AAMVA
American Association of
Motor Vehicle Administrators

Mobile Driver's License (mDL) Implementation Guidelines

Version 1.1

September 2022

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

AAMVA – Public Information

CONTENTS

TERMS AND DEFINITIONS

American Association of Motor Vehicle Administrators

AAMVA

Issuing Authority

entity legally entitled to issue driver's licenses and identification cards within a jurisdiction

Note to entry: The term “Issuing Authority” is used in this document to align with the term’s use in ISO/IEC 18013-5. The terms “Issuing Authority” and “Issuing Jurisdiction” are used interchangeably in other AAMVA documents.

mobile driver’s license

mDL

driver’s license or identification card that resides on a mobile device or requires a mobile device as part of the process to gain access to the related information

Note to entry: Adapted from ISO/IEC 18013-5

mDL app

software running on a mDL holder’s device; within the context of this document this includes a standalone app as well as a wallet type app

mdoc

document or application that resides on a mobile device or requires a mobile device as part of the process to gain access to the document or application

[Source: ISO/IEC 18013-5:2021, 3.2]

mobile security object

MSO

structured data set that enables a mDL verifier to authenticate (for both accuracy and origin) other mDL data elements received during a mDL transaction

provisioning

initial loading of mDL information into an mDL app

1 INTRODUCTION

The AAMVA Joint Mobile Driver's License (mDL) Working Group (WG) has been active around mobile identification since 2012. As the mDL evolves, the mDL WG continues to identify and address topics on which guidance to Issuing Authorities can be helpful. This document represents the bulk of the current guidance, and points to additional resources as needed.

The goal of this document is to inform and equip Issuing Authorities to achieve the following:

- Technical interoperability between different Issuing Authorities' mDL programs, i.e., an Issuing Authority being able to read an mDL issued by any other Issuing Authority.
- Trust in different Issuing Authorities' mDLs.
- Privacy preserving implementations.

It is up to Issuing Authorities to determine the extent to which the guidance in this document is followed. Nevertheless, the minimum measures deemed necessary to achieve the above are labeled as mandatory requirements in this document (i.e. "shall" or "must"). A summary of minimum measures can be found in Appendix B.

The following topics are outside the scope of this document:

1. The identity establishment, management and recordkeeping that precedes the creation of an identity credential.
2. Responsibilities of mDL verifiers.

This document leverages and expands on ISO/IEC 18013-5 (also soon to be available as INCITS/ISO/IEC 18013-5), an international mDL standard. Although ISO/IEC 18013-5 specifies an mDL solution, it was intentionally designed to support any type of mobile identity credential. ISO/IEC 18013-5, as qualified in this document, will therefore enable Issuing Authorities to issue both mobile driver's licenses and mobile identification cards. The term "mDL" as used in this document covers both credential types. Qualifications made in this document also allow for identifying an mDL as being REAL ID compliant or not, and/or as a credential issued under the Enhanced Driver's License program ("EDL"; see the AAMVA DL/ID Card Design Standard).

Additional guidance on mDL administration in the areas of legislation and procurement can be found in two other documents produced by the mDL Working Group. Those are the mDL Model Legislation, and the mDL Procurement Guidance (see the jurisdictional member area on the AAMVA website). AAMVA also conducts regular outreach to stakeholders on the topic of mDL, including town hall meetings, podcasts, and training.

It should be noted that mDL and related technologies are ever evolving. As a result, this document will continue to be updated to synchronize its content with the latest standards and practices. For this reason, readers of this document are encouraged to periodically check the AAMVA website for new versions.

2 mDL SOLUTION OVERVIEW

An mDL can be described as leveraging a mobile device to transfer (or cause to be transferred) driver's license information to an mDL verifier, who cryptographically authenticates the information using the Issuing Authority's public key. A visual rendering of a DL on a mobile device's display (and which can be misused as a "flash pass") therefore does not qualify as an mDL (also see section 8).

An mDL solution can be described in terms of the following three properties:

1. **Data retrieval method**. The **device retrieval** method (sometimes referred to as the offline model) works without outside connectivity (for both the mDL holder's device and the mDL reader) at the time the transaction takes place, thus requiring the mDL data to reside on the mDL holder's device. Under the **server retrieval** method (sometimes referred to as the online model, and not to be confused with use of an mDL in an unattended transaction setting such as over the Internet) mDL data is retrieved in real time directly from the Issuing Authority. ISO/IEC 18013-5 requires a mDL to support device retrieval, and allows a device to additionally support server retrieval.
2. **Transaction type**. An **attended** transaction is one where the mDL holder and the mDL verifier are in close proximity to each other. The engagement mechanisms currently reflected in ISO/IEC 18013-5 (QR code, NFC) were selected to support such close proximity. An **unattended** transaction is one where the mDL holder and the mDL verifier are not in close proximity, e.g. when an mDL holder wants to provide identity or proof of age to an online retailer. ISO/IEC 18013-5 does not currently support unattended transactions. However, work is ongoing to standardize a solution.
3. **Timing of (and responsibility for) matching.** This property is about the responsibility for confirming, at transaction time, that the person presenting the mDL data is the person described by the mDL data. In a **post-matched** transaction, the link between the mDL Presenter and the mDL data is made after the mDL data is shared and is performed by the mDL verifier. This happens by comparing the portrait image in the mDL with the person presenting the mDL. ISO/IEC 18013-5 supports post-matched transactions. In a **pre-matched** transaction, the link between the mDL Presenter and the mDL is made right before the mDL data is shared. Although the Issuing Authority should not be involved in real time, the Issuing Authority does take responsibility for certifying the link. The mDL verifier receives only the confirmation that the person presenting the mDL data is the person described by the shared mDL data. ISO/IEC 18013-5 does not currently support pre-matched transactions. However, work is ongoing to standardize a solution (and notably one that does not involve the Issuing Authority at transaction time).

With this as background, Figure 1 provides a high-level overview of the mDL ecosystem described in ISO/IEC 18013-5.

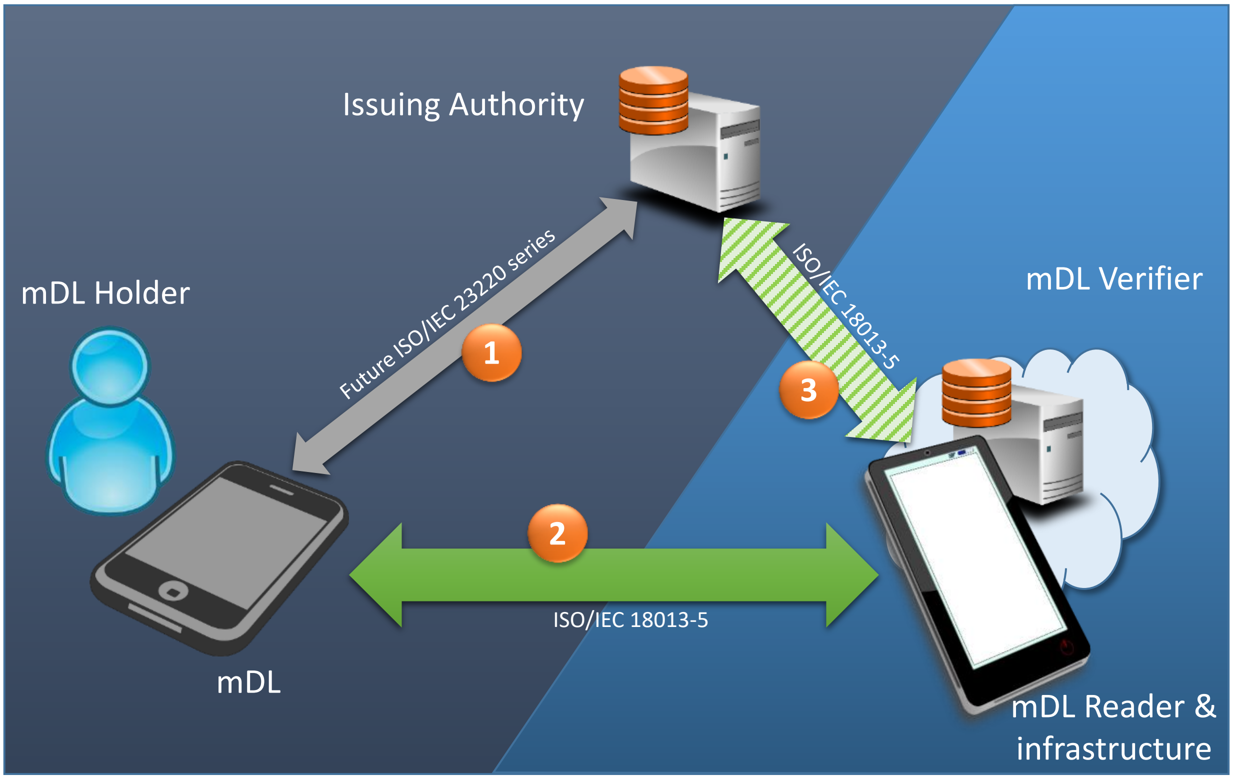

Figure 1: High level mDL ecosystem

Three interactions are involved:

1. Interaction between the Issuing Authority and the mDL. This interaction results in getting everything onto an mDL holder's device that is needed to use the mDL. There is also subsequent interaction between the Issuing Authority and the mDL to keep the mDL information updated. Technical components of this interaction will be standardized in the ISO/IEC 23220 series[1].
2. Interaction between the mDL and the mDL reader infrastructure of the mDL verifier. This interaction comprises the transfer of technical information to set up a secure communication channel between the two parties, and the subsequent exchange of the driver's license information (or of a point from where it can be retrieved) that the mDL holder agreed to share. ISO/IEC 18013-5 fully standardizes an interface describing this interaction.
3. Interaction between the mDL reader infrastructure and the Issuing Authority. This interaction can be used for different purposes, depending on the data retrieval method involved:
    a. Device retrieval method: The interaction is used by the mDL verifier to obtain the public keys needed to authenticate mDL information. Such interaction can also involve an interme-

[1] The ISO/IEC 23220 series of standards is not yet sufficiently stable for use by Issuing Authorities. This interface does however not affect interoperability between Issuing Authorities. This allows Issuing Authorities to devise their own solutions and/or to engage individually with vendors for the time being. Once available, these standards are expected to provide additional quality, cost, functionality, and privacy benefits.

diary entity that aggregates and disseminates certificates. (In North America, AAMVA's Digital Trust Service will perform this function – see section 5.) Regardless, the mDL verifier must trust that the certificate truly comes from a valid Issuing Authority. This interaction does not need to occur at the time of an mDL transaction. ISO/IEC 18013-5 fully standardizes a method supporting this interaction.

b. Server retrieval method: The interaction is used by the mDL verifier for two purposes:

   i. As in the case for the device retrieval method, to obtain the public key of the Issuing Authority.

   ii. To pass to the Issuing Authority, in real time, a token that identifies the mDL holder and the mDL, and to receive the actual mDL information back from the Issuing Authority. ISO/IEC 18013-5 fully standardizes an interface describing this interaction.

Note that ISO/IEC 18013-5 specifies system interfaces and a certificate exchange method, and on purpose does not address the user interface (e.g. the look, feel and functionality of an mDL app residing on an mDL holder's device). It is left up to Issuing Authorities (and their implementers) to innovate in this area.

3 ISO/IEC 18013-5 QUALIFICATIONS

3.1 INTRODUCTION

Issuing authorities electing to follow the guidance in this document must adhere to ISO/IEC 18013-5, including as qualified in this document.

3.2 AAMVA MDL DATA ELEMENT SET

This section specifies changes and additions to the ISO/IEC 18013-5 data element set to accommodate the unique needs of the AAMVA community[2]. All the data elements (mandatory and optional) in the ISO/IEC 18013-5 data element set, together with the changes and additions specified in this document, comprise the AAMVA mDL data element set.

The specific changes to ISO/IEC 18013-5 follow.

Replace the 1st sentence of clause 7.2.1:

> The mDL data elements shall be as defined in Table 5 belong to namespace "org.iso.18013.5.1", see 7.1.

with the following:

> The mDL data elements shall be as defined in Table 5. Data elements belong to the namespaces indicated.

In Table 5, apply the following amendments:

[2] mDL reader devices developed for use within the AAMVA community support ISO/IEC 18013-5 as published, as well as the modifications specified in this document.

Identifier	Property to amend	Old value	New value
family_name	Definition	Last name, surname, or primary identifier, of the mDL holder. The value shall only use latin1[b] characters and shall have a maximum length of 150 characters.	Family name (commonly called surname or last name), or primary identifier, of the individual that has been issued the driver license or identification document. If the individual's name is not divided into family name and given name(s), that name shall be deemed the family name or primary identifier. The value shall only use latin1[b] characters and shall have a maximum length of 150 characters.
given_name	Definition	First name(s), other name(s), or secondary identifier, of the mDL holder. The value shall only use latin1[b] characters and shall have a maximum length of 150 characters.	Given name or names (includes all of what are commonly referred to as first and middle names), or secondary identifier, of the individual that has been issued the driver license or identification document. The value shall only use latin1[b] characters and shall have a maximum length of 150 characters.
height	Presence	O	M
eye_colour	Presence	O	M
age_in_years	Presence	O	M
age_over_NN	Presence	O	M

In Table 5, add a new column titled "Namespace". For the data elements present in ISO/IEC 18013-5, enter "org.iso.18013.5.1" for each data element.

