

LAW ENFORCEMENT mDL TOOLKIT
DOC-05

Procurement Considerations & Strategy
Solicitation Requirements, Contract Language, and Adoption Pathways

Audience	Procurement Officers, Technology Officers, Command Staff, Contract Administrators
Purpose	Provides a framework for law enforcement agencies to plan and execute the procurement of ISO/IEC 18013-5 compliant mDL reader hardware and software, including mandatory requirements, suggested contract language, adoption pathway options, and total cost of ownership guidance.
Published	April 2026 American Association of Motor Vehicle Administrators (AAMVA)

Procurement Planning Principles

Procuring mDL verification technology requires balancing the urgency of immediate deployment (officers are already encountering mDL holders) with the strategic goal of full integration into existing CAD/FBR/RMS environments. Agencies that rush to deploy standalone readers without planning for integration may find themselves investing twice — once for the initial tool, and again for future integrations that can be contemplated and planned for now.

The guiding principle for all mDL procurement should be: acquire the capability that meets today's operational need while explicitly building the integration path into the contract.

Mandatory Requirements for Any Procurement

These requirements should appear as mandatory (pass/fail) criteria in all solicitations for mDL reader hardware or software. Proposals that do not meet all mandatory requirements should not advance to evaluation.

Requirement	Verification Method
ISO/IEC 18013-5 compliance (current version)	Vendor must provide compliance documentation or third-party certification. Specify requirement for update to future versions.
AAMVA mDL Implementation Guidelines compliance (current version)	Vendor must confirm and document compliance with current AAMVA guidelines, including data element handling and DTS integration.
AAMVA Digital Trust Service integration	Vendor must demonstrate active DTS use and confirm trust material is kept current. Test with credentials from at least three different states.
CJIS Security Policy compliance (for any system touching CJI)	Vendors proposing solutions that directly connect to CJIS systems and data must provide executed CJIS ISA or confirm willingness to execute before contract award. Review compliance documentation.
BLE, NFC, and QR engagement all supported	Demonstrate all three engagement methods in a technical demonstration. Test in the actual deployment environment (vehicle, outdoor conditions).
Data ownership — agency retains all transaction data	Include explicit data ownership language in contract. Vendor must deliver all agency data upon contract completion or termination.

Suggested Contract Language

Solicitation Standards Reference Language

"The offered solution shall be compliant with ISO/IEC 18013-5 (current version) and AAMVA's mDL Implementation Guidelines (current version) for in-person (proximity) mDL

verification, and shall support all device engagement methods specified therein (NFC, QR Code, and Bluetooth Low Energy). For software systems with a projected deployment lifecycle extending beyond 2027, the solution shall additionally comply with or provide a documented roadmap for compliance with ISO/IEC 18013-7 (online mDL verification). The vendor shall maintain synchronization with AAMVA's Digital Trust Service throughout the contract term. Any software component that stores, transmits, or interfaces with Criminal Justice Information shall comply with the FBI CJIS Security Policy, and the vendor shall execute a CJIS Information Security Agreement prior to contract execution. All data elements captured, stored, or transmitted through the offered solution shall be the property of [Agency Name], and the vendor shall deliver a complete export of all agency data upon contract completion, modification, or termination."

Adoption Pathway Options

Option A: Immediate Deployment — Smartphone Reader App

Deploy a compliant mDL reader application on agency-issued smartphones. This is the fastest path to mDL verification capability.

Benefits	Limitations
Can deploy in weeks, not months	Requires manual data re-entry into CAD/FBR without integration
Leverages existing device fleet (if smartphones issued)	Does not solve the core integration need long-term
OpEx model available — monthly per-device pricing	May create two-device workflow if smartphones are separate from MCT
Demonstrates capability to leadership while full integration is planned	Training must address both the reader app AND the manual data transfer workflow

Option B: Purpose-Built Portable Reader + MCT Integration

Deploy a dedicated portable mDL reader that can be worn or carried by an officer and that interfaces with the existing in-vehicle MCT. The reader captures the mDL and passes data to the MCT via the reader's integration interface.

- **Best for:** Agencies with a stable MCT/CAD environment where the MCT vendor does not yet offer native mDL integration but is capable of accepting data from a peripheral reader device.
- **Procurement note:** Require the handheld reader vendor and MCT/CAD vendor to both certify the integration in writing before award. Do not accept a statement that integration is 'possible' — require a demonstrated, tested integration.

Option C: Integrated CAD/FBR/MCT with Native mDL Support (Long-Term)

Incorporate mDL verification capability into the next planned hardware and software refresh cycle. Require any new CAD/FBR/RMS contract to include mDL integration as a mandatory deliverable.

- **Best for:** Agencies within 12-24 months of a CAD/FBR or MCT hardware refresh. Plan the mDL requirement now to ensure it is included in the next RFP.
- **Key action:** Contact your current CAD/FBR/RMS vendor now and ask about their mDL integration roadmap. Include mDL capability as a rated criterion in your next contract renewal or re-procurement.

Total Cost of Ownership

Agencies should evaluate mDL reader solutions on total cost of ownership over a 3-5 year lifecycle, not just initial acquisition cost. The following table identifies the full cost components to include in any cost analysis:

Cost Component	CapEx Model	OpEx / DaaS Model
Hardware Acquisition	One-time upfront purchase; agency owns devices	Monthly per-device fee; vendor owns devices
Software Licensing	Annual maintenance/license fees after initial purchase	Included in monthly subscription (confirm scope)
Cellular Data Plan	Monthly data plan per device	Often bundled — confirm data caps
Integration Development	One-time (or per-version) development cost to connect reader to CAD/FBR	May or may not be included — clarify upfront
Training (Initial + Ongoing)	Include in contract as a deliverable	Include in contract as a deliverable
Hardware Refresh / Replacement	Budget for ~30% annual replacement (loss, damage, failure)	Typically included in DaaS — confirm refresh cycle
AAMVA DTS Access	Confirm whether included in vendor pricing or separately billed	Confirm whether included in vendor pricing or separately billed

Related Toolkit Documents

- **DOC-03:** Available Devices & Software — current vendor landscape for market analysis
- **DOC-06:** Funding Strategies — grant programs and alternative funding for procurement
- **DOC-07:** Legal & Privacy Considerations — contract and legal requirements to include in solicitations