Mobile Driver's License Frequently Asked Questions

This FAQ was developed by the Secure Technology Alliance to answer questions about mobile driver's licenses (mDLs) that comply with the draft ISO/IEC standard 18013-5, "Personal Identification – ISO-Compliant Driving License – Part 5: Mobile Driving License Application." Additional information can be found in the Alliance white paper, The Mobile Driver's License and Ecosystem.

Glossary

The Holder is the individual who chooses to have and use a mobile driver's license (mDL). They are the legitimate owner of the identity enrolled with the DMV and associated with the physical driver's license card and the mDL.

The Issuing Authority (or Issuer) is the entity that enrolls the identity of the mDL Holder and provisions the mDL.

The Relying Party (or Verifier) is the entity that requires an identity or verified biographical information to provide a product, service or entitlement to a Holder.

The Identity Provider (or Provider) is a service provider that manages the use of mDLs online.

General

1. What is a mobile driver's license?

A mobile driver's license (mDL) is a digital representation of the information contained in a physical state-issued driver's license (DL) or non-driver identification card. Mobile driver's license issuance and use are just emerging, with implementations varying among jurisdictions. Some implementations are simple renderings of a physical driver's license (DL), which can be easily tampered with using current graphics tools. Others are using the draft ISO/IEC standard 18013-5 to implement mobile driver's licenses that are secure, accurate and interoperable and that protect privacy.

The term "mDL" in this FAQ focuses solely on those that comply with the draft ISO/IEC standard 18013-5. In this implementation, DL information is securely stored on a citizen's smart mobile device such as a smartphone or a tablet and is owned and controlled by the mDL Holder.

2. How does an mDL work?

The mDL Holder accesses, or allows access to, the data contained in the mDL through a downloadable app (an application container or wallet) approved by the state Department of Motor Vehicles (DMV) or equivalent agency. The app allows Holders to determine whether, to whom, and what mDL data they wish to share during a specific encounter. The entity that needs to confirm an individual's identity (the Verifier) receives information through an electronic reader that is capable of both confirming the authenticity of the mDL and receiving the data that has been authorized for sharing.

3. Is an mDL a replacement for a physical ID?

At least for the foreseeable future, the mDL is a companion to the physical card, not a replacement.

4. Are mDLs only useful to show law enforcement that a person has driving privileges?

Being pulled over by law enforcement is one of many instances in which an mDL is useful. mDLs could be used in any scenario where identity needs to be verified – for example, in airports, banks, hotels, retailers and more. The Alliance white paper, "The Mobile Driver's License and Ecosystem," includes brief examples of a variety of uses.

5. What are the benefits of mDLs?

mDLs benefit Issuers, Holders and Verifiers by:

- Providing secure, convenient identity verification capable of eliminating billions of dollars in fraud. The person who holds the mDL controls what information is shared and with whom.
- Providing Issuers with remote management capabilities, allowing mDLs to be updated remotely, reducing cost and improving efficiency.
- Cryptographically verifying a state-issued ID. An mDL shares identity information signed by the State government issuing authority and the recipient Verifier can electronically authenticate that information.
- Giving the mDL Verifier confidence in the presented ID without requiring specialized knowledge of the hundreds of card design and security features applicable to the driver's licenses (and their variants[1]) that are issued by 56 states and territories.

6. Why should an mDL implementation be based on standards?

An international standard is currently being drafted: ISO/IEC 18013–5, "Personal Identification – ISO-Compliant Driving License – Part 5: Mobile Driving License Application." This standard provides mechanisms for obtaining and trusting identity document data from an mDL. It also provides standardized methods of interacting with an mDL for identity and driving privilege use cases. In North America, AAMVA is coordinating among state and provincial DMVs; AAMVA Guidance for mDLs starts with this standard as a baseline capability.

Standards-based implementations of mDLs are critical to stimulate the use and adoption of mDLs by providing the foundation for interoperability across jurisdictions.

7. Do mDLs create identity?

The mDL does not create an identity. mDLs are digital replications of the identity data used by each individual state's DMV or equivalent agency to enroll citizens in the issuance of physical driver's licenses.

8. How can mDLs improve identity transactions?

mDL transactions involve the exchange of consent, identity and authentication data between the Holder's device and the Verifier's device or system. mDLs can benefit a variety of relying parties by providing a proven mobile ID that can strongly authenticate identities and offering the potential for more efficient identity transactions.

[1] Variations include designs indicating driving versus non-driving status, age compliancy (under 21 or over 21), legacy designs, and REAL ID-compliant and non-compliant ID cards.

