IDENTITY GOES ELECTRONIC

eID HEIGHTENS SECURITY FOR ONLINE TRANSACTIONS

BY JAMIE FRIEDLANDER

In a research study done by Nok Nok Labs, 47 percent of people surveyed said they would rather scrub a toilet than create a new username and password for a website. Thanks to a new initiative, however, picking yet another username and password may be a thing of the past.

Electronic Identity, otherwise known as eID, has begun to take root in the United States. In September 2012, the National Strategy for Trusted Identities in Cyberspace (NSTIC) awarded five grants aimed at helping create a secure online environment. AAMVA was one of the five recipients, and has spent the last year collaborating with various government entities and third parties on pilot programs and initiatives.

eID does not represent an actual identification card or object, but rather it signifies the idea of being able to have a trusted and private online identity.

"eID in our context is really the notion of being able to use an identifier or mechanism to go on the Internet and conduct secure transactions with a guarantee that the people behind the terminal are actually who they say they are," says Philippe Guiot, CIO at AAMVA. Guiot is also working as the principal investigator for the Cross Sector Digital Identity Initiative (CSDII), the pilot effort headed by AAMVA.

> **IF YOU CAN GIVE PEOPLE THE ABILITY TO PROVE TO A CERTAIN LEVEL THAT THEY ARE WHO THEY CLAIM TO BE, YOU CAN MAKE PROGRESS IN TERMS OF BRINGING NEW TYPES OF TRANSACTIONS ONLINE.**
>
> — Jeremy Grant, senior executive advisor for identity management and head of the NSTIC National Program Office

The working groups involved in CSDII aim to create what they call an "Identity Ecosystem," which would mean that government entities, organizations and individuals would rely on and use eID voluntarily, according to David Burhop, the deputy commissioner and CIO at the Virginia DMV, which has been collaborating with AAMVA on CSDII.

Burhop adds that while certain countries use "physical" eIDs, microchips and card readers, he does not think that the U.S. is ready for that just yet. "For now, we're zeroing in on what the U.S. is going to tolerate, and so we're staying away from physical things, [such as] cards and chips in licenses," says Burhop. "Are we going to take advantage of that technology? Absolutely, and eventually, but not right now."

HOW IT WORKS

So without the presence of a physical card, eID will encompass credentials that fall into three categories, according to Mike Farnsworth, lead technology

Visit the multimedia page on **MOVEmag.org** to watch a video in which members of the eID Working Group discuss the latest on this topic.

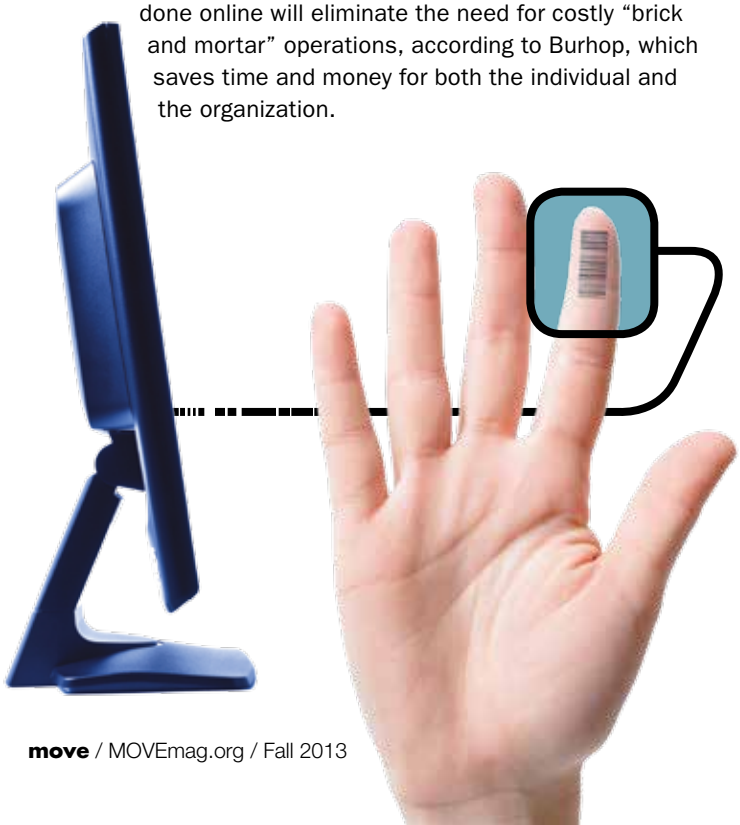
architect at the Virginia DMV. These three categories include something you know (such as a user ID or password), something you have (such as a cell phone) and something you are (such as fingerprints or a biometric identifier). Information such as date of birth and license plate number will still be relevant, though an eID will also have more secure information associated with it. Though the official solutions are still in the works, Burhop points out that one example of eID would be users getting a call back from an organization on their cell phone to prove they are who they say they are.

