

LAW ENFORCEMENT mDL TOOLKIT

DOC-10

mDL FAQs for Law Enforcement

Mobile Driver License Frequently Asked Questions

Audience	All Law Enforcement Personnel
Purpose	Plain-language answers to the most frequently asked questions about ISO/IEC 18013-5 compliant Mobile Driver Licenses. Based on AAMVA mDL FAQ v2.6. All answers address ISO-compliant solutions only.
Published	April 2026 American Association of Motor Vehicle Administrators (AAMVA)

Introduction

This document answers the questions officers most commonly ask about mobile driver licenses. Answers are intentionally brief. For deeper guidance on any topic, follow the references at the end of each answer or consult the related toolkit documents listed at the end of this guide.

All answers address ISO/IEC 18013-5 compliant mDL solutions. Non-ISO compliant digital products are addressed in Q11.

WHAT IS AN MDL

Q: What is an mDL?

A: A driver license or ID card issued by the state DMV and stored on a mobile device. It contains the same data as a physical license and can only be verified by an mDL reader.

For more detail, see DOC-01: Standards Overview.

Q: What is NOT an mDL?

A: A photo of a license, a screenshot, a digital image, or a picture of the barcode on the back of a license. None of these can be verified by a reader and none are valid mDLs.

See DOC-09: mDL Officer How-To Guide, Section 1.

EQUIPMENT AND VERIFICATION

Q: What does an officer need to read an mDL?

A: An mDL reader app or device issued by their agency — one capable of authenticating and displaying mDL data. A smartphone without an approved reader app installed is not sufficient.

See DOC-02: Hardware & Software Requirements and DOC-03: Available Devices & Software.

Q: Does the officer need to touch the driver's phone?

A: No. The officer never touches the driver's phone. All data transfers wirelessly from the driver's device to the officer's reader.

See DOC-09: mDL Officer How-To Guide for step-by-step instructions.

Q: Will the officer see a list of mDLs from people nearby in the reader app?

A: No. The officer's reader cannot detect whether anyone nearby has an mDL. The driver must actively open their wallet app and present it.

Q: How does the officer confirm the mDL belongs to the person in front of them?

A: The driver's photo is transmitted with the credential. The officer compares it to the person — the same as with a physical license.

Q: How does the officer know the mDL is real?

A: The reader automatically checks the DMV's digital signature. If it passes, the data is verified. If it fails, the reader shows a warning — do not accept that credential.

See DOC-04: Operational Workflows for guidance on authentication failures.

CONNECTIVITY AND INTEROPERABILITY

Q: Does the officer need cell service or internet to verify an mDL?

A: No. mDL verification is fully offline — device to device. Internet is still needed for CIC/NCIC queries and submitting reports.

See DOC-02: Hardware & Software Requirements.

Q: Can the officer read mDLs from other states?

A: If the reader is ISO/IEC 18013-5 compliant and has been loaded with the issuing jurisdiction's public keys, it will authenticate the mDL. Not all jurisdictions are in every reader's trust store — if the reader cannot verify the credential, request the physical license.

See DOC-01: Standards Overview for the current list of participating states.

WHEN THINGS DON'T WORK

Q: What if the driver cannot share their mDL, or the officer has no reader?

A: Request the physical credential and follow agency procedures and applicable state law. Depending on jurisdiction, failure to produce a valid license may be a citable offense.

See DOC-09: mDL Officer How-To Guide, Section 4 for a full failure-scenario reference table.

Q: What if the driver presents a non-ISO compliant digital product — a phone screen showing a license image?

A: Request the physical credential and follow standard procedures. A visual display that cannot be read by an ISO-compliant reader is not a valid mDL.

See DOC-01: Standards Overview for an explanation of ISO compliance.

Quick Reference

Question	Short Answer
What is an mDL?	A real DMV-issued license on a phone — same data as physical, digitally signed.
Is a photo of a license an mDL?	No. Photos, screenshots, and barcode images cannot be verified.
What equipment is needed?	An agency-issued mDL reader app or device with Bluetooth, NFC, and QR scanning.
Touch the driver's phone?	Never. All data transfers wirelessly.
Can I detect nearby mDLs?	No. The driver must actively present it.
How do I confirm it's the right person?	Compare the photo on your reader to the driver.
How do I know it's real?	Your reader checks the DMV's digital signature automatically.
Need internet or cell signal?	No — verification is offline. Internet is needed for queries and reports.
Out-of-state mDLs?	Readable if the reader has that jurisdiction's public keys loaded. If not, request the physical license.
Driver can't share / no reader?	Request physical credential. Follow standard no-ID procedures.
Non-ISO digital product?	Request physical credential. Visual-only displays are not valid mDLs.

Related Toolkit Documents

- **DOC-00:** Portfolio Overview — master index of all toolkit documents
- **DOC-01:** Standards Overview — how mDL technology works and the national deployment landscape
- **DOC-02:** Hardware & Software Requirements — device and software specifications
- **DOC-03:** Available Devices & Software — current market landscape
- **DOC-04:** Operational Workflows — full step-by-step procedures and report integration
- **DOC-07:** Legal & Privacy Considerations — officer authority, data handling, CJIS
- **DOC-08:** Training Plan Framework — agency training curriculum
- **DOC-09:** mDL Officer How-To Guide — step-by-step instructional field guide

Based on AAMVA mDL Frequently Asked Questions for Law Enforcement, Version 2.6. For the most current AAMVA guidance, visit aamva.org/topics/mobile-driver-license.