IDENTITY & ACCESS FORUM
Powered by SECURE TECHNOLOGY ALLIANCE

AN IDENTITY & ACCESS FORUM USE CASE

Mobile Identity Use Cases in Age Verification

July 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/

1. Mobile Identity Use Cases in Age Verification

- In-Person Age Verification for Liquor Purchase at a Licensed Establishment
- Attendant Verifies a Customers Age at a Licensed Establishment.
- Verify a Customers Age for Self-Service at an Unattended Kiosk.
- Verify Customer Age before an entry into a Bars, Restaurants, concerts etc.
  Online Age Verification for Liquor Purchase using delivery apps or websites.
- Online purchase of alcohol for pickup through a liquor store website or delivery app.
- Online purchase of alcohol with age verification before checkout and repeat verification of Age and Matching name, Portrait upon delivery.

2. Summary Snapshot

Description

Retailers and establishments selling alcohol require accurate age verification to comply with legal drinking age requirements, prevent unauthorized sales, and to maintain their liquor licenses.

Mobile Driver's License (mDL)

mDL provides a secure, portable digital solution that enhances customer convenience while reliably verifying age without sharing unnecessary data. After user consent, the mDL securely transmits age attributes that are cryptographically signed to an mDL Reader. The mDL Reader ensures that they are accurate, unaltered, and issued by a government agency. The cryptographic signature produced by the issuing government authority guarantees that the presented attributes are authentic and tamper-resistant, by verifying it against the known, valid public key of the Issuing Authority. Using interoperable, international standards, mDL enables consent-based sharing of only the necessary data, without exposing unnecessary personal details such as home address.

mDL Reader

Verifying an mDL ensures a seamless, private, and secure transaction, benefiting both the customer and the business.

Reader technology is required:

- Images of an ID document on the customer's phone screen cannot be trusted.

- Scanning and verifying the mDL can be done using existing hardware), or through solutions such as an app, a tablet, an integrated reader added into POS or KIOSK systems, or a standalone reader equipped with a camera, NFC, Bluetooth and Internet[4].

Identity Data

Retailers and establishments may retain, for audit purposes, attributes after user consent or a receipt of the transaction. The mDL typically informs the user that their data will be stored before they consent. In general, as with the physical cards, it is best to verify what is legally required and not store customer data. Adhere to data minimization principles and don't store more than necessary as data breaches can be costly.

Identity Verification

In ISO/IEC 18013-5:2021, the expectation is that the mDL Holder will consent to share the cryptographically signed portrait image from their mDL so that an Attendant – typically an employee of the Verifier or Relying Party – can visually compare the presenter to the portrait. This portrait may also be used to algorithmically compare a live picture of the mDL Holder to the shared, verified portrait image. This biometric comparison may happen in either attended or unattended transactions.

Possession of a device that can present a cryptographically valid mDL is one “user authentication” factor in a transaction. It is not typically sufficient to determine that the presenter is the rightful ID holder without visual or biometric checks. Since most commercial smart phone devices allow multiple fingerprint or face enrollments for device unlock those modalities should not be relied upon as definitive that the presenter is the rightful mDL Holder.

In ISO/IEC 18013-7:2024, during remote presentations, it is the responsibility of the Reader and Relying Party to compare a live biometric image of the mDL Presenter with their mDL Data. Device biometric releases of the data should not be relied upon as definitive user authentication. Future versions of this standard and 18013-5 are expected to incorporate user authentication methods such as the Open ID Foundation protocols, and wallet assertions. These enhancements will allow certified devices and applications to authentication users and include the authentication result as part of the “device signed” mDL Data.

Very high-risk transactions should assess and perform user authentication above and beyond that supplied by the mDL standards to mitigate risk. Out of band identity validation services, shared customer secrets, liveness algorithms, biometric equipment, and reputational checks may be appropriate in these circumstances at the cost and responsibility of the Relying Party.

[4] Additional information on readers is being published on https://www.mdlconnection.com/ during 2025

3. Use Cases for the Purchase of Alcohol

A Licensed liquor service establishment typically refers to any business or venue where alcoholic beverages are served to customers for consumption on the premises[5].
A licensed establishment is a broader term that refers to any business or property that has obtained a government-issued license to engage in regulated activities, which could include the sale, service, or distribution of alcohol.

Definition	Participants	Challenges
Sub-case 1 (attended) Goal: Verify a Customer's Age to Access Liquor Purchases/Services at a Licensed Establishment. A customer is asked to present a valid photo ID for age verification to complete an in-person liquor purchase or access related services at a Licensed Establishment. This process is facilitated by an employee or representative. Transactions might include: • In-person liquor purchases at a staffed counter. • In-person Age Verification across a bar top or table	List ecosystem participants for this use case: 1. [Issuing Authority] State Agency for issuance of mDL, not for transaction time transactions. 2. [Relying Party] Liquor Regulatory body at State/County level, for example: ABC, County Level, State Level etc. 3. [Relying Party] Liquor Service Outlet 4. [Relying Party] Employee of Liquor Service Outlet using a Reader. 5. [Consumer/Holder] Customer or Member.	List the key challenges for this use case implementation: Reader technology required, for more information, see section on mDL Reader above. It is beneficial for faster workflow to integrate the scanned document with Licensed Establishment systems; however, this may require additional development by the system providers. Personnel at the Licensed Establishment must rely on their training to authenticate physical ID documents, which carries the risk of human error when identifying fraudulent IDs. mDLs are definitive. Verifier/Reader technology required:

[5] See Appendix, References: Difference Between Liquor Service Establishment and Licensed Establishment

Definition	Participants	Challenges
		Scanning and verifying the mDL can be done using existing hardware (Required QR Code Scanner, BLE, and NFC), or through additional solutions such as a tablet, an integrated reader added to current systems, or a standalone reader equipped with a camera, NFC, and Bluetooth. Acceptance and use of mDLs for age verification typically must be pre-approved from state and local liquor boards. Several jurisdictions, including state liquor boards, have issued rulings affirming the legal use of mDL[6][7] as valid forms of identification for age restricted transactions. STA can provide a guidance template regarding acceptance of mDL upon request[8].
Sub-case 2 (unattended) Goal: Verify a Customer's Age to Approve Liquor Purchases/Services at an Unattended Kiosk or Self-Checkout	List ecosystem participants for this use case: 1. [Issuing Authority] State Agency for issuance of mDL, not for transaction time transactions. 2. [Relying Party] Liquor Regulatory body at State/County level, for example: ABC, County Level, State Level etc. 3. [Relying Party] Licensed Liquor Establishment	Reader technology required, for more information, see section on mDL Reader above. To verify the individual person is the owner of the document may require a camera and facial biometric software that can be part of the mDL Reader such as Kiosk or Self-Checkout.

