A US PAYMENTS FORUM WHITE PAPER

The Role of Mobile IDs in Payments

Version 1.0

Publication Date: July 2024

U.S. Payments Forum
544 Hillside Road
Redwood City, CA 94062

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum is a cross-industry body that brings stakeholders together on neutral ground to enable efficient, timely and effective implementation of emerging and existing payment technologies. This is achieved through education, guidance and alternative paths to adoption. The Forum is the only non-profit organization whose membership includes the whole payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on and have a voice in the future of the U.S. payments industry. The organization operates within the Secure Technology Alliance, an association that encompasses all aspects of secure digital technologies.

Table of Contents

Executive Summary

Digital identities refer to the electronic representation of personally identifying information that may be used to verify the identity of a person, encompassing a collection of information, attributes, and credentials that establish and verify a person's identity in online interactions and transactions. Mobile representations of government issued identification are referred to as mobile IDs or mIDs.

Mobile drivers' licenses, or mDLs, are a sub-category of mIDs that contain the same information as a physical driver's license and can be used to verify one's identity and driving eligibility in various situations, such as traffic stops, car rentals, or age-restricted purchases.

While the earlier implementations of mIDs were rather limited in functionality, there is a global effort for more advanced approaches that would address some of the limitations of the physical forms of government-issued IDs. The goal is to offer enhanced security, with strong cryptographic authentication of the mID, as well as interoperability and improvements in terms of privacy for the identity holder.

Mobile-based digital identity offers tremendous opportunities for combatting fraud and securing transactions, while offering the mID holder control over their personal data and the convenience of having their ID on their phone.

This white paper examines how government-issued mobile IDs, which include mDLs, can be leveraged in the payments ecosystem, both today and in the future as well as in-store and online, including examples of where digital identities and digital payment acceptance can potentially converge.

This paper also provides an overview of the acceptance of mID transactions compliant with the 2021 ISO/IEC 18013-5 standard, which defines the technical and functional requirements for mDLs and mDL readers and focuses on in-person use cases, and introduces the draft ISO/IEC 18013-7 standard, in which mDL identity verification could be leveraged in online commerce and open new possibilities for remote verification of mIDs in the payment industry.

1. Introduction

Digital identities refer to the electronic representation of personally identifying information that may be used to verify the identity of a person. Digital identities encompass a collection of information, attributes, and credentials that establish and verify a person's identity in online interactions and transactions. Digital identities are made up of a variety of different types of data, such as:

- Personal information, such as name, date of birth, and address
- Contact information, such as email address and phone number
- Account credentials, such as usernames and passwords
- Biometric information
- Online activity data, such as browsing history, purchase history, and social media activity.

Digital identities enable people to access various services and resources online. Digital identities are used in all aspects of life – from low-risk applications such as social networks, gaming, and shopping to critical applications such as banking, health care, or access to government benefits.

Digital identities have been evolving from a strictly centralized approach, which requires users to create credentials to each individual online service, to a combination of centralized and federated approach, in which major technology companies provide identification services to third parties. Whether centralized or federated, however, digital identities based on knowledge, attributes or even biometrics are not equivalent to the presentation of a government-issued ID.

With mobile phones now being ubiquitous, governments around the world have been working on the digitization onto mobile devices of government-issued IDs such as passports, drivers' licenses, and identification cards. In this white paper, we will refer to the mobile representations of government-issued identification as "mobile ID", or "mID".

While the earlier implementations of mIDs were rather limited in functionality, there is a global effort for more advanced approaches that would address some of the limitations of the physical forms of government-issued IDs. The goal is to offer enhanced security, with strong cryptographic authentication of the mID, as well as interoperability and improvements in terms of privacy for the identity holder.

There are multiple benefits to moving to mIDs. First, with strong cryptographic authentication of the mID, it is much more difficult to counterfeit IDs, and it lessens reliance on manual checks – there is no need to check the microprint and other analog features. Second, is the ability to identify mID holders remotely. As opposed to physical forms of government-issued identifications, which require in-person verification, mIDs have the potential to be verified in-person as well as remotely. Third, the digital nature of mIDs allow much more frequent updates – for example, when a person moves, that change of address could be updated near real-time on the mID, while the physical ID gets updated on expiry, which in some US jurisdictions is eight years[1], and provides the means for individuals to have more control over which identity attributes to share.