> **"IF YOU LOOK AT ANY OPERATING BUDGET TODAY, YOU'RE GOING TO SEE HOW MUCH IS BEING SPENT FIGHTING FRAUD AND ABUSE, AND IT'S HUGE.**
> — David Burhop, deputy commissioner and CIO, Virginia DMV

At its core, eID aims to prove that when it comes to online transactions, both parties involved are who they say they are. With the onset of eID, online users will be able to partake in riskier transactions, such as the casual sale (i.e., selling a car without a middleman), because both parties will be cognizant of with whom they are doing business. According to Geoff Slagle, director of identity management at AAMVA, this could do wonders for online businesses.

"In the casual sale scenario, as a buyer, I might be leery that I'm not sure whom I'm buying from is legitimate," says Slagle. "And the seller is thinking the same thing. The eID schema, when done properly, will give both of those parties the confidence to move forward with one another and to not have to be in person to do that [because] it can all happen virtually."

Allowing for more transactions—and riskier ones—to be done online will eliminate the need for costly "brick and mortar" operations, according to Burhop, which saves time and money for both the individual and the organization.



"There are a lot of transactions today that simply aren't available online, both in government and in the private sector, because the risk model associated with the transaction is simply too much," says Jeremy Grant, senior executive advisor for identity management and head of the NSTIC National Program Office. "So the idea here is that if you can give people the ability to prove to a certain level that they are who they claim to be, you can make progress in terms of bringing new types of transactions online."

THE ROAD AHEAD

In addition to more transactions moving to the cyber world, the onset of eID will also help curb identity theft and fraud. Hackers will have more trouble breaking into an online system, causing less identity fraud, which means less money spent targeting identity fraud, theft and abuse from the government. "If you look at any operating budget today, you're going to see how much is being spent fighting fraud and abuse, and it's huge," says Burhop.

With the benefits of eID, however, come a handful of challenges. Grant points out one of the most prominent challenges of eID: making it mainstream. "What NSTIC is trying to do, at the end of the day, is catalyze a marketplace that doesn't really exist today," says Grant. "There are different solutions that are out there, but there's not a ton of acceptance."

Grant points out that another big challenge has been getting a set framework of policies and standards for eID in place. However, AAMVA and NSTIC have helped create the Identity Ecosystem Steering Group, which brings together all the key stakeholders—banks, technology firms, health care and government—to "come up with a framework that can enable the identity ecosystem that's envisioned in the NSTIC," says Grant.

According to Guiot and Grant, several pilots are being rolled out over the coming months and years, such as a six-month eID pilot with Inova Healthcare in Virginia set to start in February 2014. Grant says to expect to see a real marketplace for eID take hold by the start of 2016.

"This is probably one of the most innovative initiatives that has been undertaken in a long time around identity," says Farnsworth. "We have a lot of industry leaders involved with it, and it is a very public-private sector initiative. And it's all being done under AAMVA, which is completely appropriate. Folks look to AAMVA and DMVs as the authoritative source for identity." m

Find and read the AAMVA eID Working Group's white paper, which presents the ins and outs of eID and what it means for the AAMVA community, at **aamva.org/eID-Working-Group**.