IDENTITY & ACCESS FORUM

Powered by SECURE TECHNOLOGY ALLIANCE

AN IDENTITY & ACCESS FORUM EDUCATIONAL BRIEF

Mobile Identity Use Cases in Financial Services

March 2025

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/

In-Person Identity Verification for Financial Transactions at a Branch

- Verify a Customer for Common Teller Transactions at a Branch
- Verify a New Customer at a Branch for Account Opening, Loan Application
- Verify a Customer for Self-Service at an ATM or Kiosk Summary Snapshot

Summary Snapshot

Description

Financial institutions require strong identity verification and authentication for customers to access services like balance inquiries, withdrawals, loan applications, or notarization. The Mobile Driver's License (mDL) offers a secure digital solution to improve customer experience, safeguard interactions and ensure compliance. The mDL transmits verified identity attributes, based on attributes and identity proofing done by the issuing government agency, directly from the individual holder of the identity to the financial institution. The cryptographic signature of the government issuing authority ensures a trusted and authentic identity is presented. The transfer of attributes uses interoperable, international standards that guarantee security and privacy for all parties involved. By enabling consent-based sharing of only essential, verified attributes from a tamper-proof credential, mDL safeguards both the customer, the institution, and the representative.

Use Cases in a Branch

Definition	Participants	Challenges
Sub-case 1 Goal: Verify an Existing Customer to access existing assets/accounts/services within the bank branch. An existing customer of a financial institution is asked to present a photo id for verification of identity for an in-person financial transaction in a branch that is facilitated by an employee or representative. Transactions might include: ● Traditional teller banking - Check-cashing, Withdrawal, Account Maintenance, Balance Inquiry, Cashier checks, Payday loans ● Representative-facilitated financial planning, portfolio account lifecycle, loans, line of credit ● Notarial acts	List ecosystem participants for this use case: 1. [Issuing Authority] State DMV 2. [Relying Party] Financial Institution Branch 3. [Relying Party] Employee of Financial Institution (Teller) 4. [Consumer/Holder] Customer or Member Bank Tellers have the risk of performing document authentication per their fraudulent document training when a physical ID document is presented.	List the key challenges for this use case implementation: Verifier/Reader technology required: Scanning and verifying the mDL may use existing hardware (e.g. NFC, Bluetooth) or could be added as simple extension such as tablet or stand-alone reader that has a camera and Bluetooth capability. Integration would be desirable to connect the document scanned with financial institution systems but may require new development by the financial institution or their system providers. Completing this step through a drive-through has been shown to be compatible with Bluetooth-enabled Reader/Verifiers.
Sub-case 2 Goal: Verify a new Prospective Customer within a bank branch and provide verified attributes for KYC/AML compliance An individual applies to become a new customer or open a new type of financial account or product with a financial institution. Transactions might include: ● Representative-assisted account opening and onboarding for financial accounts and services	List ecosystem participants for this use case: 1. [Issuing Authority] State DMV 2. [Relying Party] Financial Institution Branch 3. [Relying Party] Employee of Financial Institution 4. [Consumer/Holder] Applicant for a bank account Bank Tellers have the risk of performing document authentication per their fraudulent document training when a physical ID document is presented. Automated KYC/AML checks are valid against known identities.	Verifier/Reader technology required: Scanning and verifying the mDL may use existing hardware (e.g. NFC, Bluetooth) or could be added as simple extension such as tablet or stand-alone reader that has a camera and Bluetooth capability. To verify the individual person is the owner of the document may require additional local facial biometric software that can be part of the mDL Reader/Verifier installed app or follow sequentially afterward using the validated mDL portrait. mDL provides verified identity attributes and claims, but financial institutions must still enforce CIP compliance and evaluate customer financial risk.

