NEW YORK STATE OF OPPORTUNITY. | Department of Motor Vehicles

6 EMPIRE STATE PLAZA • ALBANY, NY 12228

"P" 7 (2024)

"M" 7 (2024)

Albany, New York

June 11, 2024

TO: All Enforcement Agencies and Magistrates

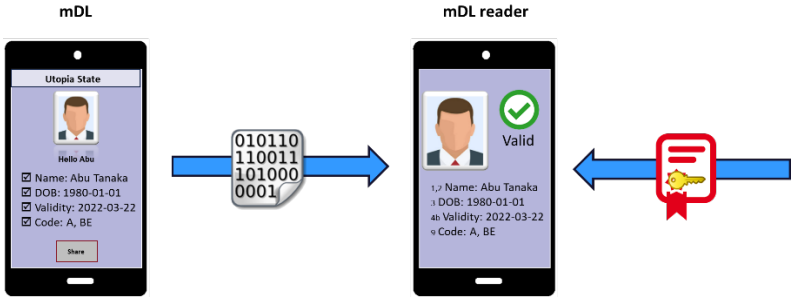
SUBJECT: New York Mobile ID (MiD)

Effective June 11, 2024, the New York State Department of Motor Vehicles (DMV) released the New York Mobile ID (MiD) application (app) for optional enrollment by any New Yorker who has a valid (not expired or revoked) driver license, learner permit, or non-driver ID card issued by DMV. For their own convenience and where it is accepted for use, New Yorkers may use MiD to present their identity data through a secure, encrypted exchange between their cell phones or other mobile devices such as tablets, and a reader device, using specific MiD reader apps.

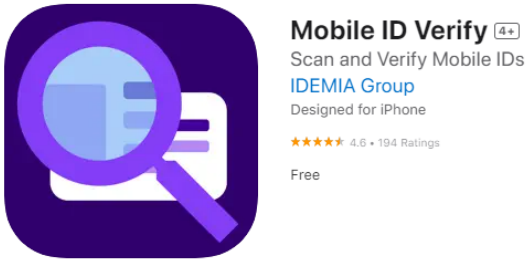
New York MiD is a standards-based interoperable digital identity credential that can be updated, cancelled, suspended, or revoked in real time. It is comprised of the same data elements that are used to produce a physical identity credential (driver licenses, learner permits, and non-driver ID cards) and can be read by an electronic reader. Several other states already offer similar forms of mobile credentials; their adoption and usage are growing nationally.

MiD is not a picture of a New York driver license, learner permit, or non-driver ID card on a phone.

MiD leverages a mobile device to securely transmit credential information to a reader device that authenticates the information electronically. To be acceptable as identification, the New York MiD ***MUST be authenticated electronically***. A court or law enforcement officer cannot authenticate the New York MiD simply by eyesight alone.



With New York MiD there is no need for law enforcement to handle, or otherwise touch the holder's device. Officers will retrieve credential data from the holder's device using a reader application. Various standards-based reader applications are available to be downloaded to a mobile device in the iOS and Google Play app stores, for use with both Apple iPhone and Android operating systems. This includes apps with no cost such as the "Mobile ID Verify" app produced by the developer IDEMIA Group.



New York DMV will continue to issue physical identity credentials and New York MiD holders should be in possession of that physical credential as required by law, including whenever they drive. Officers, following their own agency procedures, may accept MiD in place of a physical credential, they may accept only the physical credential itself, or they may request the physical identity credential if they are unable to electronically verify the MiD when produced by a holder.

Attached you will find "New York Mobile ID (MiD) Frequently Asked Questions for Law Enforcement – June 2024" to further assist your understanding of the adoption of and use of MiD in New York State. If you have any additional questions or need further information regarding the New York MiD, please contact the New York State DMV Division of Field Investigation at (518) 474-8805.

Please share this information with all appropriate staff. Thank you.

