Electronic Identity

The What, Why, How, and Who the Subject of eID Will Impact Both in and out of the AAMVA Community

Presented By:
Scott Vien, Delaware DMV
## Members of the Working Group

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization/Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dave Burhop, Chair</td>
<td>VA DMV - CIO, Deputy Commissioner</td>
</tr>
<tr>
<td>Robert Grill</td>
<td>NJ MVC - Director, Agency Services-Field Ops</td>
</tr>
<tr>
<td>Dan Haughney</td>
<td>NY DMV - Supervising Investigator</td>
</tr>
<tr>
<td>Corey Lorenz</td>
<td>IO DOT - IT Specialist</td>
</tr>
<tr>
<td>Mike McCaskill</td>
<td>FL DMV - Business Resource Consultant</td>
</tr>
<tr>
<td>Susan McCracken</td>
<td>NB DPS - Deputy Registrar</td>
</tr>
<tr>
<td>Scott Vien</td>
<td>DE DMV - Deputy Director</td>
</tr>
</tbody>
</table>

Geoff Slagle, Staff Liaison | AAMVA - Director of Identity Mgt  
Stacey Stanton             | AZ DMV - AAMVA Chair of the Board, Board Advisor
Why the focus on eID?

- With the advancement of technology, more and more people are using the internet to perform tasks that historically have been required to be done in person
  - 245 million internet connected Americans
    (Source: World Fact Book and 2010 US Census)
- eID is going to happen whether or not we are involved, so we better get involved
  - DMVs will play an important role in eID
eID Working Group Role

- AAMVA formed eID Working Group to monitor this progression (increase in online usage) and guide our membership in addressing the issues surrounding these changes.

- Our purpose is to identify solutions and standards that yield a high level of identity assurance for online transactions.
elD White Paper

Why is it important?

What does it contain?
White Paper Importance

• Topic of eID can be overwhelming.
  – Seems futuristic

• Many questions:
  – What is eID?
  – Sounds scary...a little like “big brother”?
  – How can this possibly be secure?
  – What is the DMV’s role in eID?
White Paper Importance contd...

• White paper addresses all of these questions and more

• Presents information to the reader at a high-level, with just enough detail, so anyone (business or IT) will walk away with a much clearer understanding of the topic
White Paper Content

• Current State of online commerce/services
  – User Name and Password
  – Redundancy issues (2007 Microsoft study on 540,000 online users revealed that online users maintain as many as 25 different accounts
    • 6 billion distinct accounts all with their own criteria
  – Government agencies, including MVAs rely heavily on accurate identification
    • Can create a reluctance to offer online services due to fraud risk
White Paper Content contd…

• Define eID
  – DL/ID is identification credential of choice, far beyond its original purpose, because it contains your photo and information (attributes)
  – Attributes are what can be used to develop an eID
A secure eID requires...

- Trust in...
  - Credential’s integrity
  - Individual using the credential
  - Methods used to define and vet credential
  - Level of vetting is sufficient to meet your needs.

- Leveling-up depending on business need
- Can’t easily be done with a user name and password system
Multi-factor Authentication

– Something you have
  Ex: DL/ID, Key fob

– Something you know
  Ex: How many fireplaces were in your second home?

– Something you are
  Ex: Biometric
• National Strategy for Trusted Identities in Cyberspace (NSTIC)
  – Identity Ecosystem for interoperability

• Cross Sector Digital Identity Initiative (CSDII)

• FICAM and SICAM
  – Federal and State roadmaps for Ecosystem
    • Architecture, security, cost, interoperability, trust, and process improvement
• Roles for Government and Commercial entities in eID
  – MVAs and other government entities are ideal attribute providers because of unique, long-lasting contact with constituents

• Benefits of eID
  – Provide examples of the difference between current day and a secure Identity Ecosystem
  – Discuss how an Ecosystem leverages existing separate databases to avoid centralizing PII
• Trust Framework
  – Ecosystem doesn’t work without a framework that enables trust in the eIDs people use and rely on
  – Compilation of enforceable rules, defined governance, and standards
    • Ex: AAMVA’s DL/ID Security Framework
  – Discuss and provide in Appendix the gap analysis conducted as part of CSDII