Mobile Driver’s License

Feasibility Study

Presented by:
MVC Chairman and Chief Administrator Raymond P. Martinez
# Table of Contents

I. Introduction ............................................................................................................................................. 2  
II. Definitions and Acronyms ..................................................................................................................... 3  
III. Methodology .......................................................................................................................................... 5  
IV. Executive Summary ............................................................................................................................... 8  
V. Feasibility Analysis ............................................................................................................................... 10  
VI. Technical Feasibility ............................................................................................................................. 12  
VII. Security/Privacy Feasibility ................................................................................................................. 18  
VIII. Financial Feasibility ............................................................................................................................ 23  
IX. Legal Feasibility .................................................................................................................................... 27  
X. Strategic Feasibility .............................................................................................................................. 31  
XI. Recommendation ................................................................................................................................. 36  
XII. Appendices .......................................................................................................................................... 38
I. Introduction

Senate Bill No. 2695 (S2695) took effect on January 19, 2016, requiring the New Jersey Motor Vehicle Commission (MVC or Commission), in consultation with the New Jersey Office of Information Technology (OIT), to conduct a study and report to the Governor and the Legislature its findings of the feasibility of electronic driver’s licenses. Specifically, S2695 tasks the MVC with preparing a report describing “the findings of the Commission concerning the cost and resources required, advantages and disadvantages, privacy, security issues, use by law enforcement, and any other concerns related to the issuance of electronic driver’s licenses by the Commission. . .” including “an assessment of the means of issuing electronic driver’s licenses through a mobile application, and accessibility thereof.” The MVC’s report is to provide “recommendations concerning the development and publication of a mobile application for the issuance and use of electronic driver’s licenses,” including information related to “fiscal implications such as: the cost, savings, and efficiencies of creating electronic driver’s licenses; keeping personal identifying information secure; whether charges should be assessed upon drivers for electronic driver’s licenses or the use of an application; and the anticipated amount of time necessary for effective implementation.” (S2695)

In accordance with the mandates of S2695, this report sets forth the MVC’s findings and recommendations to the Governor and the Legislature.
II. Definitions and Acronyms

**AAMVA** – American Association of Motor Vehicle Administrators. AAMVA is a tax-exempt, nonprofit organization developing model programs in motor vehicle administration, law enforcement and highway safety. AAMVA also serves as an information clearinghouse in these areas, and presents positions on issues on behalf of these interests internationally. The organization also operates many inter-jurisdictional data communication systems on behalf of its members. The federal government, as well as member states, often work through AAMVA to organize operational standards for motor vehicle services.

**Agency** – Refers collectively to the 39 existing MVC customer service centers.


**DL/ID** – Refers to a driver’s license or non-driver identification card.

**FR** – Facial Recognition. An identification and security software program used to compare a specific facial image to a set of stored and registered images based on measurable features and distinguishing landmarks.

**ISO** – International Standards Organization.

**IT** – Information Technology.

**NLETS** – National Law Enforcement Telecommunications System. NLETS is used by law enforcement to access citizen data across state jurisdictions.

**mDL** – Throughout this report, the electronic driver’s licenses referred to in S2695 are referred to as mobile driver’s licenses, or mDLs. The use of the acronym mDL is assumed in this report to include mobile non-driver identification cards in addition to driver’s licenses, and will allow the MVC to maintain consistent language with existing state, national, and international mDL programs and efforts.
Online – Refers to the scenario when the mDL is actively connected to a mobile data telecommunications network that can transmit data.

Offline – Refers to the scenario when the mDL is not connected to a mobile data telecommunications network.

State- Unless otherwise indicated by the context, “State” as used herein means the State of New Jersey.

Team – Refers to the mDL project Team of subject matter experts from within the MVC and OIT who participated in this feasibility study.

UL – Underwriters Laboratories.
III. Methodology

A. DEFINE DELIVERABLES

An MVC Team of subject matter experts assessed the feasibility of an mDL program from the perspective of five relevant categories: Technical; Security/Privacy; Financial; Legal; and Strategic. Technical feasibility assessed whether solutions are achievable within the MVC's IT system and within the existing Garden State Network. Security/Privacy feasibility assessed customer privacy interests with regard to the restriction and control of data sharing and the acceptability of anticipated data exchange protocols by those State officials responsible for protecting customer data. Financial feasibility assessed whether the anticipated structure of a future mDL is financially viable or not and what financial conditions are required for the proposed mDL program to be successful. Legal feasibility assessed whether an mDL is authorized within our existing State and federal legal authority and if the MVC requires additional authority to implement an mDL. Strategic feasibility assessed whether the implementation and operation of an mDL is possible within the framework of the MVC's existing initiatives and capabilities.

B. ESTABLISH ASSUMPTIONS ABOUT A FUTURE mDL PROGRAM

The Team identified and utilized the following assumptions regarding a potential mDL program:

1. The existing DL/ID application processes will stay the same after incorporation of an mDL.
2. "Issuing" a customer an mDL will occur only after a traditional DL/ID card is issued.
3. The mDL must include anti-counterfeit features, both covert and overt.
4. The mDL must have security and privacy levels comparable to the current DL/ID card.
5. The mDL must include wireless mobile (iOS/Android) platforms.
6. The mDL must contain all existing DL/ID information, with the potential for expansion to include additional data elements.

7. The mDL will be usable as either a commercial driver’s license, basic auto driver’s license, or identification card with the capability to include additional credentials for privileges such as motorcycle, boating or other endorsements.

8. The mDL will have central control capability so that notifications to customers can be sent electronically directly to their phone with an mDL, or so that driving privilege changes can be automatically updated on the mDL record as needed.

9. The program will have a fee structure that covers all projected implementation costs and operational costs.

10. The mDL will be a voluntary consumer program and will not replace traditional DL/ID cards.

**C. CONDUCT RESEARCH**

The Commission undertook a multi-disciplinary approach for the evaluation of mDL feasibility. MVC Team members were selected from the pertinent organizational disciplines so that each of the five relevant feasibility categories were represented. The Team identified how DL/ID cards are used today and evaluated whether an mDL could satisfy those identified uses particularly where a driving credential or identification proof is needed. The Team also conducted a participation survey of MVC customers. The purpose of the study was to determine the level of public interest in an mDL and to determine what price the participants would be willing to pay for an mDL.

