MOBILE DRIVER'S LICENSES

Backgrounder and Written Testimony House Financial Services Committee, Hearing on *Verifying Identity while Preserving Privacy in the Digital Age*

Abstract

Consumers view putting their ID Card or Driver's License on their mobile device as the last step toward the freedom of not carrying a wallet. The technology to do this exists today. Implementing Mobile Driver's License to meet the goals of privacy, equity, and freedom in American Society while ensuring higher security for American identities is the challenge. The Trust Frameworks for meeting these challenges also exist. Coordination and enforcement of business, legal, and technology can help meet American values in an Identity Ecosystem.

July 16, 2021,

A. David Kelts

david@kelts.org · https://www.linkedin.com/in/dkelts/ · @DavidKelts

Written Testimony of A David Kelts

david@kelts.org · https://www.linkedin.com/in/dkelts/ · @DavidKelts

Honorable Chair and Committee Members,

I am David Kelts from Arlington, Massachusetts, representing myself in support of forming a Mobile Driver's License ecosystem that reinforces the American values of privacy, equity, and freedom while spurring innovation and improvement.

I am the Director of Product Development for Mobile ID at GET Group North America, and a 5-year member of ISO/IEC JTC1/SC17/WG10 that wrote the 18013-5 mDL Standard. I lead the Evangelism Task Force within Working Group 10, and I was a lead author of the Privacy Annex of 18013-5. I am also a committee member and lead contributor to the Secure Technology Alliance's Identity Council, participating in mDL education efforts. The views I present today are my own proposals for your consideration.

I have prepared a Mobile Driver's License backgrounder in the attached pages. I will summarize the recommendations therein in this written testimony.

A Mobile Driver's License is a digitally signed document placed onto the mDL Holder's mobile phone for them to control. Government Issuers around the globe are the signers. When the user consents to share, individual data elements from their ID can be transmitted to a Reader device (Verifier). This is an improvement over physical cards where all data is visible on the front and decodable from the barcode. ISO 18013-5 is a standard for in-person, attended ID transactions, complementing existing online standards. The mDL Standard is designed to fit next to online identity standards such as Open ID Connect and user authentication standards such as from The Fido Alliance.

Empowering Americans with a mobile identity document carries challenges and must meet the values and goals of Americans. Protecting identity information, giving greater control and flexibility to the rightful holder of the identity, and supporting accuracy of operations come with the goals of inclusivity and access for all Americans.

There are challenges to getting a Mobile Driver's License ecosystem started. Government identity card Issuers must take the first move since they are the signatories to the accuracy and provenance of mDL Data. Support for their digital transformation that meets American goals can kickstart this digital identity transformation and help ensure that privacy and inclusiveness is achieved. Their decision thus far to embark on digital transformation and issue mDLs has been largely driven by desire to be technical leaders or through legislative mandate. The mechanisms to fund this transformation have not been easy to find, and Consumer Pays models are largely being chosen. It is worth funding this digital transformation.

Continuation of Written Testimony of A David Kelts

Challenges exist on the Verifier side as well. Businesses and Government Agencies tha accept ID and Driver's Licenses will wait for a large number of mDL holders before investing in technology for Contactless ID that can help protect their employees' healt and safety. Restaurants, for example, have moved to contactless menus out of necessary, but still must check ID manually by handling another person's ID card. Spurring innovation and the deployment of systems that accept mDL can bring Contactless ID transactions into reality. The technology is functional. Priming the pum of the business model to spur innovation would be helpful.

Identity, and the Mobile Driver's License Ecosystem, operates as a sum of many parts. The glue which holds together shared goals and values of such an ecosystem is a Trust Framework. Trust Frameworks define the business, legal, and technical "rules of the road" for an identity ecosystem. This framework is achieved in other regions by government-led initiatives, privately operated frameworks, or public-private partnership. To meet the goals and values of Americans, I recommend initiating a public-private partnership chartered to determine requirements based on our values and to enforce those requirements.

Federal Agencies have an opportunity to lead a digital transformation by accepting mD in manners that help protect the health and safety of their Agents and Americans. The Transportation Security Administration, fueled in part by the exposure of TSA Agents t corona virus, has led this kind of transformation toward accepting mDLs by participati in the creation of the standard and industry efforts to educate and initiate deployment Funding Federal Agencies toward this deployment will save lives and reinforce values.