[1] South Carolina's driver's license is issued for eight years: "Driver's License," South Carolina DMV, https://scdmvonline.com/Driver-Services/Drivers-License

In the United States, several initiatives have worked to establish a secure, standardized framework for online authentication; the National Strategy for Trusted Identities (NSTIC)[2] and the Improving Digital Identity Act of 2023[3] are two examples.

A form of digital identity that is getting traction throughout the country is the mobile driver's license (mDL), for which a standard was published in 2021 (ISO/IEC 18013-5). This white paper examines how government-issued mobile IDs, which include mDLs, can be leveraged in the payments ecosystem, both today and in the future.

[2] "National Strategy for Trusted Identities in Cyberspace," The White House, April 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

[3] "S884 - Improving Digital Identity Act of 2023," U.S. Senate bill introduced March 21, 2023, https://www.congress.gov/bill/118th-congress/senate-bill/884/text

2. Mobile ID and Mobile Driver's License

2.1 Current state

An mID is a form of digital identity that allows identity holders to carry a highly secure, state-issued personal credential that resides on their smartphone and can be used as a valid form of ID that either complements or replaces their physical ID.

Mobile drivers' licenses, or mDLs, are a sub-category of mIDs that contain the same information as a physical driver's license, such as the holder's name, date of birth, photo, address, and driving privileges. An mDL can be used to verify one's identity and driving eligibility in various situations, such as traffic stops, car rentals, or age-restricted purchases.

In 2021, the International Organization for Standardization (ISO) published the ISO/IEC 18013-5 international standard, which defines the technical and functional requirements for mDLs and mDL readers. The standard aims to ensure interoperability, security, and privacy of mDLs across different jurisdictions and use cases. The standard covers aspects such as data structure, data elements, data protection, presentation modes, authentication methods, and conformance testing.

While the ISO/IEC 18013-5 standard focuses on attended (in-person) use cases only, in which parties are in close proximity during the verification, additional standards (e.g., ISO/IEC 18013-7[4]) are in preparation that will cover unattended (online or remote) use cases. In the United States, several states have started issuing mDLs that comply with the ISO/IEC 18013-5 standard to holders of state-issued drivers' licenses. Note that in addition to mDLs, these states may also issue mIDs that comply with the ISO/IEC 18013-5 standard based on state-issued photo ID cards issued to non-drivers. The issuers are termed Issuing Authorities in the ISO/IEC 18013-5 standard. For the remainder of this document, we will use the term mID to encompass both mDLs and mIDs that comply with the ISO/IEC 18013-5 standard.

According to the U.S. Department of Homeland Security (DHS), "The mDL movement is driven by two primary factors: 2020's REAL ID Modernization Act[5] and market-driven initiatives to develop secure, privacy-protecting, and easy-to-use technologies for managing digital identities. The former allows states to accept electronic presentation of identity and lawful status information, pending DHS implementing regulations."[6]

---

[4] As of May 2024, it is in the ISO approval phase.

[5] "S.4133 – REAL ID Modernization Act," U.S. Senate bill introduced July 1, 2023, https://www.congress.gov/bill/116th-congress/senate-bill/4133

[6] "Implementing Mobile Driver's Licenses: Not as Easy as You Think," DHS feature article, March 29, 2022, https://www.dhs.gov/science-and-technology/news/2022/03/29/feature-article-implementing-mobile-drivers-licenses-not-easy-you-think

In its Identity Management Roadmap,[7] the TSA repeatedly references the importance of leveraging digital identity solutions that can enable TSA to improve identity management while simultaneously mitigating risks to our transportation systems. (Figure 1)

Objective 4.3

Engage Industry and Interagency Partners to Enable Biometric and Digital Identity Solutions

TSA will engage industry and interagency partners to expand the use and integration of digital identity solutions in its transportation arenas to mirror customer expectations (for example, digitization of key services and experiences) in their travel experience. Three key partnerships TSA will prioritize when exploring this area are its work with (1) external partners to identify opportunities to integrate their digital identity solutions for customers into the infrastructure of airports and TSA systems, (2) DHS partners such as the OBIM, CBP, and DHS Science and Technology Directorate to explore leading practices and additional data sources and linkages, where appropriate, and (3) the U.S. Government on REAL ID and digital ID responses and products to ensure alignment and seamless use of digital identity products by citizens across all government interactions. In pursuing these goals, TSA will review state and federal biometric laws and limitations and adhere to information security and privacy requirements to protect individuals' information.

