'S REVITALIZED."

NICHOLAS PIAZZOLA, VERISIGN

The next phase is addressing uses of PKI within health care reform and the adoption of electronic health records, which includes updates to the privacy framework of the Health Insurance Portability and Accountability Act.

"There is a lot of discussion about using PKI for meeting the privacy provisions of

HIPAA," Shields-Uehling said. PKI for patient consent management is a possibility, she added.

TECHNOLOGY REVITALIZATION

Piazzola, who has been working with PKI since the 1990s and at VeriSign for 13 years, said the industry has seen some slow times and is enjoying a resurgence because of the federal promotion of the technology.

"PKI has always been nontrivial; it is a fairly complex and esoteric thing," he said. "People are more amenable to PKI today. They recognize that it is the de facto mechanism for higher security and for interoperability with the federal government."

"The feds revitalized PKI with the mandate for everyone to have PKIs on the smart card," Piazzola said "Now there is continued growth because if you want to talk with the feds, you need to have PKIs." •

Alice Lipowicz is a staff writer for Washington Technology.

2009 WINNERS

7th Annual Greater Washington

Government Contractor Awards

Congratulations to the 2009 Award Winners

Contractor of the Year
(less than \$25 million)

★ Dovel Technologies

Contractor of the Year
(\$25 to \$75 million)

★ High Performance Technologies, Inc.

Contractor of the Year
(\$75 to \$300 million)

★ Whitney, Bradley & Brown, Inc.

Contractor of the Year
(greater than \$300 million)

★ CACI International

Executive of the Year
(less than \$75 million)

★ Jerry Torres, Torres Advanced Enterprise Solutions LLC

Executive of the Year
(\$75 to \$300 million)

★ Bill Hoover, AMERICAN SYSTEMS Corporation

Executive of the Year
(greater than \$300 million)

★ Sudhakar Kesavan, ICF International

Public Sector Partner

★ David Drabkin, GSA

Hall of Fame Inductee

★ Alvin E. Nashman, Former Executive, CSC

Leadership Award

★ *The Honorable John W. Warner*

The GovCon Awards are Presented in Partnership by



WashingtonTechnology

Platinum Sponsors

Grant Thornton



Gold Sponsors

- Aronson & Company
- Holland & Knight LLP
- Houlihan Lokey
- Jones Lang LaSalle
- MARSH, Inc.
- Microsoft Dynamics
- Nemaocolin Woodland Resorts
- PNC Bank

www.govconawards.com