AAMVA
American Association of
Motor Vehicle Administrators

OUR VISION
Safe drivers
Safe vehicles
Secure identities
Saving lives!

July 28, 2021

Steve Yonkers
Director, REAL ID Program
Office of Strategy, Policy, and Plans
United States Department of Homeland Security
Washington, DC 20528

RE: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Mobile Driver's Licenses [Docket No. DHS-2020-0028]

The American Association of Motor Vehicle Administrators (AAMVA) thanks the Department of Homeland Security (DHS) for the opportunity to comment on its upcoming rulemaking addressing security standards and requirements for the issuance of mobile or digital driver's licenses to enable federal agencies to accept these credentials for official purposes as defined in the REAL ID Act. The regulations DHS develops with respect to digital identity will define the identity ecosystem for years to come, and AAMVA and its member agencies are encouraged by the prospects of fulfilling the promise of the REAL ID Modernization Act. Digital identity concepts represent the continuation of our members' commitment to protecting identities as a part of their safety records, and further enhance the ability to serve as responsible stewards of the "one driver, one record" mantra that drives our mission of secure identities.

AAMVA offers the following comments to the Department in response to its request for information.

B. REAL ID Act, Current Regulatory Requirements and the Need to Amend the Regulation

This section cites that "Full enforcement of the REAL ID regulation begins on October 1, 2021." AAMVA understands that the RFI was likely vetted prior to the extension of the full enforcement deadline until May 3, 2023, but reiterates this additional time is necessary for states to realize the full potential of the REAL ID Modernization Act.

DHS states that "Because an mDL is issued for use as identification or to convey driving privileges, an mDL therefore, must meet applicable REAL ID security requirements in order for federal agencies to accept them for official purposes. Examples of such security requirements applicable to physical cards include 'common machine-readable technology' and 'security features designed to prevent tampering, counterfeiting, or duplication…for fraudulent purposes.'"

AAMVA agrees that DHS should use discretion on appropriate security requirements for federal agency acceptance for official federal purposes but urges DHS to leverage maximum flexibility in meeting the security requirements of a digital space. The pace of technology in this area is evolving rapidly, and rather than utilize the regulatory process to restrict the application of technology, the regulations could cite the existent REAL ID state certification process as a mechanism for ensuring that a state's mDL process meets the goal of the REAL ID program rather than limit the technology to a list of acceptable methodologies. Further, leverage of a state's security plan as submitted in conjunction with REAL ID requirements could help achieve additional flexibility. While AAMVA advises against the addition of requirements in submission or content of the plan, the plan could help describe sensitive or unique elements of mDL progression in each jurisdiction. The elements of submission as part of the state security plan, however, should not be tied directly to REAL ID compliance, as the pursuit of mDL as a solution must remain voluntary for all jurisdictions. This approach just provides an additional tool to be considered in conjunction with regulation. AAMVA notes that this suggestion is not meant to govern all aspects of the Department's proposal. Elements of the rulemaking that transcend state specific approach, such as interoperability, may best be reliant on standards-based regulatory action.

AAMVA thanks DHS for its citation of AAMVA's published mDL Implementation Guidelines on page 20322 and 2032 as a potential starting point for consideration of an mDL system and as a model reference.

III. Model for mDL Acceptance by Federal Agencies for Official Purposes

C. Communication Interfaces

1. DMV and mDL Device: Provisioning

The RFI also discusses provisioning in this section by stating, "The initial step of provisioning requires proving that the target mobile device belongs to the mDL applicant. Next a trusted connection would be established between the DMV and the target mobile device. Finally, the DMV would use this connection to securely transmit and update mDL data on the device (or enable the device to access the data)."

AAMVA notes that while most of the time, the target mobile device belongs to the mDL applicant, this is not always the case. Examples include: a parent who own's minor's device; a legal guardian (e.g. of a person with Alzheimer's) who may get the Alzheimer's patient's mDL provisioned to the guardian's device; or a parent may get a child's mDL provisioned on the parent's device.