Definition	Participants	Challenges
Sub-case 3 (unattended) Goal: Verify an existing customer for in-person but unassisted interactions at a kiosk, ATM, or computer provided by the institution An existing customer of the financial institution presents an mDL for digital access to an unmanned kiosk or digital device to complete financial transactions. Step-up identity verifications can be used in or out of band for higher risk transactions. Transactions might include: ● Kiosk for account maintenance, applications ● Terminal or tablet provided by the branch	List ecosystem participants for this use case: 1. [Issuing Authority] State DMV 2. [Relying Party] Financial Institution Branch 3. [Relying Party] Existing or renovated systems of Financial Institution 4. [Consumer/Holder] Customer or Member	Integration between the mDL and financial systems[4] for the purpose of identity verification of the customer is outside the scope of this document, but the mDL can provide unique, verified identity attributes, including portrait, that can be used to match the customer identity into the financial system of record. For unattended interactions, additional verification through biometrics may be desirable to ensure that the holder of the device is the real owner of the credential.

Variables to the Transaction

Tap, Nearby, Distance, and Over the Internet? Multiple Interactions to Complete the Use Case?	Is the mDL Holder device connected to Internet Services? Is the tablet device.	Typically Attended or Unattended (for User Authentication)
Tap, Nearby, Split devices where one accepts mDL and provides the results to a semi-remote device (as might be seen at a driveup window	Typically connected devices and readers. Even in remote bank branches, WiFi may be available to customers and prospective customers for connecting mDL apps to Internet service It is customary, even in portable banking scenarios, that the teller equipment will have reliable connection at least to home and through to the Internet	Typically attended by a branch employee Semi-attended (drive-up with teller inside) is achievable.

[4] Known integrations to date have included (1) standalone reader tablets, (2) reader tablets with an ESB as intermediary that controls a tablet from a teller machine, (3) USB connected reader devices to the teller computer, (4) ATM reader devices that perform mDL verification and data acquisition on behalf of an internal teller computer.

Value Proposition

Allowing and encouraging customers or members to use an mDL for presenting their form of identification provides benefits for the individual and the financial institution.

Convenience

The phone is ubiquitous, and customers have become used to presenting the phone or scanning a QR code for access for everything from payments to movie tickets to boarding a plane. Using the mDL creates contactless interactions and can be integrated into in-person systems to make it simple for a representative to quickly access appropriate personal information.

Because the transaction is contactless, Bank Tellers do not have to handle something handed to them by the customer. This can safeguard employees. In fact, it should be Bank policy that employees do not handle mobile devices of customers, even though convention dictates that ID cards are handled.

Fraud Prevention

The bank can actively verify the document cryptographically to see that the data is untampered, the document has not been revoked, and the document was issued from a trusted authority. This bypasses visual document authentication procedures that rely on training and skillset of the Teller.

The bank can bypass some external data validation procedures. In addition to authenticity, metadata information about the mDL, such as how recently the cryptographic signature was applied, can be used to assure that the document is still valid. Revoked and fraudulently marked physical documents can still be in circulation since governments often don't have a mechanism to retrieve them from circulation.

Receipt of the interaction provides evidence of validation and identity verification.

Although in the beginning, not every individual would have an mDL and fraudsters would continue to use more vulnerable processes, mDL interactions can be categorized as not likely to be at risk which frees up time and energy to put diligence into solutions for weaker channels.

Use of mDL may deter unauthorized access of customer data by employees by connecting the presentation of the mDL to the system authorization of account access.

Audit and Compliance

A clear audit trail of the verification process is critical for the safety and security of the holder, the employee interacting with the holder, and the financial institution. This creates transparency and non-repudiation around transactions.

When onboarding a new customer or opening a financial account, institutions must adhere to the KYC requirements that require verification of key attributes. The mDL can provide strong verification of the identity attributes required by Customer Identification Programs as outlined in financial regulations.

Data provided is the latest update from an authoritative source of record, which can prevent confusion around out-of-date or expired documents and accommodate scenarios like legal name changes more easily than with physical documents.

Customer Perception and Satisfaction

Adoption of mDL as a digital identity contributes to company reputation and differentiation as a technology-forward financial institution that is adopting advances in technology and improving member experiences.

mDL provides a digital representation of identity that can streamline interactions between the customer or member and a representative by automating the identification and authentication process to seamlessly connect into financial institution digital systems when a representative is assisting the customer. The customer also sees how their privacy and security are ensured by the system when it requires their mDL and consent to access accounts.

