

Mobile Driver's
License (mDL)
implementation



Empowering Trust™



Benefits of mobile driver's license

1. Reliable identity verification



The primary purposes of a driver's license is to confirm identity and convey driving privileges. The ISO 18013-5 (mDL) standard provides a mechanism to obtain and trust the data from a mobile driver's license (mDL). The integrity and authenticity of an mDL is protected through the use of cryptographic mechanisms and digital certificates managed by a public key infrastructure (PKI) under control of the department responsible for issuing the license, the issuing authority (IA).

The mDL reader requests the mDL holder's information and exchanges the signed driver's license data over near-field communication (NFC), Bluetooth Low Energy (BLE), or Wi-Fi Aware. Once the data is obtained, the reader verifies the signature on the mDL data elements using the signer certificates, this ensures that the data is genuine and unchanged. Using the verified portrait of the mDL holder displayed on the mDL reader an individual can verify that the mDL information matches the mDL holder in attended use cases.

Placing identification on a mobile device provides a method for the identification to be verified by authenticating the mDL information with a higher level of confidence than physical documents, which do not have the same checks as described above. This higher level of confidence results in more secure, current, and reliable identification, in-turn enhancing public and highway safety.


2. Modernize and streamline agency operations

☑️ — Departments of motor vehicles (DMVs) work diligently to ensure that the information contained on a driver's license or identity credential is correct and up to date at the time of issuance. A significant challenge arises when the identity or driver's license information changes between the date of issuance and when a law enforcement officer is validating the credential during a traffic stop. An mDL can be updated immediately, ensuring that the holder's information is always current. Additionally, an mDL allows anyone who needs to validate a driver's license or identity credential to do so at a high level of trust, either through direct interaction between the mDL and the mDL reader, or through online retrieval from the IA. The mDL also allows the holder to control which personally identifiable information (PII) on the credential is shared, protecting the privacy of the mDL holder and restricting the amount of data that can potentially be compromised.

The American Association of Motor Vehicle Administrators (AAMVA) has developed the Mobile Driver's License Functional Needs Whitepaper, which can be found [here](#), providing jurisdictions with guidance on the development of mDLs to encourage collaboration and cross-jurisdiction/country interoperability. The focus of this document is to help jurisdictions design an mDL that can be utilized both within the jurisdiction and outside of it. Much like the plastic driver's license today, the goal of the mDL is to be accepted anywhere a plastic license is.




3. Citizen convenience

 With 77% of the United States population having a smartphone, user convenience and mobile security are always crucial for any smartphone application. There is a growing demand to have an identity document (ID) available in cases when a physical driver's license is not present. According to AAMVA Implementation Guidelines, the following requirements should be considered while designing any mDL application:

- Allow an mDL holder to selectively share data
- Protect mDL information from unauthorized access, whether in storage or transmission
- Keep an audit log of mDL transactions, accessible only by the mDL holder
- Ensure that an mDL Holder is not tracked
- Limit the use to which mDL data can be put by mDL verifier


4. Privacy – limited data sharing

 One of the main functionalities of an mDL is to provide user consent and selective information release. An mDL transaction involves the exchange of PIIss, and the privacy and security of PII data containing identity attributes is of utmost importance to establish mDL as a trustworthy credential among citizens. To grow this trust, the amount and the type of PII data collected should be limited to that which is necessary to fulfill the legitimate purpose of the use case. For example, in the situation of a gas station selling alcohol products, currently, a cashier will see all PII, including fields such as address, which are irrelevant to the use case. For this situation, the mDL reader should only request for data elements that confirms the age to be over 21 and the portrait of the holder.

An mDL reader operated by an mDL verifier should implement “purpose limitation,” and not request more data from an mDL than required for the use case. Also, the mDL should provide consent and choice to the mDL holder whether to allow the sharing of their PII during their interaction. Based on the mDL reader's request, the mDL should inform the mDL holder what data is being requested. The basic principle is that no user identity data should be shared with another party without informed consent from the user.

All interactions between the mDL and the mDL reader should be open and transparent to both the mDL holder and the mDL verifier. The session between the parties should expire after a specific time and should not entertain follow-up requests once the connection is broken. The mDL holder should have an audit trail of their interactions with reader devices and log information about each transaction.

5. Reduce identity theft

 Physical licenses contain valuable PII such as name, license number and address that can be used to steal an individual's identity. If a user loses their wallet, the ID info is exposed. If an mDL holder loses their phone, the IA can void a holder's mDL or the user can remove all applications from their phone remotely, which will remove the PII. Even if the mobile device cannot be wiped remotely, protections are in place. Typically, a passcode or biometric is required to access a device, and the mDL will have the recommended additional security features and privacy protections.

