Mobile ID for All: Interoperability and Privacy Preservation as Key Success Factors

Dr. Evangelos Sakkopoulos*a* and Konstantin Papaxanthis*b*[1]
a University of Piraeus, Department of Informatics, Karaoli & Dimitriou 80, Piraeus, Greece;
b Scytáles AB, Polygonvägen 53, 187 66 Täby, Sweden

ABSTRACT

Mobile ID (mID) has received a number of different form factors until today. We are at the advent of an era that IDs are going into mobile smartphones to serve secure identification and enable GDPR. In this paper, we present key use cases of mobile ID that are expected to receive wide adoption such as age verification especially sensitive to privacy preservation. To maximize adoption rate and assure interoperability, we have included in our proposed solution all possible communication options available in a modern smartphone such as NFC, BLE, QR and WiFi Aware. Another key success factor for mobile ID is following closely standardization specifications such as ISO 18013 Part 5 and AAMVA paradigms for mobile Driver's License. We present a robust implementation for the uniquely widest possible range of smartphones independent of smartphone OS.

Keywords: mobile ID, mID, mobile Driver's License, mDL, Privacy Preservation, Data minimization, Issuing Authority (IA), ICAO 9303 (CSCA – Country Signing Certificate Authority).

1. INTRODUCTION

A mobile ID (mID) can be perceived to mainly serve the purpose of secure face-to-face identification equivalent to electronic Travel Document transformed to "live" in a smartphone. eDocuments are well known to travellers as well as citizens around the world. Passport, residence permit card and national electronic IDs exist as electronic machine readable travel documents eMRTDs. Until today, the governing body for their standardization is driven by the International Civil Aviation Organization (ICAO) responsible for the coordination on several technical parameters of air travelling. ICAO has set a set of specifications in its ICAO 9303 specification to set a baseline of interoperability for eMRTDs. This baseline is a de facto standard adopted by EU as well as most parts of the world to assure interoperability for travelling. However, travel documents and IDs in card ID-1 format, well known from the bank cards used at ATM withdrawals, and passport booklets even electronically enhanced do need to bring them out of the wallet in order to use them therefore posing an obstacle on convenience and ease of use.

On the other hand smartphones are already widely adopted in EU and the world with rapid penetration to any country around the world. Mobiles have enabled ideas of mobile application to be used as a bank ATM card substitution. This has started a new line of electronic transactions of mobile payments. Smartphones are commonly used in an increasing manner at all ages. Therefore, we have reached the advent of an era when IDs are going into mobile smartphones to serve secure identification and enable privacy protection actively.

In this paper, we present the key use cases of mobile ID that are expected to receive wide adoption such as age verification especially sensitive to private preservation. To maximize adoption rate and assure interoperability, we have included in our proposed solution all possible communication options available in a modern smartphone such as NFC, BLE, QR and WiFi Aware. Another key success factor for mobile ID is following closely standardization specifications such as ISO 18013-5, we are participating in the development of ISO 18013-5, and supporting fully the latest "committee draft", AAMVA paradigms for mobile Driver's License and ICAO Doc 9303.

[1] Further author information: Send correspondence to Dr. Evangelos Sakkopoulos, University of Piraeus and Chief Technology Officer at Scytáles AB: E-mail: evangelos.sakkopoulos@unipi.gr, vsakkopoulos@scytales.com, Cell.: +30 693 74 57 502, +46 72 182 88 86 and Konstantin Papaxanthis, CEO of Scytáles AB: E-mail: kpapaxanthis@scytales.com, Cell.: +46 70 208 56 95.

We present a robust implementation for the uniquely widest possible range of smartphones independent of smartphone OS.

Closing the introduction chapter, we need to mention that approximately 1.4 billion people lacks of physical documents according to statistics from World Bank, which makes it more difficult for them in contacts with banks, etc., where an mID or mDL will help them a lot. Finally the interest in the new technology is great around the world. Above all, the US, Finland and the Netherlands are far ahead, as is Sweden. The world market today is large and one example is the driver license holders, which consists of 2.5 billion.

