SECURE TECHNOLOGY ALLIANCE

A SECURE TECHNOLOGY ALLIANCE IDENTITY COUNCIL WHITE PAPER

The Mobile Driver's License (mDL) and Ecosystem

Version 1.0

March 2020

Secure Technology Alliance
191 Clarksville Road
Princeton Junction, NJ 08550

www.securetechnologyalliance.org

About the Secure Technology Alliance

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software across a variety of markets including authentication, commerce and Internet of Things (IoT).

The Secure Technology Alliance, formerly known as the Smart Card Alliance, invests heavily in education on the appropriate uses of secure technologies to enable privacy and data protection. The Secure Technology Alliance delivers on its mission through training, research, publications, industry outreach and open forums for end users and industry stakeholders in payments, mobile, healthcare, identity and access, transportation, and the IoT in the U.S. and Latin America.

For additional information, please visit www.securetechalliance.org.

Table of Contents

1 Introduction

A mobile driver's license (mDL) that is secure, accurate, interoperable, and that protects privacy is coming, and such a mobile ID could well change the identity landscape in the near future.[1] A draft international standard is available — ISO/IEC 18013-5, "Personal Identification – ISO-Compliant Driving Licence – Part 5: Mobile Driving Licence Application" — and a number of states are piloting or implementing mDLs that comply with this standard.[2] AAMVA Guidance for mDLs[3] starts with this standard as a baseline capability.

An mDL can provide secure, convenient identity verification capable of eliminating billions of dollars in fraud. The person who holds the mDL controls what information is shared and with whom. The mDL is a new way of cryptographically verifying identity.

In addition, mDLs support more efficient and secure transactions. For in-person transactions, electronic authentication can give the mDL Verifier confidence in the presented ID without requiring specialized knowledge of the hundreds of card design and security features applicable to the driver's licenses (and their variants[4]) that are issued by 56 states and territories. The mDL can also eventually be used to increase security for online purchases and interactions.

This white paper focuses solely on the mDLs being implemented in the United States that comply with the draft ISO/IEC standard 18013-5. The white paper provides an overview of how ISO/IEC 18013-5-compliant mDLs will work, what to expect, and what challenges are in building an mDL ecosystem, addressing questions such as: What are the features, challenges, and uses of an mDL? Why should someone decide to get a mDL? How will the mDL meet expectations of trustworthiness?

mDL implementations that are not compliant with the draft ISO/IEC 18013-5 standard are not covered.

1.1 mDLs and Driver's Licenses

States are the primary issuing authorities for IDs in the United States. Through a process called *identity proofing*, a state's Department of Motor Vehicles (DMV) or an equivalent agency establishes identity for most residents by receiving, reviewing, verifying, and authenticating key documents related to citizenship, residency, and the accuracy of biographic data. A DMV issues a physical document, such as a driver's license (DL) or non-driver identification card (ID), directly to the individual. This document allows other entities to verify the individual's identity and biographical information (such as age or

---

[1] The term *mDL* as used here includes forms of identification that may not grant the holder the privilege of driving, such as an ID card issued by a state's Department of Motor Vehicles (or an equivalent state agency). The driving privilege is not germane to the establishment and use of identity.

[2] Draft International Standard ISO 18013-5, "Personal Identification — ISO-Compliant Driving Licence — Part 5: Mobile Driving Licence (mDL) application," https://isotc.iso.org/livelink/livelink?func=ll&objId=20919524&objAction=Open. The Annexes provide informative guidance for issuing authorities to design and implement their mDL solutions for privacy and security. Appendix A of this white paper lists additional standards and frameworks that are applicable to the design, development, implementation, and deployment of a mobile driver's license.

[3] AAMVA mDL Resources, "Guidance for Issuers," https://www.aamva.org/mDL-Resources/

[4] Variations include designs indicating driving versus non-driving status, age compliancy (under 21 or over 21), legacy designs, and REAL ID-compliant and non-compliant ID cards.

birthdate). DMVs take their role as identity proofers very seriously, resulting in near-universal acceptance of the DMV-issued ID as a valid ID.

The mDL is a secure digital representation of DL data that is provisioned onto a smart mobile device, such as a smart phone or tablet, for use by the proper, intended mDL Holder. It can also contain information relevant to additional state privileges or national context.

1.2 mDL Stakeholders and Use

Four entities are primary stakeholders in the mDL ecosystem:

- The *mDL Holder* is the individual who chooses to have and use an mDL. The mDL Holder is the legitimate owner of the identity enrolled with the DMV and associated with the physical DL card and the mDL.
- The *Issuing Authority (Issuer)* is the entity that enrolls and verifies the identity of the Holder and provisions the mDL.
- The *Relying Party (Verifier)* is the entity that requires an identity or verified biographical information to provide a product, service, or entitlement to a Holder.
- The *Identity Provider (Provider)* is a service provider that manages the use of mDLs online.

The mDL Holder accesses, or allows access to, the data contained in the mDL through a downloadable app (an application container or wallet) approved by the DMV. The app allows Holders to determine whether, to whom, and what mDL data they wish to share during a specific encounter. The entity that needs to confirm an individual's identity (the Verifier) receives information through an electronic reader that is capable of both confirming the authenticity of the mDL and receiving the data that has been authorized for sharing.

An mDL is not a photo or rendering of a physical card, which can be easily tampered with using current graphics tools. Instead, the mDL embeds all relevant data into individual data fields, allowing the data to be compartmentalized. This framework allows mDL holders to share only the fields that they wish to share or that are required by the Verifier. The data elements are digitally signed by the DMV Issuer, allowing the Verifier to have confidence in their authenticity. The electronic reader can validate the cryptographic signatures.

Figure 1 summarizes the mDL ecosystem participations and features.

Figure 1. mDL Ecosystem and Features

Definition	An mDL is a digital representation of the information contained in a physical DL or non-driver identification card, securely stored on a smart mobile device such as a smart phone or a tablet, owned and controlled by the mDL Holder. Since it involves the interaction of multiple interconnected parties (in this case, to exchange trusted personal data), use of an mDL creates an ecosystem.
Participants	• Issuer: The entity that enrolls and provisions the identity. • mDL Holder: The individual with the identity represented on the mDL. • Verifiers: Entities using an mDL reader to verify identity or other information provided by the mDL (e.g., law enforcement, airports, air carriers, the Transportation Security Administration [TSA], proof of age verifiers [liquor/tobacco/lottery retailers, restaurants, casinos], identity verifiers [banks, mobile operators, hotels], driving privilege verifiers [car rental, car sharing]). • Identity Provider: Entity (possibly the Issuer) orchestrating online ID requests on behalf of the mDL Holder.

	• Trust framework operator: Entity that coalesces the business, technical, and legal requirements of the participants in an mDL ecosystem.
Features	An mDL must include the following key features: • Secure and accurate provisioning • Management of mDL IDs • Device platform security • Privacy protection for mDL Holders, individually and collectively • Standardized mechanism for Verifiers to establish trust in mDL attributes given multiple Issuers • Secure verification of the ID • Provisions to ensure that only the mDL Holder can operate the mDL and share data • Cross-jurisdictional operational capability • Standardized data exchange mechanisms • Adherence to regional or national regulations, such as trust frameworks legislation, and privacy protection frameworks • Worldwide interoperability.

1.3 mDL Process

At least for the foreseeable future, the mDL is a companion to a DL, not a replacement for the physical card. Individuals will have to apply for a DL to a state DMV and provide evidence of their identity before they can hold an mDL. Once the DMV verifies the applicant's identity and establishes a record in its system, the individual may choose to obtain an mDL through a DMV-determined process.[5]

The DMV (or its agents) will provision the verified identity to the Holder's mobile device or to an Identity Provider. Provisioning is a form of registration establishing the Holder's ownership of the identity, the mobile device, the account at the Identity Provider (if applicable), and the data, and a digital identity token is stored on the device. For example, ownership could be established by verification against payment records, a PIN or other shared secret, facial recognition matched against a trusted data source, or in-person registration of the device. The mDL data stored on the device or by the Identity Provider must be protected against unauthorized access; Holder data security is of paramount importance once accurately provisioned. Strong Holder authentication is required for protection and use.

The Holder maintains full control of the mDL and decides how much information to provide at what time and to whom. A Verifier (such as a merchant) initiates the sharing process by using a reader device to request the needed information. When the individual's smart device receives the request, the individual decides what (if any) information to send to the requester's device. The identity information and any data needed to verify its authenticity are sent to the Verifier's device. Based on the use stated when the information is requested, the Verifier decides what to do with the information and whether to grant the mDL Holder the requested privilege or service.

For example, suppose a 25-year-old mDL Holder wishes to use the mDL to purchase alcohol. The Verifier (merchant) sends a request for proof of age to the Holder's smart phone. The Holder allows the device to share a DMV-signed statement certifying age, based on the Holder's birth date, without the

[5] The exact process may vary by state. In-person activation, self-guided biometric registration, notarized provisioning, and remote video proofing are all possible processes, each establishing a level of identity assurance.

Holder's name or other biographical information. The Verifier's device receives the statement and verifies the signature on the data. Confident that the customer meets the age requirement, the merchant can sell the alcohol.

1.4 mDL Value to Stakeholders

The mDL can deliver significant value to all stakeholders in the mDL ecosystem.

Issuers can realize the following value:

- Providing easy to use and convenient electronic ID documents to their citizens, mDL Holders, that increase document reliability and can be used worldwide via the ISO/IEC 18013-5 standard.
- Remote management capabilities, allowing mDLs to be updated remotely, reducing cost and improving efficiency.
- The ability to assist Holders who lose a DL card or are unable to come to the DMV.
- Reduction in the use of expired and invalid DLs.
- Reduction in the use of counterfeit documents when the Issuer digital signature is verified.

Holders can realize the following value:

- Convenient availability of identity or other attributes without requiring access to a physical ID, that can be used for a variety of transactions, such as in-person transactions, online transactions (e.g., car rental, tax filing, DMV services) or for person-to-person sharing.
- Controlled access to their identity information and protection against unauthorized use, supported by capabilities of the smart device platform (e.g., PIN, biometrics).
- Selective information sharing. Only the attributes required for a transaction are shared, rather than all DL attributes. (For example, a bar employee verifying age only needs to know the mDL Holder's verified age is above a legally set limit. Sharing address and name is not required. By not exchanging unnecessary data, the mDL increases privacy and physical security for the mDL Holder.)

Verifiers can realize the following value:

- Ease and reliability of verification of an individual's identity, using digital authentication based on a global standard rather than relying on a Verifier's or card reading device's knowledge of and ability to recognize physical security features.
- Reduced exposure to liability. A Verifier can decide to receive only the attributes required for a particular transaction, thus reducing the risk of violating a Holder's privacy.
- Quality control. Transmitting mDL data digitally eliminates human errors during manual intake of attribute data.
- Potentially reduced use of expired and invalid driver's licenses due to cryptographically authenticated mDL.
- Potentially reduced identity fraud, including counterfeit DLs.

> ***In the future…***
> For both the Holder and Verifier, there is the potential to layer or link other attributes in other applications to leverage mDL identity information (for example, to verify employee identity and allow facility access).

1.5 About this White Paper

This white paper introduces the potential of an ISO/IEC 18013-5 compliant mDL to fundamentally change the identity landscape. Such an mDL can protect the Holder's privacy, control what information is shared, enable more secure in-person and online transactions, increase identity certainty for Verifiers, and repersonalize more efficient service delivery. For this potential to be realized requires, as a first step, producing and issuing an ISO/IEC 18013-5 compliant mDL. To become trusted and accepted, mDLs must also be evaluated by public and private sector policy makers, business process owners, regulators, relying parties, and identity providers.

In addition, broad acceptance requires awareness, education, and coordination. The capabilities of the mDL must be matched to each use case wisely. mDL Verifiers must understand policy and regulatory issues, potential changes in point-of-service hardware or software, verification and authentication infrastructures, business processes, risk and compliance, staffing impacts, and total costs.

The Secure Technology Alliance gathered representatives to serve as a forum to facilitate awareness, education, and coordination of U.S. stakeholders implementing and accepting mDLs. Participants in these efforts and in the development of this white paper included the following:

- Driver's license issuers and driver's license technology providers
- Mobile technology providers, security providers, and network providers
- Testing and accreditation organizations, including trust framework providers
- Relying parties, including representatives of the retail, financial and banking, health, and transportation sectors
- Key industry associations and federal and state government agencies

This white paper was developed to introduce readers to the inherent capabilities of ISO/IEC 18013-5 compliant mDLs, illustrate the ways that Verifiers can accept mDLs, and draw attention to considerations, challenges, and potential issues that require resolution. The white paper presents diverse perspectives through the following content:

- Use types and scenarios
- Architecture of usage
- Privacy
- Building trust
- Implementation considerations and challenges
- Use cases

The Secure Technology Alliance will build upon this white paper with a template for defining mDL use cases. The template can help Verifiers revolutionize the delivery of services that require ID documents. The template will be accompanied by an exemplar and use cases that illustrate the potential of mDL.

2 Use Types and Scenarios

Driver's licenses are used every day to support a diverse number of business processes. Although the DL primarily proves the privilege to drive vehicles, it is also presented to confirm legal age, name, or contact information.

Consumers are increasingly using their mobile devices for a variety of applications, including securely storing and using their payment cards. Migrating the DL to the mobile device would deliver value to consumers providing that security and privacy isn't compromised. In addition, the businesses that rely on these documents do not want the use of digital representations to compromise transaction accuracy. The rendering of a physical document or the image of a DL on a phone or in a wallet app cannot be trustworthy, because it is easy to create lookalikes using graphics editing tools or to write programs that overlay data on the screen. In contrast, an mDL can present the data, along with cryptographic proof that an Issuer validated the data.

The desire for digitization without compromise presents a challenge. In the case of tickets to an event, boarding passes, and loyalty cards that have transitioned into digital form on mobile devices, the accepting systems use QR codes containing identifiers that serve as pointers to trusted back-end systems. No common system holds all identity information for an individual. And since individual phones are not fully trusted, the industry needs a common, trusted approach. The ISO/IEC 18013–5 draft international mDL standard seeks to provide mechanisms for obtaining and trusting identity document data from a mobile driver's license.

ISO/IEC 18013–5 provides standardized methods of interacting with an mDL for identity and driving privilege use cases. The standard specifies two methods, both controlled by the mDL Holder, for a Verifier to obtain and trust the data: either directly from the mDL Holder's device, or through a pointer to a trusted back-end system (as for a boarding pass).[6] Once the data is obtained, the Verifier also needs to know that it is accurate. If the Issuer (i.e., the DMV) signs and securely places the DL data onto the phone according to ISO/IEC 18013–5, a trustworthy mDL is possible. The Issuer electronically signs the data at the time of issuance and ensures that it is provisioned to a device belonging to the legitimate DL Holder. Everything from the name to the portrait image to the driving privileges is signed and can be verified by an mDL reader.

Participants in the development of ISO/IEC 18013–5 are supporting a two-phase approach to initial mDL operating capability. The phases are called *Day 1* and *Day 2*. Day 1 standardizes in-person, attended interactions. Day 2 standardizes unattended, distance, and online interactions. Standards for provisioning an mDL are being developed separately, giving regional authorities time to develop inclusionary policies and technologies that will ensure access and fairness for all their citizens.

Table 1 summarizes Day 1 and Day 2 initial operating capabilities.

[6] The multiple communications technologies available in mobile devices offer multiple ways to accept identity information to fulfill use case requirements. For a discussion of mDL requirements, many of the use cases, and considerations germane to the use of mDLs as an alternative to physical cards, see the American Association of Motor Vehicle Administrators, "Mobile Driver's License Functional Needs White Paper," 0.9 Document Version, https://www.aamva.org/mDL-Resources/.