[6] https://www.rld.nm.gov/wp-content/uploads/2024/12/Guidance-regarding-introduction-of-New-Mexico-Mobile-ID.pdf

[7] https://sla.ny.gov/system/files/documents/2024/10/advisory_2024-2_-_use_of_new_york_state_mobile_id_for_the_sale_of_alcoholic_beverages_0.pdf

[8] https://www.mdlconnection.com/get-involved/ to request the template document, which may also become available from https://www.mdlconnection.com/mdl-uses/age-verification/

Definition	Participants	Challenges
A customer must complete an age verification process at a self-service kiosk or self-checkout system before purchasing liquor or accessing related services. This process might not involve direct employee assistance and therefore requires automated ID scanning and customer Identity Verification. Transactions might include: ● Purchasing alcohol at a self-checkout station in a retail store, stadiums, or at a market. ● Using a self-service kiosk to dispense liquor (e.g beer vending machine)	4. [Relying Party] Existing or renovated self-checkout kiosks or standalone kiosks of Liquor Outlet 5. [Consumer/Holder] Customer or Member.	Self-checkout systems rely on customers to scan and verify their own IDs, which carries the risk of accepting fraudulent IDs. At self-checkout, an employee must intervene to enter the date of birth, adding an extra step that still carries the risk when verifying IDs. Future versions of ISO/IEC mDL standards[9] may permit the mDL Holder device to verify before presenting mDL data and will include the signed result with the mDL data. Acceptance and use of mDLs for age verification typically must be pre-approved from state and local liquor boards. Several jurisdictions, including state liquor boards, have issued rulings affirming the legal use of mDL[10][11] as valid forms of identification for age restricted transactions. STA can provide a guidance template regarding acceptance of mDL upon request[12].

[9] https://github.com/ISOWG10/ISO-18013 contains pre-release standards for public review. Please look for Holder Binding or User Authentication topics.

[10] https://www.rld.nm.gov/wp-content/uploads/2024/12/Guidance-regarding-introduction-of-New-Mexico-Mobile-ID.pdf

[11] https://sla.ny.gov/system/files/documents/2024/10/advisory_2024-2_-_use_of_new_york_state_mobile_id_for_the_sale_of_alcoholic_beverages_0.pdf

[12] https://www.mdlconnection.com/get-involved/ to request the template document, which may also become available from https://www.mdlconnection.com/mdl-uses/age-verification/

Definition	Participants	Challenges
Sub-case 3 (unattended + attended) Goal: Online Purchase of Alcohol via Website or an App and then followed by Delivery of Purchased Alcohol. A customer must complete an age verification process when purchasing through a liquor store website or a delivery app before delivery. The process of verification during delivery is facilitated by a delivery employee or representative. The delivery employee will revalidate age during delivery. Transactions might include: ● Online purchase of alcohol through a liquor or delivery app. ● Online purchase of alcohol with digital age verification at checkout and additional verification upon delivery. ● In-person verification during delivery, requiring the recipient to present a valid ID to the delivery personnel.	List ecosystem participants for this use case: 1. [Issuing Authority] State Agency for issuance of mDL, not for transaction time transactions. 2. [Relying Party] Liquor Regulatory body at State/County level, for example: ABC, County Level, State Level etc. 3. [Relying Party] Liquor Purchases/Services Online. 4. [Relying Party] Delivery Employee 5. [Consumer/Holder] Customer or Member	Reader technology required, for more information, see section on mDL Reader above. Displaying and verifying the mDL using existing hardware and requiring an Internet connection, based on ISO/IEC 18013-7 standard. Delivery Agent might be held accountable during delivery, depending on the state alcohol beverage control, both the liquor establishment and delivery agent might be held accountable. Scanning and verifying the mDL may use existing hardware (e.g. NFC, Bluetooth) or could be added as simple extension such as tablet or integrated reader into existing hardware or stand-alone reader that has a camera, NFC and Bluetooth capability. An active Internet connection maybe required. For unattended interactions, additional verification through biometrics may be desirable to ensure that the holder is the real owner of the credential.

Definition	Participants	Challenges
		For website or app purchase, Identity Verification with biometrics may not be possible given hardware available and secure communications pathways. Identity Verifcation inherent in the proof of possession of an mDL may be sufficient to approve purchase when follow-up age verification is performed at the time of delivery. During Delivery the portrait associated with the order can be matched against the customer at the point of delivery for Identity Verification. If any biometrics are used for identity verification through this process, once the order is complete the biometric data must be handled appropriately, such as deleting after use, etc. Acceptance and use of mDLs for age verification typically must be pre-approved from state and local liquor boards. Several jurisdictions, including state liquor boards, have issued rulings affirming the legal use of mDL[13][14] as valid forms of identification for age restricted transactions.

[13] https://www.rld.nm.gov/wp-content/uploads/2024/12/Guidance-regarding-introduction-of-New-Mexico-Mobile-ID.pdf

[14] https://sla.ny.gov/system/files/documents/2024/10/advisory_2024-2_-_use_of_new_york_state_mobile_id_for_the_sale_of_alcoholic_beverages_0.pdf

Definition	Participants	Challenges
		STA can provide a guidance template regarding acceptance of mDL upon request15.

Table 1.1: Sub Use Cases

Variables to the Transaction

Typically, Attended or Unattended (for User Authentication)	Tap, Nearby, Distance, and Over the Internet? Multiple Interactions to Complete the Use Case?	Is the mDL Holder or Reader device connected to Internet Services? Is the tablet device.
Table 1.1: Sub-case 1 (attended)	**ISO/IEC 18013-5:** *Engagement Type:* Nearby for QR Code Scanning or Tap with NFC. *Data Transfer:* Nearby for BLE. **ISO/IEC 18013-7:** *Engagement Type*: Nearby for QR Code Scanning or Tap with NFC. *Data Transfer:* Over the Internet.	**ISO/IEC 18013-5:** Do not require mDL Holder Device to connect to Internet Services. Do not require mDL Reader Device to connect to Internet Services. **ISO/IEC 18013-7:** Both mDL Holder and Reader Device need to connect to Internet Services.
Table 1.1: Sub-case 2 (unattended)	**ISO/IEC 18013-5:** *Engagement Type:* Nearby for QR Code Scanning or Tap with NFC. *Data Transfer:* Nearby for BLE. **ISO/IEC 18013-7:** *Engagement Type:* QR Code Scanning. *Data Transfer:* Over the Internet.	**ISO/IEC 18013-5:** Do not require mDL Holder Device to connect to Internet Services. Do not require mDL Reader Device to connect to Internet Services. **ISO/IEC 18013-7:** Both mDL Holder and Reader Device need to connect to Internet Services.

