IDENTITY & ACCESS FORUM

Powered by SECURE TECHNOLOGY ALLIANCE

AN IDENTITY & ACCESS FORUM WHITE PAPER

Building Trust and Accountability in Digital Financial Transactions with the Mobile Driver's License

October 2024

Identity & Access Forum
544 Hillside Road
Redwood City, CA 94062

www.securetechalliance.org

About the Identity and Access Forum

The Identity and Access Forum is a cooperative, cross-industry body dedicated to developing, advancing, and adopting secure identity technologies, including physical and logical access. Through the collaborative efforts of a diverse group of stakeholders, the Forum advocates for market adoption of trusted, user-centric, and interoperable digital identities to ensure safe and seamless access to services across all interactions. The organization operates within the Secure Technology Alliance, an association that encompasses all aspects of secure digital technologies.

The Identity and Access Forum currently has six different Working Groups and Committees establishing the acceptance of Mobile Driver's License (mDL) across the United States ecosystem. IAF's "Jumpstart mDL Committee" publishes content on mDL Connection[1] for the public to understand, trust, and build acceptance of mDL. This Educational Brief is the product of the "mDL in Banking & Financial Services" Working Group. To become involved in any of these efforts, see the membership information on the STA website[2].

Secure Technology Alliance's white paper "The Mobile Driver's License (mDL) and Ecosystem[3]" remains the authoritative source on the concept, usage, and acceptance of mDL across the United States.

[1] https://www.mdlconnection.com/

[2] https://www.securetechalliance.org/membership-information/

[3] https://www.mdlconnection.com/the-mobile-drivers-license-mdl-and-ecosystem/

1. Trust and Accountability in Financial Transactions

In today's digital-first world, financial institutions continue to struggle with the continuously growing challenge of maintaining trust and accountability in their interactions with customers. Identity fraud, through schemes such as account takeovers, fraudulent loans and credit, and synthetic identities have resulted in billions of dollars in losses impacting financial institutions[4].

Data Validation Alone is Not Enough

The continued exposure of personal data, including the recent hack of National Public Data[5], has made it increasingly difficult to verify identities accurately using knowledge-based Q&A or passwords alone, leading to higher risks of fraud. This erosion of trust is further compounded by the widespread loss of privacy and control over personal data. Customers are increasingly aware that their personal information is vulnerable to misuse, leading to a decline in confidence and engagement with digital financial services.

Physical Documents Alone are Not Enough

Document and biometric verifications to translate physical documents to digital formats has strengthened Identity Verification but suffers from high friction and common errors. Problems can occur from bad lighting, damaged documents or bad photos that block good customers. Additionally, there is a growing concern for AI generated attacks as altered documents and images are injected into the capture process.

Strong Authentication Needs Strong Identity

Multi-factor authentication solutions, such as passkeys from the FIDO Alliance, are strengthening our authentication systems by eliminating phishing and other attacks, but only provide part of the solution. These solutions require strong identity verification to ensure true authenticity and accountability for financial transactions. These do not address whether the data presented during financial transactions is for a real, current person and whether that person is the one presenting their own data.

The lack of robust and secure digital identity verification not only exposes Financial Institutions (FIs) to significant fraud risks, but it also creates considerable customer friction and undermines customer trust—an essential element in the relationship between FIs and their clients.

[4] https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf (pg 10)

[5] https://securityintelligence.com/news/national-public-data-breach-publishes-private-data-billions-us-citizens/

2. The Value of Mobile Driver's License (mDL) Approach

Mobile Driver's License (mDL) technology offers a compelling solution to these challenges. mDL is a secure, digital version of a physical driver's license that is issued by a trusted state government authority that contains the core personal attributes about the individual. The mDL also carries the digital signature of the Issuer, meaning that the data cannot be tampered with, and the entity accepting the mDL (called a Relying Party (RP)) can verify the provenance, accuracy, and integrity of the data. Using the standard ISO/IEC 18013-* specifications for mDL, the presenters also have control over the data they share. It serves as a digital identity, providing a highly secure and efficient means of identity verification for financial institutions.

Fraud Reduction

mDLs are issued by government authorities, ensuring a high level of trust and accuracy in the original identity verification process and at the time of issuance. By accepting mDLs, FIs can significantly reduce the risk of impersonation and synthetic identity fraud, as the identity information is securely encrypted and can be verified directly with the issuing authority. The FI may also know that the device from which they were presented the mDL is the one to which it was originally issued, all under the mDL holder's control and without compromising any of their privacy.

Cost Reduction

The use of mDLs can streamline the identity verification process, reducing the need for third-party data validation or extensive manual checks and the associated costs. This not only speeds up onboarding and transactions but also reduces operational expenses. mDL data, direct from the Issuer, is more accurate and up to date than that aggregated by third parties and eliminates errors from typos, optical character recognition (OCR) from scanned physical documents.