The RFI also states that "the Department is not aware of any mature industry standards defining standardized communication protocols to assure comparable levels of trust between the in-person and remote methods of provisioning. Accordingly, DHS seeks comment (see Part IV) on the security and privacy risks, as well as mitigating solutions, concerning provisioning to ensure that federal agencies can trust mDLs provisioned either in-person or remotely."

AAMVA is currently unaware of any mature industry standards in this area. However, the trust we are seeking is really limited to making sure the mDL gets provisioned onto the appropriate target mobile device. As with the current physical driver credential (or ID), this is similar to ensuring the physical credential is properly delivered to only the individual bound to that identity. Inappropriate delivery, or in this instance, inappropriate provisioning, in itself does not compromise the card or the mDL. In case of a mDL the relying party's trust point is the public key used to authenticate the mDL, and not the device on which the mDL resided.

3. Federal Agency and DMV: Online Data Transfer and Offline Authentication

Before providing more in-depth reaction, AAMVA notes that the scope of the federal agency – DMV interactions should be limited to attended (Day 1) solutions. Current federal use cases are anticipated to be in person entering of federal buildings, nuclear power plants and federally regulated aircraft.

"In an online transaction, a federal agency would receive mDL data directly from a DMV instead of from a mobile device. In this step, a mobile device would first pass a token to a federal agency, which would use the token to retrieve mDL data from the DMV. Draft standard ISO/IEC 18013-5 governs communication protocols and methods for online verification functionality. This interface can also be used for offline authentication, although development of infrastructure and additional related procedures are required."

It should be understood that standard ISO/IEC 18013-5 describes both the server retrieval and device retrieval methods. The statement, “This interface can also be used for offline authentication, although development of infrastructure and additional related procedures are required” may be unclear as currently drafted, and could be considered to be inaccurate. The bulk of scenarios AAMVA has observed tested during mDL test events were conducted using device retrieval, meaning that the device retrieval method may be *more* established than server retrieval.

“An ISO/IEC 18013-5 compliant mDL must include both online and offline functionality. DHS is considering referencing pertinent parts of ISO/IEC 18013-5 in a future rulemaking and seeks commenters views (see Part IV) on the appropriateness of this approach. In particular, DHS seeks comments concerning the security and privacy risks, as well as mitigating solutions concerning both offline and online data transfer modes.”

With respect to the statement that “an ISO/IEC 18013-5 compliant mDL must include both online and offline functionality,” AAMVA notes that standard ISO/IEC 18013-5 currently requires an mDL to support device retrieval. Support for server retrieval is optional.

D. Other Considerations

1. Data Trust and Security Features

“For all transactions, (offline and online) DHS preliminarily believes mDL data requires protection, both during transmission (known as “data in transit”) and during storage on a mobile device (known as “data at rest”). Draft standard ISO/IEC 18013-5 requires encryption of data in transit, but not data at rest. The AAMVA Implementation Guidelines, however, seek to address this gap by affirmatively recommending such encryption. Accordingly, DHS is considering requiring, in a future rulemaking, mandatory encryption of both data in transit and data at rest. DHS seeks comment (see Part IV) concerning proposed and alternative solutions to provide the requisite levels of security to establish the trust required for federal agencies to accept mDLs for official purposes.”

With respect to the concept of “data at rest”, while it is understandable that data “at rest” on a physical card needs to be protected, the need is perhaps less critical in the case of an mDL (for the Day 1 solution, where the relying party confirms the match between the authenticated data and the mDL presenter). Any alteration of data will immediately be evident to a relying party. Protection of data at rest therefore is primarily about protecting the privacy of the mDL holder (i.e. not allowing access to the data without the consent of the mDL holder). These considerations have broad implications which may lie outside the scope of this rulemaking and is best relegated to the issuing authority to establish controls inclusive of current and improved state and federal statute. Considerations for the Day 2 solution, where the issuing authority takes responsibility for matching the person to the mDL at transaction time, are different.

2. Data Freshness

“Preliminary, DHS believes that shorter data freshness periods may bring security benefits, and is exploring the benefits and costs of requiring specific data freshness periods in the regulation.”

