

## Mobile Driver License (mDL) Frequently Asked Questions – Law Enforcement

### Questions:

1. Why the movement and interest in having identification on a mobile digital device vs. the current plastic credential?

Law enforcement officers when presented an identification document typically verify the information contained on the document with the issuance source. This is a result of experience in realizing the information on the identification was current at the time of issuance but may not be any longer. For example, this validation with the issuance source may result in the officer learning the vehicle operator no longer has valid driving privileges. Placing identification on a mobile digital device provides a method for the identification to be verified by operationally authenticating the mDL information with a higher level of confidence than is the case for physical documents by anyone having the need to do so. This results in more secure, current, and reliable identification, in-turn enhancing public and highway safety.

2. Is the identification on the mDL stored inside the phone? If so, how is the identification secured to prevent unlawful use and identity theft?

Depending upon how the jurisdiction designs their mDL, all or a portion of the identity information may be stored on the digital device. This information is recommended to be stored within a digital device and app that is protected by levels of security measures (e.g., biometrics). Also, upon notification of a mobile device being lost or stolen, a driver license service center may potentially be able to remove the mDL app and accompanying information from the digital device preventing the potential for unlawful use of information. When the customer obtains a new digital device, the driver license service center may apply the mDL to the new device after secure validation. The current plastic credential, when lost or stolen, provides anyone who views it access to the subject's personal identifying information and allows for the continued victimization and illegal use of the credential.

3. Today I authenticate a plastic credential by observing covert and overt security features, how will I authenticate the mDL app?

An mDL is an interactive digital identity that will have security features (like cryptography) in place to protect access to the identity information and protocols for verification and validation of the information. Also, the officer authenticating the mDL will have information notifying them when the mDL was last updated with the issuance source, providing a higher degree of probability that the information is accurate. Additionally, the "verification and validation" is performed electronically by the officer's infrastructure, and not a visual verification of any physical security features.

4. When I interact with a subject on the roadside, I ask for the license, examine it, and may take it back to my police cruiser. Will I need to physically touch the device the mDL is on? How will I get identity

information from the mobile device to complete a citation or report? Am I responsible for damage I may cause to the device?

The process of how an officer obtains information from an mDL is currently in pilot and testing stages. Wireless technology such as Bluetooth Low Energy, Near-field Communication, WiFi Aware, and other solutions such as bar codes are being tested to allow for an officer to obtain mDL information through contactless methods. It is not necessary for an officer to have physical control of the mDL device to validate or obtain information from it. It is understood that officers need their hands free and shouldn't be required to have additional hardware to validate mDL's. For the near future, it is envisioned that an mDL will be issued in addition to, and not in lieu of, the plastic license - anyone operating a motor vehicle will still need to have the physical credential in their possession. This will allow for continued research in to how law enforcement will interact with the mDL. This is very important in light of the generally held position by subject matter experts that we will in the not too distant future see physical credentials start to disappear and experience an ever increasing electronic landscape when it comes to credentials (identification, registration, inspection, etc). Since it is not recommended officers physically touch the mDL device, there should not be a problem with officers damaging the device. Any interaction with the mDL digital device should follow standard department protocol for officer interaction with digital devices.

5. How will I interact with mDL's that are presented to me from other states or countries?

AAMVA has developed an mDL Functional Needs Whitepaper providing jurisdictions with guidance on the development of mDL's to encourage collaboration and cross jurisdiction/country interoperability: see link below. The focus of this document is to help jurisdictions design an mDL that can be utilized both within the jurisdiction and outside of it. Much like the plastic driver's license today, the goal of the mDL is to be accepted anywhere a plastic license is.

6. Where I work cell coverage is poor. How will I authenticate and obtain information from an mDL if there is no cell coverage?

The standardized solution supports mDL authentication when both mDL and the reader are offline.

7. What software and hardware will I need to use to authenticate the mDL and to obtain information from it?

How law enforcement will interact with the mDL is still in pilot and testing stages but it is recommended that no new hardware be required for law enforcement to authenticate the mDL. If law enforcement agencies provide smartphones to their officers currently, these may be able to be utilized as one method for validation of the mDL.

8. How will I obtain identity information if the mDL digital device is not operational?

It is understood that an mDL digital device needs power to operate properly and there may be times when the device doesn't operate as it should. The process used today by officers when someone doesn't have their plastic driver's license with them is recommended to be followed the same when interacting with mDL's that are not operational.

9. How will I obtain identity information from the mDL if it is locked or the holder is not cognizant?

This is an example of a test case to determine if there are secure methods for law enforcement and other first responders to obtain mDL information from the digital device in these situations. As mentioned in response to question #8, officers who are unable to obtain information from an mDL should follow standard procedures the same they do today if someone doesn't have their plastic driver's license with them.

10. How soon will I be seeing mDL's in use by the general public? How soon before the plastic license is no longer issued?

mDL's are already available in some jurisdictions on a limited basis. As mentioned in question #4, it is recommended that the mDL be issued as a supplement to the plastic license and it is recommended that a vehicle operator have their plastic license with them when operating a motor vehicle on the highway.

To learn more about mDL's, visit the following website:

<https://www.aamva.org/Mobile-Drivers-License/>