Mobile Driver License (mDL) Frequently Asked Questions (FAQ) for Law Enforcement

v2.4

September 2021

American Association of Motor Vehicle Administrators

4401 WILSON BLVD, SUITE 700, ARLINGTON, VA 22203 | 703.522.4200 | aamva.org

Contents

Introduction

The intention of this document is to provide Law Enforcement with answers to the most frequently asked questions regarding Mobile Driver License (mDL). This document is intended to compliment other AAMVA mDL resources.

This document provides responses based on ISO standards compliant mDL solutions to frequently asked questions. Non-ISO compliant solutions are not considered a part of the responses below. Officers in jurisdictions (or neighboring jurisdictions) that have implemented non-ISO compliant solutions should reach out to the appropriate issuing authority and refer to local laws for information pertaining to the use and acceptance of these products.

1. Resources

The following is a list of AAMVA and non-AAMVA Resources that are available to assist in providing more detailed information on mDL:

Item	Details	Location
Functional Needs White Paper	Outlines the functional needs that a mobile driver license/ID solution needs to be safe, secure, privacy centric and interoperable. This document was used by ISO in the creation of the standard, as well as the baseline for AAMVA's Implementation Guidelines.	https://www.aamva.org/mDL-Resources/
Mobile Driver License Implementation Guidelines	Prescribes domestic (U.S. and Canada) requirements and best practices for mDL. This document is to be used as a companion document to the ISO/IEC 18013-5. The Joint mDL Working Group is making significant edits to this document and the older version has been pulled from the site.	Once the updated version is available it can be found at: https://www.aamva.org/mDL-Resources/

ISO/IEC 18013-5 Mobile Driving License (mDL) Application	Prescribes the requirements that must be met to implement interoperable mDL solutions. Specifically, this document addresses the functionality between the holder device and the reader device. ISO is working to publish this document in fall 2021.	Once this document is published, it will be available for purchase at: https://www.iso.org/standard/69084.html
Mobile Driver License Model Legislation	Offers guidance and recommendations and considerations to jurisdictions on creating and updating legislation to allow for mDL. The Joint mDL Working Group is making significant edits to this document and the older version has been pulled from the site.	Once this document is published it will be available for purchase at: https://www.aamva.org/mDL-Resources/
Mobile Driver License Procurement Guidance	Offers guidance, recommendations, and considerations to jurisdictions on procurement for mDL.	https://www.aamva.org/mDL-Resources/
Mobile Driver License Testing Guidelines	The Joint mDL Working Group is currently working on this document. There is no estimated time of publication.	Once the updated version is available it can be found at: https://www.aamva.org/mDL-Resources/
Mobile Driver License Training Modules	The Joint mDL Working Group is currently working on a series of training modules for Issuing Authorities and Law Enforcement. The training consists of a set of general	Once the modules are available, they can be found at: https://www.aamva.org/mDL-Resources/

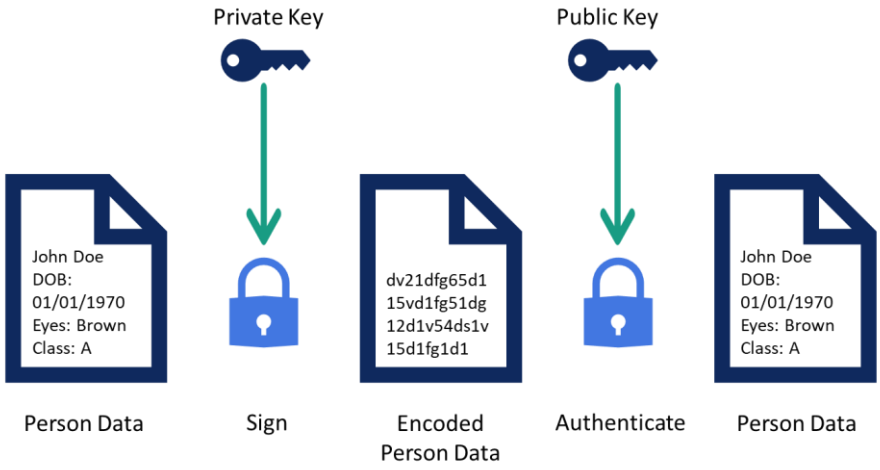
	modules that will help viewers establish a base knowledge of mDL, as well as a set of more targeted modules that will meet the needs of different skill sets, job functions and needs etc. The training modules are pre-recorded allowing viewers the flexibility to take what they need on their own time. Training modules will be rolled out monthly after the initial module is posted. There is currently no estimated time of completion on when training modules will be posted.	