**D. EXTERNAL BENCHMARKING**

The Team then conducted research on various mDL activities, such as legislative activity, proof of concept activity, and research from state, federal and international entities. The Team used this existing body of work to define the major elements of an mDL, anticipate customer uses of an mDL, and create a program structure that would fit within the MVC and OIT operating environments. Benchmark documents are appended hereto as *Appendices 1 – 4*. 
**E. VENDOR COMMUNITY INPUT**

The internal research and benchmark information identified above was used to formulate a request for information (RFI) that the New Jersey Department of Treasury, Division of Purchase and Property, posted on behalf of the MVC to engage the vendor community for technical solutions. The MVC project team received eight RFI responses, all from qualified vendors. Each vendor set forth its proposed technical solution and responded to the specific questions contained in the RFI. Those questions sought information regarding how the vendor’s mDL program would be structured, delivered and administered with regard to the technical, security/privacy, financial, legal and strategic elements of the anticipated program. A copy of the RFI is appended hereto as *Appendix 5*. 
IV. Executive Summary

The mDL is a technologically advanced application that is envisioned to be a useful and convenient identification and driving privilege tool, enabling real-time electronic validation of an individual’s identity. Each day, New Jersey citizens are asked to present their identification, or driver’s license, for various reasons. Those who request proof of DL/ID are then required to visually inspect a physical card to verify its authenticity. With a New Jersey authorized mDL, the entire ID verification process could be conducted digitally with the added confidence of being electronically verified. MVC customers would benefit from the convenience of carrying a digital credential, while those who require customers to show an ID would be empowered to immediately validate them with the issuing authority. The mDL would certainly change the future, creating new choices for citizens to exchange trusted information.

Mobile Driver’s License technology already exists. Mobile devices already secure digital wallet payment information, communication protocols already enable encryption for the safe transfer of sensitive information, and reader technologies exist that enable real time person-to-person validations. These mobile technologies can be incorporated into developing an mDL. The challenge lies in developing a new legal framework that integrates an mDL with State and federal requirements as well as one compatible across state lines.

MDL alternatives to traditional DL/ID cards already exist in the U.S. and abroad. In the United States, the states of Iowa, Louisiana, Delaware, Illinois, North Carolina, North Dakota, Arizona, Kentucky, Missouri, Florida, California, Utah, Texas, Virginia and Tennessee either have pilot programs or are actively working on programs to create and offer mDLs. Internationally, Canadian provinces, Britain, Australia, New South Wales, Netherlands, India and other countries either have pilot programs or are actively working on programs to create and offer mDLs. With so many jurisdictions offering or planning to offer an mDL, the demand calls for mDL interoperability between
jurisdictions. The AAMVA organization, the International Standards Organization (ISO), and Underwriters Laboratories (UL) are all currently working together to develop these standards.

The result of this feasibility study is a favorable finding, that an mDL program is feasible. Before an mDL is issued in New Jersey, there would have to be standardization so the mDL would work across jurisdictions. Various conclusions and recommendations for the legislative and executive branches of government are included in the following sections. The MVC is pleased to present this report to the Governor and the Legislature and hopes it will serve as a resource to help our decision makers meet the needs of New Jersey residents.
V. Feasibility Analysis

FEASIBILITY – GENERAL STATEMENT

The feasibility of a New Jersey mDL was assessed by analyzing five relevant categories: Technical; Security/Privacy; Financial; Legal; and Strategic. The following sections provide assessments for each category and offer recommendations that support an mDL program.

Before considering the feasibility of an mDL, identification of possible users and uses of an mDL is appropriate. Users would include New Jersey residents with valid DL/ID cards, whereas possible uses of an mDL could include, but are not limited to, the following:

- Proof of identity;
- Roadside or traffic stops by law enforcement;
- Proof of age, such as for the purchase of alcohol or cigarettes;
- Identity confirmations for services such as car rentals, hotels and financial institutions;
- A communication tool for first responders and others that could share relevant data such as organ donor status and insulin dependency; and
- A means to send MVC renewal notices or reminders to users.

Special Note: MVC Chairman and Chief Administrator Raymond P. Martinez was recently appointed as an AAMVA Board Advisor to the Card Design Standard Committee, which includes the mDL initiative on a national level. Board advisors will have an opportunity to provide state and jurisdictional perspective and to influence national policy on the development of DL/ID standards, including mDL technical specifications, legal framework, security, and privacy issues, which may be later evaluated and addressed by AAMVA, ISO, and UL.
Listed below are the general operational components of a comprehensive mDL system that will be referenced throughout the remainder of this report. General feasibility of an mDL must consider each of the following mDL components:

**mDL user application** – The mobile application that the customer uses to display the mDL content, including identification, age and driving privileges and restrictions;

**mDL reader/verifier application** – The mobile application that law enforcement, government agencies, banks, alcohol and cigarette sales establishments, casinos and others use to validate the mDL content presented by the mDL user;

**Backend server/mDL server** – The hardware that stores the mDL software program as well as transaction and system activity records;

**Verification service** - A communication service that enables the mDL user and mDL reader applications to send and receive data for online verifications;

**Customer and technical support units** – The MVC units that would be dedicated to support the new mDL system, including support to customers; and,

**Administrative support unit** – The MVC unit that would monitor customer use of the system and have the capacity to change, revoke and suspend mDLs centrally to prevent and inhibit fraudulent use.
VI. Technical Feasibility

There are three essential technical components to a typical mDL system that are identified in Figure 1 below. Figure 1

1. The mDL User Application: The first essential component of an mDL system is the mDL user application. This application is used by the driver to establish personal information.

2. The Reader Application: The second essential component of the mDL system is the reader application, also referred to as the verifier application. It is this part of the mDL that is used to electronically validate another user’s mDL content. There are two mDL reader application types, one for law enforcement and another for general use by the business community and emergency responders. The reader application works in conjunction with the user application and must be able to verify both New Jersey-issued mDLs and mDLs issued by other states.

3. The Backend Server: The third essential component of the mDL system is the backend server. The backend server is the backbone of the mDL system and acts as
the communication hub that relays and verifies mDL information to and from mDL users and readers.

Each of the three mDL system components has the capacity to offer numerous features and capabilities. This feasibility study does not identify desirable system feature choices, but instead identifies only the mDL components that are undesirable as incompatible with the existing Garden State Network and MVC IT infrastructure.

The Team observed that some mDL systems are simple and easier to implement and operate, like Virginia’s mDL pilot program, while other state programs are more comprehensive and rich with customer convenience features, such as Iowa’s pilot program.