[15] https://www.mdlconnection.com/get-involved/ to request the template document, which may also become available from https://www.mdlconnection.com/mdl-uses/age-verification/

Typically, Attended or Unattended (for User Authentication)	Tap, Nearby, Distance, and Over the Internet? Multiple Interactions to Complete the Use Case?	Is the mDL Holder or Reader device connected to Internet Services? Is the tablet device.
Table 1.1: Sub-case 3 (unattended and attended)	**ISO/IEC 18013-7:** *Engagement Type:* Nearby for QR Code Scanning or Tap with NFC. *Data Transfer:* Over the Internet. And in addition, during delivery as needed. **ISO/IEC 18013-5:** *Engagement Type:* Nearby for QR Code Scanning or Tap with NFC. *Data Transfer:* Nearby for BLE or NFC.	**ISO/IEC 18013-7:** Both mDL Holder and Reader Device need to connect to Internet Services. And in addition, during delivery **ISO/IEC 18013-5:** Do not require mDL Holder Device to connect to Internet Services. Do not require mDL Reader Device to connect to Internet Services.

Table 1.2: Variables in Interaction Modes

Internet Connectivity

Licensed Establishments typically already have devices and readers that connect to internet via Ethernet or Wireless. For example: Point of Sale Systems, Menu and Kiosk Systems and Order Taking devices are typically already connected via Wireless or through Ethernet LAN.

ISO/IEC 18013-7 can be preferred with a fall back to ISO/IEC 18013-5 Interaction Mode if the Reader or the mDL Device doesn't have internet access.

Regardless of which Interaction Mode is selected, connectivity at least on a periodic basis, is an important consideration for keeping Issuer Public Keys up to date (see Security Measures to Be Implement below).

Wi-Fi may be available to customers and prospective customers for connecting mDL Device to Internet. Nearly all mDL implementations do implement QR code display, NFC and Bluetooth data connections – called Scan/Tap & Go interaction mode[16].

[16] Interaction Modes are defined in section 2 of https://www.mdlconnection.com/the-mobile-drivers-license-mdl-and-ecosystem/ published by Secure Technology Alliance

Even in portable setups, teller equipment typically has reliable connection, often through local or portable Wi-Fi network. This connectivity can be essential for ISO/IEC 18013-7 based identity verification and age checks at the time of home delivery, at concerts and in similar scenarios.

Under optimal network conditions, ISO/IEC 18013-7 can support fast transaction times.

4. Value Proposition

Allowing and encouraging customers to use an mDL as form of identification provides benefits for the individual **and** for the Liquor Stores, Convenient Stores, Concerts, Music Venues, Online Liquor Stores, and Alcohol Delivery Apps.

Convenience

Customers are increasingly accustomed to using their smartphones for digital transactions, including payments, ticketing, and access control. Using an mDL (mobile Driver's License) for age verification offers a seamless, contactless experience in liquor stores, online liquor purchases, and during alcohol delivery.

Tap or scan transactions have increased significantly since covid and have remained consistently high. The includes a rise in Tap to Pay, QR Code scanning for menus at restaurants and bars, and other similar contactless interactions.

Online liquor stores and delivery apps can integrate mDL verification at checkout, reducing manual review processes and ensuring compliance before an order is placed.

Delivery verification is enhanced by matching the recipient's portrait to the order, ensuring alcohol is delivered only to the rightful, age-verified individual.

For In-person interaction at licensed establishments, employees can focus on providing service while an automated verifier checks age from the mDL. Unlike manually inspecting physical IDs, which can be challenging when detecting Fake IDS, automated verification provides reliable, age verification. This reduces the burden of accountability for accepting fake IDs on both employees and the establishment. Additionally, it increases efficiency, speeds up service and ensures more accurate age verification.

Fraud Prevention

Liquor retailers and alcohol delivery services can **cryptographically verify** the mDL, ensuring that:

- The data is untampered.
- It was issued by a trusted authority.
- The credential has not expired**.**
- The credential is legitimate, mDL verification bypasses visual physical IDs, which typically relies on employee training and judgment. This significantly reduces human error and liability for relying parties.
- The portrait from the mDL can be used to match the person who is sharing the mDL.

mDL verification reduces risks associated with outdated, suspended or stolen IDs, as revoked physical documents can still be in circulation.

Using mDLs can deter underage purchases. Fraudulent attempts using fake or borrowed IDs become significantly harder.

Employee access to customer data can be restricted to prevent unauthorized viewing or misuse during ID verification.

Audit and Compliance

- Regulatory compliance for age-restricted purchases is strengthened by an **audit trail** of verification, ensuring transparency in transactions.
- Liquor stores and delivery apps must comply with state laws and alcohol sales regulations. The mDL provides a stronger verification method aligned with evolving digital identity standards.
- Time-stamped records of verification provide proof during due diligence.
- Online and mobile sales platforms can integrate mDL authentication to comply with age-verification mandates before checkout and during delivery, minimizing liability risks.

Cost Reduction

1. Reduced Labor Costs & Faster Checkouts

- Faster Verification: mDLs can be scanned quickly, reducing the need for employees to manually inspect IDs.
- Fewer Employee Interventions: At self-checkout, automatic age verification removes the need for staff to physically check an ID and manually enter the date of birth.

2. Lower Fraud-Related Losses

- More Accurate Authentication: mDLs incorporate cryptographic security, making them more difficult to counterfeit than physical IDs. This helps reduce the risk of underage alcohol sales due to fake IDs, thereby lowering the chance of fines or license suspension.

3. Compliance & Legal Cost Reduction

- Automatic Recordkeeping: Some mDL systems can log verification events securely, providing proof of compliance in case of audits or legal disputes.
- Avoiding Fines & Penalties: Enhanced security reduces the risk of underage sales violations, avoiding costly fines or lawsuits.

Revenue Expansion

The use of mDLs can enable stores to verify age for online liquor sales something that may not currently be feasible. This can create new revenue opportunities and service channels previous not available.

Customer Perception and Satisfaction

Adopting mDL as a form of digital identity positions it as a technology-forward store focused on innovation and improving customer experience.

mDL simplifies customer interactions by streamlining ID checks across in-store systems, online alcohol sales, and delivery apps.

It offers fast, secure age verification while protecting customer privacy by only sharing essential information with their consent.
Customers value the speed and convenience of digital ID checks, which reduce the hassle of manual ID handling in stores, apps, and deliveries—especially for online alcohol purchases.

This selective data sharing builds customer trust by demonstrating a commitment to privacy and responsible data handling.