Preparing for the Future

As mDLs become mainstream and the remote presentation standards are ratified and implemented, financial institutions are well-suited to take advantage of Cost-Savings and Customer-Satisfaction in being able to offer more things remotely at the convenience of the member by using the security capability of mDL.

Risk Levels and Mitigation

Issuing Authority Risk	Relying Party Risk	Consumer (Holder) Risk
N/A	If the end user has granted access to their device to another individual, there may be risk that someone other than the individual is able to present the mDL. Applicable State laws, if any, should indicate that the acceptance of mDL meets the same criteria as physical ID. This is true in all mDL issuing jurisdictions, and should be verified by the Bank.	
	Mitigations 1. Include Server-Side verification to check document status 2. Perform face verification against the document to confirm and audit that the individual presenting the ID is the owner of the credential 3. With appropriate Member/Customer consent, create a record of the event and hold PII for a limited time for fraud investigation purposes 4. Follow-up review by a Bank Employee once mDL processing is complete – double check or identity verification.	Mitigations 1. Only put the mDL on devices for own personal use 2. Consumers should revoke any mDLs that are not within their control

Legal and Compliance Requirements

Know Your Customer (KYC)

Financial Institutions operating in the US must adhere to regulations to identify and verify customers in order to do business. This is often referred to as Know Your Customer (KYC). FDIC and FINRA provide guidance around Customer Identification Program (CIP) that is required for maintaining compliance:

1. Verify the identity of any person seeking to open an account, to the extent reasonable and practicable;
2. Maintain records of the information used to verify the person's identity; and
3. Determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to brokers or dealers by any government agency.

The mDL provides identity documentation evidence and data validation through strong cryptographic means to support the KYC process as well as a clear audit trail of the presentation and validation of the evidence through the ISO/IEC 18013-* protocols.

Note that the verification mDL does not provide any verification against Anti-Money Laundering (AML) or Office of Foreign Assets Control (OFAC) lists and those checks must still be performed by the financial institution.

Organizations may introduce additional safeguards to further ensure the connection between the mDL and the individual presenting it through capture and validation of additional evidence, verification through biometric checks and additional risk assessment.

Anti Money Laundering

Banks may proceed with AML verification as per current processes because the attribute set from the mDL will have already been verified to be from a trusted government issuing authority.

NIST Identity Assurance Levels

NIST is updating the NIST 800-63 Digital Identity Guidelines to incorporate the presentation of digital credentials such as the mDL into standard approach and formal assurance levels. Although financial institutions in the US may not required to adhere to NIST, many use the guidance for their own policies in Identity Verification and approach to Customer Identification Program compliance.

mDLs that conform to AAMVA's mDL Implementation Guidelines[5] have been assessed currently to supply IAL-2 identity assurance conforming to 800-63-3. The physical card has been assessed as IAL-3 because of the pervasive and well-known delivery mechanism (direct or US Mail). The physical card, however, is more prone to usage after loss or theft since it cannot be deactivated remotely in the way that the mDL can be. Please perform internal investigation to ensure that IAL-2 is sufficient and consider the RealID flag that is part of the AAMVA mDL namespace as risk mitigation if IAL-3 is required for your use case. This relates only to the proofing level to obtain the credential. User authentication must be performed at the time of credential acceptance according to policy or Authentication Assurance Level.

Data Required to Complete Use Case

The data requirements for compliance include at a minimum the Name, Date of Birth, and if available Social Security Number, to verify the identity against required AML/OFAC services for KYC. In addition,

[5] https://www.aamva.org/assets/best-practices,-guides,-standards,-manuals,-whitepapers/mobile-driver-s-license-implementation-guidelines-1-2

per bank policy, the Issuer (State) and Document Number (DL#, ID#) may be obtained as evidence of identity or if SSN is not available. There may be legitimate business and security needs for additional personal information from the mDL. A full set of data elements is available through the ISO 18013-5 standard. Data minimization is one major advantage of mDL for you to consider conformance.

Data Attributes

Attribute	Used For	Collected Today	Required to Store
State & Card Number	Audit	Yes	Not Required
Full Legal Name	Compliance	Yes	Yes
Date of Birth	Compliance	Yes	Yes
Social Security Number or Foreign Tax ID	Compliance	Yes	Yes

When data is obtained from an mDL, the reader device should indicate “Intent To Retain” for all data.