Table 1: ISO/IEC 18013-5 Day One and Day Two Capabilities

	Day One Capabilities In-Person Attended Transactions	Day Two Capabilities Unattended and Online Transactions
Connecting	QR code and Near Field Communication (NFC) tap ensures nearby usage as proximal consent.	Adds Bluetooth beacons and low cost (non-smartphone) NFC tags and devices.
Transferring	NFC, Bluetooth, and WiFi Aware for data transfer at short to mid-range. Online lookup for speed when connected to the internet.	Adds web services and hooks for request and response, therefore distance transfer. Protects Holder from rogue readers when not line of sight.
Verifying identity	Human attendant manually compares appearance of the Holder to received photo, limiting distance.	In-person and distance Holder authentication for automated identity without a portrait.[7]

mDLs offer Holders and Verifiers more flexibility than traditional DLs in multiple ways:

- mDLs can be used remotely or in person.
- mDLs can be stored securely on a smart device or in the cloud.
- mDL data can be transmitted online, at a far distance, in proximity, or by tap.
- mDLs can be authenticated through the internet or an offline device.
- Verification can be in-person (attended) or automated (unattended).
- mDLs can be connected to the internet (online) or disconnected from the internet (offline).

Any iteration or architecture must incorporate certain core features:

- The data on the mDL must be provided by the Issuer and reflect the information that the Issuer collects and validates (verifies) when proofing the Holder's identity.
- The data must be secure. Every element of the system must include safeguards to protect the data from unauthorized access.
- Holder privacy is paramount. The Holder must decide whether to have an mDL and be able to maintain full control over whether and what data to share. Informed consent is valuable to both parties. The Verifier can choose not to proceed with the transaction if the necessary data is not provided.
- A trust framework is needed to protect all parties and ensure common policy and mechanisms.
- Verifiers must be able to validate that the mDL data is authentic, accurate, and has not been altered by unauthorized parties.

[7] The mechanisms used to establish bidirectional trust are different for in-person interactions. In the absence of line of sight, the mDL Holder struggles to ensure that the reader device is trusted before sharing, and the Verifier must use technology to establish that the Holder is the intended mDL Holder. Holder authentication technologies are emerging, gaining strength, and becoming easier to use, so it is sensible to wait for their maturity to adopt strong, prevalent, standardized mechanisms.

Standardizing the digitization of identity can bring greater accuracy and consistency to identity transactions, in addition to providing better privacy for citizens. Having a smart platform for digital IDs enables an mDL to support a larger set of use cases than a traditional card and opens the way to re-envisioned workflows for traditional interactions that increase trust, efficiency, and personalization. Hosting the mDL on a trustworthy, smart platform enables online, unattended, or distance identity transactions that may not be possible with physical documents.

2.1 Provisioning

How the mDL gets to the correct device of the intended mDL Holder is critical to establishing and maintaining trust at the time of a transaction. mDL records, like DLs, are created at an established identity assurance level, and the level of trust a Verifier places in the communication of this data should adequately address the level of risk associated with the conveyance of the data from the Holder to the Verifier. Physical documents are most often created by the Issuer at a secure facility and mailed to a validated address in plain packaging (to minimize theft or incorrect delivery). The Issuer must choose provisioning methods that protect the mDL's security and assure identity.

Standards that govern mDL provisioning are not part of ISO/IEC 18013-5. Issuers must select mDL apps and issuing infrastructures that meet regional or national requirements and provide accurate provisioning. Another ISO working group is developing a standard (ISO 23220-3) that will govern registration. Groups like the FIDO Alliance have developed measurement technologies that are applicable both to provisioning and authenticating users during transactions. Regional and national guidelines such as NIST SP 800-63-3 *Digital Identity Guidelines*, Digital ID and Authentication Council of Canada (DIACC) Draft *Pan-Canadian Trust Framework (PCTF)*, the *Australian Trusted Digital Identity Framework (TDIF),* and Kantara *Identity Assurance Framework* provide minimum requirements for establishing identity assurance levels.

In the absence of standards or local legislation, it is expected that Issuers will choose a provisioning technology that provides the required level of trust and meets their standards for identification. Additionally, it is critical for Verifiers only to accept mDLs from Issuers and mDL apps that they trust to operate within their own boundaries of risk acceptability. To facilitate trust, Issuers and mDL app providers can make development and acquisition decisions based on industry best practices and measurement technologies, reducing risk below the tolerance levels for their physical IDs. Also, Issuers and mDL app providers can engender public trust by performing independent, third-party audits of their systems and technology and openly publishing the findings.

2.2 Use at Transaction Time

mDL transactions involve the exchange of consent, identity, and authentication data between the Holder's device and the Verifier's device or system.

The Holder can share mDL data through a number of mechanisms. The sharing mechanisms can be categorized generally as offline/transmit or online/token and request.

- **Offline/transmit**. Offline/transmit sharing takes place when the mDL is resident on a secure smart device and the Verifier's reader is not necessarily connected to the internet. The Verifier requests the mDL Holder to transmit identity attributes over communication channels supported by both devices. Data is transmitted from the Holder's device over a secure encrypted channel to the Verifier's reader, along with a cryptographic signature from the Issuer proving that the data have not been altered. The reader can check that the mDL data was transmitted by the device to which it was originally issued.

- **Online/token and request**. In online/token and request sharing, the mDL sends a token to a connected (online) reader that authorizes the reader to request (and receive) specific, signed, Holder-consented identity data from an online source (i.e., the Identity Provider for the Issuer). The token contains no personal data about the mDL Holder. The retrieval mechanisms can be RESTful Web API or OpenID Connect (OIDC), each of which has advantages when deployed as part of a comprehensive identity system for Issuers.

Appendix C: Use Cases provides high-level overviews of a variety of potential mDL uses.

2.2.1 Offline/Transmit (Offline Transmission)

2.2.1.1 Current State

Transmission uses one of two current mechanisms: a tap, a quick exchange of connection parameters over Near Field Communication (NFC); or a scan, an optical exchange of connection parameters implemented by the reader device decoding a QR code presented by the mDL. In either case, the Holder initiates the connection, which constitutes consent to connect the reader and the mDL. This step is called *device engagement* in the ISO/IEC 18013-5 standard.

After the two devices are engaged, the mDL uses passive authentication (i.e., signed by the Issuer) to ensure that the identity data is the data provisioned by the Issuer and has not been altered. Passive authentication depends on Verifiers having access to trust lists of certificates that can be used to validate Issuer signatures. The ISO-standardized mechanism for passive authentication is very much the same as the process used for the ePassport and reflects established cryptographic techniques.

In addition, active authentication can ensure that the mDL data is not cloned from the original device.

Figure 2 illustrates device-to-device transmission.

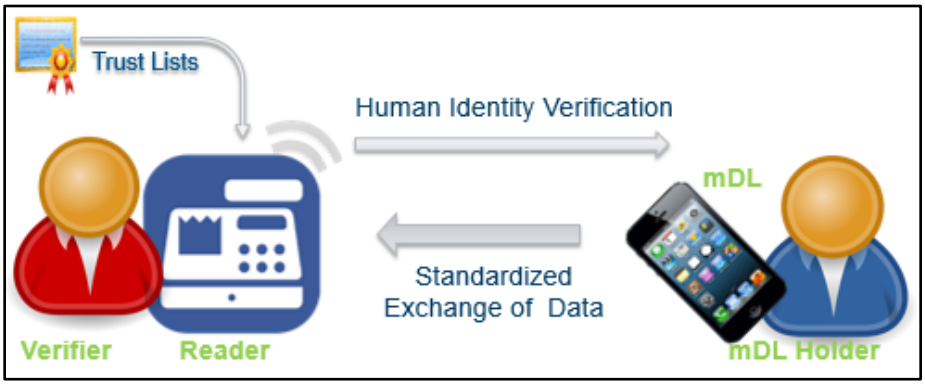

Figure 2: Device-to-Device Transmission per ISO/IEC 18013-5 for Offline Attended Verification

Offline transmission is useful when internet connectivity is not guaranteed or when it is desirable to restrict data transmission to local channels. For the data to be considered trustworthy, it is critical that the Verifier have offline access to certificates that verify data from any Issuer of mDLs that the Verifier expects to encounter while disconnected. Verifiers can connect periodically to update subscriptions to trust lists of certificates, rather than maintain a real-time connection.

2.2.1.2 Attended vs. Unattended Verification

Offline transmission can be attended or unattended. In both cases, data is transmitted between the Holder's and Verifier's devices, but the type of data is different.

In an offline attended scenario, a human verifies the connection between the Holder and the mDL data, usually by visually comparing the Holder to a facial image in the mDL record. Typically, the Holder's device transmits the mDL portrait to the Verifier's device so that the attendant can authenticate the portrait and display it on the Verifier's screen. Attended verification adds to transmission time, as portrait images range in size from about 15 kb to 1 MB, with the typical size being 60 kb.

Unattended offline verification relies on automated biometric capture and comparison technology. The biometric factor may be a facial image, a fingerprint, or any other biometric factor that the issuer provisions onto the mDL. The Verifier can capture this biometric from the mDL Holder at the time of verification and compare the freshly captured data to the biometric data on the mDL.

2.2.2 Online (Token and Request)

When Verifiers and mDLs are connected to the internet during a transaction, they can negotiate a lookup of identity data that takes advantage of internet connectivity. This is a two-step process: first, the mDL shares a one-time use token with the Verifier, and next, the Verifier uses the token to request mDL data from an Identity Provider (either an internal component or an external vendor, selected by the Issuer, who stores mDL identity data securely on the cloud). This process is known as token and request (Figure 3).

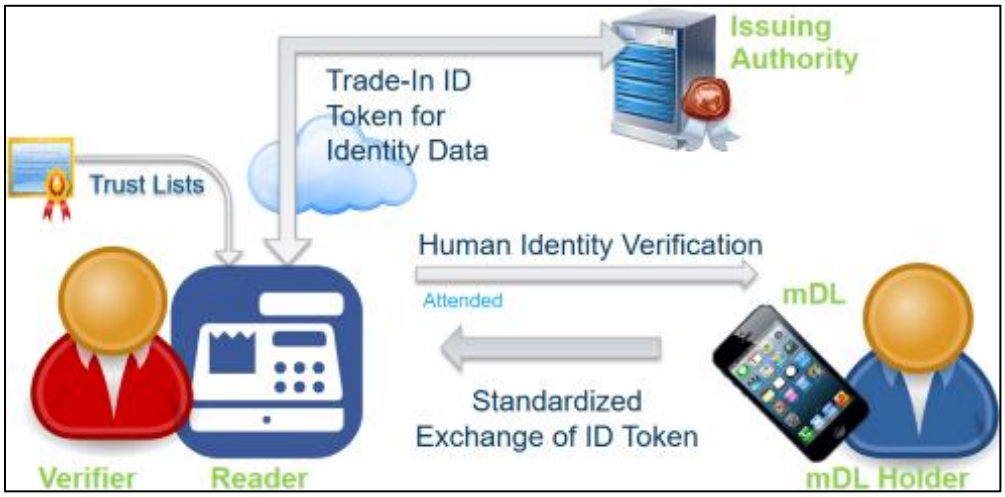

Figure 3: Token and Request Mechanism for Online Attended Verification

The Holder uses the mDL to share a token with the Verifier over some communication channel (optical scanning, nearby communication, a distance connection, or even the internet). Tokens can be privacy-preserving, single-use tokens.

The Verifier can then make a request of the mDL Holder by connecting to the Identity Provider associated with the mDL. Requests both confirm that the possessor of the mDL is the actual mDL Holder and gather data authorized by the Holder to be shared with the Verifier.

Security certificates, Transport Layer Security (TLS) encryption, and the OIDC infrastructure for preregistering

In the future…

With an Identity Provider using (for example) Open ID Connect, possibilities for online usage expand to include:

- Unattended, with the Identity Provider and mDL doing Holder authentication
- Delayed/deferred lookup using refresh tokens
- Distance use cases with negotiated Holder consent

Verifiers (called clients) help protect Verifier connections to the Identity Provider. OIDC Dynamic Client Registration can also be used for lower security infrequent connections. Data returned by the Identity Provider is signed for integrity (passive authentication); device management and optional Holder authentication perform anti-cloning (active authentication from the offline transmit model) and impersonation resistance.

An online mDL transaction sends only a small token from the mDL device to the Verifier on the slow channel (QR, NFC); the larger amount of data is retrieved directly from the Issuer on the faster channel (Internet connection).

2.2.3 Future Possibilities for Connecting mDLs

While the current version of ISO/IEC 18013-5 specifies only two methods for device engagement, several more are in the works for Day Two. Some can be implemented now, and technology providers may roll these out before the Day Two standard is published. Transmit mechanisms may remain unchanged or add improved cryptographic proofs that further minimize data sharing.

Future methods include the following:

- Reader-first QR presentation
- Bluetooth distance device engagement
- OIDC for login
- OIDC refresh tokens

In the reader-first method, the reader device produces device engagement information for a service that it is advertising. The mDL reads the device engagement parameters and connects, and the currently standardized data request and response mechanism takes over. This method has the advantage of using static mDL reader service parameters that can be encoded on cards, printed material, or static NFC tags, such as stickers or NFC logo tap pads on electronic devices.

In the Bluetooth method, the reader device advertises a common Bluetooth service with sufficient identifying information about the Verifier for the mDL Holder to safely decide to connect to the reader. Data request and response then take place as currently specified. This model supports interaction modes such as check-in (see Table 2 below).

To use OIDC for login, an mDL can be associated with a username (email address or Holder-chosen name) that is used to log into one or more web sites. Holder authentication is then performed using mDL data on the mDL device. Using a DL to log into a state agency's web site to obtain services can expand service delivery and reduce complexity for state agencies and centralized IT services.

OIDC Refresh Tokens[8] require that the web site of an mDL Verifier store a token that identifies the mDL and mDL Holder. The token need not contain identifying information; it is usable only by the OIDC Identity Provider. The token is used for scheduled or event-driven operations. Verifiers obtain fresh mDL data with Holder consent whenever an operation (such as sending mail) is to be performed without ever storing the Holder's data and exposing themselves to the risk of a data breach.

[8] https://auth0.com/docs/tokens/refresh-token/current and https://openid.net/specs/openid-connect-core-1_0.html#RefreshTokens

2.2.4 Privacy Considerations

The token and request mechanism can support privacy by design[9] principles, because the Holder manages their data and provides informed consent to decide what data to share. Using the token and request mechanism, privacy protection techniques such as data minimization and non-traceable identifiers are easier to implement and enforce than when using the transmit mechanism. Token and request requires, however, that Issuers incorporate strong policy and technical controls into their relationships with their Identity Providers to ensure that transaction metadata cannot be used to trace the mDL Holder's location or activities. Individual participation within citizen-managed identity solutions empowers the Holder and builds mDL Holders' trust and confidence to ensure widespread use of mDL.

Privacy protection can be implemented through data minimization using OIDC scopes that are profiles or attribute sets. The Issuer can create dynamic signatures for very fine-grained (e.g., date of birth) or highly aggregated (e.g., driving privileges) attributes in a controlled environment.

When using the OIDC interfaces, Verifiers can consider storing refresh tokens from the OIDC provider to use for future data retrieval. Storing refresh tokens establishes the possibility of deferred device engagement, in which the request phase is delayed until the data is needed (or needed again). It is considerably safer to store a refresh token and request consent data from an mDL Holder when the data is needed (e.g., when a renewal notice is about to be sent) than it is to store the data itself. Refresh tokens have no value other than to the OIDC client (the Verifier) and include no identifying information.

> ***In the future…***
> Since many governments have expressed a strong desire for a secure digital online ID, use of the mDL could evolve to protect the privacy of online accounts.

2.3 Interaction Modes

Verifiers want to design business flows that provide their customers with appropriate and personalized service. Delivering efficient service attracts and retains customers. But different Verifiers may have different equipment, workflow patterns, physical environments, security policy, and customer needs. The multiple combinations of environmental variables, connectedness, personnel, and connection and transmission mechanisms make possible a variety of interaction modes (Table 2). Selecting the correct interaction mode is critical to designing a use case for accepting mDL that can delight customers. The ISO 18013-5 standard supports various interaction modes. Figure 4 illustrates the possibilities.

Interactions can take place at close-range or from a distance and may in fact require multiple steps in order to complete the transaction.