Better Customer Experiences

mDLs offer a seamless and user-friendly way for customers to verify their identities. Instead of remembering multiple passwords, answering knowledge-based security questions, or scanning documents, customers can use their mDL to quickly and securely present authentic identity data. This leads to a more convenient and satisfying user experience.

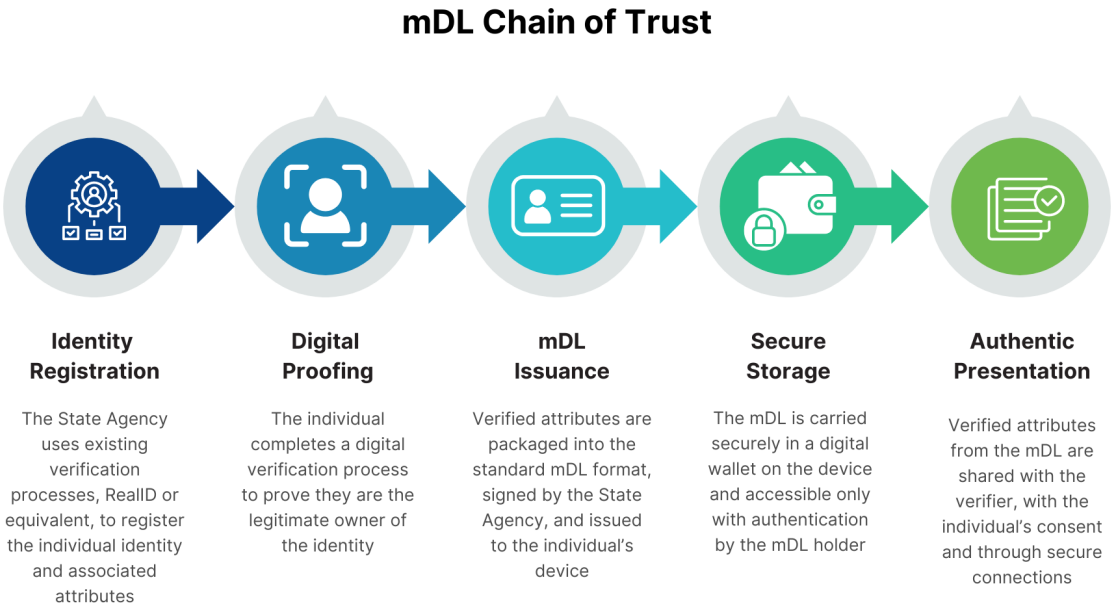
Alignment with Federal Compliance Requirements

Accepting an mDL provides core personal data attributes about customers that are required by regulators to meet their Customer Identity Program, KYC/AML Requirements, as well as strong assurance that the individual interacting with financial systems is the true owner of the identity. National Institute of Standards and Technology (NIST) is actively incorporating mDLs into their version 4 of NIST 800-63 Digital Identity Guidelines[6] and collaborating with FINRA and FDIC regulators to standardize the use of mDLs to meet regulatory requirements.

[6] https://csrc.nist.gov/pubs/sp/800/63/4/2pd

3. Building Trust in Digital Identity

The mDL Ecosystem offers a Chain of Trust that secures each step in building a trusted and reusable digital identity. There are transparent, secure processes at each step in the identity process to ensure that the personal data presented in an mDL is authentic and issued from an authoritative government source. mDLs use technical implementations that protect against fakes, cloning, eavesdropping, and digital manipulation so that Relying Parties/Verifiers can trust them.



The authentic identity presented through this Chain of Trust serves as a strong base for building additional trust, including financial risk checks, AntiMoney Laundering (AML) and Office of Foreign Assets Control (OFAC) checks, and enrolling strong authenticators to keep accounts secure.

4. Security and Risk Considerations

As with any security technology, it is key that implementers follow the standards specification and security guidelines to ensure that bad actors cannot manipulate the process. The following considerations are critical in implementing a secure process as a Relying Party Verifier.

Cryptographic Verification of the Presented mDL

The ISO/IEC 18013-* standard provides technical specifications for the authentication of the wallet and verification of signatures on the mDL document to ensure integrity and authenticity. mDLs should always be verified with an ISO-certified verifier application or equivalent process to ensure integrity and validity through cryptographic verification. The relying party should not depend on visual inspection of the mDL on an individual's device or photos/screenshots of the mDL.

Management of Verification Certificates

Just as cryptographic verification of the document is key to ensuring the integrity of a presented mDL, Relying Parties must pay careful attention to the source of the Verification Certificates shared by Issuers. If Relying Parties were to accept unauthorized Issuer certificates, there is a significant risk that fraudulent mDLs, signed with an unauthorized key, could be accepted as cryptographically valid.

