Succeeding with Mobile Driver's Licenses

How to Build the Best mDL Solution for Your State

THE MDL REVOLUTION

Mobile driver's licenses (mDLs) are gaining traction across the U.S. Given the possibilities — a quick tap of your phone at the airport to verify your identity, easy integration with other permits that your state issues for hunting or social services — it's not hard to see why. And while the market is changing quickly, mDLs are already being piloted by several different states.

Yet much remains uncertain. Approaches to mDLs diverge from state to state, and technical standards are still a work-in-progress. How can you make sure you develop an mDL that meets your needs well into the future? In this white paper, we'll assess different development options and share detailed technical and structural guidelines about building solutions that are secure, convenient and flexible.

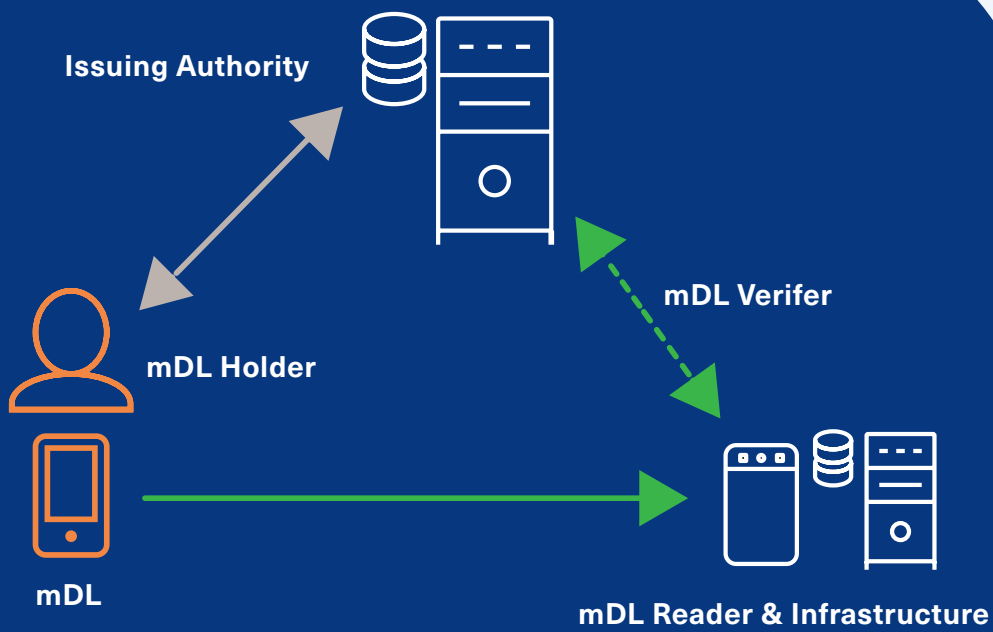
WHITE PAPER

What is an mDL?

An mDL is a secure digital ID that leverages a mobile device to transfer someone's driver's license data to a reader that can authenticate the information electronically. mDL solutions are thus much more than visual reproductions or images on a digital display. Instead, they represent an ecosystem that includes issuing authorities (i.e., drivers license bureaus), mDL readers and mDL holders and their devices.

To maximize convenience and safeguard driver data, mDL solutions must ensure:

- Interoperability between states and across different user devices
- Trust in the validity of the information that's issued to each mDL
- Protection of mDL data from compromise or misuse
- Flexibility for states to make changes as technology and needs evolve



Understanding mDL Development Options

The mDL development process — and any vendors you choose to work with — should deliver a solution that's tailored to your needs and makes it easy for you to manage how things evolve in the future. Here are key elements to consider as you navigate this landscape.

THE mDL DEVELOPMENT PROCESS

There are several different ways to develop an mDL:

OPTION	What it is	Benefits	Risks
END-TO-END SOLUTION	A third-party vendor delivers a comprehensive mDL solution.	The development risk is assumed entirely by the vendor.	Issuing authorities often have few choices when it comes to features, functionality or future developments.
CUSTOMIZABLE MOBILE ID ECOSYSTEM	A third-party vendor provides an ecosystem that powers the issuance, management and verification of mobile identities — and supplies a set of tools that enable municipalities to integrate these functionalities into the mobile wallet of their choosing.	Issuing authorities can assemble the mDL's development according to their state's needs while benefitting from vendor knowledge about best practices.	Issuing authorities must select partners that can guide them through the process and help them understand the contingencies of each design choice.
CUSTOM-BUILT SOLUTION	Issuing authorities assemble an internal team to design and deliver an mDL.	States take full responsibility for the development process and can leverage any existing backend and provisioning services.	Experienced talent may be difficult to engage. States also have little recourse if anything goes wrong.

mDL DESIGN AND ARCHITECTURE

Each state has its own needs — and its own vision of how mDLs should look, feel and function.