While AAMVA is unable to definitively provide guidance at this time on data freshness, stakeholder deliberations have identified a refresh period of 30 days as a starting point until such time as operational implementations have provided a greater sample of appropriate measures. However, AAMVA strongly recommends that DHS leave the timeliness of data freshness to the states, or let the states determine and govern appropriate timeframes themselves, rather than prescribe this via regulation. There are direct financial implications that will vary by state and could impact the utility of the regulation and its associated mandate.

IV. Questions for Commenters

1. *Security Generally.* Provide comments on what security risks, including data interception, alteration, and reproduction, may arise from the use of mDLs by Federal agencies for official purposes, which includes accessing Federal facilities, boarding federally-regulated commercial aircraft, and entering nuclear power plants.

a. Explain what digital security functions or features are available to detect, deter, and mitigate the security risks from mDL transactions, including the advantages and disadvantages of each security feature.

AAMVA provides the following enumerated digital security functions and their associated advantages and challenges:

1. Public/Private Key Infrastructure

a) Signature over Mobile Security Object authenticates data and data origin.

- Advantage: The authentication process results in a yes/no answer.
- Challenge: Verifier needs to trust the public key it uses for the authentication.

b) Mobile Document (mdoc) authentication confirms binding to device (i.e. it was not copied).

- Advantage: The authentication process results in a yes/no answer.

2. Encrypted data transfer

- Advantage: mDL data is protected during transmission.
- Challenge: None.

3. Passive authentication

- Advantage: Does not require the relying party (RP) to place any trust in the device that carries the mDL.
- Challenge: RP must obtain the issuing authority's public key, and trust that the key actually belongs to the claimed issuing authority.

b. Provide comments on how mDL transactions could introduce new cybersecurity threat vectors into the IT systems of Federal agencies by, for example, transmitting malicious code along with the mDL Data.

While AAMVA is not positioned to provide the best answer regarding the latest global cybersecurity threat environment, we do offer that a key component of safeguarding transaction data exchanges relies on the mDL authentication process. If the digital signature on the mDL data does not authenticate, then the data, and the transaction, should not be trusted.

c. Sections 37.15 and 37.17 of 6 CFR part 37 set forth specific requirements for physical security features for DL/ID and other requirements for the surface of DL/ID. Provide comments on what requirements are necessary to provide comparable security assurances for mDLs.

Passive authentication, which is at the heart of a mDL, arguably provides better security than physical security features.

***2. Privacy Generally.* Provide comments on what privacy concerns or benefits may arise from mDL transactions, and how DHS should or should not address those concerns and benefits in the REAL ID context. Explain what digital security functions or features are available to protect the privacy of any personally**

identifiable information submitted in mDL transactions, including the advantages and disadvantages of each security feature.

Privacy benefits associated with mDL transactions:

- The device retrieval method supported by ISO/IEC 18013-5 offers the benefit of sharing government-issued and certified identity data, yet without any involvement of the government (issuer) in the actual mDL transaction. When using device retrieval the government (issuer) does not know that the mDL was used, does not know what was shared, does not know with whom it was shared, does not know where the transaction took place, or that it took place at all.
- The selective data release supported by ISO/IEC 18013-5 allows a verifier to ask for specific driver's license data elements, and for a mDL holder to approve the sharing of only some of the data requested by a verifier.
- The data minimization supported by ISO/IEC 18013-5 adds granularity to traditional driver's license data fields. For example, in addition to a person's date of birth, ISO/IEC 18013-5 supports an age statement, as well as statements in the format "the mDL holder is older than x years". This allows for the exchange of less "privacy revealing" data: Sharing that a person is older than 21 reveals less personal information than sharing a date of birth.
- The "intent to retain" indicator required by ISO/IEC 18013-5 for all data elements requested by a verifier informs mDL holders if a verifier intends to retain data beyond the immediate transaction.
- An mDL app design can contribute to mDL holder privacy in numerous ways, including clearly communicating what data is being requested, allowing easy means for approving the release of specific data elements, and clearly warning a mDL holder if a verifier intends to store information.
- ISO/IEC 18013-5 was designed so that an mDL holder always stays in control of device; the protocol does not require a verifier to access or view holder's device.

