Next Generation Identity: Mobile Driver's License

Science and Technology

IDENTITY MODERNIZATION

In 2020, the U.S. Congress passed the REAL ID Modernization Act, allowing the Department of Homeland Security (DHS) to accept electronic transmission of user identity information and opening the possibility that novel digital technologies could be used to verify and maintain identity.

MOBILE DRIVER'S LICENSE

A range of initiatives are now underway to develop technically robust, secure, interoperable, privacy protecting, and easy to use technologies to allow users to manage their digital identity information. Many of these approaches are still proof-of-concept or exploratory in nature, however, some have gained interest among state driver's license and identity document issuers, financial service institutions, and technology developers. Mobile Driver's License (mDL) is an early front-runner, consisting of standardized technologies and processes that enable a digital-identity ecosystem that replicates and potentially improves upon physical identity credentials.

The DHS Science and Technology (S&T) Biometric and Identity Technology Center (BI-TC), in collaboration with the National Institute of Standards and Technology (NIST) and the Transportation Security Administration (TSA), is engaging states, standards development organizations, and technology developers to assess risks and develop guidance to facilitate the development of a secure, privacy protecting, and trustworthy digital identity ecosystem.

PROCESSES AND ROLES

In this process, Issuing Authorities (①) represent state or other authorities responsible for issuing identification cards, driver's licenses, and future mDLs. Relying Entities (③) represent the identity verifiers, like TSA. The mDL Holder (②) represents a person presenting an mDL (and themselves) to the Relying (or Verifying) Entity. The identity verification process takes place between the mDL Holder and Relying Entity, which can be done offline with no external network connections using common cryptographic digital signature verification techniques.

In the case of a TSA Checkpoint, a traveler (②) presents their mDL to a TSA mDL reader (③) by holding it near the reader. The authenticity of the mDL is cryptographically verified automatically, with no need to inspect physical anti-counterfeit features. The traveler's name is verified against their ticket, and the traveler's face portrait is verified as the correct mDL holder.

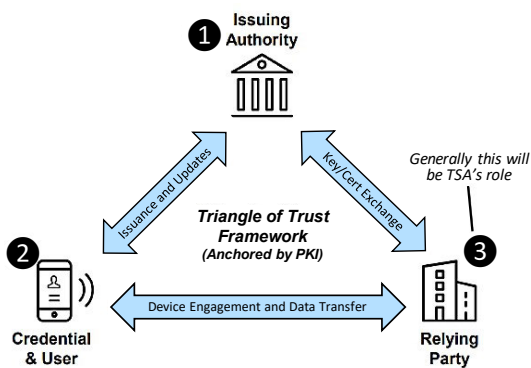Source: *TSA Identity Management: Digital Identity Privacy Roundtable, (briefing) June 23, 2021*

CORE ACTIVITIES

The BI-TC is engaging in mDL standards and technology development by:

- Coordinating with NIST to provide Subject Matter Expert support to DHS Policy and TSA through the DHS mDL and Digital Identity Working Group

- Sponsoring NIST development of a reference reader implementation for interoperability testing based on the international standard (ISO/IEC 18013-5)

- Sponsoring NIST development of Interagency Report (NISTIR) that provides recommendations for security, privacy, and interoperability for mDLs

- Conducting trade studies of processes to assess the integrity, risk, and trustworthiness of Digital Identity approaches for potential DHS acceptance and use

- Participating in standards development, interoperability testing, and developing privacy and security test cases

PERFORMERS AND PARTNERS

DHS S&T is sponsoring research with NIST and the MITRE Corporation, engaging the standards community, coordinating development and testing efforts between TSA and NIST, developing candidate processes to review mDL implementations for DHS acceptance, and enabling broader conformance and interoperability with other federal agency partners.