Consent for Purpose and Extended Use

Financial Services regulations, in particular Bank Secrecy Act and enhancements from the Patriot Act, require entities to hold appropriate personal data for audit and security purposes, and any fields retained from the mDL must follow laws and regulations for protecting personal data. This should follow existing regulations, particularly Gramm-Leach-Bliley Act for Consumer Financial Privacy. While scanning physical cards exposes the Bank to all personal data from the card, mDL does give the opportunity to reduce data storage liability and ask only for what is necessary.

Data fields and the intent of the provider to hold data from the mDL must be clearly requested for user consent and the entity must publicly post appropriate privacy policies and terms and conditions as is required by laws and security practices in place to protect consumer data.

Implementation

The mDL Reader must verify the digital signature on the data received from presented mDL to ensure that it is authoritative, from a known Issuer, intact, not tampered, and current/fresh. The reader or associated systems should display the appropriate data for inspection by a qualified employee, including the portrait for identity verification of the applicant – visual or biometric (see below). mDL data can be retrieved from the mDL Reader into the Teller software, ensuring accuracy and provenance.

As the mDL becomes more integrated with existing Identity and Authentication systems, the verified mDL data may be forwarded securely to an existing financial services system to create a secure session anchored by the identity presented in the mDL.

Identity Verification is performed by the teller/operator for Attended Sub-Cases 1 and 2 (above table). When the financial institution or teller interactively determines that there may be elevated risk of impersonation, the photo data from the mDL can be used to biometrically match the applicant.

User Journey Example

	Secure Wallet Access	Activate Presentation	Verification Processing	(Optional) Verification of the Person Presenting the mDL	Verification Success
Holder (Customer)	Holder opens the mDL wallet and authenticates locally	Holder activates the QR code or holds the unlocked device close to the reader	Holder provides consent on data being shared with the Verifier	(Optional) Holder presents clear view of face for the camera on the Verifier System	Holder can request assistance with service transactions
mDL Wallet	Wallet enforces local authentication (Device Face, Fingerprint or Code)	Compliant wallet generates QR code or initiates NFC handshake with the reader			
Verifier System		Verifier application scans QR code or accepts NFC handshake with the device	Verifier application computes appropriate cryptographic checks and may check assertion against revocation list in privacy preserving protocol	(Optional) Verifier system matches face of individual present against the mDL data	(Optional) Verifier application securely passes required data to financial institution system to invoke a session or pre-fill required fields
Financial Rep (Employee)			Employee representative can see the basic required info and that the mDL is successfully verified		Employee representative can assist the Holder/Customer with service transactions

Note: The above can be customized into UML sequence diagrams specific for the use case.

Proposed Metrics

Adoption and Volumes - What is the number of transactions secured by the mDL as compared to other accepted identification and verification processes?

Error Rates - For customers who choose the mDL, what number are able to successfully present the mDL to the reader and have it verified appropriately by the system?

Fraud Rates - For transactions secured by the mDL, how has mDL impacted the amount of fraud compared to other accepted identification and verification processes?

Processing Time – What is the average processing time of mDL versus DL transactions, including all data scanning time and document authentication time and the savings of avoiding form-fill?

Customer Satisfaction - How much time does it take to verify the mDL in comparison to other accepted identification and verification processes? If Net Promoter Score (NPS) is captured for the experience, does mDL change the outcome compared to other identification and verification processes?

New Unattended Operations Attained – Is the Bank able to offer services through new channels that it was not previously able to.

Challenges

Challenge	Mitigating Actions
Availability of ISO 18013-5 compliant mDL	Not all US States and Territories have an mDL yet, but 17 states have received full certification of their ISO compliant solution and many additional states are working toward their solutions: https://www.mdlconnection.com/implementation-tracker-map/
Adoption and Setup by Holders	Within those states, adoption rates are still in their infancy, but the use of mDL at TSA at airports across the US and multiple rollouts in retail (e.g. Liquor and grocery stores) and banking (regional Credit Unions) demonstrates to holders that there are places to use the mDL that provide convenience and value.
Hardware for Reading mDLs	There are implementations for in-person mDL that utilize specific hardware (e.g. TSA) to combine the full capability of the mDL presentation and verification plus biometric verification of the individual, but verification of the mDL itself can be accomplished with a simple verification app on a standard phone or tablet device that supports a camera or NFC and Bluetooth. SDKs are also available for most computer and phone models.

