GljlwdoGQhzv
RQOLQH DQG GLJLWDO LGHQWLILFDWLRQ/VHFXULQJ ZHE 513/SNLDQG GLJLWDO FHUWLILFDWHV

Trusted identity plan unleashed

Share Thursday, June 9, 2011

Now comes the hard part for NSTIC

By Zack Martin, Editor, AVISIAN Publications

When the National Strategy for Trusted Identities in Cyberspace was released in April some described it was "Woodstock for identity geeks." Industry officials were excited to see the plan and hear what was announced, but there weren't a lot of surprises.

The goal of the strategy is to protect privacy, fight identity theft and fraud, drive economic growth by driving business online and create a platform for new Web services, said a White House administration official. User names and passwords are no longer good enough and potentially pose a national security risk. In order to secure online identities, something more is needed–be it a smart card, USB token, mobile device or something else.

The government would work on setting standards and facilitating the process while the private sector takes the lead in deploying the credentials and systems used to read them. "Our goal is to have a credential that would work anywhere online. If consumers want to have more than one they can," said a White House official.

The Department of Commerce is leading work on the strategy, with the program office located with the National Institute of Standards and Technology, says Jeremy Grant, senior executive advisor of ID management at NIST. There are also plans to fund pilots in fiscal year 2012 with $24.5 million earmarked for these tests in the Commerce Department budget.

NIST will also be having a series of workshops across the country this summer to discuss the strategy. The first two will be held on the east coast with one on the west coast slated for late summer. Governance of the identity system will be a topic covered in the first meting scheduled for early June with future meetings addressing implementation, Grant says.

"We can hear from folks in the private sector–not just industry but other stakeholders like privacy advocates, consumer advocates, nonprofits and get their views as to how as we move forward," Grant says. "We'll get feedback in terms of what's out there today rather than have to try and start from scratch."

Trying to build on work that's already been done is important, Grant says. "Companies have an incentive to be working around common standards and operating rules," he says. "Industry is excited about NSTIC as a way to bring everybody together to solve some of these issues and frankly to provide some clarity where there isn't any right now."

In the past the private sector has been hesitant to offer solutions to the public around securing identities, but the strategy aims to change that, the administration official said. There have been concerns around liability for companies involved in identity, but the strategy intends to clarify these issues. There are no plans, however, to draft legislation around the strategy, Grant adds.

"Anytime you're counting on legislation to enable you to do something, you're setting up a very big barrier," Grant says. "Congress does not pass a lot of standalone legislation. A lot of this gets back to the governance structure that we were talking about, and we won't really know until we really start to get stakeholders together collaborating."

Overall, reaction to the strategy has been positive. A common refrain regarding the document is its perfection. "It is a utopian document," says Aaron Titus, chief privacy officer and vice president of business development at Identity Finder. "Hating NSTIC, in its current form, is like hating puppies and rainbows because it just about says anything that anyone would want. My concern is in the implementation, there's a lot that can go wrong."

Titus has been following the strategy since it was first announced more than a year ago. Originally he had concerns regarding privacy, but the document soothed some of

Subscribe

To subscribe for free to our weekly email newsletters and print magazines, **enter your email below.** Or, find out more »

Enter Email Here

- Health Care
- Internet Security
- OTP
- PKI
- Payments

Print Magazine

Regarding ID Magazine in print & PDF. **Click to subscribe.**

Featured Events

ASIS International 57th Annual Seminar and Exhibits · *September 19*

2011 Smart Cards in Government Conference · *November 1*

Links

- Follow us on Twitter
- About AVISIAN
- Advertise
- *DigitalIDNews* RSS Feed
- Subscribe
- Purchase back issues
- Purchase online Library access

those concerns.

Grant says making sure privacy concerns were met was a priority. “Privacy ideals like the Fair Information Practice principles are reflected in there,” he says. “One message that we’ve gotten is it really did strike the right balance which will enable us to help to bring people together from different sectors around a strategy that’s going to work best for the American people.”

Still policy is going to have to be developed around privacy concerns with the strategy, Titus says. For example, a 13-year-old wanting to logon to a site needs to authenticate his age. This is done now by providing a date of birth, which is too much private information. In an NSTIC world he would provide his credential and the identity provider would verify that he met the age requirement to access to the site.

Not having to give up the additional information, such as date of birth, is privacy enhancing, but what has yet to be determined is what the identity provider can do with the information in its control.

“The identity ecosystem does create some potential problems,” Titus says. “There’s a new central hub and unless done properly your ID provider knows your date of birth and potentially every other piece of information along with your transaction history.”

There needs to be policies put in place to make sure that the ID providers can’t sell that information to third parties, Titus says. “While my retail privacy might be enhanced my wholesale privacy might disappear,” he adds.

Consumers and privacy advocates need to have a voice as the policies and technologies that will make up the strategy are unveiled, Titus says. The identity providers will have a lot of consumer information and what happens with it needs to be regulated. “We should be prepared to regulate these businesses the same we do with credit reporting agencies,” he says.

Titus is also watching how NIST’s role in facilitating the strategy will develop. The organization has a great reputation when it comes to creating standards while keeping out of the political discourse. This may have to change as many of the larger companies with possible roles in the identity ecosystem get ready to contribute.

“They have the right team but when things start getting contentious and the bullet start flying I worry that NIST will retreat back to its comfort zone and leave the policy creation to those with the most fire power, the Google’s and Facebook’s,” Titus adds.

The National Strategy for Trusted Identities in Cyberspace was released on April 15 with comments from U.S. Commerce Sec. Gary Locke, Howard Schmidt, White House Cybersecurity Coordinator, and U.S. Senator Barbara Mikulski, as well as a panel discussion with private sector, consumer advocate, and government ID management experts.