Append the following to Table 5:

Namespace	Identifier	Meaning	Definition	Presence	Encoding format
"org.iso.18013.5.1.aamva"	domestic_driving_privileges	Domestic categories of vehicles/ restrictions/ conditions	Vehicle types the license holder is authorized to operate. See 7.2.4.	M	See 7.2.4

Namespace	Identifier	Meaning	Definition	Presence	Encoding format
“org.iso.18013.5.1.aamva”	name_suffix	Name suffix	Name suffix of the individual that has been issued the credential. Only the following values are allowed: • “JR” (Junior) • “SR” (Senior) • “1ST” or “I” (First) • “2ND” or “II” (Second) • “3RD” or “III” (Third) • “4TH” or “IV” (Fourth) • “5TH” or “V” (Fifth) • “6TH" or “VI” (Sixth) • “7TH" or “VII” (Seventh) • "8TH" or “VIII” (Eighth) • “9TH" or “IX” (Ninth)	O	tstr

Namespace	Identifier	Meaning	Definition	Presence	Encoding format
org.iso.18013.5.1.aamva	audit_information	Audit information	A string of letters and/or numbers that identifies when, where, and by whom the credential was initially provisioned. The value shall only use A, N or S characters[c] and shall have a maximum length of 25 characters. Support for this identifier is not required after 2022-01-31.	O	tstr
"org.iso.18013.5.1.aamva"	organ_donor	Organ donor	An indicator that denotes whether the credential holder is an organ donor. This field is either absent or has the following value: • 1: Donor	O	uint
"org.iso.18013.5.1.aamva"	veteran	Veteran	An indicator that denotes whether the credential holder is a veteran. This field is either absent or has the following value: • 1: Veteran	O	uint

Namespace	Identifier	Meaning	Definition	Presence	Encoding format
"org.iso.18013.5.1.aamva"	aamva_version	AAMVA version number	A number identifying the version of the AAMVA mDL data element set. The number of the version described in this document is 2. Support for this identifier is not required after 2022-01-31.	M	uint
"org.iso.18013.5.1.aamva"	family_name_truncation	Family name truncation	A code that indicates whether the field has been truncated ("T"), has not been truncated ("N"), or unknown whether truncated ("U"). No other values are defined for this field.	M	tstr
"org.iso.18013.5.1.aamva"	given_name_truncation	Given name truncation	A code that indicates whether either the first name or the middle name(s) have been truncated ("T"), has not been truncated ("N"), or unknown whether truncated ("U"). No other values are defined for this field.	M	tstr

Namespace	Identifier	Meaning	Definition	Presence	Encoding format
"org.iso.18013.5.1.aamva"	aka_family_name	Alias / AKA family name	Other family name by which credential holder is known. The value shall only use A, N or S characters[c] and shall have a maximum length of 40 characters. Support for this identifier is not required after 2022-01-31.	O	tstr
"org.iso.18013.5.1.aamva"	aka_family_name.v2	Alias / AKA family name	Other family name by which credential holder is known. The value shall only use latin1[b] characters and shall have a maximum length of 150 characters. Support for this identifier is required by 2022-02-01.	O	tstr
"org.iso.18013.5.1.aamva"	aka_given_name	Alias / AKA given name	Other given name by which credential holder is known. The value shall only use A, N or S characters[c] and shall have a maximum length of 75 characters. Support for this identifier is not required after 2022-01-31.	O	tstr

Namespace	Identifier	Meaning	Definition	Presence	Encoding format
“org.iso.18013.5.1.aamva”	aka_given_name.v2	Alias / AKA given name	Other given name by which credential holder is known. The value shall only use latin1[b] characters and shall have a maximum length of 150 characters. Support for this identifier is required by 2022-02-01.	O	tstr
“org.iso.18013.5.1.aamva”	aka_suffix	Alias / AKA Suffix name	Other suffix by which credential holder is known. The same values as for Name suffix applies.	O	tstr

Namespace	Identifier	Meaning	Definition	Presence	Encoding format
org.iso.18013.5.1.aamva	weight_range	Weight range	Indicates the approximate weight range of the credential holder: 0 = up to 31 kg (up to 70 lbs.) 1 = 32 – 45 kg (71 – 100 lbs.) 2 = 46 - 59 kg (101 – 130 lbs.) 3 = 60 - 70 kg (131 – 160 lbs.) 4 = 71 - 86 kg (161 – 190 lbs.) 5 = 87 - 100 kg (191 – 220 lbs.) 6 = 101 - 113 kg (221 – 250 lbs.) 7 = 114 - 127 kg (251 – 280 lbs.) 8 = 128 – 145 kg (281 – 320 lbs.) 9 = 146+ kg (321+ lbs.)	O	uint
"org.iso.18013.5.1.aamva"	race_ethnicity	Race / ethnicity	Codes for race or ethnicity of the credential holder, as defined in AAMVA D20.	O	tstr

Namespace	Identifier	Meaning	Definition	Presence	Encoding format
"org.iso.18013.5.1.aamva"	DHS_compliance	Compliance type	DHS required field that indicates compliance. Only the following values are allowed: "F" = fully compliant "N" = non-compliant Applicable only in the US.	O[d]	tstr
"org.iso.18013.5.1.aamva"	DHS_temporary_lawful_status	Limited duration document indicator	DHS required field that denotes whether the credential holder has temporary lawful status. This field is either absent or has the following value: 1: Temporary lawful status Applicable only in the US.	O	uint
"org.iso.18013.5.1.aamva"	EDL_credential	EDL indicator	This field is either absent or has one of the following values if the credential is an EDL[e]: 1: Driver's license 2: Identification card Applicable only in the US.	O	uint

Namespace	Identifier	Meaning	Definition	Presence	Encoding format
"org.iso.18013.5.1.aamva"	resident_county	Resident county	The 3-digit county code of the county where the credential holder lives, as per the 2010 FIPS Codes for Counties and County Equivalent Entities[f]. Applicable only in the US.	O	tstr
"org.iso.18013.5.1.aamva"	hazmat_ endorsement_ expiration_date	HAZMAT endorsement expiration date	Date on which the hazardous material endorsement granted by the document is no longer valid. Applicable only in the US.	O	full-date
"org.iso.18013.5.1.aamva"	sex	Sex	Credential holder's sex, see 7.2.9	M	uint

[c] As defined in the AAMVA Card Design Standard.

[d] If the 'DHS_compliance' element is present, an mDL shall not require mdoc reader authentication as a precondition for the release of the element.

[e] Under current REAL ID legislation an enhanced driver's license (EDL) is a REAL ID compliant credential. Consequently, if the 'EDL_credential' element is present the 'DHS_compliance' element shall have a value of "F".

[f] Available at https://www.census.gov/library/reference/code-lists/ansi.html

In Table 5, the field names map to field names in the AAMVA Card Design Standard (CDS) as follow:

18013-5	**AAMVA CDS**
Licence number	Customer identifier / Customer ID number
Administrative number	Audit information

18013-5	AAMVA CDS
Sex	Cardholder sex

Domestic categories of vehicles/ restrictions/ conditions	Vehicle classifications / categories;
	Endorsements;
	Restrictions / conditions / information codes

Append the following to clause 7.2.4:

> The domestic categories of vehicles/restrictions/conditions contain information describing the driving privileges of the mDL holder.
>
> For data transfer the domestic categories of vehicles/restrictions/conditions shall have the following CDDL structure:

```
DomesticDrivingPrivileges = [
    * DomesticDrivingPrivilege
]

DomesticDrivingPrivilege = {

    ? “domestic_vehicle_class” : DomesticVehicleClass
    ? “domestic_vehicle_restrictions” : DomesticVehicleRestrictions
    ? “domestic_vehicle_endorsements” : DomesticVehicleEndorsements

}

DomesticVehicleClass = {

    “domestic_vehicle_class_code” : tstr   ; Vehicle category code as per
                                           ; issuing authority rules
    “domestic_vehicle_class_description” : tstr
                                           ; Vehicle category description as
                                           ; per issuing authority rules
    ? “issue_date” : full-date             ; Date of issue encoded as
                                           ; full-date per RFC 3339
    ? “expiry_date” : full-date            ; Date of expiry encoded as
                                           ; full-date per RFC 3339

}

DomesticVehicleRestrictions = [+ DomesticVehicleRestriction]

DomesticVehicleRestriction = {

    ? “domestic_vehicle_restriction_code” : tstr
                                           ; Restriction code as per
                                           ; issuing authority rules
    “domestic_vehicle_restriction_description” : tstr
                                           ; Vehicle restriction description as
                                           ; per issuing authority rules
}

DomesticVehicleEndorsements = [+ DomesticVehicleEndorsement]

DomesticVehicleEndorsement = {
    ? "domestic_vehicle_endorsement_code" : tstr
                                           ; Endorsement code as per
                                           ; issuing authority rules
    "domestic_vehicle_endorsement_description" : tstr
                                           ; Vehicle endorsement description as
                                           ; per issuing authority rules

}
```

Because issuing authorities must populate the standard ISO vehicle category codes in addition to populating the domestic information (rendered in the DomesticDrivingPrivileges structure), the following apply:

1. Verifying entities shall treat the DomesticDrivingPrivileges as the primary source of driving privilege information.
2. When mapping domestic vehicle privileges to the standard ISO vehicle category codes, if an exact match is not available, issuing authorities should find the closest ISO category that provides less privileges. The same approach should be followed when mapping endorsements and restrictions: Find the closest ISO rendering that provides more strict restrictions, or more restrictive endorsements. If a mapping is compiled by a vendor, the issuing authority must approve the mapping before use.
3. When an mdoc receives a request only for DrivingPrivileges, the user interface should make it clear to the mDL holder that, due to the mapping, the information shared may convey less privileges than would have been conveyed by the domestic codes.
4. When an mdoc receives a request for both DrivingPrivileges and DomesticDriving-Privileges, the mdoc shall respond (given approval by the mDL holder) at least with the DomesticDrivingPrivileges.

NOTE 3 Readers compliant with this document should ask for both DrivingPrivileges and DomesticDrivingPrivileges. This is because the reader will not know if the mdoc supports DomesticDrivingPrivileges (although in practice it often will). The intent of #4 above is to, in this case, share the domestic data the reader is looking for. How the request is presented to the mDL holder, and how approval to share is administered, is left to implementers. Nevertheless, a simple approach could be for a mdoc to ignore the request for DrivingPrivileges and to only ask for approval to share DomesticDrivingPrivileges (given that both were requested).

Note 4 The DomesticDrivingPrivileges element is a mandatory element, and consequently has to be included in the mDL equivalent of an ID card. In this case DomesticDrivingPrivileges will be empty.

Append the following to clause 7.2.5:

The issuing authority shall identify age questions that are common in its jurisdiction, and shall include in a mDL an age_over_NN statement for each of these ages for the mDL holder.

EXAMPLE 1 An issuing authority determines that mDL verifiers often need to determine if a person is at least 18 or 21, or older than 65. The issuing authority decides to only include mandatory age_over_NN statements in an mDL.

For a 20-year-old person, the issuing authority is required to include the following age_over_NN statements in the mDL:

age_over_18=True
age_over_21=False
age_over_65=False

It is recommended that an issuing authority additionally includes in an mDL age_over_NN statements for all ages between and including age$_{low}$ and age$_{high}$, where a suitably high percentage (determined by the issuing authority) of the issuing authority's mDL holders has an age within this range.

EXAMPLE 2 An issuing authority determines that mDL verifiers often need to determine if a person is at least 18 or 21, or older than 65. The issuing authority further determines that 95% of its mDL holders fall within the ages of 16 and 85, and that it wants to include age statements for all ages in this range.

For a 25-year-old person, the issuing authority is required to include the following age_over_NN statements in the mDL:

age_over_18=True
age_over_21=False
age_over_65=False

The issuing authority also includes the following age_over_NN statements, per the recommendation:

age_over_16=True
age_over_17=True
age_over_19=True
age_over_20=True
age_over_22=True
…
age_over_25=True
age_over_26=False
…
age_over_64=False
age_over_66=False
…
age_over_85=False

Add a new clause 7.2.9:

7.2.9 Sex

An additional element for sex is defined in the "org.iso.18013.5.1.aamva" namespace. In line with the AAMVA Card Design Specification, this element can have one of the following values:

- 1: Male
- 2: Female

- 9: Not specified

NOTE 1 The addition of org.iso.18013.5.1.aamva.sex is necessitated by the different meaning assigned to value 9 in the AAMVA Card Design Standard (i.e. "not specified") compared to in org.iso.18013.5.1. sex (i.e. "not applicable"). Although the meaning currently is arguably not too different, the difference in meaning could increase in future versions of the org.iso.18013.5.1.aamva namespace[3].

