MOBILE DRIVER'S LICENSE

FUNCTIONAL NEEDS WHITE PAPER

0.7

Document Version

American Association of Motor Vehicle Administrators

This White Paper discusses functional needs for and practical considerations associated with a mobile driver's license solution.

The American Association of Motor Vehicle Administrators (AAMVA) is a nonprofit organization, representing the state and provincial officials in the United States and Canada who administer and enforce motor vehicle laws.

American Association of Motor Vehicle Administrators

Address AAMVA

4401 Wilson Boulevard
Suite 700
Arlington, Virginia 22203

Telephone 1-703-522-4200

Fax 1-703-522-1553

Website http://www.aamva.org

CONTENTS

TERMS, DEFINITIONS AND ABBREVIATIONS

Term	Abbre-viation	Explanation / Notes
Card Design Standard	CDS	
carrier		The digital medium on which a mDL resides.
consumer		An entity that uses a DL (or mDL), e.g. to confirm the identity of the DL (or mDL) holder, or to confirm driving privileges. In this draft of this White Paper a consumer is a person. In the case of a mDL the consumer could however also be a system.
mobile driver's license	mDL	A driver's license stored on or accessed via a device such as a smart phone or tablet.
driver's license	DL	Within the context of this White Paper, the term DL refers to a document, in physical or digital form, that contains sufficient information to link the document to the document holder, and which optionally conveys other information about the document holder such as driving privileges. Examples include traditional driver's license cards, identification cards, and non-CDL driving permits.
driver's license holder	DL holder	
near field communication	NFC	
personally identifiable information	PII	
personal identification number	PIN	
physical DL		A traditional DL, e.g. a credential issued in compliance with ISO/IEC 18013-1.
law enforcement	LE	

1 INTRODUCTION

The topic of "putting a driver's license on a cellphone" has enjoyed much attention in the press recently. Various initiatives are being undertaken in this area. At this time most appear to be proof-of-concept or exploratory in nature. Interest is being expressed by a variety of stakeholders, including driver's license administrators, legislators, vendors, and the general public.

This document is a product of the AAMVA Card Design Standard (CDS) committee[1], supported by the AAMVA Electronic Identity (eID) WG[2]. This document presents these committees' current understanding of the conceptual framework and functional requirements associated with a "driver's license on a cellphone", or mobile driver's license (mDL). This document also explores ancillary topics stakeholders may want to consider in connection with mDLs.

A White Paper states requirements, but also formulates questions (without providing answers) on issues that require further investigation, analysis and discussion. This document can be considered to be a White Paper. That is, this document is by no means the definitive and final word on mDL functional requirements. It is fully recognized that this topic will likely see significant growth in the months and years to come. Consequently this document intends to serve as a basis for further discussion, investigation and research.

[1] The CDS committee is responsible for enhancing interoperability between issuing authorities in respect of, among other things, driver's licenses. The CDS committee also strives to present the AAMVA community's point of view within other organizations, including standards organizations.

[2] The eID WG has been charged with the review and potential leveraging of existing identity credential standards, and to recommend standards to the AAMVA membership relating to the emergence and rising popularity of electronic identity. In wanting to further flesh out their work and to show how eID concepts can be operationalized, the WG is now assisting with the standardization guidance for a MDL.

2 FUNCTIONAL NEEDS

2.1 FUNCTIONAL REQUIREMENT SUMMARY

Today, a DL is used for the following two primary goals:

1. Confirm identity.
2. Convey driving privileges. (This also requires confirmation of identity.)

For a physical DL to fulfil these goals, it has to comply with all of the following:

1. Contain sufficient information to tie the physical DL holder to the physical DL.
2. Convey driving privileges granted to the physical DL holder.
3. Be trusted. That is, the physical DL consumer must establish an appropriate level of confidence that:
    a. The DL was issued by the claimed issuing authority, and
    b. The information conveyed by the DL has not changed since it was issued (unless updated by the issuing authority).

The traditional physical DL in Figure 1 complies by virtue of the following:

1. It conveys driving privileges granted to the DL holder.
2. It contains a portrait image to visually tie the DL holder to DL.
3. The security features are intact and matches the features expected on the driver's license, thus enabling the DL consumer to establish within a reasonable level of confidence that:
    a. The DL was issued by the claimed issuing authority (the State of Virginia in this case), and
    b. The information conveyed by the DL has not changed since it was issued.

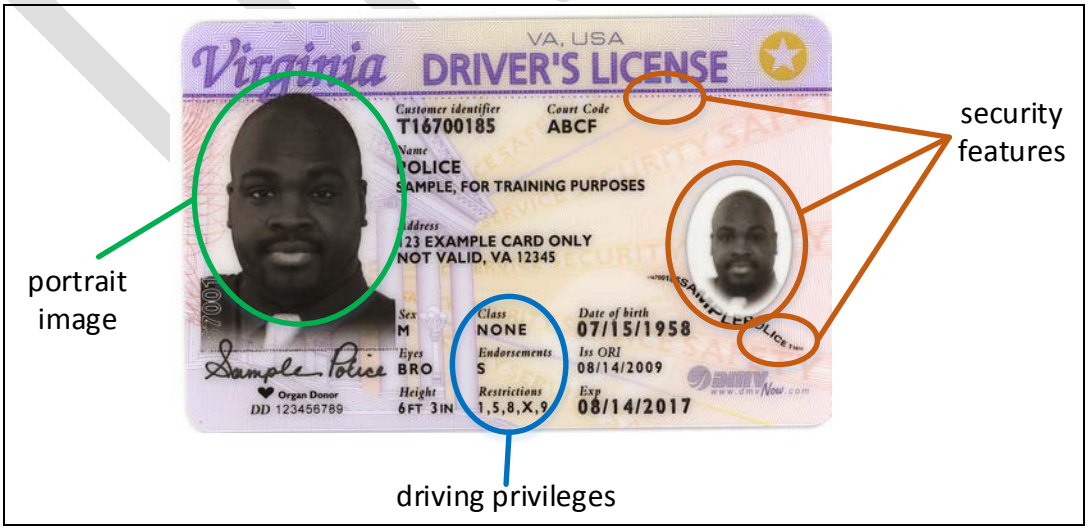

Figure 1: Traditional driving license example

A mobile driver's license (mDL) is a digital representation of the information contained in a physical DL, stored on or accessed with the help of a device (owned and controlled by the DL holder) such as a cell phone or tablet[3]. The primary goals of a mDL however remain to confirm identity and to convey driving privileges. These are not the only goals though. The differences between a physical DL and a mDL lead to additional requirements. The CDS committee and the eID WG identified the following goals and or properties that are required for a mDL:

1. Capable of functioning in an off-line environment.
2. Include mechanisms or comprise of an architecture that allows a mDL consumer to establish trust in the information provided by the mDL.
3. Confirm the mDL holder's identity.
4. Convey driving privileges.
5. Allow reading of the information across issuing authorities.
6. Allow the mDL holder to selectively authorize the release of information.
7. Support remote mDL management.
8. Easy to use.
9. Acceptable processing time.

These requirements are discussed in more detail in the sections that follow.

2.2 OFFLINE OPERATION

It should be possible to read the mDL and to authenticate the issuing authority and integrity without the presence of a real time communication link from the reader to another system. This is referred to as off-line operation. Off-line operation can be divided into the following scenarios:

1. Reader is off-line
2. mDL is off-line

For each of these, the device can be always off-line (after initiation), or intermittently off-line, or never off-line. This is presented in Table 1.

[3] It would be possible to devise a mDL solution that resides on a fob (i.e. a stand-alone chip). For purposes of this White Paper though a mDL is assumed to involve a device that allows user input.

Table 1: Off-line scenarios

Device	Scenario	Probability & Notes
mDL	Always off-line (after initiation)	Possible. A mDL solution has to support this condition.
	Sometimes off-line	Possible.
	Always on-line	Default.
Reader	Always off-line (after initiation)	Unlikely. A mDL solution does not have to support this condition. It is considered likely that any reader will have periodic connectivity.
	Sometimes off-line	Possible.
	Always on-line	Default.

Table 1 implies the following:

1. For most verification actions, both the mDL and the reader will be on-line.
2. For some verification actions, either the mDL or the reader will be off-line, or both the mDL and reader will be off-line.
3. It can be assumed that a reader will from time to time have connectivity.
4. A mDL solution should support a mDL that does not have connectivity beyond the point at which it is created/initiated.

It is recognized that off-line use may not provide all the functions available during on-line use. At a minimum though, off-line use must enable the mDL consumer to confirm a mDL holder's identity and driving privileges, with an acceptable level of confidence.

Given the above, **this document assumes that the mDL solution will store sufficient information on a mDL holder's mobile device to satisfy the goals of a DL**.

It is realized that a requirement for off-line operation narrows the mDL solution space. However, off-line operation is expected to remain a requirement for the foreseeable future.

2.3 TRUST ESTABLISHMENT

In order to trust a mDL, the mDL consumer must establish with an appropriate level of confidence that:

1. The information comprising the mDL was issued by the claimed issuing authority; and
2. The information has not changed since it was issued (unless updated by the issuing authority).

In the physical domain, a DL consumer typically establishes trust in a DL based on an assessment of the DL's visual and tactile security features (mostly human discernible features, but on occasion also using simple equipment). It is also possible to validate the authenticity of a physical DL using automated solutions, e.g. via passive (or active) authentication of machine-readable data and subsequent comparison with the human-readable data. Such solutions are not currently common.

Trust in a mDL cannot be established by a consumer by using his/her sense of touch, or by using his/her sense of sight alone. **An additional component, trusted by the consumer, is required to do this.** This document refers to this additional component as a reader.

At a high level, the process can be described as follows:

1. The mDL consumer trusts the reader.
2. The reader obtains information from the mDL.
3. The reader authenticates the information and passes it along to the mDL consumer.

Possible (logical) solutions include, but are not limited to:

- The mDL consumer uses an imaging reader to read an image (e.g. of a 2D barcode) being displayed on a cell phone, and uses digital watermark technology to confirm the authenticity and integrity of the 2D image (and by extension of the mDL contained within the barcode).
- The mDL consumer uses a near field communication (NFC) reader to retrieve a mDL from a cell phone, and then uses passive authentication to confirm authenticity and integrity of the mDL.
- The mDL consumer uses a reader and active authentication to communicate with and authenticate a contactless integrated circuit in the carrier, and to retrieve only the information supported by the active authentication digital certificate on the reader.
- A mDL (that supports offline operation) determines that a real time communication link is available. Instead of exchanging PII with the reader, it obtains a one-time token from the issuing jurisdiction which it then shares with the reader, e.g. via barcode. The reader submits the token to the issuing jurisdiction, which then responds with the information originally requested by the mDL holder to be released.

On a side note, it is anticipated that the process of establishing trust in a mDL will, in most operational cases, yield a much more definitive outcome than is the case with physical cards today.

2.4 IDENTITY CONFIRMATION

2.4.1 General requirements

Identity confirmation has as goal to confirm that a mDL "belongs to" the holder of the mDL, that is, that the person whose face (or biometric) and biographic details appear in the mDL is the person presenting the mDL for consumption.

At a minimum, this link must be established using visual comparison, by the mDL consumer, of the portrait image contained in the mDL with the mDL holder.

Other solutions that use biometric methods must not require the mDL consumer to be a biometrics expert, or to undergo training in the use of the biometric.

Any solution that requires visual comparison between the mDL holder and the portrait image by the mDL consumer must allow the mDL consumer to view the portrait image and mDL holder at the same time. With a physical DL, a DL consumer typically compares the portrait image to the DL holder by shifting his/her view between the card and the person. To support the same approach in case of a mDL, the portrait image displayed on the reading equipment should be visible to the DL consumer such that the DL consumer can easily switch his/her gaze between the image and the person.

The sections that follow reflect additional considerations regarding specific ways in which a mDL can be linked to a mDL holder.