5. Preparing for the Future

As mDLs become more widely adopted and remote presentation standards are finalized, liquor stores, convenience stores, and alcohol delivery platforms will be well-positioned to benefit from both cost savings and improved customer satisfaction. By leveraging the security features of mDLs, these businesses can offer more remote and self-service options such as self-checkout for liquor purchases and automated age verification for online orders while maintaining regulatory compliance with minimal manual effort.

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.	Transaction Surveillance: Consumers do not want their transactions tracked locally within shops, and across locations, or by their phone vendors or issuing authorities.

Issuing Authority Risk	Relying Party Risk	Consumer (Holder) Risk
	Mitigations 1. Include additional 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 service and fraud investigation purposes. 4. If additional verification is needed after the mDL has been processed, an establishment or delivery employee should perform a follow-up check or identity verification.	Mitigations 1. Only put the mDL on devices for own personal use. 2. Consumers should request to revocation of any mDLs that are not under their control from their issuers. 3. Choose the wallet application you trust. 4. Review information being requested and intent to retain by the relying party. 5. Follow your State Agency Guidelines and recommendations. 6. Don't share your mDL data with relying parties you don't trust

Table 1.3: Risk Level and Mitigations

Legal and Compliance Requirements

Retailers and service providers selling alcohol must comply with federal, state, and local laws to verify the age of customers before completing a transaction.

Regulations vary by state, and commonly require businesses to:

- Verify the age and match the ID to the person purchasing alcohol, ensuring they meet the legal drinking age.
- Maintain records of the verification process, particularly for online purchases and deliveries, to demonstrate compliance.
- State by state law might require maintain of records of identity and/or age.
- Prevent sales to underage individuals by ensuring age verification processes align with government regulations and industry best practices.

The mDL (mobile Driver’s License) provides strong cryptographic identity documentation that supports the age verification process, through *ISO/IEC 18013- protocols**.

To enhance security, businesses may implement additional safeguards to verify that the person presenting the mDL is its rightful owner. These may include:

- Biometric matching using the picture received from the mDL at self-checkouts or during delivery, ensuring the recipient matches the individual who placed the order.
- 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.

6. Data Required to Complete Use Case

To comply with age verification regulations, businesses may collect and verify specific data elements from the mobile Driver's License (mDL) while adhering to data minimization principles to protect user privacy.

Minimum Required Data Elements is one of the following:

- Age in Years or Age Over NN: Some transactions may only require confirmation that the individual is over a certain age (e.g., "Over 21") without revealing the exact date of birth.
- Portrait (Photo): Used in self-checkouts, kiosks, or deliveries to confirm that the person presenting the mDL matches the credential holder.

Additional Data (Depending on Store Policy, State Policy & Use Case):

- Date of Birth (DOB): To verify that the customer meets the legal drinking age.
- Issuer (State of Issuance): Identifies the issuing authority.
- Document Number (DL# or ID#): Provides an audit trail and evidence of verification.

- Name: Useful for registered customers, loyalty programs, or repeat purchases (e.g., convenient store memberships or alcohol delivery apps).

Business-Specific & Security-Driven Data Needs:

Some businesses may require **additional personal information** for security or operational reasons, such as verifying identity for **high-risk transactions**, fraud detection, or delivery authentication.

The ISO/IEC 18013-5 standard defines a **full set of data elements** that businesses can access when necessary. It is important to follow latest standard releases to stay up to date with the defined data elements, as well as current security and privacy considerations.

7. Data Minimization & Privacy Considerations

mDLs offer a key advantage in data minimization, enabling businesses to request only the data required for transaction, without exposing unnecessary personal details.

Businesses should minimize the data requested to meet the business needs. For example, readers can request age confirmation (e.g AgeOver21) instead of full date of birth, enabling a privacy preserving approach for age verification.

By utilizing mDL-based verification, liquor stores, online alcohol vendors, and delivery services can enhance compliance, security, and user privacy while maintaining a streamlined customer experience.

8.Consent for Purpose and Extended Use

mDL gives the opportunity to reduce data storage liability and ask only for what is necessary. When data is obtained from an mDL, the reader device should indicate "Intent to Retain" for any data that it intends to store.
Unless you have regulatory requirements to store the data, you should not retain the data ("intent to retain").
Data fields and the intent of the provider to hold data from the mDL must be clearly requested for user consent and the entity may publicly post appropriate privacy policies and terms and conditions as is required by laws. The entity may choose to publish security practices in place to protect consumer data.

9.Updated Data Handling and Privacy Policies

Businesses accepting mDL should review their posted Privacy Policies and data handling procedures. Whenever practical, those should be modified to indicate reduced data collection and the elimination of data storage from electronic transactions.

Once any order or transaction is complete the biometric or portrait data for that customer associated with the order should be deleted. Customers do not expect their portrait images or images of their physical ID documents to be retained and will not look at retention favorably.

10.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 as per the ISO Standards.