Figure 1. Objective 4.3 from the "TSA Identity Management Roadmap"

In 2023, TSA started piloting the acceptance of eligible ISO/IEC 18013-5 compliant mIDs at select TSA checkpoints throughout the country. [8]

[7] "TSA Identity Management Roadmap," TSA, February 2022, tsa_idm_roadmap_2022-03-01_508c_final.pdf

[8] For the latest map of available checkpoints, see "TSA Digital ID Map," Transportation Security Administration, https://www.tsa.gov/travel/digital-id/map

2.2 Outlook into the future of mobile IDs

As interest in mIDs is growing throughout the United States and Canada, payments stakeholders should begin exploring how mIDs can be leveraged for payment scenarios as well as for other non-payment events, in person or online.

mID use cases enabled by the ISO/IEC 18013-5 standard are limited to in-person verification only. However, the standard organization is working on the draft of the ISO/IEC 18013-7 standard, which would describe the use of mIDs in unattended (online) mode. The new ISO/IEC 18013-7 standard would open the way to promising use cases in the payment and financial spaces, in which mDL identity verification could be leveraged in online commerce or could facilitate remote KYC to create a new account with a financial institution.

Figure 2 shows an example of where digital identities and digital payment acceptance can potentially converge.

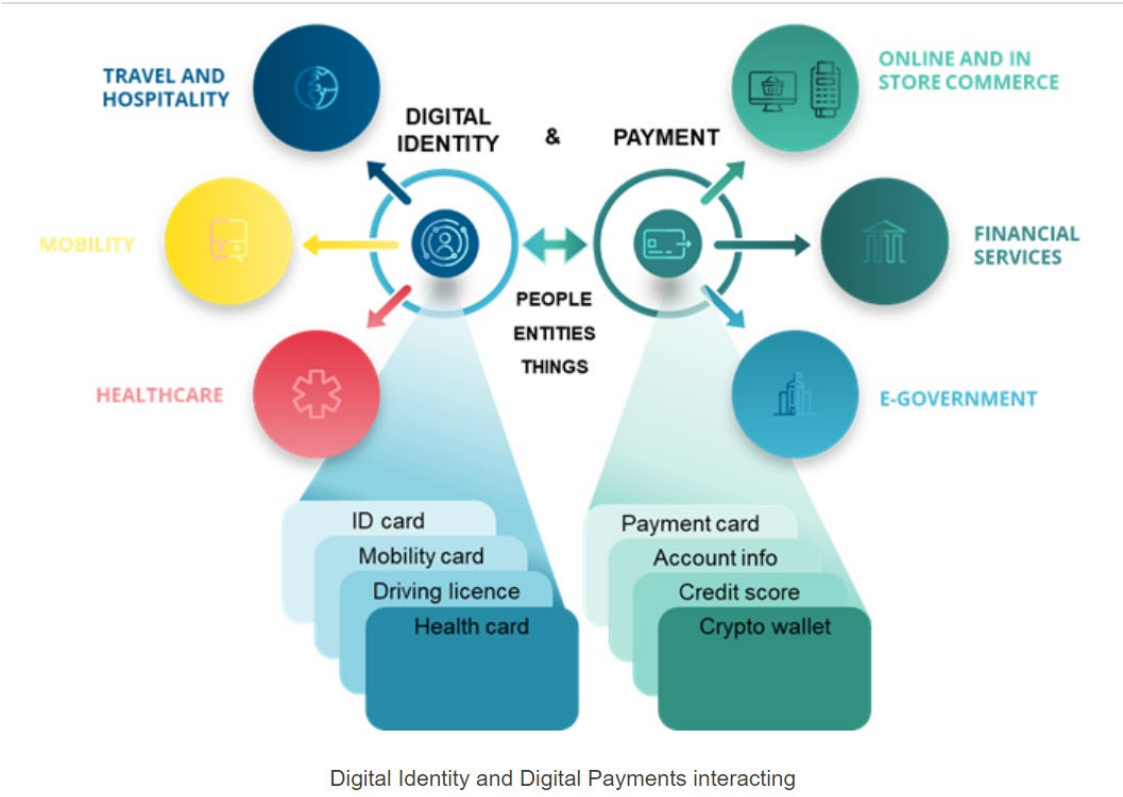

Figure 2. Example of Convergence of Digital Identities and Digital Payment Acceptance[9]

[9] "Digital identity is coming to payments. Are you ready?," The Paypers, March 8, 2023, https://thepaypers.com/thought-leader-insights/digital-identity-is-coming-to-payments-are-you-ready--1261687

2.3 Acceptance of ISO/IEC 18013-5 compliant mIDs

An mID transaction compliant with ISO/IEC 18013-5 can be initiated either by displaying a QR code on the device of the mID holder, or by a near field communication (NFC) tap to a verifier's device. The verifier, which is the entity that requires identity information from the identity holder, is also referred to as relying party.

