Procurement Guidance

For Mobile Driver License (mDL)

August 2018

American Association of Motor Vehicle Administrators

In the process of developing standards for a Mobile Driver License (mDL), the mDL Working Group (WG), a joint effort of the AAMVA Card Design Standards Committee (CDS) and the AAMVA Electronic Identity Working Group (e-ID), identified a need for procurement guidance for members. It borrows liberally from the good work done in the AAMVA System Modernization Best Practice and is meant as an aide that provides a good foundation to build on as necessary. For more information on AAMVA's mDL initiative click here. For more information on other AAMVA best practices click here.

The American Association of Motor Vehicle Administrators (AAMVA) is a nonprofit organization, representing the state and provincial officials in the United States and Canada who administer and enforce motor vehicle laws.

Address AAMVA
4401 Wilson Boulevard
Suite 700
Arlington, Virginia 22203

Telephone 1-703-522-4200

Fax 1-703-522-1553

Website http://www.aamva.org

AAMVA – Public Information

Do not share with or forward to additional parties except as necessary to conduct the business for which this document was clearly intended. If in doubt, contact the originator for guidance. If you believe that you received this document in error, please advise the sender, then delete or destroy the document.

Procurement Guidance for Mobile Driver License Program (mDL)

Depending on the approach to mDL implementation, multiple procurements may be required. After a jurisdiction has determined that a procurement is necessary, organizing and developing procurement documents that ultimately become contracts will take research and effort to complete. In writing any procurement document, whether it is for staff augmentation, data cleansing activities, an oversight vendor, or a complete build of a new system, attention to detail and a clear understanding of what is being asked are required. It is always a good practice to consider the role of a vendor or the "receiving" side of a procurement document — to be sure work statements are clear, specific deliverables are outlined, and all instructions are easy to follow. For example, a desire to have the mDL solution align with and comply with any AAMVA standards and/or guidance. Ultimately, a procurement strategy develops into a contract, one that should be managed and followed, so take the time to make the procurement document clear and as inclusive and detailed as necessary.

Procurement assumptions specific to mDL

The following are encapsulated in the AAMVA guidance being developed from the standardization work in ISO SC17/WG10. The existing physical DL/ID application processes will stay the same after incorporation of an mDL program. MVA's (along with all other relying parties) should accept the mDL just the same way that they would accept a physical DL/ID. The mDL is a derivative of the process of applying for a physical DL/ID and having undergone the required proofing. It is envisioned that the mDL will at a minimum have the same level of security (resistance to imitation/manipulation) as the physical DL/ID.   mDLs must be 'operating system encompassing' – as they will potentially be used on a myriad of devices (phone, tablet, notebook, wearable, others). mDLs are envisioned to at a minimum have the same data as a physical DL/ID and would also be expected to serve for all the same types (commercial, motorcycle, non-driver ID, etc.) that are issued for physical cards. The mDL should serve as a "vehicle for communication" with the customer/holder – mDLs should be capable of being updated as associated privileges change.

As stated in the mDL functional requirements and mDL model legislation the initial implementation of an mDL program is done as a supplement to the physical DL/ID and not initially as a replacement. Due to the fact that the mDL is a variety of electronic identification it is anticipated that it will be used and depended on as a form of identification by other governmental entities, law enforcement, and the commercial sector.

Additionally, jurisdictions may want to consider what choices they should be making up front when looking at technologies and developing a procurement. These choices may warrant consideration before a jurisdiction decides to define scope of work, or invest time evaluating and considering multiple types of vendor technologies. Some examples include:

Features	Technology Type	Advantage / Disadvantage
mDL Enrollment	In Person	Higher level of identification assurance. Ensures the customer's device and application are aligned to the right motor vehicle record. Requires a customer to visit an agency, a slightly longer transaction time and additional employee training.