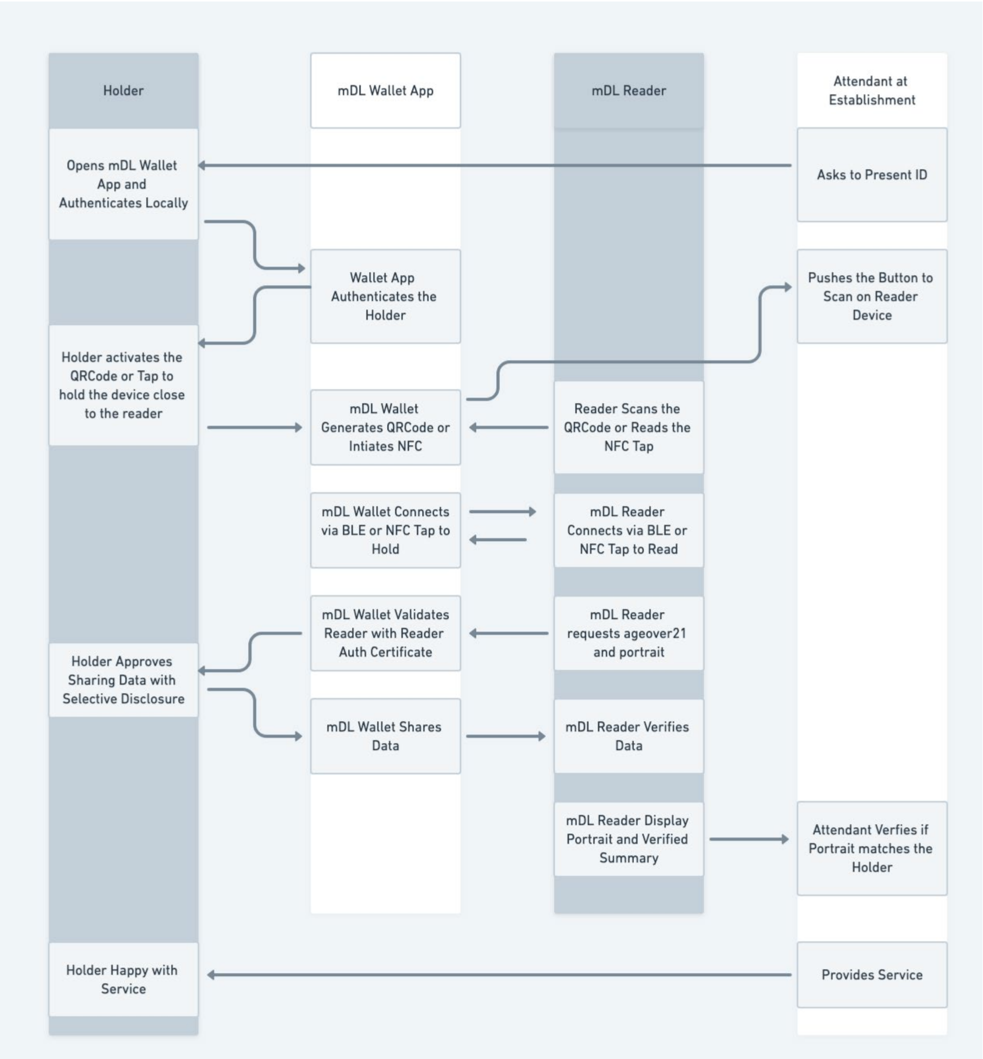
The reader or associated systems should display a summary of the verified data for inspection by a trained employee, including the portrait for verification of the applicant (As per the 2021 version of ISO Standard 18013-5).

It should not be necessary to display all data when an indicator (e.g green/red) is sufficient to convey age and validity of the ID. Data minimization at display time protects customer privacy and reduces the on-the-spot calculations of age that employees of the licensed establishment must make.

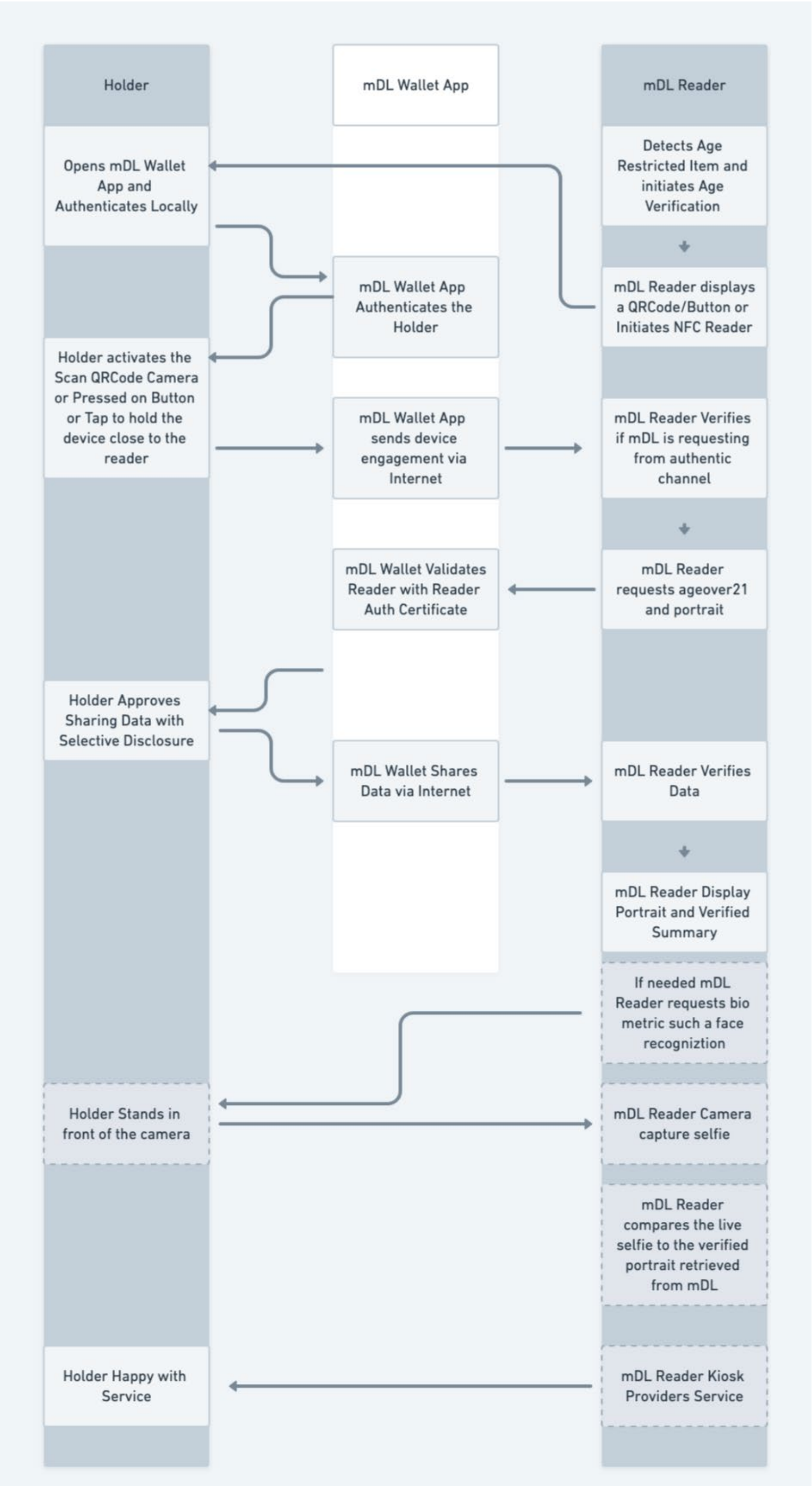
mDL can be integrated with existing Identity and Authentication systems, the verified mDL data may be forwarded securely to an existing online store services system to create a secure session anchored by the identity presented in the mDL. Identity Verification is performed by the operator for Attended use cases by matching the person to the portrait and biometrically match for unattended uses cases.