An interaction may be attended, with an agent to verify the identity of the mDL holder to the mDL, or unattended where machines or mobile devices aid in Holder authentication or identity verification.

As is the nature of today's mobile devices, connections to the Internet (and thus to the Issuers' servers or Identity Provider) may be available to the mDL or reader or either may be disconnected at the time.

[9] Privacy by design is a software engineering goal introduced by Dr. Ann Cavoukian while Privacy Commissioner of Ontario, Canada. It comprises seven principles to be achieved in order to ensure good computer system design.

Consider reserving and driving a rental car, where the mDL Holder may engage with the car rental agency in advance, and then at multiple touchpoints within the process of confirming, selecting, and driving the car off the lot. Many of these steps require the renter to identify themselves and to ensure they have the privileges to drive. Each may be optimized for a specific distance, connection capability, and attended or unattended operation.

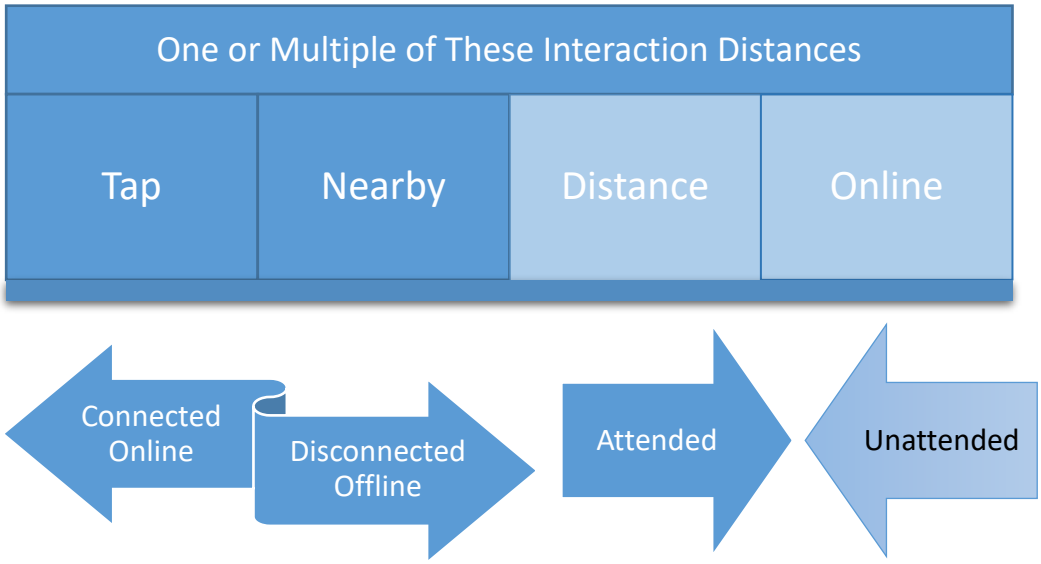

Figure 4. Possibilities/Variables that Verifiers Consider that Create Interaction Modes (Lighter blue are Day Two interactions)

Table 2. Potential Interaction Modes for Verifiers

Mode	Device Engagement	Data Transfer	Holder Authentication (if unattended)	Description and Example Use Case
Modes Supported by Day One				
Tap & Go	NFC	BLE or WiFi Aware	NA	NFC tap establishes BLE or WiFi Aware for data transfer. The Holder can move the mDL while transferring data to the reader. Example use case: Seating at a bar
Tap & Request	NFC	Online	NA	NFC contains REST or OIDC token that returns data with a portrait for an attendant. Example use case: Liquor store point of sale
Tap & Hold	NFC	NFC	NA	Full engagement and data transfer over NFC. Example use case: Offline liquor store
Tap & Look	NFC	Online	Biometric camera	NFC contains REST or OIDC token that returns data for biometric matching. Example use case: Beer vending machine or eGate at an airport

Mode	Device Engagement	Data Transfer	Holder Authentication (if unattended)	Description and Example Use Case
Tap & Consent	NFC	OIDC	OIDC AuthN	NFC contains an OIDC token that, when traded to the Identity Provider, triggers Holder authentication by mDL and data release.
Scan & Go	QR	BLE or WiFi Aware	NA	Holder holds an mDL QR code up to the reader camera and can move the mDL while data is transferred using nearby method.
Scan & Request	QR	Online	NA	Holder holds an mDL QR code up to the reader camera. Data appears on the reader after online retrieval.
Scan & Look	QR	Online	Biometric camera	Holder holds an mDL up to the reader camera to transmit a token. Reader obtains data online, including a portrait, then takes a picture of the mDL Holder. Example use case: ATM for bank account opening
Scan & Consent	QR	OIDC	OIDC AuthN	The QR code contains an OIDC token that triggers both Holder authentication and data release when traded into the Identity Provider.
Delayed Request	Stored refresh token	Delayed OIDC	OIDC AuthN	The Holder receives a request for consent and fresh data from a known Verifier. Example use case: IRS requests approval of tax refund
Extended Modes				
Interrupting Request	Reader BLE Advertised	BLE or Online	NA	A Bluetooth beacon advertises a reader service that requests mDL data from the Holder. The mDL Holder can validate the authenticity of the request and then consent to share identity data.
Check-In	Reader BLE Client	BLE or Online	NA	The mDL Holder uses the mDL to actively share data and discovers a service for the Verifier to receive identity data.
Login	Open ID	OIDC	NA	The mDL Holder identifies to an online service provider who triggers Holder authentication through the Identity Provider and the proper mDL. Once authenticated, the Holder is granted access to the service. This is Open ID login, in use today.

Mode	Device Engagement	Data Transfer	Holder Authentication (if unattended)	Description and Example Use Case
Link DL to Account	Open ID	OIDC	NA	Similar to Login, but the service provider retains a refresh token to be used later instead of storing mDL data and risking a data breach.

3 Usage Architecture

The interactions between the different participants in the mDL ecosystem support one of three general functions (Figure 5):

1. Arrow 1 identifies the interaction required for mDL provisioning, data-signing, issuing, and management, typically performed by the Issuer (the Issuing Authority).
2. Arrow 2 indicates the interaction between an mDL and a reader to establish the device connection, share attributes, and perform authentication (Section 2.2.1).
3. Arrow 3 identifies the interaction required for trust model adherence used by the readers, which requires certificates published by multiple Issuers. It also shows the implementation of the online model, a real-time interface to web services (Section 2.2.2).

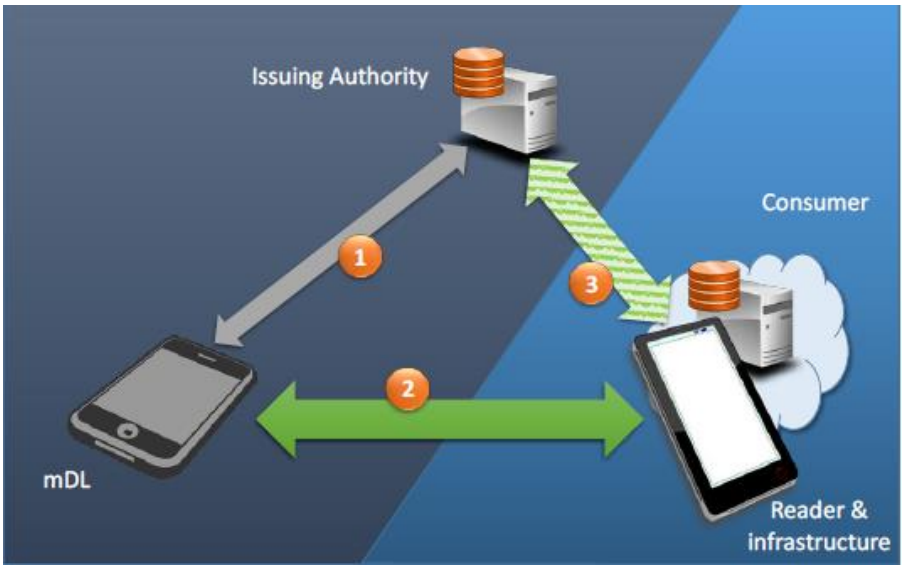

Figure 5: Simplified mDL Architecture

ISO/IEC 18013-5 specifies the interfaces to Issuers for transmitting trust lists or requests (Arrow 3) and for the mDL to reader protocol (Arrow 2), but it does not standardize provisioning or management of mobile devices on which the mDL is provisioned (Arrow 1).

This omission is intentional at this stage of the mDL ecosystem's development. For an mDL ecosystem to flourish, it must allow multiple means of securely exchanging identity attributes with readers so that transactions can be performed according to business-appropriate workflows. It must also give mDL Holders control over their identity attributes, and it must protect the privacy of Holders while meeting the legal requirements of mDL Verifiers. Since multiple models for provisioning or managing readers can coexist under current conditions, creating an artificial standard without the benefit of practical experience seemed likely to stifle creativity and investment in finding the best solutions for the long term.

Instead, standards for provisioning are being developed in a parallel process[10] while the ecosystem builds out. Requirements for trustworthy provisioning and management must come from Issuers' jurisdictional requirements. In North America, AAMVA is coordinating among state and provincial DMVs, with the U.S. and Canadian federal governments likely to play an additional role related to mDL use in their various programs. These efforts may map to and leverage one or more existing trust frameworks. In Canada, DIACC has laid the groundwork with the Pan Canadian Trust Framework (PCTF).[11] In most countries, a combination of legislation and regulation will establish mDL requirements. In the absence of formal requirements, NIST 800-63-3 should be used to guide best practices for identity assurance, federation assurance, and authentication assurance. High quality, accurate provisioning is required to retain the NIST Identity Assurance Level (IAL) 3 proofing that help make a state-issued DL/ID such a widely trusted document.

3.1 Provisioning and Issuance Management

The legal authority for an mDL, as for a traditional DL or ID card, resides with the Issuer. The Issuer generates the mDL data record, signs it, and provisions the mDL onto the mDL Holder's smart device. The Issuer assumes the responsibility of selecting a provisioning scheme that is convenient and provides the necessary security, privacy, and identity assurance to correctly match the device and the Holder while also complying with applicable legal requirements.

The Issuer is also responsible for providing updates and managing the lifecycle of the credential on the device according to policies that support legal use in the Issuer's jurisdiction. Ideally, to maximize the mDL's utility to the Holder, the Issuer should select technology for securing and managing the credential and data that satisfies legal requirements, as well as the functional needs of desired Verifiers. To build global trust in mDLs, the ecosystem will need a trust framework that includes and is understood by Verifiers. Legal requirements and desired assurance levels should be mapped to this trust framework. ISO/IEC 18013-5 suggests that memorializing mappings could be done through a decentralized system of publicly distributed Master Lists[12] of Issuer signing certificates, but other architectures are also possible.

An mDL must be provisioned to the authentic smart device of the Holder, and it must stay there. Issuers must select accurate and secure methods of provisioning mDLs to devices and communicate the associated levels of assurance to the Verifiers through publicly available trusted certificates. The methods currently used for internet IDs—e.g., possession of an email address, SMS of a one-time passcode, and self-asserted enrollment—do not provide sufficient security to allow trust. At the same time, Issuers want to minimize the in-person demand for mDLs at their physical locations. The industry and Issuers can work together to provide secure and straightforward provisioning technologies for both in-person provisioning and remote (sometimes called *selfie*) provisioning.

3.2 In-Person Use

Standardizing the transactions between the mDL Holder and the Verifier ensures interoperability and security. The technology chosen should not be proprietary and should operate on the operating systems and device capabilities of as many of the smart devices as possible that are available to both

[10] ISO/IEC JTC-001/SC-17/WG 04

[11] https://diacc.ca/pan-canadian-trust-framework/

[12] Master Lists are signed lists of certificates from actual, real-world verified Issuers.

mDL Holders and Verifiers. (Section 2.2 describes the mDL sharing mechanisms.) Transactions rely on trustworthy Holder authentication, mDL Holder consent, and verifiable attribute transmission.

In addition to interoperability and security, standardization opens the aperture to providing in-person service in new and even personalized ways. In a robust ecosystem with full implementations of standardized mDL solutions, Verifiers can provide ever more efficient services to Holders who retain control of their identity information. Standardized interactions jump start an ecosystem where privacy-preserving interactions leave all parties with little risk while enjoying more efficient services.

3.2.1 Holder Authentication

Day Two (Table 1) functions make it possible to provide Holder authentication at different trust levels (in NIST terminology, authentication assurance levels). Options already exist to allow Issuers to provision mDLs to retain the highly proofed IAL of DL cards,[13] and a mobile device's security capabilities can protect the provisioned mDL on an ongoing basis. Increasingly stringent Holder authentication, provisioning, and mDL data management would greatly mitigate risk for Verifiers and enable unattended and distance use cases.

In the Day Two mode, relying parties should be able to select the level of trust they need to address their transaction risk. In the offline/transmit mode, identity verification is likely to be handled out of band, by a human attendant. In OIDC implementations of online/token mode, an authentication request matching the Verifier's risk can be included in the request using the Authentication Context (acr) or Vector of Trust (vot) parameters.

3.2.2 Consent

Informed consent is critical to Holder trust in the mDL and has value for Verifiers as an indication of the Holder's participation in the transaction (even more critical in light of the EU General Data Protection Regulation [GDPR] and privacy legislation enforcement). (For a full discussion of informed consent, see Section 5.3.)

3.2.3 Attribute Assurance

Regardless of how identity attributes are transmitted from an mDL, they must convey the characteristics that contribute to trust for the Verifier.[14] The main characteristics or metadata about identity attributes that Verifiers would evaluate in order to determine their trust in the data are (Figure 6):

- Provenance, or the authoritativeness of the validator of the identity attributes. For mDL, the validator is the Issuer who digitally signs the mDL data elements.
- Accuracy, which measures how stringently the identity attributes were examined.
- Freshness, which conveys how recently the identity attributes were determined to be accurate.

[13] Paul A. Grassi, Michael E. Garcia, James L. Fenton, NIST Special Publication 800-63-3, *Digital Identity Guidelines*, National Institute of Standards and Technology, June 2017, https://pages.nist.gov/800-63-3/sp800-63-3.html.

[14] Attribute trust is described by NIST in Internal Review document 8112, "Attribute Metadata: A Proposed Schema for Evaluating Federated Attributes Public Draft Open For Comments!," https://pages.nist.gov/NISTIR-8112/.

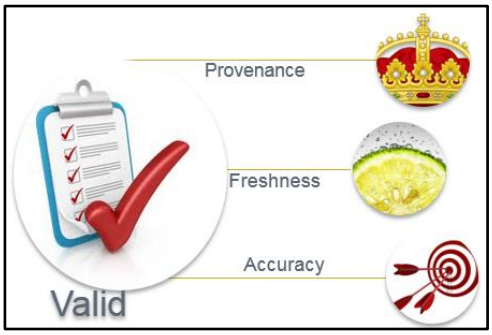

Figure 6. Components of Identity Attribute Validation

The mDL can convey all of these characteristics in both Transmit and Token and Request operating modes (see 2.2.1 and 2.2.2). Accurate attributes are signed by the Issuer when provisioned, and checking those cryptographic signatures demonstrates provenance. The Verifier can check freshness using the last and expected refresh times available within the mDL data.

3.3 Issuer Interfaces and Certificate Trust Models

Issuers sign mDL data so that Verifiers can trust the data. Issuers are also required to publish a signing certificate (a public key) that is used to validate the signatures.

Verifiers authenticate the mDL and the mDL data digitally. They can see that the data is unaltered and that it is being presented to them from the device to which it was originally provisioned. Verifiers should ensure that the verification process is secure and adheres to the best practices stipulated by applicable state and federal laws and regulations.

In online mode, Issuers either implement their own system or work with an Identity Provider that authorizes requests from Verifiers for identity information about the mDL Holder. The request is authorized by asking the proper mDL Holder for consent to release the specific set of requested mDL data.

In transmission mode, Verifiers are responsible for obtaining and trusting the certificates used to authenticate the transferred data.

In token and request modes, certificates identify and secure TLS connections to the online interfaces. Verifiers can use a standardized means of discovery or can present the mDL Holder with identifying information from certificate chains to trusted root certificates. This process is currently used by SSL-secured web sites to ensure that sites identify themselves properly to consumers and to help consumers avoid inadvertently connecting to rogue sites.