The Department of Homeland Security has invested in the development of technologie for online identity. Similar initiatives to spur innovation, new development, and the deployment of privacy-enhancing, accessible technologies for accepting mDL can complement existing efforts by adding the in-person transactions all of us perform wit identity documents.

Industry Efforts, such as those by the Secure Technology Alliance, Better Identity Coalition, Kantara Initiative, Future Identity Council, and others welcome the continue and expanded investment by the Federal Government and Federal Agencies. There is expertise to be shared in bringing effective digital identity into reality in a way that reinforces our values.

Thank you,

Backgrounder: What is Mobile Driver's License (mDL)?

A Mobile Driver's License is a digitally signed document placed onto the mDL Holder's mobile phone for them to control. Government Issuers around the globe are the signers. When the user consents to share, individual data elements from their ID can be transmitted to a Reader device (Verifier). This is an improvement over physical cards where all data is visible on the front and decodable from the barcode. ISO 18013-5 is a standard for in-person, attended ID transactions, complementing existing online standards.

Electronic images of ID Cards are insecure and easy to spoof.

Most people immediately think that you **show** your mDL to a verifier. Photo editing tools and spoof applications make this impossible to trust. Imagine the fraud if we were showing Credit Card numbers on phone screens as payment. After unlocking the mDL app, the mDL Holder taps their phone or shows a QR code to a Reader. That action means the mDL Holder wants to share. Initially, they share a connection token.

Figure 1: Showing a phone screen is simple to spoof. Tap or Scan for cryptographic proof of ID and encrypted data sharing.

Cryptographic proof of ID data – Token to Share

The initial token does not contain any identifying information about the mDL Holder. Its purely a token setting up a transfer, which is the same methodology used for electronic tap payments. The token is exchanged for data by the Reader through a Web API (server retrieval) or directly from the mDL (device retrieval). Either model ensures encrypted transfer of data and resists eavesdropping or replay.

Control over Data Sharing and Device; Collection Limitation and Business Need to Store

Figure 2: Contactless ID transactions with ISO 18013-5

The phone never leaves the mDL Holder's hand and they have granular consent over the data they share. The Reader asks just for the data they require, and gets cryptographic proof that the subset of mDL Data is intact, unaltered, and came directly from the Issuer. This is how Contactless ID transactions can be accomplished. Since accurate, fresh data is available at each transaction, it is no longer architecturally required for Verifiers to store customer data. Data that is not stored does not expose a business to liability of leaks.

The demand for Contactless payment has grown significantly during the past 18-months, while Contactless ID verification has not been possible. Protecting the health and safety of the American public, business employees, and Federal Agents such as TSA is critical.

Multiple Interaction Modes

ISO 18013-5 is a data transmission protocol for trusted data. Sharing data is always initiated by the mDL Holder and nothing ever leaves the device without mDL Holder consent. The current version of the standard supports QR code and NFC tap to initiate connection, NFC, Bluetooth, and WiFi Aware for device retrieval of mDL Data (offline when not connected to the Internet), and REST API and Open ID Connect for server-retrieval of mDL Data (when online). This is the same Open ID connect widely used for login to web sites.

This means that mDLs can support multiple different interaction modes[1] at different distances. Interaction Modes support different workflows that businesses and agencies that accept mDL can deploy for faster customer processing, more trustworthy transactions, and enhanced customer privacy. ISO 18013-5 mDL is presently designed for in-person transactions.

Security of Data in Transit when using ISO 18013-5

The token that kicks off an mDL device-retrieval contains key material that is combined with key material from the Reader device to create a one-time encrypted transmit session. No nearby device can eavesdrop on a session because it cannot generate the same decryption keys. The public key of the Government Issuer is used to validate that the mDL Data was not altered and is official ID.

For server-retrieval, the public key of the Government Issuer is used to secure the channel to an online web service. This is equivalent to connecting to a website and seeing the lock icon in the browser. Data is never released without a token granting permission by the mDL Holder or without transaction-time identity verification and consent from Open ID Connect (that is widely used across login systems).

In both models, unlinkable identifiers and rotating public keys can be used to ensure some level of anonymity of the consumer participating in the transaction. Both models were created from the beginning using Privacy By Design principles. It is, on the other hand, possible in either device-retrieval or server-retrieval models to make mistakes or intentionally violate privacy principles. The technology for privacy must always be paired with the business models and legal protection to meet shared goals.