As mentioned above, you only share the information needed for the relevant party, so your information is shared less. For example, doctor's offices can retrieve an address without gathering license number. The less information that is shared, the less likely PII is to be compromised. An mDL should implement access control to avoid unauthorized use of the credentials. In addition, an mDL has security features to authenticate the mDL. For example, the face image of the legitimate holder can be authenticated through verification of the IA's electronic signature (issuer data authentication). In this way, impersonation through substitution by the photo of another user can be detected. In addition, the mDL contains a cryptographic key pair used to prove that the mDL is not a clone, or that the mDL data is not replayed (mDL authentication). This will prevent an mDL holder's ID from being stolen and reused across the web easily.



6. Enabler for cost savings



Implementing an mDL opens a wealth of opportunities for cost savings for DMVs and other (government) service providers. While the first edition of ISO/IEC 18013-5 standardizes so-called “attended use cases,” hard work is put into the standardization of technologies for “unattended use cases,” which include online authentication at a high level of assurance. This will enable DMVs and other government agencies to provide many of today’s over-the-counter services online, such as:

- online vehicle titling
- online vehicle registration (transfer of ownership)
- online vehicle registration (review of vehicle status)
- online review of DL information
- online driver’s license (DL) renewal
- online review/payment of citations

These are only examples of government services in the mobility domain. The introduction of a highly trustworthy mDL can enable the deployment of high-value online services for many other (government) service providers.

7. Enabler for Mobility-as-a-Service (MaaS)



The introduction of an mDL enables the electronic authentication of drivers and digital verification of driving privileges. Trusted electronic credentials of drivers can become a major enabler for e-commerce in the mobility domain, facilitating secure online reservation of vehicles. Also, vehicle manufacturers and fleet owners can automate physical access to vehicles after successful authentication of their customers, leveraging the mDL. Moreover, fleet owners, or even vehicles themselves, can verify the mDL holder’s driving privileges before allowing a vehicle to start. In addition, a vehicle could automatically apply any restrictions to the driving privileges identified in the mDL, enhancing road safety.

Summary — mDL benefits



1. Reliable identity verification



2. Modernize and streamline agency operations



3. Citizen convenience



4. Privacy – limited data sharing



5. Reduce identity theft



6. Enabler for cost savings



7. Enabler for Mobility-as-a-Service (MaaS)

Recommended practices for mDL

Based on broad and deep experience with mobile phone-based end-customer transaction systems, UL recommends the following

1. Mobile mindset



The digital transformation integrates physical assets into a digital world. While a physical DL can hardly be used in a digital world, the introduction of chip-enabled physical DL demonstrated an important step toward digital relevance. A mDL tightly connects the physical and digital worlds. The mobile phone provides the user a window from the physical into the digital world. An mDL gives the mDL holder control over their identity data and provides multiple technologies to securely communicate only the data required to enable the use case, whether in the physical or in the digital world.

UL recommends IAs, mDL verifiers and industry players to apply this “mobile mindset” when thinking about mDLs. Think about:

- Shorter time-to-market with new functions, no 5-15 year replacement cycle like for a physical DL
- Privacy and security enablement, where the mDL only shares a subset of its data with an mDL reader, which can electronically authenticate that data
- Remote management, where the IA refreshes the content of mDL after initial provisioning

2. Options analysis for use cases



ISO/IEC 18013-5 states, “As the world transitions to digital, mDL has the opportunity to revolutionize workflows by providing multi-channel access to secure and privacy-protecting identifiers for Users that support brand new workflows at any level of security”. In an informative annex, ISO/IEC 18013-5 lists possible use cases such as: convey driving privilege,

purchase age restricted items, enter a bar/club/restaurant, car rental and car sharing, and airport security.

It is important that stakeholders think through these and other use cases where the mDL could be accepted. UL recommends to analyze for the various use cases:

- Which data is required for each use case
- Communication technology options
- Connectivity requirements, considering online real-time verification with an IA, but also availability of credentials when any internet connectivity is absent

3. Enterprise architecture viewpoint



When designing the information technology of an mDL use case, UL recommends to take an enterprise architecture point of view. This point of view takes into consideration the other information and IT systems of the IA and/or mDL verifier.