Is it a national ID?

While NIST, other government officials, academics and private sector executives have said that the national strategy is optional and not a national ID program, some are not convinced. Jim Harper, director of information policy studies at the Cato Institute, says the government’s role in the strategy is too large.

“What’s important to me is making sure that we avoid having a national ID system and the privacy and civil liberties consequences that flow from that,” says Harper, also author of *Identity Crisis: How Identification is Overused and Misunderstood*. “It’s a Soviet style planning document that won’t move the ball forward. If it does, we’re at substantial risk of a poorly designed system.”

In his book Harper says the private sector should be left to come up with an online identity scheme if one is needed. Even though the national strategy calls for the private sector to implement the program, Harper is still critical.

“One justification I’ve heard for NSTIC is that the companies haven’t gotten together to work on an interoperable system,” Harper says. “That doesn’t mean that there’s a government role in doing that, society might not be ready for it.”

As for solutions to solve the problem of online identity, some already exist. “Friends of mine in the identity community kind of wrinkle their noses when I say ‘look at Facebook Connect,’ (suggesting) that it’s a dumb simplistic solution,” Harper says. “Little experiments done by big companies or by small entrepreneurs are going to poke at this problem from various directions.”

Harper warns that while a lot of time and money will be absorbed by the national strategy it's more likely that the right identity solution will come from somewhere else. "The exciting things that may come in the identity debate will come from small entrepreneurs," he adds.

NIST's Grant knows there are concerns that NSTIC is a national ID, but he says they are unfounded. He points out that the route the U.S. is taking is the opposite of what other countries have done where a specific technology was mandated. "The role the government does play with NSTIC is to facilitate and work with the private sector to come up with best practices," Grant says.

Still he does understand the concerns. "The devil is in the details and how it will be implemented," he says. "I believe it can be done, and I wouldn't have come back to government otherwise."

SAFE-BioPharma: An NSTIC model?

SAFE-BioPharma was created to try and transition the health care world to an electronic environment. The organization, created by the biopharmaceutical industry, is using and issuing credentials to help ease what can be paper-intensive research projects.

Mollie Shields-Uehling, president and CEO at SAFE-BioPharma, says that the organization fits with the ideas behind the national strategy. "We fit in as part of a growing network of cross-certified cyber communities," she says. "We trust the identities of other communities because we have a set of standards."

SAFE-BioPharma has been cross-certified with the U.S. Federal PKI Policy Authority. Researchers with the organization's credentials can send signed documents to government officials. SAFE BIO-Pharma can certify for level three, a high level, of identity assurance.

SAFE-BioPharma conducted a 2010 pilot study that involved government and industry cancer researchers indicates that using interoperable digital identities, digital signatures and cloud computing to accelerate initiation of a clinical trial while lowering its costs.

The ongoing study involves researchers at the National Cancer Institute's Cancer Therapy Evaluation Program, a sponsor of cancer treatment clinical trials, and the pharmaceutical company Bristol-Myers Squibb.

The National Cancer Institute's researchers used PIV credentials issued by the government while industry participants were issued credentials through SAFE-BioPharma.

In the pilot, electronic documents were placed in the cloud, where the researchers were able to access and sign them immediately. The digital signatures cryptographically guarantee the integrity of documents to which they are affixed. Prior to the study, the signature process was delayed by use of courier service, fax or travel.

The first phase of the program ran from July to October 2010 and showed the use of digital identities for authentication and the application of digital signatures to electronic documents

The second phase started early 2011 and expanded the study to include researchers in pharma company sanofi-aventis. The third phase is starting this summer and will include researchers at universities and academic cancer research centers.

The new digital identities will be part of the Research Education Bridge Certification Authority, an identity trust hub serving the country's higher education sector, which currently is in the process of cross-certifying with other trusted cyber-communities.

The pilot has successfully demonstrated the ease with which interoperable digital identities could be deployed and used to access electronic documents and apply digital signatures. It successfully eliminated the use of paper copies and allowed signed documents to be exchanged rapidly and securely online.

RELATED ARTICLES

ISG, LifeMed ID unveils the Trusted Patient Identity solution suite

Identification Systems Group and LifeMed ID, announced the release of a suite of Trusted Patient Identity solutions for the health care industry.

Built with LifeMed ID's proprietary software and a variety of hardware and identity card options, the Trust Patient Identity solutions suite connects vital patient health information to networks of hospitals, clinics and health care providers.

read more »

NSTIC online

The National Strategy for Trusted Identities in

BNC protects customers from cyber thieves with IronKey Trusted Access

Bank of North Carolina is now offering IronKey Trusted Access for Banking to help keep its business clients safe while banking online. With Trust Access, BNC provides customers an online banking experience isolated from financial malware, including key loggers, man-in-the-middle attacks and DNS attacks.

read more »

Fairfield County Bank selects Trusted Access isolated online banking

Conn.-based Fairfield County Bank is moving to

Cyberspace document is online and can be downloaded here.

Story on the document to be posted later.

read more »

protect its business clients by now offering them the IronKey Trusted Access for Banking. Trusted Access isolates online banking customers from financial malware, including key loggers, man-in-the-middle attacks and DNS attacks.

read more »

COMMENTS

Be first to comment...

COMMENT ON THIS ARTICLE

NAME

EMAIL

WEBSITE

Your full name and URL will be displayed with your comment.

Your email is not shown or shared, and is used only for your Gravatar image.

5000 characters left.

SUBMIT