GET Mobile ID™

I. Introduction

GET Mobile ID allows people to use a mobile phone as a form of secure digital ID. When you place your Driver's License into GET Mobile ID on your own device, this is called a Mobile Driver's License or mDL. To truly leave your ID card at home means that a Mobile ID needs to be accepted at all of the places where your identity is necessary. Like the physical ID card, GET Mobile ID can be used as a flash pass for age and identity verification, but unlike physical cards mobile phone screens do not have "linked and layered" security features and data displayed on a mobile phone screen *cannot* and should not be trusted. Fortunately, there is **ISO 18013-5[1] a standard** for easily obtaining and trusting data from a mobile ID on a phone. Adoption of ISO 18013-5 will enable tap & go identity transactions.

GET Mobile ID fully supports ISO 18013-5 so that citizens can use their ID everywhere- at point of sale, for fast entry into every establishment, at the roadside, across borders. GET Mobile ID utilizes formidable data encryption algorithms and communication security to combat fraud, reduce identity theft, and allow interoperability while putting the citizen in control of their ID. ISO 18013-5 does not require a card reader for acceptance; it can interface through Bluetooth, NFC, WiFi Aware, or barcode readers. GET is a pioneer in the implementation of ISO 18013-5, and our Mobile ID

Advantages of GET Mobile ID™

- LEAVE YOUR ID CARD IN YOUR POCKET
- CITIZEN CONTROL OVER THEIR IDENTITY
- CAN'T BE FORGED OR IMPERSONATED
- SIMPLE INTEGRATION TO SYSTEMS OF RECORD

In the future, Mobile IDs can offer the ability to access secure online e-services and digitally sign documents for permanent records.

Works across the widest set of consumer devices & transport	Consumers can use their existing mobile phone
Does not rely on visual display of the ID; holds data securely	Cannot be spoofed or impersonated or tampered
Full ISO 18013-5; follows all US & International Standards	Consumers can use their mobile ID everywhere
In-Person or Accurate Remote Provisioning	An **Official** copy of your ID without a trip to the DMV
Engineered for privacy and security of citizen data	Complete control over your ID

The GET approach to Mobile ID leverages all existing standards issued by the U.S. Federal Government (as in the Federal Information Processing Standards (FIPS)), International Civil Aviation Organization (ICAO), and the International Standards Organization (ISO). ICAO is operating a global interoperable system for authenticating electronic passport documents for international travel. This architecture, standards, and experience has been leveraged to create the International standards for Mobile ID and Mobile Driver's Licenses. The level of proofing is similar to the current enrollment and capture process for ID cards, but with emphasis on the trust model for binding the identity holder to the mobile credential. This trust model enables the use-case examples identified in §IV. Use Cases Enabled. Innovation on additional use cases once mobile IDs are commonplace will be driven by consumer demand for better identity protection and more convenient use.

This document will present an overview of the state of the technology; the processes for increasing the level of assurance in identity management; the underlying standards published and being developed to support identity; and the use cases with a value proposition for deployment in the market.

II. Primer on Identity

GET Group has a rich history in secure document issuance, being a leading supplier of passport personalization services to governments in every part of the globe. Our Mobile ID solution builds on this secure history to bring the future of identity to citizens now. To build this trust, every process and component in the GET solution must be aligned with the highest standards in identity available today. This means GET Mobile ID must be compliant with a trust framework for high-assurance credentials, be reliant on strong identity proofing and secure credential issuance and utilize standards for storage and transactions that enable high levels of assurance between the user and the relying party.

[1] https://medium.com/@dkelts.id/mobile-driver-licenses-mdl-how-to-use-iso-18013-5-5a1bbc1a37a3

A. Proofing & Registration

Identity proofing is the process of collecting and verifying information about a person for the purpose of proving that the person, who has requested an account, a credential, or other special privilege, is indeed who he or she claims to be and that the claimed person is historically unique. Proofing will validate identity attributes about the person against official records so that the identity information is accurate. This accuracy benefits the citizen being proofed as much as it benefits the government agency – a strong identity is the cornerstone for receiving the privileges and services to which the person is legally entitled in our society. Proofing is typically done in-person at government authorities in order to achieve the highest Identity Assurance Levels (IAL). For lower IAL, remote virtual proofing using secure kiosks can be utilized, and remote self-guided proofing using mobile devices is possible. For mDL, the State DMV has already done the identity proofing (the hard part) but the mDL still must be delivered accurately to the rightful holder (see Registration paragraph below).