User Journey Examples

In Person Flow


Holder
mDL Wallet App
mDL Reader
Attendant at Establishment
Asks to Present ID
Opens mDL Wallet App and Authenticates Locally
Wallet App Authenticates the Holder
Pushes the Button to Scan on Reader Device
Holder activates the QRCode or Tap to hold the device close to the reader
mDL Wallet Generates QRCode or Intiates NFC
Reader Scans the QRCode or Reads the NFC Tap
mDL Wallet Connects via BLE or NFC Tap to Hold
mDL Reader Connects via BLE or NFC Tap to Read
mDL Wallet Validates Reader with Reader Auth Certificate
mDL Reader requests ageover21 and portrait
Holder Approves Sharing Data with Selective Disclosure
mDL Wallet Shares Data
mDL Reader Verifies Data
mDL Reader Display Portrait and Verified Summary
Attendant Verfies if Portrait matches the Holder
Holder Happy with Service
Provides Service

Unattended: Kiosk or Self-Checkout


Holder
mDL Wallet App
mDL Reader
Opens mDL Wallet App and Authenticates Locally
Detects Age Restricted Item and initiates Age Verification
mDL Wallet App Authenticates the Holder
mDL Reader displays a QRCode/Button or Initiates NFC Reader
Holder activates the Scan QRCode Camera or Pressed on Button or Tap to hold the device close to the reader
mDL Wallet App sends device engagement via Internet
mDL Reader Verifies if mDL is requesting from authentic channel
mDL Wallet Validates Reader with Reader Auth Certificate
mDL Reader requests ageover21 and portrait
Holder Approves Sharing Data with Selective Disclosure
mDL Wallet Shares Data via Internet
mDL Reader Verifies Data
mDL Reader Display Portrait and Verified Summary
If needed mDL Reader requests bio metric such a face recogniztion
Holder Stands in front of the camera
mDL Reader Camera capture selfie
mDL Reader compares the live selfie to the verified portrait retrieved from mDL
Holder Happy with Service
mDL Reader Kiosk Providers Service

11. Proposed Metrics of Success

Adoption and Volumes

What is the number of age verification transactions from mDL compared to other accepted identification and verification processes (e.g., physical ID)

Error Rates

For customers who choose the mDL for age verification, what percentage were able to successfully present the mDL to the reader and have their age verified appropriately by the system?

Fraud Rates

For age verification transactions secured by the mDL, how has the use of mDL impacted the amount of fraud compared to other accepted age verification methods (e.g., fake IDs, manual checks)

Processing Time

What is the average processing time for age verification using the mDL versus traditional ID checks? This includes all data scanning time, document authentication time, and any savings from eliminating manual form-filling or other delays.

Customer Satisfaction

How much time does it take to verify the customer's age using the mDL compared to other accepted identification and verification processes? If Net Promoter Score (NPS) is captured for the experience, does mDL improve customer satisfaction compared to traditional age verification methods.

New Operations Attained

Is the organization able to offer age verification services through new channels (e.g., self-checkout kiosks, online platforms) that were not previously possible with traditional identification and verification methods.

12. Challenges

Challenge	Mitigating Actions
Availability of ISO/IEC 18013-5 compliant	Not all US States and Territories have an mDL yet, but

mDL	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/ Market research estimates[17] that there will be 100 million mDLs in circulation during 2026 across more than half of the US States[18].
Adoption and Setup by Holders	Within states that deployed mDL, adoption rates are growing steadily. The acceptance of mDL by TSA at airports across the US, rollouts in retail (e.g. Liquor and grocery stores), and banking (regional Credit Unions), and other locations demonstrates to mDL holders that there are places to use the mDL that provide convenience and value.
Hardware for Reading mDL	There are implementations for in-person mDL that utilize custom hardware (e.g. TSA) to combine the full capability of the mDL presentation and verification, plus biometric verification of the individual, however 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. Apps are available to download on App Stores by searching “mDL Verification” or “mDL Reader”
Integrations with Existing POS and Establishment Systems	Convenience Stores, Grocery Stores and Licensed Establishments gain the most from mDL when integrated with existing POS or Menu systems, or inventory systems or any store Specific systems to facilitate account services and generate appropriate audit and system records as part of the verification process. mDL Jumpstart[19] will continue to partner and build relationships with software providers to promote the integration of mDL into traditional POS and platform systems. The results will be listed on mDL Connection.

[17] https://trinsic.id/mdl-ebook/

[18] https://trinsic.id/exploring-the-global-landscape-of-digital-id-adoption/

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

13.Security Measures to Be Implemented

Cryptographic Verification of Presented mDL based on ISO 18013-*

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 an ISO 18013-* compliant verifier application or equivalent process to ensure integrity and validity through cryptographic means. The Attendant 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.

By minimizing the data collected, you are limiting the exposure of data during breaches. The cost of a data breach and the subsequent repair of reputation likely does not outweigh the value of storing customer data unless required by law.

Customer loyalty program applications should be handled in a separate workflow when accepting the mDL. Unlike Age verification, customers applying for loyality programs may expect additional data to be collected beyond just AgeOver21 and Portrait. Separating this from purchase transaction is more transparent to the purchaser and ensures that purchasers can provide *informed consent*[20] , aligning with data privacy laws for storing and use of mDL data.

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. For a Relying Party to verify and trust any presented mDL, the Relying Party must have access to a trusted list of public keys called IACA (Issuing Authority Certificate Authority) known issuers. Relying parties may acquire public keys directly from the Issuer or through a trusted service such as their mDL Reader Service Providers and or through another mechanism.

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 Digital Trust Service

[20] **Informed consent** is a process in which an individual agrees to participate in an action, treatment, or research after being fully informed of all relevant facts, including the risks, benefits, and available alternatives.

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. Liquor Establishments or Software Providers for these institutions should register for access to VICAL and appropriate key material and metadata for verifying mDLs.

VISA Issuing Authority Authenticator (VIAA)

Another implementation of a trusted service provider for protecting the integrity of mDLs is the VISA Issuing Authority Authenticator (VIAA). VIAA enables Relying Parties access to verify credentials against all legitimate Issuing Authorities worldwide.

Designed as a single point of contact for global interoperability, VIAA ensures that only legitimate Issuing Authorities are onboarded into the secured system.

This service validates the authenticity of the mDL, without sharing PII, all through a single API call. VIAA is accessible via the Visa Developer Center. For further information, contact your Visa representative.

Commercial Readers with Public Keys

Most Reader publishers or manufacturers maintain a short list of known acceptable Issuer Public Keys that are synchronized with or embedded in their Reader software. Check the list of supported Issuers for your Reader. Because the work to maintain a current, accurate list is not small, expect the value of this service to be part of the cost of your Reader. It may be a better choice as the cost of maintaining mDL Public Keys being added (often) or revoked (rare) is high.

Other Digital Trust Services

There are other trusted services provided by Reader vendors, countries or regions. This list is not exhaustive and such we have minimized the providers. It is the responsibility of the merchant to ascertain that their mDL Reader supports the Issuing Jurisdictions.