mID acceptance forms part of the mID "triangle of trust framework". Figure 3 illustrates this concept. In this example, the mID transaction is initiated via a QR code by the merchant, and the merchant retrieves identification data online from the issuing authority. The merchant is the relying party in this example.

When the relying party is not connected to the issuing authority, ISO/IEC 18013-5 also supports offline verification modes, in which case data is only retrieved locally from the mID and no real-time data is retrieved from the issuing authority. In either case, cryptography protects the trust between the merchant and the issuing authority.

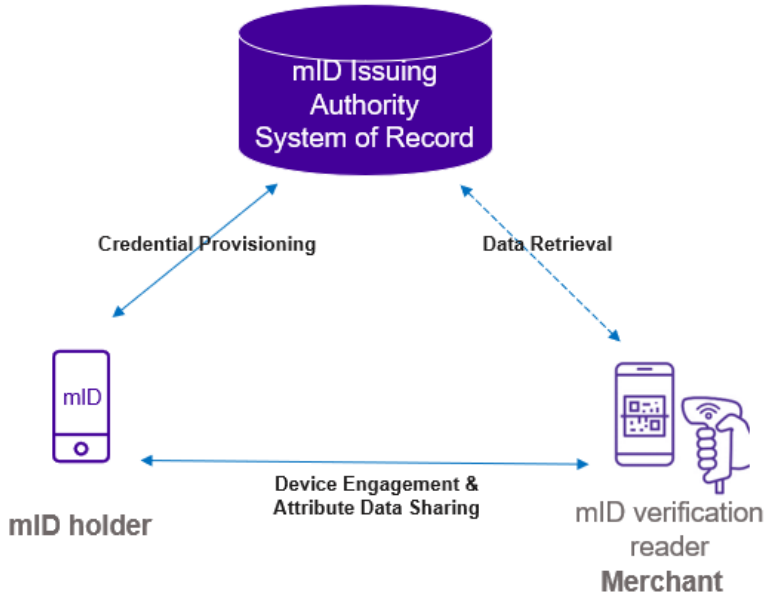

Figure 3. Example of an mDL verification in the Triangle of Trust Framework. Figure provided by IDEMIA

As of the publication of this white paper, no known integrations of mID verification applications with payment terminal platforms exist. However, merchants are still able to validate an mID and request specific identity attributes from the mID holder using either a dedicated mID verification app or mID readers developed in accordance with the ISO/IEC 18013-5 standard.

Figure 4 gives an example of such implementation. In this example, the merchant scans a QR code generated and displayed by the mID holder, with the QR code containing a unique authentication key. The mID verification app connects to the mID app of the identity holder through Bluetooth®, sending a request to the mID holder to share the relevant identity information. Once the user consents, identity and authentication data is transferred to the verification app, which can then validate if the mID is authentic, providing the verifier assurance of the legitimacy of the data received.