Take for example, the use case of car rental or car sharing. The mDL could not only speed up the enrollment and pick up of a vehicle but also the temporary registration of the mDL holder in case that person assumes liability for road taxes, citations, and pay-per-trip insurance. This type of record keeping may provide legal certainty to all stakeholders in an ecosystem that gradually shifts from car ownership by default to a more flexible MaaS ecosystem.

The enterprise architecture viewpoint equally enables IAs and mDL verifiers to spot opportunities for improvement of their technology implementation and for process optimization.

4. Value for money



UL recommends IAs and mDL verifiers to connect architecture choices and system design with “make or buy” decisions. A modular design enables isolation of clearly scoped components in the system. Rather specific components in the system might require in-house development. For generic components or services, it may be most economically advantageous to procure those from the market, or even have them externally operated.

In addition, allowing multiple suppliers of high volume generic components often increases the “value for money.” For example, the mobile app might be a component that could be supplied by multiple sources, facilitating choice for consumers, market access for multiple suppliers, and ongoing competition to maximize customer value.

5. Standards compliance



For the identified system interfaces, UL recommends standards compliance as much as possible. The ISO 18013-5 standard identifies the interfaces:

1. Issuing authority infrastructure – mDL
2. mDL – mDL reader
3. mDL reader – IA infrastructure

Requirements for interfaces Nos. 2 and 3 are defined in ISO/IEC 18013-5. Standardization work is currently ongoing for the interface No. 1 between IA infrastructure and mDL in ISO/IEC 23220-3.

UL recommends to select standards for mDL and supporting systems with care and to encourage the implementation of high-quality, proven standards. UL uses the following general rule of thumb: “There is no better standard than an implemented standard.” That’s why UL organizes test events to

corroborate standards, sometimes even before they are finalized. The case study below shows how that was done for mDL.

6. Future proof security requirements



Special care should be given to security in the design of the mDL solution. This should cover both functional security requirements and nonfunctional security requirements. Often the needs for security change with a higher pace than the functional needs. Hence, today’s security solution might need to evolve faster than the functionality.

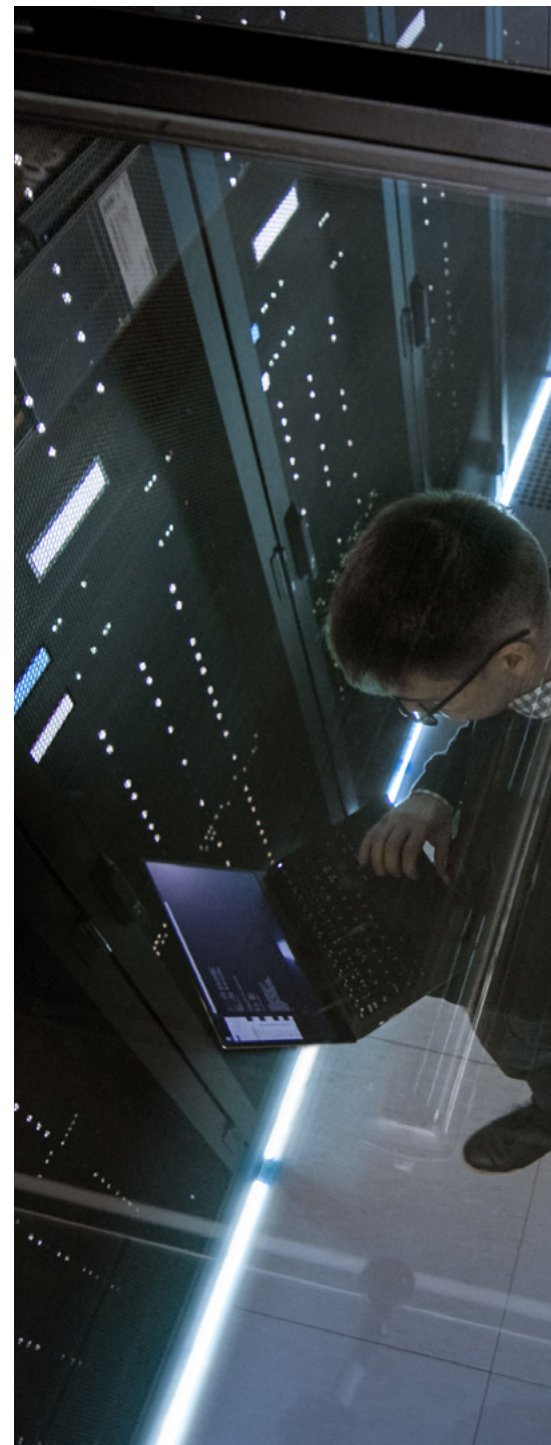
UL recommends to future proof the security requirements by isolating the security functions of the solution from the operational functions. For example, mDL operational functions may be protected by security functions in an mDL app, which are separately maintained by the provider of the mDL app, or rely on security functions provided by a mobile operating system and/or a mobile device.