Adoption and Uses

9. In what scenarios would mDLs be used?

An mDL can be presented to confirm driving privileges, legal age, name, or contact information. mDLs can be used in all of the same scenarios as a physical DL, for example, purchasing age-restricted items, opening bank accounts, renting or sharing cars, going through airport security, accessing secure locations and more.

10. What are the benefits to states of issuing mDLs?

Benefits to state Issuers include:

- Providing easy to use and convenient electronic ID documents to their citizens, mDL Holders, that increase document reliability and can be used worldwide via the ISO/IEC 18013-5 standard.
- Remote management capabilities, allowing mDLs to be updated remotely, reducing cost and improving efficiency.
- The ability to assist Holders who lose a DL card or are unable to come to the DMV.
- Reduction in the use of expired and invalid DLs.
- Reduction in the use of counterfeit documents when the Issuer digital signature is verified.

11. What are the benefits to relying parties of accepting mDLs?

Benefits to relying parties (e.g., banks, law enforcement, retailers, hotels) include:

- Ease and reliability of verification of an individual's identity, using digital authentication based on a global standard rather than relying on a Verifier's or card reading device's knowledge of and ability to recognize physical security features.
- Reduced exposure to liability. A Verifier can decide to receive only the attributes required for a particular transaction, thus reducing the risk of violating a Holder's privacy.
- Quality control. Transmitting mDL data digitally eliminates human errors during manual intake of attribute data.
- Potentially reduced use of expired and invalid driver's licenses due to cryptographically authenticated mDL.
- Potentially reduced identity fraud, including counterfeit DLs.

12. What markets can benefit from accepting mDLs?

Any market that needs to verify identity can benefit from accepting mDLs. Eleven use cases, including retail, banking, law enforcement and travel, can be found in "The Mobile Driver's License and Ecosystem" white paper.

13. Will mDLs be interoperable across states?

While some implementations may not start out this way, the goal is for standards-based mDLs to be interoperable across state lines. AAMVA is actively working to publish guidance for interoperability across issuing jurisdictions for the U.S. and Canada. To promote country-wide adoption and acceptance across jurisdictions, both mDL Verifiers and mDL solution providers should ensure that solutions are tested, certified, and compliant with ISO/IEC 18013-5.

Security and Privacy

14. Are mDLs secure?

Yes, mDLs follow the highest security standards. ISO 18013-5 provides and documents many security requirements related to the exchange and validation of mDL data from the mDL to the Verifier.

15. Can mDLs be trusted?

Yes. mDLs are issued by a trusted authority, use established cryptographic techniques, and can be cryptographically authenticated offline and online.

16. What are the privacy considerations of mDLs?

The mDL Holder manages their data and provides informed consent to decide what data to share, giving the holder full control.

17. What information is on an mDL, and how much can a Verifier access?

There are both mandatory and optional data elements specified for mDLs. Issuing authorities will determine the optional data elements that they will support in their mDL implementation. Mandatory information reflects what is displayed on a physical driver's license, such as name, a portrait, birth date, issue date, expiry date and driving privileges. Examples of optional information are gender, height and weight, age in years, and nationality.

The mDL Holder controls access to the data when responding to a Verifier request. The mDL Holder accesses, or allows access to, the data contained in the mDL through a downloadable app (an application container or wallet) approved by the issuing authority. The app allows Holders to determine whether, to whom, and what mDL data they wish to share during a specific encounter.

18. How can Verifiers authenticate that mDL data is authentic and accurate and has not been altered by unauthorized parties?

Data is transmitted from the Holder's device over a secure encrypted channel to the Verifier's reader, along with a cryptographic signature from the Issuer proving that the data have not been altered. The reader can check that the mDL data originated from a valid issuer and was transmitted by the device to which it was originally issued.

About the Secure Technology Alliance

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software across a variety of markets including authentication, commerce and Internet of Things (IoT).

The Secure Technology Alliance, formerly known as the Smart Card Alliance, invests heavily in education on the appropriate uses of secure technologies to enable privacy and data protection. The Secure Technology Alliance delivers on its mission through training, research, publications, industry outreach and open forums for end users and industry stakeholders in payments, mobile, healthcare, identity and access, transportation, and the IoT in the U.S. and Latin America.

For additional information, please visit www.securetechalliance.org.

described in this report is accurate as of the publication date. The Secure Technology Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report. This white paper does not endorse any specific product or service. Product or service references are provided to illustrate the points being made.