2. Glossary

The following is a list of terms and abbreviations used in this document, and a description to ensure common understanding for readers.

Term/Acronym	Description/Explanation
Authentication	The process or action of proving the mobile driver license or ID to be true, genuine, and valid.
Credential	Driver license or ID issued by the issuing authority.
Data Element	Any unit of data defined for processing is a data element (i.e. first name, address, height, license class etc.)
Digital	Data that represents other forms of data using specific machine language systems that can be interpreted by various technologies.

Electronic Transmission	Any form of communication not directly involving the physical transmission of paper that creates a record that may be retained, retrieved, and reviewed by a recipient.
Flash Pass	The act of showing a digital representation of a DL/ID on a mobile device. (Not supported by ISO standard or AAMVA Implementation Guidelines.)
Functionality	The range of operations that can be run on a computer or other electronic system.
Interoperable	The capability of exchanging data via a common set of exchange formats, allowing mDL information to be shared between the mDL holder and the relying party.
Issuing Authority	The jurisdictional entity responsible for issuing driver licences or identification cards.
ISO	International Organization of Standardization
mDL Holder	Person to whom the mDL is issued by the issuing authority.
mDL Reader	The device/software used to authenticate and retrieve the mDL data from the mDL holder's device.
Mobile Device	A piece of portable electronic equipment that can connect to the internet (i.e. smart phone, tablet, or laptop).
Mobile Driver License (mDL)	DL/ID data stored in a digital format on a mobile device.
Offline (AKA device retrieval)	Not controlled by or directly connected to a network.
Online (AKA server retrieval)	Controlled by or connected to a network.
PDF417 Barcode	Portable Data File (PDF) stacked linear barcode format. Specifically, in the case of physical credentials the PDF417 barcode contains encoded credential information and can be read by verifiers to receive credential data. *Example:* 
Private and Public Keys	Digital equivalent of a physical key. Keys come in pairs. When data is signed by one of the keys in a key pair, only the other key can be used to authenticate the data. In the case of an mDL, the mDL data is signed by the key held only by the Issuing Authority. This key (the "private key") is protected very securely

	to ensure that only the Issuing Authority can use it. The other key (the "public key") is distributed widely. Verifiers use the public key to confirm that (a) the mDL data has not been changed since issuance, and (b) the mDL was issued by the actual Issuing Authority. 
Provision	Securely loading mDL data onto the device.
QR Code	Matrix barcode. In the case of mDL the QR code doesn't contain any credential information, it only contains enough information to establish a secure connection. *Example:*
Standards Compliant	Meets the ISO/IEC 18013-5, and AAMVA Implementation Guidelines requirements for interoperability.
Verifier	The entity using a mDL reader to retrieve data from the holder's device (also referred to as a "relying party").

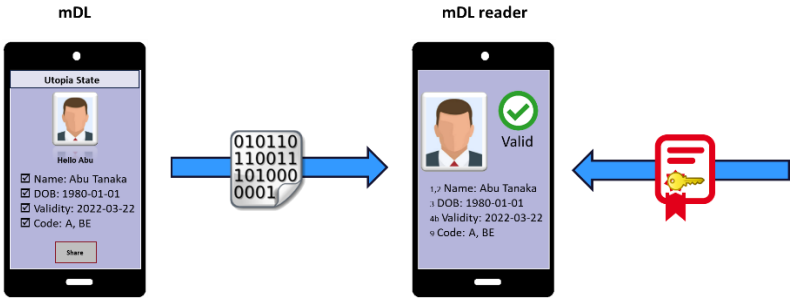
3. Overview of Mobile Driver License

What is mDL?

An mDL is a driver license (or ID card) that is provisioned to a mobile device with the capability to be updated in real time. It is comprised of the same data elements that are used to produce a physical driver license and can be read by an electronic reader.

The ISO standards effectively create solution guidelines for mobile identity with additional driver privilege attributes.

A mDL leverages a mobile device to securely transmit credential information to a reader device that authenticates the information electronically.



