The American Association of Motor Vehicle Administrators (AAMVA)

Testimony Before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Transportation and Maritime Security

"Identity Management Innovation: Looking Beyond REAL ID"

December 5, 2023

Chairman Gimenez, Ranking Member Thanedar, thank you for the opportunity to submit testimony on the important issue of identity management innovation and the future of identity credentialing.

The American Association of Motor Vehicle Administrators (AAMVA) is a tax-exempt, nonprofit organization that develops model programs in motor vehicle administration, law enforcement, and highway safety. The association also serves as an information clearinghouse in these areas. Founded in 1933, AAMVA represents the state and provincial officials in the United States and Canada who administer and enforce motor vehicle laws. AAMVA's programs encourage uniformity and reciprocity among the states and provinces.

Since the advent of the driving credential, state driver licensing agencies have worked diligently to find effective ways to connect an individual's driving record to a specific individual. Because roadway safety is critical to the nation's overall public safety, state driver licensing agencies have consistently sought to solve a complex issue – ensuring that the person is who they say they are. This seemingly simple, yet critical and highly technical question, is the foundation of states' efforts in identity management.

AAMVA members serve at the critical nexus of public safety and law enforcement by working to reach the goal of "one driver, one license, one record" for every individual operating a motor vehicle in The United States. What began simply as credential displaying a legal authorization to operate a motor vehicle has evolved over time to the becoming the de facto identity document. It is the state-issued driver's license and identity card that serves as the access document of choice for state services, financial institutions, and other entities seeking identity assurance.

To support our members evolving role in identity management, AAMVA provides guidance, standards, and best practices for the vetting of identities and issuance of a secure and interoperable identity credential. AAMVA is expanding members support with the fundamental understanding that identity management is not a commodity but the conveyance of a public benefit.

The development of future credentialing cannot be performed in a vacuum. AAMVA is part of both national and international bodies that develop standards defining the identity ecosystem. AAMVA has provided leadership in the work within the bodies of the International Organization for Standardization's (ISO) which is responsible for the development and maintenance of the Personal Identification – ISO Compliant Driving Licenses international standard (18013) establishing guidelines in the format and content of motor vehicle driver licenses (DLs). AAMVA published and maintains the DL/ID Card Design Standard which localizes the international standard for use by North American jurisdictions. These documents create a common basis for international use and recognition of driver's licenses and identity cards across state and international borders.

The most recent addition to the ISO 18013 standard is the Mobile Driving License (mDL) Application. This part provides the interface and data model requirements for safe, secure, trusted, and interoperable mobile driving licenses and IDs. AAMVA drafted the functional requirements that were used as a basis for the published standard and has served as convenor of the ISO working group for many years.

The development of new standards in the identity space has been spurred by drastic technology change. As the world continues to become more technologically enabled and interactions shift toward digital channels, there is an obvious need for advancement of government-grade identity management to address these new domains. It is becoming increasingly clear that the future of identity management lies in the credential's ability to be integrated onto a mobile device. It is for this reason that AAMVA and its membership have been thought leaders in transitioning the credential to a mobile driver's license, or mDL, platform. Within the realm of digital identity administration, the primary goal of issuing authorities remains the preservation of identity integrity as a public good by continuing to be its most secure, trusted, privacy preserving and convenient source.

The mDL is the future of licensing and proof of identity. An mDL is a driver's license that is provisioned to a mobile device with the capability to be updated in real time. It is comprised of the same data elements that are used to produce a physical driver's license, however, the data is transmitted electronically to a relying party's reader device and authenticated.

The mDL is a significant improvement over physical credentials which can easily be lost or stolen, become damaged, become outdated as information changes, offer too much information (including personally identifiable information not related to specific transactions), and more easily be replicated by counterfeiters. The mDL offers safe, secure, and trustable technologies that allow for completely touchless transactions, selective information release, data protection, and so much more. The mDL operates on the premise that the identity's owner is always in full control of what data is shared with the option of only providing those data elements (such as age) that are necessary for that particular use case.

A physical credential represents a snapshot in time. It is a credential subject to change with no faculty for updating the credential once it has been issued until it is reissued, revoked, or modified (sometimes over the course of many years). Additionally, with a physical credential, the person inspecting the credential may be in a situation where they are making assumptions on the validity of the physical document by the very nature of visual examination. When the relying party authenticates an mDL using a reader, they immediately know that the mDL was issued by a bona fide issuing authority, was issued to the person with whom they are transacting, was issued to that specific holder's device, that the data is less than 30-90 days old, and that the data hasn't changed since it was provisioned to their device.

Currently, for a relying party (or end user) to adequately inspect a physical document's validity, they must meet complex conditions. They need intricate knowledge of security features the state uses on the credential, and they need the tools to confirm that the exact same security features are included in the document in the places they need to be. In the case of an mDL that authentication happens seamlessly behind the scenes, so the relying party does not have to know what security features are part of the mDL - all they need is the public key. The public key is used to authenticate the mDL data on the device, and if authenticated, the data is displayed on the relying party's device. If the data doesn't authenticate, no data renders for the relying party, protecting the credential holder's data.

