Case study

Iowa DOT Partners with UL to Test Their Mobile Driver's License Solution

mDL assurance: crucial to project success in Iowa, critical for worldwide interoperability and trust

Empowering Trust®

Our wallet – including our driver's license – goes mobile

Following the trend toward contactless and mobile interactions set by the payment sector, driver's license issuers around the world are preparing for the introduction of a mobile driver's license (mDL). One of the world's first, the state of Iowa decided to help Iowans take their driver's licenses out of their wallets and put them into their mobile phones. To do so, they chose to work with UL because of our deep experience with identity management and security and our leading role in the international standardization of mDL.

One critical difference between a physical driver's license and an mDL is that the latter is verified electronically. Rather than taking a plastic card at face value, a verifier uses an mDL reader app to obtain driver's license data from the mDL through secure wireless communication.

This brings much more confidence to many stakeholders:

- Users preserve their privacy by only sharing what they choose to disclose.
- Those who check the driver's license verify an electronic signature, the cryptographic proof that the driver's license data is authentic.
- Issuers remotely manage the mDL and driving privileges in real time.

Moreover, mDL helps combat identity fraud because counterfeit mDLs will fail electronic verification.

The challenge

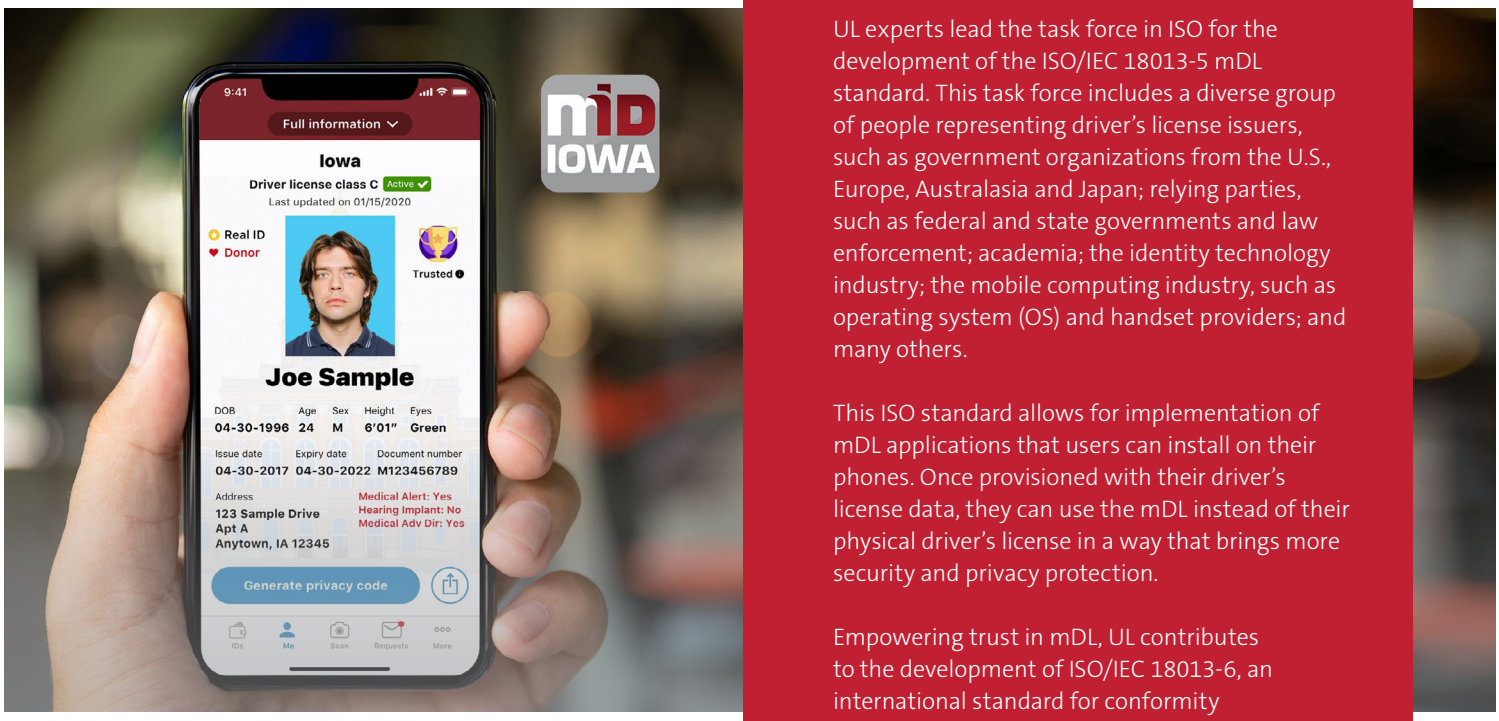
These benefits are only realized if both the mDL and the mDL reader speak the same language. This can be achieved by strictly conforming to the standards that define the mDL protocols and technologies. To ensure that an mDL works with a standard conformant mDL reader — even in a different state or country — it needs to be tested thoroughly. Also, the cybersecurity of the system needs to be strong enough to help prevent attackers from making unauthorized use of the system, for example, fraudulently issuing a "real" mDL or stealing personal data.