At transaction time, both the mDL and mDL reader can operate offline. The credential information is stored in a secure container on the phone and transmitted regardless if there is no, or poor cellular signal. In addition to the offline case, some jurisdictions may choose to support an online model (referred to at server retrieval); however, this method of transacting is not recommended by the standards community due to the privacy implications introduced. A standards compliant solution is required to support the offline option.

With mDL there's no need for law enforcement to handle, or otherwise touch the device. Officers will retrieve credential data from the holder's device using a reader application.

What mDL is NOT

As stated above, mDL is in interactive driver license (or ID Card) provisioned to a mobile device that can be updated, cancelled, revoked, etc. in real time; to that extent, mDL is <u>not</u> a picture of a driver license on a phone. Digital solutions that require the credential holder to 'show' a verifier their phone to obtain information visually (flash pass concept, such as how physical credentials are shared today) or the verifier to scan a PDF417 barcode[1] (to receive credential information), carry significant risk and vulnerabilities for fraud and counterfeiting beyond what's seen today with physical credentials.

[1]**Note:** This reference pertaining to a scan of the PDF417 barcode to receive credential data (as done today with physical credentials) should not be confused with scanning a QR Code to securely connect the reader to the mDL holder's device. The QR code does not contain any credential information, it only contains what needed to establish a secure connection.

Functional Requirements

The functional requirements for mDL were developed with privacy and security at the core. High level requirements prescribe that the mDL must:

Requirement	Explanation
Confirm Identity	Have the ability to confirm the identity of the holder.
Convey Driving Privileges	Have the ability to convey driving privileges, and other credential information. *Note – other types of attributes such as a fishing license or concealed weapons permit could also ride on the identity to offer a mobile solution.*
Trustable	Offer verifiers the ability to trust that the data is accurate and has not been tampered with. The trust anchor for the mDL solution is the electronic authentication that occurs as a part of the transaction. This allows the verifier to know that the mDL was issued by a legitimate issuing authority.
Interoperable	Offer verifiers the ability to transact with an mDL using a standards compliant mDL Reader.

Selective Information release	Allows the holder to provide only the data needed for the transaction. For example – The bartender only needs to know that the holder is old enough to buy alcohol; the holder's exact DOB and address aren't needed. With selective information release, the holder would have the ability to share that they are over 'X' years of age without sharing any other information from their credential.
Attended Use	Face to face use case (in person transactions).
Unattended Use	Online use case (internet transactions).
Remote Management	Offer the issuing authority the ability to remotely manage the credential. This would include updating information on the credential and revoking the credential etc.
Work Offline	Work in situations where there is no connectivity/cell coverage.

General/Miscellaneous

Some innovations and features for mDL solutions are not required as a part of the ISO/IEC 18013-5 standard, but would offer additional benefits to the mDL implementation, such as the use of a biometric, or a combination of features required for the holder to access the mDL on the device. Features such as these are dependent on and will vary based on the issuing authority's implementation.

4. Frequently Asked Questions (FAQ)

(1) Why the move to a mobile digital device vs. the current physical identity credential?

Placing identification on a mobile digital device provides a method for the identification information to be verified with the issuance source in almost "real time". This results in more secure, up-to-date, and reliable identification, which in-turn enhances public, highway, and officer safety. For more information regarding mDL benefits visit (video): https://www.youtube.com/watch?v=Oy1hyQ_gE0k.

mDL technologies help to solve several of the identification problems encountered today with physical credentials and offers improvements for:

Benefit	Explanation
Trust from the source	Uses the issuing authorities public key to authenticate the credential.
More efficient way to obtain information	The electronic transmission of data allows for the officer to receive the credential information without taking anything from the driver.
Time savings	Can significantly reduce the time at roadside.
Reduces the risk of identity theft	Measures in place to access the credential on the device such as a pin code or biometric, or combination of features will be required to access the credential. This means mobile credentials can't effectively be lost or stolen.
Data minimization to deter identity crimes	Holders only need to share the data needed for a transaction reducing the risk of overexposing sensitive information.
Counterfeit deterrence	The mDL will make it more difficult for counterfeiters to produce convincing credentials because the transaction will electronically authenticate the credential using the issuing authority's private and public keys.
Data accuracy	The information on the credential is dynamic, and digital, meaning information such as a name or address change could be reflected in real time. Issuing authorities would also have the capability of removing driving privileges in cases where the person's privileges are revoked or withdrawn, while leaving the identity part of the credential available to the holder to use as ID.