The processes of identity proofing are standardized by NIST or by Regional Identity Schemes (see Trust Framework below) subject to the intended level of assurance and use cases for the credential. For example, to issue a US driver's license, strong proof of identity with a citizenship document such as a passport or birth certificate and another form of photo ID, along with a proof of residency within the issuing jurisdiction, is required, Without these, parental involvement is required for younger citizens. Higher levels of assurance and multi-factor authentication may also require collection of a biometric, such as a fingerprint or portrait, and these biometrics can be used to ensure others are not fraudulently applying for multiple IDs.

Registration or enrollment results in granting a credential or privilege. It is sometimes performed at the same time as the Identity Proofing, and sometimes uses a credential or record from a prior identity proofing transaction. The goal of registration or enrollment is establishing a reliable relationship with the person, and possibly to grant them some privilege that depends on their accurate record of identity, for example a seasonal Hunting & Fishing License is granted to one resident of a State.

B. Credential Issuance

Once the identity has been proofed, a credential can be securely issued to the individual. The credential can be either a traditional physical ID card, a Mobile Identity, an online Digital Identity account, or a combination of these types of credentials.

The issuance process is subject to different requirements depending on the level of assurance required. As an example, a driver's license is typically mailed to the individual after the enrollment and proofing process because delivery by the US Postal Service is highly accurate. This is acceptable since the driver's license always visually compared to the holder, ensuring again that the credential is in the proper hands, and grants the ID holder the privilege to drive a vehicle. Driver's licenses in the USA have become de-facto National ID documents and are used for many other use cases such as age verification and identity.

Higher-assurance or special purpose identity documents require multi-factor authentication to more securely identify the card holder and bind that identity document to the cardholder. The issuing process for high-assurance credentials typically requires in-person acceptance of the ID document with biometric verification of the ID document holder prior to issuance of the credential. This process binds the credential to the cardholder.

1. Physical credential
The physical or traditional ID document can be issued either at the time of identity proofing, over the counter, or mailed to the card holder after identity proofing.

2. Mobile Credential
It's critical to deliver the credential to the device in control of the person who was proofed. This can be accomplished through combinations of device authentication and device identification along with data-driven methods or biometrics.

3. Online Credentials
Credentials for online accounts are typically stored in an Identity Provider (IDP) so that they can be used reliably across myriad online web portals and services. Secure credential storage in an IDP is very possible, and most credential leaks in the news come from people improperly guarding single-factor passwords. Multi-factor authentication (multiple credentials of the knowledge, inherence, and possession types used simultaneously) reduces IDP risk dramatically.

4. Derived credential
Mobile identities can be read into the secure storage areas of phones directly when the physical ID card contains a chip or electronically readable and cryptographically protected feature. Some remote provisioning processes are derived ID.

C. Transaction-time Identity Assurance

It is critical that an identity proven and delivered to the proper holder remains in their possession. At the time of each identity transaction, across any of the contexts of in-person, nearby, distance, remote, or online, the user must be authenticated against the

credential. We think of this most typically as the shop clerk looking at our ID card and using the portrait to ensure that we are the proper holder, while assessing the card itself compared to others the shop clerk has seen to ensure it is genuine and untampered.

1. User Authentication

Assuring that the credential holder is the subject of the credential itself, the intended holder, assures that the user is authentic. Determining user authentication in attended situations, when a human is responsible for approving the transaction, is typically done by portrait identity verification. The user authentication for unattended transactions, whether in-person or over the internet, can be performed using techniques like Fido WebAuthN and CTAP.