> ***In the future…***
> Business models may develop that enable Verifiers to subscribe to curated master lists of up-to-date certificates.

4 Privacy

The right to control personal data is considered fundamental.[15] For this reason, the AAMVA mDL Working Group highlighted the requirements for mDL Holder consent, selective release of information, and mDL Holder visibility into processing within the original mDL functional needs white paper.[16] The right to privacy has evolved further to include the concepts of data protection, audit logging, and resistance to tracking.[17] Privacy is the measure by which citizens will trust an mDL ecosystem.

The recommended approach to protecting privacy is for Holders to choose identity applications that give them control over the release of their personally Identifiable Information. Issuers should therefore consider architectures that permit Holders to choose between multiple applications. Since in many instances, Issuers are opting to use a single mobile application to meet the needs of all Holders, they should evaluate candidate apps using ISO/IEC 18013-5 DIS Annex E, *Privacy and Security Recommendations*, as a guide.[18] The Annex lists privacy protection measures embedded in the design of the protocol and specific recommendations for both Issuers and Verifiers to follow when they implement the standard protocol. The Annex is designed to be used by Issuers as requirements listed in a request for proposal (RFP), but it applies equally well to Verifiers (discussed below).

4.1 Principles of Privacy

The often-quoted privacy by design principles (first published by Dr. Ann Cavoukian) set the following goals for computer systems to implement both privacy and full application functionality:

- Implement data minimization and anonymization wherever possible.
- Be proactive, to prevent data breaches.
- Make privacy the default setting.
- Embed privacy in the design, flows, and architecture.
- Do not trade off privacy for full functionality.
- Protect the full lifecycle of the user's identity.
- Keep all operations visible and transparent to the user.
- Design for user-centricity and user-control of the user's identity.

4.2 Information Processing Privacy Principles

ISO/IEC 29100:2011 lists a set of goals to be met whenever personal information (identity attributes, personal data, or usage information and statistics) is processed by a software system acting as a data controller that stores data or as a data processor. It is important to note that the Issuer is not often the data processor in an mDL transaction – the act of connecting the mDL to the reader constitutes Holder

[15] There is both legal (Brandeis) and academic (Acquisti) determination of the fundamentality of this right.
[16] American Association of Motor Vehicle Administrators, *Mobile Driver's License Functional Needs Whitepaper*, v0.9, https://www.aamva.org/mDL-Resources/
[17] American Association of Motor Vehicle Administrators, *mDL Implementation Guidelines*, released April 2019, https://www.aamva.org/mDL-Resources/.
[18] ISO/IEC 18013-5 N1800, op. cit.

consent. The Issuer, acting as data controller, implements a sharing and consent mechanism, supported by ISO/IEC 18013-5, that allows the Verifier to become a data processor.

Before mDL application or reader software is implemented, it should be evaluated for adherence to the information processing principles specified in ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework* (Table 3).

Table 3. Privacy Principles

Principle	Explanation
1. Consent and choice	Data subjects must consent to the processing of their personal data.
2. Purpose legitimacy and specification	Data subjects should be fully aware of the purpose for which their personal data is being collected, processed, and potentially stored.
3. Collection limitation	The data controller and data processors should only collect the data necessary for their purpose and should only collect data consistent with these principles.
4. Data minimization	Processing of data should be minimized to that specifically necessary for the purpose specified.
5. Use, retention and disclosure limitation	Data processors should not use personal data of the data subject except for the purposes specified and consistent with these other principles. Personal data should only be retained for the period necessary to provide the service.
6. Accuracy and quality	High accuracy of data being processed and held is in the best interest of the data subject and data processors should take measures to ensure accuracy.
7. Openness, transparency and notice	What data and how data is being processed should be well known to the data subject, including obtaining consent and posting and updating clear notices.
8. Individual participation and access	Data subjects should be involved in the collection, consent, processing, and storage management of their personal data.
9. Accountability	Data controllers and data processors must be accountable for all aspects of the processing of personal data and provide audit logs and auditability to the data subject.
10. Information security	Personal data should be protected by security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.
11. Privacy compliance	Personal data should be processed according to all applicable laws, including laws that apply to the data subject.

Incorporating these principles into the software design and examining their implementation during design reviews can indicate whether privacy protections are being met. One way to evaluate mDL application or reader software is to ask what the software does to enforce each of these 11 principles. For example, the ISO/IEC 18013-5 data model and signature mechanisms are designed so that the mDL Holder can consent to share individual data fields, thus addressing Principle 4, data minimization. The mDL reader can request, and the mDL Holder can approve, a subset of the available mDL data. This both

supports data minimization and permits the application developers to decide how consent is obtained from the Holder and translated into the Holder experience for data sharing (Principle 1).

4.3 Privacy for Verifiers and mDL Readers

Ensuring privacy is a collective effort to which all components in an mDL ecosystem must contribute. Verifiers make decisions about access to services using mDL readers that implement the standard protocol. It is in the Verifier's best interest to protect an mDL Holder's privacy since it can drive improved customer relationships.

The following principles help to mitigate privacy risks:

- Minimize the data requested.
- Register readers and identify them to the mDL Holder.
- Communicate expectations to the mDL Holder.
- Store the minimum amount of data, paying attention to the "intent to store" flag.
- Do not submit data to a centralized data service.

4.3.1 Minimize Data Requested

To minimize the requested data, ask only for the data required by the compliance needs of the use case. Use-case evaluation can identify what mDL data elements are legally necessary.

For example, to purchase alcohol, an unexpired government-issued ID confirming an age and held by the proper anonymous person may be all that is necessary to comply with the law. Asking for additional data can expose the requestor to liability and create friction. All that is necessary is to determine that the mDL is not expired, that the Holder is over the legal age, and that the person present is the authentic mDL Holder (in Day One, this verification is done by asking for the mDL's digital portrait of the Holder and manually performing a visual confirmation). Other identifying attributes that are available on today's physical cards but are not required for legal compliance, such as the driver's license number or home address, should not be requested.

Any Verifier policy that includes the request for additional personal data (e.g., customer contact information for a mailing list) should be reevaluated. If additional services are offered based on personal data beyond what is required for compliance, allow mDL Holders to opt into those services without appearing to require them to approve the transaction. To store any of the data received in an mDL transaction, use the Intent to Store flag.

4.3.2 Register Readers and Identify Them to the mDL Holder

Registering the reader encourages Holder confidence that personal information is protected (reader registration is optional in Day One). To identify reader devices to Holders, it is very useful to register the mDL reader with the local issuing authority and obtain a certificate that clearly identifies the Verifier's business and validates the authenticity of the reader device. The practice of skimming credit card numbers using a rogue reader (for example, at a gas pump) has become common. The equivalent privacy threat to mDL Holders can be mitigated by clearly identifying the mDL reader both visually and electronically.

In addition, perform a privacy assessment of the mDL reader and adhere to the principles described in Section 4.2.

4.3.3 Communicate Clear Expectations to mDL Holders

Customers should always see clear signage and electronic communication identifying what personal data are required to meet compliance requirements and what additional personal data will be requested. An easy-to-follow process with a clear, consistent result is good business and will enhance the mDL Holder's confidence.

4.3.4 Store the Minimum Amount of Data and Follow the "Intent to Store" Flag

Storing identifying personal data increases exposure in case of a data breach. Audit logs can be created that demonstrate legal compliance (for example, by using a transaction or receipt number) without including information identifying the Holder.

When the Intent to Store flag is set for individual data elements, store only those elements. Impose proper encryption and storage protection for the data, and never share the data with other entities unless required by law.

4.3.5 Do Not Submit Personal Data to Centralized Services

Do not report Holders' personally identifying information to any centralized service that compiles usage data, regardless of whether the data is obtained from offline or online mDL interactions. For example, an Alcohol and Tobacco Control Board should not create a centralized service to compile usage data on mDL Holder transactions, even anonymously. Such a service is a vector for tracking citizens and businesses, whether intentionally or if the data is leaked.

5 Building Trust

Generally, transactions requiring identity verification carry a certain amount of risk. The Holder needs to be able to trust that the Issuer and Verifier will protect the Holder's identity data and use it only for the purposes to which the Holder consents. The Issuer needs, to an extent, to trust that the Holder has not falsified or misrepresented the data during enrollment beyond the Issuer's ability to authenticate the data independently. The Verifier needs to trust that the Issuer proofed and provisioned the identity data responsibly, that the Holder has a legitimate claim to the data, and that the data has not been falsified or altered post-provisioning. Trust is not and should not be a default state. It is built through transparency and adherence to policy and technical standards.

Because a fully trustworthy mobile identity (e.g., mDL) requires the participation of many different entities, there must be a framework for participation and legal adherence. Issuers must work with the industry to provision data accurately, maintain freshness, and secure mDL Holders' identity data. Verifiers must have simple mechanisms and processes for interacting with mDLs. Standardization will make transactions transparent and allow trust to permeate throughout the ecosystem (Figure 7).

Figure 7: Global and Regional Groups Involved in Standardization

This section discusses the general requirements for building trust in an identity ecosystem, then highlights how ISO/IEC 18013-5 compliant mDLs implement these requirements.

5.1 Current Trust Frameworks

A number of efforts to create a trust framework are currently under way, including the following:

- The U.S. Government's Federal Public Key Infrastructure (FPKI) provides the U.S. Government with a trust framework and infrastructure to administer digital certificates and public-private key pairs.

- The Kantara Initiative's Assurance Framework and related programs accredit assessors and approve services operated by credential service providers at assurance levels applicable to any trust framework or scheme rules globally, based on service assessment criteria developed, maintained and managed by Kantara.
- SAFE Identity's Trust Framework facilitates trust by providing a combination of policies and services for digital signatures, authentication, federation and encryption that are implemented by certified product and service providers.
- The Transglobal Secure Collaboration Program (TSCP) The Public Key Infrastructure (PKI) Bridge Service operates under the authority of the TSCP Bridge Certification Authority (TBCA) to facilitate interoperability among PKI domains.
- tScheme's list of schemes that set out the parameters and standards that are required of a trust service. Trust service providers (TSPs) use schemes to create and administer trust services. (A scheme is a definition of a trust framework, rather than the trust service itself.)
- The Trusted Digital Identity Framework (TDIF) from the Digital Transformation Agency (DTA), Australia is a set of rules and standards that accredited members of the digital identity federation must follow.
- The Draft Pan-Canadian Trust Framework, under the oversight of the Digital ID and Authentication Council of Canada, the Identity Management Subcommittee (IMSC) of the Joint Councils, and others (Canada), is intended to standardize trusted digital representations (i.e., identities, attributes, relationships) of people, organizations, and things in Canada.
- The Draft Digital Identity Trust Framework from New Zealand has a similar but not identical goal to that of Australia.

Each of these frameworks defines how to provide effective identity assurance, credential security, and authentication for citizens within the appropriate Issuer's jurisdiction. These frameworks can be integrated by mapping to ISO/IEC standard 29115.[19]

5.2 Identity Confidence

In any particular transaction, the Verifier's risk from inaccurate identity information can be mitigated using verification methods that are appropriate to the risk level of the transaction: anonymous, low, substantial, or high. The Office of Management and Budget (OMB) Memorandum M-04-04 defines these risk levels.[20] An updated version, OMB M-19-17,[21] matched these levels more closely to newer NIST identity assurance guidelines. The definitions of each level may differ slightly from region to region; however, efforts such as the LIGHTest Community[22] are attempting to map the definitions to other non-U.S. regional trust authentication efforts.

[19] ISO/IEC 29115:2013, *Information technology — Security techniques — Entity authentication assurance framework*, https://www.iso.org/standard/45138.html.

[20] Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2004/m04-04.pdf.

[21] Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

[22] https://www.lightest-community.org/

These levels quantify the risk to Verifiers and also determine the identity proofing, credential protection, and Holder authentication risk mitigation measures needed at transaction time. Protecting anonymity when some identity information may be necessary is critical to Holder trust in the identity ecosystem and can be achieved through proper privacy engineering.

5.2.1 Sensitivity or Risk in Transactions

In determining risk level, the Verifier should consider the impact of accepting a false identity or rejecting a true identity, and the cost of the verification method (e.g., acquisition, maintenance, transaction time, and availability) relative to the benefit provided by the level of assurance. Table 4 describes the different risk levels and verification methods that apply to some example transactions.

Table 4: Example Transactions with Verifier's Identity-Related Risk Level

Transaction	Verifier Risk Level	Verification Method
Using a coupon at a merchant	None *Requires no identity certainty*	There is no need to identify the Holder.
Registering for a social media account	Anonymous *Requires little identity certainty*	Use a unique identifier to access an account or service. Little or no personal identifying information is required.
Banking using an ATM	Low *Requires some identity certainty*	Identity verification and document authentication are fulfilled by an unassisted check. Compliance requires an official, legal document. The transaction may require and record some personal identifying information.
Employment enrollment	Substantial *Requires high identity certainty*	Often additional authentication tools (e.g., lights, scanners) are used, and biometric comparison may be performed.
U.S. Customs and Border Protection verification of enrolled Global Entry member	High *Requires very high identity certainty*	Equipment has been necessary to improve upon human accuracy for identity verification and document authentication. Accurate and recent identity attributes are required to perform the transaction.

Note that the mDL constitutes a mobile identity with security technologies that permits any citizen to carry a mobile authenticator.

In order for Verifiers to trust an mDL, the mDL and the Issuer must operate at assurance levels that mitigate the Verifier's risk digitally. Without this mitigation, Verifiers will not choose to accept an mDL but will continue to use current transaction methods that may seem secure but do not provide comparable security or efficiency.

5.2.2 Levels of Assurance in Identity

The ISO 29115 Entity Authentication Assurance Framework establishes four levels for confidence in the veracity of the identity of the asserted individual (Figure 8). The four levels can be mapped to any

regional trust framework that may use other terms or levels for components such as identity assurance and user authentication assurance.

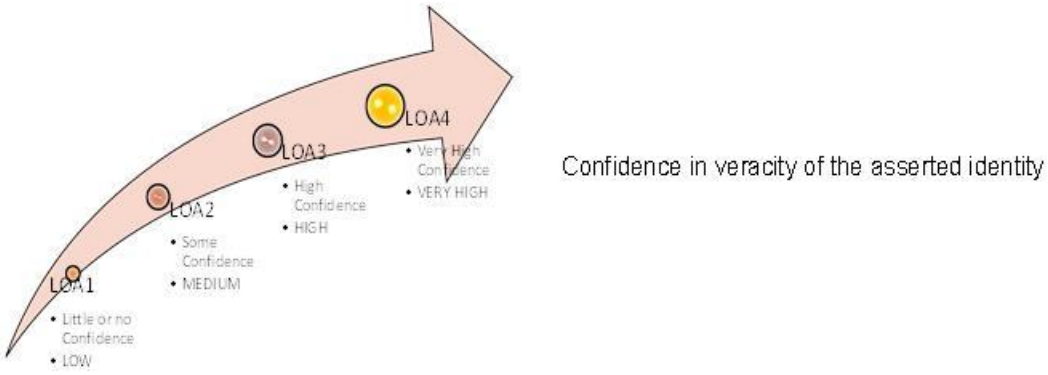

Figure 8. Levels of Assurance According to ISO/IEC 29115:2011

5.2.3 Identity Assurance, ID Protection, and Holder Authentication

To mitigate Verifier risk and provide the confidence needed by the Verifier and the Holder to complete a transaction, identity systems must provide three things:[23]

- Identity assurance. When issuing an ID, the Issuer must prove the Holder's identity is legitimate and unique and the attributes are accurate, and then issue the ID to that human being.
- ID protection. During the period between issuing the ID and a transaction, the identity system must protect the ID from tampering, change, mismanagement, and theft.
- Holder authentication. At the time a transaction takes place, assurance must be given to the Verifier that the ID is being presented by the legitimate Holder.

Due to the rapid evolution of technologies such as biometrics and mobile device management, mobile technology currently includes technical methods that provide easy-to-use assurance, protection, and authentication.