Additional Security Considerations

Expiration for mDL

State and Local Laws on the acceptance of expired ID documents vary. Some States have explicit law and others leave it to Alcohol Control Boards or State Policy. Check that your Reader has a setting that allows you to remain conformant with policy or law by accepting mDLs with valid signature or rejecting even valid signatures because of the expiration date.

mDLs always contain the expiration date matching that on the printed physical license. mDLs also contain an additional "freshness" indicator for the cryptographic signature. There are data fields set by State Issuer policy that contain the date the cryptographic signature was applied and the expected data of the next refresh of that signature per policy. When conformant with AAMVA mDL Guidelines[21], State issued mDLs will typically have a monthly expected refresh.

This means a signature outside of State policy is a marginal indicator of risk but does NOT mean that the person's identity is not accurate because it was at the time of signing.

For Readers implementing Device Retrieval, the metadata about the digital signature on the mDL and the "freshness" 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 so that cardholders are aware of who they communicate with. This is particularly important for unattended situations where the cardholder needs assurance that they are tapping/scanning on your reader device, and not of a fraudster, even if the location of the device seems relatively secure. As of 2025, Reader Authentication Certificates are available through the vendor provider reader service, but they are not yet widely available through a trusted service provider comparable to Issuing Authority certificates.

14.Examples

Secure Technology Alliance – mDL Connection – Age Verification Use Case

There are examples showcased and listed on the Age Verification Use Case Pages[22] on https://www.mdlconnection.com/mdl-uses/age-verification/. This page will evolve over time with additional guidance, information, and illustrative examples.

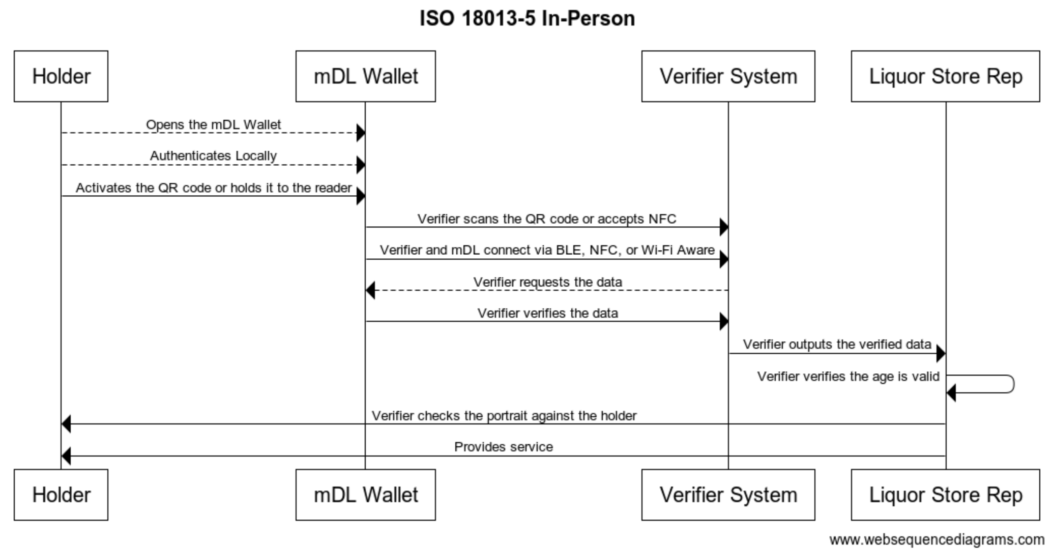
15.References

In March 2020, Secure Technology Alliance published the definitive resource[23] on mDLs and the new mDL Ecosystem. This document remains definitive today and introduces in-depth all aspects of the mDL, trust models, interaction modes, and challenges to build the ecosystem.

Secure Technology Alliance - MDL Connection
Secure Technology Alliance – mDL Connection – Age Verification Use Case
ISO/IEC 18013-5 Standard for Mobile Driving License
AAMVA mDL Digital Trust Service
Secure Technology Alliance – mDL Connection – Implementation Map

[21] https://www.aamva.org/topics/mobile-driver-license
[22] https://www.mdlconnection.com/mdl-uses/age-verification/
[23] https://www.mdlconnection.com/the-mobile-drivers-license-mdl-and-ecosystem/

16.Appendix


ISO 18013-5 In-Person
Holder
mDL Wallet
Verifier System
Liquor Store Rep
Opens the mDL Wallet
Authenticates Locally
Activates the QR code or holds it to the reader
Verifier scans the QR code or accepts NFC
Verifier and mDL connect via BLE, NFC, or Wi-Fi Aware
Verifier requests the data
Verifier verifies the data
Verifier outputs the verified data
Verifier verifies the age is valid
Verifier checks the portrait against the holder
Provides service
Holder
mDL Wallet
Verifier System
Liquor Store Rep
www.websequencediagrams.com