A Truly International Standard

Members of the ISO Working Group over the last 5 years included hundreds of participants from over 50 companies representing countries from every inhabited continent. Meetings were held in Africa, Asia, Australia, Europe, and North America to ensure accessibility to meetings and content. mDL Interoperability Tests have been held in Japan, Brisbane, and Omaha, NE. mDL pilot programs and contracts have been implemented in Sweden, Kosovo, New South Wales, Queensland, Ecuador, Indonesia, and multiple US States[2]. mDL Standard development was contributed to by AAMVA, eReg, Austroads, and the Motor Vehicle Associations of each continent. AAMVA has published guidelines[3] for North American issuers that mandate the use of ISO 18013-5 mDL.

Privacy Assessments Performed

Assessments of mDL Technology and the potential for a positive impact on privacy have been published. These are exceptionally well-researched, well-written publications fairly representing the concerns of Americans and technologists world-wide. They express concerns, positives, and shortcomings.

- *Annex E: Privacy & Security Recommendations*, **ISO/IEC** FDIS 18013-5:2021 (E)[4]
- **ACLU**: *Identity Crisis* What Digital Driver's License Could Mean for Privacy, Equity, and Freedom[5]
- **Kantara Initiative**, *Privacy & Identity Protection in mDL Ecosystems*[6]

[1] https://www.securetechalliance.org/publications-the-mobile-drivers-license-mdl-and-ecosystem/ section 2.3 defines and names the Interaction Modes of an mDL.

[2] https://www.mdlconnection.com/implementation-tracker-map/ shows updated mDL progress

[3] https://www.aamva.org/mDL-Resources/

[4] https://isotc.iso.org/livelink/livelink?func=ll&objId=21927996&objAction=Open, Annex E

[5] https://www.aclu.org/report/identity-crisis-what-digital-drivers-licenses-could-mean-privacy-equity-and-freedom

[6] https://docs.kantarainitiative.org/PImDL-V1-Final.html

- **Google** Security Blog: *Privacy Preserving Features in the Mobile Driver's License*[7]

The universal recommendation is that mDL holds promise with a warning. If done well, mDL can improve our privacy and identity security. To ensure that mDL is, in fact done well, will take a coordinated Business, Legal, and Technology effort such as in-place in other parts of the world (see Regional Fit below).

References – What has been written about mDL?

One of the first and most comprehensive white papers on the mDL is *The Mobile Driver's License (mDL) and Ecosystem*[8], from the Secure Technology Alliance. It is accompanied by an Executive Summary and a series of informative webinars[9] on mDL. Privacy, Trust, Business Model, and an Operating Framework for trust are key topics and concepts explained in this series.

The Mobile Driver's License (mDL) and Ecosystem accurately describes advantages of mDL, its flexible use, and the challenges that the mDL ecosystem, or any identity ecosystem, will face as it gets started with nascent technology trying to meet the needs of many. Section 6 of the white paper on *Challenges to a Robust mDL Ecosystem* is the rallying call around which Secure Technology Alliance members will collaborate to solve problems for years to come.

mDL Programs are in various states of development in the United States. The most accurate map of the present-day advancement of mDL Technology is available from mDL-Connection.com[10]. It is evident that the pace of these developments is quickening. Cross-state testing is beginning to happen, and use cases are being deployed in banking, retail, age-based purchase, restricted goods purchase, car-rental, transportation, and law enforcement. All are presently in-person with eventual online use case extensions.

How did mDL create an ecosystem?

Two participants in a transaction plus the signatory

In every mDL transaction, there is the mDL Holder who consents to share a subset of their identity information with a Verifier to receive a service or good for which confirmation of government-issued identity attributes is required. That Government Issuer, passively, is the third participant in the transaction. This naturally forms an Ecosystem. ISO 18013-5 mDL allows that third participant to be entirely passive – they can make known the public key that confirms their signature on the mDL Data and their position as an authoritative identity proofer in the eyes of the Verifier (who chooses the public keys that they trust and will accept).