2. Credential or Device Authentication

Determining that an ID card id genuine, whether by visual or machine-assisted inspection, provides credential authentication. For mobile identities, where no visual authentication can be performed, the identity data must be confirmed to still be on the device it was issued to. Confirming this determines that the data and credential was not cloned or copied to another device, an indicator that the credential is still in possession of the rightful holder.

3. Data or Passive Authentication

For physical credentials, we can see the State name and seal on the printed card and feel that it is genuine. For mobile credentials, the ISO 18013-5 Standard prescribes that the data resident on the device, and exchanged via the standardized protocol, maintains a cryptographic signature that shows it was issued by the proper authority. Verifier devices will obtain a certificate from the Issuing Authority that is used to confirm the integrity and source of the data.

D. Trust Frameworks

A Trust Framework is a set of "rules of the road" for the proofing, registration, issuance, and usage of identities across all relevant contexts. Along with this set of rules comes the legal framework that supports usage of proper identity in these contexts and the business model in which this proper usage functions – who pays for the value chain. Because of the legal and business models need to be highly fused with the identity rules, Trust Frameworks are typically regional or operate in specific business contexts. Some examples are DIACC.ca in Canada, SAFE BioPharma for healthcare in the United States, and the Trusted Digital Identity Framework in Australia.

Trust Framework development is difficult work and requires the consensus of many parties within an identity ecosystem, while preserving citizen privacy and reflecting the values of the region and diverse constituents within those regions. Still, frameworks are developing at rapid pace and converging on a global set of rules that can promote interoperability in our highly mobile, global society.

III. Government and International Standards

The GET mID solution follows government and international standards to ensure scalability and interoperability with open industry standard solutions. GET mID is at the forefront of compliance to permit future adoption and support in the market.

A. FIPS 140

The National Institute of Standards and Technology (NIST) issues the 140 Publication Series to coordinate the requirements and standards for cryptographic modules which include both hardware and software components for use by departments and agencies of the U.S. federal government. FIPS 140 does not purport to provide sufficient conditions to guarantee the security of a module conforming to its requirements, nor the security of a system built using such modules. The requirements cover not only the cryptographic modules themselves but also their documentation and (at the highest security level) some aspects of the comments contained in the source code.

B. FIPS 201

FIPS 201 (Federal Information Processing Standard Publication 201) is a U.S. federal government standard that specifies Personal Identity Verification (PIV) requirements for federal employees and contractors.

In response to the Homeland Security Policy Directive 12 (HSPD-12), the NIST Computer Security Division initiated a new program for improving the identification and authentication of federal employees and contractors for access to federal facilities and information systems. FIPS 201 was developed to satisfy the technical requirements of HSPD-12, approved by the Secretary of Commerce, and issued on February 25, 2005.

C. NIST Special Publications

FIPS 201 together with NIST Special Publications are required for U.S. federal agencies, and apply to U.S. national security systems:

- SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, NIST, February 2010 or as amended.
- SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations, NIST, August 2009 or as amended.
- SP 800-59 Guideline for Identifying an Information System as a National Security System, NIST, August 2003 or as amended.
- SP 800-63 Electronic Authentication Guideline, NIST, December 2011 or as amended.
- SP 800-73 Interfaces for Personal Identity Verification, NIST, February 2010 or as amended.
- SP 800-76 Biometric Specifications for Personal Identity Verification, NIST, July 2013 or as amended.
- SP 800-78 Cryptographic Algorithms and Key Sizes for Personal Identity Verification, NIST, December 2010 or as amended.
- SP 800-79 Guidelines for the Accreditation of Personal Identity Verification Card Issuers, NIST, June 2008 or as amended.
- SP 800-85A PIV Card Application and Middleware Interface Test Guidelines (SP800-73-3 compliance), NIST, July 2010 or as amended.
- SP 800-87 Codes for the Identification of Federal and Federally-Assisted Organizations, NIST, April 2008 or as amended.
- SP 800-96 PIV Card to Reader Interoperability Guidelines, NIST, September 2006 or as amended.
- SP 800-116 A Recommendation for the use of PIV Credentials in Physical Access Control Systems (PACS), NIST, November 2008 or as amended.
- SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), NIST, April 2010 or as amended.
- SP 800-156 Representation of PIV Chain-of-Trust for Import and Export, NIST.PERSONAL IDENTITY VERIFICATION (PIV) OF FEDERAL EMPLOYEES AND CONTRACTORS
- SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials, NIST.