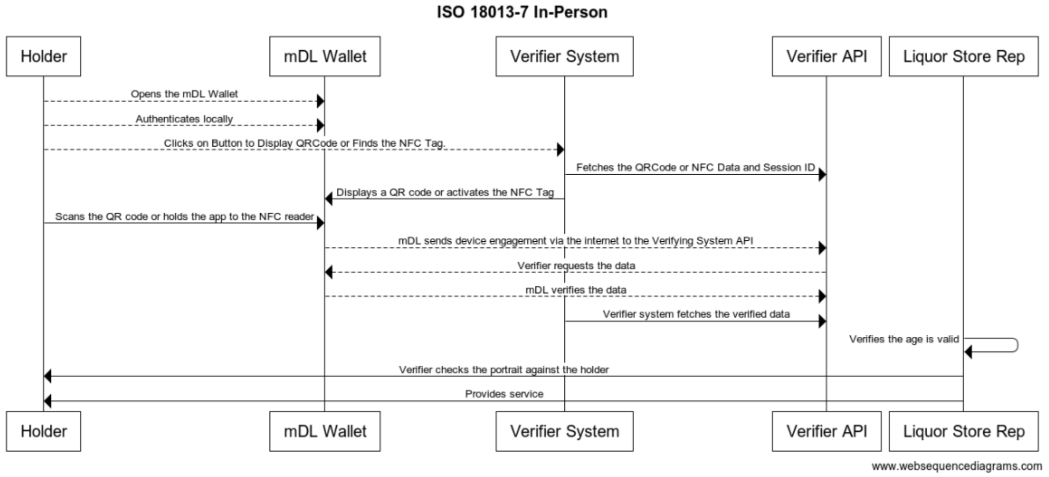
Example UML Journeys

These are example

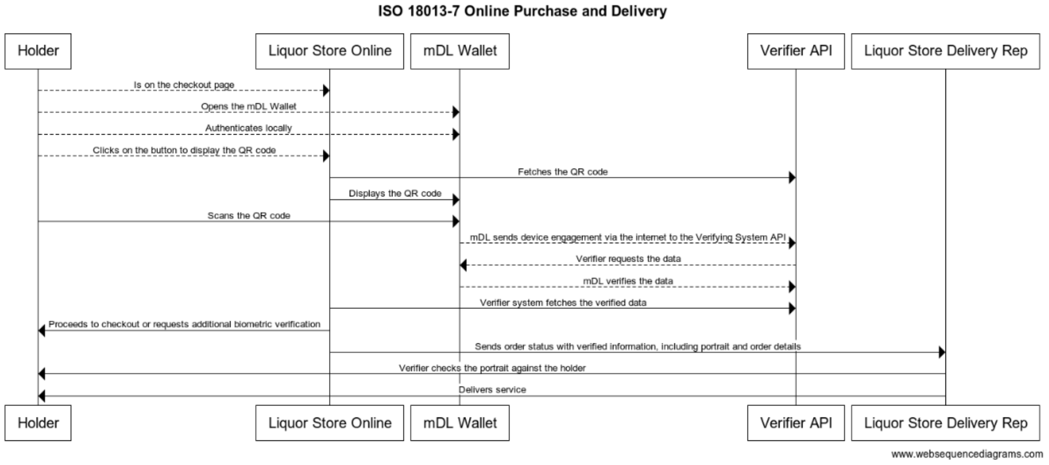
Example UML In Person Journey

As per 2024 ISO/IEC 18013-7 Version 1.

Example UML Remote Journey


ISO 18013-7 In-Person
Holder
mDL Wallet
Verifier System
Verifier API
Liquor Store Rep
Opens the mDL Wallet
Authenticates locally
Clicks on Button to Display QRCode or Finds the NFC Tag.
Fetches the QRCode or NFC Data and Session ID
Displays a QR code or activates the NFC Tag
Scans the QR code or holds the app to the NFC reader
mDL sends device engagement via the internet to the Verifying System API
Verifier requests the data
mDL verifies the data
Verifier system fetches the verified data
Verifies the age is valid
Verifier checks the portrait against the holder
Provides service
Holder
mDL Wallet
Verifier System
Verifier API
Liquor Store Rep
www.websequencediagrams.com

Example UML Online Order and In Person Delivery Journey


ISO 18013-7 Online Purchase and Delivery
Holder
Liquor Store Online
mDL Wallet
Verifier API
Liquor Store Delivery Rep
Is on the checkout page
Opens the mDL Wallet
Authenticates locally
Clicks on the button to display the QR code
Fetches the QR code
Displays the QR code
Scans the QR code
mDL sends device engagement via the internet to the Verifying System API
Verifier requests the data
mDL verifies the data
Verifier system fetches the verified data
Proceeds to checkout or requests additional biometric verification
Sends order status with verified information, including portrait and order details
Verifier checks the portrait against the holder
Delivers service
Holder
Liquor Store Online
mDL Wallet
Verifier API
Liquor Store Delivery Rep
www.websequencediagrams.com

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

UML Data for ISO/IEC 18013-5 In person:
Holder-->mDL Wallet: Opens the mDL Wallet
Holder --> mDL Wallet: Authenticates Locally
Holder -> mDL Wallet: Activates the QR code or holds it to the reader

mDL Wallet->Verifier System: Verifier scans the QR code or accepts NFC
mDL Wallet->Verifier System: Verifier and mDL connect via BLE, NFC, or Wi-Fi Aware
Verifier System-->mDL Wallet: Verifier requests the data
mDL Wallet->Verifier System: Verifier verifies the data
Verifier System->Liquor Store Rep: Verifier outputs the result
Liquor Store Rep->Liquor Store Rep: Verifier verifies the age is valid
Liquor Store Rep->Holder: Verifier checks the portrait against the holder
Liquor Store Rep->Holder: Provides service

UML Data for ISO/IEC 18013-7 In Person:

Holder --> mDL Wallet: Opens the mDL Wallet
Holder-->mDL Wallet: Authenticates locally
Holder-->Verifier System: Clicks on Button to Scan QR Code or Finds the NFC Reader.
Verifier System->Verifier API: Fetches the QR Code or NFC Data and Session ID

Verifier System->mDL Wallet: Displays a QR code or activates the NFC Tag
Holder->mDL Wallet: Scans the QR code or holds the app to the NFC reader
mDL Wallet-->Verifier API: mDL sends device engagement via the internet to the Verifying System API
Verifier API-->mDL Wallet: Verifier requests the data
mDL Wallet-->Verifier API: mDL Shares the data
Add a loop similar to ISO/IEC 18013-5.
Verifier System->Verifier API: Verifier system fetches the verified data
Liquor Store Rep->Liquor Store Rep: Verifies the age is valid
Liquor Store Rep->Holder: Verifier checks the portrait against the holder
Liquor Store Rep->Holder: Provides service

UML Data for ISO/IEC 18013-7 Online Order and Delivery:
Holder-->Liquor Store Online: Is on the checkout page
Holder-->mDL Wallet: Opens the mDL Wallet
Holder-->mDL Wallet: Authenticates locally
Holder-->Liquor Store Online: Clicks on the button to display the QR code
Liquor Store Online->Verifier API: Fetches the QR code
Liquor Store Online->mDL Wallet: Displays the QR code
Holder->mDL Wallet: Scans the QR code
mDL Wallet-->Verifier API: mDL sends device engagement via the internet to the Verifying System API
Verifier API-->mDL Wallet: Verifier requests the data
mDL Wallet-->Verifier API: mDL verifies the data
Liquor Store Online->Verifier API: Verifier system fetches the verified data
Liquor Store Online->Holder: Proceeds to checkout or requests additional biometric verification
Liquor Store Online->Liquor Store Delivery Rep: Sends order status with verified information, including portrait and order details
Liquor Store Delivery Rep->Holder: Verifier checks the portrait against the holder
Liquor Store Delivery Rep->Holder: Delivers service

17.Acknowledgements

Participants
Madhu Goundla – Oneproof.com – Lead Editor and Contributor; Chair of mDL for Alcohol Age Verification Working Group
Lori Daigle – AAMVA – Publisher of mDL Implementation Guidelines
David Kelts – Decipher Identity, LLC – Contributor and Chair of mDL Jumpstart Committee
Diego Koga – MATTR Global - Contributor
NLLEA – National Liquor Law Enforcement Agency
NABCA – National ALCOHOL Beverage Control Association

18.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.