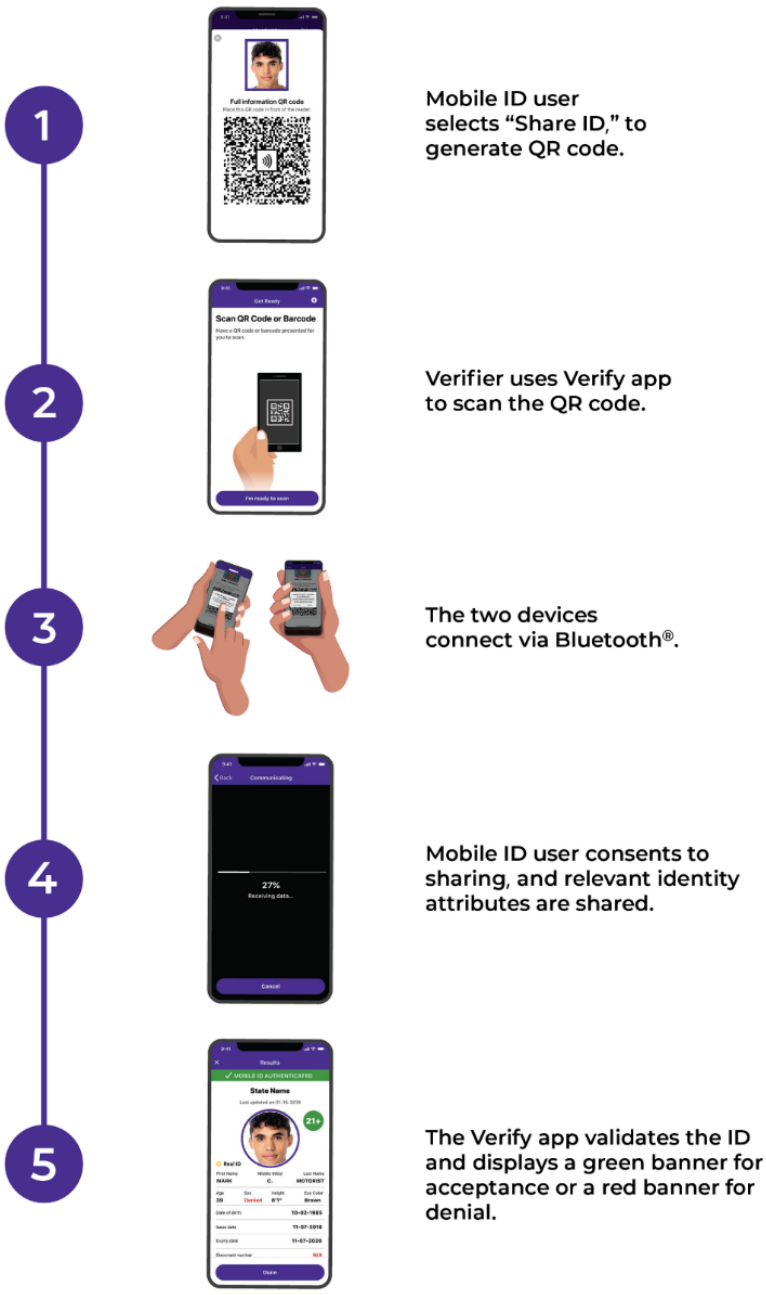

Figure 4. Mobile Identity Verification Example. Figure provided by IDEMIA

mID verification at checkout could be used during age-restricted sales, such as for alcohol or tobacco, where the privacy of the mID holder can be preserved by allowing the mID holder to share only the minimum identity data to prove their eligibility for the purchase. The mID could also be used to securely verify the purchaser’s identity for restricted purchases such as firearms, or to verify the purchaser’s identity on pick-up of online purchases in store**.**

Table 1 and Figure 5 list examples of use cases, both payment related and non-payment related, that mIDs could enable today or in the future.