The process of sharing public key certificates from Issuers is not currently defined in the ISO/IEC 18013-* specification, which puts the responsibility onto the Relying Party and/or their technology partners. Currently, several states are publishing public key certificates through AAMVA's Digital Trust Service (DTS)[7] and Verified Issuer Certificate Authority List (VICAL), while others are sharing through public website locations or are sharing directly with Relying Parties upon request.

[7] https://www.aamva.org/identity/mobile-driver-license-digital-trust-service

5. Call to Action: The Time is Now for Innovation

Identity risks are currently everywhere and significant. Identity fraud remains high. When there are failures in an identity verification mechanism, financial institutions face financial losses and reputational damage. Moreover, as customers become more aware of privacy issues and privacy regulations increase, Financial Institutions that fail to offer secure and private interactions will see a decline in customer trust and engagement.

The adoption of mDLs is not just a technological upgrade; it is a strategic imperative for the future of financial services. Accuracy, data integrity, and reinforcing privacy are key to meeting these goals. Financial institutions that act swiftly to support the integration of mDLs into their systems will realize the greatest benefit, and enhancement of their reputation as leaders. The benefits of accepting mDLs extend beyond fraud prevention to enhancing overall customer trust and engagement.

Accepting mDLs is crucial to creating a viable digital identity ecosystem. Issuers are presently doing their part[8]. As of July 2024, ISO-certified mDLs are available to about ~40% of the US population.[9] Additional states have programs in progress to deploy mDL. Financial institutions have a unique opportunity to lead this transformation, helping to prevent financial fraud and mitigate the social harms associated with identity fraud.

The time to act is now, and the support of the financial sector is vital to ensuring the success of this initiative.

[8] https://www.mdlconnection.com/implementation-tracker-map/

[9] Implementation Tracker Map - mDL Connection

6. Glossary: Terms

Account Takeover (ATO): A type of identity fraud where cybercriminals gain unauthorized access to a user's online account, often leading to financial loss or misuse of personal data.

Biometric Verification: A method of identifying individuals based on their unique biological characteristics, such as fingerprints, facial recognition, or iris scans. Biometric verification is often used to enhance security in digital identity systems.

Chain of Trust: A security model where each step in a process is verified by a trusted source, ensuring the authenticity and integrity of data at every stage. In the context of mDLs, the chain of trust ensures that personal data presented is legitimate and securely issued by an authoritative government source.

Customer Identity Program (CIP): A regulatory requirement for financial institutions to verify the identity of their customers. It is part of the broader Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations.

Digital Identity: An electronic representation of an individual's identity that can be used to access digital services. Digital identities can include data such as usernames, passwords, and biometric information.

ISO/IEC 18013-* Standard: The set implementation standards for Mobile Driver's Licenses developed including ISO/IEC 18013-1 to ISO/IEC 18013-7, with special attention to 18013-5 and 18013-7 for the definition of the data structure and implementation of technical protocols. Following and certifying implementations against this standard ensures that solutions are secure and interoperable.

Mobile Driver's License (mDL): A digital version of a physical driver's license issued by a government authority. The mDL serves as a secure, encrypted form of digital identity that can be used for identity verification in various contexts, including financial transactions.

Phishing: A type of cyberattack where attackers deceive individuals into providing sensitive information, such as usernames, passwords, or credit card numbers, by pretending to be a trustworthy entity.

Relying Party (RP) for Verifier: An entity that relies on the verification of identity information provided by an external source, such as a government-issued mDL. The RP uses this verified identity information to grant access to services or perform transactions. May also be referred to as the Verifier.

Synthetic Identity Fraud: A type of identity fraud where criminals combine real and fake information to create a new, synthetic identity. This identity is then used to open fraudulent accounts or commit other financial crimes.

7. Acknowledgements

Participants
Christine Cobuzzi – Get Group NA
Lori Daigle - AAMVA
Simon Hurry - Visa
Alex Jones - MATTR
David Kelts - DecipherID
Anthony Lopreiato - Mastercard
Carolyn Manis Sorensen – Skavi Dev
Ed Perez - Verifone

8. Legal Notice

The Identity & Access Forum endeavors to ensure, but cannot guarantee, that the information described in this document is accurate as of the publication date. This document is intended solely for the convenience of its readers, does not constitute legal advice, and should not be relied on for any purpose, whether legal, statutory, regulatory, contractual, or otherwise. All warranties of any kind are disclaimed, including but not limited to warranties regarding the accuracy, completeness, or adequacy of information herein. Merchants, issuers, and others considering Device Identification & Authentication technologies are strongly encouraged to consult with the relevant identity & access networks, vendors, and other stakeholders prior to implementation.