**Virginia Program:** Virginia’s mDL pilot program is simple because it is an extension of their existing “myDMV” web portal, which is an online account that customers can use to register and enroll in web services including electronic reminders, change of address and payment options. The Virginia mDL pilot program enhances their existing web service enrollment application to include a mobile delivery platform and image file of the customer’s license or identification. Virginia’s mDL is only available as an online platform. The Team observed that more basic programs are easier to implement and maintain as opposed to more complex systems, which while available, are more time consuming and costly to operate and maintain.

**Iowa Program:** In contrast to the Virginia program, the Iowa program proposes an mDL that has significantly greater functionality. Not only will the Iowa solution function in an online environment like Virginia’s mDL, it will also function and allow electronic verification offline. This means that personal information and data will be stored and encrypted on the user’s phone either within the application software or within the phone’s storage system. The offline functionality offers increased convenience to customers, but also represents a slightly greater data security risk if a hacker or someone seeking illegally to obtain personal information is able to breach the system.
Additional options available with a more complex mDL solution may include the following: the ability to process payments for either renewals or duplicate card requests; the capability to update the user’s file record; and the capacity for the State to push notifications and alerts to customers. Additionally, user enrollment in the mDL program can be accomplished by an application download outside of an agency office, or the State can require a more secure in-person transaction that includes verification of identity, phone, and application download that is matched to the user’s mDL record.

Regardless of which type of mDL system the State chooses to implement, either simple or complex, a hard copy DL/ID card will still need to be issued to customers in the foreseeable future. This way, customers will always have the ability to present a DL/ID physical card in the event a user’s mDL experiences phone battery or network connectivity failure.

**TECHNOLOGY FEATURES:** For the purposes of exploring mDL feasibility, a table is provided below that highlights common technology features of an mDL. Advantages and disadvantages for each feature are also included to show some initial choices that would need to be made to move an mDL program forward.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Technology Type</th>
<th>Advantage / Disadvantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>mDL Enrollment</td>
<td>In Person</td>
<td>Higher level of identification assurance. Ensures the customer’s phone 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.</td>
</tr>
<tr>
<td></td>
<td>External Download of Application</td>
<td>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.</td>
</tr>
<tr>
<td>Push Notification</td>
<td>Central server control</td>
<td>Central control is critical to the functionality of the mDL system. In the event a user reports a lost or stolen phone, or if a court or the MVC system initiates a license suspension, the MVC can “deactivate” the mDL at any time.</td>
</tr>
<tr>
<td>mDL Log in</td>
<td>PIN number, or facial recognition</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>mDL Availability</th>
<th>Online Only</th>
<th>Online and Offline</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 phone and data is therefore not at risk if the mobile unit is stolen. Customers will need a DL/ID card backup in certain scenarios.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>This type of mDL is not dependent on mobile telecommunication connectivity and is always available for use because encrypted data is housed on the phone. This is more reliable for users. This type of mDL also records the age of last data “refresh” to the phone, which is a separate data element that must be tracked and managed by the State 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 don’t “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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Payments Accepted</th>
<th>Yes or No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inclusion of this technology allows users to avoid most visits to MVC agencies 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.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Update record</th>
<th>Yes or No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permits two-way communication between the mDL server and the mDL user application. It also requires the mDL server to update the MVC central mainframe as the official record. Customer consent must be obtained to change the official record, and would require touchpad-enabled signatures, similar to the New Jersey Division of Elections</td>
<td></td>
</tr>
</tbody>
</table>
system which requires a signature to authorize a voter address change. The mDL must accommodate signatures to process both Elections and MVC record updates, such as organ donor status and voter registration. The Division of Elections would need to accept the MVC mobile solution.

<table>
<thead>
<tr>
<th>mDL</th>
<th>Verify with Issuing Authority</th>
<th>Verify Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification</td>
<td>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. This technical approach is given a higher identification rating with a higher degree of trust. 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 card.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Using an offline validation – When a reader application scans and recognizes an authentic mDL without connecting to the backend server. This technical approach is given a lower identification rating.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interoperability</th>
<th>Vendor</th>
<th>Proprietary</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Refers to the capability of an mDL to be electronically validated by another state mDL system and vice versa. This technology is critical to any successful mDL system and should be included in any State solution. Some vendors are able to achieve interoperability using their own technology solution to validate out-of-state mDLs.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AAMVA</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAMVA is planning to facilitate the development of an interoperability standard that all mDL-issuing authorities could use. Until a standard exists that could satisfy interoperability, there is no assurance that a New Jersey mDL will be accepted in other states.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Non-contact validation</th>
<th>Bluetooth</th>
<th>Near Field Communication (NFC)</th>
<th>WiFi</th>
<th>Mobile Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any of these solutions would satisfy the technical ability for a reader to validate an mDL without having to touch the user’s phone. This technology eliminates the possibility of tampering by a validator, unauthorized phone searches and phone damage. Validations are offered with permission only by the mDL holder.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Emergency Mode</th>
<th>Bluetooth enabled</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>This functionality would allow an emergency responder to access a user’s mDL record on their mobile device using a generally-activated</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The MVC Team concludes that each of the identified technology features is feasible to implement based on the vendor responses to the RFI. Furthermore, any technical mDL complications do not present a major barrier toward the implementation of an mDL program. If an mDL program is statutorily authorized, the choice of features would dictate the complexity of the mDL project and, therefore, the project budget, schedule, operational cost and program risk. At this time the Team recommends the off-line mDL verification model.
VII. Security/Privacy Feasibility

One of the MVC’s statutory obligations is to maintain secure custody of DL/ID holders’ personal information and credentials. The Commission ensures the privacy of records by securing customer data at every point in its internal processes. An mDL program requires additional security measures in order to eliminate the vulnerability of the customers’ data to external threats.

Any mDL program requires a strong security and privacy component to protect customer information and data. Even the most basic mDL system, one that simply stores a digitized DL/ID, requires a security and privacy component. The complexity of the security and privacy component increases with the complexity of the mDL program selected. In addition to securing a customer’s personal information and data, the mDL program’s challenge is to reduce the risk of illegitimate and fraudulent duplication of mDLs. A Commission-issued mDL must, therefore, be unique to each individual customer as well as be accessible only by that same individual customer or any other permitted verifier.

Since maintaining public trust in the Commission’s ability to maintain the current high level of quality and integrity of Commission services is fundamental to the Commission’s mission, the importance of developing an MVC process to identify and prosecute mDL fraud cannot be overstated.