Note 1: In the case of a physical DL, the link between the DL and the license holder is established via visual comparison (by a DL consumer) of the portrait image with the person presenting the DL (the customer). In the case of a mDL, it is expected that at least in initial solutions this will remain the primary means of linking the mDL to the mDL holder.

Note 2: Given the prevalence of e.g. fingerprint readers on mobile devices, other solutions are anticipated too. However, since such solutions must not require the consumer to be a biometric expert, visual interpretation of the portrait image is expected to remain an important part of the process.

2.4.2 Portrait image

Given the requirements above, the following implications apply to the use of the portrait image to link a mDL to a mDL holder:

1. The mDL has to include the mDL holder's portrait image. Optionally, if real time communication is available, the solution may also retrieve the image from the issuing jurisdiction.
2. Reading equipment is required to read the portrait image from the mDL (or to retrieve it from the issuing jurisdiction), and to display the image. The following are logical examples of readers:
    a. A mDL resides on a mDL holder's cell phone. The cell phone serves as a reader and displays the portrait image on the cell phone's screen.
    b. A mDL resides on a mDL holder's cell phone. The mDL is retrieved from the cell phone using a separate reader and NFC technology. The portrait image is displayed on the reader's screen.
3. To support the portrait image and the mDL holder being visible to the mDL consumer at the same time, many use cases (e.g. roadside LE) will require the reader to be mobile.
4. As illustrated in example 2.a above, it is possible for the reading equipment to also serve as the carrier (the mDL holder's cell phone in this case). In this case the portrait image contained in the mDL on the cell phone will be displayed on the same cell phone. The following items are relevant to such an approach:
    a. Since the reader is not under control of the mDL consumer, additional means are required to establish the trust in the mDL (see Section 2.3).
    b. Liability issues arise when the mDL consumer is required to physically handle the carrier.
    c. Consider a case where the mDL consumer does not physically handle the cell phone and has to rely on the image displayed on the carrier to link the mDL carrier to the mDL. Even if trust in the mDL has been established (see Section 2.2), this case operationally compares to trying to link a physical card to a card holder while the card holder does not hand over the card to the card consumer but just "flashes" the card.

2.4.3 Biometric

Given the general requirements listed in Section 2.4.1, use of a biometric to link the mDL to the mDL holder has the following implications:

1. Reading equipment is required to read the biometric from the mDL, or optionally to retrieve the biometric from the issuing jurisdiction if real time communication is available.
2. Equipment is needed to obtain the mDL holder's biometric.

3. A 1:1 comparison of the mDL biometric and the mDL holder's biometric needs to be performed. For most applications, this has to be a real time action.
4. The reading equipment (both for reading the mDL and the mDL holder's biometric) should be under the control of the DL consumer.
5. Unless the biometric does not result in false positive or false negative outcomes, the solution should support the visual comparison of the portrait image with the mDL holder to resolve such cases.

2.4.4 PIN

Yet another means that has been suggested to link a mDL to a mDL holder is via a personal identification number (PIN). The PIN is stored in the mDL in a protected manner yet such that an authentication process can take both information from the mDL and the PIN as input, and confirm if they "belong together". Concepts that apply to such a solution include the following:

1. If the PIN has been compromised (e.g. if it becomes known and is being used by someone other than the actual DL holder), this can remain undetected (unless a biometric is also used).
2. The authentication process has to be trusted by both parties (i.e. the mDL holder and the mDL consumer). For example, the mDL holder may not always be amenable to entering the PIN into a reader offered by the mDL consumer, for fear of compromising the PIN. On the other hand, the mDL consumer may not trust a solution where the authentication process resides on equipment (e.g. a cell phone) owned by the mDL holder.

2.5 CROSS-JURISDICTIONAL USE

The existence of standards such as the AAMVA Card Design Standard is a testament to the need for a DL to be used across jurisdictions. While the current AAMVA Card Design Standard addresses physical cards only, the need for interoperability extends to all forms of a DL.

Since not all issuing authorities use the same vendor, cross-jurisdictional use also implies cross-vendor use.

From a practical perspective, it makes sense to think about cross-jurisdictional use from the point of view of the mDL reader. Cross-jurisdictional use means that one mDL reader should be able to read mDLs issued by many different issuing jurisdictions.

At a high level, the mDL environment can be visualized as reflected in Figure 2.