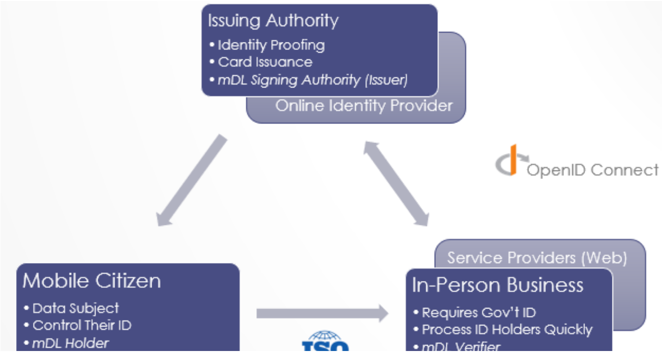


Figure 3: Participants in mDL in-person ecosystem (blue) next to the predominant online identity system (gray)

Every Issuer from the initial AAMVA Guidelines to present has stated that they wish their participation to remain passive. Tracking and

[7] https://security.googleblog.com/2020/10/privacy-preserving-features-in-mobile.html

[8] https://www.securetechalliance.org/publications-the-mobile-drivers-license-mdl-and-ecosystem/

[9] https://www.securetechalliance.org/the-mobile-drivers-license-and-ecosystem-webinar-series/

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

surveillance will not by policy or technology be tolerated.

ISO 18013-5 mDL was designed to create an ecosystem for in-person transactions. The secondary intention was to ensure that these in-person transactions could exist beside and in harmony with identity-backed transactions in the online, web world. ISO 18013-5 can work very well next to Open ID Connect. Open ID Connect is the majority technology in use for login credential providers. Adding unattended transactions has always been envisioned as utilizing Fido Alliance user authentication – a privacy-enhancing, flexible standard for authenticating users.

Many open source and SaaS implementations of Open ID Connect are widely available and highly functional. It is expected the same will hold true for mDL implementations.

Viewpoints of "Trust" from those participants

Accepted Every where
Makes Life Better
Improves My Privacy
Contactless ID
Consumer View
Verifier View
Always Available
Accurately Identify the Person
Cannot Be Spoofed
Protect Employees

In addition to the convenience of potentially not carrying their wallet, Consumers (mDL Holders) will use and trust their mDL if it makes their life easier, protects their identity better than currently, is accepted everywhere, and provides them the opportunity for Contactless ID transactions.

Verifiers are typically business with requirements to accept government-issued ID. They need the reliability of an always available system that cannot be spoofed, will protect their employees from disease transmission, and will accurately identify the person to whom they are granting the transaction.

Issuers also, from their arm's length of these transactions, need to accurately provision each mDL to the right citizen and trust the distribution mechanisms for their public keys (sometimes called PKDs). They also may need to make the technology decisions to ensure the high-availability and security of their deployment systems and the mobile applications.

When any one of these viewpoints of trust falls short, trust in the ecosystem will begin to erode. This is why kickstarting the ecosystem, ensuring its smooth and seamless operation, and providing enforcement capabilities with consumer redress actions is necessary for mDL to be trusted and used.

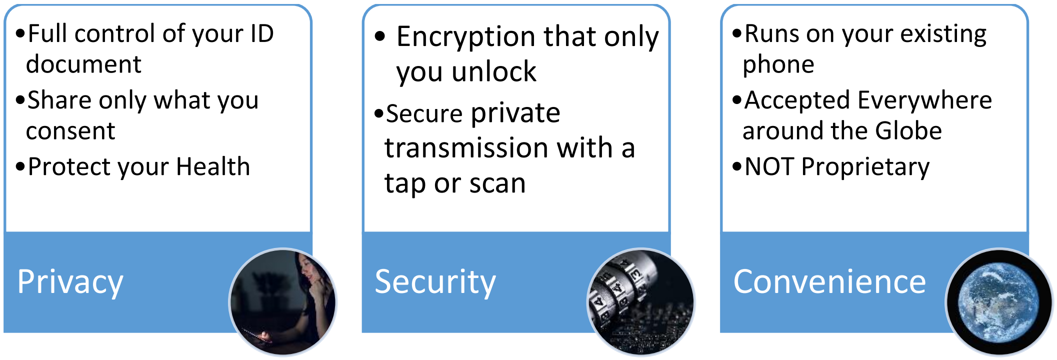
In blockchain or distributed ledger identity systems, there is potentially an additional entity in the ecosystem – those with the privilege to write to the ledger. This privileged group is often formed by consortium and the privileged ledger-writers are called Stewards. Other models exist.