The Team evaluated each technical feature identified in the previous section of this report from a security and privacy perspective and identified the possible risk elements of an mDL program. It is the Team’s recommendation that any mDL program introduced in the State must mitigate or eliminate the following risks:

**RISK ELEMENT 1 - SECURE LOGON**

Currently, there are two types of mDL application logons. The first uses a secure Personal Identification Number, or PIN, established by the user at the time of registration. PINs can be secure but are subject to the risk of the user sharing their
PIN with others. A shared PIN permits unauthorized people to have access to and utilize a user’s credentials, therefore potentially devaluing the strength of the mDL credential. Only a biometric solution, such as fingerprint or FR software, can more securely ensure that only the customer of record can access his or her mDL.

**Risk Element 2 – Remote Enrollment**

As identified in the Technical Feasibility section of this report, enrollment refers to the customer registration of a mobile device into the mDL program. Enrollment can be accomplished in either one of two ways. The first way is through remote enrollment that requires the user to download a software application from an online marketplace, entering the user’s personal information into the device and then obtaining electronic validation of their new mDL. With remote enrollment, the customer does not need to visit an MVC agency for the new service.

The other way to enroll users in the mDL program is to require an agency visit. An agency visit offers a more secure option than the remote method because there is a stronger guarantee that the customer is indeed the registered mDL user tied to a specific device. A greater level of trust in the mDL is realized since the customer in this enrollment type is directly linked to their DL/ID record, their source documents and a specific mobile device. Notably, users who delete an mDL from a registered device or who move their mDL to another device may need to do so in-person at an agency to ensure that the record holder is properly identified and the specific device is verified.

The MVC is cognizant of the need to balance security with customer convenience. The Team concludes that with regard to enrollment, an in-person agency based system is less customer-friendly but significantly more secure, whereas a remote enrollment system is more customer-friendly but less secure. Since the enrollment type will depend on the level of system complexity and the data security requirements of the combined mDL features, this decision point is most appropriate toward the end of the mDL development and after a properly evaluated proof of concept.
RISK ELEMENT 3 – EXPOSURE OF USER INFORMATION

Properly securing personal information within the mDL system is an essential component of a successful program. A user’s mDL information may be located in two places: either encrypted on the user’s mobile device or on the mDL server. The likelihood of decrypting identity data on a mobile device is extremely low, but is nonetheless a risk that must be minimized. Some users will want their mDL stored on the phone to have it available for offline mDL use if they need to access it where no mobile services are available. This type of storage creates a risk that data can be stolen, decrypted and used for fraudulent or illegal purposes if the mobile device is lost or stolen and then hacked. One way to protect this risk is to remove the data from the phone completely. This solution requires that each time the mDL is accessed, the user must “call” for their mDL in order to retrieve it. This solution vastly increases the security of the mDL program but decreases customer convenience by eliminating immediate availability of the mDL. Notably, AAMVA best practices provide for offline mDL functionality as identified in the AAMVA Mobile Driver’s License Functional Needs White Paper - Version 7 (see Appendix 1).

RISK ELEMENT 4 - ELECTRONIC VERIFICATION OF mDL WITH THE ISSUING AUTHORITY

A verifier needs to be able to quickly and reliably verify the authenticity of an mDL. Electronic verification is a quick and reliable method to verify whether or not an mDL is authentic. With electronic verification, the user and verifier operate independently by connecting with a secure registry of known mDLs, creating a high degree of reliability. A less desirable mDL verification option is an mDL attribute-scanning application. This application is used to scan the user’s mDL for special attributes, typically a specially-registered code or certificate that acts as an authentication key, identifying the mDL as authentic to the verifier. An attribute-scanning application determines if the software and user record contain key characteristics that identify the presented mDL as legitimate. Although a scan verification is considered more effective than the current
visual inspection of a DL/ID card, the electronic verification process provides the most trusted identity proof.

Reliable verification is particularly important if out-of-state mDLs are expected to be accepted in the State. The scan application option, if capable of authenticating both in-state and foreign-state mDL attributes, presents the most direct and uncomplicated solution. More secure options for electronic verification for out-of-state mDLs is complicated. With electronic verification, New Jersey verifiers would need to verify an out-of-state user’s mDL with the state of origin. While this may not be a problem for law enforcement because law enforcement uses the National Law Enforcement Telecommunications System (NLETS), it is a very real problem for other verifiers such as local businesses, including banks, restaurants and other retail establishments that may not have adequate out-of-state electronic verification options. The Commission recommends that New Jersey’s mDL program utilize offline scan types of verification methods for in-state and out-of-state mDLs to maximize customer and verifier convenience and use until online types are more readily available. Notably, AAMVA will be offering a subscription fee service for online mDL validation to business entities and others. This service, called Driver License Data Verification Service (DLDV), will verify the authenticity of mDLs and would replace the visual inspection method currently used for DL/ID cards. The DLDV service queries the mDL issuing authority for an active record and receives a “match” or “no-match” response. This would satisfy MVC security concerns, since validation would be obtained directly from the state of origin.

**SECURITY FEASIBILITY ASSESSMENT**

An mDL program presents security risks not present with traditional DL/ID cards, and should be undertaken with the highest reasonably-available security measures in place. From a security standpoint, the Team recommends that any State mDL program include technology features that address and minimize the above mentioned risks, including the following:

1. In-person enrollment;
2. FR and PIN logon;
3. Online functionality with encrypted data transfer (offline functionality may be acceptable, but only if OIT determines that its encryption requirements are met); and
4. Electronic verification with issuing authority.

The Commission also recommends running a proof of concept for at least six months’ duration to identify and evaluate any security weaknesses and improvement opportunities in an mDL operation before a full program rollout is contemplated.
VIII. Financial Feasibility

The general assumptions regarding the financial feasibility of an mDL system are:

1) The MVC would seek regulatory authority, pursuant to N.J.S.A. 39:2A-36, to charge a customer fee to cover the following cost elements of any mDL system: Vendor implementation and hosting costs, customer account maintenance, customer service, technical support and any third party fees associated with out-of-state validation lookups, such as from AAMVA’s DLDV. DLDV fees are determined by AAMVA.

2) Any new mDL service fee would be retained by the Commission in accordance with N.J.S.A. 39:2A-36(b), to cover the cost of the complete system.

3) Public demand for the mDL system will be based on a public survey conducted by the Team. The survey will capture the public’s level of interest in the mDL by determining what percentage of our existing customers would choose to participate in using the new product. The survey will also be used to estimate an acceptable public fee for an mDL. Both pieces of information were needed to calculate future revenue estimates.

