Redefining trusted ID with mDL

ISO 18013-5 Mobile Identities will revolutionise service delivery worldwide

by David Kelts

ISO 18013-5 standardises cryptographic proof of personal identity via mobile phones and other mobile devices, opening a world of possibilities for document issuers and citizens. The real revolution for mobile driving licences (mDL) and mobile national identity cards (mID) will come, however, when relying parties figure out how to take advantage of what sets mobile IDs apart from ID cards – securely communicating nearby and from a distance while using biometrics and device management to authenticate users.

***David Kelts** leads GET Mobile ID products. His goal of bringing high-trust identity into the control of every citizen started in 2013 with two NSTIC grants proving trust can be created online. It continues today with GET Mobile ID and mDL. David is a Certified Information Privacy Technologist and certified SOA Architect. He joined GET after 15 years in Identity, Biometrics, and ID Documents at IDEMIA.*

What is an mDL?

A mobile driving licence (mDL) is an official copy of your identity document and driving privileges under your control on your mobile device. What makes it official is that your data are signed by an issuing authority and moved into the secure storage areas of your mobile device. The signature can be verified when you use your mDL.

What makes an mDL authoritative?

Because of the signed data on the mDL, a verifier can use the public key of the issuing authority to easily validate mDL data as authoritative and unaltered. The signature is what makes the electronic document official. Nothing else, even downloading the app from your issuer, can make your mDL official or protect the verifier from fakes. The signature must be verified. Public keys, as certificates, are freely distributed by the document issuer, and can be assembled into trusted Master Lists by countries or associations of issuing authorities.

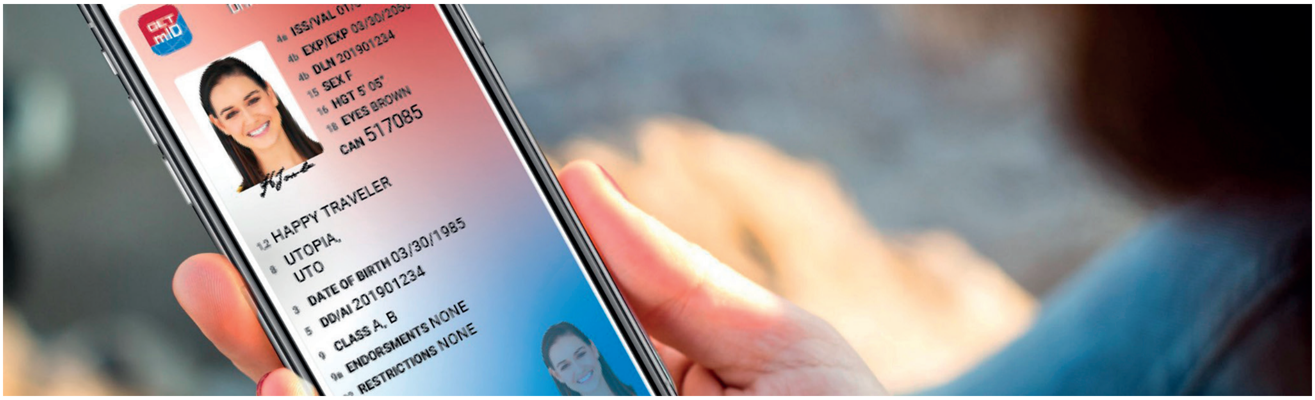
Transmission mechanisms

Having an international standard can ensure world-wide interoperability. ISO 18013-5 standardises cryptographic proof of identity documents on mobile devices. Issuing authorities, technology vendors, and the mobile platform providers have come together to agree on mechanisms to exchange and cryptographically verify mDL data. Multiple standardised transmission mechanisms open a world of possibilities for document issuers and citizens: not only mDLs and mIDs, but also subsidiary documents such as professional licences or fishing licences.

> ISO 18013-5 standardises cryptographic proof of identity documents on mobile devices

Resisting fakes

The temptation with an mDL is to think you can show a rendering on your phone screen to a verifier, or that the verifier can even interact with it. Neither can be trusted. Photo manipulation, movie tools and rapid prototyping tools make it easier to create fake visual mobile ID apps than it is to create fake physical ID cards. At least with printed cards, there is the burden of the manufacturing



cost for special equipment, ink and holograms. With mobile documents, only the cryptographic signature can resist forgery. Verifiers can never rely on the validity of visual versions of cards on mobile devices.

> Verifiers can never rely on the validity of visual versions of cards on mobile devices

Trusting an mDL

In the mobile software world, everything can be copied – except for private keys stored in the trusted secure elements of each mobile device platform. Nothing substitutes for a cryptographic signature on the data of an ISO 18013-5 mDL, and signed mDL data are simple to verify using the issuer's public key. Although the shared screen architectures of mobile platforms mean that spoof applications can even write over the top of authentic mDL applications, nobody can sign on behalf of an issuer. ISO 18013-5 can solve the trust problem. Cryptographic trust beats visual presentation every time.

