

LAW ENFORCEMENT mDL TOOLKIT
DOC-01

Standards Overview

ISO/IEC 18013-5 & 18013-7, AAMVA Guidelines, and the National mDL Landscape

Audience	Law Enforcement Leaders, Technology Officers, Command Staff
Purpose	Provides a plain-language explanation of the technical standards underlying mDL technology, their implications for law enforcement, and the current state of mDL deployment across the United States.
Published	April 2026 American Association of Motor Vehicle Administrators (AAMVA)

What Is an mDL?

A Mobile Driver License (mDL) is a digital version of a state-issued driver's license or identification card that resides in a secure container on the holder's smartphone. Unlike a photo of a physical license or a simple barcode, a standards-compliant mDL is cryptographically signed by the issuing state DMV. This digital signature allows any authorized reader to verify — without contacting the DMV in real time — that the credential is authentic, has not been altered, and was issued by a trusted government authority.

An mDL is not a picture of a driver's license on a phone. It is an interactive credential that the holder actively presents, with data selectively shared only upon the holder's explicit consent. The holder's device must be unlocked and the holder must approve each transaction.

What mDL Is NOT

An mDL is not a screenshot, a PDF417 barcode scan, a photo, or a visual display of a license on a phone screen. Solutions requiring the holder to 'show' their screen carry significant fraud risk. This toolkit focuses exclusively on ISO/IEC 18013-5 compliant solutions that use cryptographic authentication.

ISO/IEC 18013-5: The In-Person mDL Standard

ISO/IEC 18013-5:2021 is the foundational international standard for mobile driver's licenses. It was published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It establishes the interface specifications for mDL presentation, authentication, and data exchange in proximity (in-person) scenarios — the primary use case for law enforcement.

A revised draft (ISO/IEC DIS 18013-5) is currently in the enquiry phase with ISO members and will replace the 2021 edition when finalized. Agencies should ensure procurement language requires compliance with the current version and includes provisions for updates.

Core Technical Components

Component	How It Works in Practice
Device Engagement	The mDL session is initiated when the officer's reader scans a QR code displayed on the holder's screen, or when the officer's reader device performs an NFC tap against the holder's phone. This establishes the encrypted communication channel.
BLE Data Transfer	After engagement, credential data is transferred over Bluetooth Low Energy (BLE). This is a short-range, encrypted wireless channel. The officer never needs to handle the holder's device.
Offline Operation	The entire transaction — engagement, transfer, and validation — can be completed with no internet connection. The credential data is stored on the holder's device and the reader validates it using pre-loaded public

	keys from AAMVA's Digital Trust Service.
Cryptographic Validation	The reader verifies the mDL's digital signature against the issuing state's public key. This confirms (a) the data was not altered since issuance, and (b) it was issued by a legitimate DMV.
Selective Disclosure	The officer's reader requests specific data elements (e.g., name, DOB, DL number). The holder's device presents only those fields. Address, vehicle restrictions, or other data not requested are not transmitted.
Holder Consent	The holder's device displays the data elements being requested and requires the holder to actively approve before any data is transmitted. The holder can deny the request.

Privacy Protections Built Into the Standard

ISO/IEC 18013-5 was explicitly designed with privacy as a core principle, not an afterthought. Key protections include:

- No centralized transaction logging — the standard does not include any mechanism for a central database of mDL verification events. Verification is peer-to-peer.
- No real-time DMV notification — when an officer reads an mDL, the issuing state's DMV is not notified. There is no "phone home" functionality in the standard itself.
- Selective disclosure — only the data elements requested and approved are transferred. The full credential is not exposed.
- Holder-controlled — the holder must actively unlock their device and approve every transaction.

Note on Privacy Risks

While the standard itself is privacy-protective, individual mDL wallet apps or reader software could be built with additional logging or data retention. Agencies should review vendor privacy policies and confirm that reader applications do not create surveillance capabilities beyond what is operationally necessary. See DOC-07 (Legal & Privacy Considerations) for detailed guidance.

ISO/IEC 18013-7: Online mDL Verification

ISO/IEC Technical Specification 18013-7:2025 extends the mDL framework to remote/internet-based verification scenarios. While the primary law enforcement use case remains proximity-based (in-person), Part 7 is relevant for agencies planning software systems with multi-year lifecycles.

AAMVA's mDL Implementation Guidelines v1.6 (July 2026) incorporated guidance for Part 7, including reference to the W3C Digital Credential (DC) API currently under development by the World Wide Web Consortium. Procurement language for any software expected to be in service beyond 2027 should reference both standards.