Privacy challenges associated with mDL transactions:

- The protection of data after having been shared is dependent on local legislation. DHS may want to consider regulating the use and retention of mDL and related information by relying parties. It should be noted though that this challenge is not unique to a mDL, and applies to physical credentials as well.
- Jurisdictional law can require physical credentials to be confiscated, typically to effect the revocation of driving privileges. This is undesirable in the case of a mDL. Potential mitigating solutions include:
    - Having jurisdictions update local law to focus on the end result (i.e. the revocation of driving privileges) rather than on the method (confiscation of the credential).
    - Requiring states to convey driving privilege revocation, especially for out-of-state drivers, in a timely fashion via existing channels (specifically the electronic conviction reporting capability available in the S2S system).
- Verifier tracking of mDL holder: For Day 1 (where the relying party confirms the match between the authenticated data and the mDL presenter , and therefore needs the photo), this is just a special case of not controlling the data once released (see above). For Day 2, where the issuing authority takes responsibility for matching the person to the mDL at transaction time, ISO/IEC 18013-7 is expected to support implementations that do not share any identifying information (including metadata).
- It would be possible for an mDL app to contain functionality that is not declared to the mDL holder (e.g. recording activity, location, or to allow access without permission). One way of addressing this would be for Issuing Authorities to allow open source apps.

3. Industry Standards. **Executive Order 12866 directs Federal agencies to use performance-based standards whenever feasible. DHS is considering including technical standards for mDL transactions in its proposed rule, drawing heavily on standards under development by the industry, to support compatibility and technical interoperability across all interested Federal agencies nationwide. If commenters believe an industry standard should be chosen, provide comments on how DHS should choose the correct standard(s) for mDLs, and on the appropriate baseline standard(s) that DHS should impose.**

- AAMVA recommends adherence to 18013-5, as qualified in the AAMVA mDL Implementation Guidelines (soon to be updated and publicly published).
- The ISO process for mDL standard is open to anyone (upon joining the domestic standards body; INCITS for the US), and includes world-wide participation; the use of mature technologies; and several test events confirming direction.
- AAMVA recommends its mDL Implementation Guidelines as reflective of the work of the specialized mDL working group representing AAMVA members in the US and Canada.
- Other benefits provided by ISO/IEC 18013-5:
  - The mDL holder is in total control of what data is released.
  - The mDL holder is in total control of the decision to whom to release information.
  - The mDL concept supports the idea of minimized data (e.g. are you older than 18?)
  - The mDL concept supports the idea of selective data release (i.e. only releasing some of the data elements for which the relying party asked)
  - The mDL can be implemented such that the government (state) that issued the mDL is not at all involved in the actual transaction. That is, by technical design the government (issuing state) does not have any information on or control over actual use of the mDL.
  - The mDL is underwritten (actually cryptographically signed) by the government (issuing state), a trusted party.
  - The solution is implemented by a mature and working protocol (as demonstrated by multiple interoperability events).
  - The technical solution can be used for other mobile documents as well. Existing initiatives use ISO/IEC 18013-5 (with adaptations only to the data elements stored) for vehicle title and registration certificates, and for vaccination certificates.

4. ***Industry Standard ISO/IEC 18013-5: Communication Interfaces Between mDL Device and Federal Agency, and Federal Agency and DMV.*** **DHS may adopt certain requirements that may be established in forthcoming international industry standards that specify digital security mechanisms and protocols with respect to the communication interface between a mobile device and a Federal agency, and the communication interface between a Federal agency and a DMV.**

a. Provide comments on what concerns commenters have regarding such standards and DHS's adoption of their requirements. In particular, explain whether commenters believe the current drafts of industry standard ISO/IEC 18013-5 are mature enough to support secure and widespread deployment of mDLs.

AAMVA is not aware of any concerns. Test events have confirmed the direction of the standard and the use of the technologies employed. Contributors to ISO/IEC 18013-5 represent experts from a broad spectrum of interested parties. Participation was (and is) open to anyone wanting to join (via their domestic standards body; INCITS in the US). And ISO/IEC 18013-5 comprises both a data model and an interface standard.