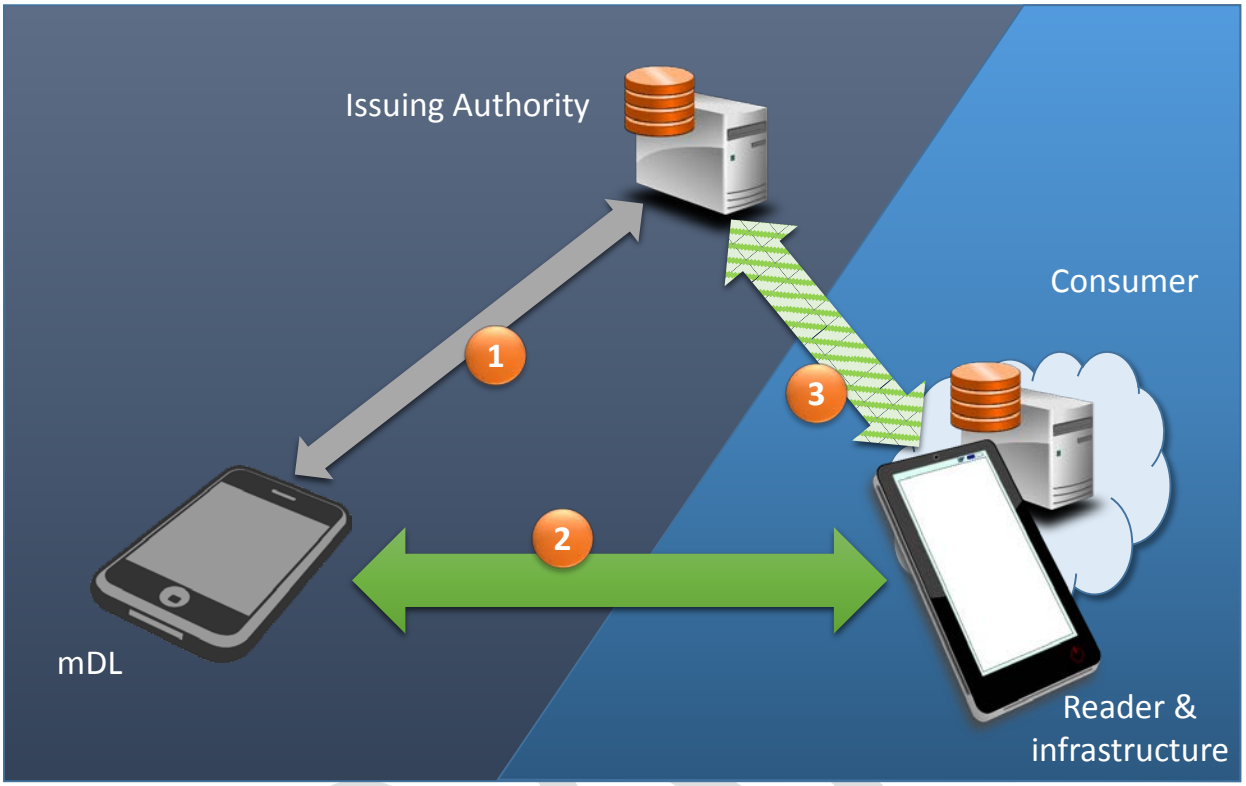

Figure 2: mDL Environment

In the diagram, the "consumer" represents any reader infrastructure not controlled by the Issuing Authority. This could for example be a bank, a store selling alcoholic beverages, or a law enforcement officer in a different jurisdiction.

In addition, the following notes apply to the numbers in Figure 2:

1. Interface between the mDL and the Issuing Authority, controlling amongst others how the mDL data is put onto the carrier and how updates are made.
2. Interface between the mDL and the reader. This is a real-time interface.
3. Interface between the Issuing Authority and the consumer . This interface facilitates the exchange of the information required to allow a reader to confirm the authenticity of mDL information. This interface is between the consumer and the Issuing Authority (either directly or via intermediaries) rather than directly between the reader and the Issuing Authority. This interface does not have to be a real-time interface. This interface may also be used by the Issuing Authority for readers under its control.

For cross-jurisdictional interoperability purposes, standards have to be established for the two green arrows in the diagram (numbers 2 and 3)[4]. While the mDL/reader interface (number 2 in the diagram) is the first

[4] To this end, AAMVA is involved heavily with ISO/IEC JTC1/SC17/WG10, a work group currently focusing on creating a mDL standard.

that comes to mind when talking about a mDL, it is important to realize that a mDL solution also has to implement the (cross-jurisdictional) Issuing Authority/consumer interface (number 3 in the diagram) in order to be of any use.

Note 1: Some of the functional requirements and other considerations discussed in this White Paper pertain to the areas to be standardized, and some do not.

Note 2: Although the mDL/Issuing Authority interaction does not directly impact cross-jurisdictional interoperability, it may help issuing authorities if this interface could be standardized. It is recognized that such a standard would have to assume a particular type of mDL implementation. It is also possible that such a standard could apply to credentials other than a mDL.

2.6 DATA PRIVACY AND PROTECTION

2.6.1 mDL holder consent and selective information release

In the case of a physical DL, the DL holder explicitly "authorizes" a DL consumer to peruse the data on the DL when handing over the DL to the consumer. A similar concept should apply to a mDL. That is, a consumer should be able to read a mDL only if the mDL holder expressly agrees to such use.

In addition, when the mDL holder is interacting with a non-official mDL consumer (e.g. a private establishment selling alcohol), the mDL holder should be able to control what data is released, and should have the option to limit the information to something about a field rather than die field itself. For example, the mDL holder should be able to release only the fact that the holder is above a certain age, rather than the actual date of birth. This concept is sometimes referred to as data minimization.

Note 1: In case of a physical DL, the DL holder does not always hand over the DL to the DL consumer. An example would be a LE officer obtaining a DL from e.g. the wallet of an unresponsive person in case of an accident. This may not be possible for a mDL any more, with consequences e.g. for organ donation.

Note 2: Because of the issue noted in Note 1, it would be possible for an issuing authority to require unrestricted access to a mDL (i.e. access without consent) in case of "justifiable need". It is expected that such access will be restricted to the mDLs issued by the issuing authority itself.

Note 3: Data minimization could lead to additional requirements being added to this document in future. One such requirement would be to prevent a mDL consumer to tie different mDL interactions back to a specific mDL (unlinkability). This could be achieved by technical, legislative or functional means. For example, at functional level an issuing authorities can prescribe different customer/mDL identifiers to be used depending on whether the interaction is for official (governmental) or non-official (private industry) purposes. At technical level, communication protocols providing the necessary protection can be devised. Legislation (e.g. similar to that controlling automated number plate recognition data) can be applied too, although this would be less failsafe than e.g. a technical solution.

2.6.2 Other data protection considerations

The mDL should allow the mDL holder to have visibility of all personal information contained in the mDL.

2.7 REMOTE MDL MANAGEMENT

2.7.1 General requirement

An issuing authority must have the capability to remotely manage a mDL, i.e. without the mDL holder visiting an office of the issuing authority. Remote management includes the following:

- Adding, updating or revoking driving privileges.
- Revoking a mDL in its entirety.
- Updating the technical solution (e.g. if the mDL comprises an app, to update the app itself).

Short of letting an mDL expire, it is logically impossible to remotely manage a mDL in an off-line scenario (i.e. where all reader terminals, and the device on which the mDL resides, do not have any communication with the issuing authority after mDL issuance). The requirement for a mDL solution to support remote management therefore assumes some level of on-line operation.

Remote management of the mDL is not restricted to the issuing authority. The mDL holder too may have a need to remotely manage the mDL. However, remote management is limited to within the "home" jurisdiction. The mDL/reader interface standard should prevent readers outside the "home" jurisdiction from updating "home" jurisdiction mDL information.