D. ICAO Doc 9303

Document 9303 specifications are published in three separate parts, one for each type of travel document: Part 1 for Passports, Part 2 for Visas, and Part 3 for Official Travel Documents (Cards). All three parts have a common structure. The first two "sections" of each part contain the introductory material, definitions and references.

The third section contains technical specifications common to all machine-readable travel documents. For example, all MRTDs are required to meet the same physical requirements regarding deformation, toxicity, resistance to chemicals, temperature stability, humidity and light, and incorporate appropriate security safeguards to protect against fraudulent use and counterfeit.

All MRTDs follow a standardized layout to facilitate reading of data on a global basis by both human-readable and machinereadable means. While the content, use and dimensional (size) flexibility of the visual inspection and machine-readable zones are common in all MRTDs, these can differ slightly to accommodate the unique requirements of different types of documents and the diverse requirements of issuing states and organizations. Section 3 also specifies how the name of the holder is to be written, in both zones, and contains specifications for the holder's portrait (i.e. photograph or digital image).

E. ISO 18013

ISO/IEC 18013-1:2005 establishes the design format and data content of an ISO-compliant driving license (IDL) regarding the human-readable (visual) features and the placement of ISO machine-readable technologies on the card. It creates a common basis for international use and mutual recognition of the IDL without restricting individual domestic or regional driver licensing authorities from incorporating their specific needs on the IDL.

The intent of the ID-1 sized IDL is to allow one document to serve the purpose of both what is currently known amongst driver licensing authorities as a domestic driving permit and an international driving permit (IDP). Thus, the IDL replaces the need for two separate documents. Alternatively, those countries that choose to maintain their individual domestic design can issue a second card (with or without ISO machine-readable technologies), a domestic driving license (DDL), whilst the IDL serves to replace the current IDP paper document only.

ISO 181013-5 addresses the requirements for mobile devices containing Driver' s Licenses (mDL).

IV. Use Cases Enabled

The philosophy of GET Mobile ID is to enable mass adoption of a cryptographically secure identity document on mobile devices while maintaining ease of use so that Mobile ID can be usable everywhere identity matters. The standards-compliant GET Mobile ID can even be a more trustworthy identity than the current physical ID credential which is used as a simple "flash pass" identity credential. GET Mobile ID gives the citizen control over the identity data they share and permits the Verifier to prove that the identity data is genuine,

unaltered, from the issuing authority, and still residing on the same mobile device to which it was originally issued. This closes nearly all of the doubt in most identity transactions save for the goal of verifying the identity of the holder. In the current version of the ISO 18013-5 standard, a portrait is sent across the channel between devices, validated cryptographically, and the attendant to the transaction can compare that portrait to the mDL holder who presented it.

Why is visual usage of a mobile device not trustworthy?

The screen on a mobile device is architecturally a shared resource. Multiple applications on a mobile device share their section of the screen for information display with the operating system itself, that may post notifications, overlay updates, or bring up keyboards and other system tools. The screen is not designed to be a secure enclave and therefore cannot be protected from these overlays and overwrites.

The concept of a Trusted Screen Environment has not been developed even though Trusted Execution Environments for calculations and communications (NFC controlled by secure element) are now common. Therefore ISO 18013-5 standardizes the *communication* of validated identity data and. You can protect, encrypt, and secure the communication of signed data all the way in its pathway from one secure element storage area into another device. You cannot protect its display on the screen being read by another human. You must transmit and cryptographically validate data, including portrait photos, for that data to be trustworthy.