7. Quality assurance

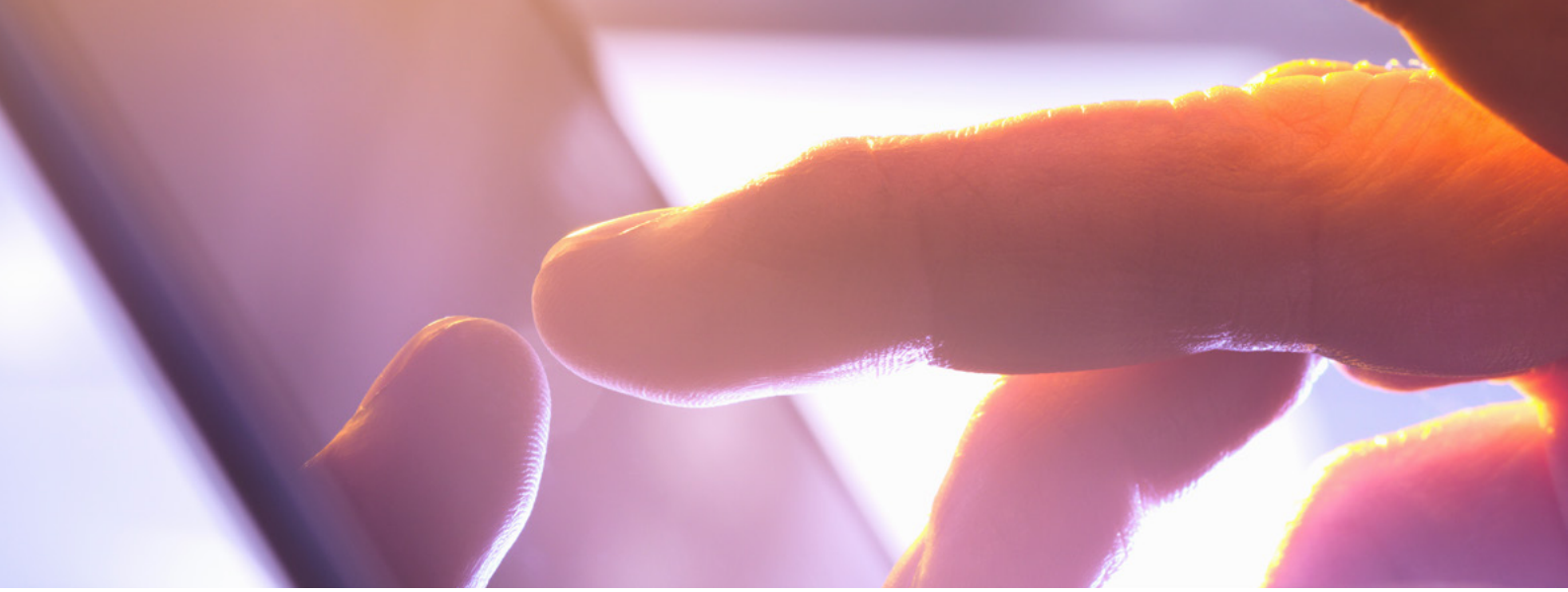


Ensuring the quality of a multicomponent IT solution has its challenges. The selected interfaces during the architecture design identify these components. UL recommends to apply thorough testing on the components in isolation. Test methods for the ISO/IEC 18013-5 mDL interfaces and components are currently defined in ISO/IEC 18013-6. Other interfaces and components also allow tests to be specified and performed.

A proper simulation of the interfacing components allows for both positive and negative test cases, increasing the test coverage. Only when the components in isolation are of sufficient quality,



the testing of the integrated components should be performed. UL recommends this testing at least on the operational functions, security functions, privacy features, and interoperability aspects. In addition, the user experience of the solution should be assured.



8. Ongoing support for handset updates



Mobile device manufacturers continuously release updated hardware and software to keep up with customer demand. These releases include changes in the physical dimensions of screens, new cameras, new user interface screens, improved user authentication methods and many more. In order for an mDL to work properly, the development team needs to ensure their implementation accommodates these changes. This includes ensuring new hardware is supported through maintenance of and updates to existing mDL implementations, and that new mDL implementations have a reasonable degree of backward compatibility with existing hardware.