Integrations with Existing FI Systems	Financial Institutions gain the most from mDL with integration into existing FI systems to facilitate account services and generate appropriate audit and system records as part of the verification process. mDL Jumpstart[6] will continue to partner and build relationships with software providers to incorporate mDL into traditional IAM and financial platform systems. Some mDL reader systems utilize web services and therefore can be controlled through Bank ESB.

[6] https://www.securetechalliance.org/identity-and-access-forum/

Security Measures to Be Implemented

Cryptographic Verification of Presented mDL

The ISO-18013-* standards provide technical specifications for the authentication of the wallet and verification of signatures on the mDL document to ensure integrity and authenticity. mDLs must always be verified with a verifier application or equivalent process to ensure integrity and validity through cryptographic means. The relying party must not rely on visual inspection of the mDL on an individual's device.

Selective Disclosure and Data Minimization

Organizations should strive to minimize the personal data requested and stored to protect customer privacy, adhere to privacy regulation, and limit their own liability for protection of personal information. mDL standards support selective disclosure such that the Relying Party can request and verify individual attribute fields, for example the age range 21+, without the disclosure of all attributes in the mDL document.

Additional Security Considerations

Distribution of Public Keys

The mDL ecosystem includes multiple legitimate issuers of digital credentials and each State Issuing Authority will have different public keys for verification of their respective mDL credentials. In order for a Relying Party to verify and trust any presented mDL, the Relying Party must have access to a trusted list of public keys used by known good issuers. Relying parties may acquire public keys directly from the Issuer or through a trusted service. Accepting public key material from any entity other than the government issuer or trusted service provider opens the Relying Party to risk of acceptance of fraudulent mDLs.

AAMVA mDL Digital Trust Service

One implementation of a trusted service provider for public key material is the AAMVA Digital Trust Service (DTS). This service stores and distributes public key material for mDL verification on behalf of the State Issuing Authorities. The State Issuing Authorities provide public key material to DTS, which is then available to Relying Parties as Verified Issuing Authority Certificate Authority List (VICAL). This service is also responsible for certificate revocation in the case that Issuing Authorities rotate key material. Financial institutions should register for access to VICAL and appropriate key material and metadata for verifying mDLs.

Revocation Checks and Expiration for mDL

For readers implementing the server retrieval method, status and revocation of the mDL will be verified at the time of verification. Relying parties should not accept mDLs that have been revoked or are expired. For readers implementing local phone-to-phone communications, the metadata about the digital signature on the mDL and the expected duration of validity of the signature can be used for high assurance situations.

Reader Identification Certificates

It is recommended that reader devices identify themselves as an official reader of the Bank so that cardholders are aware of who they communicate with. This will particularly hold true for unattended situations where the cardholder needs assurance that they are tapping/scanning on an official Bank

reader device, even if the location of the device seems relatively secure. (At this time, commercial reader certificates are not in wide circulation.)

Examples

Utah Community Credit Union Accepts mDL

Utah Community Credit Union (UCCU) was one of the first financial institutions to accept the certified Utah mDL in an In Person verification process in branch offices.

America First Credit Union Accepts Utah and Arizona mDL at Branch Locations

America First Credit Union (AFCU), based in Utah, is one of the first Financial Institutions to embrace the convenience and security of presenting an mDL at its branch locations in Utah, Idaho, Arizona and Nevada.

References

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

Secure Technology Alliance - MDL Connection

ISO/IEC 18013-5 Standard for Mobile Driving License

AAMVA mDL Digital Trust Service

Bank Secrecy Act

Customer Identification Program (FDIC)

GBL Act - Financial Privacy Rule

Acknowledgements

Participants
Lori Daigle - AAMVA
Simon Hurry - Visa
David Kelts - DecipherID
Diego Koga - MATTR
Carolyn Manis Sorensen – Skavi Dev
Ed Perez - Verifone
Gregory Wren - Discover

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.