> Cryptographic trust beats visual presentation every time

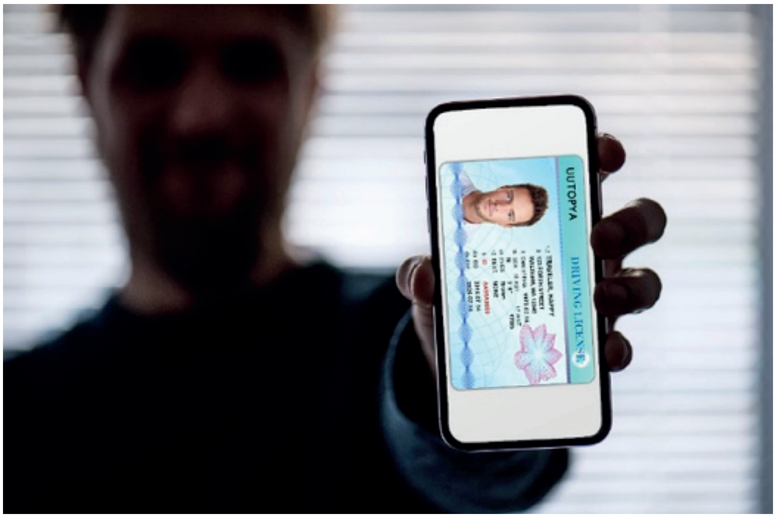
mDL interoperability

Although cryptographic trust is established by ISO 18013-5, the real revolution of mobile ID will come as relying parties figure out how to take advantage of what sets mobile IDs apart from ID cards. Where ID cards can only operate at the range of the verifier's eyesight, mobile devices can securely communicate both nearby and from a distance, and they are nearly always connected to the internet, not to mention always near at hand.

The mDL device operated by the mDL holder, and the mDL reader device operated by the verifier need to exchange some basic connection information during the device engagement that permits them to create a shared transport mechanism and a secure channel for exchanging messages and transmitting data. Alternatively, the mDL reader could use its internet connection (go online) to request mDL data from a service.

Device engagement

ISO 18013-5 empowers the mDL holder to initiate a transaction by taking a specific action. An NFC tap or presenting a verifier with a QR code acts as proximal consent for the verifier to create a connection and request data from the mDL. In the current version of the ISO standard, the reader cannot initiate a request for data, the mDL holder must give the reader connection parameters to an NFC, Bluetooth, or Wi-Fi Aware service.



NFC has the shortest connection distance and a defined speed profile, but its low-power mechanisms have led to widespread support on Point of Sale devices, credit cards, transit systems, and even hard-coded stickers and tags.[1]

Bluetooth has an effective communication range that matches that of optical QR scanning and can be reliable up to several meters. Approaching or exceeding 10 meters per the Bluetooth specs will introduce degradation and retry, resulting in a slowdown or failed transmission. Bluetooth suits short-range messaging in isolated or low-traffic environments.

Wi-Fi Aware is a software upgrade rolling out in the latest mobile operating systems using existing Wi-Fi chipsets. It will serve as a successor to Wi-Fi Direct and promises extended range, faster transmission speed, and TCP-style reliable transport. Wi-Fi Aware can handle multiple simultaneous connections, and its speed will support true Tap & Go interactions using ISO 18013-5.

As ISO 18013-5 evolves beyond the initial release, reader devices will likely gain a mechanism to identify themselves to the mDL holder. This mechanism will open up distance device engagement over Bluetooth beacons and other reader devices that can advertise a reader service. This revision will permit the police squad car to identify itself as official and the officer to be verified as official, before the mDL holder permits mDL data to be released to the officer's reader device.

Data request and transmission

NFC allows for tap transfer transactions; Bluetooth communicates nearby; Wi-Fi Aware provides reliable short-range communication; web services and Open ID Connect are the backbone of internet identity and communications. Each can serve as a data transport mechanism from any mobile identity on a device to any reader device, whether a mobile device, Point of Sale terminal, laptop, thin-client tablet, or connected device.

Offline data transmission

When two devices create a connection and exchange data locally, this is an offline data transmission; no internet connection is used. There are currently three supported transmission mechanisms: NFC, Bluetooth and Wi-Fi Aware.

Online data requests

As part of the device engagement parameters, an mDL can share an 'online token': an identifier of the mDL record to be used at one of two interfaces: a WebAPI RESTful interface or an Open ID Connect authorisation grant code flow. Either interface accepts the online token as a parameter that identifies one user and authorises the reader device to access a subset of mDL data. The ISO 18013-5 Privacy Annex requires that online tokens be single use, untraceable identifiers and that no central service ever log or track the individual user.