UL recommends to maintain mDL implementations so that they rely on the latest available mobile device hardware and operating system software. Such a proactive approach facilitates mitigation of cybersecurity risks, avoiding vulnerability to identity theft or loss of personal data. In addition, the user experience and customer satisfaction can be maintained when the mDL continues to operate flawlessly. Ongoing handset interoperability testing is a powerful instrument to ensure the mDL implementation continues to meet needs, requirements and standards across many device types and mobile OS releases.

Summary — recommended practices



1. Mobile mindset



2. Options analysis for use cases



3. Enterprise architecture viewpoint



4. Value for money



5. Standards compliance



6. Future proof security requirements



7. Quality assurance



8. Ongoing support for handset updates



America's First mDL Prototype Interoperability Party

- First-ever North American test event for mDL technology is a great success.
- Thirty prototype implementations from all over the world corroborate ISO/IEC 18013-5, the draft international standard for mDL.
- Global endorsement of ISO/IEC 18013-5 standard and test event by AAMVA, EReg and Austroads.

During the AAMVA Annual International Conference in Omaha, Nebraska, in August 2019, UL coordinated America's first mDL Prototype Interoperability Party. This event was held to hands-on test the ISO/IEC 18013-5 CD2 standard. More than 60 participants from 16 different organizations came together and brought in 30 prototype mDL and mDL reader implementations.

The event enjoyed endorsement of AAMVA, the Association of European Vehicle and Driver Registration Authorities (EReg), and Austroads, the peak organization of Australasian road transport and traffic agencies. These organizations all delegated observers to the mDL Prototype Interoperability Party in Omaha.

The objectives of the event were to allow issuing authorities, mDL solution providers, and the standardization community to try out prototype mDL and mDL reader implementations, evaluate the interoperability of their implementation with other prototypes, and confirm their interpretation of the draft standard. It was also important to generate further feedback to clarify requirements and to enhance uniform interpretation of provisions in the standard under development. The event

also contributes to keeping momentum in standards development and toward adoption and rollout of standards-compliant mDL solutions.

Some of our main takeaways from the event:

- Many major providers of mobile and digital identity technology have demonstrated to embrace the ISO/IEC 18013-5 standard, even in draft.
- Many parts of the standard have been demonstrated to work.
- Details in the standard that need refinement have been identified.
- All security protocols have been proven to work well – the security concepts are well established and are not expected to change.
- The most commonly used technologies in the test event are available to the majority of smartphone users around the world.

All participants worked hard in a collaborative atmosphere, leading to an extremely successful event.

Many of the participants in the test event contribute the ISO group that develops the international standard for mDL. This group already resolved most identified issues in the three-day ISO standardization meeting that immediately followed the test event.



Geoff Slagle, director of Identity Management at AAMVA and observer to the test event commented: “It was fantastic to see experts from around the planet, that in many cases are competitors, lowering their ‘company hats’ for common purpose. To have a front row seat and witness their working together to make refinements that gets the ISO standard across the finish line is inspiring.”

EReg observer Bas van den Berg, head of Driver’s License at RDW, NL, and secretary of EReg’s mDL Topic Group, said:

“It was great to witness 60 people with 30 implementations from 16 companies working together on perfecting their solutions and the standard. Seeing all the enthusiasm and a lot of successful transactions makes me feel we are getting ready for truly interoperable mDL solutions.”

Christopher Goh, general manager, Registration and Licensing Modernization, Queensland Department of Transport and Main Roads and observer on behalf of Austroads concluded:

“The mDL test event gave us confidence that industry was onboard in ensuring that whatever we develop, and whomever we develop an mDL with, we would be able to interoperate with other jurisdictions if they use the future ISO standard.”

Arjan Geluk, lead principal advisor, Identity Management and Security, UL, ISO Task Force leader for mDL standardization and special technical advisor to AAMVA’s Joint mDL Working Group said: “It is extremely rewarding to see that we have been successful in translating the functional needs brought forward by issuing authorities and other key stakeholders into technical requirements for security and interoperability that work. Many thanks to our hosts AAMVA and the State of Nebraska for helping to put on such a successful event. We also would like to thank all the participants and observers for their support.” The next challenges are to finalize the standard and to ensure that mDL implementations strictly conform to the standard. Only then we can jointly reap the benefits of security, privacy and global interoperability. UL develops test and certification programs for mDL. UL is committed to Empowering Trust™ in mDL!



UL.com

UL and the UL logo are trademarks of UL LLC © 2019.