4) In accordance with N.J.S.A. 39:3-10f1, no county or municipal law enforcement entity shall be required to acquire and use an electronic reader or other device in order to verify the authenticity of a license unless the cost to acquire and use the equipment is paid for by the State. For the purposes of this study, MVC assumes that the mDL system and its use by both citizens and law enforcement would be voluntary and, therefore, the only costs referred to are those that MVC would incur.

**mDL Customer Participation Survey**

A survey of MVC customers was conducted to determine two pieces of information. One, the percentage of the State’s drivers that would utilize an mDL, and two, the fee that those surveyed would be willing to pay for the mDL service. The results of the survey are set forth in the Customer Participation Survey (Survey) results report (appended hereto as Appendix 6). The results of the survey showed that 69% of
respondents would be interested in using an mDL. The Team believes this number to be credible since our benchmark study resulted in similar findings. The State of Utah reported in its feasibility study survey that 68% of its survey respondents indicated they would participate in an mDL program.

Of those surveyed here in New Jersey, 95% of the participants would pay $5 for the mDL service, and 89% would pay $10 for the service (the fee would be paid at each DL/ID renewal). This survey data supports the conclusion that customers value an mDL enough to pay $10. A more comprehensive study, included as part of an mDL proof of concept, is recommended to determine the appropriate price to charge customers for the mDL.

**mDL Revenue Estimate**

The MVC annually conducts about 1.8 million DL/ID card transactions each year. If 69% of those individuals, initiating 1.2 million DL/ID transactions, choose to add a $10 mDL option at the time of renewal, MVC can estimate approximately $12 million annually in revenue to support an mDL program.

To assess whether an mDL program is financially feasible, however, the Commission must also consider the project costs and ongoing operational costs, including hardware and software maintenance. Project costs are the one-time costs of designing, building, testing, proving concept, and delivering the mDL system to the public. Typical project costs include, but are not limited to the following:

- Selection of technical program specifications and vendor contracts;
- Procurement and contract awards;
- Application customization and wireless communications processes;
- Mainframe integration;
- Staff resource costs to develop a regulatory framework;
- Consultant and internal staff resource costs to develop field agency and backend business processes;
- Report programming and auditing development costs;
• Proof of concept with small population set;
• Public awareness and messaging campaigns; and
• Full proof of concept, including modification and expansion based on results of small sample population set.

The most basic of the mDL systems are ones that are only accessible where there is an online connection, utilize a downloadable application enrollment method and do not accept payments or record changes. The basic systems cost less than $500,000 to purchase, but are replete with hidden costs based on customization, which drives the real costs into the millions.

The most accurate and reliable way to benchmark project costs involving so many undetermined variables is to use an analogous estimation approach, by comparing similar costs from the Iowa program. Over the last two and a half years, Iowa ran an mDL proof of concept, which most recently resulted in its issuance of an RFP, scheduled to be awarded in the near future. New Jersey can use the public award in Iowa to establish a cost benchmark for New Jersey’s anticipated mDL program. This use assumes there would be a high degree of technical and functional similarity between the Iowa mDL program and the one selected by New Jersey, which is an unknown variable.

The operational costs of an mDL program, as opposed to the project costs, have no benchmarks for comparison. Operational costs of an mDL system include, but are not limited to, the following items:

• Hosting, storage, and network service costs;
• Staff resource costs for:
  o Business intelligence and performance monitoring;
  o Central management of the program to include customer identity and credential management, logon and access management;
  o Auditing;
  o Policy and standards development; and
• Public communications.
Note, N.J.S.A. 39:3-10f1 mandates that the State pay for any electronic reader or other devices required by any county or municipal law enforcement agency to verify the authenticity of a DL (or mDL in this case). While there would be a cost for readers to verify an mDL, for the purposes of this study, MVC assumes that an mDL program would be voluntary for users and, therefore, may not require the State to fund statewide mDL reader infrastructure.

Cost estimates for the remaining operational items listed above are best calculated by extrapolating all resource requirements needed to run an mDL proof of concept. Further details on this approach are included in the Strategic Feasibility section of this report.

**FINANCIAL FEASIBILITY ASSESSMENT —**

An mDL program is financially feasible based on drivers’ willingness to pay for the mDL service that covers both project implementation and operational costs. The MVC would expect the total costs estimated to align with projected annual program revenue. The MVC has the authority, pursuant to N.J.S.A. 39:2A-36(b), to collect and retain 100% of any new service fee, and this authority remains a key assumption for the reported financial feasibility. If an mDL authorizing statute is passed, and the MVC is given authority to promulgate regulations, MVC will determine and establish a program fee that covers program costs through regulation.
IX. Legal Feasibility

An enabling legal framework for an mDL program is critical to the success and widespread use of the mDL program by drivers (users) on the one hand, and businesses and law enforcement agencies (verifiers) on the other. This section identifies statutes that will need to be amended as part of any authorizing legislative package for an mDL program to be viable.

**LEGAL REQUIREMENT 1 – DIVISION OF ELECTIONS PROCESS REQUIREMENT:** The New Jersey Division of Elections (DOE) currently requires an original signature on all voter registration applications and applications for voter changes and does not accept electronic signatures. The MVC is required to offer voter registration to all applicants for DL/IDs and renewals. DOE does accept digital signature pad signatures at agency offices. However, with regard to an mDL, remote mDL renewal would be subject to DOE approval and possible law or regulation changes regarding voter registration requirements.

**LEGAL REQUIREMENT 2 – ACCEPTABLE DOCUMENT:** The mDL must be recognized as an acceptable DL/ID format when a law enforcement officer stops a motor vehicle. All drivers must possess three documents when driving: a valid driver’s license, a valid insurance identification card and a valid vehicle registration. Ideally, all three of these primary documents would be available and acceptable to law enforcement in electronic form, but that is not yet the case. An electronic version of an insurance identification card was recently authorized by law, but there is no provision for electronic versions of registrations or driver’s licenses at this time. N.J.S.A 39:3-29 must be amended to allow the driver’s license component of the required documents to be in electronic form (the mDL).

**LEGAL REQUIREMENT 3 – CHANGES TO OFFICIAL RECORD:** If an mDL application is to be fully functional, it should be a platform from which a user can make changes to his or her MVC record. Currently, N.J.S.A 39:2-3.8 provides for electronic and digital signatures which, along with a customer’s use of a registered username and password,
constitute acceptance of a record change. An mDL application should be permitted to accept customer record changes, such as a change to organ donor status, with the change becoming part of their official record and binding on the user.