Feature	ISO/IEC 18013-5 (Part 5)	ISO/IEC 18013-7 (Part 7)
Scenario	In-person, proximity verification	Remote, internet-based verification
Primary LE Use Case	Traffic stop, arrest, field interview	Remote identity verification, online case management
Connectivity Required?	No — fully offline capable	Yes — internet connection required
Device Engagement	QR code or NFC tap	QR code / browser redirect / DC API
Data Transfer Protocol	Bluetooth Low Energy (BLE)	HTTPS / W3C DC API
LE Readiness	Deploy now — market solutions available	Emerging — include in long-term procurement planning

AAMVA mDL Implementation Guidelines

The American Association of Motor Vehicle Administrators (AAMVA) is the primary coordinating body for mDL programs across U.S. and Canadian jurisdictions. AAMVA's mDL Implementation Guidelines (current version: 1.6, July 2026) expand upon ISO/IEC 18013-5 to define the specific data elements, privacy requirements, and trust infrastructure applicable to the North American mDL ecosystem.

Compliance with AAMVA guidelines — not just ISO/IEC 18013-5 — is required for an mDL reader to be interoperable with the full range of U.S. and Canadian jurisdictions. Any reader that is only "ISO-compliant" without AAMVA DTS integration may fail to validate credentials from many states.

AAMVA Digital Trust Service (DTS)

AAMVA operates the Digital Trust Service — the infrastructure through which issuing authorities' public keys are distributed to verifiers. An mDL reader should receive mDL public keys from the DTS to cryptographically authenticate credentials from any state. Using public keys from the DTS, a reader can confirm whether an mDL was issued by a legitimate issuing authority, it was provisioned to the device being presented, and the data has not been tampered with or altered.

- All agencies procuring mDL reader solutions should confirm that the vendor is integrated with the AAMVA DTS.
- DTS integration should be verified during procurement, and vendors should provide documentation of current DTS integration status.

Key AAMVA Resources for Law Enforcement

- **mDL Implementation Guidelines v1.6 (July 2026):** aamva.org/topics/mobile-driver-license
- **mDL FAQ for Law Enforcement (January 2024):** aamva.org/law-enforcement/mobile-driver-license-faq

- **mDL Model Legislation:** aamva.org/policy/legislation/model-legislation
- **mDL Jurisdiction Map (live deployment tracking):** aamva.org/topics/mobile-driver-license

National mDL Deployment Landscape

As of April 2026, mDL adoption across the United States has reached a critical threshold. An estimated 76% of Americans live in states that have adopted or are piloting mDL programs.

States with Active TSA-Recognized mDL Programs (as of early 2026)

The following 21 states plus Puerto Rico have active mDL programs recognized by TSA for airport checkpoint use. Officers in these states have the highest immediate likelihood of encountering mDL holders:

State
Arizona
California
Colorado
Delaware
Georgia
Hawaii
Illinois
Iowa
Kentucky
Louisiana
Maryland
Montana
New Mexico
New York
North Dakota
Ohio
Puerto Rico
Utah
Virginia
West Virginia

Rapid Growth

The AAMVA mDL map is updated frequently as new jurisdictions complete deployment. Officers should expect to encounter mDLs from states other than their own — especially in jurisdictions near state borders or with high tourism and travel activity.

Glossary of Key Terms

Term	Definition
mDL	Mobile Driver License — a digital driver's license or state ID credential on a mobile device compliant with ISO/IEC 18013-5.
ISO/IEC 18013-5	The international standard governing in-person mDL presentation and verification. The primary standard for law enforcement mDL encounters.
ISO/IEC 18013-7	A technical specification extending 18013-5 for internet-based (online) mDL verification.
AAMVA	American Association of Motor Vehicle Administrators — coordinates mDL standards for North American jurisdictions.
DTS	AAMVA's Digital Trust Service — distributes Issuing Authority public keys to mDL verifiers.
BLE	Bluetooth Low Energy — the wireless protocol used for mDL data transfer between devices.
NFC	Near-Field Communication — short-range wireless technology used for mDL session initiation.
Selective Disclosure	The holder shares only the specific data elements requested — not the full credential.
Issuing Authority	The state DMV or equivalent agency that issues and digitally signs the mDL.
Relying Party / Verifier	The entity reading the mDL — in law enforcement contexts, the officer and their reader device.
PKI	Public Key Infrastructure — the cryptographic framework that enables mDL authentication.
mdoc	The ISO/IEC 18013-5 term for a signed digital document (mobile document) format used for mDLs and other credentials.

Related Toolkit Documents

- **DOC-02:** Hardware & Software Requirements — technical specifications for compliant readers
- **DOC-03:** Available Devices & Software — current market landscape

- **DOC-07:** Legal & Privacy Considerations — state law, data retention, CJIS, and Fourth Amendment
- **DOC-09:** mDL FAQ for Law Enforcement — plain-language answers to common officer questions