Table 1. mID Use Case Examples

Examples of mID Use Cases	
Verifying age when entering a bar	Checking into a hotel
Passing through airport security	Proving driving privilege to police
Purchasing age-restricted items	Picking up a rental car
Registering guests or visitors	Opening bank accounts
Verifying identity of a medical patient	Activating vehicle insurance
Verifying identity for state services such as unemployment benefits	Matching a purchaser's name with a payment card
Picking up high value merchandise	Verifying identity for online gambling

Citizen Benefits

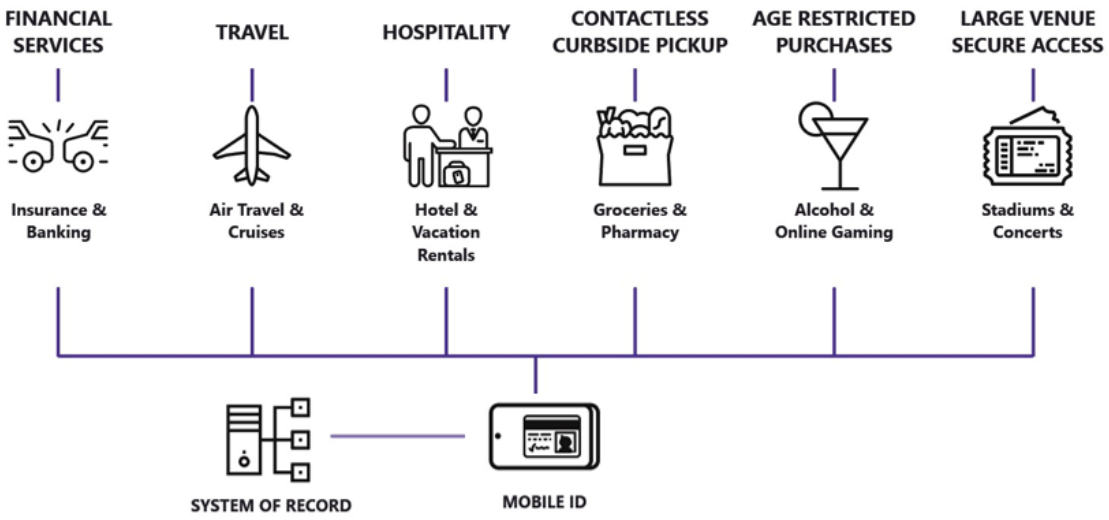

Figure 5. Citizen Benefits of a Mobile ID. Figure provided by IDEMIA

2.4 Benefits for mobile ID ecosystem stakeholders

Table 2 summarizes the benefits of mIDs for the holder, the issuer, and the verifier.

Table 2. Benefits for Mobile ID Ecosystem Stakeholders

	Benefits		
Benefits of Mobile ID	**Holder**	**Issuer**	**Verifier**
Holders can determine what data to share during a specific encounter.	✓		
Verifiers receive only the information required for a particular transaction, reducing the need to safeguard unwanted data.	✓		✓
Attribute data is accessed from a mobile phone, reducing the need to carry around a physical card.	✓		
Implementations follow robust security standards and can be digitally authenticated online and offline.	✓	✓	✓
Implementations provide cryptographic proof that an issuer validated the data. This reduces the acceptance of counterfeit documents.	✓	✓	✓
Mobile IDs can be used worldwide via the ISO/IEC 18013-5 standard.	✓	✓	✓
Mobile IDs can be issued remotely.	✓	✓	
Mobile IDs can be updated remotely, improving efficiency and minimizing the use of expired and invalid driver's licenses.	✓	✓	✓
Use of mobile IDs has the potential to increase security for online purchases and interactions in the future.	✓	✓	✓

3. How mIDs Can Be Used in Today's Payments Ecosystem

To verify an mID, relying parties would leverage a verification application with a means of getting the keys of valid issuing authorities. The verification system could be a dedicated stand-alone device, a smartphone with verification software, or it could be built into point-of-sale systems and handheld scanners.

Relying parties could use mIDs for:

- Authentication: proving attributes from the mID holder; for example, for:
  - Age verification. mIDs can be used to reduce the risk of legal exposure from accepting fraudulent IDs presented by underage customers attempting to purchase age-restricted items such alcohol and tobacco.
  - Identity verification for buy online, pick up in-store (BOPIS)/buy online, return to store transactions
  - Identity verification for high-value transactions
  - Identity verification for rentals (e.g., cars, tools, and lodging)
- Compliance with Know-Your-Customer (KYC) legislation and onboarding customers securely. mIDs can help reduce the risk of accepting a fraudulent ID.

