

LAW ENFORCEMENT mDL TOOLKIT

DOC-04

Operational Workflows

Step-by-Step Officer Guidance for mDL Verification

Audience	Patrol Officers, Supervisors, Field Training Officers
Purpose	Provides practical, scenario-based guidance for law enforcement officers on how to verify ISO/IEC 18013-5 compliant mDLs during traffic stops and other field encounters, and how mDL data integrates into downstream reporting workflows.
Published	April 2026 American Association of Motor Vehicle Administrators (AAMVA)

Read Before Deploying

Officers should not use this guidance until their agency has formally deployed a compliant mDL reader application and provided training on its specific use. This document describes general workflow principles applicable to ISO/IEC 18013-5 compliant solutions. Specific steps may vary based on the reader application and CAD/FBR system your agency uses.

Understanding the mDL Transaction

Before walking through specific scenarios, officers should understand three fundamental principles that govern every mDL interaction:

- **You will never need to handle the holder's phone.** All data transfer occurs wirelessly. The holder keeps their device. This is both an officer safety advantage and a privacy protection.
- **The holder must actively consent.** The holder's device will display what data you are requesting and require them to approve it before anything is transmitted. If they decline, the transaction ends.
- **The credential is cryptographically validated, not just displayed.** Your reader verifies the digital signature from the issuing DMV. A valid result means the data is authentic — not just visually convincing.

Traffic Stop: Step-by-Step Workflow

Phase 1: Pre-Approach

1. Complete standard pre-stop procedures (radio, CAD entry, etc.) per agency policy.
2. Activate your mDL reader application on your reader device before or during your approach to the vehicle. Having the app ready reduces dwell time at the vehicle window.
3. If using a two-device workflow (smartphone reader + MCT), confirm the reader device is paired and ready to transfer data to your MCT.

Phase 2: Initial Contact

4. Make initial contact with the driver using standard protocol.
5. Request identification. If the driver states they have an mDL: inform them you will read it wirelessly and they should open their mDL wallet app (Apple Wallet, Google Wallet, or their state's app). The driver does not need to hand you their device.
6. If the driver offers a physical credential, accept it and process normally — do not require them to produce an mDL instead.

Phase 3: mDL Verification

7. Ask the driver to display the QR code in their mDL app, or hold their device near your reader for NFC (depending on the method your reader app uses).

8. Scan the QR code or complete the NFC tap. Your reader app will establish an encrypted Bluetooth connection with the driver's device.
9. Your reader app will display a consent screen on the driver's device showing what data you are requesting. The driver must approve. If they decline, you cannot proceed with mDL verification — fall back to physical credential if available.
10. Once the driver approves, your reader app will display the verified credential data, including the driver's photo. Compare the photo to the person in front of you.
11. Check the validity indicators displayed by your reader app — license status (valid, suspended, revoked, expired), expiration date, and any displayed restrictions or endorsements.

Phase 4: Data Integration & Downstream Actions

12. If your reader app is integrated with your CAD/FBR system, mDL data should auto-populate the active incident, query fields, and any open report forms. Confirm the data populated correctly.
13. If using a two-device workflow, transfer or export the mDL data to your MCT per your agency's procedure.
14. Submit CIC/NCIC queries using the DL number captured from the mDL — this eliminates transcription errors that can cause missed hits.
15. Complete the stop using standard procedures. Issue citation, warning, or take other appropriate action. mDL data should auto-populate the citation form if your reader is integrated.

Officer Safety Advantage

An officer can verify an mDL from outside the vehicle window using QR scan from a safe distance. Some reader deployments support BLE engagement that can initiate from several feet away. Agencies should explore long-range engagement options to keep officers out of the window line as long as possible, while ensuring they are interacting with the correct mDL(i.e. differentiating between the driver's mDL vs. a vehicle passenger).

Downstream Report & Query Integration

The full value of mDL technology is realized when credential data flows automatically to downstream systems. The following table describes how mDL data supports specific officer actions:

Action	mDL Data Benefit	Without Integration
e-Citation	Name, address, DOB, DL number, and license class auto-populate citation fields	Officer manually reads and types all fields — error-prone and time-consuming
Crash/Accident Report	All involved party identity fields auto-populated; DL status confirmed at time	Manual transcription from physical credential under stress conditions

	of crash	
CIC/NCIC Query	DL number auto-submitted — eliminates transcription errors that cause missed hits on wanted persons	Officer manually reads DL number aloud or types — common source of errors
Arrest Report	Booking identity data sourced from cryptographically verified credential — reduces identity fraud at intake	Risk of incorrect identity data entering booking records
Vehicle Tow Log	Driver identity captured at time of tow for accurate record and notification	Manual data entry, often completed after the fact from memory or notes
Field Interview / Contact	Person contact accurately captured and linked to RMS master name index	Manual entry; subject may provide false information that goes unchallenged
DUI/DWI Investigation	Accurate subject identity and license status captured at initial contact; linked through investigation	Additional steps required to confirm identity and license status under time pressure

Handling Common Failure Scenarios

Officers will regularly encounter situations where standard mDL verification cannot be completed. The following guidance covers the most common scenarios:

Holder's Device Has No Battery / Is Damaged

Treat the same as a driver without a physical credential. If the driver has a physical credential, process normally. State law in most jurisdictions still requires drivers to carry a physical credential; verify your jurisdiction's current legal requirement.

Reader Cannot Establish Session (Technical Failure)

Fall back to physical credential verification or standard identification procedures. Document the reader failure and report it to your technology contact for troubleshooting.

Out-of-State or International mDL

Any ISO/IEC 18103-5 compliant reader should be able to validate mDLs from all 21+ participating U.S. jurisdictions so long as it has the jurisdictions' public keys. Your reader app should display the issuing state clearly. For international mDLs, check whether your reader app has international trust chain support — coverage varies by vendor.

Driver Declines to Share mDL Data

The holder has the right to decline the consent prompt on their device. If the driver declines: request their physical credential. If they have no physical credential, follow your agency's standard protocol for a driver without identification.

Reader Displays an Authentication Warning or Failure

If your reader app displays a warning that the credential cannot be authenticated (invalid signature, expired trust chain, etc.), do not treat the credential as valid. Document the failure. Treat the situation as if no valid credential was presented and follow agency policy. Do not attempt to manually verify a credential that your reader has flagged as potentially invalid.

Related Toolkit Documents

- **DOC-01:** Standards Overview — how the technology works
- **DOC-08:** Training Plan Framework — officer training curriculum
- **DOC-09:** mDL FAQ for Law Enforcement — quick answers to common questions