

LAW ENFORCEMENT mDL TOOLKIT
DOC-02

Hardware & Software Requirements

Technical Baseline Specifications and Integration Architecture

Audience	Technology Officers, IT Staff, System Administrators
Purpose	Defines the minimum hardware and software requirements for ISO/IEC 18013-5 compliant mDL verification, describes integration architecture options, and outlines CJIS compliance obligations for law enforcement deployments.
Published	April 2026 American Association of Motor Vehicle Administrators (AAMVA)

Minimum Hardware Requirements

Any device used to verify ISO/IEC 18013-5 compliant mDLs must support all three of the following communication technologies. These are non-negotiable technical minimums — a device lacking any one of them cannot establish a compliant mDL session.

Requirement	Technical Detail	Notes
Bluetooth Low Energy (BLE)	BLE 4.0 minimum; BLE 5.0 or higher recommended for range and stability. Required for the primary data transfer session.	Present on virtually all smartphones and tablets made after 2015
Near-Field Communication (NFC)	NFC ISO 14443 compliant. Used as one of two device engagement initiation methods. Range typically <4 cm.	Confirm NFC is enabled on device — some enterprise MDM profiles disable it
QR Code Reader (Camera)	Rear-facing camera with autofocus capable of scanning QR codes. Alternative to NFC for device engagement. Most modern smartphones qualify.	Some purpose-built scanners use integrated laser/imager instead of camera
Operating System	iOS 16.5 or later (iPhone 8 or later) for Apple devices; Android 8.0 or later for Android devices. Windows 10/11 for MCT-based solutions.	Confirm OS version requirements with specific reader app vendor
Cellular Connectivity (Conditional)	Not required for mDL verification itself, which operates offline. Required for CIC/NCIC queries and CAD/FBR data submission.	Vehicle-mounted hotspot can serve multiple officer devices

Verify NFC Separately From Hardware

A device may have NFC hardware but have it disabled by Mobile Device Management (MDM) policy or carrier settings. Before deploying reader apps, confirm NFC is enabled and accessible to third-party apps on every device in the fleet.

Software Requirements

Hardware alone is insufficient. The software stack running on the reader device must accomplish five distinct functions to provide a complete, operationally useful mDL verification capability:

Function	Description & Verification Question
mDL Session Management	Initiates the engagement (QR scan or NFC tap), negotiates the encrypted BLE session, requests specific data elements, receives the mDL response, and closes the session. ASK VENDOR: What engagement methods are supported? Is BLE session handling

	compliant with ISO/IEC 18013-5 Section 8?
Trust Chain Validation	Validates the mDL's digital signature against AAMVA's Digital Trust Service public keys. Without this, the software cannot confirm the credential is authentic. ASK VENDOR: Is the application using issuing authorities' public keys obtained from the AAMVA DTS?
Data Display & Photo Comparison	Presents parsed mDL data clearly to the officer, including the credential photo for identity comparison against the physical holder. ASK VENDOR: What data elements are displayed? Is the portrait/photo displayed? Are validity indicators shown?
Data Export / Integration	The most operationally critical capability: passing mDL data to CAD, FBR, RMS, and query systems. Without this, officers must re-enter data manually. ASK VENDOR: What API, SDK, or integration mechanism is available? Which CAD/FBR systems are already integrated?
CJIS Compliance	Any software interfacing with Criminal Justice Information must comply with the FBI CJIS Security Policy. ASK VENDOR: Provide your CJIS Security Policy compliance documentation and your current CJIS Information Security Agreement (ISA).

Integration Architecture

The decision of how to deploy mDL readers within your existing technology stack is the single most important infrastructure planning decision. Two primary architectures exist:

Architecture A: Unified Device (Long-Term Integration)

A single ruggedized device — such as a 2-in-1 tablet, purpose-built handheld, or future-generation MCT — serves as both the mDL reader and the officer's primary computing terminal. The CAD/FBR/RMS software and the mDL reader application either run natively together or communicate directly on the same device OS.

Advantages	Considerations
Single device to manage, provision, and support	Requires CAD/FBR/RMS vendor to support mDL integration natively or via SDK
No data hand-off between devices — reduced failure points	May require a new or upgraded MCT device if existing hardware lacks BLE/NFC
Streamlined officer workflow — one screen, one tool	Procurement and deployment timeline tied to CAD/FBR vendor integration roadmap
Lowest total cost of ownership at scale	Transition planning needed if replacing existing MCT fleet

Architecture B: Two-Device Workflow (Available Now)

A smartphone or standalone mDL reader device reads the mDL, then transfers data to the in-vehicle MCT or laptop via Bluetooth pairing, local Wi-Fi, or a vendor-provided data sharing mechanism. The officer runs queries and populates reports on the MCT using the transferred data.

Advantages	Considerations
Deployable immediately without modifying MCT/CAD software	Data hand-off reliability between devices must be confirmed in testing
Preserves existing MCT investment	Some manual re-entry may still be required for non-integrated fields
Lower initial procurement cost	Two devices per officer to manage, charge, and support
Allows agencies to begin mDL acceptance while long-term integration is planned	Higher total cost of ownership over time vs. unified device

CJIS Security Policy Requirements

The FBI Criminal Justice Information Services (CJIS) Security Policy governs the handling, storage, and transmission of Criminal Justice Information (CJI). Any mDL reader software that connects to, transmits data to, or receives data from CJIS systems — including CAD, RMS, NCIC, and state criminal history databases — must comply.

Key CJIS requirements relevant to mDL deployments include:

- **Encryption:** All CJI data in transit must be encrypted. Confirm the reader app – if directly integrated with CJIS-connected software or hardware - and any integration middleware use FIPS 140-2 compliant encryption.
- **Multi-Factor Authentication:** Access to systems containing CJI requires advanced authentication. Confirm MFA is implemented for officer login to integrated systems.
- **Audit Logging:** All access to CJI must be logged with user ID, timestamp, and action. Confirm the system maintains audit logs meeting CJIS requirements.
- **Personnel Security:** Personnel with unescorted access to CJI must have appropriate background checks. This includes vendor employees with system access.
- **Information Security Agreement:** All vendors accessing or processing CJI must execute a CJIS Information Security Agreement (ISA). Require this from all mDL reader software vendors before contract execution.

CJIS Compliance Is Non-Negotiable

An mDL reader that connects mDL data directly to NCIC/CIC queries or populates fields directly into an RMS must comply with CJIS Security Policy. Failure to enforce this requirement exposes the agency to potential loss of CJIS access. All vendor contracts should include CJIS ISA requirements, and compliance should be verified before deployment.

Device Procurement Checklist

Use this checklist when evaluating any hardware device for mDL reader deployment:

- ☐ Bluetooth Low Energy 4.0 or higher confirmed and enabled
- ☐ NFC capability confirmed and enabled (not disabled by MDM or carrier)
- ☐ Rear-facing camera with QR code scanning capability confirmed
- ☐ Operating system meets reader app vendor's minimum version requirement
- ☐ Device form factor appropriate for law enforcement field use (drop resistance, weather resistance, screen readability in sunlight)
- ☐ Battery life adequate for a full shift without recharging
- ☐ MDM/EMM compatibility confirmed for agency device management platform
- ☐ Integration path to CAD/FBR/MCT confirmed with software vendor

Related Toolkit Documents

- **DOC-01:** Standards Overview — detailed explanation of ISO/IEC 18013-5 technical components
- **DOC-03:** Available Devices & Software — current vendor market landscape
- **DOC-05:** Procurement Considerations & Strategy — solicitation language and contract requirements