5.3 Privacy and Informed Consent[24]

Issuers must select technology and make design choices that meet privacy regulations and surpass the needs of their Holders.

5.3.1 Holder Control

One of the key concepts supporting privacy and informed consent is Holder control. Key to Holder control is informed consent. Holders must be provided with information any time they make a choice to share information, not using a blanket permission or providing it solely in advance. Informed consent

[23] ANSI/NSPI IDV-2018, *Requirements and Implementation Guideines for Assertion, Resolution, Evidence, and Verification*.

[24] Additional information on privacy and consent can be found in ISO/IEC standard DIS 29184, *Online privacy notices and consent*, and Kantara Consent Receipt specification v1.1 (likely to form part of the text for WD0.1 ISO/IEC TS 27560 Privacy technologies – Consent record information structure).

should provide three pieces of information every time the Holder must make a decision about sharing information: the identity of the entity with whom the holder is sharing the personal information, the personal information being shared, and the purpose for sharing. The entity should then respect the Holder's choices. mDL apps and reader devices should be designed to enforce the Holder's choices.

5.3.2 Known Person Identifiers

One privacy concept that is critical is the *known person identifier*. A Verifier must always receive the same number to identify a particular Holder, but the number must be unique to that holder and that verifier (in OIDC, the known person identifier is a pairwise, pseudonymous user identifier). The Identity Provider cannot use the same number to identify the Holder to different Verifiers. Using pairwise, pseudonymous user identifiers helps prevent the release of a number that could be used to correlate holders across events in which they used their credentials.

5.3.3 One-Time Tokens

Tokens sent by mDLs to Verifiers should be one-time use tokens, both to protect privacy against tracking by the Issuer or Verifier and to avoid security breaches and replay attacks.[25]

5.3.4 Privacy Goals

The use cases in Appendix C: Use Cases describe what is needed to assess Verifier risk and provide appropriate informed consent to the mDL Holder. Individual implementations are responsible for the level of consent and the Holder experience that lead to the fastest, most efficient exchange.

ISO/IEC 18013 supports informed consent and Holder control for both offline and online transactions. Use case designs and implementations should adhere to the standard when planning the Holder experience for maximum workflow efficiency. The combination of privacy protection with improved workflows will lead to adoption and usage.

[25] A replay attack is an attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.

6 Challenges to a Robust mDL Ecosystem

Implementation of an mDL requires both technical and policy considerations. Each stakeholder's requirements should be addressed to perform implementation properly.

Major considerations are:

- The security and the identity assurance level of the mDL issuance process (Section 5.2)
- The security of the smart device that hosts the mDL credential and its platform
- Communication between the mDL device and the Verifier device, especially in offline mode (Section 2.2.1)
- Verifier trust in the credential across states, countries, and other jurisdictions (Section 5)
- Verifier trust that the credential is in the possession of the proper, intended Holder (Section 5)
- Privacy protection for mDL Holders (Section 5.3)
- Liability and safety considerations for Verifiers and mDL Holders

Other considerations include:

- Phasing of feature roll-out and avoiding the risk of least common denominator solutions
- Verifier understanding of state and global regional policies for identify and verification and security
- Processes for ensuring interoperability among states and solution providers
- Testing, education, and training for both Holders and Verifiers
- mDL Holder signing functionality for use cases where "signing with your ID" is warranted

6.1 Least Common Denominator Roll-out

One of the biggest risks to the adoption of the mDL and to the effectiveness of the mDL ecosystem will be a "wait and see" approach to mDL standards, the rollout of reduced feature sets (because low-end smartphones do not support the required technology), and, therefore, slow uptake because Verifiers cannot get a large enough benefit from accepting mDLs.

This problem is a classic business problem: innovative technology providers must jump ahead and produce what the mDL market needs in the future to gain initial market share, while market-survey-driven companies will focus on what Holders will request next. Issuers and technology providers should support full mDL technology now to kickstart the ecosystem.

Further compounding the issue for mDLs is that vendor lock-in with Issuers could affect what interaction modes Issuers can provide and limit the choice of Verifiers. For example, the technology used in the first demonstrations of mDLs was QR code device engagement accompanied by Bluetooth Low Energy (BLE) data transfer. This technology was chosen because, in 2015, it was available on all device platforms. If in 2020, as mDLs roll out, some mDL technology providers support only these same technologies, Verifier options for interaction modes will be extremely limited. Some Verifiers will consider Bluetooth unacceptable technology, some will require device engagement that operates over a greater distance than optical line of sight (because of physical layout), and some will already have an investment in NFC devices

To spur mDL ecosystem growth, mDL solution providers should build the full range of interaction modes to encourage Verifiers to adopt what suits their workflow needs and therefore provide full citizen value

at the point of sale. An absence of mDL solutions will discourage adoption by Verifiers, which will lower the utility of the mDL for early adopter Holders, which will stunt the mDL ecosystem.

6.2 Identity Enrollment Considerations

The mDL does not create an identity. Issuers establish the Holder's identity through their own enrollment processes. State DMVs are independent and how they proof and enroll identities is not federally regulated. Instead, DMVs coordinate among themselves and through associations to share best practices that safeguard against identity fraud. State DMVs vary in their practices, and these variations are not transparent to Verifiers.

The REAL ID Act, passed by Congress in 2005, enacted the 9/11 Commission's recommendation that the Federal Government "set standards for the issuance of sources of identification, such as driver's licenses." The Act established minimum security requirements for issuing and producing state-issued DL and ID cards and prohibits Federal agencies (as Verifiers) from accepting any state-issued DL or ID cards for official purposes that do not meet these requirements. As defined in regulation, official purposes are accessing Federal facilities, entering nuclear power plants, and boarding federally regulated commercial aircraft. The Act does not authorize the Federal Government to regulate state DMVs, but rather standardizes the requirements for Federal agencies to accept state-issued DLs and IDs.

All states have agreed to adopt REAL ID requirements and issue compliant driver's licenses for those specific use cases.[26] As a result, the Act potentially has a dual effect on mDLs.[27] First, a Verifier can know that a notional REAL ID-compliant mDL has met the Act's requirements for proofing an identity.[28] Second, not all Holders will have REAL ID-compliant DLs and, therefore, not be able to have compliant mDLs. In some cases, individuals will hold DLs that predate their state's compliance; in others, the Holder may have been ineligible for a compliant license or chose not to obtain one.[29] Therefore, mDLs will need to be able to electronically communicate to a reader device whether the mDL is compliant or not.[30] Federal Government Verifiers applying the three official purposes will need to determine whether the mDL is REAL ID-compliant. Verifiers may not use the REAL ID designation for any other purposes including voting, banking, and applying for employment or other benefits. The mDL, just like the REAL ID, is not intended to serve as a national ID card.

Five states issue enhanced driver's licenses (EDLs), which provide proof of identity and U.S. citizenship.[31] EDLs are not automatically considered REAL ID compliant but are Western Hemisphere Travel Initiative (WHTI)-compliant border crossing cards. The state must independently fulfill REAL ID requirements and

---

[26] As of October 2019, 51 states and territories are compliant, and the remaining are committed to become compliant. As of the REAL ID deadline, every air traveler 18 years of age and older will need a REAL ID-compliant driver's license, state-issued enhanced driver's license, or another acceptable form of ID to fly within the United States. For more information, see https://www.tsa.gov/real-id.

[27] DHS is currently reviewing the mDL and has not issued a policy about acceptability.

[28] Compliant cards are marked with a star that may be gold, white, black in several different approved formats. Noncompliant licenses include one of various statements, approved by DHS, that signify the card is not acceptable for official federal purposes. Licenses with neither marking are legacy licenses issued before a state became compliant with REAL ID and are noncompliant cards.

[29] To be eligible, an applicant must establish lawful presence among other qualifications, as defined in the REAL ID Act of 2005 and implementing regulations.

[30] AAMVA *mDL Guidance for Issuers* has defined a REAL ID flag for mDL, https://www.aamva.org/mDL-Resources/.

[31] Michigan, Minnesota, New York, Vermont, and Washington.

submit a compliance certification to DHS.[32] The standard allows Issuers to create additional data elements, so an EDL or WHTI indicator could be added.

6.3 Transmit Model Challenges

Despite the widespread availability of technologies such as BLE, NFC, and WiFi Aware, it is still challenging to establish a connection and transmit a larger amount of data reliably between heterogeneous untrusted smart devices. mDL portraits can be sizable and take time to transmit.

Holders may not know the correct location of the NFC antenna in their smartphones and may have to double tap to first connect the two devices and then transmit data using NFC. Ticket takers at stadiums that have implemented NFC ticketing can attest to the variability and learning curve being different than NFC point-of-sale devices were one device is in a fixed position.

Establishing a connection using unpaired BLE can be difficult, even between smartphones from the same vendor, due to different BLE stack implementations. The actions to establish reliable transmissions may not be the same between any pair of devices – mDL and reader.

Furthermore, Holders will have to grant their mDL apps access to multiple system functions (e.g., BLE, NFC) at the operating system level. They are free not to permit what they do not wish to open up, which can lead to reduced usability and frustration.

6.4 Online Model Challenges

In the online model, the Verifier and possibly the mDL device should be connected to their respective internet providers. The Verifier must connect to the URL of the Issuer received from the mDL. Some architectures may require both parties to be connected.

An online mDL should increase the chance that the mDL Verifier will always receive the freshest data, which also means that credentials can be revoked or certain attributes updated immediately (such as after a theft).

Battery management and connectivity are improving rapidly, as boarding passes and other high-reliability use cases go online, but both still represent some of the most common challenges for Holders – running low on battery or dropping connection.

Privacy is also a concern for potential mDL Holders in the online model since the Verifier will be connecting to the Identity Provider or Issuer at transaction time. Some identity ecosystems operate on a model that monetizes Holder information and Holders explicitly or without knowing accept being tracked for access to services. For mDL implementations, Issuers and Verifiers should implement privacy safeguards (discussed in Section 4.2) to build and keep trust. Both the online model and offline models should enforce these safeguards and not use calls back to an Issuer for tracking Holders.

6.5 Trust Framework Considerations

A trust framework has been defined as “a legally enforceable set of specifications, rules and agreements regulating an identity system,”[33] or “a complete set of contracts, regulations or commitments that

[32] EDLs are issued through a secure process that incorporates passport requirements and include technology that makes travel easier. For more information on EDLs, see https://www.dhs.gov/enhanced-drivers-licenses-what-are-they.

enable participating actors to rely on certain assertions by other actors to fulfill their information security requirements."[34] It encompasses a set of policies that determine the strength of digital identities as well as the operational requirements to which all parties – Issuer, Holder, Verifier, and others – operating under the framework must adhere.

While specifications written by ISO and the identity community describe certain aspects of a trust framework, there is currently no overarching infrastructure, policy suite, or group of issuing members to correlate mDLs from various states for the benefit of relying parties and citizens. Once there are cross-jurisdictional uses of mDL, a framework will be necessary (e.g., to maintain the integrity of the mDL identity assurance and interoperability).

A trust framework serves the following goals for an mDL:

1. Establishes a common set of minimum criteria for Issuers and Verifiers. Publishing the criteria allows all parties, including the mDL Holder, to make an educated decision concerning trust.
2. Provides a certification process for Issuers participating in the trust framework and monitors and audits Issuers for continued adherence to trust framework policies.
3. Tests for technical interoperability of identity credentials from different Issuers to ensure acceptance by relying parties.
4. Provides a mechanism for conveying trust to Verifiers within the framework. Master Lists of signer certificates are the technical mechanism used by mDL.
5. Provides minimum requirements for binding a human identity to a digital credential in a way that is comparable to how physical credentials are bound.
6. Cooperates with Verifiers to develop specifications for verifying and relying on mDL data within the framework.
7. Protects the privacy of citizens participating in the ecosystem.

It is reasonable to expect that each national entity will establish a trust framework to streamline trust across a wide range of Issuers and ensure seamless mDL interoperability. These regional trust frameworks will require a trust framework or operational body to unify them.

In the United States, it is reasonable to expect that several trust frameworks would be established, perhaps geographically, to serve the 56 states and territories (including the District of Columbia) that could be expected to participate. A U.S. regional trust framework would provide national oversight and accreditation for each of the local trust frameworks.

With regional or country trust frameworks developed, it may be necessary to map these to other regions in order to promote true global interoperability and trust.

---

[33] Esther Makaay, Tom Smedinghoff, Don Thibeau, Trust Frameworks for Identity Systems, Open Identity Exchange, June 2017, https://openidentityexchange.org/blog/2017/06/22/trust-frameworks-for-identity-systems/.

[34] Rainer Hörbe, *Trust Framework Meta Model*, June 22, 2012, Kantara Initiative, https://kantarainitiative.org/confluence/display/archive/Trust+Framework+Meta+Model.

6.6 Verifier Understanding of Another State's Policies

A Verifier relies not only on the provenance of an mDL but also on the identity being linked to the correct Holder. Verifiers may have different requirements for the degree of certainty applicable to these linkages given the risks of the specific transaction and the consequences of fraudulent usage. Some Issuers may require Holders to be physically present and provide multiple sources of identification in order to be issued an mDL, and this type of identity and verification policy provides Verifiers with a high degree of confidence in the identity associated with the mDL. Other Issuers may allow remote issuance, with few factors of identification.

The draft ISO standard for mDL does not contemplate a means for Verifiers to know what policies were enforced by Issuers to provision the mDL, nor does it specify Holder authentication methodology. This absence suggests that implementers of solutions that accept mDL will need to customize their treatment on a state-by-state basis, which could prove daunting. Unfortunately, Verifiers may be compelled to downgrade their trust in each and every mDL to the level assigned to mDLs issued under the weakest of identity assertion policies. Neither scenario is ideal, because the value stakeholders receive from the system is greatly diminished.

Verifiers should be cognizant of the varying degrees by which Issuers could establish the identity and verification policy and consider their individual use cases against that other state's policies. The many-to-many relationships for doing this are a complexity that a trust framework can reduce.

As the ISO 18013-5 Working Group continues its work in 2020, Holder authentication and the retention of identity assurance during provisioning should both be top considerations for mDL to flourish.

6.7 Testing and Certification

Today's environment is becoming more mobile, and states are already adopting and implementing the mDL. The mDL can authenticate citizens in a number of use cases in which a physical DL is being used today at varying levels of security and accuracy. Verifiers are expected to implement an mDL reader that can validate that the person presenting the mDL is the rightful Holder (e.g., verify facial image from the mDL). These solutions should comply with the ISO/IEC 18013-5 specifications and be interoperable across jurisdictions.

One of AAMVA's goals is to publish guidance for interoperability across issuing jurisdictions for U.S. and Canada. To achieve this, device engagement and data transfer methods must be standardized. Requests by Verifiers must be able to satisfy the use cases detailed in Section 11 of this white paper, regardless of the mDL Issuer or Verifier. This is critical both to drive mDL adoption across jurisdictions and to build trust among the participants in an mDL ecosystem.

ISO/IEC standard 18013-5 requires an interoperable interface between the mDL and the mDL reader. ISO/IEC 18013-5 specifies different data transfer methods to support offline and online interactions and specifies the implementation of security mechanisms to protect the mDL data on the Holder's device and enable secure communication during each interaction.

To promote country-wide adoption and acceptance across jurisdictions, both mDL Verifiers and mDL solution providers should ensure that solutions are tested, certified, and compliant with ISO/IEC 18013-5. Testing and certification not only ensure that a solution complies with the specification but also ensures that solutions interoperate through secure and standardized interactions when engaged with implementations supported by different Verifiers. At the time of this white paper publication, the mDL testing and certification infrastructure is still being developed. The industry anticipates that the process

will progress using ISO certification processes and establishing third-party testing and certification services.[35]

Issuers, Verifiers, and application developers should work together to further the adoption of testing and certification by all involved parties. In addition to adopting testing and certification processes, it is important that Issuers and Verifiers appropriately educate mDL Holders on the value of the integrity and trust that certified products offer. The Issuers, Verifiers, and application developers should also find clear and accessible methods to communicate testing and certification status to mDL Holders in order to establish trust and encourage mDL Holders to make informed decisions about their personal data.