(2) What will an officer need to interact with mDL information?

Officers will need a reader device (i.e. smart phone, tablet, laptop etc.) to interact with mDLs.

(3) Will the officer see a list of potential mDLs to transact with in the reader app?

The officer will not know if the individual has an mDL until the individual offers it as proof of DL/ID.

(4) How does the officer's reader device connect with the mDL of interest?

The mDL technology requires the holder device and reader device to establish a secure connection (prompted by the holder) before data can be transmitted.

(5) How will officers collect information for more than one mDL at a time?

Currently mDL technology does not support the collection of more than one credential at a time.

(6) How will officers know that the mDL data received is for the person they're interacting with?

The holder's photo will be a part of the data that is transmitted to the reader device.

(7) How will officers know that the mDL is authentic (from an issuing authority)?

Authentication occurs during the electronic transmission of data. If authentication fails (meaning it could not be confirmed that the credential was produced by a jurisdiction issuing authority) then a message will be displayed on the reader device. If authentication passes, then the data requested will display on the reader device. The officer authenticating the mDL will not have to look for security features to know the mDL is genuine. Instead, the mDL app will perform a check to see the credential is valid.

(8) Will the officer need to physically touch the mDL holder's device?

Officers do not need to touch the holder's device to obtain mDL information. The mDL information will be displayed on the officer's reader device after the connection has been made and the data has been transmitted.

(9) How will officers interact with mDL's that are from other states or countries?

mDLs that comply with international interoperability standards will allow the mDL to be read by an officer with a compatible mDL reader device.

(10) How will an officer receive information from an mDL if there is no cell coverage?

An mDL provides information without cell coverage. The mDL is stored in a secure container on the holder's device and can be transmitted to the officer's device offline.

(11) How will an officer receive information if the holder is not able to share the mDL or if the officer does not have mDL reader capabilities?

The mDL will be issued in addition to the physical credential for the foreseeable future. Officers should follow current procedures and request the physical identity credential.

(12) What is being done to prevent unlawful use and identity theft related to an mDL?

The mDL can be stored on the mobile device or app and the jurisdiction will require, at minimum, the holder to provide a code to access the data. While the access code provides a minimum level of security, it is likely issuing authorities would choose to implement solutions that require stronger security measures to protect the data such as biometrics or a combination of features.

5. Use Case Matrix

For ease of reference, this matrix outlines common use cases and explains/compares what happens today with the physical credential to what happens with mDL:

Use case	Physical Credential	Mobile Credential	Other/Comments/Notes
Traffic stop	Ask for driver license. Holder provides physical DL to the officer.	Ask for driver license. Holder will indicate they have an mDL. Use reader device to connect and send data request to the holder. Credential data will be sent to the reader device.	
Phone battery dies	N/A	Ask for the physical credential. If holder does not have the physical credential, they do not have proof of license/ID.	This is not any different than use cases today where the holder does not have their credential.
No cell coverage	N/A	mDL is stored in a secure container on the holder's device and can be transmitted to the officer's device offline (no coverage).	

Out of state drivers	Ask for driver license. Holder provides physical DL to the officer.	Ask for driver license. Holder will indicate they have an mDL. Use reader device to connect and send data request to the holder. Credential data will be sent to the reader device.	
Foreign drivers	Ask for driver license. Holder provides physical DL to the officer.	Ask for driver license. Holder will indicate they have an mDL. Use reader device to connect and send data request to the holder. Credential data will be sent to the reader device.	
Unresponsive, or incoherent individuals	Look for the physical credential.	Look for the physical credential.	For example: fatal crash, subject unconscious, etc.
Individuals with non-ISO compliant digital identity products	N/A	Ask for the physical credential. Follow agency communication protocols. If holder does not have the physical credential, they do not have proof of license/ID.	For example – pictures of a Driver License or ID card on the device, or another solution that uses electronic data transmission but is not interoperable.
Drivers without a license.	Follow agency protocols for driver's that do not have proof of license.	Follow agency protocols for driver's that do not have proof of license.	

6. Release History

Release	Date	Name	Comments
2.3	August 2021	M. Stephens	Document Published
2.4	September 2021	M. Stephens	Corrected mistake with image and made a minor change to definition in Glossary for Public/Private Keys.