2. MOBILE ID: GIVE SCYTÁLES TO DATA MINIMIZATION

The key objective of a mobile ID is to demonstrate minimal and selective disclosure of personal information based on international standards like ICAO 9303 (e-Passport), and ISO 18013 (Driver's License) taking into consideration in particular latter part 5 going mobile, fully supporting the latest "committee draft" of the technical standard and in its latest almost final version for the mobile Driver's License (mDL) to be published Q2 2020, mID and mDL are used in this context interchangeably to show that a mobile ID may include more than identification of the individual holder of the smartphone. The ISO 18013 Part 5 will according to our predictions, be the backbone and a very important brick, for many countries schemes, enterprises and organizations for issuing/provisioning Mobile IDs to its users.

In this work we present that mobile ID is possible to be an effective instrument for data minimization enabling user active explicit consent to share pieces of personal information in cases that need i.e. age verification, address verification but also used in offline and online scenarios among others.

Figure 1. General Age Verification Flow

Instead of disclosing the full dataset of the mDL, the user provides the appropriate information about age, making proof of that one is older than minimum age established by law. At the moment the approach is designed to support attended cases. Verification should be made by an individual verifier and not an unattended system.

Depending on the IA's decision, a mDL may be available offline only or alternatively may also be online. Offline determines that both mDL holder and mDL Verifier are not connected to the IA through any network.

Online assumes connectivity between the mDL Verifier and the IA of the holder's mDL. All IA worldwide that is following the standard should be available for access by any mDL Verifier without any pre-registration. In the Online case mDL holder might also be connected to his/her IA (not any IA worldwide).

The following entities participate in this use case:

- Issuing Authority – Governmental, State Agency or Authority responsible that issues the ID.
- User – in the use case, the main user is the mDL holder, i.e. an individual that has an electronic Driver's License (mDL) in a mobile device.
- Verifier – an individual that needs to validate the identity and attributes of an mDL Holder. Examples of Verifiers are merchants and law enforcement agents.

The verification process is as follows:

1. User needs to prove age towards a relying party.
2. (optional) RP asks for ID for minimum age verification.
3. User uses mDL app and pairs with the Merchant's mDL Verifier (via NFC tap or QR-code), establishing a Bluetooth or NFC or WiFi connection as a second step.
4. User explicitly chooses to just share age proof that are transferred by the mDL app to the mDL Verifier through Bluetooth or NFC or WiFi.
5. Verifier checks the authenticity and integrity of the data using PKI Signatures (example CSCA) or other security schemes.

3. OFFLINE CASE

A proposed solution for the offline case where holder and verifier are both offline is presented below.