However, a critical, and missing component of a rollout solution is a trusted manner to obtain public keys. This challenge is not unique to the utilization of 18013-5. The same challenge would be present in use of any other standard as well. In response, AAMVA is launching an initiative to collect and disseminate public keys; expected to be available in mid 2022. This initiative, called the “digital trust service” (DTS), is a cornerstone to the successful rollout of an mDL program, and could serve DHS well in authenticating REAL ID compliant credentials. Once this initiative is operational, AAMVA recommends that DHS require issuing authorities to provide their public keys to the DTS.

b. Explain the impact on stakeholders and mDL issuance if such standards are not approved in a timely manner.

Not adhering to the standard could lead to fragmentation of the market, a decrease in trust, non-interoperable solutions, and a global diminishing benefit of the mDL concept. Standard ISO/IEC 18013-5 is expected to be available by the fourth quarter of 2021.

c. Quantify the initial and ongoing costs to a stakeholder to implement these standards.

With the expectation that mDL issuance remains optional, cost shouldn't be a consideration for inclusion in the regulations, though it does reinforce the important voluntary nature of mDL issuance.

While AAMVA defers to the cost estimates from the jurisdictions that have implemented or are currently implementing mDL solutions, AAMVA and its members have expressed that it would be beneficial to implementing states if DHS provided grant funding for issuing authorities for solution implementation and ongoing support costs related to authentication for federal purposes.

d. Provide comments on what, if any, key areas related to mDLs are not covered in these standards that DHS should consider addressing by regulation.

AAMVA notes that interoperability is fully addressed in ISO/IEC 18013-5.

An additional operational component to consider is the establishment of a trusted public key administration initiative. As noted elsewhere, AAMVA is launching an initiative to collect and disseminate public keys that is expected to be available by 2022.

e. Identity what, if any, alternative standards or requirements DHS should consider.

AAMVA believes ISO/IEC 18013-5 provides a complete data model and communication interface description, with support for offline operation, and that it is the only standard to do so at this time.

5. *Industry Standard ISO/IEC 23220-3: Communication Interface Between DMV and mDL Device.* DHS understands that forthcoming international industry standard ISO/IEC 23220-3 may specify digital security mechanisms and protocols with respect to the communication interface between a DMV and a mobile device, specifically concerning provisioning methods, data storage, and related actions. Although DHS may seek to adopt certain requirements anticipated to appear in this standard, the Department understands that this standard may not be finalized for several years.

AAMVA provides the following general comments to the question, given the context of a Day 1 solution (where the relying party confirms the match between the authenticated data and the mDL presenter):

- The communication interface should have limited impact on DHS' need for a secure document. Key management and the creation of the MSO is a more important element of the trust chain. As previously noted, DHS could utilize the existing REAL ID security plan to provide a forum where issuing authorities could explain their technical and operational provisioning process to REAL ID in a compartmentalized fashion. AAMVA again notes that this process should not be mandated given the voluntary nature of pursuing an mDL solution.

- Day 1 solutions have been designed to minimize verifier dependence on the mDL device. As long as the document can be authenticated, the projected risk is similar to today's risk associated with physical cards.

a. Explain whether commenters believe the current drafts of standard ISO/IEC 23220-3 are mature enough to support secure and widespread deployment of mDLs.

Though standard ISO/IEC 23220-3 (which addresses putting a mDL on the right device in a secure manner) is under development, the need for a mature provisioning standard shouldn't affect widespread deployment. An issuing authority's key administration practices and MSO creation process (making sure the traditional identification data and driving privilege information is correct) would be much more important than the process of loading mDL data onto a device.

b. With the ongoing development of ISO/IEC 23220-3, provide comments on what, if any, alternative standards or requirements DHS should consider before the standard is finalized.

Since provisioning does not directly (or arguably indirectly) affect DHS, DHS should not set requirements in this area. As previously mentioned, should DHS need insight into an issuing authority's technical and operational provisioning process, the state submitted security plan could provide an avenue for additional information.