Central to realizing these visions is the **mobile wallet**, the element on a driver's mobile device that connects to an issuing authority and stores their mDL data. To store mDLs, states may choose to develop or rely on:

- A standalone mobile wallet
- A mobile wallet that's integrated into a different government app (whether new or pre-existing)
- A mobile wallet that's integrated into the device's native wallet (i.e., Apple Wallet or Google Pay)

If your state's goal is simply to issue a mobile driver's license, leveraging the device's native wallet is a convenient and user-friendly option. But integrating your mDL into a broader government app gives you an opportunity to increase the solution's utility and incorporate additional features, from emergency notifications to social services. Governments may also choose to offer both options, enabling drivers to select where and how they prefer to access their credentials.

Above all, it's important to recognize that drivers' preferences may evolve in the future; the right solution architecture gives you the flexibility to adapt to these changes without compromising security.

HID

THINK BIG

Are you building an mDL or creating an ecosystem? No matter what type of app and mobile wallet you choose for your mDL, be sure it has the flexibility to grow and change in the future. Your goal is to maximize value and deliver a convenient and compelling user experience.

Selecting mDL Features and Standards

Standards for mDLs are evolving quickly. The International Standards Organization, or ISO, has outlined specifications for the interface between the mDL and the reader/verifier in ISO 18013-5 and the ISO 23220 series. The American Association of Motor Vehicle Administrators (AAMVA), meanwhile, has formed an mDL working group whose work is broader, covering both functional needs and implementation guidelines to ensure technical interoperability and trust.

UNDERSTANDING ISO STANDARDS AND AAMVA RECOMMENDATIONS

Following ISO standards — which cover not just mDLs but all mobile identity documents — helps ensure interoperability and data security. But delivering a compelling user experience is equally important, because it promotes adoption and enhances loyalty.

That's why ISO 23220 introduces many features that go beyond ISO 18013-5 requirements.

Feature	ISO 23220	ISO 18013-5
Offline attended operation so that mDLs can be authenticated without an Internet connection	X	X
A data signature that enables an MDL reader to verify that an mDL was issued by a bona fide issuing authority — and that no information has changed since its issuance	X	X
A trustworthy mechanism — like a portrait or biometric data — for confirming an mDL holder's identify	X	X
An authentic and up-to-date description of the mdL holder's driving privileges	X	X
Interoperability guarantees that enable the mDL to be used in other jurisdictions and countries	X	X
Data provisioning mechanisms that make it easy for drivers to understand how their personal information is collected and used — and enables them to control which elements are shared	X	X
The ability to issue other types of identity related privileges, like hunting licenses or social entitlements	X	X
Remote management capabilities that make it easy for issuing authorities to update or revoke mDL privileges and credentials	X	
A safe, efficient solution for mDL authentication and law enforcement stops	X	
Fast processing times for reading and verifying an mDL	X	
Authentication methods that do not rely — but can leverage —the security mechanisms that may be present on the mDL holder's device (e.g. fingerprint readers or secure hardware elements).	X	
A standardized mobile wallet provisioning interface that enables issuing authorities to provision mDLs to multiple types of mobile wallets	X	

Any mDL vendors you work with should be able to demonstrate how they'll maintain compliance with ISO standards. They should also help you understand how incorporating additional AAMVA recommendations can contribute to a more compelling and useful solution.

HID

ENSURING SECURITY

Jurisdictions are understandably concerned about creating a solution that doesn't make sensitive information vulnerable to attack or even inadvertent compromise.

The architecture of your mDL ecosystem is key to maintaining security. mDL provisioning platforms should include:

- **An on-premise provisioning system —** Every mDL must be signed using data from your state's driver database. These signatures are handled by your provisioning system's data preparation module — using a private key that is easiest to secure when it is stored on-premise, behind the government firewall.
- **A provisioning gateway service —** Your provisioning gateway ensures secure, scalable communication between your internal network and your drivers' mobile devices. It will be easier to scale — and more secure — if it is hosted not on-site but by a vendor with a proven commitment to efficient, secure communication. Relying on a hosted provisioning gateway will also help protect your on-premise provisioning system from attack or compromise.
- **Secure information storage —** Your solution should be able to securely store each driver's mDL independently of any SIM or Secure Element. Interactions with mDL readers should be managed according to ISO18013-5 standards.