**LEGAL ISSUE - INCONSISTENCY BETWEEN mDL DATA AND DL/ID CARD:** The DL/ID card is an official State record that can be used to establish not only identity, but address and organ donor status. Currently, changes to these types of data can be made by the customer through the secure myMVC web portal, and are immediately reflected on the customer’s official MVC record. The customer, however, does not automatically receive an updated DL/ID card after online changes are made. As a result, the customer may possess a DL/ID card that contains outdated information inconsistent with their official MVC record. Under these circumstances, the official MVC record takes priority. For example, a customer submits an address change online and the official MVC record is updated but the DL/ID in their possession is not. The customer is stopped by law enforcement and presents their outdated DL/ID card, which when checked by law enforcement on NLETS discloses an inconsistency. In this scenario the law enforcement officer will utilize the more up to date information contained in the NLETS system, the new address and not the outdated address on the DL/ID card, when issuing a summons. The Team envisions that an mDL would eliminate the above scenario. With an mDL application, the official record is updated by the user with an online connection; it is then vetted through the interactive application for accuracy and the update is immediately reflected on the mDL. This way, the customer always has an updated electronic version of their official state-issued DL/ID, without the need to visit a motor vehicle agency for an updated hardcopy.

**LEGAL REQUIREMENT 4 – IDENTIFICATION VALUE:** For purposes of this study, the MVC-issued mDL credential will be assumed to hold the same identification value as the current DL/ID card. We note that evaluation of whether this is viable will occur after a determination of whether an mDL program will be authorized in the State. The evaluation will include whether the mDL may be added to the list of acceptable documents that count toward the current “6-points of ID” requirements, and if so, amendments to the current 6-points of ID regulations would be required. While an
mDL may be provided a 4-point identification value, same as the current New Jersey DL/ID card, toward the application for a New Jersey DL/ID, the mDL is not capable of being electronically scanned as a “Proof of Identity” document. The Real ID Act of 2005 requires scanning of proof of identity documents, so the mDL may not be permitted toward the application of a future Real ID DL/ID card.

**Note:** During initial rollout of an mDL program, New Jersey could only accept the DL/ID card versions of out-of-state licenses as proof of identity. The reason is that when an out-of-state customer applies for a New Jersey license, the MVC will invalidate the customer’s out-of-state driver’s license by punching a hole in it, signaling to law enforcement that the out-of-state license is invalid. In the case of an mDL, however, the MVC would not initially have the means to invalidate a customer’s previously issued out-of-state mDL upon the issuance of a New Jersey one. In the future, AAMVA will be creating the necessary infrastructure to permit state-to-state communications. AAMVA’s State Pointer Exchange Service (SPEXS) allows participating states to ensure only one identity document per person exists between states. As a person moves from one state to another, the mDL system will signal the deactivation of a person’s mobile credential after another state-issued mDL is activated. This way, identity security is preserved when an mDL is presented in New Jersey. The previous mDL-issuing jurisdiction will have a trusted means to deactivate a customer’s mDL after New Jersey issues a new one.

**Disclaimer:** This legal feasibility section is not intended to address any federal statute, rules or regulations that may conflict with New Jersey’s allowable use of an mDL in this State, nor is it intended to be an exhaustive list of State statutes and regulations that will require modification to accommodate an mDL program. Rather, it is intended only to highlight the initial legal hurdles expected to arise. It is not possible to identify all legal issues until an mDL is authorized in the State and the particulars of the mDL program are selected and proposed, at which time legal viability must be thoroughly evaluated. Notably, out-of-state use of an mDL will initially encounter some use cases that may inconvenience New Jersey mDL users. For example, Commercial Driver’s License (CDL) holders who travel to other states with their New Jersey license are
regulated by the Federal Motor Carrier Safety Administration (FMCSA). FMCSA anticipates taking the lead from AAMVA to create acceptable use case scenarios for those using a commercial mDL in another state. Questions that may have to be answered on the federal level are:

1. Will an out-of-state state law enforcement entity accept another state’s mDL if a backup card is not available?
2. Will commercial mDLs be acceptable outside the state of issuance when a backup card is not available?
3. If an out-of-state law enforcement entity does not have reader technology, and no backup card is available, will phone handoff be required?

These questions, and others, will soon be addressed by AAMVA, which is taking the lead in developing standards for state use.

**LEGAL FEASIBILITY ASSESSMENT:** An mDL program is only legally feasible if legislative support for each of the above legal requirements can be assumed. Additional legislative support will likely be required if other legal issues, not considered in this report, are identified. Furthermore, other entities, such as AAMVA, DHS and FMCSA must advance their policies in order for any mDL program to achieve widespread acceptance across state borders. These long term goals will take time to achieve but are feasible.
X. Strategic Feasibility

This section addresses how an mDL effort will fit into the priorities of both the MVC and OIT. From a planning perspective, an mDL service offering aligns with MVC’s goal of promoting more online and mail-in service options for our customers. Both business delivery channels represent low cost of service options when compared to our more costly agency business channel. The more MVC can secure mobile service options, the more efficiently it can utilize its collective resources, and the more it can offer customer convenience. The Commission is currently engaged in efforts to promote low cost, more convenient online services. For example, the Commission recently began mailing driver’s license reminder postcards as part of a promotional campaign to promote mail-in renewals. MVC is also exploring ways to expand third-party service offerings such as additional remote transaction services, including the following:

- Enabling a registration renewal and mobile payment application;
- Using AAA to offer registration renewals;
- Using MVC kiosks for select services;
- Expanding MVC’s existing dealer online services program to include salvage titles, trailers, and motorcycles; and
- Enabling online commercial and fleet registrations.

All of these potential offerings have one thing in common: they remove high customer volume from MVC agencies. An mDL program fits into this MVC goal.