Since the AAMVA mDL data element set includes two data elements for sex, the following apply:

1. Verifying entities shall treat org.iso.18013.5.1.aamva.sex as the primary source of sex information.
2. If an mDL supports org.iso.18013.5.1.sex, the value of the element shall have the meaning closest to the meaning of the value chosen for org.iso.18013.5.1.aamva.sex.

   NOTE 2: At publication time of this document, like values of the two elements map to each other (i.e. "1" for org.iso.18013.5.1.aamva.sex maps to "1" for org.iso.18013.5.1.sex, "2" maps to "2", and "9" maps to "9".). None of the values for org.iso.18013.5.1.aamva.sex map to "0" for org.iso.18013.5.1.sex.
3. When an mdoc receives a request only for org.iso.18013.5.1.sex, if a value of 9 is stored, the user interface should make it clear to the mDL holder that the information shared carries a different meaning compared to org.iso.18013.5.1.aamva.sex.
4. When an mdoc receives a request for both org.iso.18013.5.1.sex and org.iso.18013.5.1.aamva.sex, the mdoc shall respond (given approval by the mDL holder) at least with org.iso.18013.5.1.aamva.sex.

NOTE 2 Readers compliant with this document should ask for both org.iso.18013.5.1.sex and org.iso.18013.5.1.aamva.sex. This is because the reader will not know if the mdoc supports org.iso.18013.5.1.aamva.sex (although in practice it often will. The intent of #4 above is to, in this case, share the domestic data the reader is looking for. How the request is presented to the mDL holder, and how approval to share is administered, is left to implementers. Nevertheless, a simple approach could be for a mdoc to ignore the request for org.iso.18013.5.1.sex and to only ask for approval to share org.iso.18013.5.1.aamva.sex (given that both were requested).

3.3 PORTRAIT IMAGE

The portrait image is the primary means by which an mDL is matched to the person presenting the mDL in an attended transaction. The portrait image therefore needs to be of suitable quality for this purpose. ISO/IEC 18013-5 requires the portrait to comply with Annex D of ISO/IEC 18013-2:2020, which in turn requires the portrait image to be at least 192 pixels wide and 240 pixels high. In addition, ISO/IEC 18013-2 requires portrait images intended for automated face recognition to comply with ISO/IEC 19794-5, which among other

[3] In AAMVA systems, the value of 9 currently already means "Not specified or Non-binary gender".

requirements requires 90 pixels between the centers of the eyes. However, it should be noted that these requirements were created in the context of storage on a physical card and in machine-readable formats with limited storage capacity compared to an mDL.

It would therefore be possible to include a portrait image of much higher resolution in an mDL. Arguments for going this route include higher accuracy when using the portrait image as a probe image in 1:n biometric searching, and making it easier for a human to compare the portrait image with the mDL holder. Arguments against going this route include the following:

1. A larger portrait image can negatively affect mDL transaction times.
2. A better-quality portrait image could arguably be less privacy preserving than a smaller portrait image.
3. The primary purpose of the portrait image is a 1:1 match with the mDL holder. If this match is performed biometrically, the smaller portrait size should be sufficient.

Issuing Authorities should carefully consider all these points when deciding on a portrait image size. It is recommended that Issuing Authorities opt for a smaller rather than for a larger portrait image.

3.4 Signature image

ISO/IEC 18013-5 does not prescribe anything other than that the image shall be in JPEG or JPEG2000 format. Building on the requirements for a signature image in ISO/IEC 18013-1 and in the AAMVA Card Design Standard, the signature image must be an accurate and recognizable representation of the original signature. Care should be given to image capture, processing, digitization, and compression.

3.5 Cryptographic protocols

In line with recommendations from the US National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security, certain cryptographic constructs must not be supported for mDL solutions built in accordance with this document. At the same time, interoperability needs to be retained so mDL readers can successfully interact with an mDL originating from elsewhere.

To this end, the AAMVA mDL Implementation Guidelines require the following changes to be applied to ISO/IEC 18013-5:

1. Replace the 3rd paragraph of 9.1.4.4:

   > When cipher suite 1 is used (see 9.1.5.2) the following operations shall be performed and the mdoc reader shall use of the ECDSA or EdDSA curves from Table 22 for the mdoc reader authentication key.

   with the following:

   > When cipher suite 1 is used (see 9.1.5.2) the following operations shall be performed and the mdoc reader shall use Curve P-256, Curve P-384 or Curve P-521 from Table 22 for the mdoc reader authentication key.

2. Replace the 6th paragraph of 9.1.4.4:

> The `alg` element (RFC 8152) shall be included as an element in the protected header. An mdoc reader should use one of the following signature algorithms: "ES256" (ECDSA with SHA-256), "ES384" (ECDSA with SHA-384), "ES512" (ECDSA with SHA-512) or "EdDSA" (EdDSA). "ES256" should be used with curves P-256 and brainpoolP256r1. "ES384" should be used with curves P-384, brainpoolP320r1 and brainpoolP384r1. "ES512" should be used with curves P-521 and brainpoolP512r1. "EdDSA" should be used with curves Ed25519 and Ed448.

with the following:

> The `alg` element (RFC 8152) shall be included as an element in the protected header. An mdoc reader should use one of the following signature algorithms: "ES256" (ECDSA with SHA-256), "ES384" (ECDSA with SHA-384), or "ES512" (ECDSA with SHA-512). The mdoc reader shall not use the "EdDSA" (EdDSA) signature algorithm. "ES256" should be used with curve P-256. "ES384" should be used with curve P-384. "ES512" should be used with curve P-521.

3. Append the following to the 1st paragraph of 9.1.5.2: "Only cipher suite 1 shall be used." Since ISO/IEC 18013-5 does not explicitly prevent the use of additional cipher suites, absent this clarification it would technically be possible for an Issuing Authority and an mDL verifier that agree on a cipher suite X to claim compliance with ISO/IEC 18013-5.
4. Add the following after the 2nd paragraph of 9.1.5.2: "An mdoc shall support only the 1st three curves listed in Table 22 (i.e. Curve P-256, Curve P-384 and Curve P-521)."
5. Replace the 5th paragraph of 9.2.1:

> A TLS version 1.2 connection shall use one of the cipher suites listed in Table 23. The mdoc reader and issuing authority infrastructure shall support TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 and should support TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256.

with the following:

> A TLS version 1.2 connection shall use one of the cipher suites listed in Table 23. The mdoc reader shall support TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 and should support TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256. The issuing authority infrastructure shall only support TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.

6. Replace the 6th paragraph of 9.2.1:

> The key exchange shall make use of an elliptic curve listed in the NamedCurve enumeration in RFC 8422, section 5.1.1 for TLS 1.2 or RFC 8446, section 4.2.7 for TLS 1.3. No deprecated or reserved curves shall be used.

with the following:

> A TLS version 1.2 key exchange shall make use of an elliptic curve listed in the NamedCurve enumeration in RFC 8422, section 5.1.1. The mdoc reader shall support all the listed curves.

> No deprecated or reserved curves shall be used. The issuing authority infrastructure shall only support curves secp256r1, secp384r1 and secp521r1.
>
> A TLS version 1.3 key exchange shall make use of an elliptic curve listed in the NamedGroup enumeration in RFC 8446, section 4.2.7. The mdoc reader shall support all the listed groups. No deprecated or reserved curves shall be used. The issuing authority infrastructure shall only support curves secp256r1, secp384r1 and secp521r1.
>
> NOTE: Given current industry practices, it is unlikely that an 18013-5 compliant issuing authority infrastructure that does not follow this document (e.g. an issuing authority in Europe) will support only x25519 and/or x448. An mdoc reader that supports only secp256r1, secp384r1 and secp521r1 should therefore be able to connect to most issuing authorities. Nevertheless, there remains a logical possibility that an issuing authority infrastructure that does not follow this document supports only x25519 and/or x448, hence the requirement for mdoc readers to support these curves.

7. Replace the 7th paragraph of 9.2.1:

   > A TLS version 1.3 connection should use one of the cipher suites listed in Table 24. The mdoc reader and the issuing authority infrastructure shall support TLS_AES_128_GCM_SHA256 and should support TLS_AES_256_GCM_SHA384 and TLS_CHACHA20_POLY1305_SHA256.

   with the following:

   > A TLS version 1.3 connection should use one of the cipher suites listed in Table 24. The mdoc reader shall support TLS_AES_128_GCM_SHA256 and TLS_AES_256_GCM_SHA384 and should support TLS_CHACHA20_POLY1305_SHA256. The issuing authority infrastructure shall only support TLS_AES_128_GCM_SHA256 and TLS_AES_256_GCM_SHA384.

8. In tables B.1, B.3, B.5, B.6, B.7 B.8 and C.1, remove the brainpool curves from the "Subject public key info, parameters" certificate component.
9. In tables B3 and B.6, remove the Ed25519 and Ed448 curves from the "Subject public key info, algorithm" certificate component.
10. Replace the last paragraph of C.1.7.1:

    > The VICAL provider should use one of the signature algorithms for calculating the signature over the VICAL: "ES256", "ES384", "ES512" or "EdDSA". The VICAL provider should use one of the elliptic curves as specified in Table 22.

    with the following:

    > The VICAL provider shall use one of the following signature algorithms for calculating the signature over the VICAL: "ES256", "ES384" or "ES512". The VICAL provider shall use Curve P-256, Curve P-384 or Curve P-521 as specified in Table 22.

NOTE: The intent of requirements 8 and 9 is that issuing authorities shall not generate certificates using one of these curves. However, to ensure interoperability, mdocs and mdoc readers shall be capable of verifying a certificate that uses one of these curves, and shall be capable of using the public key in such a certificate for the applicable cryptographic operation specified in Clause 9 of ISO/IEC 18013-5.

3.6 IACA ROOT CERTIFICATE

In Table B.1 of ISO/IEC 18013-5, on the table row for the "ISSUER" certificate component, replace:

> `stateOrProvinceName` is optional. If this element is present, the element shall also be present in the end-entity certificates and hold the same value.

with the following:

> `stateOrProvinceName` is mandatory. The element shall also be present in the end-entity certificates and hold the same value.

3.7 VERSIONING

The data structure for the 2D barcode in the AAMVA Card Design Specification contains a version number. This enables readers to always know which version of the data structure is present on a credential since the full data string is always read. This is not true for a mDL. A mDL reader has to explicitly request individual data elements, and does not know in advance which data elements are present or what version of a data set is supported.

One approach to address this is to add a "version" data element to the AAMVA namespace. To be useful a mDL reader would have to obtain this data element before making a subsequent request for additional data. Allowing the release of this data element without mDL holder approval is possible; requiring approval may confuse a mDL holder and increase transaction friction. Regardless, the 2-step process would add complexity (an mDL reader would still have to allow for not receiving a response to such a request) and add time to the transaction. Such an approach would also be unique to mDL in North America.

Instead, versioning of the AAMVA mDL data element set is achieved as follows:

1. If needed, create a new identifier. This applies if there is a change to an existing data element, or if a completely new data element is added. Set a date by which mDL apps and mDL readers must support the new identifier.
2. For the old identifier, set a date by which mDL apps and mDL readers do not need to support the old identifier anymore.

For the data element changes introduced in this version of the AAMVA mDL Implementation Guidelines the two dates are on consecutive days. Ideally mDL readers would ask for the old identifier up to the change date and for the new identifier thereafter. However, it is likely that readers would, at least around the change date, ask for both. It is also likely that an mDL would, especially around the change date, include both identifiers. How the request is presented to the mDL holder, and how approval to share is administered, is left to implementers. Nevertheless, a simple approach could be for the mDL to present only one request, for the more recent identifier, to the mDL holder.

Future data element changes may separate the two dates such that the date by which a mDL reader must support a new identifier would be some time before the date by which the mDL reader does not need to support the old identifier anymore (see Figure 2). The main advantage of this approach is that the Issuing Authority will have the time between the two dates to provision the new identifier (and deprecate the old identifier) to all its mDLs with the knowledge that mDL readers should be able to accommodate either identifier (the highlighted option in Figure 2).