Device retrieval (commonly known as offline attended operation), which enables mDLs to be authenticated without an Internet connection, is also critical to security. In most cases, both mDL and reader will be online. However, because the two devices can communicate offline, there is no need for mDL solutions to be capable of retrieving data from an online server. In fact, server retrieval would force issuing authorities to open their driver database to the Internet and expose information on the whereabouts of their drivers, greatly increasing the risk to both security and privacy.

Best-in-class security practices like code obfuscation, tamper detection, reverse engineering protection and analysis protection further safeguard mDL solutions — while end-to-end data encryption protects data from being exposed to unauthorized entities.

The Integration Journey

Your mDL vendor should be able to demonstrate how they will support you throughout the mDL development process — and what they will do to make sure implementation is fast and efficient. Development phases might include:

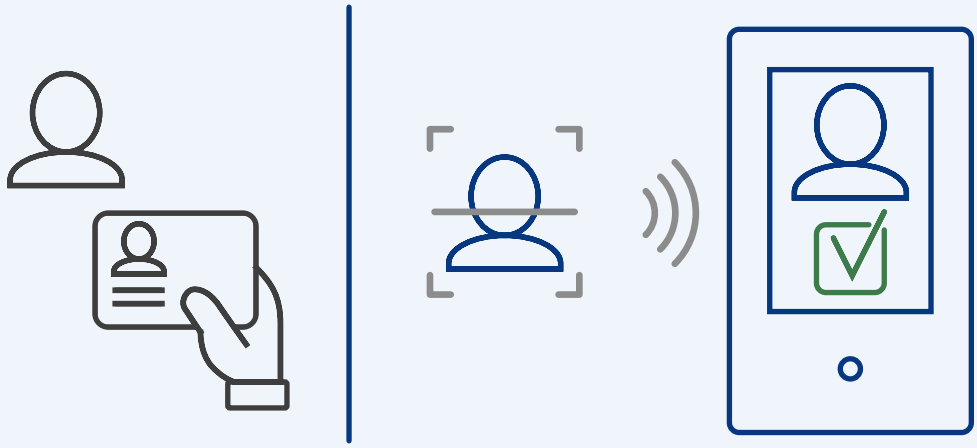
- A more formal proof-of-concept in your environment to help you see how the solution serves your state's specific needs
- A pilot project that's rolled out to a subsection of users
- A project launch phase that delivers the mDL solution to a production environment for further testing and refinement
- Full integration with your systems and database
- Post-launch support and updates

HID

The Importance of Verification

Though dedicated devices can validate a physical driver's license with a swipe or scan, most card verification still relies on analog visual inspection. The verificiation of mDLs, on the other hand, must be digital — not simply to maintain trust and security, but because citizens will only adopt mDLs if they have clear, convenient opportunities to use them.

For that reason, mDL verification services should be available both on- and offline — and easily and securely integrated into websites, apps and kiosks at banks, restaurants, retailers and other places that require people to verify their ages or identities. Issuing authorities must ensure that their mDL's graphical layout does not foster the impression that the credentials will be authenticated via a "flash pass" that gives verifiers no means by which to authenticate the accuracy or origin of the information.



From Promise to Reality

mDLs have the potential to reinvent the way that states issue and manage not just driver's licenses but many different types of identity documents and licenses: vehicle registrations, park passes, social programs and any other documents you issue that are bound to a person's identity. The design choices you make now should power that broader vision and give your residents compelling reasons not just to download but use their new digital IDs. Secure, convenient and flexible — so you can serve their needs no matter where they go.

LEARN MORE ABOUT THE POWER OF MDL:

- Visit our information hub about mDL.
- Download our guide to selecting the right mDL vendor.
- Book time with one of our mDL specialists to discuss your business needs

HID
hidglobal.com

North America: +1 512 776 9000 | Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800 | Latin America: +52 (55) 9171-1108
For more global phone numbers click here

2022-04-27-cid-succeeding-mobile-driver-licenses-wp-en PLT-06582
Part of ASSA ABLOY