6. *Provisioning.* DHS understands that provisioning may be conducted in-person, remotely, or via other methods.

AAMVA encourages the Department to be very clear in distinguishing between provisioning and identity proofing. Generally, the risk posed by provisioning to relying parties in the attended solution is minimal. The relying party concerns should be on the private key administration (root and document signer) and the creation of the MSO.

a. Explain the security and privacy risks, from the perspective of any stakeholder, presented by in-person, remote, or other provisioning methods.

The primary risk is that the mDL is provisioned onto a device other than the one the actual mDL holder wants it to be provisioned to. This concern represents a privacy risk for the mDL holder, but does not represent a risk for the relying party. This same risk exists today for an unintended person using a stolen physical identity credential. This risk exists for both cases cited by DHS, but is elevated in remote provisioning (over in-person provisioning.)

b. Provide comments on the security protocols that would be required for DMVs to mitigate security and privacy risks presented by in-person, remote, or other provisioning methods, and to ensure at a high level of certainty that a REAL ID compliant mDL is securely provisioned to the rightful owner of the identity and the target mDL device, for in-person or remote applications.

AAMVA offers that this could be voluntarily addressed by each state in its separately detailed Security Plan. For the reasons noted previously, DHS should not prescribe additional requirements via regulation, but could utilize the tools already in place to satisfy voluntary mDL security concerns via communications in an already established channel.

AAMVA members have separately expressed that for remote provisioning, the process should contain 2 out of three of the following – something you know (though there is a need to guard against question limitations), something you have, and something you are.

Additionally, the potential use of 3rd party verifiers could enhance security, with the understanding that remote provisioning may not be the ideal solution for all instances.

c. Provide comments on whether mDL Data should include data fields populated with information concerning the method of provisioning used.

For Day 1 solutions (where the relying party confirms the match between the authenticated data and the mDL presenter), the method of provisioning isn't important for the chain of trust. The onboarding process for the proposed "digital trust service" (DTS) will include minimum, publicly known, requirements for key management.

Given that the relying party trusts the DTS to enforce these requirements, this should be sufficient for the relying party to trust the key management of the issuing authority.

d. Provide estimated costs for a DMV to implement in-person or remote provisioning. Costs may include IT contracts, hiring full or part-time IT staff, as well as software and hardware.

AAMVA defers to its state member expertise in these matters as they have direct experience.

7. *Storage.* DHS understands that mobile device hardware- and software-based security architectures can be used to secure mDL Data on a mobile device.

a. Provide comments on the advantages and disadvantages, with respect to security, functionality, and interoperability, of the different mobile security architectures for protecting, storing and assuring integrity of mDL Data.

The storage medium/method is not part of the trust chain for Day 1 solutions (where the relying party confirms the match between the authenticated data and the mDL presenter). The process of making sure that the verifier trusts that the public key has been properly created and maintained by the issuing authority is the more important aspect of the trust chain.

b. Explain whether a hardware- or software-based solution, or both, would provide the requisite security in a competitively-neutral manner.

As noted above, the storage medium/method is not part of the trust chain for Day 1 solutions. The process of making sure that the verifier trusts that the public key has been properly created and maintained by the issuing authority is a more important part of the trust chain.

8. *Data Freshness.* Provide comments regarding whether and to what extent security risks concerning data validity and freshness can be mitigated by defining the frequency by which mDL Data should synchronize with its DMV database.

a. Provide comments regarding what data synchronization periods commenters believe are appropriate for mDL transactions. Explain the advantages and disadvantages of a longer or shorter periods.

Per previous comment, AAMVA (via its mDL working group) has suggested 30 days until such time as more operational data is available, at which time this metric should be reassessed based on implementation experience. Generally speaking, a shorter period minimizes the risk posed by a scenario where all of the following happen together:

- A state makes an update in their system, e.g. by revoking a person’s driving privileges;
- The state that is unable to push that update to the mDL (e.g. because the capability exists but the device was taken offline, or because the capability does not exist); and
- The missed update affects the relying party. For example, a missing change in driving privileges will not affect the use of the mDL for the holder to prove identity. Likewise, a missing change in last name or address will not affect the validity of driving privileges.