Multiple Interactions Improve Ease-of-Use of Transmission

The key to making transmission of identity data usable is to offer multiple different methods and mediums for transmission. Two devices must exchange some information (a token) that facilitates a connection (a process called Device Engagement), and then the identity data itself must securely move to the verifier device (called Data Transfer). Device Engagement must be quick. The mechanisms used for Data Transfer – NFC, Bluetooth Low Energy, WiFi Aware, RESTful web services, and Open ID Connect, must support varying speeds and distances in order to facilitate different kinds of interactions between two people.

Device Engagement is currently supported in ISO 18013-5 via an NFC tap or the Reader optically scanning a QR code from the mDL. When NFC is paired with a very quick Data Transfer, such as web services, mDLs can achieve quick "Tap & Go" usage, which is ideal for many nearby solutions for in-person use cases or unattended gates and vending machines. The GET Mobile ID product also can support Device Engagement over a longer distance via a Bluetooth low energy extension to the ISO standard. This can allow Bluetooth beacons to be Readers involved in distance solutions for in-person use cases like Roadside Stops and Restaurant check-in.

For each identity use case, there are multiple methods for which two devices can be connected and the data to be transferred. Since no two locations are the same and every business flows their customers differently, it's critical that your mobile identity application support as many different types of interactions as possible. Supporting use across a wide range of businesses and scenarios should be the goal of any Issuing Authority's mDL program. Consumers will keep the applications which to them are the most useful and necessary.

Trust, Encryption, and Security

Data Validation

mDL can provide information that the identity data received by the Reader is genuine, untampered, and freshly provisioned from a trusted Issuing Authority. mDL and the Readers use cryptographic protocols at transaction time to ensure these metadata characteristics of identity data by validating signatures placed on the data during the provisioning time. These mechanisms are described in ISO 18013-5.

Device Authentication

It is important to know that the mDL was not cloned from the device it was originally issued to be used by an impersonator. This would be the equivalent of giving your kid brother your ID card. To resist against impersonation and misuse, the ISO 18013-5 protocol concludes every local data transaction with a handshake known as mDL Authentication

In the online models of REST and Open ID Connect, mDL Authentication is not accomplished the same way because the identity data itself comes from the API of the Issuing Authority. Reader devices can use the TLS Certificates from known Trust Lists to ensure they are connecting to the API of the Issuing Authority itself, and not an imposter IA. Data will be returned for the citizen requested and can be used as is for identity verification and fulfillment of the business rules of the use case.

Data in Transit

There is a growing concern about privacy and confidentiality of information exchanged over nearby networking protocols such as Bluetooth and public networks such as the Internet.

A Mobile ID holding an encryption certificate can provide the means to effectively protect sensitive documents and information in general. For example, a Relying Party needing to send a PDF file can encrypt it using the user's public key. When the user accesses the document, it can decrypt the file using his private key associated to the encryption certificate.

Likewise, a Mobile ID can utilize a Verifier Certificate to encrypt data for an mDL Reader to access.

Two devices can negotiate a shared (symmetric) key using an unbreakable negotiation of keys called a Diffie-Hellman Key Exchange. This is the negotiation that takes place for each session in which mDL data is exchanged between two devices – the mDL and the Reader. Since this negotiation happens per transaction session, it's not possible to calculate offline what key is being used and then re-use that key for subsequent transactions. Session-encryption is a highly secure method even over the top of transmission mechanisms rumored to be insecure, such as Bluetooth.

Over Internet transactions, the same encryption principles can apply. TLS 1.2 is available for connection-level encryption. On top of transport encryption, session encryption is negotiated in the identity data retrieval (REST or Open ID Connect) by providing the public key of the Reader in the Data Request, and encrypting the JWT – the data format of the identity data response – so that only the appropriate Reader can decrypt, read and use the identity data.