6.8 Considerations to Ensure Interoperability

Apart from complying with the ISO/IEC standard, an mDL Holder application and an mDL reader solution should provide the same level of consistency and standardized data transfer across jurisdictions. For example, during implementation, both Verifiers and mDL solution providers need to ensure that requested data elements and PII are consistent and available from the mDL. If an optional mDL data element is requested but is not a data element supported by the mDL Holder's app, the identity transaction will not be completed as designed by the Verifier. It is important that developers of verification hardware and software work to ensure these transactions fail gracefully and with instructive messages for completing the transaction as needed.

There is a need for industry-specific bodies to play a role to define the best practices for data transfer and consistency that affect mDL implementation for their applications (e.g., age verification at retailers, identity verification in healthcare). Much like the case when a transaction fails due to optional data elements which are unavailable, graceful and informative transaction failure is also needed for cases where an mDL Holder does not consent to the data requested by the Verifier. It is essential that the cause of failure is properly communicated to involved parties so they may make informed decisions about how to proceed.

The primary objective of the mDL is to confirm identity and convey driving privileges. It is anticipated that Verifiers will need customized data elements, as defined in the standard (e.g., hunting license, TSA trusted traveler indicator). Verifiers need to ensure that any customized data element requests outside the scope of ISO/IEC 18013-5 are implemented carefully and comply with local rules and state PII policies. Issuers will need to make custom data elements available to the mDL Holder's app in the regions where they are used.[36] Finally, the entire digital transaction between the mDL Holder's app and the mDL reader should not deviate from the privacy principles and security recommendations listed in ISO/IEC 29100:2011.

Like a traditional driver's license, an mDL should be usable in many different geographical areas and legal jurisdictions. There is therefore a need for readers that can authenticate the cryptographic aspects of an mDL, which may raise interoperability issues. To ensure that mDLs can be successfully authenticated requires sharing signed public keys (signer certificates) that are trusted by several different geographies. Both offline and online models are supported by ISO/IEC standard 18013-5.

[35] It is important to note that some states are implementing mDLs using ISO 18013-5 in advance of the final standard and testing and certification processes.

[36] Additional work is needed by ISO to define data structures and signing capability, and by industry to gain agreement on how to implement customized data elements that are interoperable across jurisdictions.

In the offline model, Verifiers will need to obtain public keys from other jurisdictions to verify the signature on data obtained from an mDL. It is currently envisioned that associations of Issuers or payment networks will assemble trusted public keys and distribute them to Verifiers.[37] Verifiers will need to preload certificates from any Issuers that they expect to encounter and hold them, to verify data while they are offline. Verifiers should also periodically connect to update their trust lists of certificates and verify that the signer certificate complies with the trust list signer certificate profile.

6.9 mDL Holder Document Signing

One logical extension of mDL functionality is for Holders to be able to use their mDLs to sign documents. Many use cases, such as visiting a notary or completing the mortgage process, require a DL or ID card to verify identity, after which a physical document is signed. When these processes involve two distant locations (e.g., buying a home in Massachusetts while living in California), participants must either travel or use inconvenient, legally binding remote procedures. To allow these use cases to be completed online or to automate them require the proofing assurance of the mDL with transaction-time Holder authentication, as well as a full rollout of mDL technologies. The logical extension of Day Two unattended mDL operation is remote "login" usage, a precursor to digital signing of documents.

Cryptographic signatures are widely used in organizations which deploy smart cards for assured identity, and the standards for digital signing and electronic signature are well established.[38] The signing feature is typically used to sign digital documents such as PDFs or emails.

mDL technology can provide mechanisms that an mDL Holder can use to create digital cryptographic signatures on documents. A private-public key pair generated during the creation of the mDL is used as a device identifier and these keys are bound to the Holder's identity through the issuance process. These keys, which are used as part of the mDL device authentication process, could also be used to provide a cryptographic signature on any data or documents the Holder chooses.

Implementation of cryptographic signatures would require an mDL app that supports both the ISO/IEC standard 18013-5 and digital signature standards. There are many use cases where a wet-ink signature on paper could be replaced by a digital signature with stronger security and non-repudiation features. Additionally, signing with an mDL provides document integrity; digital signatures are performed on a cryptographic hash of a document, which only remains valid if the document is unchanged after signing.

In use cases requiring wet-ink signature verification, the mDL can provide additional integrity. An image of the Holder's signature is an optional data element in ISO/IEC 18013-5. This image can be incorporated into the authentication and signing process for a Verifier who may wish to digitally compare a signature on paper and the signature image provided by the mDL data.

6.10 General Security Considerations

ISO 18013-5 provides and documents many security requirements related to the exchange of mDL data from the mDL to the Verifier. To generate requisite trust from all parties in an mDL ecosystem, other security requirements must be met by mDLs, Verifiers, Issuers, and the environment in which they operate. The Secure Technology Alliance and the broader community of interested parties can begin

[37] ISO 18013-5 Annexe C – Master List Provider - https://isotc.iso.org/livelink/livelink?func=ll&objId=20919524&objAction=Open

[38] NIST FIPS 186-4, *Digital Signature Standard* (DSS)

the discussions around security of the ecosystem prior to deployment of a trust framework. While this topic is very broad with many interested parties requiring a seat at the table, some areas to consider immediately are focused on community education and outreach.

For all transactions, it is of utmost importance to obtain cryptographic proof of the integrity of data being presented and verification the correct Holder is presenting that data to the Verifier. This is the only process in place to prevent fake ID applications or impersonators from being widely used. It is of critical importance for the community to educate both relying parties and state and local officials on the pitfalls of accepting the display of mDL data on the screen of a mobile device as the means of transaction. Spoof applications are simple to write and will be very difficult to distinguish from real mDL applications in transaction environments such as age-verification purchases.

The security documentation of ISO 18013-5 does not define the entire transaction ecosystem envisioned for all Holders, Verifiers, and Issuers. The broader community will need to reach a consensus on what technologies and augmenting standards are needed to develop the full trust framework required. These may include complementing standards to support data exchange outside of the ISO/IEC 18013-5 specifications, such as the FIDO mobile user authentication standard. There may also be a need for accompanying standards to complete the ecosystem for things which are out of scope of the ISO/IEC 18013-5 standard, such as regional trust framework considerations or specific state and national laws.

Additionally, the mobile device manufacturer community has an important role to play in the overall security of the mDL ecosystem. Mobile app protection is limited to the secure hardware and operating system APIs that it can access. It will be imperative that the broader community continue to press vendors to make platform security features available which will ensure secure applications can be developed and deployed at scale.

6.11 Jumpstarting the mDL Ecosystem

The mDL represents a significant change to the physical identity card ecosystem that is largely paid for by Holder purchase of the physical card. Whereas the current system depends on the Holder paying fees to the DMV for issuance of a physical DL or ID card, this payment model cannot be expected to finance the mDL ecosystem and infrastructure. With the emergence of mDL technology, a new business model may be required.

For mDLs, there are interdependencies that could affect market adoption and have an impact on the mDL business model. These include:

- Holders want to have mDLs available for their own convenience and benefit, but do not have a channel to demand it. They have concerns that they will not be able to use the mDL everywhere and for all desired purposes.
- Issuers do not have a mandate and may not be hearing market demand to implement mDLs. Within this environment, first issuers are visionaries moving forward without clear relying party commitment or demand.
- Relying parties will need to invest in capabilities – equipment or services – to consume and verify mDLs. Relying parties may need to accept mDLs without a clear understanding of the Issuer's enrollment and provisioning processes, how mDLs are tested and certified, adoption rates, and cost for operations. Relying parties proceeding forward without a clear means of discerning levels of trust may incur increased legal and operational risk.
- Early adopter relying parties may experience increased operational costs to support and trust a variety of mDLs issued by diverse provisioning methods. This diversity may increase if the

relying party chooses to support mDLs issued in many different regions or through different identity providers.

- Payment for, and the flow of money within, the mDL ecosystem is not consistently envisioned by all potential participants. Regional differences in business model, once adopted, could eventually clash.
- Short-circuiting the trustworthiness of providing cryptographic proof of ID (e.g., visual presentation of the phone screen to a verifier) could undermine the initial trust of mDL and delay roll out or acceptance of the full mDL Ecosystem.

Within a federated digital environment, new DL ecosystem capabilities are required to support jumpstarting the ecosystem economic model and address the elements of uncertainty. Points for consideration include:

- The need for an organizational structure enabling coordination and cooperation among participating issuers and relying parties, to create common or compatible mDL issuance policy across states
- Collaboration with certification bodies and testing organizations to:
  - Identify best policies and practices appropriate to common mDL trust
  - Ensure proper products are available for consumption and are consumed correctly, including product and issuer certifications
  - Ensure definition of necessary expertise to do certifications competently
  - Develop the value proposition and economic model for secure operation and trust of mDLs
- Recognition of a certification body(ies) with the delegated responsibility to certify mDL Issuers to be part of a larger trust framework
- Definition of the necessary enabling and uniform legislation and/or regulation
- Clarification of the value proposition and business cases for relying parties to accept mDLs both within and across jurisdictions and for Issuers to facilitate that acceptance
- Education on the value of mDL federation supporting Issuer and relying party participation

Within 2020, the Secure Technology Alliance, Alliance chapters, and the Alliance mDL program participants look forward to supporting and participating in efforts as appropriate to support progressing this critical issue.

6.12 New Market Opportunities

Adoption of mDLs creates new market opportunities, including opportunities for application developers and opportunities to leverage the mDL for product and service delivery.

> ***In the future…***
> mDL Holders could choose to authorize a trusted third party to link additional attributes to their mDL. For example, an employer could link an individual's employment status to support physical access to closed facilities.

Application developers could leverage mDLs for business transactions and interactions such as a peer-to-peer local data exchange between two mDL Holders. For example, two drivers involved in a fender-bender could select and exchange the minimum amount of required personal data securely (including insurance coverage information). mDL solutions could facilitate this exchange while protecting Holder privacy, even perhaps supporting receipt by the reciprocal insurance companies of information about the two drivers that the

two mDL Holders do not receive. Another peer-to-peer use case might be to verify age of consent between two mDL Holders.

7 Conclusions

The Secure Technology Alliance Identity Council developed this white paper to provide an educational primer on mDLs being implemented in the United States that follow the ISO 18013-5 international standard (that is currently in draft form). Having a standards-based mobile form of digital identity that offers the same trust as a state-issued physical driver's license brings greater utility, convenience, and security benefits for Holders while managing their daily lives. mDLs can benefit a variety of relying parties by providing a proven mobile ID that can strongly authenticate identities and offering the potential for more efficient identity transactions. The mDL market is developing rapidly, with states in varying stages of implementation.

As discussed throughout this white paper, the mDL ecosystem must incorporate certain core features:

- The data on the mDL must be provided by the Issuer and reflect the information that the Issuer collects and validates (verifies) when proofing the Holder's identity.
- The data must be secure. Every element of the system must include safeguards to protect the data from unauthorized access.
- Holder privacy is paramount. The Holder must decide whether to have an mDL and be able to maintain full control over whether and what data to share. Informed consent is valuable to both parties. The Verifier can choose not to proceed with the transaction if the necessary data is not provided.
- A trust framework is needed to protect all parties and ensure common policy and mechanisms.
- Verifiers must be able to validate that the mDL data is authentic, accurate, and has not been altered by unauthorized parties.

Implementing the ecosystem changes that enable broad issuance, use and acceptance of mDLs requires collaboration among all industry stakeholders to address implementation questions and challenges. The Secure Technology Alliance mobile driver's license initiative was launched to raise awareness, support development, accelerate adoption, and educate the U.S. market on the technology and applications for mDLs. Alliance efforts are focusing on:

- Providing resources to educate U.S. relying parties and other stakeholders on the rollout of the technology and the key uses for mDLs.
- Advocating for adoption of the ISO 18013-5 standard to ensure cross-jurisdiction interoperability and secure acceptance of mobile IDs.
- Providing guidance on the security and privacy of mDLs and the methods deployed for authentication.
- Facilitating discussions among industry stakeholders of implementation opportunities and challenges for broader adoption.

The Alliance initiative includes participation from AAMVA, driver's license technology providers, mobile technology providers, security providers, testing organizations, certification bodies, and relying parties including retailers, financial institutions, car rental community, aviation community, first responder community, healthcare organizations, and Federal, state and local government agencies. Through this collaborative initiative, the Alliance hopes to accelerate adoption of mDLs by businesses and services providers who rely on customers having trusted forms of identification.

8 Publication Acknowledgements

This white paper was developed by the Secure Technology Alliance Identity Council to: provide an overview of ISO/IEC 18013-5-compliant mDLs and the ecosystem needed to support their issuance and acceptance; outline example use cases; and highlight key challenges to address to support a robust mDL ecosystem.

Publication of this document by the Secure Technology Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Secure Technology Alliance wishes to thank Council members and guests for their contributions. Participants involved in the development and review of this white paper included: Aetna, a CVS Health Company; American Association of Motor Vehicle Administrators (AAMVA); Burns Engineering; CPI Card Group; Exponent, Inc.; Georgia Department of Driver Services (DDS); Gemalto; GET Group NA; HID Global; ID Technology Partners; IDEMIA; IDentity Check; Intercede; Kantara Initiative; Maryland DOT; Mastercard; NextgenID; NIST; SAFE Identity; SHAZAM; Thales; Underwriters Laboratories (UL); U.S. Department of Defense (DoD); Visa; XTec, Inc.

The Secure Technology Alliance thanks **David Kelts**, GET Group NA, **Geoff Slagle**, AAMVA, and **Suraj Sudhakaran**, Gemalto, who wrote the initial version; **Ted Sobel**, **Christopher Williams**, Exponent, **Tom Lockwood**, NextgenID, **Mark Dale**, XTec, Inc**., Kyle Neuman**, SAFE Identity, **Jerrin Thomas**, UL, **Colin Wallis**, Kantara Initiative, and **David Kelts**, GET Group NA, who drafted additional content as this white paper expanded to include relying parties; and the Council members who participated in the review of the document, including:

- **Andreas Aabye**, VIsa
- **Negash Assefa**, Maryland DOT
- **John Atkinson**, IDEMIA
- **Alan Bachman**, Aetna,
- **Abbie Barbir**, Aetna
- **Eric Berg**, ID Technology Partners
- **Ken Dagg**, Kantara Initiative
- **Mark Dale**, XTec, Inc.
- **Phil Davidson**, CPI Card Group
- **Robin Fong**, IDentity Check
- **Scott Green**, SHAZAM
- **Brandon Gutierrez**
- **Paul Hirons**, Intercede
- **Tracy Hulver**, IDEMIA
- **Brandon Iske**, DoD
- **Jordan Kaplan**, UL
- **David Kelts**, GET Group NA
- **Tom Lockwood**, NextgenID
- **Angelique Mcclendon**, Georgia DDS
- **Cathy Medich**, Secure Technology Alliance
- **Ketan Mehta**, NIST
- **Jean-Baptiste Milan**, HID Global
- **Manish Nathwani**, SHAZAM
- **Michel Nerrant**, HID Global
- **Kyle Neuman**, SAFE Identity
- **Micheal Pettibone**, Mastercard
- **Devon Rohrer**, Secure Technology Alliance
- **Adam Shane**, Burns Engineering
- **Gerry Smith**, ID Technology Partners
- **Ted Sobel**
- **Suraj Sudhakaran**, Thales
- **Jerrin Thomas**, UL
- **Colin Wallis**, Kantara Initiative
- **Christopher Williams**, Exponent
- **Steve Yonkers**
- **Rob Zivney**, ID Technology Partners

Trademark Notice

About the Secure Technology Alliance Identity Council

The Identity Council provides leadership and coordination and serves as focal point for Alliance's identity and identity related efforts leveraging embedded chip technology and privacy- and security-enhancing software. Directly and in partnership with other Secure Technology Alliance councils, the Identity Council supports a spectrum of physical and logical use cases and applications, form factors, attributes, and authentication and authorization methods. The Council serves to influence standards and best practices, serve as an educational resource, and provide a voice in public policy influencing adoption, implementation, and use.