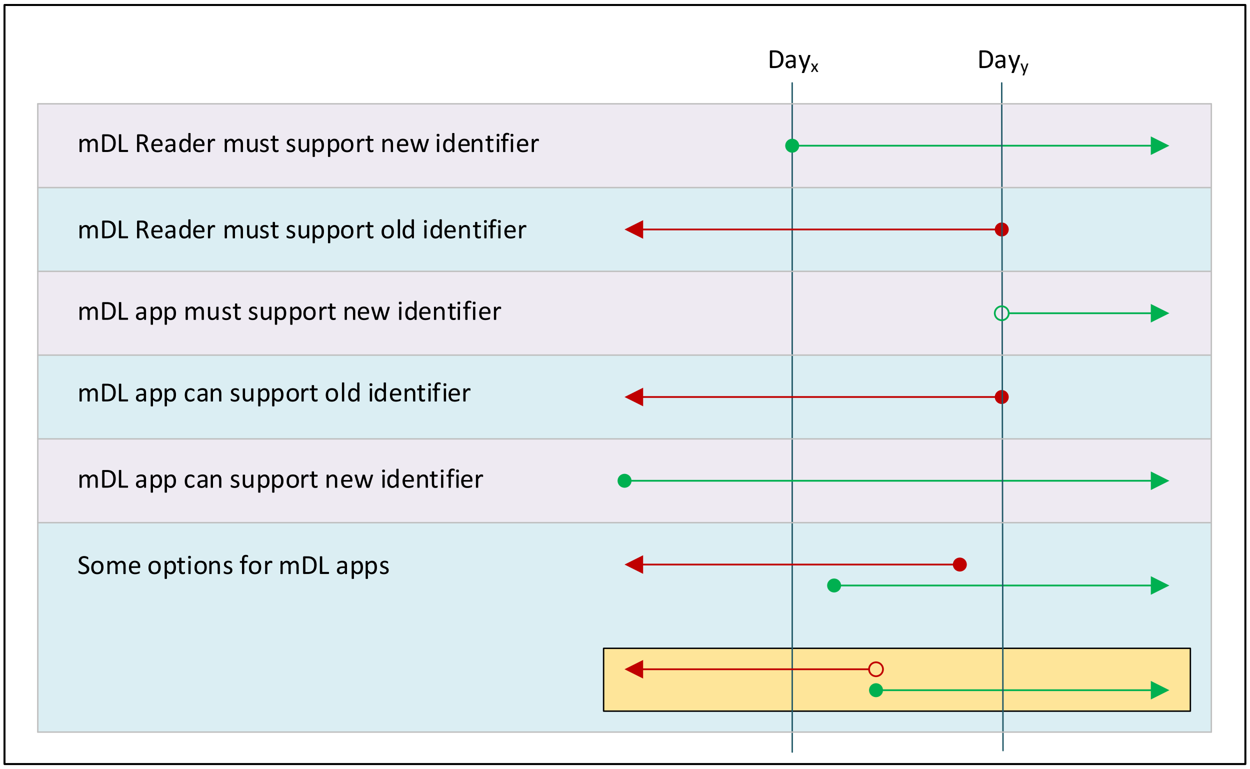
Day$_x$
Day$_y$
mDL Reader must support new identifier
mDL Reader must support old identifier
mDL app must support new identifier
mDL app can support old identifier
mDL app can support new identifier
Some options for mDL apps

Figure 2: Future versioning concepts

3.8 Issuing Authority Specific Data

ISO/IEC 18013-5 allows for the creation of additional namespaces, in like manner as the AAMVA namespace defined in this document (see clause 7.2.8 in ISO/IEC 18013-5). Issuing Authorities can use this mechanism to add additional fields to a mDL. The Issuing Authority would be responsible for communicating such an additional namespace to mDL verifiers that need to be able to read the Issuing Authority-specific data.

Note: ISO/IEC 18013-5 also lends itself to being adopted for the issuing of credentials separate from a mDL, for example fishing licenses, health credentials, or watercraft licenses.

4 Privacy and Security

4.1 Introduction

The privacy of an mDL holder has been paramount in the mDL design process from the start. Care was and is being taken in all the work to ensure that methods and means are available to protect mDL holder privacy.

The subsections that follow elaborate in more detail on different aspects of privacy protection and security.

4.2 Data Minimization and Selective Data Release

A primary component of privacy involves the ability of an mDL holder to only share some information. This is achieved by two related but distinct measures:

1. Data minimization: A decision by an Issuing Authority to record fractional information about an attribute in a mDL, thus empowering a mDL holder to share less information than would otherwise have been the case. For example, an Issuing Authority can decide to include[4] the optional age_birth_year field in a mDL in addition to the (mandatory) date of birth. This will allow the mDL holder to share only a birth year as opposed to a date of birth. Another example would be to include the resident city in addition to a full address.
2. Selective data release: Allowing a mDL holder to decide which of the data fields requested by an mDL verifier will be released to the Verifier.

As noted in section 2, it is important for Issuing Authorities to understand that ISO/IEC 18013-5 primarily specifies interfaces. The interfaces support both data minimization and selective data release. It is recommended that Issuing Authorities implement and provision as many of the optional minimized data elements, defined in ISO/IEC 18013-5 and in this document, as possible.

In addition, Issuing Authorities must ensure that mDL apps to which they provision data support at least the following:

- In case the request was received electronically, the mDL app must clearly convey what data was requested, and whether the mDL verifier intends to retain the information. If the request is presented in summarized form in the user interface (e.g. "Identity and driving privilege data" as opposed to "First Name, Last Name, DOB, Driving privileges"), means must be available to give the mDL holder visibility of the details of such a summarized form, both before and during a transaction.
- The mDL app must provide the mDL holder full control over which data elements to share with the mDL verifier.
- ISO/IEC 18013-5 requires the portrait image to be shared if the portrait was requested and if any other data element is released (to enable the mDL verifier to tie the mDL information to the person presenting the information). The app must support a graceful and informed exit from the request if the holder opts not to share the portrait image when requested.
- If blanket sharing options are used, measures must be implemented to ensure that the mDL holder remains aware of what is being released when such an option is in effect. An mDL holder must also be able to opt out of or cancel any blanket sharing function.
- The mDL holder must at any time (i.e. during a transaction as well as outside a transaction) be able to view at least the following information if the mDL holder so chooses:
    - Data elements listed in Table 5 of ISO/IEC 18013-5.
    - The data elements appended to Table 5 of ISO/IEC 18013-5 by section 3.1 of this document.
    - The contents of the `signed`, `validFrom`, `validUntil`, and `expectedUpdate` (if present) data elements from the mobile security object (MSO).

[4] It is logically possible for a mDL to calculate such information given a date of birth. However, ISO/IEC 18013-5 on purpose does not support this approach since it would have required the mDL verifier to place trust in the mDL device's ability to do this securely. As it is, the mDL verifier needs to trust only the Issuing Authority's public key.

Issuing Authorities (and their app providers) are encouraged to devise solutions that will minimize transaction friction without compromising the above requirements.

4.3 PROTECTING DATA

It is up to Issuing Authorities to ensure that all mDL data stored on the mDL holder's device is adequately protected. As standards in this respect are still under development, each Issuing Authority should take great care to ensure that the design of its solution supports this requirement. At minimum, Issuing Authorities must adhere to the following:

- mDL information must be stored in encrypted form.
- Private key material must be protected in a security module designed for the safekeeping of key material.
- Issuing Authorities must not rely on device unlocking to protect mDL data, since this feature can be disabled by the mDL holder. The mDL app must require mDL holder authentication, separately from device unlocking, each time mDL data is accessed or released (also see section 7).
- mDL data must be released to an mDL verifier only via an ISO/IEC 18013-5 compliant interface.

  Note 1: This requirement rules out the sharing of mDL data between apps on a phone using an interface other than standardized in ISO/IEC 18013-5.

  Note 2: This requirement rules out the sharing of mDL data using the mDL as a "flash pass" (i.e. by showing an image of a credential to a verifier); also see section 8.

4.4 AUDIT LOG

The mDL app must be capable of maintaining an audit log. The mDL app must allow the mDL holder to decide if an audit log must be maintained or not. It is recommended that the mDL app requires the mDL holder to explicitly choose for or against keeping an audit log upon setup (i.e. no defaults, and in addition to being able to change this subsequently). The audit log and related settings must be accessible only to the mDL holder (also see section 4.6). The audit log must allow for the recording of all mDL transactions. In this context, an mDL transaction is the sharing of information by a mDL holder with a mDL verifier, as well as any provisioning, update, or communication action between the mDL and the Issuing Authority. At minimum, the following must be recordable for any transaction: Transaction timestamp; type of transaction (e.g. update or data sharing); in case of a data sharing transaction the data that was shared, and to the extent that it can be gathered, information about the identity of the mDL verifier. It is recommended that the mDL app provides the mDL holder the capability to select what types of activities are recorded in the audit log (i.e. rather than only an "all or nothing" option). It is also recommended that the mDL app includes functionality to help the mDL holder monitor and manage the size of the audit log within the capabilities of the mDL holder's device.

If an Issuing Authority allows an mDL holder to hold the same mDL on more than one device, the audit log settings on each device should be independent of each other. It is recommended that there be no synchronization of the audit log or audit log settings between the two devices. Any synchronization features that are provided must adhere to the following:

1. Synchronization must be an option that can be enabled or disabled by the mDL holder. The process to enable synchronization must require the mDL holder to prove access to both devices.

2. Synchronization must occur directly between the devices in question. A synchronization action must not give visibility of any of the following to anyone other than the mDL holder:
    a. Audit log information.
    b. Audit log settings.
    c. The fact that a synchronization action/selection took place.
    d. Any information that may convey that the mDL holder has an mDL on more than one device.

4.5 DELETING MDL INFORMATION FROM A DEVICE

An mDL holder must have the capability to delete the mDL holder's mDL from the mDL holder's device. Such deletion:

1. Must delete all mDL information, log information, and any metadata (e.g. settings) that could impart information about the deleted mDL or its use.
2. Must not require approval by the Issuing Authority.
3. Must be an option available to a mDL holder on the mDL device.
4. Should be available to a mDL holder via a request to the Issuing Authority (see below).

Should an mDL device (i.e. a device containing an mDL) be lost or get stolen, it could be beneficial for the mDL holder to have the mDL remotely deleted (or temporarily suspended[5]) by the Issuing Authority. Besides the obvious advantage to the mDL holder, other considerations apply too:

1. The mDL holder's request must be authenticated. It must not be possible for someone other than the mDL Holder or the Issuing Authority to delete (or suspend) a mDL.
2. A "push" capability (from the Issuing Authority to the mDL device) is needed for immediate deletion (or suspension) (see section 6).
3. Successful deletion (or suspension) depends on network connectivity to the mDL device.
4. The mDL will automatically become unusable (although potentially not inaccessible) when the MSO expires (see section 6).

In addition, mDL deletion may be needed when an mDL holder wants to transfer an mDL to a new device, when a person moves to another jurisdiction, or when a person dies.

Issuing Authorities should weigh the benefits and challenges associated with a remote delete (or suspension) capability when considering its implementation (see Appendix A).

An mDL holder must have the capability to delete audit log information (as defined in section 4.4) the mDL holder may previously have elected to maintain. It is recommended that this capability allows selective deletion (i.e. specific log entries, rather than only an "all or nothing" option).

[5] Deletion ensures that an mDL cannot be accessed or used any more. Suspension may still leave the mDL information open to unauthorized access, since the mDL still resides on the device. On the other hand, lifting a suspension would be less involved for an mDL holder than having to go through the provisioning process again.

4.6 No tracking

"Tracking" is the act of compiling information about an mDL holder and/or an mDL Holder's activity. Any stakeholder (including Issuing Authorities, technology providers, service providers and mDL verifiers) must not track mDL Holders or the usage of any mDL except as required by law (e.g. when a drug store dispenses products containing ephedrine).

Tracking by an mDL verifier can be performed as soon as two different mDL transactions can be linked to each other. This can be countered by designing the solution to maximize anonymity ("characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly", from ISO/IEC 29100) and to maximize unlinkability. Anonymity can be hampered by metadata that may be associated with multiple mDL transactions, e.g. hardware or network addresses, long-term public keys, or session tokens. Consequently, care must be taken to minimize the sharing of static or long-lived metadata.

Although pre-matched transactions hold the promise of maximizing anonymity at a user data level, anonymity in post-matched transactions is limited since the portrait image is always shared. For these transactions it is recommended that Issuing Authorities pursue regulatory protection against tracking by mDL verifiers.

Solutions using the server retrieval method also pose challenges in preventing tracking. As per design, the Issuing Authority is involved in real time each time an mDL is used by the mDL holder. The Issuing Authority would technically be able to keep track of when an mDL holder uses his/her mDL and keep track of what data is shared. Based on IP address analysis the Issuing Authority would also be able to track an mDL holder's physical location to some extent. This can be mitigated by placing regulatory limitations on the Issuing Authority[6], and will be of value to the extent an mDL holder trusts the Issuing Authority's adherence to the regulatory limitations. Consequently, Issuing Authorities considering a server retrieval solution should carefully weigh the advantages of this approach against its privacy implications.

Since the audit log (see section 4.4) contains a full record of when and potentially where an mDL was used, access to the audit log must not be possible by anyone other than the mDL Holder.

