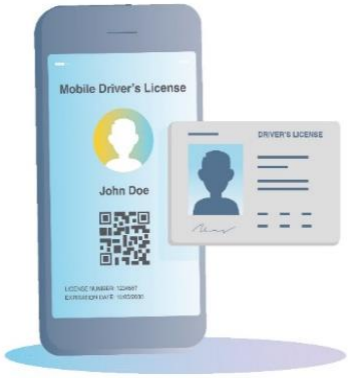
ACCELERATING THE ADOPTION OF MOBILE DRIVER'S LICENSES (mDLs)

The National Cybersecurity Center of Excellence (NCCoE) is helping to accelerate the adoption of mobile driver's license standards and best practices. In collaboration with technology vendors, government agencies, regulators, standards bodies, and organizations seeking to adopt mDLs, the NCCoE will build a reference architecture demonstrating real world business use cases, integrating mDLs with commercially available technology and into business processes.



Challenge

Credential compromise and online fraud are major challenges in today's cyberthreat landscape. The reality is that physical driver's licenses were not designed for our online world. Current best practice for online identity verification asks users to take a picture of their driver's license with a smart phone and to answer knowledge-based questions. The efficacy of these methods is being eroded by new technology such as AI-generated images of driver's licenses accurate enough to bypass document scanning tools and by the ability of bad actors to get ahold of the information needed to answer knowledge-based questions.

Why mDLs?

mDLs function much like a traditional driver's license, carrying information such as name, date of birth, and address but in a digital format accessible through a dedicated mobile application, often referred to as a *digital wallet.* Compared to physical driver's licenses, mDLs have several capabilities that make them easier to use with online and digital transactions:

- mDLs are underpinned by public key cryptography, making the credential cryptographically verifiable.
- mDLs can be integrated natively with device biometrics for user verification.
- mDLs can communicate natively between two mobile applications but also in cross device flows between mobile applications and the web browser on a laptop or tablet.
- mDLs offer the potential for selective disclosure, allowing users to pick and choose which information to share with third parties.

Transactions at financial institutions, healthcare providers, government services, and many other organizations could benefit from enhanced customer experiences, more accurate identity verification, and reduced fraud if they supported mDLs.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE
For more information about this project, visit: https://www.nccoe.nist.gov/projects/digital-identities-mdl

@NISTcyber

linkedin/showcase/nccoe

NCCoE Project Use Cases

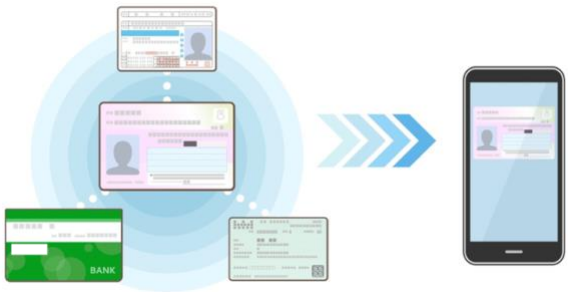
To realize the full value of mDLs, collaboration is needed to mature standards, best practices, and protocols that safeguard user data while promoting adoption of mDLs. For this reason, the NCCoE is bringing together stakeholders from across the mDL ecosystem to build out a reference implementation to promote standards and best practices for MDL deployments and to address mDL adoption challenges. Over the next two years the project will produce guidance addressing:

1. **Know Your Customer/Customer Identification Program Onboarding and Access** which will demonstrate the use of an mDL and/or Verifiable Credentials (VC) for establishing and accessing an online financial account.
2. **U.S. Federal Government Credential Service Provider (CSP) and Federation** which will demonstrate the use of an mDL and/or VC for establishing a CSP account to access federated agency systems.
3. **Healthcare and Electronic Prescribe** which will demonstrate the use of an mDL and/or VC for provider access and prescription uses.

Exploring Multiple mDL Capabilities

The reference architecture for this project will explore multiple mDLs capabilities to include:

- **Remote Identity Proofing** – remote presentment of mDLs as identity evidence with verifiable user attributes as part of an identity proofing process to establish core identity and meet CIP requirements.
- **Authentication** – user authentication after identity proofing and account issuance. This may include using the mDL as an authenticator or may leverage the binding of a phishing-resistance multi-factor authenticator.
- **Step-Up Verification** – after user authentication, using the mDL as a step-up verification for high-risk transactions or when fraud is suspected.



Contact us to learn more at **mdl-nccoe@nist.gov**.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

For more information about this project, visit: https://www.nccoe.nist.gov/projects/digital-identities-mdl

@NISTcyber

linkedin/showcase/nccoe