4. Data Privacy Considerations for Payments

The ISO/IEC 18013-5 standard suggests that each participant in the mID ecosystem should make technology choices in line with privacy protection principles. A new upcoming standard—ISO/IEC 18013-7—will be able to support remote ID verification.

Two important privacy considerations are:

- **Informed Consent**. Relying parties should provide adequate informed consent to the mID Holder, including the purpose and scope of data requested.
- **Data Minimization**. Relying parties should be selective in which attributes they request and avoid requesting all data elements. Relying parties carefully consider the minimum data from the mID holder is necessary for the transaction, and they should only store personally identifiable information for critical business or legal requirements. Furthermore, this should be conveyed to the mID Holder. For example, for the age-restricted purchase use case, a merchant should only request age confirmation (and not the date of birth) and the portrait of the holder.

There are three core types of personal information that should be protected: Personally Identifiable Information (PII), Payment Card Industry (PCI) data, and Protected Health Information (PHI). The following table illustrates these types of personal information.[10]

Table 3. Differentiation among PCI, PII, and PHI Impact. Source: PrivateAI

Acronym	Meaning	Origin	Examples	Terms in other jurisdictions
PII	Personally Identifiable Information	U.S. (federal); not defined in any act; most commonly used definition is from OMB Memorandum M-07-16	Name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, postal code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), internet protocol addresses, biometric identifiers (e.g., fingerprints), photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual	Personal information (e.g., CCPA, PIPEDA); Personal data (GDPR, proposed New York privacy act)

[10] "What are PII, PCI and PHI?" PrivateAI, March 28, 2023, https://www.private-ai.com/2023/03/28/pii-pci-aphi/

Acronym	Meaning	Origin	Examples	Terms in other jurisdictions
PCI	Payment Card Industry	PCI is sometimes used as a shorthand for the information protected under the PCI Data Security Standard (PCI DSS)[11]	**Cardholder data:** Primary account numbers (PAN) that identify the issuer and the cardholder account; cardholder name; expiration date; service code. **Sensitive Authentication Data (SAD)** which is information used to authenticate cardholders and/or authorize payment card transactions, including card validation verification codes/values (CVV), full track data (from magnetic stripe or equivalent on a chip), PINs, and PIN blocks.	"Personalized security credentials" and "sensitive payment data" (*Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market*, aka PSD2)[12]
PHI	Protected Health Information	United States: HIPAA Privacy Rule	Individually identifiable information relating to a person's health contained in medical records, such as medical diagnoses, treatment information, as well as lab results and billing information	"Personal health information" (Personal Health Information Protection Act/PHIPA, Canada), "special categories of personal data" (GDPR)

[11] PCI Security Standards Council Document Library, https://www.pcisecuritystandards.org/document_library/

[12] "DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC," EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366

5. The Future of mID and POS Integration

The adoption of mIDs within a payment stream may take longer due to a few constraints. At this time, with the exception of the mID reader itself, POS vendors have not received any direction about which data elements should be examined or stored, nor has there been any guidance from the payment networks about whether any data elements should be included in a payment transaction message. The U.S. Payments Forum recommends that merchants implement a privacy-by-design approach and, as far as possible, minimize the number of attributes requested.

Samples of attribute sets are outlined in Table 4 and are not all-inclusive. As the mID specifications evolves, especially with the publication of ISO 18013-7, other types of online and offline use cases could be developed.

Table 4. Sample Attribute Sets for Merchant mID Use Cases

Age restricted purchase of alcohol	Portrait and 21+ age status
High-value transaction	Portrait, first name, last name, address
Rental car	Portrait, first name, last name, driver's license number, driving privilege, address, state, country, 25+ age status
BOPIS	Portrait, first name, last name
Check guarantee	Portrait, first name, last name, driver's license number
Self-service locker pickup	Portrait, first name, last name, address

Due to the lack of definition of required data elements and policies, and as the issuance of mIDs increases along with the continued deployment of merchant mID readers, any POS integration would most likely require custom development work performed by or on behalf of the merchant.