The Iowa Department of Transportation (Iowa DOT), the agency responsible for issuing driver's licenses in Iowa, understood these challenges from the beginning. Apart from seeking a vendor for developing, hosting and marketing their mDL solution, the Iowa DOT requested separate proposals for independent testing services to validate the functionality and security of their implementation.

The solution

The Iowa DOT selected UL as their partner for these independent testing services. Based on the requirements and use cases defined by the Iowa DOT and the solution proposed by their vendor, UL developed a test strategy and executed test services, including functional, integration, performance and security testing. Within that broad range of test services, two testing and assurance activities are key enablers for obtaining and conveying trust in mDL technology: conformity assessment and cybersecurity evaluation.

IOWA DOT



International standardization for mDL

UL experts lead the task force in ISO for the development of the ISO/IEC 18013-5 mDL standard. This task force includes a diverse group of people representing driver's license issuers, such as government organizations from the U.S., Europe, Australasia and Japan; relying parties, such as federal and state governments and law enforcement; academia; the identity technology industry; the mobile computing industry, such as operating system (OS) and handset providers; and many others.

This ISO standard allows for implementation of mDL applications that users can install on their phones. Once provisioned with their driver's license data, they can use the mDL instead of their physical driver's license in a way that brings more security and privacy protection.

Empowering trust in mDL, UL contributes to the development of ISO/IEC 18013-6, an international standard for conformity assessment of mDL technologies.

Conformity assessment of mDL solutions involves performing hundreds of tests to confirm that the mDL data, functional behavior of the apps and security protocols conform to the latest version of ISO/IEC 18013-5 and underlying standards. Strict conformity to standards is fundamental for open systems that need to interact outside of a closed environment. Iowans should not only be able to use their mDL with an Iowa law enforcement officer – their mDL should also work across jurisdictional borders, at a retailer that needs to confirm age and potentially for federal ID purposes, no matter who their technology vendors are.

Cybersecurity evaluation activities cover both the mDL apps and the issuing authority's back-end systems. For the mDL apps, UL performed security design reviews, source code reviews and mobile app penetration testing. For the issuing authority's back-end systems, UL cybersecurity experts performed an audit on the administrative network managed by the Iowa DOT's vendor, as well as a delta assessment to gauge the effectiveness of the remediation efforts performed. Also, a penetration test was performed on the back-end systems of the Iowa DOT and their vendor. The objective of this approach was to obtain assurance that security configurations are effective, that the segmentation between the Iowa DOT internal network and the vendor's cloud environment is effective, and that the applications hosted are sufficiently secure.

The result

According to Melissa Gillett, director of the Iowa DOT's motor vehicle division, UL provided a differentiating factor by empowering trust in their mDL solution: "UL's testing and security evaluation activities have provided real value towards the assurance that the Iowa mDL is conforming to the latest ISO standard, and to confirm that appropriate security measures are in place, both with our agency and with our vendor."

Recognizing the potential of mDL assurance results to convey trust in mDL technology toward those that will use and accept mDLs issued in Iowa, Gillett went on to say, "This value is not only for Iowa as an individual jurisdiction, but also for other states and stakeholders in the mDL ecosystem. We encourage the adoption of an mDL assurance program, as it really helps to jointly achieve the shared goal of trustable, interoperable mDL solutions."

For an mDL conformity assessment and cybersecurity evaluation, contact UL at imsecurity@ul.com.

UL.com

© 2021 UL LLC. All rights reserved. This document may not be copied or distributed without permission. It is provided for general information purposes only and is not intended to convey legal or other professional advice.

0421