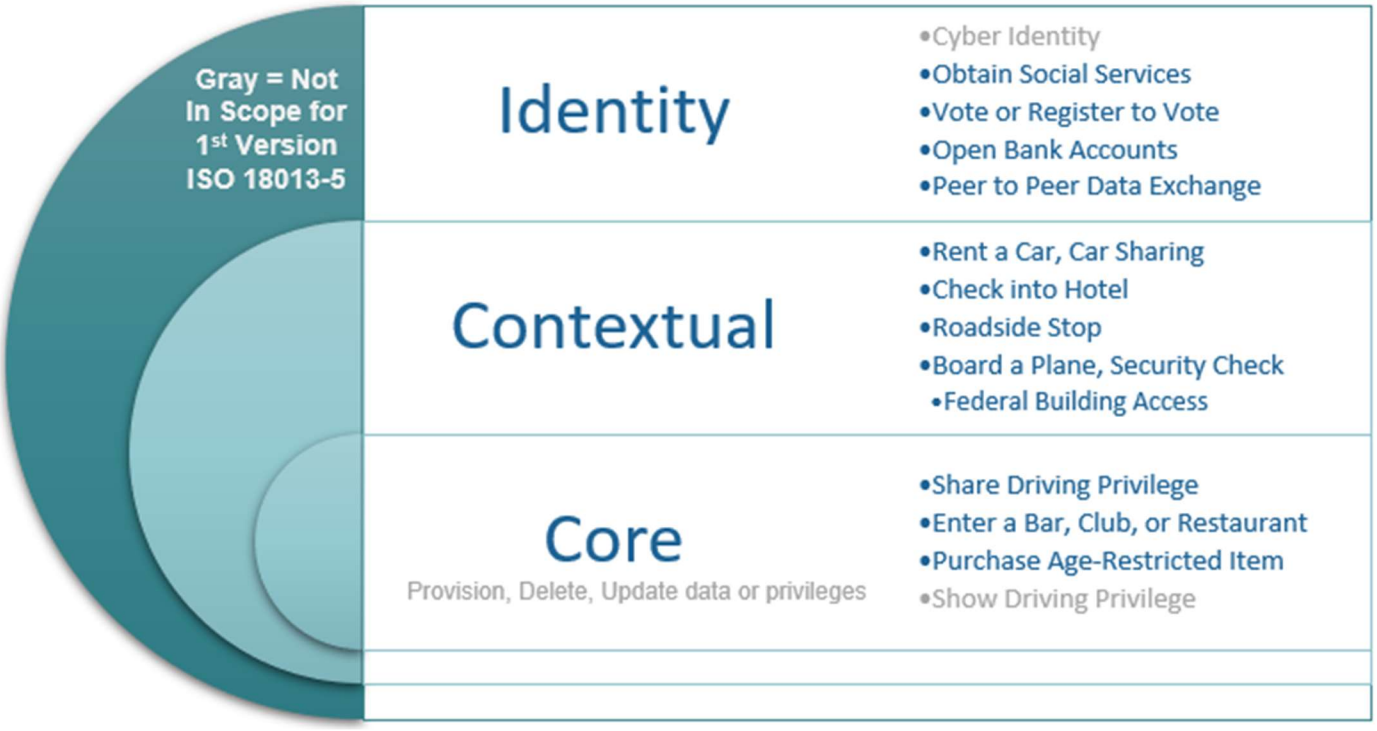
Data at Rest

Each major Operating System platform provides storage mechanisms, using secure elements when available, for symmetric and asymmetric keys – called Key Stores and Key Chains. The APIs for these keychains also provide facility to encrypt and store data elements of sensitive nature. It is industry standard to use these APIs to store identity data. GET Group solutions pre-encrypt data with a secret obtained from the user before utilizing these platform APIs, thus providing the most secure storage mechanisms that will only present identity data to the intended user after proper authorization.

Identity Verification (a/k/a User Authentication)

The first versions of the ISO 18013-5 standard prescribe the transfer of the portrait image from the mDL to the Reader device in order for the Verifier attendant to perform an out-of-band identity verification – to visually verify the mDL Holder versus the portrait.

Use Cases for Mobile Identity



In AAMVA's white paper on Mobile Driver's License Functional Needs[2], they listed a set of use cases for Driver's Licenses and ID Cards in the United States that form the basis of mDL design and the ISO 18013-5 standard. These included the core reasons that people use their DL, which are not typically expected to cost either party any money to execute, and additional use cases that happen in situ – within the contexts of everyday life – or in both online and in-situ.