A shorter period requires a larger capacity in the provisioning system (meaning more frequent updates). However, any update frequency shorter than the validity periods associated with physical credentials (typically 5 to 7 years) should be considered a risk improvement.

b. Provide estimated costs to a stakeholder to implement the data synchronization periods stated above.

AAMVA again defers to the expertise of its member jurisdictions.

9. *IT Security Infrastructure.* Provide comments on whether IT security infrastructure, such as Public Key Infrastructure, would provide the level of privacy and security sufficient to implement a secure and trusted

operating environment, for both offline and online use cases, and if not, explain what alternative approaches would be better.

AAMVA suggests the true question should be whether a particular implementation of the IT security infrastructure will be sufficient. The IT security infrastructure required to make a mDL work is one that will adequately protect the generation, use and distribution of public-private key pairs.

a. Identify any additional or alternative IT security infrastructure (*e.g.,* a public key distributor or aggregator such as a trusted public certificate list, Federal PKI) that would be required to facilitate trusted mDL transactions between mDL holders, verifying entities, and issuing authorities.

AAMVA believe that DHS should set requirements for how public/private key pairs are administered by states.

ISO/IEC 18013-5 recommends the use of a VICAL (master list) to collect keys from states, and to act as a single point of trust for relying parties. AAMVA is about to pilot a basic version of such a solution.

It is important that states be allowed to issue and administer their own public-private key pairs. The idea of utilizing one central key issuer poses the following undesirable properties:

- Infringement on state sovereignty. An IACA root is the key under which the issuing authority mDLs are signed. It is important for states to stay sovereign by allowing them to issue their own IACA root so that they maintain complete control of their certificate. No authority outside the state should be able to revoke or modify a state's IACA root.
- Relying parties cannot use public key certificates to control which issuing authorities credentials it trusts. (Even though a CA may trust the issuing authority, a particular relying party may have policies to not accept that issuing authority's credentials.)

b. Provide estimated costs for a DMV or Federal agency to implement necessary IT security infrastructure. Costs may include IT contracts, hiring full or part-time IT staff, as well as software and hardware.

AAMVA defers to its member jurisdictions to provide cost estimates.

10. *Alternative IT Security Solutions.* Provide comments on whether DHS should consider privacy or security solutions adopted in other industries, such as finance (*e.g.,* mobile payments), automotive/telecommunications (*e.g.,* vehicle-to-vehicle or "V2V"/"V2X" communications), or medical (*e.g.,* electronic prescriptions for controlled substances), that rely on digital identity and/or secure device-to-device transactions. Explain what those solutions are and how they could be adapted or implemented for Federal mDL use cases.

AAMVA is not aware of any other solution that provides all the following advantages offered by 18013-5. Those advantages include:

- Complete and secure device-to-device protocol (supporting multiple technologies), confirmed via multiple test events.
- A defined data model that has built in features supporting data minimization (e.g. "Are you older than 21?").
- Explicit support for the mDL holder to respond selectively (i.e. to allow the release of only some of the data elements requested).
- A requirement for the relying part to indicate, for each data element requested, whether the information will be retained or not.
- Scalability to support other document types.

- Will always work offline (i.e. when neither the mDL device nor the relying party device have a network connection), with the option for an issuer to also provide a method to retrieve mDL information (released by a mDL holder) directly from the issuer in real time.
- Does not require the relying part to place trust in the mDL device outside the requirement to ensure the public key from the device matches the device public key in the MSO.

11. *Offline and Online Data Transfer Modes.* DHS understands that mDL Data may be transferred to a Federal agency via offline and online modes.

a. Explain the security and privacy risks, from the perspective of any stakeholder, presented by both offline and online data transfer modes.

There are privacy and security risks pertinent to both to include:

1. Sharing more information than is needed.
2. Not being in control of information after it has been shared.

For device retrieval there are no additional risks pertaining only to device retrieval. However, server retrieval includes one additional privacy risk, in that it allows the issuing authority to be aware of each use of a mDL by its holder, and of which data was shared. (The protocol does not convey information to the issuer about who the relying party is or where the mDL is being read.)