Mark J.F. Schroeder
Commissioner

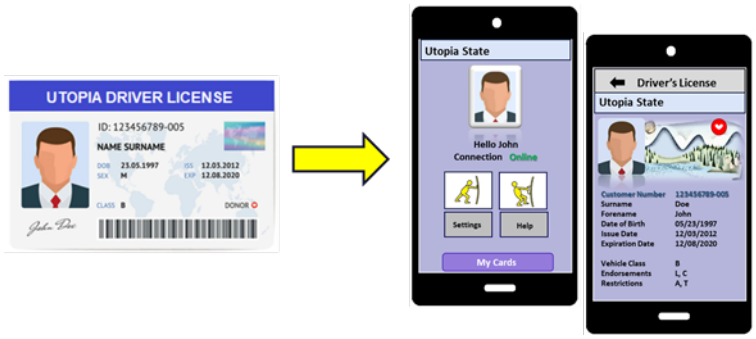
Attachment

New York Mobile ID (MiD) Frequently Asked Questions for Law Enforcement – June 2024

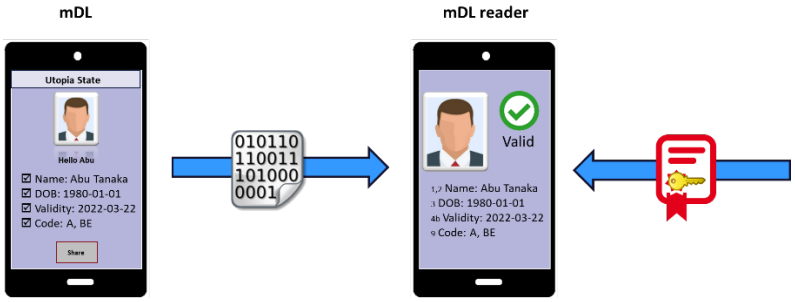
Introduction

What is New York Mobile ID (MiD)?

New York MiD is a standards-based interoperable digital credential that can be enrolled in by any New Yorker who has a valid (not expired or revoked) driver license, learner permit, or non-driver ID card issued by the New York State Department of Motor Vehicles (DMV). Updates to the credential such as name or address changes, revocations or suspensions are pushed to MiDs in real time. They are comprised of the same data elements that are used to produce a physical driver license and can be read only by a digital reader, which is usually an application (app) installed on another cell phone or other mobile device.



New York MiD leverages a mobile device to securely transmit credential information to a reader device that authenticates the information electronically.



At transaction time, both the MiD and MiD reader can operate offline. The credential information is stored in a secure container on the phone and transmitted even if there is no, or poor cellular and Wi-Fi signal. ***There is no need for law enforcement to handle or otherwise touch the holder's device.*** Officers will retrieve credential data from the holder's device using a reader application.

MiD is NOT a picture of a New York driver license, learner permit, or non-driver ID on a phone. The New York MiD is not designed to be *shown* to a verifier to obtain credential information visually. Nor is it intended for the verifier to scan a PDF417 barcode[1] to receive credential information. Digital credentials that are designed to appear like a digital picture of a physical credential carry significant risk and vulnerabilities for fraud and counterfeiting and should not be relied upon as identification.

[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 MiD holder's device. The QR code does not contain any credential information, it only contains what is needed to establish a secure connection between devices.

Frequently Asked Questions (FAQ)

(1) Why create a Mobile ID?

Placing identification on a mobile device provides a method to verify the credential information with the issuing authority (DMV) almost instantly. This results in more secure, up-to-date, and reliable identification, which in turn enhances public, highway, and officer safety. For more information regarding MiD benefits visit https://www.youtube.com/watch?v=KLa0-krQidA

The technology powering the New York MiD helps to solve several challenges encountered today with physical credentials and offers the following benefits:

Benefit	Explanation
Trust from the source	Uses the DMV's public key, contained in the MiD reader app or software, to authenticate the identity data transmitted from the MiD holder's device. The identity data has come from the DMV as the data was encrypted when placed on the device using DMV's private key for encryption.
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 on a traffic stop or in other law enforcement encounters.
Reduces the risk of identity theft	Measures in place to access the credential on the device such as a pin code or biometric identifier, or combination of features will be required to access the credential. This means MiDs are much more difficult to steal or spoof.
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 MiD will make it more difficult for counterfeiters to produce convincing digital identity credentials because the transaction will electronically authenticate the digital identity credential using the issuing authority's public and private keys.
Data accuracy	The information in the MiD is dynamic and digital, meaning information such as a name or address change could be reflected in real time. DMV also has the capability to remove driving privileges in cases where the person's privileges are revoked or suspended, while leaving the identity part of the credential available to the holder to use as an identification.

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

Law enforcement agencies will need to develop their own policies about whether and under what circumstances they will accept MiD in place of a conventional physical credential. Officers will need a reader device (e.g., smart phone, tablet, laptop) that contains a verification app or software to interact with MiDs.

Various standards-based reader applications are available to be downloaded to a mobile device in the iOS and Google Play app stores, for use with both Apple iPhone and Android systems. This includes apps with no cost such as the "Mobile ID Verify" app produced by the developer IDEMIA Group.

Mobile ID Verify 4+
Scan and Verify Mobile IDs
IDEMIA Group
Designed for iPhone
★★★★★ 4.6 • 194 Ratings
Free

There are also numerous vendors that also provide reader solutions that can be integrated in existing point-of-sale systems, another verification system, or platforms through a MiD software development kit (SDK).

(3) How does the officer's reader device connect with the MiD of interest?

The MiD technology requires the holder device and reader device to establish a secure connection (prompted by the holder) before data can be transmitted. This can be done by reading a QR code on the holder's device.

(4) How will officers collect information for more than one MiD at a time?

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

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

The holder's photograph will be part of the data that is transmitted to the reader device. It is still the responsibility of the officer to look at and use that photograph with the presenter as they would if presented a physical credential.

(6) How will officers know that the MiD is authentic and 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, the data requested will display on the reader device. The officer authenticating the MiD will not have to look for security features to know the MiD is genuine. Instead, the MiD app will perform a check to see the credential is valid.

(7) Will the officer need to physically touch the MiD holder's device?

No, the officer does not need to touch the holder's device to obtain MiD information. The MiD information will be displayed on the officer's reader device after the connection has been made and the data has been transmitted.

(8) How will officers interact with MiDs or similar electronic credentials that are from other states or countries?

MiDs and other similar electronic credentials that comply with international interoperability standards can be verified by any compatible reader.

(9) How will an officer receive information from the MiD if there is no cellphone coverage or Wi-Fi?

The MiD provides information without cellphone coverage or Wi-Fi. The MiD is stored in a secure container on the holder's device and can be transmitted to the officer's device offline through a Bluetooth connection.

(10) How will an officer receive information if the holder is not able to share the MiD or if the officer does not have a MiD reader?

Physical credentials will continue to be issued and holders should continue to carry them, especially when driving, even if they have a MiD.

Use Case Matrix

This matrix outlines common use cases and explains and compares what happens today with the physical credential to what happens with MiD:

Use case	Physical Credential	Mobile Credential	Other/Comments/Notes
Traffic stop	Ask for driver license. Holder provides physical driver license to the officer.	Ask for driver license. Holder will state they have MiD. 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 or identification.	This is not any different than use cases today where the holder does not have the credential.
No cell coverage	N/A	MiD 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 driver license to the officer.	Ask for driver license. Holder will state they have MiD or similar electronic credential. 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 driver license to the officer.	Ask for driver license. Holder will state they have MiD or similar electronic credential. 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 standard non-compliant digital credentials	N/A	Ask for the physical credential. Follow agency communication protocols. If holder does not have the physical credential, holder does not have proof of license or identification.	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 drivers who do not have proof of license.	Follow agency protocols for drivers who do not have proof of license.	