Additional Objectives of mDL in an Ecosystem

mDL Usage by Americans is predicated on fulfilling certain privacy, security, and convenience goals. mDL Holders can be given the opportunity to choose their solution that fits these values (as in the model chosen by the State of Florida[11] [12]), and Issuers can choose to provide these values in the applications they select for their residents. ISO 18013-5 mDL provides the opportunity to achieve these goals.

[11] https://www.flhsmv.gov/floridasmartid/

[12] https://www.wtsp.com/article/news/regional/florida/florida-drivers-license/67-ff420646-1c55-40c7-99cd-55acb3c0e296



- Full control of your ID document
- Share only what you consent
- Protect your Health

Privacy

- Encryption that only you unlock
- Secure private transmission with a tap or scan

Security

- Runs on your existing phone
- Accepted Everywhere around the Globe
- NOT Proprietary

Convenience

Regional Values

Inclusivity – Equal Access to All – is a clear objective of identity systems to re-enfranchise those who may be missing documentation of their birth and name. The technology itself must operate equitably. State Government Issuers – DMVs – operate with identity proofing guidelines that allow the vast majority access. In many municipalities, City IDs have attempted to fill any gaps in inclusiveness. All can be targets for mDL given that the businesses and agencies accepting mDL decide from which Issuers they will accept mobile identities.

In the United States, privacy, freedom, and inclusiveness are national values with the additional technological goals of interoperability, ease of use, and accuracy of identification.

Regional Fit

For use of an mDL to meet the objectives of any region around the world, it must operate within a Trust Framework that defines the Business, Legal, and Technical "rules of the road" for identity operations. Such frameworks can be **privately operated**, as in the example of a consortium like Sovrin[13], **government operated**, as in the example of TDIF[14] from the Australian Digital Transformation Agency, or a **public-private partnership** such as DIACC Pan-Canadian Trust Framework[15] in Canada. In addition, technology companies with the means to implement an end-to-end solution could also privately operate a trust framework for mDL or online identities.

[13] https://sovrin.org/library/sovrin-governance-framework/

[14] https://www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework

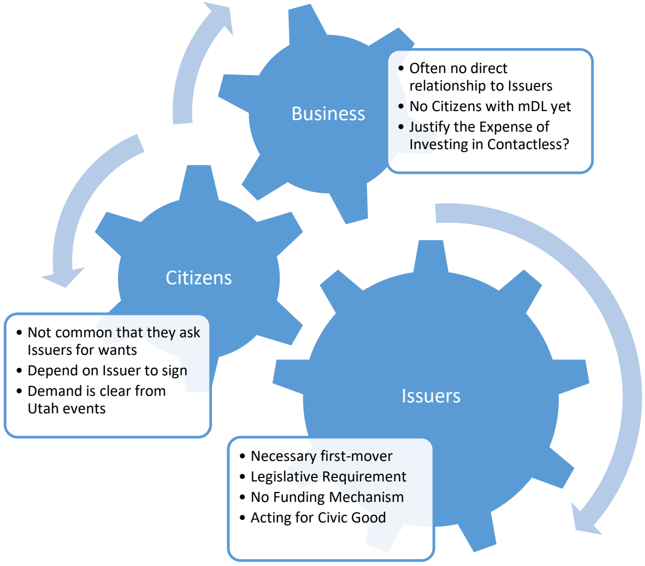
[15] https://diacc.ca/trust-framework/

Why hasn’t mDL happened already?

Demand is Growing, The Catalyst is Missing

To turn the wheels of this nascent mDL Ecosystem, typically the Government Issuer must be the first to act. The impetus and business rationale for action of a State Agency is not always clear. Standing out as a technology leader and achieving the public good are currently the determining or driving factors in a decision to pursue mDL.

In Utah[16], the Driver’s License Division[17] has taken first action upon legislative mandate and had the foresight to include business partners in the evaluation of a public contract award process. Businesses such as Utah Consumer Credit Union[18] have jumped to the forefront to accept mDLs before they were widely issued and have seen a boost in their membership due to technology leadership.