**TIMELINE:** Providing the Governor and the Legislature with a recommendation for the amount of time necessary to effectively implement an mDL program can only be done by analysis of the major project components. Those components and estimated times for completion of each item are identified in Table 1.
### Table 1 – Project estimated timeline

<table>
<thead>
<tr>
<th>Step</th>
<th>Major Project Component</th>
<th>Who</th>
<th>Time Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>mDL authorizing statutes (project initiating step)</td>
<td>Legislature</td>
<td>12 months</td>
</tr>
<tr>
<td>2</td>
<td>AAMVA and ISO mDL guidelines development</td>
<td>AAMVA</td>
<td>8 months</td>
</tr>
<tr>
<td>3</td>
<td>DHS and FMCSA guidelines (starts after AAMVA guidelines are completed)</td>
<td>DHS</td>
<td>6 months</td>
</tr>
<tr>
<td>4</td>
<td>mDL regulations – process and fees – Rules included in vendor solicitation requirements.</td>
<td>MVC</td>
<td>10 months</td>
</tr>
<tr>
<td>5</td>
<td>RFP development</td>
<td>MVC</td>
<td>24 months</td>
</tr>
<tr>
<td>6</td>
<td>Service Provider begins – Application development</td>
<td>MVC, OIT, &amp; vendor</td>
<td>12 months</td>
</tr>
<tr>
<td></td>
<td>Wireless communications gateway</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mainframe integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Business process development</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reporting and auditing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Proof of concept and evaluation</td>
<td>MVC &amp; OIT</td>
<td>8 months</td>
</tr>
<tr>
<td>8</td>
<td>Program expansion</td>
<td>MVC</td>
<td>4 months</td>
</tr>
<tr>
<td></td>
<td>Process distribution</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Public campaign</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Employee training</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Customer and administrative support development</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Some of the project components identified above rely on the completion of foundational components before they can begin, such as the enactment of statutes and the development of State and federal guidelines and regulations. These foundational components represent milestones that must be completed before the MVC can begin its project components. Assuming the MVC is provided with the proper authority, each of the remaining project components will need to be evaluated and incorporated into the MVC’s project portfolio based on organizational priority and capability. Some of the existing projects in MVC’s portfolio include:

1. The MVC Transformation project, consisting of four significant components:
   - An update to the MVC’s CDL information system, mandated by FMCSA;
   - An update to the MVC’s driver’s licenses offered, pursuant to federal REAL ID requirements as regulated by DHS;
• An update of the MVC’s Customer Abstract Information Retrieval system; and
• An update of the MVC’s scheduling system.

2. State mandates for autocycles, slow moving vehicles and rearview backup cameras.

3. A queuing system for all field agencies.

4. Statewide inspections program updates.

5. Mobile agency rollout.

6. Online customer service expansion initiatives, mentioned above in this section.

**PROJECT RISK:** A foreseeable risk in establishing an mDL program is to integrate the additional project workload into the existing work volume and backlog currently managed by both the MVC and OIT. Not only are both organizations actively working on the suite of projects listed above, but there are also internal organizational demands, continuous improvements, legislative queries and laws, demand from the public, emergencies, and Executive priorities that must be continuously addressed by the MVC organization. The result of all this combined workload is the continuous management of changing priorities.

**NOTE:** The project timeline shown in Figure 3 represents a reasonable estimated schedule to execute the mDL project. It should be noted that the New Jersey procurement cycle represents a significant portion of project implementation time, which includes the development, evaluation and award of a formal request for proposal.
**Proof of Concept:** An additional variable regarding project implementation must be emphasized. The MVC would not consider a project of this magnitude without executing a proof of concept first. Only through a proof of concept can the MVC and OIT jointly commit sufficient time and resources to refine all technical, legal, security, and financial elements before full commitment. A proof of concept will also permit the MVC some degree of experimentation allowing, if necessary, for operational refinement before the program is finalized.
**STRATEGIC FEASIBILITY ASSESSMENT:** An mDL program is likely strategically feasible, assuming significant legislative support and reasonable flexibility to accommodate the Commission's organizational priorities exists. The MVC's current project load consists of mandated initiatives and previously budgeted projects such that no existing project item can be displaced on the priority list. The proposed mDL project timeline is feasible only if current MVC projects are completed as planned, allowing adequate time and resources to include an mDL effort.
XI. Recommendation

Table 2, below, provides a summary of the MVC’s recommendations for a feasible mDL project:

**Table 2 – Summary of Recommendations**

<table>
<thead>
<tr>
<th>Category</th>
<th>#</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>1</td>
<td>Provide for central server control of the mDL.</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Permit for facial recognition features.</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Use Encryption.</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Allow for mDL payment processing.</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Allow for remote record updating with touchpad signature acceptance.</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>Allow for electronic verification with issuing authority.</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>Allow non-contact validations.</td>
</tr>
<tr>
<td>Security/Privacy</td>
<td>8</td>
<td>Provide for in-person enrollment.</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>Permit facial recognition capabilities.</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>Allow for electronic verification with issuing authority.</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>Allow for both online and offline functionality with OIT acceptance of encryption.</td>
</tr>
<tr>
<td>Financial</td>
<td>12</td>
<td>Establish the mDL as a voluntary program with fee to be set either by statute or through regulation, with the appropriate statutory authority to promulgate regulations.</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>Anticipate using the AAMVA DLDV service.</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>100% of mDL fee is dedicated for MVC use.</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>MVC not responsible for voluntary reader infrastructure for law enforcement (N.J.S.A.39:3-10F.1)</td>
</tr>
<tr>
<td>Legal</td>
<td>16</td>
<td>Electronic signatures through the mDL shall be acceptable for Division of Elections use.</td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>mDL must be added as an acceptable document to satisfy the proof of possession required by N.J.S.A. 39:3-29.</td>
</tr>
<tr>
<td></td>
<td>18</td>
<td>mDL must accept user requested changes to their official record, such as with address and organ donor status (N.J.S.A. 39:2-3.8). When there is a difference between the record and card, the record via the mDL takes priority.</td>
</tr>
<tr>
<td></td>
<td>19</td>
<td>Permit mDL point value through MVC regulatory amendments. The mDL shall carry a similar point value as a current DL/ID card toward the 6 pts of ID program for a DL/ID. Customers must know that the mDL, however, may not be used toward the proof of identity requirements for a Real DL/ID card, absent federal regulatory amendments.</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>mDL must satisfy all conditions of license construction set forth in N.J.S.A. 39:3-10h.</td>
</tr>
<tr>
<td>Strategic</td>
<td>21</td>
<td>Suggested effective date for an mDL shall be 72 months, allowing time to develop an mDL legal framework, solicit and rollout services, and deliver a public awareness campaign.</td>
</tr>
</tbody>
</table>
These recommendations have been prepared in good faith using the most current available information. The Motor Vehicle Commission appreciates the opportunity to present to the Governor and the Legislature the feasibility of an mDL service option and we hope that our presented findings will serve as a useful policy guide to make New Jersey government services more convenient.
XII. Appendices