	External Download of Application	Lower level identification assurance but more convenient for the customer. Avoids the need for a trip to an agency to enroll. Ensures that the customer enrollee has an existing motor vehicle record by allowing enrollment only by existing customers.
Push Notification	Central server control	Central control is critical to the functionality of the mDL system. In the event a user reports a lost or stolen device that carries an mDL, or if a court or the MVA system initiates a license suspension, the MVA can “deactivate” the mDL at any time.
mDL Log in	PIN number, or facial recognition	Both features enhance the security of data. A PIN is a Personal Identification Number that is set up by the user to protect their mDL account and data. Facial recognition, or FR, is a software program that is used to compare a specific facial image to a set of stored and registered images based on measurable features and distinguishing landmarks. FR would be used to prevent the use of stolen or corrupted mDLs as well as to prevent users from sharing mDLs with friends.
mDL Availability	Online Only	This type of mDL assumes that customers will have uninterrupted mobile telecommunication connectivity for mDL access. In this case, no data is stored on the device and data is therefore not at risk if the device is stolen. Customers will need a DL/ID card backup in certain scenarios.
	Online and Offline	This type of mDL is not dependent on mobile telecommunication connectivity and is always available for use because encrypted data is housed on the device. This is more reliable for users. This type of mDL also records the age of last data “refresh” to the device, which is a separate data element that must be tracked and managed by the jurisdiction or service provider. This type of mDL poses a higher data security risk. Both types will require a card backup. License suspensions or notifications may be delayed in appearing on the mDL if customers do not “refresh” their mDL. mDLs with both online and offline functionality will expire data after a pre-defined period of time from either non-use or repeated offline use. A routine mDL verification, however, would catch this scenario by finding “old” mDL data and requiring an online connection update.
Payments Accepted	Yes or No	Inclusion of this technology allows users to avoid most visits to MVAs for services such as driver’s license renewals or duplicate card requests. However, this ability also makes the mDL application more complicated from a mobile interface and fee processing perspective.

Update record	Yes or No	Permits two-way communication between the mDL server and the mDL user application. It also requires the mDL server to update the MVA central databases which serve as the official record.
mDL Verification	Verify Attribute	Using an offline validation – When a reader application scans and recognizes an authentic mDL without connecting to the backend server.
	Verify with Issuing Authority	Using an online validation – When a reader application verifies both the validity of the presented mDL and runs a lookup on the system of record. Facial recognition further enhances verification trust. Both methods of identification verification are likely more trustworthy than the current identification check process where a verifier visually inspects a presenter's physical DL/ID card.
Interoperability	Vendor Neutral	Refers to the capability of an mDL to be electronically validated by another jurisdiction's (or any relying party) mDL system and vice versa. This capability is critical to any successful mDL program and should be included in any jurisdiction solution.
	AAMVA	AAMVA is developing an interoperability standard that all mDL-issuing authorities should use.
Non-contact validation	Bluetooth Near Field Communication (NFC) WiFi aware Mobile Network	Any of these solutions would satisfy the technical ability for a relying party to validate an mDL without having to touch the user's device. This technology eliminates the possibility of tampering by a relying party, unauthorized device searches and device damage. Validations (authentication) are offered with permission only by the mDL holder.
Emergency Mode	Bluetooth enabled	This functionality could allow an emergency responder to access a user's mDL record on their mobile device using a generally-activated permission from the user, for information such as organ donor status, medical condition and contact information.
Help Desk	Jurisdiction or Vendor	There will be a need for this communication function. There should be a determination prior to procurement on which entity will be handling this functionality.

Procurement Strategy for the Vendor or Solution

The approved procurement strategy should be designed to ensure a fair, open, and transparent competitive procurement process while at the same time meeting specific requirements of an mDL program. It should be developed in accordance with the applicable jurisdictional procurement policies, standards, guidelines, and approval process and should allow for future enhancements and value added offerings.

Consultations with legal and procurement advisors should be scheduled regularly to ensure ongoing adherence to all applicable procurement laws, policies, standards, and guidelines. Processes should be managed and followed to obtain the required project and funding approvals, architectural approvals, and procurement approvals. Consultation with appropriate stakeholders should continue on a regular ongoing basis.

Procurement Methodology Development

Ensure an industry, supplier, or jurisdictional market review (external analysis) has recently been conducted to understand the vendor marketplace and the solutions offered (commercial software product, custom-built solution, others). Updates may be required depending on the timeframe in which a previous review was completed. The strategy and approach to procurement and the various levels of approval should be identified during development of the business case. An internal analysis of what is being procured, for what timeframe, ROI and fee structure possibilities, and the objectives should result in identification of the procurement methodology (e.g., open, competitive, sole source) and best fit for the agency.

Agencies need to assess various procurement and delivery approaches to establish the most appropriate option. For example, if the decision is to mandate the IT solution, then the prime focus of the evaluation is on the vendor's expertise of that software and its ability to deliver on the prescribed technology platform. If the decision is to assess multiple information technology (IT) solutions, then the focus is on both how the technology platform will be able to deliver the program objectives, as well as the vendor's ability and expertise to implement the program.

One method to consider is an additional validation step in the contract award. As an example, contract award could include all requirements of the vendor-developed project plan before proceeding to implementation. The contract could be structured to allow for an early termination by either party without liability and then proceed to the next ranked bidder. Agencies can do this in multiple ways and should work with their procurement office on how to structure payment and proper language to allow for a two-step method. The procurement process should allow for underperforming vendors to be replaced with the next highest scoring vendor without having to retender (avoids delays and additional costs), if applicable under jurisdictional law.