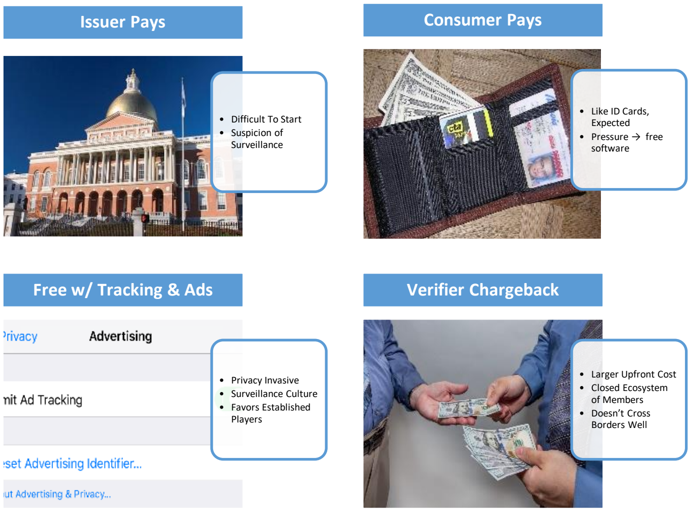


- Often no direct relationship to Issuers
- No Citizens with mDL yet
- Justify the Expense of Investing in Contactless?

- Not common that they ask Issuers for wants
- Depend on Issuer to sign
- Demand is clear from Utah events

- Necessary first-mover
- Legislative Requirement
- No Funding Mechanism
- Acting for Civic Good

No Uniform Business Model



- Difficult To Start
- Suspicion of Surveillance

- Like ID Cards, Expected
- Pressure → free software

- Privacy Invasive
- Surveillance Culture
- Favors Established Players

- Larger Upfront Cost
- Closed Ecosystem of Members
- Doesn’t Cross Borders Well

ISO 18013-5 mDL does not specify a business model, it is a technology interchange specification. Issuers without funding that want to act on behalf of their citizens face a difficult choice to move first. In the USA, the **Consumer-Pays** model fits with how residents currently pay for physical cards, so the Consumer Pays model has been adopted when high-technology vendors provide the solution.

The model of Issuers developing mDL technology (therefore **Issuer Pays**) is also in use, in the US and in places like New South Wales, with those solutions now needing to retrofit an mDL standard and find funding to expand beyond purely local usage.

Verifier Chargeback models are most effective when the ecosystem is closed-loop, membership led, or operated by a single entity or consortium. This allows for an accounting system that funnels money in a highly appropriate way – from those whose risk is reduced, and processes are improved (Verifiers) back to those who did the work to proof the individual identities (Issuers). Verifier Chargeback is difficult to kick-start because often the entire system must be in place before money starts flowing. Governance in these systems includes accounting services as well as Trust Framework enforcement.

[16] Please note that the author’s employer is affiliated with each entity used in this example of ecosystem startup. The author has worked directly on these products and project.

[17] https://publicsafety.utah.gov/2021/04/20/new-mobile-driver-license-to-offer-utahns-enhanced-privacy/

[18] https://www.cutimes.com/2021/06/24/utah-community-cu-to-test-mobile-drivers-licenses/

Free With Tracking and Ads is a business model widely in use across the Internet today. If the software is free, you the User are likely the product. This model is largely why today's hearing exists. Mixing mDL with this business model is likely to feel extremely creepy to Americans and deter usage.

What happens without a Catalyst or Business Model?

Lacking the catalyst or precipitant to kick-start any of these business models or the mDL Ecosystem, it is highly likely that a large player with deep pockets will step in to impose their business model on the mDL Ecosystem.

The *Verifier-Chargeback* model is one option when pockets are deep enough that the up-front development costs could be entirely R&D funded. The owner of the mDL Ecosystem in this model would own the chargeback mechanisms at a percentage analogous to those of software application distribution mechanisms (App Stores). Even if that technology giant only provided half of the mDL devices in the Ecosystem, the price pressure on the other half of smartphone applications would be driven to zero. The Consumer Pays model would be eradicated. The expectation of free software could drive ad or privacy-invasive funding alternatives. Privacy, in general, for all identity transactions flowing through one system could then become the responsibility of one tech giant to carry out.

Another potential move toward a *Free With Tracking and Ads* business model could be precipitated by other technology giants. To date, data on identity-backed business transactions with visual inspection of physical cards is not consolidated or correlated. It is possible with systems that scan PDF417[19] barcodes.