Key areas of focus for the Identity Council are: identity trust frameworks; digital identity; strong authentication; authorization; and biometrics. Additional information on the Identity Council can be found at: https://www.securetechalliance.org/activities-councils-identity/.

9 Appendix A: Applicable Standards and Frameworks

This appendix lists standards and frameworks applicable to the design, development, implementation, and deployment of a mobile driver's license.

- "Mobile Driver's License Functional Needs Whitepaper" from AAMVA: https://www.aamva.org/mDLWhitepaper_0_7/
- International Standards Organization (ISO) 18013
  - Part 1 (Data), https://www.iso.org/standard/63798.html
  - Part 2 (Machine Readable), https://www.iso.org/standard/70486.html
  - Part 3 (Access & Authentication), https://www.iso.org/standard/72366.html
  - Part 4 (Testing), https://www.iso.org/standard/74961.html
  - Part 5 for Mobile Driver License is under development
    - Day One: Transmission standards, trust lists, and online token and request
- Digital identity-related trust frameworks from industry and government, such as:
  - U.S. Government Federal PKI, https://www.idmanagement.gov/topics/fpki/. The Federal Public Key Infrastructure (FPKI) provides the government with a trust framework and infrastructure to administer digital certificates and public-private key pairs.
  - Kantara Initiative, https://kantarainitiative.org/trustoperations/. Kantara's Assurance Framework and related programs accredit assessors and approve services operated by credential service providers at assurance levels applicable to any trust framework or scheme rules globally, based on service assessment criteria developed, maintained and managed by Kantara.
  - SAFE Identity, https://makeidentitysafe.com/trustFramework.html. The SAFE Identity Trust Framework facilitates trust by providing a combination of policies and services for digital signatures, authentication, federation and encryption that are implemented by certified product and service providers.
  - Transglobal Secure Collaboration Program (TSCP), https://www.tscp.org/tscp-pki-bridge-service/. The TSCP Public Key Infrastructure (PKI) Bridge Service operates under the authority of the TSCP Bridge Certification Authority (TBCA) to facilitate interoperability among PKI domains.
  - tScheme, https://www.tscheme.org/schemes-and-profiles. A scheme is a definition of a trust framework, rather than the trust service itself. So a scheme will set out the parameters and standards that are required of a trust service. Trust service providers (TSPs) use schemes to create and administer trust services.
  - Trusted Digital Identity Framework (TDIF, https://www.dta.gov.au/our-projects/digital-identity/join-identity-federation/accreditation-and-onboarding/trusted-digital-identity-framework) (last revised 2019), Digital Transformation Agency (DTA), Australia. The Trusted Digital Identity Framework (TDIF) is a set of rules and standards that accredited members of the digital identity federation must follow.
  - Draft Pan-Canadian Trust Framework (PCTF, https://diacc.ca/pan-canadian-trust-framework/), Digital ID and Authentication Council of Canada (DIACC),the Identity Management Subcommittee (IMSC) of the Joint Councils, and others (Canada). The PCTF is intended to standardize trusted digital representations (i.e., identities, attributes, relationships) of people, organizations, and things in Canada.

- Draft Digital Identity Trust Framework (DITF, https://www.digital.govt.nz/standards-and-guidance/identity/digital-identity/digital-identity-transition-programme/digital-identity-trust-framework/) (New Zealand)

- Identity assurance standards from industry and government, such as
  - NIST SP 800-63-3 Digital Identity Guidelines, last revised 2017 (USA), https://pages.nist.gov/800-63-3/
  - Good Practice Guide (GPG) 45 (last revised 2019), https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual; Government Digital Service (GDS) and others (UK)
  - Electronic Identification, Authentication and Trust Services (eIDAS) Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market (last revised 2016), https://ec.europa.eu/digital-single-market/en/trust-services-and-eid (EU)
  - ISO/IEC 29115 Entity Authentication Assurance Framework: 2013 (ISO), https://www.iso.org/standard/45138.html
  - ISO/IEC TS 29003 Identity Proofing: 2018 (ISO), https://www.iso.org/standard/62290.html
- Authentication standards from industry and government, such as
  - OIDC 1.0[1] (OIDC), 2014 (Open ID Foundation), https://openid.net/specs/openid-connect-core-1_0.html
  - Draft iGov Profile of OIDC – in progress from the iGov Working Group of Open ID Foundation, https://openid.net/specs/openid-igov-openid-connect-1_0-ID1.html
  - JSON Web Tokens (JWT) Claims Registry RFC7519; (last revised 2019) (Internet Engineering Task Force), https://tools.ietf.org/html/rfc7519
  - Client to Authenticator Protocol (CTAP) 2018 W3C and FIDO Alliance, https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-client-to-authenticator-protocol-v2.0-id-20180227.html
- Privacy standards from industry and government, such as
  - ISO/IEC 29100 Privacy Framework 2011 (ISO), https://www.iso.org/standard/45123.html
  - ISO/IEC DIS 29184 Online privacy notices and consent (ISO), https://www.iso.org/standard/70331.html
  - Consent Receipt specification v1.1 2018 (Kantara Initiative), https://kantarainitiative.org/file-downloads/consent-receipt-specification-v1-1-0/
  - General Data Protection Regulation 2016/679 (GDPR) 2016 (European Commission), https://eur-lex.europa.eu/eli/reg/2016/679/oj

10 Appendix B: ISO/IEC 18013-5 Data Elements

The following table lists the data elements available in draft ISO/IEC standard 18013-5 as of the publication of this white paper. The table shows whether the data is mandatory or optional. Please refer to the most current published standard for up-to-date information.

Table 5. Data Elements in Draft ISO/IEC Standard 18013-5 Section 7.4.1

Data Element	Name	Definition	Presence Mandatory (M), Recommended (R) or Optional (O)
family_name	Family name	Last name, surname, or primary identifier of the license holder	M
given_name	Given names	First name(s), other name(s), or secondary identifier of the license holder	M
birth_date	Date of birth	Day, month, year on which the license holder was born. If unknown, approximate date of birth	M
issue_date	Date of Issue	Date license document was issued	M
expiry_date	Date of Expiry	Date license document expires	M
issuing_country	Issuing country	Country code as alpha 2 code, defined in ISO 3166-1, of country which issued the mDL or within which the licensing authority is located	M
issuing_authority	Issuing authority	Name of licensing authority, or issuing country if separate licensing authorities have not been authorized. See 7.4.3.	M
document_number	Licence number	The number assigned or calculated by the issuing authority	M
administrative_number	Administrative number	An audit control number assigned by the licensing authority	O
driving_privileges	Categories of vehicles/ restrictions/ conditions	Driving privileges granted to the license holder. It consists of category issue date, expiry date, restriction/condition sign code, restriction/condition sign and	M

Data Element	Name	Definition	Presence Mandatory (M), Recommended (R) or Optional (O)
		restriction/condition value. See ISO/IEC 18013-5 Section 7.4.4.	
un_distinguishing_sign	UN distinguishing sign	Distinguishing sign of the issuing country according to 18013-1 annex F. This field is added for purposes of the UN conventions on driving licenses	R
gender	Gender	License holder's gender: M for male, F for female, X for not specified	O
height	Height (cm) a	License holder's height in centimeters	O
weight	Weight (kg) a	License holder's weight in kilograms	O
eye_color	Eye colour	License holder's eye color: blue, brown, black, hazel, green, grey, pink, dichromatic	O
hair_color	Hair colour	License holder's hair color: brown, black, blonde, grey, red, auburn, sandy, white, bald	O
birth_place	Place of birth	Country and municipality or state/province where the license holder was born	O
resident_address	Permanent place of residence	The place where the license holder resides and/or may be contacted (street/house number, municipality etc.)	O
portrait	Portrait of mDL Holder	A reproduction of the license holder's portrait. See ISO/IEC 18013-5 Section 7.4.2.	M
portrait_capture_date	Portrait image timestamp	Date when picture was taken	O
age_in_years	Age attestation: How old are you (in years)?	The age of the mDL Holder	O
age_birth_year	Age attestation: In what year were you	The year when the mDL Holder was born	O

Data Element	Name	Definition	Presence Mandatory (M), Recommended (R) or Optional (O)
	born?		
age_over_NN	Age attestation: Nearest "true" attestation above request	See ISO/IEC 18013-5 Section 7.4.5 for definition	O
issuing_jurisdiction	Issuing jurisdiction	Country subdivision code as defined in clause 8, ISO 3166-2. The first part of the code shall be the same as the value for issuing country. This element is intended to be used in cases where the issuing jurisdiction is different than the issuing authority.	O
nationality	Nationality	Nationality of the mDL Holder as two letter country code (alpha-2 code) defined in ISO 3166-1	O
resident_city	Resident city	The city where the mDL Holder lives	O
resident_state	Resident state/province/district	The state/province/district where the mDL Holder lives	O
resident_postal_code	Resident postal code	The postal code of the mDL Holder	O
biometric_template_xx	Biometric template XX	See ISO/IEC 18013-5 Section 7.4.6 for definition	O
name_national_character	Full name of holder in full UTF-8 character set	The full name of the mDL Holder in his/her national characters	O
signature_usual_mark	Signature / usual mark	Image of the signature or usual mark of the mDL holder	O
online_token_xxxx	Online token	See ISO/IEC 18013-5 Section 7.4.8 for definition	O
online_url_xxxx	Online URL	See ISO/IEC 18013-5 Section 7.4.8 for definition	O

11 Appendix C: Use Cases

This section describes some of the major use cases for an mDL or state government issued ID card (Figure 9). The mDL can revolutionize workflows by providing multiple interaction modes (see Section 2.3), untraceable privacy-protecting identifiers for Holders, and quick access to government-backed attributes for Verifiers. mDLs can support brand new workflows at any level of security.

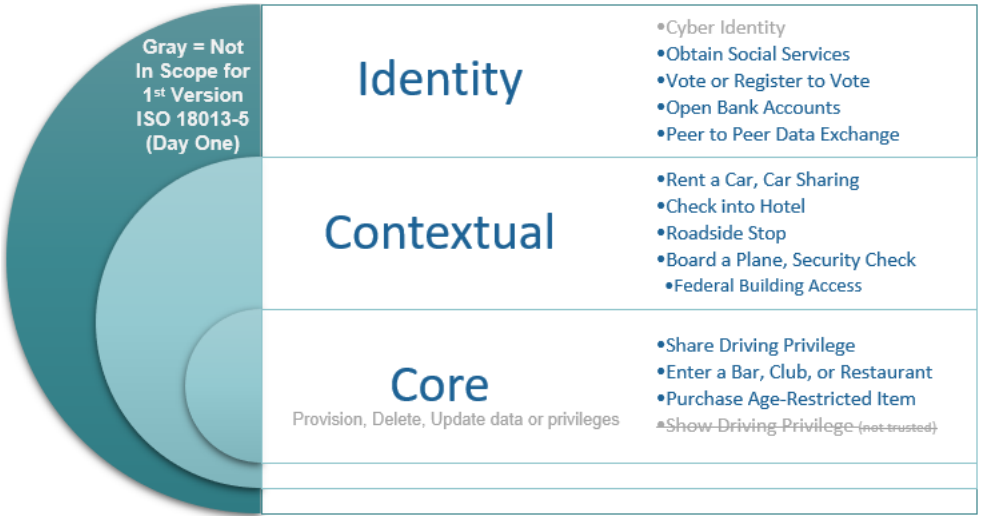

Figure 9: Use Cases for a Mobile Driver's License

In the most basic use cases for mDLs, a human attendant performs identity verification in a face-to-face transaction – that is, an attendant visually compares the mDL Holder's face against a portrait image obtained from the mDL. These are attended, in-person use cases, that involve nearby transmission or lookup of valid mDL attributes for the Holder.

Attended use cases are in scope for Day One ISO/IEC 18013-5. Several items listed above in gray text, are not in scope (Cyber ID), are not technically supportable (showing a card on screen), or will be standardized in another ISO standard (provisioning, privilege management).

For Day Two unattended use cases, there is no human attendant verifying identity. Identity verification happens in one of two ways:

- Holder authentication requests. The Holder's mDL device is challenged by the Issuer or by the Verifier to authenticate the Holder.
- Machine-enabled identity verification. Equipment at the Verifier location compares the identity of the mDL Holder to data received from the mDL and performs the identity verification.

In distance use cases, the Verifier and the mDL are separated by a distance that exceeds line of sight. Distance use cases are unattended transactions. Because the transmission cannot begin with a tap or snapping a QR code, additional security considerations are needed to protect the mDL Holder from unauthorized access to the data on the mDL. Distance use cases operate the same way as over-the-internet online transactions.

Internet transactions – Cyber Identity – support login to web sites and linking the mDL to a Holder's account at a web-based or app-based service provider, such as a car rental app.

The next sections provide high level overviews of 11 different uses for mDLs. The descriptions provide examples of how an mDL might be used by different relying parties and are intended to stimulate discussion of these and other uses. Some use cases require Day Two ISO/IEC 18013-5 functionality; Section 2 includes additional information on Day One and Day Two functionality.

Each use case includes a table. The table includes the typical use with variants, provides an example of the interaction mode used (how the Holder and mDL-provisioned mobile device interact with the Verifier) that incorporates definitions from Section 2.3, and describes the role of the Verifier, privacy considerations, and the sensitivity of the transaction. Sensitivity is categorized as follows:

- *None*, which requires no certainty in identity. There is no need to identify the visitor to the service provider.
- *Anonymous*, which requires little certainty in identity. The verification method would use a unique identifier to access an account or service. Little or no PII is required.
- *Low*, which requires some certainty in identity. Identity verification and document authentication are fulfilled by an unassisted check. Compliance requires an official, legal document. The transaction may require and record some PII.
- *Substantial*, which requires a high certainty in identity. Often additional authentication tools (e.g., lights, scanners) are used, and biometric comparison may be performed.
- *High*, which requires very high certainty in identity. Equipment is necessary to improve upon human accuracy for identity verification and document authentication. Accurate and recent identity attributes are required to perform the transaction.

The table also includes examples of the data needed by the Verifier for the use case, including both data from the mDL and other data that the Verifier requires that is not provided by the mDL. Note that some mDL data is mandatory and some is optional; optional data may not be available from all Issuers.

11.1 Confirming, Sharing, or Transmitting Driving Privileges

The primary purpose of a DL is to convey that the licensee has earned and retained the privilege of being allowed to drive a certain type of vehicle. This is important when renting a vehicle (covered in Use Case 11.5) and at other times when drivers must represent their current privileges, such as to DMV personnel or police officers.

Use Case	Context	Example Interaction Mode	Verifier Role	Sensitivity/ Risk	Examples of Data Needed by Verifier	Privacy
Typical	Testing, upgrades at the DMV	Tap & Go	DMV	Substantial	Facial image, DL number (DLN), issuance, driving privileges. Some Verifiers may also require current driver status to ensure privileges are still in effect.	NA

Use Case	Context	Example Interaction Mode	Verifier Role	Sensitivity/ Risk	Examples of Data Needed by Verifier	Privacy
Variant	Roadside stop (see Section 11.2)	Scan & Request	Law enforcement	Substantial	Full data set	Holder does not need to give the officer their device. mDL Holder needs assurance the officer is legitimate.
Variant	Online knowledge testing at DMV.gov	Login	DMV	Substantial	Facial image, DLN, issuance, driving privileges, Holder authentication	NA

11.2 Stopping at the Roadside for Law Enforcement

Being pulled over by law enforcement is the first use case mentioned by potential Holders and Issuers alike. During a roadside stop, the law enforcement officer conducting the road stop typically tries to identify the driver of the vehicle. The obvious document to use for this purpose is a DL. The DL number is a key into enforcement systems that the officer can use to obtain additional information.

Use of an mDL would be very convenient for the Holders while also increasing safety for the law enforcement officer, since it allows the officer to query the mDL from a distance. Secure, fresh, and accurate information about the driver of a vehicle, retrieved early during the event, can improve response time and officer safety. Holders must have their privacy concerns addressed and know that a true law enforcement official has requested their identity information. A roadside stop does not provide the same contextual clues that border crossings provide to passport holders, and impersonation of police officers has happened.