4.7 Limiting use of mDL data

Apart from limiting tracking (see section 4.6), Issuing Authorities may also want to place other limitations on the use of mDL data. However, once data is shared with a verifying entity, the data is beyond the technical control of both the mDL holder and the Issuing Authority. Consequently, it is recommended that Issuing Authorities pursue regulatory solutions for limiting the use of such data.

It is also recommended that mDL holders be made aware that they are the front line of defense against unauthorized use of data by virtue of their ability to limit data release. mDL holders should be sensitized to be very circumspect about with whom and what data is shared. In particular, regulatory protection is jurisdictionally based and may not be the same or even present everywhere. It is further recommended that these messages be conveyed in the form of continued education throughout the life of the mDL.

[6] The potential challenges noted here for an Issuing Authority would apply equally if the Issuing Authority employed any contractors to implement all or part of a solution. Ultimately, all safeguards would be procedural/regulatory rather than technical in nature.

4.8 Fraud attempts

The mDL has been designed to be more trustworthy and less easy to compromise than a physical driver's license (or ID card). As a result, it is expected that people with nefarious intent will try other avenues to obtain a fraudulent credential. For example, fraudsters may increase attempts to establish a fraudulent identity in the Issuing Authority's systems (to subsequently be issued with a genuine mDL). Renewed attacks could also be seen against physical cards. Issuing Authorities should remain alert for such changes in the security landscape and institute appropriate mitigating measures.

4.9 mDL app access

Physical credentials are sometimes legally accessed by persons other than the holder. For example, if a person becomes incapacitated in a traffic crash, a law enforcement officer could legally retrieve the person's physical credential from the person's wallet.

Given this scenario, it has been suggested that mDL apps allow similar access in case of justifiable need.

However, because such a feature could easily be misused when the mDL holder is not incapacitated, an mDL must not allow access to the mDL information by anyone other than the mDL holder. (Note that in this context "mDL holder" is understood to include another named person legally authorized by a court or by law to act on behalf of the mDL holder. For example, a parent would need access to a minor child's mDL, and a caregiver legally appointed as a guardian would need access to the ward's mDL.)

4.10 App feature disclosure

An Issuing Authority must endeavor to provide full transparency to an mDL holder about all the features supported by an mDL app. For example, an mDL holder can be informed that:

1. Your mDL data resides on this device. The DMV is not involved in any transaction at transaction time.
2. Your mDL data needs to be refreshed every 30 days. You can choose this to occur automatically, or to occur only when clicking on the "Update mDL data" button. If your mDL data becomes older than 30 days, your mDL data can successfully be verified again by an mDL verifier as soon as you refresh the data.
3. Your mDL app has been independently certified as complying with both ISO/IEC 18013-5 and with the AAMVA mDL Implementation Guidelines.
4. The source code for the app is available at mDL.sourcecode.DMVx.gov.

Note that this is a non-exhaustive list and includes topics not addressed by this document. The intent is to provide examples of information an Issuing Authority may want to share, and to illustrate how it could be conveyed.

5 Trust model

An mDL verifier generally trusts mDL information if both the following conditions are met:

1. The mDL verifier can verify that the mDL was issued by a bona fide Issuing Authority.

2. The mDL verifier can confirm that the mDL information has not been changed since it was created by the Issuing Authority.

ISO/IEC 18013-5 supports the above conditions by way of public-private key cryptography. If an mDL verifier can:

1. Obtain an Issuing Authority's public key;
2. Trust that it really is that Issuing Authority's public key;
3. Trust that the Issuing Authority's private key has not been compromised; and
4. Successfully authenticate an mDL issued by that Issuing Authority using said public key;

then the conditions stated above are met.

To facilitate items 1 to 3, ISO/IEC 18013-5 defines a Verified Issuer Certificate Authority List (VICAL). In concept, a VICAL Provider collects public keys from bona fide Issuing Authorities, confirms that the Issuing Authority manages its keys securely, aggregates the public keys into one VICAL, and provides the VICAL to mDL verifiers.

In support of its members, AAMVA is (as of the date of this document) working to establish a minimally viable product (MVP) version of a Digital Trust Service (DTS). The MVP DTS will perform the function of a VICAL Provider. Specifically, the DTS will:

1. Be governed by AAMVA members.
2. Confirm the bona fides of an Issuing Authority wanting to have its public key added to the VICAL.
3. Set minimum requirements, including for key administration, for an Issuing Authority's mDL program to have its public key added to the VICAL. Until such time as the DTS expands on this, Issuing Authorities should consult NIST SP 800-57 for guidance on key management.
4. Ensure the integrity of the VICAL and of all associated operations and systems, at both the DTS and at Issuing Authorities.

The above approach will support interoperability of mDL solutions between Issuing Authorities in North America. Looking beyond that, AAMVA has already started conversations with like organizations in Europe (EReg) and Australia/New Zealand (Austroads) on this topic. The vision is to work towards a solution that will enable AAMVA members eventually to also authenticate mDLs issued in other parts of the world, and vice versa.

Until such time as the DTS is operational, Issuing Authorities may want to consider publishing public keys on Issuing Authority websites, and to conduct outreach actions directly to major mDL verifiers.

6 mDL DATA REFRESH

6.1 INTRODUCTION

From time to time, events occur that require an identity credential (such as a driver's license) to be updated before its natural expiration date. Examples are driving privilege revocation, address change, physical card format change (when turning 21 in the US), or a name change. Some of these are changes a credential holder would want, and for which the credential holder would typically approach the Issuing Authority with a request to issue a new credential. Other changes could be less desirable (e.g. driving privilege revocation), in which case a credential holder may try to hold on to an outdated credential (with potentially negative consequences).

These challenges are not easily solved in the case of physical credentials. In contrast, an mDL provides the ability to improve the timely application of changes.

The two subsections that follow address the following:

1. mDL refresh mechanisms.
2. Operationally handling differences between a physical credential and an mDL because they were not updated at the same time.

6.2 mDL REFRESH MECHANISMS

6.2.1 Server retrieval method

mDL data provided to an mDL verifier under the optional server retrieval method is always as current as the Issuing Authority's database. Changes in the Issuing Authority's database regarding a specific person's mDL are immediately available to mDL verifiers upon reading the associated mDL.

6.2.2 Device retrieval method

mDLs are required to support the device retrieval method. In this case, the data residing on an mDL device needs to be updated after an Issuing Authority applies a change to its database. To support this, it is recommended that Issuing Authorities include an "Update mDL" function in its mDL app that can be invoked by the mDL holder.

The Issuing Authority may also decide to offer an auto update function. To provide full transparency to an mDL holder about any communication between the mDL and the Issuing Authority, it is recommended that the mDL app not refresh the mDL data automatically unless the mDL holder opted in for such behavior.

To address cases where the Issuing Authority deems an update to be necessary and the mDL holder does not initiate the update, an Issuing Authority can leverage either or both the following mechanisms (also see Appendix A).

1. Build a "push" function into the mDL app that would enable the Issuing Authority to send an instruction to the mDL to prevent mDL information (or at least the outdated mDL information) from being shared until such time as the mDL holder refreshes the mDL. Any push action must include an accompanying notification to the mDL holder. (Also see section 4.5, which presents a use case requiring a stronger form of a "push" function.)
2. ISO/IEC 18013-5 distinguishes between the validity period of the legal credential (which often ranges from 5 to 7 years and is the same for both the physical credential and the mDL), and the technical validity period of the MSO. The MSO validity period can be set to a period shorter than the validity period of the legal credential. Once the MSO validity period has expired, the mDL will fail any authentication attempt by an mDL verifier. An Issuing Authority can therefore wait until the MSO expires and the mDL holder chooses to refresh the mDL. The implication is that the mDL information may be outdated for almost up to the duration of the MSO validity period.

Until such time as more operational experience is gained in this area, the recommendation is to set the MSO validity period to 30 days.

6.3 Operational considerations

It is likely that updates in an Issuing Authority's database record of a person will not be applied to the physical credential and to the mDL (or to multiple mDLs of the same person, if supported by an Issuing Authority) at the same time. As a result, an mDL holder may hold two credentials that reflect different information.

It should be rare for an mDL verifier to become aware of a such a difference. Nevertheless, if that were to happen, it may cause confusion and/or distrust on the part of the mDL verifier. Issuing Authorities should therefore endeavor to institute processes that minimize the duration of differences between a physical credential and the associated mDL (or between multiple mDLs of the same person, if supported by an Issuing Authority).

It is recommended that Issuing Authorities enact local legislation clarifying that the mDL information takes precedence over information from a physical credential in case the information differs.

7 Multiple credentials and shared devices

7.1 Device:mDL holder combinations

Arguably the most common relationship between an mDL holder and an mDL device that can be expected is that the mDL device will be used by only one mDL holder, and that an mDL holder will use a single mDL device. This is illustrated in Figure 3.

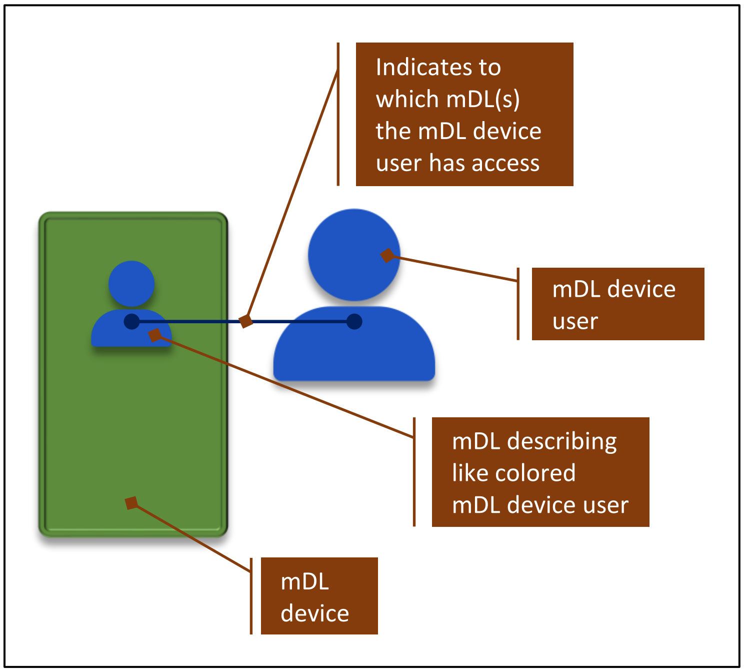
Indicates to which mDL(s) the mDL device user has access
mDL device user
mDL describing like colored mDL device user
mDL device

Figure 3

However, there are cases where this relationship does not apply, as indicated by the following 3 examples.

1. An mDL holder may need to have the mDL holder's mDL installed on more than one device used by the mDL holder. An example (Figure 4) would be for an mDL holder to have the mDL holder's mDL on the mDL holder's phone and on the mDL holder's tablet at the same time.

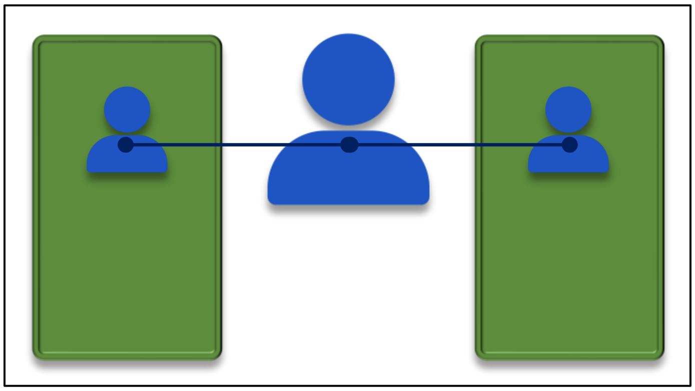

Figure 4

2. An mDL may have to be installed on more than one device, each device used by a different person. Examples would be where a child's mDL is installed on both parents' mobile devices (Figure 5), or where a young person's mDL resides on that person's device as well as on a parent's device (Figure 6).