The sections that follow discuss additional considerations regarding specific remote driving privilege management scenarios.

Not all issuing authorities will have a need for all use cases discussed. In addition, the extent to which an issuing authority wants to charge for a particular service, and the means at its disposal to collect such fees from a mDL holder, may also influence its need for remote management capabilities.

Note 1: A solution that has been discussed to support remote revocation of driving privileges, or more broadly remote revocation of a mDL, especially for partly off-line solutions, is to have a mDL expire automatically unless it "checks in" with the issuing authority's systems from time to time (e.g. once every week).

Note 2: If a mDL is issued in addition to a physical DL, remotely changing the mDL can lead to a difference between the information conveyed by the physical DL and the mDL. See Section 3.6.3.

2.7.2 Revoking a mDL

Issuing authorities typically require a DL holder to hand in a prior physical card when issuing a new card. This is however not a rule, and does depend on an issuing authority's policies. (Also see Section 3.7.)

In the case of a mDL, it is possible that an issuing authority may require a mDL holder to "hand in" a prior card before issuing a new one. If that is the case, the mDL solution must support such a requirement.

When issuing a new card, some issuing authorities hand back an old physical card to a holder after applying some physical alteration to the card (e.g. punching the word VOID into the card). The need for such business processes will have to be re-evaluated when issuing a mDL.

An issuing authority may also have a need to completely revoke a mDL when fraud is suspected.

A mDL holder too may have a need to completely revoke a mDL, for example if the carrier (i.e. cell phone) is lost or stolen. It is of course possible to effect this via the issuing authority. Alternatively, a solution can be devised for a mDL holder to effect such a revocation directly, without going via the issuing authority.

2.7.3 Temporarily revoking driving privileges

In some jurisdictions, a LE officer is today under some conditions allowed to physically take possession of a person's DL even though there has been no conviction yet. Technically the DL is not revoked, but practical steps are taken to prevent the driver from legally driving until such time as the administration of the issue has run its due course.

A mDL solution should support similar actions in respect of a person holding a mDL. That is, it should be possible for a LE officer to put a mDL in a state equivalent to taking possession of a physical DL. Note that this requirement applies specifically to a LE officer in the "home" jurisdiction. It does not apply to a LE officer in a "foreign" jurisdiction.

2.7.4 Permanently revoking driving privileges

Permanent revocation of driving privileges usually follows only after due process has been followed, which often takes time. The DL holder is typically informed via official communication of the termination of privileges, and instructed to hand in or destroy the DL.

A mDL solution should support the permanent revocation of (driving) privileges associated with a mDL. In a fully on-line scenario this can likely be achieved simply by updating the mDL holder's privileges in the privilege repository. However, in a partially on-line scenario, the mDL solution should devise other means to revoke the privileges associated with a mDL. (Although many solutions may exist, one that has been mentioned is to set the mDL up such that it has to communicate with a central system from time to time or expire, and that it "self-adjusts" based on instructions received back from the central system.)

2.7.5 Adding driving privileges

A need to add driving privileges can occur when e.g. a commercial driver that has been granted the privilege to drive a class B commercial vehicle qualifies to drive a class A vehicle. In such cases though it is likely that the DL holder will visit an issuing authority office. The concept of "remote" management of a mDL in this case therefor is very similar to cancelling a prior mDL when issuing a new mDL.

2.7.6 Changing from a DL to an ID card

When changing from an ID card to a DL, a customer typically will visit an issuing authority office. This case therefor is similar to cancelling a prior credential and issuing a new credential. On the other hand, changing a DL into an ID card does not need a customer to visit an issuing authority office. This can happen e.g. when a person's driving privileges are revoked, but the mDL can still be used for identification purposes. This is very similar to the cases discussed in sections 2.7.3 and 2.7.4.

2.7.7 Changing devices

It is likely that a mDL holder will want to transfer the mDL from one device to another at some point. It would be desirable if the mDL holder did not have to visit an issuing authority office for this purpose.

2.8 Operational ease of use

Any mDL solution should be easy to use. More specifically, especially when compared to a physical card, a mDL solution should have the following properties:

1. Not require a consumer to physically handle the carrier when reading the mDL.
2. Not be negatively affected by sunlight intensity, rain or snow.
3. Work at any time of the day or night.
4. Operate in an office environment.
5. Be physically sufficiently robust to operate outside an office environment, e.g. when a traffic LE officer conducts a roadside traffic safety stop.
6. Minimize any additional equipment that a LE officer would have to carry to process a mDL.
7. Minimize additional equipment that private entities (e.g. vendors and the public) would require to process a mDL.

2.9 Processing time

Not all use cases are equally sensitive to time required to read and verify a mDL (the "processing time"). However, there are many examples of cases very sensitive to processing time. One such an example is the use of DLs to prove identity at airport security checkpoints. A few seconds more per individual read action may have a significant negative impact on overall wait times and/or security personnel requirements. Another example is roadside traffic LE, during which a LE officer has a need to quickly and accurately identify a driver. Non-official use too has time limitations. If using a mDL to verify age when buying alcohol is not performed in a speedy manner it most likely will not become the method of choice for this purpose.

Due to the prevalence of this and similar use cases, any mDL solution should allow a mDL to be processed and compared to the mDL holder in about the same time it would take to do this with a physical DL.

2.10 Reading infrastructure

As with any rollout, stakeholders would prefer to minimize cost. This applies to the mDL too. Especially the LE and retail industry stakeholders have already indicated that the reader infrastructure should preferably use existing equipment.

2.11 Use case examples

The following is a set of practical examples of where a driver's license (or identification card) is currently used, and consequently where a mDL may in future be used.

2.11.1 TSA

In the US, any person wishing to enter the secure area of a commercial airport has to identify him or herself. These checks are performed by the Transportation Security Administration (TSA). For domestic commercial flights, the most common means of identification is a DL.

In 2014, 761 million passengers enplaned at commercial service airports in the US. (The number was 739 million in 2013.) While the percentage that uses a DL is unknown, an estimate places this at 80%. This translates into 609 million DL verification actions by TSA in 2014.