The process of authenticating a digital identity credential includes the technical trust point of relying party possessing an issuing authority's public key certificate. In a future environment where many issuing authorities (state driver licensing agencies) are each publishing their own public key certificate, it will be challenging for relying parties to obtain and trust all the issuing authorities' public key certificates. AAMVA's work in the mDL environment includes the development of a "Digital Trust Service" (DTS). The established AAMVA DTS collects public key certificates from vetted issuing authorities and ensures each key and the corresponding mDL product meets minimum international standards. The DTS aggregates the public keys so relying parties can easily access them in a singular and trusted location. The DTS provides validation that the state is a vetted issuing authority, validation that they are creating and maintaining their public and private keys per industry standards and comply with the ISO 18013-5 interoperability standard. Without the assurance of 18013-5 standard compliance, the credential may not be interoperable, the customer is not ensured control of their data, and there is no certainty that the mDL adheres to appropriate privacy protections.

While AAMVA anticipates the mDL will eventually be used as a singular identity credential, we recognize for the immediate future both the physical card and the mDL must coexist for redundancy and operationally significant reasons. This includes the lack of available readers in all situations, including potential law enforcement interactions (or other unanticipated scenarios where a reader is absent). For these reasons, the mDL is currently viewed as an extension of the physical card rather than an immediate replacement.

Additionally, AAMVA emphasizes that mDL interaction with relying parties will be a critical component in the future of identity management. Relying parties represent the other half of the identity equation, and in the sensible progression of identity management, the education and onboarding of those who seek access to the data provisioned on a device must be prioritized. While AAMVA and its members continue to work toward common goals in terms of public benefits, relying parties must also work collaboratively to fulfill the tenants and best practices of identity protection.

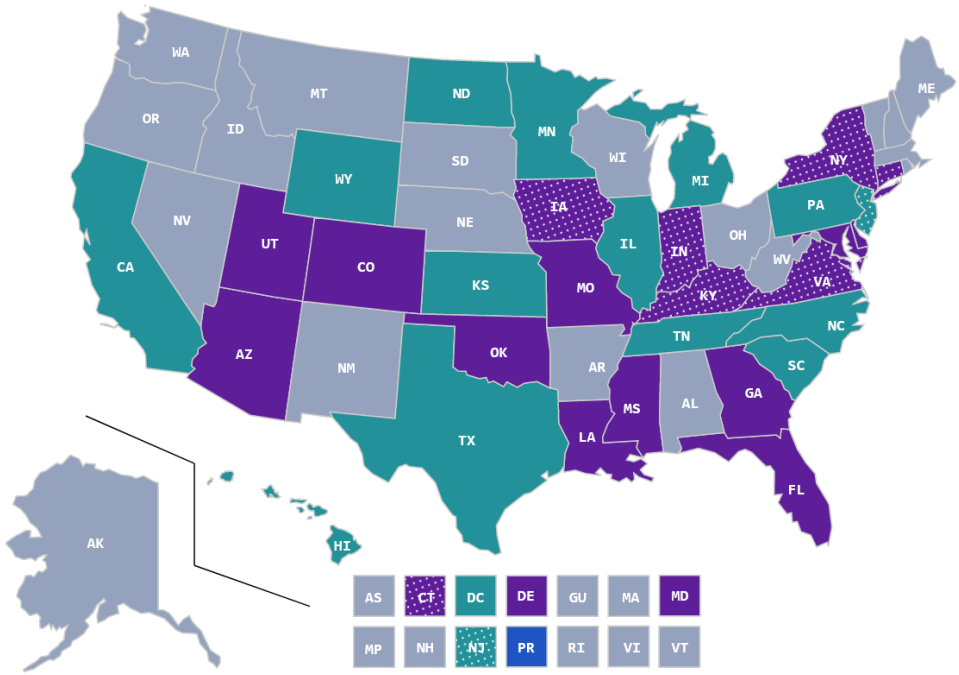
As Congress continues its consideration of the future of identity management and its impact on constituent-government interactions, AAMVA emphasizes trust as the determining factor for success. As we seek shared solutions on how to best build that trust, AAMVA urges Congress to continue studying what the future looks like and consider investments that will be critical to establishing trust networks. This includes availability of grant awards to states who invest in the foundational systems that support mobile driver's license platforms or expansion of identity transaction architecture. These investments will help ensure that as citizens make the transition to new identity models in the very near future, they are reassured that the government is supporting that transition in the best way possible. Just as we have seen with traditional driving credentials, the purpose and opportunity of identity management extends well beyond the driving credential itself.

AAMVA thanks the Subcommittee for the opportunity to testify and stands ready to continue the important conversation of how we can help further the shared interests of security and identity management.

Current State Status of mDL Implementation

Currently, 32 jurisdictions have either engaged in some form of mDL implementation or have been legislatively instructed to study or pursue mDL solutions. The breakdown by jurisdiction is provided below and is also available at: https://www.aamva.org/topics/mobile-driver-license.

Figure 1. Current State Status of mDL Implementation



Interoperable Implementation

Interoperable Implementation in Progress

Jurisdiction Specific Implementation

Jurisdiction Specific Implementation in Progress

Legislative and/or Study Activity

Attempt to Execute Legislative and/or Study Activity

Table 1. Current State Status of mDL Implementation

Stage of Implementation	Jurisdiction
Interoperable Implementation (11)	AZ, CO, DE, GA, FL, LA, MD, MO, MS, OK, UT
Interoperable Implementation in Progress (6)	CT, IA, IN, KY, NY, VA
Legislative Study or Attempt to Study (14)	CA, HI, IL, KS, MI, MN, NC, ND, NJ, PA, SC, TN, TX, WY
Jurisdiction Specific Implementation (1)	PR