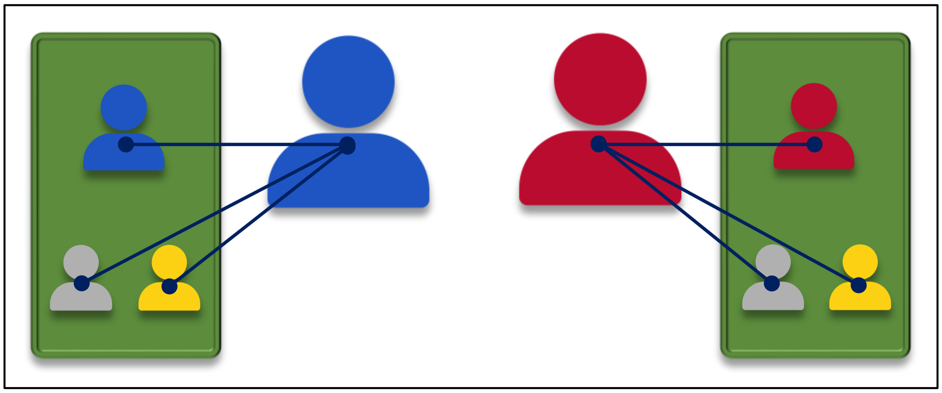

Figure 5

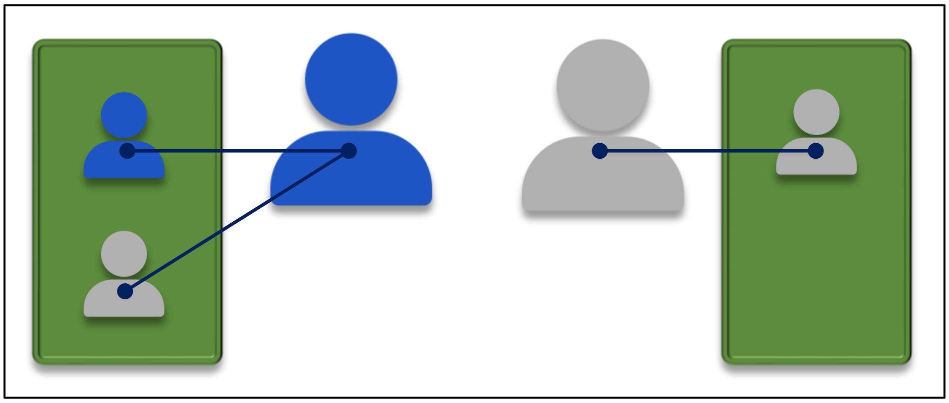

Figure 6

3. mDL holders share the same device. In this case, multiple mDLs are installed on the same device, with the single device used by multiple persons. Two different examples of configurations are shown in Figure 7, Figure 8 and Figure 9.

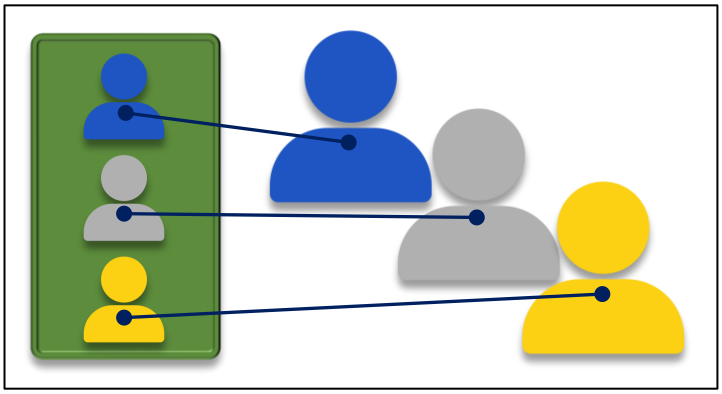

Figure 7

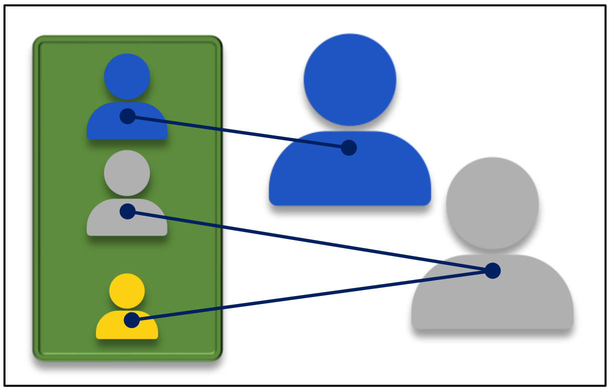

Figure 8

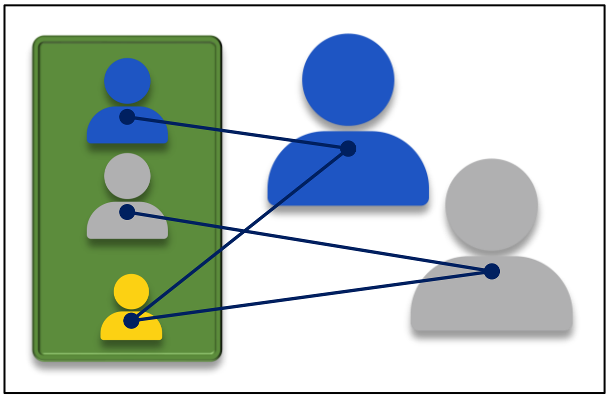

Figure 9

Issuing Authorities should identify the combinations that may apply in its jurisdiction and make a conscious decision on which combinations it will support.

7.2 LIMITATIONS ON MULTIPLE CREDENTIALS

The following are examples of rules that currently apply to identity records and to physical identity credentials:

1. In some jurisdictions, a person may legally hold more than one physical identity credential (e.g. a driver's license card and an identification card).
2. In some jurisdictions, a person may legally hold only one physical identity credential.
3. In the US, the REAL ID Act effectively limits a person to hold only one driver's license and only one REAL ID credential.
4. Some jurisdictions allow their customers to also hold identity credentials in other jurisdictions.
5. Some jurisdictions do not allow their customers to also hold identity credentials in (some) other jurisdictions.
6. In the US, the rules of the State-to-State system (S2S) limit a person to hold only one driver record, regardless of the type of credential with which it is associated. The Canadian Driver's Licence Agreement sets out similar requirements.

Rules such as these result in many valid identity record and physical credential combinations. Assuming that existing rules for identity records and for physical credentials stay in place, mDL introduces the following questions:

1. Should a person be allowed to hold both a physical credential and an mDL at the same time?
2. Should a person be allowed to hold the same mDL on multiple devices at the same time?

These questions can be discussed based on their privacy implications, operational implications, and (for the US) REAL ID requirements.

1. Should a person be allowed to hold both a physical credential and an mDL at the same time?
   a. Privacy implications: Privacy advocates have expressed concern about not having the option of a physical credential. Having to choose between a physical or electronic credential could be perceived as pressuring customers into an electronic only situation.
   b. Operational implications: The availability of mDL readers will be limited as the ecosystem grows. In addition, an mDL holder may want to provide for the possibility that the mDL device becomes nonfunctional (e.g. when it runs out of power). This will require Issuing Authorities to allow mDL holders to also carry a physical credential as fallback credential.
   c. REAL ID implications: The REAL ID Rule limits a person to one REAL ID card and requires the termination of a driver's license in any other state before issuing a REAL ID driver's license. Informal discussions with DHS have indicated that holding a physical REAL ID card and an mDL of the same credential at the same time does not contravene the spirit of either the REAL ID Act or the Rule. The mDL is viewed as an extension of the physical card.
2. Should a person be allowed to hold the same mDL on multiple devices at the same time?
   a. Privacy implications: Each additional copy of an mDL increases the attack surface for unauthorized access to the underlying information. If an Issuing Authority allows an mDL holder to have an mDL provisioned onto more than one device, this should therefore only be at the request of the mDL holder. On the other hand, holding the same mDL on multiple devices

may yield a privacy benefit. If an mDL holder wants to retain logs of mDL activities, such logs can be split between the different mDL devices (assuming that logs will not be synchronized between instances). Regardless, an Issuing Authority should consider placing place a limit on the number of such instances.

b. Operational implications: Concern has been expressed in the past that allowing unlimited copies of an mDL may lead to fraudulent attempts to use a copied mDL. Applied to physical credentials this would be similar to having a large number (tens of thousands) of authentic copies of one person's physical card, and having this occurring for many persons. To prevent this, ISO/IEC 18013-5 requires an mDL to be cryptographically bound by the Issuing Authority to the device onto which the Issuing Authority provisions it. The mDL reading protocol will terminate if this condition is not true. This prevents an mDL holder (or other nefarious agents) to use unauthorized copies of an mDL. The Issuing Authority may however provision an mDL holder's mDL onto more than one device if it so chooses. Such use, since limited to devices controlled by the mDL holder, does not pose the same risk as the concern raised above. There are also realistic use cases that can benefit from allowing an mDL holder to request provisioning of the mDL to multiple devices. For example, an mDL holder may want a limited mDL provisioned onto a wearable form factor with the ability to only prove being above 21 years of age (in addition to the full feature mDL on a regular mobile phone). As technology evolves, some use cases may also consider a vehicle's systems as a device into which an mDL can be provisioned.

c. REAL ID implications: It could be argued that, especially given an Issuing Authority's improved ability to limit the circulation of stale mDL information (see section 6), holding an mDL on more than one device does not contravene the intent of the REAL ID Act or Rule. Informal discussions with DHS did not convey any immediate intent to limit this practice (i.e. of holding an mDL on more than one device).

In summary, it can be stated that:

1. mDL does not change the rules for physical credentials or for identity records.
2. It is acceptable to hold a physical credential and an associated mDL at the same time.
3. Issuing Authorities must continue to offer physical credentials to customers.
4. Provided that jurisdictional rules allow, it is acceptable to hold the same mDL on different devices at the same time.

8 "FLASH PASS" USE

"Flash pass" use is where an mDL verifier consumes an mDL by viewing human-readable information and a portrait image rendered on an mDL holder's device. However, the value of an mDL comes from authentication using the Issuing Authority's public key. Absent this authentication there is no trust in the information. Issuing Authorities must therefore take care that the rendering of information on a mobile device does not create the impression that it can be used as a "flash pass".

An argument has been made that "flash pass" use will speed up adoption of the mDL concept. While this may be true in the short term, such use also poses the following risks:

1. There will be no incentive for verifying entities to acquire mDL readers, and that crucial part of the trust model will never get established.

2. Creation of a fraudulent "flash pass" mDL is easy. A proliferation of fraudulent "flash pass" mDLs will damage the image of the true mDL concept. Besides making it easier to commit fraud, supporting "flash pass" use could therefore also set back efforts to bring the true benefits of an mDL to mDL verifiers and to consumers.

This also applies to the PDF417 barcode typically found on the back of a physical identity credential. It has been suggested that this barcode can be rendered by an app on a mobile device's display in support of a "flash pass" use scenario. Such use poses the following risks:

- The receiver of the information has no means by which to authenticate the accuracy or origin of the information.
- Due to size requirements for a portrait image, a PDF417 barcode most likely will not contain the credential holder's portrait image. There would therefore be no way in which the verifier can independently tie the barcode to the person presenting the barcode.

9 REVOCATION IN CASE OF OUT-OF-STATE/PROVINCE/TERRITORY ACTION

9.1 NEW STATE OF RECORD

REAL ID requires an existing credential to be cancelled before a new one can be issued by a different state. Likewise, some reciprocal agreements among provinces/territories in Canada require cancellation of prior products. For physical cards, this consists of two actions: Notifying the prior Issuing Authority, and (if available) confiscation of, or rendering as unusable, the old physical card. Upon receipt of a notification, the prior Issuing Authority records the fact that it is not the jurisdiction of record for the person anymore. Prior Issuing Authorities typically do not take any further action, assuming that the new Issuing Authority deals with the old physical credential if presented.

However, since the new Issuing Authority cannot "deal with" an old mDL, the old Issuing Authority now has the additional responsibility to revoke the mDL (i.e. to render it unfit for use). It is recommended that this be performed within 30 days.

9.2 OUT-OF-STATE/PROVINCE/TERRITORY CONVICTION

Some jurisdictions may impound a person's physical driver's license at the roadside in cases of serious violations.

For in-state/province/territory drivers, the mDL equivalent could be an immediate cancellation of a person's mDL (see section 6), with the advantage that the identification function of the mDL can stay intact if the mDL holder so chooses.

For out-of-state/province/territory drivers, it is recommended that Issuing Authorities immediately notify the driver's state/province/territory of record about the situation. In the US, this can be done via the S2S system[7].

[7] This requires both states to be on functional release 6.2 or later.

10 Provisioning

10.1 Introduction

Issuing Authorities have the responsibility to:

1. Ensure the effective, accurate and secure provisioning of an mDL holder's mDL onto the mDL holder's device.
2. Before exchanging sensitive information with an mDL, confirm that mDL app and the hardware on which it is being presented, support the functional requirements of the Issuing Authority.

At this time, standards, mechanisms and approaches according to which this can be achieved are being drafted. Until such time as these standards can be referenced, Issuing Authorities should take extra care to achieve the goals noted.

The remainder of this section provides guidance on select provisioning topics. This section will be expanded as relevant standards become available.

10.2 Encryption

Communication between an Issuing Authority and an mDL device must be encrypted. The process by which an encrypted channel is set up must not exchange information by which the mDL holder can be identified.

10.3 Remote provisioning

10.3.1 For purposes of post-matched transactions

In a post-matched transaction, the mDL device by and large is not a point of trust for the mDL verifier. The mDL verifier trusts that the information received has not been changed based on a successful signature checking process using a public key the mDL verifier trusts to originate from a valid Issuing Authority. An Issuing Authority on the other hand does need to place trust in the mDL device to adequately safeguard the mDL information while at rest.