Given this additional concern, AAMVA is of the opinion that it is very important for DHS not to require states to support server retrieval.

b. Provide comments on the security protocols that would be required to mitigate security and privacy risks presented by both offline and online data transfer modes.

ISO/IEC 18013-5 requires a mDL to support device retrieval and allows issuers to decide if they want to support server retrieval. AAMVA recommends DHS adhere to this aspect of the standard. Requiring server retrieval would force states to have more information about a citizen than necessary. It could also place additional administrative and cost burdens on states to institute mitigation measures.

12. *Unattended Online mDL Verification.* Provide comments on what capabilities or technologies are available to enable unattended online mDL verification by Federal agencies. Explain the possible advantages and disadvantages of each approach.

a. Explain the security and privacy risks, from the perspective of any stakeholder, presented by unattended online mDL verification.

There are three major risks for unattended online use of the mDL:

1. If the verifier is responsible for properly matching the person and the data, it is very difficult to do so.
2. If the issuing authority is responsible for matching the data the question becomes is the process good enough.
3. For the mDL holder, the risk is that the relying party is not who the holder thinks they are.

Currently the risks are high given that the ISO/IEC 18013-5 standard requirements for unattended use (Day 2, where the issuing authority takes responsibility for matching the person to the mDL at transaction time) are still being developed. Until such a time that the standard matures, there is not a standard approach for how to securely transact online.

b. Provide comments on the security protocols that would be required for DMVs to mitigate security and privacy risks presented by unattended online mDL verification.

ISO is currently working on solutions to mitigate the security and privacy risks mentioned above.

13. *Costs to Individuals.* Provide comments on the estimated costs, including savings, to an individual to obtain an mDL,

AAMVA again defers any comment on costs associated with mDL implementation to its state members.

14. *Considerations for mDL Devices Other than Smartphones.* Provide comments on whether provisioning an mDL on, or accessing an mDL from, a device other than a smartphone (*e.g.,* a smartwatch accessing mDL Data from a smartphone paired to it, or a mobile device authorized to access mDL Data stored remotely), poses security or privacy considerations different than provisioning an mDL on, or accessing an mDL from, a smartphone. Explain such security or privacy considerations and how they can be mitigated.

There are a variety of devices and device combinations leading to many different levels of security and privacy considerations. If the issuing authority decides that a particular device or device combination provides adequate features, that should be good enough. As noted earlier, the device should not matter to the relying party.

15. *Obstacles to mDL Acceptance.* Describe any obstacles to public or industry acceptance of mDLs that DHS should consider in developing its regulatory requirements. Provide comments on recommendations DHS should consider addressing such obstacles, including how to educate the public about security and privacy aspects of digital identity and mDLs.

- DHS should ensure that federal entities have the means to transact with standards compliant mDL solutions (to include devices, apps, and education).
- Funding to issuing authorities to implement interoperable solutions.
- Funding to help establish a Digital Trust Service (DTS). This service is instrumental in the ability to consistently rely on any mDL credential.
- Interoperability domestically and internationally.
- Foreign mDL interoperability and trust.
- Careful consideration of how “flash pass” presentations of a credential could impact the long-term proliferation, trust, and acceptance of mDL as a model. A “flash pass” is the act of showing a digital representation of a driver’s license or ID on a mobile device. Acceptance of a flash pass could reduce trust in mDL as a concept and inhibit the proliferation of mDLs. Flash passes are not supported by the ISO standard nor the AAMVA Implementation Guidelines.

AAMVA thanks the Department for its important work in pursuing digital identity solutions. Undoubtedly, digital identity solutions represent the future of credentialing and represent numerous potential improvements over the current physical credential. AAMVA stands ready to partner with its membership, its associate partners, the Department, and all stakeholders to find effective solutions to building identity ecosystems appropriate for the information age.

Cian Cashin
AAMVA Director of Government Affairs
ccashin@aamva.org