The verification process is typically conducted in a controlled physical environment by a person who is trained in handling DLs. DLs presented can originate from any US issuing authority. DLs presented can conceivably also originate from a non-US issuing authority, although it is surmised to happen less frequently. Online operation can be expected. Processing time is important.

2.11.2 Road stop

A road or traffic stop can technically be defined as a temporary detention of a driver by police to investigate a possible violation of law. During a road stop, the law enforcement officer conducting the road stop typically tries to identify the driver of the vehicle. The obvious document used for this purpose is a DL.

According to the US Department of Justice (Bureau of Justice Statistics), there were 26 million road stops in 2011.

The verification process is typically conducted in a non-controlled physical environment by a person who is trained in handling DLs. DLs presented originate primarily from US issuing authority, although DLs from other issuing authority can be expected. Operation can be either online or offline. Processing time is important, but not as critical as e.g. in the TSA case.

2.11.3 Proof of age

In the US, the purchase of alcohol is generally restricted to persons aged 21 and older. Alcohol selling establishments are responsible for complying with such laws. This is typically performed by perusing the DL of any person appearing youngish (e.g., all persons appearing to be 25 or younger).

The total alcoholic beverage sales in the US was $211.57 billion in 2014[5]. If it is assumed that an average purchase of alcohol is $50, that implies 4.2 billion individual purchases in 2014. According to the Census Bureau, in 2014 the 20 to 24 age group made up 9.7% of the total population aged 20 and above. If it is further assumed that:

- Alcohol purchases are spread equally among persons of legal buying age;
- Only persons 25 and younger are "carded"; and
- The 20 to 24 age group is more or less the same size as the 21 to 25 age group;

then 410 million DL verification actions took place in 2014. (Although this calculation is based on several assumptions, it is considered sufficient for purposes of the discussion.)

The verification process is typically conducted in a controlled physical environment by a person who is not trained in handling DLs. DLs presented originate primarily from US issuing authority, although DLs from other issuing authority can be expected. Online operation can be expected, although offline operation is possible. Processing time is very important.

When using a physical DL, the DL consumer obtains access to all the information on a DL. In future, if a mDL were to be used, it is envisioned that the consumer will only obtain sufficient information to confirm that the mDL belongs to the person presenting it, and that the person is of legal drinking age.

[5] http://www.statista.com/statistics/207936/us-total-alcoholic-beverages-sales-since-1990/ , as on 2016-01-18.

2.11.4 Other use cases

Additional traditional use cases where a DL is used include the following:

- Car rental. In this case, a DL is used to identify the renter, as well as to provide driving privileges.
- Confirming identify in order to obtain social services.
- Confirming identity to a hotel on checking in.
- Confirming identity to financial institutions when conducting face-to-face business.
- Confirming identity in order to vote. (This is not a requirement in all jurisdictions.)
- Access control, e.g. to federal facilities. This can be seen as an extension of the TSA use case discussed earlier.

New use cases brought about by the nature of a mDL can be expected. Online use is one example. Online use can take many forms, e.g.:

- Signing documents electronically
- Improving security of other solutions/credentials on a mobile phone.

3 PRACTICAL CONSIDERATIONS

Whereas Section 2 provided high level generic functional needs, Section 3 considers practical issues and implications associated with the use of a mDL and the establishment of the associated environment.

3.1 CARRIER

In principle, the carrier on which a mDL resides is irrelevant. As was discussed in Section 2, there are logical solutions that can operate on carriers as diverse as cell phones and thumb drives. However, it is recognized that the choice of carrier can be influenced by other limitations or requirements such as reader infrastructure, authentication solution, and political needs.

3.2 MINIMUM INFORMATION

In addition to the fields specified in Data Group 1 of ISO/IEC 18013-2:2008, the portrait image must also be included in the mDL. The portrait image will be the primary means of matching the mDL holder to the mDL.

This has implications for the use of ISO/IEC 18013-2:2008, which identifies the portrait image data group as an optional data group.

3.3 READER-CARRIER INTERACTION

Due to liability concerns, it may be preferable for the interaction between the reader and carrier to not require physical contact. This is especially true where the carrier is of high value, for example in the case of a cell phone.

Various contactless communication technologies exist, each with its own properties and challenges. This White Paper does not express an opinion on the suitability of any such communication technology. It is worth noting though that the read distance will likely impact operations. Standard operating procedure to conduct a traffic stop could be very different if the read distance is 1 inch vs. 10 yards.

A mDL solution should take suitable precautions to safeguard against an attack on the reader during interaction with the mDL.

3.4 FINANCIAL CONSIDERATIONS

Financial items to consider in association with a mDL include, but are not limited to, the following:

1. Availability and deployment of a reader infrastructure, everywhere a mDL is to be consumed. Of most concern would be the infrastructure within the issuing authority, but it may also be prudent to consider the cost to other DL consumers, e.g. private industry and regular citizens.
2. Changes in office processes to support the issuing of a mDL.
3. System infrastructure to support the issuing and authentication of mDLs.
4. Outreach/education/training. For example, an issuing authority may want to consider the cost of (and funding sources for) involving industry in pilot projects.

Existing processes that generate revenue may also be impacted by a mDL solution. The extent of such an impact, how to manage that (to prevent negative effects), and creating new revenue streams should be considered.

An issuing authority may also want to keep in mind that the potential beneficiaries of a mDL solution include entities other than the issuing authority itself. Such indirect benefits may not be immediately apparent and may be challenging to quantify, but should nevertheless be part of the discussion when an issuing authority considers the implementation of a mDL solution.

3.5 LEGAL CONSIDERATIONS

It is considered likely that existing laws and agreements (at all levels of government, including local, regional, national and supra-national) will have to be updated to accommodate the use of a mDL. It can also reasonably be expected that such laws will evolve over time as the use of mDLs become more prevalent. The following are general areas to consider:

- Use for official (government) purposes within the issuing authority's jurisdiction.
- Use for commercial purposes within the issuing authority's jurisdiction. This may or may not have to be regulated.
- Use for official (government) purposes outside the issuing authority's jurisdiction. (For example, the Real ID Act may have to be amended to accommodate a mDL.)
- Use by citizens.
- Fraud definitions, and any associated penalties.