The seamless integration of biometric and digital identity solutions holds immense promise for streamlining processes, enhancing security, and empowering individuals. However, successfully navigating this landscape requires a collaborative effort from both industry and government partners, to address key considerations, including the following:

- Addressing ethical considerations around bias and discrimination in biometric algorithms is crucial.
- Regular audits and independent oversight mechanisms are essential to ensure fairness and accountability.
- International cooperation and harmonization of standards can facilitate cross-border transactions and identity verification, further boosting the potential of these technologies.

6. Conclusion

Mobile-based digital identity offers tremendous opportunities for combatting fraud and securing transactions, while offering the mID holder control over their personal data and the convenience of having their ID on their phone. As the amount of fraud increases, particularly in the online environment, the appeal of standards-based digital identity solutions will only grow.

This white paper identified several use cases for mID verification in the payment space, both in-store and online, but merchants and vendors would benefit from more guidance and cross-industry collaboration on how to accept this new technology in order to reap its benefits while being mindful of privacy constraints.

In-person verification of mIDs compliant with ISO/IEC 18013-5 is already made possible using apps or mID readers, however there are no known integrated solutions available today that combine mID verification and payment in the same system.

The upcoming ISO/IEC 18013-7 standard will open new possibilities for remote verification of mIDs and the payment industry should stand ready to design and develop new use cases that would benefit from remote identity verification in the online space.

7. Acknowledgements

This white paper was developed by the U.S. Payments Forum to provide information and insights on how mIDs can be leveraged in the payments ecosystem, both today and in the future. Publication of this document by the U.S. Payments Forum does not imply the endorsement of any of the member organizations of the Forum.

The U.S. Payments Forum thanks **Edward Perez** of Verifone for leading this project, **Teresa Wu** and **Annemarie Mattheyse** of IDEMIA and **Astrid Wang-Reboud** of Visa for drafting the white paper, and Working Committee members for their contributions. Participants involved in the project team developing and reviewing this white paper included:

Participants	
Gregory Aurre, FIS	**Tim Mansfield, Truist**
Teresa Wu, IDEMIA	**Henk Van Dam, Fime**
Annemarie Mattheyse, IDEMIA	**Edward Perez, Verifone**
Eric Steffensen, JCB USA	**Astrid Wang-Reboud, Visa**
Steve Cole, Merchant Advisory Group	**Kathy-Jean 'KJ' Condie, Voyager/U.S. Bank**
David True, PayGility Advisors	

8. References

"Digital identity is coming to payments. Are you ready?," The Paypers, March 8, 2023, https://thepaypers.com/thought-leader-insights/digital-identity-is-coming-to-payments-are-you-ready--1261687

"Implementation Tracker Map," mDLConnection – A Secure Technology Alliance Resource, https://www.mdlconnection.com/implementation-tracker-map/

"Implementing Mobile Driver's Licenses: Not as Easy as You Think," DHS feature article, March 29, 2022, https://www.dhs.gov/science-and-technology/news/2022/03/29/feature-article-implementing-mobile-drivers-licenses-not-easy-you-think

"Mobile Driver License, AAMVA website, https://www.aamva.org/topics/mobile-driver-license

"Mobile Driver's License (mDL) Implementation Guidelines," AAMVA, January, 2023, https://www.aamva.org/getmedia/b801da7b-5584-466c-8aeb-f230cef6dda5/mDL-Implementation-Guidelines-Version-1-2_final.pdf

"The Mobile Driver's License (mDL) and Ecosystem," Secure Technology Alliance, March 2020, https://www.securetechalliance.org/publications-the-mobile-drivers-license-mdl-and-ecosystem/

"National Strategy for Trusted Identities in Cyberspace," The White House, April 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

NIST Special Publication 800-63A-4 ipd, "Digital Identity Guidelines Enrollment and Identity Proofing," initial public draft, available at no charge from https://doi.org/10.6028/NIST.SP.800-63a-4.ipd

"What are PII, PCI and PHI?," PrivateAI, March 28, 2023, https://www.private-ai.com/2023/03/28/pii-pci-aphi/

9. Legal Notice

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