None of the above testimony is other than informed speculation about the possibilities of the development of the mDL Ecosystem. What is clear is that the business model and legal framework for an mDL Ecosystem must reflect the values of the American people and the ecosystem must remain open to many participants to provide and extract value – a free market. The physical ID market has many players, starting with innovators and, as with many mature markets, gravitating toward consolidation, consistency, or stagnation. Technology improvements have made the manufacture of fake IDs easier. Cryptography improvements will be the moving target of the mDL Ecosystem to stay ahead of forgeries.

What protections are necessary?

Security Standards to avoid a Privacy Problem.

Any Trust Framework would contain Business, Legal, and Technical rules by which all participants abide. Participants must abide by these rules and requirements to continue operation. Enforcement is both voluntary, collective, and backed by rules of recourse.

ISO 18013-5 mDL provides security mechanisms for data in-transit, but the secure storage of data is not specified. The security of mDL Data when stored on mobile phone, in cloud repositories, or even in aged, single-location, on-premise data centers is not part of a data transmission standard. Minimum acceptable standards for data at rest must be designated and measurable. Google has advanced this concept on Android with its Identity Credential API[20] [21]. Security audits and compliance certifications should be made available to all participants in the ecosystem by all providers.

Privacy is a Collective Responsibility

Identity protection and the resulting privacy is always an Ecosystem responsibility shared among all participants. A failure in security by any one participant can compromise the privacy of many. For this

[19] https://www.aamva.org/DL-ID-Card-Design-Standard/ contains PDF417 data formatting

[20] https://developer.android.com/reference/android/security/identity/IdentityCredentialStore

[21] https://www.xda-developers.com/google-android-digital-drivers-license/

reason, enforcement must be available and channels to resolve and remedy dispute must exist. The current environment for binding together mDL implementations in the US may be State laws.

In my many discussions with State Issuers, every single one wants to distance themselves from person-to-verifier transactions. The technology for unlinkable transactions is available and the will exists.

Where does the Consumer turn for protection?

Enforcement of Consumer Protection of Privacy has developed into the responsibility of the Federal Trade Commission. mDL is an evolution of present day card-based in-person transactions, and similar enforcement may be applicable when mDL transactions begin to happen during 2021 – 2022.

The question of consumer protection is not the expertise of the author, but a concern highlighted in order for it to be addressed in appropriate channels.

Considerations for Federal action

Action to organize the Trust Framework, and the enforcement of it within the United States is recommended. It should take a form suitably organized and agile for the technology world of 2021+ so that it is adaptable to change and always carries out the principles and vision of Americans.

NIST previously was chartered with organizing and running an Identity Ecosystem Steering Group (IDESG[22]) responsible for defining how identity could work in the US. The remnants of the IDESG and charter are now part of Kantara Initiative. Technology has evolved sufficiently that many of the visions of the 2000's and 2010's, including those piloted in many NSTIC[23] Grants, have become feasible and usable. This sort of public-private partnership toward shared common goals is still viable in the US.

The Secure Technology Alliance has many members in the Verifier space. STA is currently responding to the active *DHS/TSA Request For Information* with a set of considerations for DHS and Federal Agencies to assist with the formation of the mDL Ecosystem in a way that reflects American values and creates a playing field for innovation and growth. The following is an excerpt used with permission.

> STA commends DHS, and its component TSA, for active participation in early efforts by STA to start to overcome the challenges [outlined in Section 6 of The Mobile Driver's License (mDL) Ecosystem (ed.)].
>
> STA now recommends:
>
> (a) Strengthening DHS engagement in the concepts and efforts to kickstart the ecosystem. STA welcomes and encourages DHS participation at STA and at the other industry groups working toward the realization of a secure mDL Ecosystem
>
> (b) Defining the security, provisioning, and privacy requirements that attach meaning to the "Real ID" flag defined in the AAMVA Guidelines since RealID is central to the acceptance of mDL for Federal Use Cases
>
> (c) Encouraging all federal agencies and interagency bodies to participate in overcoming these challenges and realizing the ecosystem
>
> (d) Using STA Use Case Development resources (published along with the white paper) to capture and publish business processes and interactions where federal agencies rely upon driver's licenses or where a trusted digital ID credential could:
>
> - Reduce risk and control costs
> - Enhance quality of life, service, and user experience
> - Promote the growing interest in touch-free interaction

[22] https://idesg.edufoundation.kantarainitiative.org/ IDESG now part of Kantara Initiative

[23] https://en.wikipedia.org/wiki/National_Strategy_for_Trusted_Identities_in_Cyberspace