Deliverables and Evaluation Development

Procurement deliverables should be clearly outlined, as should the roles of both the jurisdiction and the vendor in developing deliverables. For example, a vendor is responsible for developing a schedule, while the jurisdiction will provide information for schedule development and approve the schedule. Another example would be that the data created through the mDL process flow is owned by the jurisdiction and should be delivered at contract completion in a format determined by the jurisdiction.

Including the evaluation criteria for written as well as software deliverables will go a long way in preventing later disagreement on what constitutes "acceptable." The procurement should consider both mandatory and optional scope items. After the contract has been awarded for the mandatory scope, the structure should allow time to elect to purchase options based on an internal analysis.

When developing evaluation criteria, ensure the agency's goals for the procurement are accurately reflected in scoring potential bidders. In other words, determine what defines success for the jurisdiction — the timeline, quality, or some combination. Be sure the criteria are reflected in the scoring methodology. Appendices to include in a procurement document to assist vendors in preparing their proposal include:

- project governance
- business and technical requirements
- data models
- current and target architecture

Contract Award

Award to the successful vendor should be a deliverable-based, fixed-price contract. Acceptance of deliverables and payments are managed in accordance with terms and conditions negotiated and included in the final contract.

Procurement Management Team

The magnitude and complexity of the mDL project will require a procurement team structured to support procurement activities. Recommended team members include subject matter experts, technical advisors, legal, and representatives from business, IT, and procurement. To maintain the integrity of the procurement process, procurement team member should sign a nondisclosure agreement (NDA) before starting on the project.

Vendor or Contract Management

An mDL project can be a substantial undertaking and may involve multiple vendors with contractual obligations to the agency. Whether the agency opts for IT staff augmentation, a complete vendor supplied solution, or some combination of options, the agency has an ongoing task to ensure that the terms and conditions of the contract(s) are followed. This can be a time-consuming effort and may require a dedicated resource to manage.

Given that contracts can run over multiple years and include staffing changes from either the agency or the vendor, it is critical to properly set expectations. Following solid contractual practices at the beginning of the contract and ensure continuity of those practices throughout the lifecycle of the contract will help ensure success. Ensuring good contract practices are in place will not necessarily prevent a failure but can be of tremendous assistance if a failure occurs.

The following are some of critical items to consider in developing contract and vendor management plans.

- Ensure all contracts are included in the plan because managing multiple vendors is critical for the agency.
- Consider adding a contract compliance officer or similar role to the project team whose responsibility is to work with the project manager to ensure deliverables, timelines, and other contractual terms are being followed and adhered to. If jurisdictions do not use a contract compliance officer, determine who will have that responsibility in assisting the project manager.
- Develop clear roles and responsibilities for both jurisdiction and vendor staff.
- Ensure regular open communication takes place between the contractor and the agency.
- ALWAYS communicate problems and issues early on. Do not think things will improve over time. As soon as a concern is identified, be open and talk about remedies, ensuring contractual obligations are followed. Identify and address the source of the problem.

- The jurisdiction and the vendor have separate roles and responsibilities to their respective organizations. The project team should develop respect for the obligations of both parties.
- Develop a consistent process for acceptance of all contract deliverables. Determine the process flow and sign-off criteria. Continually update processes and ensure contract amendments are completed if changes occur within the agency or vendor team.
- Develop a jurisdiction contract file, organized by contract terms, that contains all deliverables and sign-offs.
- Determine if documents are going to be maintained in an electronic or paper format.
- Be sure to follow agency or jurisdiction requirements for retention and disposal of all contract related materials.
- Assume and think "audit" when developing a contract file. Set up a filing system to allow for easy and adequate response to an outside or internal audit, which can save hours of effort.
- Consider the use of an "expectations" document for all deliverables to ensure that both the agency and the vendor are clear on the objectives of contract requirements.
- Ensure scope documents are maintained and handled through formal change management processes that include updating the contract if required.
- Develop clear "go/no-go" criteria well ahead of launch to ensure clarity exists between the agency and the vendor regarding requirements and decision points to move to production.
- Develop a list of "rollback" criteria, ensuring mutual understanding of what will have to take place if significant issues are present during a rollout.
- Identify contractual checkpoints in the project plan.
- For jurisdictions requiring annual compliance reports, be prepared to complete required form(s) and demonstrate examples of items in compliance and noncompliance.
- Communicate noncompliance items to the vendor first and try to resolve them at the project level before contract issues are escalated.
- An oversight vendor can assist with contract compliance requirements. Agencies need to clearly specify expectations of the oversight vendor in this process so they have a clear understanding of their role.
- Communicate the role of the oversight vendor to all parties, agency members, and to all other vendors.
- Remember, the oversight vendor is also a contract with terms and conditions that should be followed.