	Context	Example Interaction Mode	Verifier Role	Sensitivity/Risk	Examples of Data Needed by Verifier	Privacy
Variant	Distance – vehicle to vehicle	Interrupting request (Day Two capability)	Law enforcement	Substantial	DL number Full name Facial image	mDL Holder must know that the officer is official and on duty.

11.3 Entering a Bar, Club, or Restaurant

Many consumers do not want to go to a club with a full wallet or purse, but they will typically take their phones. The physical conditions for this use case, however, are the most challenging for Holder authentication and authenticity – darkness, long lines, makeup, and the ever-present undercurrent of a desire to spoof the bouncer in order to gain entry. After meeting security and accuracy requirements to gain entry, the actual identity requirements are low (e.g., the Holder meets age requirements).

A variant of this use case is entering a casino, where additional legal requirements may require consumers to divulge their names or where consumers may volunteer their names to be checked against no-gamble lists.

	Context	Example Interaction Mode	Verifier Role	Sensitivity/Risk	Examples of Data Needed by Verifier	Privacy
Typical	Bouncer outside club entrance	Tap & Hold	Venue	Low	Age > Policy Facial image	Data minimization and anti-tracking are essential.
Variant	Cashier Counter	Tap & Consent	Casino	Low	+ Full name	Opt-in for loyalty programs only

11.4 Purchasing Age-Restricted Items

In the U.S., the purchase of certain commodities, such as alcohol and tobacco products, is generally restricted to persons above a certain age. State agencies often administer state regulations and monitor the purchase of age-restricted items across the jurisdiction. Establishments complying with state regulations typically verify age using the DL or an ID card. An mDL could be an alternate convenient mechanism for such establishments to provide secure verification of age-related attributes and identity.

	Context	Example Interaction Mode	Verifier Role	Sensitivity/Risk	Examples of Data Needed by Verifier	Privacy
Typical	Liquor store and convenience store	Tap & Go	Trained clerk	Low	Age > Policy Facial image	Should not report usage to any central service
Variant	Online retailer	Login (Day Two capability)	Web payment portal	Substantial	Age > Policy Full name Address Facial image for delivery *Additional non-mDL data: Signature*	

11.5 Renting or Sharing Cars

When an mDL Holder is renting an automobile, the mDL can identify the renter, provide contact information, and confirm driving privileges. In higher risk rentals, an mDL could perhaps even obtain up-to-the-minute driving privileges. The mDL can be presented by the mDL Holder at a rental counter or vehicle exit gate.

Many renters are members of loyalty programs, and their DL number is on file; however, having the number on file does not prevent someone with a suspended license from renting a vehicle. In addition, exit gate checks are high friction for the renter and high cost for the rental company.

The rental car experience is one where reimagining the Holder's experience from start to finish could make for an optimal experience for Holders. Smart rental companies will reimagine the whole process from booking the vehicle through arriving, walking past the rental counter, having the reserved vehicle unlock automatically when it detects the proper mDL, and allowing the mDL Holder, after identity verification, to drive off the lot without stopping.

Car-sharing programs have become popular in urban areas. Program members pick up a car from a nearby location to travel to a particular destination. Some areas and some car-sharing programs offer high value automobiles, so the car sharing company may consider their transaction risk to be high.

	Context	Example Interaction Mode	Verifier Role	Sensitivity/Risk	Examples of Data Needed by Verifier	Privacy
Typical	Rental counter	Tap & Request	Agent of car rental company	Substantial	Age > Policy Driving privileges Contact information Facial image	Holder expects that they would not be monitored or tracked by rental agency.
Variant	Automated exit gate	Tap & Go (Day Two capability)	Rental car company (automated)	Substantial	As above *Additional non-mDL data: Updated status may be required*	
Variant	Car sharing, often in parking lots	Tap & Request (Check-in as Day Two capability)	The vehicle itself, unattended	Substantial	As above *Additional non-mDL data: Known person ID of car-sharing program member*	

11.6 Checking into a Hotel

It is common to have to confirm identity and provide contact information upon checking into a hotel. While many hotels perform this function through their loyalty programs and apps, they do so because the customer information is on file and the identifying number is their loyalty number.

However, people do check into new hotels or new chains, and in many locations, document checks are required by law. Photocopying identity documents, then leaving the copies in unsecured piles, has unfortunately become commonplace. This scenario is one where using a mobile identity can improve consumer privacy and the security of personal information. The DL issuing authority and number are not data elements that are required to rent a hotel room, so with use of an mDL, the data exchange can be minimized to exclude non-essential tracking information.

	Context	Example Interaction Mode	Verifier Role	Sensitivity/Risk	Examples of Data Needed by Verifier	Privacy
Typical	Hotel lobby	Tap & Consent	Front desk clerk	Substantial	Age > Policy Full name Identity verification Address	Many hotels photocopy identity documents, ignoring the risk

	Context	Example Interaction Mode	Verifier Role	Sensitivity/Risk	Examples of Data Needed by Verifier	Privacy
					Facial image	of record storage. An mDL could improve this.
Variant	Digital key provisioning	Tap & Consent	Hotel web or app services	Low	As above	Opt-In for loyalty programs only

11.7 Accessing Secure Buildings, Federal Buildings

Most federal agencies that require identification for access accept a state-issued DL or identification card for that purpose. In the United States, any federal facility that requires ID for access and allows state-issued DL and ID cards to be used for identity proofing will require those DLs and IDs to be REAL ID-compliant beginning on October 1, 2020.

	Context	Example Interaction Mode	Verifier Role	Sensitivity/Risk	Examples of Data Needed by Verifier	Privacy
Typical	Reception desk	Tap & Go	Agency clerk	Substantial	Full name REAL ID status[39] Facial image *Additional non-mDL data: Trackable contact information in case of an event; agency being visited*	
Variant	Pre-registration and escorted visit	Tap & Go	Agency employee Agency clerk	Low (agency employee assumes identity verification risk)	Same as above	
Variant	Online pre-registration	Open ID	Online web site	Low (web site assumes identity verification risk)	Same as above, DL number and state	

An mDL-based identity-proofing process would increase security while also improving audit logging and visitor verification. It is possible that distance exchange of mDL information between an agency employee and a visitor, or an agency desk clerk and a visitor, could streamline the process to allow an mDL holder to receive access privileges to select secure/federal buildings and other access points. That is, a Holder could present their mDL during an online pre-registration process managed by a web site

[39] https://www.aamva.org/mDL-Resources/ contains the guidance that defines the REAL_ID flag for U.S. jurisdictions.

that collects mDL information and verifies the mDL, or the visitor could present their mDL in person at a security office within a building where targeted access is desired.

When a meeting is scheduled, an agency employee could provide the agency's building physical access control system (PACS) with a visiting holder's email address and the time of the scheduled visit. The system could also trigger an email reminder for the Holder to register in advance by presenting their mDL through a distance exchange to ensure identity verification. Upon arrival, the Holder could be granted a temporary visitor access token (e.g., temporary visitor smart card such as a PIV, PIV-I or CIV card) for access to specific areas, similar to the way hotel keys are managed in digital systems. Or, the visitor could present the mDL itself to the PACS for access without needing an alternative access token (see Section 11.11).

11.8 Going through Airport Security, TSA

In the United States, travelers must present an acceptable form of Identification to be able to proceed through the Transportation Security Administration (TSA) checkpoint to the gate. DLs are the most common form of identification used for this purpose. Beginning on October 1, 2020, every air traveler must present a REAL ID-compliant DL, valid passport, U.S. military ID, or other form of acceptable identification[40] to fly within the United States. Individuals who are unable to verify their identity with an acceptable document will not be permitted to pass the TSA checkpoint and will not be allowed to fly. TSA is currently reviewing the mDL and has not issued a policy about acceptability.

It is important to note that, unlike the roadside stop use case, the context and nearby transmit mechanisms typically will protect mDL Holders from TSA impersonation, but consideration for the Holder must be built into the design of any future security checkpoint process.

	Context	Example Interaction Mode	Verifier Role	Sensitivity/Risk	Examples of Data Needed by Verifier	Privacy
Typical	Airport security	Tap & Go	Credential authentication technology system and TSA officer	High	Name, date of birth, gender, expiration date, biometric picture	mDL Holder cares that TSA touchpoint is official and that travel is not being tracked.
Variant	Airline check-in counter	Tap & Hold or Tap & Go	Airline agent	High	Full name matched to boarding pass *Additional non-mDL data: TSA Precheck number included*	
Variant	Airport security for international flight	Tap & Hold or Tap & Go	Trained TSA or CBP security personnel	High	Same as domestic plus *potential additional non-mDL data: passport number and*	

[40] For more information about acceptable forms of ID, see https://www.tsa.gov/travel/security-screening/identification.

	Context	Example Interaction Mode	Verifier Role	Sensitivity/Risk	Examples of Data Needed by Verifier	Privacy
					data	
Variant	Automated bag check	Tap & Go or Tap & Hold	Airline agent	Substantial	Full name matched to boarding pass *Additional non-mDL data: boarding pass information such as destination, airline flight number*	

11.9 Receiving State DMV or Social Services

Many state agencies accept the DL as proof of identity when residents apply for social services or register vehicle titles. An mDL can identify and authenticate a Holder for any online services provided by a DMV or other state agency. The mDL app on the smart device can take advantage of multiple Holder authentication mechanisms to provide a higher level of assurance for these transactions, enabling them to be moved to additional delivery channels, such as kiosks or a web site.

Many states use DLs or ID cards to identify applicants to benefit programs but cannot require an identity card to approve services. This creates the opportunity for fast lane access for benefit recipients who choose to use their mobile identity to apply for and manage state benefits. Fast lanes are suitable for in-person transactions, and equally important is priority processing for back-office transactions or online management of benefits by the recipient. The cost savings to the state agencies of reducing in-office traffic can be considerable, and the delivery of services to those who need them can be sped up.

	Context	Example Interaction Mode	Verifier Role	Sensitivity/Risk	Examples of Data Needed by Verifier	Privacy
Typical	Social services office	Tap & Request	Clerk representing agency	Low	State residency Facial image *Additional non-mDL data: Known person identifier; family information*	Cross-agency knowledge of benefits should be avoided, even within the same state.
Variant	Social services website	Login (Day Two capability)	Agency	Substantial	State residency Facial image *Additional non-mDL data: Known person identifier; family information*	As above
Variant	Vehicle title website	Login (Day Two capability)	Vehicle Registry	Substantial	Full name, address, facial image *Additional non-mDL data: Issuance information*	

11.10 Opening Bank Accounts

Banks, brokerages, and financial institutions that open new customer accounts must meet their internal identity policies and worldwide Know Your Customer (KYC)/Anti-Money Laundering (AML) regulations. At a minimum, the applicant's identity must be verified against an unexpired government-issued ID, and the identifying numbers from that ID document must be retained by the bank, regardless of whether the account is opened.

Bank employees are very often trained in both fraudulent document inspection and identity verification. As banks search for technology to perform these two services, the accuracy requirements may be selective. The mDL provides the opportunity to fulfill both of these functions in a convenient mobile package that the bank can accept in person or online. Automating these functions may result in some banks selecting a high risk level for account opening or adjusting risk sensitivity based on external factors.

A few banks in some regions have a policy of photocopying ID documents and filing them. There is an inherent insecurity in allowing an ID card to be photocopied, and the mDL, even with its own privacy risks, can mitigate the risks of paper trails and unlocked file cabinets.

	Context	Example Interaction Mode	Verifier Role	Sensitivity/Risk	Examples of Data Needed by Verifier	Privacy
Typical	Bank branch	Tap & Consent	Financial institution	Substantial	Full name, DL number, unexpired, address or contact info, facial image	Must not compromise mDL Holder
Variant	Online banking	Login (Day Two capability)	Financial institution	High	Full name, DL number, unexpired, address or contact information, facial image *Additional non-mDL data: Lookup to AML lists*	Upon account opening, bank can store a persistent token to permit future login access with mDL as authentic-Ation.

11.11 Entering Secure Areas, Access Control

An mDL, and the mobile device on which it resides, can potentially perform as a cryptographic token for physical access to buildings, rooms, parking garages, and other secure areas, similar to how smart cards and RFID tokens are currently used. Access to secure areas is managed by physical access control systems (PACS), which consist of readers deployed at the secure-area entry points with localized actuators that unlatch doors or open gates. The readers and actuators are controlled by a centralized computer/server that hosts the PACS software and database. The database contains access control lists (ACLs); usernames, identifiers, and user privileges; and token information (e.g., an mDL or portions thereof), all of which are entered into the PACS database during a pre-registration or enrollment process.

During access to entry points, the mDL mobile device is held up to an entry-point mDL reader; a communications session is established, and mDL identifiers read from the mDL are used to look up the identifier in an ACL to determine whether the mDL holder has previously been granted access to the

entry point. Authentication of the mDL security object is performed to validate the provisioned mDL on the device, and an additional authentication factor may be required, such as entering a PIN on a reader keypad. In addition, PACS systems may periodically download a Master List of mDL Issuer root certificates, so that mDLs can be verified against a known list of official mDL Issuer certification authorities.

	Context	Example Interaction Mode	Verifier Role	Sensitivity/Risk	Examples of Data Needed by Verifier	Privacy
Typical	Secure area entry; e.g., buildings, rooms and parking garages	Tap & Hold	Unattended (reader only) Attended (reader and security personnel)	Substantial or High (off-hours)	Full name mDL unique identifier (e.g., DL number and state)	Identifying data at enrollment time is appropriate. Speed is critical at access time.
Variant	Secure area entry; e.g., buildings, rooms and parking garages	Tap & Go	Unattended (reader only) Attended (reader and security personnel)	Substantial or High (off-hours)	Full name mDL unique identifier (e.g., DL number and state)	Identifying data at enrollment time is appropriate. Speed is critical at access time.

12 Appendix D: Mobile Security Object

In addition to the data elements detailed in Appendix A, ISO/IEC standard 18013-5 defines a Mobile Security Object (MSO) for the purpose of verifying the integrity and authenticity of mDL data as provided to verifying parties by the Holder's mobile device. The MSO contains digest values for each data element contained within the mDL, along with the mDL device key and validity information. At the time of issuance or update, the Issuing Authority (IA) cryptographically signs the entire MSO data structure with the IA private key (the IA public key is distributed as part of the mDL Master Lists). This information set allows any verifier to check the validity of the mDL data passed during the transaction and verify that it has been signed by a trusted issuer though the validation of the IA signature.

The concise data definition language (CDDL) data structure of the MSO included in the draft standard as of the publication date of this white paper is below. Please refer to the most current published standard for up-to-date information.

```
MobileSecurityObject = {
   "digestAlgorithm" : tstr,
   "valueDigests" : ValueDigests,            ; Array of digests of all data elements,
                                               digest value is computed for each data
                                               element which includes a random
integer
                                               of at least 16 bytes to protect
                                               confidentiality of non-released data
                                               elements during mDL transaction
   "deviceKey" : COSE_Key,                   ; Device key used for non-clonability
                                               and mDL authentication
   "docType" : tstr,
   "validityInfo" : ValidityInfo
}

ValueDigests = {
   "nameSpaces" : NameSpaces
}

NameSpaces = {
   + NameSpace => DigestIDs
}

DigestIDs = {
    + DigestID => Digest                     ; Digests are salted with random
}

ValidityInfo = {
   "signed" : tdate,
   "validUntil : tdate,                      ; Date when MSO is no longer valid,
                                               shall not be a value beyond mDL
                                               expiration date
   "validFrom" : tdate,                      ; Date from when MSO validity begins,
                                               Shall not be a value before mDL issue
                                               date
   ? "expectedUpdate" : tdate                ; Next expected update of MSO
}

NameSpace = tstr                             ; NameSpace as used in IssuerSigned
DigestID = uint                              ; DigestID as used in IssuerSignedItem
Digest = bstr                                ; digest(IssuerSignedItem)
```