- Reduce fraud that harms the privacy, security, or identity of our countrymen

(e) Utilizing available funding, such as Silicon Valley Innovation Program, to roll out the acceptance of mDL for Federal Use cases. This program has been successful at pursuing architectural goals, and can now be used to encourage adoption of Contactless ID at scale in order to protect the health of our nation and improve security

(f) Lobbying for the nationwide legislation and funding that will encourage States to issue, businesses to accept, and citizens to have contactless options available to them

(g) Empowering and educating Federal Agencies with the authority to enforce privacy standards and requirements across mDL usage in the ecosystem within the USA`

Since the publication of the STA White Paper, demand for Contactless ID transactions has grown proportional to the growth in usage of Contactless Payment. The potential health benefits are clear in a post-covid world, and the protection of TSA Agents, Federal Employees, and the general public are critical to the operation and security of our country. STA encourages DHS to utilize whatever resources are available to assist a transition to a Contactless ID society.

Relying Party interest in accepting mDL as official government ID is blossoming inside STA and in the ecosystem at large. These driving forces of ecosystem momentum and healthier contactless ID are fueling interest and development.

Outside of the STA White Paper, members experiences in the implementation of state and major urban center identity programs prove that momentum is growing rapidly. They also seem to reiterate and compound the Least Common Denominator (LCD) problem described in STA White Paper section 6.1. The compounding of this LCD problem is, in practice in the field in jurisdictions that are rolling out mDL, slowing the number of locations where mDL will be accepted Day One and opening the door to competing standards not geared toward in-person usage. There are three major points where LCD is happening:

1) NFC that is widely used at point of sale and point of service is not available for mDL communications on all major phone operating systems, which results in hesitancy of Relying Parties to adopt or to bias their acceptance mDL to just the Android platform.
2) Vendor implementations that include a single Interaction Mode (see section 2 of STA White Paper that names these Interaction Modes) simply to achieve a rubberstamp of conformity are limiting the choices of relying parties in how they will accept mDL. In fact, some implementations have mutually exclusive technologies for mDL interaction, leaving Relying Parties considering waiting before they accept mDL. Wait and see approaches can hurt mDL ecosystem momentum.
3) Visual approaches that short-circuit cryptographic proof of identity are being rolled out in States because the ecosystem is not developed, and Federal Agencies (as well as other relying parties) are not yet equipped to accept mDL transmission and cryptography. Since there is no way to secure the screen renderings of mobile devices (the secure elements do not protect screen memory), visual implementations are injecting uncertainty into concept of mDL and exposing the potential for this mDL marketplace to blow up before it gains full momentum.

STA encourages DHS participation to alleviate these developing shortcomings in the ecosystem, fund the transition to cryptographic proof of identity at all agency points of service, promote what is known to be acceptably secure and fraud-resistant solutions, and seed the development of relying

> party technology to accept mDL. Innovation Programs within DHS could be tuned to develop acceptance of mDL and not just to solve online identity or espouse particular architectures.
>
> Major considerations for achieving public or industry acceptance are:
>
> - The security and identity assurance level of the mDL provisioning process (Section 5.2)
> - The security of the smart device that hosts the mDL credential and its platform
> - Verifier trust in the credential across states, countries, and other jurisdictions (Section 5)
> - Verifier trust that the credential is in possession of the proper, intended Holder (Section 5)
> - Enforcement of privacy protection for mDL Holders (Section 5.3) across all Interaction Modes
> - Liability and safety considerations for Verifiers and mDL Holders
> - Incentives of any form, including tax incentives such as those spurring electric vehicle markets, that allow Verifiers to adopt as pioneers in the mDL Ecosystem. This speeds up the transition to Contactless ID that will protect security and health of citizens.
>
> Other considerations include:
>
> - Phasing of feature roll-out and avoiding the risk of least common denominator solutions
> - Eradicating solutions with visual presentation or unsigned, unprotected barcode data
> - Verifier understanding of state and global or regional policies for proofing and issuance
> - Testing, education, and training for Issuers, Holders, and Verifiers
> - mDL Holder signing functionality for use cases where "signing with your ID" is warranted
> - Adoption of standardized user authentication for assisted or unattended use cases

The text box above is quoted with permission from The Secure Technology Alliances' response to DHS/TSA active Request for Information on Mobile Driver's Licenses.