Trusting the mDL

mDL data come to the reader device field by field or in sets. This permits the reader to minimise the data requested to what is necessary for granting approval for the transaction. This data minimisation is a key privacy feature of ISO 18013-5 and an advantage over physical cards.

mDL data are accompanied by a 'mobile security object' that contains the signatures for each data element that the reader can verify against its trusted Master List of public key certificates. The reader can prove that the mDL data are authentic and unaltered since it was provisioned by the signing issuer. This mechanism, called Passive Authentication, enables the verifier to trust the integrity of the data.

> Data minimisation is a key privacy feature of ISO 18013-5

Protecting against clones

In addition to proving the trustworthiness of its data, the mDL can demonstrate its resistance against cloning. Active Authentication ensures that those signed attributes were obtained from the device to which they were originally issued, which protects against cloning and reuse of the mDL.

Protecting against unauthorised use

The mDL apps will use proper user authentication mechanisms to unlock for usage, just as banking apps do now. App unlock does not confirm mDL transactions; the mDL holder must be confirmed to be the proper holder of the mDL data with each transaction.
ISO 18013-5 presently allows for the signed portrait photo to be confirmed as authentic and used visually to verify the identity of the mDL holder. Reader devices can automate this process. This part of ISO 18013-5 will evolve to support standardised user authentication mechanisms that do not require portrait sharing.

Protecting against tracking

Both online and offline transmission scenarios, and any electronic transaction, can provide a mechanism for tracking individuals when they use their credential. A transmission protocol cannot protect against all privacy attacks, but the ISO 18013-5 Privacy Annex provides a set of privacy requirements for issuers to include in Requests for Proposal, and for technology vendors to use when determining engineering guidelines.

Interaction modes

Mobile ID interaction modes, such as Tap & Go, Tap & Hold, and Scan & Look will facilitate use cases from nightclub access to beer vending machines to mortgage applications.[2] NFC, QR, Bluetooth, Wi-Fi Aware and online mechanisms bring a variety of choices to verifiers provided that mDL applications build the appropriate support. The mDL application vendors must support all interaction modes for this ecosystem to flourish.

The interaction mode can be selected by the verifier to suit their use case and how they want the customer interaction to be designed. Considering the number of locations where ID cards and driving licences are used today, it is not hard to envision that these businesses that rely on identity may want to request it through different channels that suit or improve their business flow. They will no longer be bound by the constraints of line of sight.

Night clubs, stadiums, and even the Transport Security Administration could set up special fast lanes for mDL holders where one attendant taps or scans the mDL, quickly pulls data from the online service of the mDL, verifies the authenticity of age statements and the identity of the mDL holder, matches them to their ticket, and permits them to pass. This Tap & Request interaction mode supports fast lookup of just the data elements required for the transaction, protecting the privacy of the citizen while speeding up service.

Restaurants may initially equip their waiters with mDL checker devices, but in a near-future revision of ISO 18013-5 can enable a Bluetooth beacon that services their restaurant (in tandem with their Wi-Fi access point) and truly personalises service. The mDL holder ‘checks in’ to the restaurant while in line or when seated at their table. They can join the local Wi-Fi and submit their age and photo from their mobile ID. When the waiter approaches the table, they can immediately see the photo and confirmed age, and maybe even call the customer by their first name (if consent was granted). This use of technology can return the days of personalised service where businesses knew their customers and treated them like neighbours.

Most ID card interactions in the physical world have a human attendant. When ID documents go mobile, verifier computing systems can be deployed in unattended modes. These mDL readers can use biometrics and standards such as Fido WebAuthN tokens to authenticate users. The interactions brought by e-Passport systems can be available to mDL users.

Conclusion

mDL can be used differently than physical ID documents. When you go beyond the thought of simple visual usage of mDL – which cannot be trustworthy – and unlock the potential of multiple interaction modes that each provide cryptographic proof of ID, you can begin to revolutionise service delivery in the mechanised computer age. Relying parties that need ID documents to authorise a service can design flows that fit their place of business and how they want to treat their customers. The marriage of thoughtful design of proper business flows matched with the personalised experiences of our mobile devices will spur a revolution in the delivery of personalised service while protecting the privacy of mDL holders in ways that our current physical documents cannot.

References

1 *Prindle, D. (2018). How to make coasters that connect guests to your Wi-Fi with a single tap. Digital Trends. https://www.digitaltrends.com/how-to/diy-nfc-coasters/*

2 *Secure Technology Alliance Identity Council (2019). The Mobile Driver's License (mDL) Ecosystem. [online] Available at the STA web site: https://alliance-forumgroups.org/wg/mobiledriverslicense/document [Accessed October 26, 2019].*