Appendix 1 = AAMVA Mobile Driver’s License Functional Needs White Paper - Version 7

Appendix 2 = Iowa DOT Request for Proposal for Mobile Driver License Application

Appendix 3 = Utah electronic driver license report

Appendix 4 = International Standards Organization (ISO) 18013

Appendix 5 = RFI solicitation

Appendix 6 = Customer Survey
MOBILE DRIVER’S LICENSE

FUNCTIONAL NEEDS WHITE PAPER

0.7

Document Version

This White Paper discusses functional needs for and practical considerations associated with a mobile driver’s license solution.
Appendix 2 = Iowa DOT Request for Proposal for Mobile Driver License Application

(Right click on image to open Acrobat Document Object)
Electronic Driver License

DRAFT Report to the Utah State Legislature in response to HB227 (July 13, 2016)

The smartphone is the new wallet. In fact, many people no longer carry a wallet, while ‘digital wallets’ are now a common feature on all smartphones. A digital wallet refers to an electronic device that allows an individual to make electronic commerce transactions. This can include purchasing items online with a computer or using a smartphone to purchase something at a store. An individual's bank account can also be linked to the digital wallet.

An individual’s driver license is one of the key documents that people keep in their purse or wallet. The driver license is not only the identifying document that allows people to drive a vehicle, but has also become a key document for other types of authentication such as at banks, retail outlets, air travel, etc. With all of that in mind, however, the driver license is one of the last document types to go digital. HB227, passed by the 2016 Utah State Legislature requires that the Department of Public Safety and the Department of Technology Services work together to identify the challenges and the opportunities to developing an electronic or digital driver license.

Several other states in the US have also begun the process of exploring an electronic driver license.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iowa</td>
<td>In September 2015, Iowa began a 90-day pilot to test a product from MorphoTrust, the company that makes most drivers licenses. The solution uses a mobile app that allows the license to be updated immediately. The Iowa license, developed by Morpho Trust, used a 3D-like photo or digital watermark for validation. A quick screen swipe tips the license to its back, revealing a bar code and the class of the license.</td>
</tr>
<tr>
<td>Louisiana</td>
<td>Louisiana HB461 would give drivers the ability to access their digitized license through a smartphone app offered by the Department of Motor Vehicles. The bill passed the House by a vote of 88-3. Louisiana has stated that the app would cost between $3 and $5.</td>
</tr>
</tbody>
</table>

ISO 18013

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of international Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare international Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75% of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 18013-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 17, Cards and personal identification.

ISO/IEC 18013 consists of the following parts, under the general title Information technology — Personal identification — ISO-compliant driving licence:

- Part 1: Physical characteristics and basic data set
- Part 2: Machine-readable technologies
- Part 3: Access control, authentication and integrity validation
- Part 4: Test methods

Introduction

ISO/IEC 18013 establishes guidelines for the design format and data content of an ISO-compliant driving licence (IDL) with regard to human-readable features (ISO/IEC 18013-1), machine-readable technologies (ISO/IEC 18013-2), and access control, authentication and integrity validation (ISO/IEC 18013-3). It creates a common basis for international use and mutual recognition of the IDL without impeding individual countries/states to apply their privacy rules and national/community/regional motor vehicle authorities in taking care of their specific needs.

ISO/IEC 18013-1 defines the basic terms for ISO/IEC 18013, including physical characteristics, basic data element set, visual layout, and physical security features.

ISO/IEC 18013-2 specifies the technologies that may be used for ISO/IEC 18013, including the logical data structure and data mapping for each technology.
REQUEST FOR INFORMATION
ELECTRONIC DRIVER’S LICENSES
MAY 2016

NJ MVC
225 EAST STATE STREET
TRENTON, NJ 08666

Open Public Records Access Rider

Information provided in response to this Request for Information can be released to the public under the New Jersey Open Public Records Act, N.J.S.A. 47:1A-1 et seq., (OPRA) or the common law right to know. All information submitted in response to this Request for Information is considered public information, notwithstanding any disclaimers to the contrary submitted by a bidder, except as may be exempted from public disclosure by OPRA and the common law.

Any proprietary and/or confidential information, which you provide, will be redacted by the State. A person responding to this Request for Information may designate specific information as not subject to disclosure pursuant to the exceptions to OPRA found at N.J.S.A. 47:1A-1.1, when such person has a good faith legal and or factual basis for such assertion. The State reserves the right to make the determination as to what is proprietary or confidential, and will advise the responding person accordingly. The location in the response to this Request for Information of any such designation should be clearly stated in a cover letter. The State will not honor any attempt by a respondent to designate all materials submitted in a response to this Request for Information as proprietary, confidential and/or to claim copyright protection for such materials. In the event of any challenge to an assertion of confidentiality with which the State does not concur, the person responding to this Request for Information shall be solely responsible for defending its designation by submitting a response to this Request for Information, the responding person waives any claims of copyright protection set forth within any materials submitted in the response.

Section 1 – Introduction, Background, Intent and Purpose

This is a REQUEST FOR INFORMATION (RFI) only, issued solely for information gathering and possible planning purposes within The State of New Jersey (State, NJ) and The NJ Motor Vehicle Commission (NJ MVC, MVC). This RFI does not constitute either a Request for Proposal (RFP) or Quote (RFQ) respectively. The State and the NJ MVC make no express or implied commitment to award a contract for any goods or services described within or identified in response to this RFI. The MVC and State do not seek pricing or proposals and will not accept any unsolicited proposals in response to this RFI.

The purpose of this Request For Information (RFI) is, in part intended to meet the requirements of Senate Bill No. 2852, enacted into law on January 19, 2016 requires S2852 the Motor Vehicle Commission to conduct a feasibility study and make recommendations concerning electronic driver’s licenses and mobile applications by January 19, 2017, ref. (Appendix A.) Under the terms
Question #1 - Percentage of customers that expressed interest in using an mDL

- Interested: 69%
- Not Interested: 31%

Question #2a - Would you pay a fee for an mDL?

- Yes: 95%
- No: 5%
Question #2b - Would you pay $5 for an DL/ID?

- Yes: 95%
- No: 5%

Question #2c - Would you pay $10 for an DL/ID?

- Yes: 89%
- No: 11%
Question #3 - What would be your top concern with having you DL/ID on your phone?

- a. Security of data: 48%
- b. Privacy of your information: 23%
- c. Wireless signal accessibility: 7%
- d. Cost: 0%
- e. Other: 22%