Neither of these are affected by whether the provisioning to an mDL device occurs in person or remotely. Consequently, remote provisioning in principle is acceptable.

Nevertheless, an Issuing Authority should institute reasonable measures to ensure that an mDL is provisioned onto the correct device. This is the mDL equivalent to ensuring that a physical card makes it into the hands of the correct person (e.g. by mailing a card to the address on file).

To this end, Issuing Authorities must confirm at least two out of the following three authentication factors before concluding a remote provisioning process:

1. Something the mDL holder has.
2. Something the mDL holder is.
3. Something the mDL holder knows.

In addition, the following apply:

1. The authentication factors used must be independent of each other. For example, a physical credential (something the mDL holder has) and an online account with the Issuing Authority (effectively something the mDL holder knows) are not independent of each other if the online account can be created or changed using only the physical credential.
2. It may be possible to leverage 3rd party services to confirm "something the mDL holder knows". Care should however be taken to ensure such a service's processes/questions are independent from the other authentication factor used. For example, if the other authentication factor is a physical credential (something the mDL holder has), the 3rd party's process should not consider any information that is available on or could be obtained using the physical credential.
3. NIST SP 800-63A, section 5.3.2, addresses "something the mDL holder knows" type questions. Although applicable specifically to initial identity establishment ("proofing"), the guidance also applies when using "something the mDL holder knows" as an authentication factor.
4. Remote provisioning may not be appropriate for all credential holders. It is recommended that Issuing Authorities establish minimum requirements for which existing credential holders would qualify for remote mDL provisioning.
5. Remote provisioning may not be appropriate for all platforms (device / operating system / app combination). It is recommended that Issuing Authorities determine which platforms qualify for remote provisioning.
6. A remote provisioning process must not be used by an Issuing Authority to establish an identity record. Establishment of an identity record must occur in person.

10.3.2 For purposes of pre-matched transactions

The technical solution for pre-matched transactions is under development. Nevertheless, in line with NIST SP 800-63B 6.1.2.3[8] a credential holder will have to appear at the Issuing Authority in person (or undergo a supervised remote process using hardware under control of the Issuing Authority) and be identified via biometric means for the Issuing Authority to establish a suitably trustable binding[9] between the mDL holder and the mDL holder's device. It is therefore recommended that Issuing Authorities prepare for pre-matched transactions by, at the earliest in person opportunity, establishing cryptographically verifiable information that can bind credential holders to their devices.

10.3.3 For any purpose

The Issuing Authority should notify the person whose identity is being provisioned of the activity. This should be performed using a method other than the device involved (e.g. email, letter, other device).

[8] In discussions with NIST, section 6.1.2.3 of SP 800-63B was identified as applicable to binding a mDL to a person where the Issuing Authority has already established a record for the person previously.

[9] I.e. at IAL3. At IAL2, a remote binding process using the mDL device could be possible.

10.4 mDL RECORD

The mDL record maintained by an Issuing Authority must include the following:

1. All functional data elements provisioned to an mDL.
2. All supporting data provisioned to an mDL, e.g. cryptographic salts for message digests within the MSO.
3. The current copy of the MSO (or MSOs) for the mDL holder's device (or for each of the mDL holder's devices, if active on more than one device at the same time).
4. Public mDL cryptographic key material by which an mDL device can uniquely be identified.
5. Logs of an Issuing Authority's interaction with an mDL device. Logs must include the following:
    a. Timestamp
    b. Action performed. At least the following actions must be captured:
        i. Provisioning request (including key material and identifying information within the signing request) and outcome (successful / unsuccessful)
        ii. Deletion action, by whom initiated (Issuing Authority or mDL holder), and outcome (successful / unsuccessful)
        iii. Update action, by whom initiated (Issuing Authority or mDL holder), and outcome (successful / unsuccessful)

It is recommended that the record maintained by an Issuing Authority also includes the following:

1. Whether or not the binding between the mDL holder and the mDL device was performed in person (see section 10.3.2).

The following minimum retention periods are recommended:

mDL record component	Retention period
All functional data elements provisioned to an mDL.	As long as the mDL remains valid, and for 1 year thereafter.
All supporting data provisioned to an mDL, e.g. cryptographic salts for message digests within the MSO.	30 days after an MSO was replaced or deleted, or 30 days after the expiration date of the MSO, whichever comes earlier.
The current copy of the MSO (or MSOs) for the mDL holder's device (or for each of the mDL holder's devices, if active on more than one device at the same time).	30 days after an MSO was replaced or deleted, or 30 days after the expiration date of the MSO, whichever comes earlier.

mDL record component	Retention period
Public mDL cryptographic key material by which an mDL device can uniquely be identified.	As long as the device remains bound to both the mDL and the mDL holder, and for 1 year thereafter.
Logs of an Issuing Authority's interaction with an mDL device.	2 years

11 Miscellaneous

11.1 Terms and conditions disclosure

It is expected that Issuing Authorities may have legal terms and conditions applying to an mDL service. It is recommended that, in addition to ensuring the availability of the actual terms and conditions, Issuing Authorities communicate the terms and conditions to mDL holders in clear and simple language. At minimum, this should be done before the mDL holder can share mDL information with an mDL verifier.

Examples of such language are:

> "Only you can release your data. Once released, you may have other means (e.g. local legislation) to control the subsequent use of your information by the receiving party."
>
> "If you are asked to release data you feel uncomfortable sharing, do not share it."
>
> "To keep your mDL active and your data secure, your data needs to be updated periodically. You can choose to initiate this update yourself, or you can choose this to happen automatically."
>
> "If you believe your digital identity data is being misused, report it [here]."

11.2 Interim documents

When a person has applied for a physical credential (DL or ID card) and the final card is not immediately available, a temporary document is typically issued. The AAMVA Card Design Standard recommends that the interim document only be a receipt containing no security features and no photograph. Such an interim document is intended only as a proof of the transaction, and not intended for identification purposes. The AAMVA Card Design Standard does however leave the option for the interim document to reflect a person's driving privileges.

Issuing Authorities may have a need for a similar receipt, albeit in digital form, when dealing with mDLs. Two cases, have been identified:

1. The mDL applicant's identity has been validated, e.g. in accordance with REAL ID rules, yet the Issuing Authority's process includes additional steps (such as to biometrically check in the Issuing Authority's own database that the person has only one record). In this case, it is recommended that the Issuing Authority issues the final mDL.
2. The mDL applicant's identity validation has not concluded. In this case, it is recommended that the Issuing Authority only issues a receipt, and not an mDL. Such a receipt could be rendered inside the

mDL app the Issuing Authority uses; however, the format and content would be jurisdiction specific and not intended to be interoperable.

11.3 DATA PRESENTATION

Data elements defined in ISO/IEC 18013-5 follow ISO units of measurement, e.g. yy.mm.dd for date, and meter for length. It is recommended that Issuing Authorities ensure that mDL apps and readers have the capability to display such information using local conventions and units of measurement.

Similarly, mDL apps (and mDL readers) can support different display languages without affecting the interoperability of the underlying mDL data. This allows Issuing Authorities to tailor the mDL app user interface (and mDL verifiers to tailor the mDL reader app user interface) to local needs.

It is recommended that Issuing Authorities consult digital interface accessibility requirements (e.g. as set out in the Web Content Accessibility Guidelines) for purposes of mDL app design. Issuing Authorities may also consider addressing accessibility requirements for mDL apps and mDL readers in their authorizing statutes.

11.4 mDL ACCEPTANCE

Especially as the mDL concept is in the beginning stages of being rolled out, acceptance will not be universal. While a federal agency such as the Transportation Security Agency (TSA) in the US may accept an mDL as a valid form of identification, the agencies may not yet accept an mDL. In short, legal acceptability will vary from location to location.

It is therefore recommended for Issuing Authorities to:

1. Adequately inform mDL holders about legal acceptability in its own jurisdiction.
2. Point out that legal acceptability in other jurisdictions will vary.
3. Pursue measures to allow legal use in its own jurisdiction.

Issuing Authorities should also be attentive to any bias that may emerge in the marketplace, either in respect of individuals having an mDL, or in respect of individuals that have a physical credential only and take appropriate action when needed.

11.5 mDL APP PROCUREMENT SCHEMES

Issuing Authorities broadly have the following options when it comes to the creation of an mDL app:

1. Build an mDL app in-house.
2. Contract out the mDL app to a vendor.
3. Allow mDL holders to bring their own mDL apps.

Regardless, an Issuing Authority remains responsible for ensuring that the requirements and recommendations pertaining to the mDL app are followed. Suitable mechanisms to achieve this must therefore be instituted by the Issuing Authority. The mechanisms will vary depending on the situation.

For example, an Issuing Authority that allows mDL holders to bring their own apps could do the following in respect of those apps:

1. Publish a set of mDL app requirements; and
2. Require apps presented by customers to be independently certified against the requirements. The Issuing Authority would identify which certification entities it trusts.

APPENDIX A: MDL UPDATE/DELETE OPTION COMPARISON

This document discusses various operational needs for updating or deleting mDL information on an mDL device. These needs can be met in different ways, each of which has its own implications. This Appendix provides a comparison of the different ways in which these needs can be met. The purpose is to help inform Issuing Authorities about the features and implications to consider when deciding on the approach to follow. Note that the options outlined are not mutually exclusive; an Issuing Authority can pick different options depending on the change in the mDL information. For example, the approach for deleting a mDL in case of theft of a device may be different from the approach used when a person's last name has changed. The options are also not intended to be complete; an Issuing Authority may be able to devise hybrid or other options.

Four options are considered here:

1. Always let MSO expire; no push. Under this option, an Issuing Authority will not initiate ("push") any updates to an mDL. Any update is always initiated by a request from the mDL holder.
2. Always let MSO expire; no push. Under this option, an Issuing Authority will not initiate ("push") any updates to an mDL. Any update is always initiated by a request from the mDL holder. However, the Issuing Authority does inform the mDL holder via a notification that an update is available.
3. Limited push: To minimize privacy concerns, the push action is limited to preventing the app from sharing information (via an ISO/IEC 18013-5 compliant interface) with any mDL verifier. At the same time, the mDL holder is notified of the action and of the availability of an update. The app can still be opened (there is no change to the app access control method), the mDL holder can still view all mDL information, and can request an update.
4. Full push: This push action is initiated by the Issuing Authority. Depending on the scenario, this can:
   a. Delete all mDL information (including the MSO, all logs, and all metadata), leaving only the app.
   b. Update the mDL to reflect a change in information. The mDL holder is also notified of the update.

The same four options can also be described as shown in the following table:

#	Option	Issuing Authority action	mDL holder action
1	No push (1)	No action required.	If mDL holder selected automatic updates: Do nothing; updated information will be obtained with next automatic update initiated by mDL app. If mDL holder did not select automatic updates: Manually request update when mDL is needed and MSO has already expired.

#	Option	Issuing Authority action	mDL holder action
2	No push (2)	Send notification to mDL holder that an update is available.	If mDL holder selected automatic updates: Do nothing; updated information will be obtained with next automatic update initiated by mDL app. If mDL holder did not select automatic updates: Manually request update when mDL is needed and MSO has already expired. In addition to the two courses of action above, the mDL holder can also decide to manually request an update upon receipt of notification from Issuing Authority.
3	Limited push	Send to mDL: 1. Instruction that prevents app from sharing mDL information with mDL reader. 2. Notification to mDL holder (about action taken and that update is available).	If mDL holder selected automatic updates: Do nothing; updated information will be obtained with next automatic update initiated by mDL app. No mDL transactions are possible in the meantime. If mDL holder did not select automatic updates: Manually request update when mDL is needed. In addition to the two courses of action above, the mDL holder can also decide to manually request an update upon receipt of notification from Issuing Authority.
4	Full push	Send to mDL: 1. Update. 2. Notification of update.	No action required.

The options can be compared as reflected in the table below.

Evaluation criterion	#1 No push (1)	#2 No push (2)	#3 Limited push	#4 Full push
When phone gets stolen, period during which all mDL data remains potentially accessible[a]	Indefinitely	Indefinitely	Indefinitely	Until successful completion of the push action[b]
When phone gets stolen, period during which mDL remains potentially usable (for post-matched transactions)	Until the MSO expires	Until the MSO expires	Until successful completion of the push action[b]	Until successful completion of the push action[b]

Evaluation criterion	#1 No push (1)	#2 No push (2)	#3 Limited push	#4 Full push
When driving privileges get revoked[c], period during which driving privileges remain sharable (and will look valid to the mDL verifier)	Until the MSO expires	Until the MSO expires	Until successful completion of the push action[b]	Until successful completion of the push action[b]
Relative desirability as seen from a privacy advocacy point of view[d]. 1 = Least desirable; most privacy invasive; 5 = Most desirable; least privacy invasive	5	4.5[e]	1.5[f]	1

[a] The method by which access to the app is controlled is up to each Issuing Authority. The probability of unauthorized access depends on the strength of the access methods employed. An Issuing Authority should consider this probability when weighing this evaluation criterion against the other evaluation criteria.