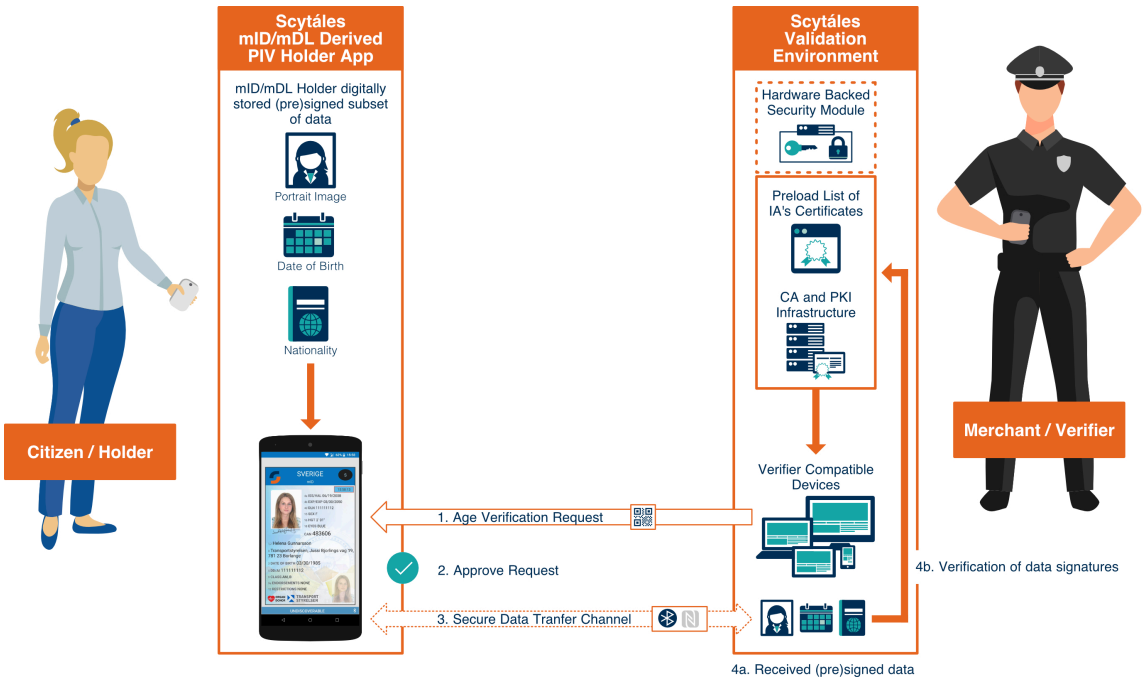

Figure 2. Offline Case Basic Flow – Age Verification Privacy Protection to Mock DMV – IA – IDP

4. ONLINE CASE

A proposed solution for the online case for verification towards Data minimization is proposed based on the ISO 18013-5 as it is currently 5.2019 that drives us to the following flow:

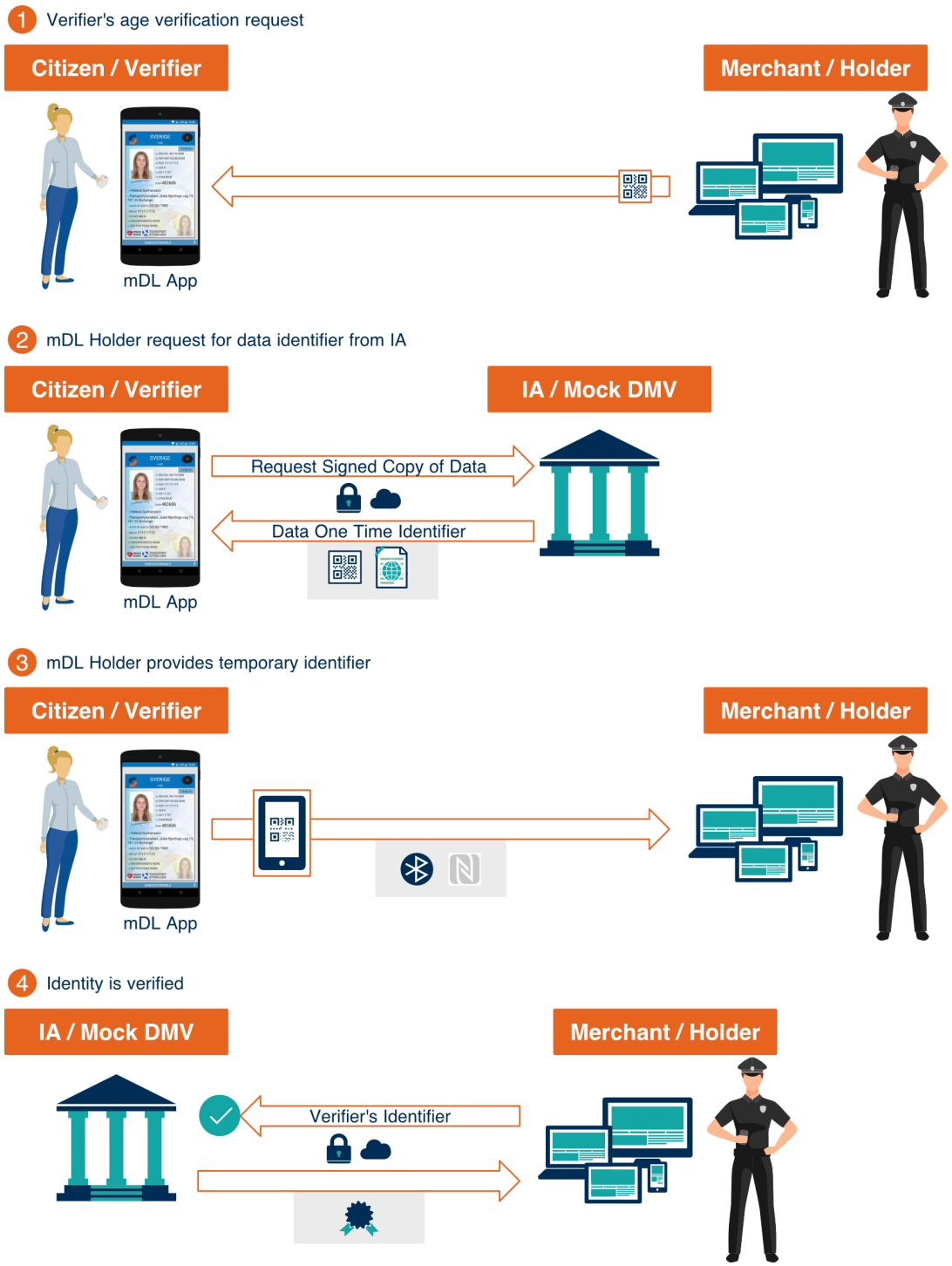

Figure 3. Online Case Basic Flow – Age Verification no Data on the Holder Device

Age verification is performed in person i.e. in attended cases from a relying party person.

In devices where there is hardware back security available, it is possible to store securely the amount of mDL data and to prevent unauthorized reading.

On rest of devices, risk assessment can be performed to allow storing the data in a software based secure wallet.

5. STANDARDIZATION FOR MOBILE ID: USE CASE

In order to achieve wide acceptance on the adoption of mobile ID last years have brought a number of key players and stakeholders at the round table of ISO standardization WG10 group of 18013 part 5 process. We present below the solution proposed that enables both offline and online use cases presented previously. The solution supports now Android and iOS devices allowing the widest possible choices for end-users and allowing any Issuing Authority to be assured that the approach will have a total success. The proposed solution has proven itself to be effective after passed international tests and end-user feedback already.

Figure 4. General Architecture of the mobile ID ecosystem proposed

6. CONCLUSIONS

This document describes an effective approach for a popular and well known Use Case where real world problems are hopefully resolved with the technology building blocks proposed. Most of the problems under research are related with data privacy and minimal disclosure of information through the use of mobile ID.

Next steps include unattended use case facilitation as well as zero knowledge proof incorporation of approaches into the eco system proposed.

7. REFERENCES

[1] Draft N1677 ISO/IEC CD 18013-5:2018(E), Information technology -- Personal identification -- ISO-compliant driving licence -- Part 5: Mobile Driving Licence application (mDL)

[2] Evangelos Sakkopoulos, Zafeiria-Marina Ioannou, Emmanouil Viennas: Mobile Personal Information Exchange Over BLE. 9th International Conference on Information, Intelligence, Systems and Applications, IISA 2018, Zakynthos, Greece, July 23-25, 2018. IEEE Computer Society 2018, ISBN 978-1-5386-8161-9, pp. 1-8

[3] ICAO 2015, Doc 9303, Machine Readable Travel Documents Part 1 — Introduction, ISBN 978-92-9249-790-3

[4] Article 2019-03-25 in Swedish in the daily newspaper Dagens Industri, Tjänstebilen, translated into English with the title “The driver license becomes a digital document” and message that our ID documents are about to be digitalized and transferred into the mobile. First out is the digital driver license that will be introduced in 2020 as a new service.