3.6 POLICY ISSUES

Policy guidance should be considered to cover the following topics. (Since the line between law and policy varies between issuing authorities, these topics may also be addressed in legislation.)

3.6.1 Inability to read or authenticate

It is likely that scenarios will be encountered where a mDL cannot be read or authenticated due to a breakdown somewhere in the process. Actions to be taken by the consumer in such cases will likely depend on (among others) where the breakdown occurs, and on whether it is possible to determine this point. Consider the following examples:

1. A reader is unsuccessful in reading a mDL from the carrier. How does the consumer establish if the reader or the carrier is at fault? What action should be taken? An appropriate course of action can of course differ depending on the use case. The action taken by a traffic LE officer at the roadside may be different from the action taken by an examiner in an issuing authority field office.
2. The mDL consumer is unable to authenticate the mDL due to technical problems within the mDL consumer's infrastructure.
3. The carrier malfunctions (e.g. a cellphone's battery dies).

4. Two issuing authorities have an existing agreement honoring each other's DLs. A mDL holder of one of the issuing authorities travels to the other issuing authority and presents a valid mDL to a LE officer. The LE officer does not have the means to read or authenticate the mDL.

One approach is to make the mDL holder responsible for the successful operation of the carrier, for the safekeeping of the mDL, and for the ability of the consumer to process a mDL. If a mDL consumer is unable to read a mDL due to a problem with the carrier or with the mDL, or if the consumer is not equipped to read the mDL, the mDL holder is treated as if it did not present a driver's license. The following items are relevant to this approach:

1. How will the mDL holder know if something is amiss with a mDL?
2. It is anticipated that, for the time being, a mDL will be an option, and that obtaining a traditional physical DL will remain mandatory. The mDL holder can then decide if he/she wants to carry both or only one of the solutions. When carrying only the mDL, the mDL holder would take responsibility for the carrier's successful operation, and accepts the risk that a DL consumer may not have the means to read the mDL.

A concern with this approach is that an inability to read a mDL may be as a result of a problem with the reader infrastructure (as opposed to a problem with the carrier or mDL), and that under operational conditions it may be difficult to determine where the problem lies. The above approach would make this the mDL holder's problem regardless.

3.6.2 Non-official use

A narrow view of official use of a mDL would be to confirm driving privileges. Any other use, including identification by non-issuing authority entities, would be non-official use under this view.

A more practical view of official use would be use by any government entity regardless of whether the goal is to confirm identity or driving privileges. Under this view, non-official use would be use by private industry or citizens. Examples include the following:

- Confirming age (for accessing age restricted services).
- Confirming identity (e.g. for banking purposes).
- Confirming driving privileges (e.g. by a car rental company).

An issuing authority may want to consider, among others, the following issues relevant to non-official use of a mDL:

- Data minimization options put at the disposal of a mDL holder.
- When a person is involved in an accident, identity information is typically exchanged between the drivers involved. This often is based on the drivers' DLs. What would the responsibilities of the drivers be if one or both present a mDL that cannot be read by the other?

3.6.3 Data privacy

It is suggested that the issuing authority carefully consider the following items, and then clearly communicate relevant policies to a mDL holder.

- Privileges/actions that any application that may reside on the carrier will have or can perform.

- What information is collected, be that when the issuing jurisdiction updates the mDL information, updates the mDL application, or when the mDL is read.

3.6.4 Difference between mDL and physical card

Differences between a mDL and a physical card can came about for a variety of different reasons. For example, if an issuing authority is able to perform remote management of a mDL, it would be possible to update the privileges associated with a mDL remotely. Until such time as the physical card gets updated with the same change, the mDL and the physical card would not be in sync.

For a consumer to become aware of a difference between a physical card and a mDL, the consumer would have to peruse both items. Since it will most likely be the physical card that contains "old" information, a difference is only likely to be detected if consumption of a physical card raises questions, and the DL holder subsequently offers a mDL to a user. Even though this may not be expected to happen often, policies should be devised to address instances where a difference between a physical card and a mDL is discovered.

3.7 Number of mDLs

3.7.1 Historical reasons for limitations

It is currently common for an issuing authority to limit a person to only one physical DL. The goal of such a requirement is to ensure that the information (and specifically information other than the expiration date) on a DL remains current.

Conceptually, information on a card can be divided into information identifying a person, and information about privileges bestowed on a person (e.g. driving privileges). Typically, information identifying a person changes less frequently than information about privileges. Also, changes in information identifying a person are most often driven by the person and would be something the DL holder would want to have updated. (The exception is where fraud is involved and the issuing authority cancels the card.) On the other hand, changes in e.g. driving privileges is something a card holder may not want to have updated, and typically is something initiated by the issuing authority.

In an on-line use case, the typical modus operandi is:

1. Verify identity (with assistance from an on-line system)
2. If identity could not be verified, identify the person (using an on-line system)
3. Determine privileges (from the on-line system)

If the identifying information on the card were to be incorrect, Step 1 will fail, and Step 2 will be next. If the privilege information on the card were to be incorrect there would be no negative impact since the privilege information is not obtained from the card.

In summary: In an on-line use case holding multiple cards is not a concern.

In an off-line use case, the typical modus operandi is:

1. Confirm that the card belongs to the card holder (using a biometric, typically visual comparison between a photograph on the card and the card holder).
2. Obtain the necessary privileges (or other attributes of the person) from the card for further processing.

Obviously, it can be a problem if the a card holder's personal information or the privileges have changed since the particular card was issued. That is, not presenting the most recent card in an off-line use environment poses problems.

In short: Limiting a person to a single card has most applicability in an off-line use case.

3.7.2 Policy/solution options

As discussed in Section 3.6.1, it is possible (and currently considered highly likely) that a mDL will augment rather than replace a physical card. It is also logically possible and operationally desirable that a mDL holder be allowed to maintain multiple instances of the same mDL (e.g. on a mobile phone and on a tablet). Conceptually this would provide the DL holder with more than one DL.