[b] Push actions depend on the availability of a data connection to the mDL app.

[c] This also applies to other changes in mDL information, e.g. a change in address. In the context if the comparison in the table, driving privilege revocation is most relevant. If other scenarios are specifically important for an Issuing Authority (e.g. to be able to limit the number of devices on which a person can simultaneously hold an mDL, including when a person wants to move an mDL to a new device), additional evaluation criteria can be added. The comparison should remain the same though.

[d] The ratings provided are not definitive and should be reviewed considering each Issuing Authority's privacy environment.

[e] Sending a notification to a mDL requires a transaction between the Issuing Authority and the mDL holder. Any transaction generates data about a mDL holder. Consequently, Option 2 is seen as less desirable from a privacy point of view compared to Option 1 (which does not include this data point).

[f] Compared to Option 4, Option 3 is slightly more desirable since the mDL holder controls when the update to the mDL information is applied.

APPENDIX B: MANDATORY REQUIREMENT LIST; CERTIFICATION TYPE

The table in this appendix is a summary of requirements that are mandatory for Issuing Authorities that want to comply with the AAMVA mDL Implementation Guidelines.

The table also specifies, in the last column, the type of certification required if an Issuing Authority decides to join the AAMVA Digital Trust Service (DTS). In this column, "independent expert certification" means certification by an entity with proven expertise and whose daily operations are not under the control of the entity being certified. The information in the last 3 columns of the table is maintained by the AAMVA DTS Steering Committee. The current information applies specifically to states wanting to join the MVP version of the DTS. For the MVP, it is recognized that not all implementations may initially comply with all requirements, and that the DTS Steering Committee (with the necessary feedback to the AAMVA Board) has the flexibility to grant exceptions provided it does not undermine the tenets of the DTS.

Requirement	Page	Risk of non-compliance	Certification steps	Certification type
Issuing authorities electing to follow the guidance in this document must adhere to ISO/IEC 18013-5, including as qualified in this document.	9	Interoperability issues; security issues	Compare app/wallet against 18013-5. Requires test platform/certified reader, and detailed test plan	Independent expert certification
Issuing authorities must populate the standard ISO vehicle category codes in addition to populating the domestic information	20	Interoperability issue	Check IA-specific mapping document. Test using test platform / certified reader.	Self-certified Independent expert certification

Requirement	Page	Risk of non-compliance	Certification steps	Certification type
The issuing authority shall identify age questions that are common in its jurisdiction, and shall include in a mDL an age_over_NN statement for each of these ages for the mDL holder.	20	Less privacy preserving	Confirm existence of IA's common age questions.	Self-certified
			Confirm presence of common age statements in mDL	Independent expert certification
The mDL app must be capable of maintaining an audit log.	29	Less privacy preserving	Check mDL app functionality	Self-certified
Building on the requirements for a signature image in ISO/IEC 18013-1 and in the AAMVA Card Design Standard, the signature image must be an accurate and recognizable representation of the original signature.	23	Inability to use mDL signature to compare against physical signature	Check mDL app functionality	Self-certified
In case the request was received electronically, the mDL app must clearly convey what data was requested, and whether the mDL verifier intends to retain the information. If the request is presented in summarized form in the user interface (e.g. "Identity and driving privilege data" as opposed to "First Name, Last Name, DOB, Driving privileges"), means must be available to give the mDL holder visibility of the details of such a summarized form, both before and during a transaction.	28	Less privacy preserving Data retention w/o knowledge Less mDL holder control	Check mDL app functionality	Self-certified
			Check that the information released by a holder is actually all and only what is received by a verifier	Independent expert certification

Requirement	Page	Risk of non-compliance	Certification steps	Certification type
The mDL app must provide the mDL holder full control over which data elements to share with the mDL verifier.	28	Less privacy preserving Less mDL Holder Control	Check mDL app functionality	Self-certification
The app must support a graceful and informed exit from the request if the holder opts not to share the portrait image when requested.	28	Suboptimal user experience	Check mDL app functionality	Self-certification
If blanket sharing options are used, measures must be implemented to ensure that the mDL holder remains aware of what is being released when such an option is in effect. An mDL holder must also be able to opt out of or cancel any blanket sharing function.	28	Less privacy preserving Less holder control	Check mDL app functionality	Self-certification
mDL information must be stored in encrypted form.	29	Less privacy preserving	Requires test platform	Independent expert certification
Private key material must be protected in a security module designed for the safekeeping of key material.	29	Possibility of copying mDL to a different device Possibility of insecure transaction communication channel	Review detailed key management procedures	Independent expert certification
Issuing Authorities must not rely on device unlocking to protect mDL data, since this feature can be disabled by the mDL holder. The mDL app must require mDL holder authentication, separately from device unlocking, each time mDL data is accessed or released	29	Less privacy preserving	Check mDL app functionality	Self-certification

Requirement	Page	Risk of non-compliance	Certification steps	Certification type
mDL data must be released to an mDL verifier only via an ISO/IEC 18013-5 compliant interface.	29	Less privacy preserving Interoperability issues	Check mDL app functionality Test using test platform / certified reader.	Self-certification, possibly based on a written confirmation from the app vendor that the app complies with the requirement
The mDL app must be capable of maintaining an audit log.	29	Less holder visibility about activity	Check mDL app functionality	Self-certification
The mDL app must allow the mDL holder to decide if an audit log must be maintained or not.	29	Less privacy preserving	Check mDL app functionality	Self-certification
The audit log and related settings must be accessible only to the mDL holder	29	Less privacy preserving	Check mDL app functionality	Self-certification
The audit log must allow for the recording of all mDL transactions.	29	Less privacy preserving	Check mDL app functionality	Self-certification
At minimum, the following must be recordable for any transaction: Transaction timestamp; type of transaction (e.g. update or data sharing); in case of a data sharing transaction the data that was shared, and to the extent that it can be gathered, information about the identity of the mDL verifier.	29	Less privacy preserving Inability to know with whom mDL data has been shared	Check mDL app functionality	Self-certification

Requirement	Page	Risk of non-compliance	Certification steps	Certification type
Any synchronization features that are provided must adhere to the following: 1. Synchronization must be an option that can be enabled or disabled by the mDL holder. The process to enable synchronization must require the mDL holder to prove access to both devices. 2. Synchronization must occur directly between the devices in question. A synchronization action must not give visibility of any of the following to anyone other than the mDL holder: a. Audit log information. b. Audit log settings. c. The fact that a synchronization action/selection took place. d. Any information that may convey that the mDL holder has an mDL on more than one device.	29	Less privacy preserving	Check mDL app functionality	Self-certification, possibly based on a written confirmation from the app vendor that the app complies with the requirement
An mDL holder must have the capability to delete the mDL holder's mDL from the mDL holder's device. Such deletion: 1. Must delete all mDL information, log information, and any metadata (e.g. settings) that could impart information about the deleted mDL or its use. 2. Must not require approval by the Issuing Authority. 3. Must be an option available to a mDL holder on the mDL device.	30	Less privacy preserving Less holder control	Check mDL app functionality	Self-certification
It must not be possible for someone other than the mDL Holder or the Issuing Authority to delete (or suspend) a mDL.	30	Less privacy preserving Less holder control	Check mDL app functionality	Self-certification

Requirement	Page	Risk of non-compliance	Certification steps	Certification type
An mDL holder must have the capability to delete audit log information (as defined in section 4.4) the mDL holder may previously have elected to maintain.	30	Less privacy preserving	Check mDL app functionality	Self-certification
Any stakeholder (including Issuing Authorities, technology providers, service providers and mDL verifiers) must not track mDL Holders or the usage of any mDL except as required by law (e.g. when a drug store dispenses products containing ephedrine).	31	Less privacy preserving	Check mDL app functionality	Self-certification
care must be taken to minimize the sharing of static or long-lived metadata	31	Less privacy preserving	Check mDL app functionality	Self-Certification
An mDL must not allow access to the mDL information by anyone other than the mDL holder.	32	Less privacy preserving	Check mDL app functionality	Self-certification
An Issuing Authority must endeavor to provide full transparency to an mDL holder about all the features supported by an mDL app.	32	Holder misuse of app	Check mDL App functionality	Self-Certification
The mDL holder must at any time (i.e. during a transaction as well as outside a transaction) be able to view at least the following information if the mDL holder so chooses: • Data elements listed in Table 5 of ISO/IEC 18013-5. • The data elements appended to Table 5 of ISO/IEC 18013-5 by section 3.1 of this document. The contents of the `signed`, `validFrom`, `validUntil`, and `ex–pectedUpdate` (if present) data elements from the mobile security object (MSO).**Error! Reference source not found.**	28	Holder distrust of mDL content	Check mDL App functionality	Self-Certification/
Any push action must include an accompanying notification to the mDL holder.	34	Holder privacy concerns	Check mDL App functionality	Self-Certification/

Requirement	Page	Risk of non-compliance	Certification steps	Certification type
Issuing Authorities must continue to offer physical credentials to customers.	39	Inability for holder to prove identity	Review jurisdictional statutes/regulations for physical card issuance requirement	Self-Certification/
Issuing Authorities must therefore take care that the rendering of information on a mobile device does not create the impression that it can be used as a "flash pass".	39	Fraudulent use of credential	Check mDL App functionality	Self-Certification
Issuing Authorities must confirm at least two out of the following three authentication factors before concluding a remote provisioning process: 1. Something the mDL holder has. 2. Something the mDL holder is. 3. Something the mDL holder knows.	41	mDL provisioned onto a wrong device	Check jurisdictional provisioning procedures	Self-Certification
The authentication factors used must be independent of each other.	42	mDL provisioned onto a wrong device	Check jurisdictional provisioning procedures	Self-Certification
A remote provisioning process must not be used by an Issuing Authority to establish an identity record. Establishment of an identity record must occur in person.	42	Fraudulent record established	Check jurisdictional provisioning procedures	Self-Certification
The mDL record maintained by an Issuing Authority must include the following: All functional data elements provisioned to an mDL.	43	IA unable to confirm what was issued	Check IA issuance record for mDL	Self-Certification

Requirement	Page	Risk of non-compliance	Certification steps	Certification type
The mDL record maintained by an Issuing Authority must include the following: All supporting data provisioned to an mDL, e.g. cryptographic salts for message digests within the MSO.	43	IA unable to confirm what was issued	Check IA issuance record for mDL	Self-Certification
The mDL record maintained by an Issuing Authority must include the following: The current copy of the MSO (or MSOs) for the mDL holder's device (or for each of the mDL holder's devices, if active on more than one device at the same time).	43	IA unable to confirm what was issued	Check IA issuance record for mDL	Self-Certification
The mDL record maintained by an Issuing Authority must include the following: Public mDL cryptographic key material by which an mDL device can uniquely be identified.	43	IA unable to properly administer mDL issuance	Check IA issuance record for mDL	Self-Certification
The mDL record maintained by an Issuing Authority must include the following: Logs of an Issuing Authority's interaction with an mDL device. Logs must include the following: a. Timestamp b. Action performed. At least the following actions must be captured: i. Provisioning request (including key material and identifying information within the signing request) and outcome (successful / unsuccessful) ii. Deletion action, by whom initiated (Issuing Authority or mDL holder), and outcome (successful / unsuccessful) iii. Update action, by whom initiated (Issuing Authority or mDL holder), and outcome (successful / unsuccessful)	43	Inability to audit issuances	Check IA issuance record for mDL	Self-Certification

REVISION HISTORY

Release	Date	Name	Comments
0.1	2019/03/06	AAMVA	Initial release
0.2	2019/04/25	AAMVA	Added additional domestic data elements
0.3	2021/09/13	AAMVA	Updated to accommodate the final (FDIS) version of ISO/IEC 18013-5. Expanded to cover additional input from the mDL WG, a report (funded by the US Department of Homeland Security) on technical guidance for the implementation of mDLs under the REAL ID Act, the Future Identity Council, NIST, the Canadian Centre for Cyber Security, and topics raised by the ACLU.
1.0	2021/11/10	AAMVA	Updated to refer to the published version of ISO/IEC 18013-5. Applied updates based on reviews by the Joint mDL WG, and by AAMVA Associate members that are also members of ISO/IEC JTC1/SC17/WG10.
1.1	2022-07-29	AAMVA	Added Appendix B. Added mdoc definition. Editorial updates, including for logical consistency within the document. Update to cryptographic curves allowed for use by the VICAL provider. Added a requirement that an mDL holder must be able to opt out of any blanket sharing function. Specified the minimum content that an mDL holder must be able to keep in a transaction log. Added an exception to tracking in case required by law.

OUR VISION

Safe drivers
Safe vehicles
Secure identities
Saving lives!

American Association of
Motor Vehicle Administrators
4401 Wilson Blvd, Suite 700
Arlington, Virginia 22203
703.522.4200 | **aamva.org**