Think in terms of the complete lifecycle of the project when planning for contract and vendor management. As with most items, clear and open communications will go a long way to assist both the agency and contracted vendor in developing and maintaining an open and effective working relationship. Best practices require all parties to articulate expectations, establish frank and open communications, and set a clear plan on how contract documentation and sign-offs will occur.

Vendor Performance Analysis

The vendor should be subject to formal performance analysis. This may be completed through regular performance measurement, a performance scorecard, or contract compliance report encompassing multiple areas of performance analysis. Self-reporting by the vendor should not be the sole method of performance evaluation. The purposes of vendor performance analysis are to identify areas in which the vendor is performing as expected and to identify required corrective action in order to maintain delivery effectiveness and compliance if necessary. Require vendor(s) to sign a service-level agreement (SLA) that includes penalties, liquidated damages, or service credits. Monitor and administer the SLA to ensure vendor compliance.

Vendor Payment Schedule

The vendor is paid according to the payment schedule associated with the release schedule developed during contract negotiations. Plan to pay a percentage of the overall cost upon acceptance of specific deliverables. The remaining percentage (hold-back) is part of the final payment upon acceptance of project implementation.

Contract Administration

Key contract compliance activities will ultimately assist both the jurisdiction and the vendor. Following are several items to be considered when setting up contract files and processes.

- Key personnel – The vendor provides a listing of its project team, including the key personnel identified in the vendor proposal. Contract clauses should outline the conditions of key personnel including requirements to be on site and penalties for changing members without appropriate notice or approval. The project team maintains the list of key personnel. The contract or SLA should contain procedures for replacement of key personnel. Ensuring the contract is current if key personnel are changed is the agencies responsibility, as is following the contract for "how" the change should occur.
- Vendor team forecasting – The vendor may be required to maintain and provide a three-month rolling forecast of project team members (to be updated monthly). This information allows the agency to plan for office allocation, system access, ID setup administration, and access requirements.
- Security clearance requirements – The vendor should comply with all security policies and procedures as outlined in the established agreement.
- Annual security statements – Receipt of signed resource security statements should be included as a requirement in the contract or as part of the onboarding of vendor staff. Receipt of other required documents, such as signed moral rights waivers, should also be included as a requirement.
- Asset management – A spreadsheet should be set up to track assets (e.g., computers, telephone, printers) allocated to on- or offsite vendor team members.
- Document management and filing – Responsibility for document management and filing should be established and maintained by the agency. A repository for documentation and links to file locations should also be maintained. Documents should be updated as activities and needs change; it is worth the time to do so.
- Scope management – When a formalized change control is initiated to add or remove scope, contract documents should be updated to reflect the specific change. Not doing so can create issues in the future. Follow a formalized change control process and ensure responsibility for maintaining the integrity of the contract document is included.
- Project software management – A master spreadsheet of all project software should be developed and maintained and should include:
  - the initial purchase order for software licensing and first-year maintenance and support
  - timeframes and subsequent purchase orders associated with the renewal of software support and maintenance
  - responsibility for managing software renewals should be part of the project team's efforts
  - impacts to timelines should be managed appropriately through the change control process (if required)
- Peripheral management – A master spreadsheet should be developed on new peripherals acquired and used by the project team. Examples include scanners, bar code readers, and other such devices.

Upon Contract Completion

Project teams should follow retention guidelines related to the completion of a contract. Ensure the contract contains inclusive language from initiation to closure and associated activities for either, regardless of when or why closure is initiated. When it comes to closing out a completed contract, following retention guidelines may be all that is needed, but files typically require attention to ensure that only required documentation is retained. If a project is being closed out for any other reason(s), such as termination for cause, termination for convenience, or other closing method, then a very different set of documentation retention requirements may be followed. Legal advice should be sought. Ensure that files are adequately maintained through the lifecycle of any project that uses contracted vendors and that all contractual obligations are followed. Do not underestimate the effort for this work; it should be considered part of the project lifecycle and staffed adequately.

Summary and Recommendations

Ensure sufficient time is allotted to develop any procurement document and understand that it ultimately becomes part of the contract requiring monitoring and adjustments during the journey. Research what others have done and use multiple resources in developing the procurement document itself. Learn from other jurisdictions that may have insights into identifying new or emerging approaches. When through the procurement effort, the level of effort required for oversight and management of contracts and deliverables cannot be underestimated. Many jurisdictions completing similar efforts have learned the hard way that contract management can be a single point of failure for a project. Ensure adequate resources and processes are in place to track contractual requirements against project activities.