[2] https://www.aamva.org/FunctionalNeedsWhitepaper-9/

These are by no means the only usages of Identity Documents world-wide, and exclude use cases typically assigned to passports such as border control. One large retailer has detailed out 19 different uses for some form of identity document within the context of their many outlets and establishments.

It is critical to consider that how you use an Identity *Card* today is not how you could possibly use a mobile phone as an identity *credential* in the future. Mobile phones can communicate securely, be used from distances much greater than the fonts on a 2" x 3" card support and are nearly continually connected to a wide range of Internet services. mDLs provide the opportunity to completely revamp and re-personalize service delivery that has become mechanized and anonymous in the early computer age.

- Consider whether you can fit identity verification into a workflow that better suits your establishment
- Consider if you can provide more personalized service, on a first name basis, after obtaining minimal trusted identity data
- Consider converging loyalty programs to a repeatably anonymized identity token received every time from the same mDL Holder
- Have employees greet a new customer as though they are already a loyal customer when confirming age and portrait

Future Extensions to mDL

A mID with a signature certificate can be used to sign electronic documents, providing non-refutable evidence of commitment over the document content.

Given this legal and technological framework, it is possible to deploy a Mobile ID Signature Portal where Relying Parties can present documents to their users and collect electronic signatures. Mobile ID signing could be a feature of existing document signing services in widespread use today.

When a Relying Party needs a document to be signed, it redirects the user to the mID Signature Portal. The document is rendered and shown in the browser, where the user can carefully review it. This is an important step to fulfill the WYSIWYS requirement (What You See Is What You Sign). If the user agrees with the contents, the document is signed using the signature certificate in the mID and the signed document is returned to the Relying Party.

Additional utility with electronic signature and verification is "proof of presence" for transactions. The electronic signature process is non-refutable evidence of user presence in a transaction.

V. Summary

Identification is going digital. Mobile Driver´s Licenses or Mobile IDs can offer convenient alternatives to physical IDs while helping to combat fraud and establishing the foundation for a wide array of in-person and online digital services. Widespread adoption of mobile IDs is dependent on secure verification capabilities and the adoption of standards such as ISO 18013-5 that make mIDs usable everywhere.

The GET Mobile ID, providing high-assurance identity on a user's mobile device, represents a convenient, secure and instant alternative to traditional, physical identification documents. By utilizing data encryption algorithms, device and user authentication, and communication security measures, GET Mobile ID can combat fraud and reduce identity theft.

Because GET Mobile ID is built on ICAO, ISO and AAMVA standards, the foundation is set for acceptance at every point of service where ID cards are currently accepted, and for a wide range of online identity-based services as the future develops. Supporting ISO 18013-5 in the variety of forms of data exchange – tap, nearby, distant, remote, and online – means that Verifiers and Relying Parties can re-envision how they provide service to their customers and achieve their compliance requirements. Traditional face-to-face in-person methods of service delivery, mired in the past requirements of face-to-face identity verification, can be drastically changed to other models people have come to expect from digital identities – check-in when entering the business, pre-clearance while waiting in line, online shopping followed by express delivery. Service delivery can improve with the flexibility of GET Mobile ID.

ABOUT GET GROUP NA

GET Group North America is an experienced provider of high-assurance security solutions that enhance Identity, Credential, and Access Management (ICAM) operations. As a leading-edge systems integrator, GET Group NA and its partners design, manufacture, and implement end-to-end solutions for secure credentials that enable government agencies, motor vehicle departments, municipalities and law enforcement organizations to implement the latest in identity management technologies. From photo ID cards to driver's licenses to passports, GET Group NA delivers advanced personalization capabilities that prevent identification fraud and accommodate diversified customer needs.

GET Group NA has over 20 years of experience in identity management and is certified under CMMI Level 3 and ISO 27001.

To learn more, visit **www.getgroupna.com** .

+1 781 890 6700 | 230 Third Ave. Waltham, MA 02451 USA