For argument's sake, consider the following two different approaches to this issue:

1. Tie the mDL(s) to a physical document. That is, the mDL logically is incomplete without the existence of a specific physical card. Implications of such an approach include:
    a. A re-issuance of both the card and mDL are required if any information changes.
    b. In an on-line use case the mDL can probably be validated without the presence of the physical card.
    c. In an off-line use case, since the mDL is incomplete without the physical card, the presence of the physical card is required. Consequently, in an off-line use case the required presence of the physical card is likely to negate the benefits of having a mDL.
    d. In an off-line use case, it would not be possible to confirm if the information in the mDL (or on the associated card) is current. This is a limitation of the off-line scenario today already.
2. Relax the requirement to have only a single credential. That is, the card and the mDL would exist independently of each other. Implications of such an approach include:
    a. Having more than one physical card will be acceptable.
    b. Having more than one mDL will be acceptable.
    c. In an on-line scenario any mDL or physical card can be validated.
    d. In an off-line scenario, it would not be possible to confirm if the information in a mDL or physical card is current.

With both approaches, on-line use is not negatively impacted by a person potentially holding multiple credentials, whereas in an off-line use case a person holding more than one credential poses concerns.

3.7.3 Additional practical considerations

Practically, for most non-official uses (and probably for a good deal of official uses), the off-line use case would apply. In the off-line case, holding more than one credential would be a concern. As explained above, the specific concern would be that a credential is not current any more, and that the privileges (or even personal details) are not current any more.

Traditionally, limiting a person to only one credential was a way in which to mitigate this issue. However, this is not a failsafe approach. A customer can easily claim that a credential has been lost, get issued with a new one (with the old one getting cancelled), and still use the old one in an off-line scenario without detection.

Does this mean that limiting a person to one credential is of limited use in an off-line situation? Or, approaching the issue from the other extreme, what are the implications if a person holds an unlimited number of credentials?

Policies can probably limit the number of credentials a person holds, but realistically cannot eliminate that from happening. It is surmised then that the core issue is the effort required to obtain multiple credentials. With physical cards, the issuing authority has some control over the number of credentials held by a person, since the issuing authority is the only issuer. With a mDL not tied to a physical device, copies can be created without issuing authority involvement.

3.8 CONTINUITY PLANNING

A physical DL is typically issued with a validity period of 5 to 8 years. This paradigm will likely have to be adapted when dealing with a mobile DL. Given how fast mobile technology evolves (and become outdated/unsupported), it is considered unlikely that a mDL "issued" in year 1 will remain in the same format and on the same device until the end of year 8. Given an 8-year mDL, it is considered even more unlikely that a mDL solution designed in Year 1 of a 5 year procurement contract can still economically be supported at the end of its life (which will be 13 years later).

This has implications in a number of areas, including:

- Technical: Solutions will have to adapt much more quickly and potentially much more significantly than is the case for physical cards. This would affect not only mDLs already issued, but also issuance and reader infrastructure.
- Contractual: DL contracts for the production of physical cards typically focus on one technology and on one solution. The process and requirements associated with handing over operations from one contractor to another at the end of a contract is also fairly well understood. With an mDL, both of these issues will likely have to change significantly.
- Operational: Each time the actual solution changes or evolves, it will impact not only the issuing authority's staff, but all parties (including private entities) that consume the mDL.

3.9 OTHER USES

A mDL can potentially be used for purposes other than conveying driving privileges. For example, interaction between the mDL and a vehicle is possible. Another example would be to confirm eligibility for medical services. Other uses may evolve over time.

3.10 INITIAL LOOK AND FEEL

The initial look and feel of a mDL on a cell phone may have to have the same look and feel as a physical DL to facilitate adoption and use. On the other hand, care should be taken that such an approach does not compromise the security features of the mDL.

One solution would be that, whenever PII is displayed on a carrier, the information be rendered using basic text, and the image be shown without any "security features". This could be packaged within a standard "wrapper" that would be common for all mDLs issued by the issuing jurisdiction. The "wrapper" can then be used for branding purposes.

3.11 CUSTOMER SUPPORT

In the case of a physical DL, once the DL is produced, there is very little in the way of subsequent customer support required (except if the physical DL has to be replaced). In the case of a mDL though, pilot programs have shown that customer support is a crucial component of making a mDL implementation work. Issues pertinent to customer support include the following:

- All participants in them mDL ecosystem could potentially require support. This includes the mDL holder and consumers (including "foreign" consumers).
- Hours of operation. mDL holders may need to interact with their mDLs at any time. Support should be available accordingly.

REVISION HISTORY

Release	Date	Name	Comments
0.1	2015/05/20	AAMVA	Initial release, based on AAMVA CDS Committee thoughts
0.2	2015/05/25	AAMVA	Reflecting AAMVA CDS committee discussions on Release 0.1
0.3	2015/06/03	AAMVA	Reflecting AAMVA CDS committee comments on Release 0.2
0.4	2015/10/12	AAMVA	Reflecting AAMVA CDS committee and eID WG comments on Release 0.3 Reorganization of existing information
0.5	2015/11/20	AAMVA	Reflecting AAMVA CDS committee and eID WG comments on Release 0.4, including those made during the meeting on November 2015
0.6	2016/01/28	AAMVA	Reflecting AAMVA CDS committee and eID WG comments on Release 0.5 Clarification of off-line operation Addition of use cases Editorial updates
0.7	2016/08/03	AAMVA	Reflecting AAMVA CDS committee and eID WG comments on Release 0.6 Editorial updates Added mDL environment figure and discussion to Section 2.5 Added Section 2.6.2, and grouped this along with the prior section 2.6 under a new heading, "Data privacy and protection" In Section 2.7.1, clarified that remote management is limited to the "home" jurisdiction In Section 2.7.3, clarified that revocation is limited to the "home" jurisdiction In Section 2.8, added a new mDL property (#1) Added Section 3.6.3 Expanded Section 3.10 Added Section 3.11