SECURE TECHNOLOGY ALLIANCE

A SECURE TECHNOLOGY ALLIANCE IDENTITY COUNCIL WHITE PAPER

The Mobile Driver's License (mDL) and Ecosystem: Executive Summary

Version 1.0

March 2020

Secure Technology Alliance
191 Clarksville Road
Princeton Junction, NJ 08550

www.securetechnologyalliance.org

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.

Contents

1 About This Summary

This document is an introduction that highlights the key elements included in the Secure Technology Alliance's white paper, "The Mobile Driver's License (mDL) and Ecosystem." The full white paper, which focuses solely on U.S. implementations of mDLs that comply with the ISO/IEC standard 18013-5, can be downloaded at https://www.securetechalliance.org/publications-the-mobile-drivers-license-mdl-and-ecosystem/.

The white paper was developed to help stakeholders understand how mDLs will change the way identification is managed. It answers essential questions around the standards, features and uses of an mDL; why someone should use or accept an mDL; and how the mDL will meet expectations of trustworthiness.

It is strongly encouraged that you share this Executive Summary and the full white paper with others within your organization to expand their foundational understanding of this rapidly emerging technology.

2 Overview of mDLs and the Ecosystem

The mDL[i] is a secure digital representation of driver's license (DL) data that is provisioned by a state's Department of Motor Vehicles (DMV) or equivalent agency onto a smart mobile device, such as a smart phone or tablet, for use by the proper, intended mDL Holder. It can also contain information relevant to additional state privileges or national context. The mDL market is developing rapidly, with states in varying stages of implementation.

Primary stakeholders in the mDL ecosystem:

mDL Holder (Holder): Individual who chooses to have and use an mDL.

Issuing Authority (Issuer): Entity that enrolls the Holder and provisions the mDL.

Relying Party (Verifier): Entity that requires government ID to provide a service.

Identity Provider (Provider): A service provider that manages the use of mDLs online.

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

An mDL that is secure, accurate, and interoperable, and that protects privacy is coming, and such a mobile ID could well change the identity landscape in the near future. A draft international standard is available — ISO/IEC 18013-5, "Personal Identification – ISO-Compliant Driving License – Part 5: Mobile Driving License Application" — and a number of states are piloting or implementing mDLs that comply with this standard. AAMVA Guidance for mDLs starts with this standard as a baseline capability and defines mDLs as a companion to physical DLs.

Having a standards-based mobile form of digital identity that offers the same trust as a state-issued physical DL brings greater utility, convenience and security benefits for holders while helping to manage their daily lives. mDLs can benefit a variety of relying parties by providing a proven mobile ID that can strongly authenticate identities and offer the potential for more efficient identity transactions.

Capabilities of an mDL include:

- Providing secure, convenient identity verification capable of eliminating billions of dollars in fraud. The person who is the mDL holder controls what information is shared and with whom.

- Providing issuing authorities 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[ii]) that are issued by 56 states and territories.

3 mDL Ecosystem Considerations

The white paper provides technical details and thoughtful analysis on a number of topics that need to be considered when evaluating mDLs.

Provisioning mDLs: How the mDL gets to the correct device of the intended mDL holder is critical to establishing and maintaining trust at the time of a transaction.

Use at Transaction Time: mDL transactions involve the exchange of consent, identity, and authentication data between the holder's device and the verifier's device or system.

Interaction Modes: Verifiers want to design business flows that provide their customers with appropriate and personalized service. But different verifiers may have different equipment, workflow patterns, physical environments, security policy, and customer needs.

Usage Architecture: The architecture described in this white paper follows the draft international standard, ISO/IEC 18013-5. This standard specifies certain interactions between the different participants in the mDL ecosystem.

Privacy: The right to control personal data is considered fundamental. Privacy will ultimately be the measure by which citizens decide to trust or not trust an mDL ecosystem. The mDL is privacy-enabling by allowing holders to choose identity applications and control the release of their personally identifiable information to verifiers.

Building Trust: Generally, transactions requiring identity verification carry a certain amount of risk. All participants in the mDL ecosystem need to trust one another to ensure data is legitimate and is being used for legitimate purposes. The mDL architecture enables the development of a robust trust framework.

Challenges to a Robust mDL Ecosystem: Building a robust mDL ecosystem requires both technical and policy considerations. Each stakeholder's requirements should be addressed to encourage adoption. The industry is working to develop the ecosystem to ensure security, privacy and trust, as well as implementation and architecture guidance.

4 Building a Robust mDL Ecosystem

Implementing the ecosystem changes that enable broad issuance, use and acceptance of mDLs requires collaboration among all industry stakeholders to address implementation questions and challenges. The Secure Technology Alliance launched an mDL initiative to raise awareness, support development, accelerate adoption, and educate the U.S. market on the technology and applications for mDLs.

The Alliance initiative includes participation from AAMVA, driver's license technology providers, mobile technology providers, security providers, testing organizations, and relying parties including retailers, financial institutions and government security agencies.

Participation in the Secure Technology Alliance mDL initiative is open to Alliance members and relying parties. Visit the Secure Technology Alliance website for additional information on the initiative and participation opportunities.

---

[i] The term *mDL* as used here includes forms of identification that may not grant the holder the privilege of driving, such as an ID card issued by a state's DMV (or an equivalent government agency). The driving privilege is not necessary for the establishment and use of identity.

[ii] 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.