Digital and mobile identities

Holger Funke[1]

Abstract: In this paper current developments in mobile identities are described. A scalable architecture, standard future-proven technologies such as ISO/IEC 23220 and a Cryptographic Service Provider build the framework for secure, failsafe and large deployments. The building blocks specified in ISO/IEC 23220 deliver a framework that can be easily used for identities stored on secure devices such as smartphones. This paper lists a selection of outstanding projects using mobile and digital identities in the field of mobile ID. The focus is on Digital Travel Credentials (DTC) which are currently specified by the International Civil Aviation Organization (ICAO).

Keywords: Mobile ID, Digital ID, Digital Travel Credentials, Smartphone, Cryptographic Service Provider, eIDAS, identification

1 Introduction

As in many areas of life, a paradigm shift from ‘one size fits all’ to ‘bring your own device’ can be observed for the use of official documents. People have become accustomed to completing their daily tasks with their smartphone and now want to do the same with their eID card or eMRTD (electronic machine readable travel document). After all, they almost always carry their smartphone with them and are used to using it or even expect to use it for a wide range of applications. Examples include airport boarding passes or entrance tickets, which many people prefer to access digitally via their smartphones instead of in paper form. Rail transport passengers are also increasingly using their smartphones to store tickets and specific railway cards digitally.

Which technological options already exist for a digital or mobile identity and what international efforts are being made to uncouple official identities from their previous form factor and digitise them? One idea is the ‘ID Wallet’, through which the owner can manage and release a range of identities online and offline, from user ID cards and driving licences to passports. The smartphone is fast becoming the focus of such efforts and is playing an increasingly important role for users – particularly for identification and authentication. A survey conducted by the International Air Transport Association (IATA) in 2017 showed that air passengers want to use their smartphones more and more at the airport. Design and technical aspects of identification and authentication are playing an increasingly important role not only online, but also in the real world. Given the ubiquity of smartphones, it makes sense to use them to store identity data. Of course,

[1] secunet Security Networks AG, Division Homeland Security, Paderborn, holger.funke@secunet.com

the security of the data stored is of great importance, as it constitutes key information about each individual.

The guidelines of the German Federal Office for Information Security (BSI) [Fe19] and the EU's eIDAS Regulation [Eu14] therefore specify rules for the implementation of authentication procedures in order to achieve specific security levels. However, the smartphone should only be seen as a representative of an entire class of devices. In principle, other mobile devices can also be used for this purpose, for instance smart watches or wearables. Regarding the design and architecture, a few fundamental questions arise:

- Does an original identity already exist and how is it initially transferred to the smartphone derivation?
- Where is the identity data stored? On the smartphone? In the cloud? In a hybrid solution?
- Which interfaces are used to access the data and how is it secured?

The answer to the first question is relatively obvious in the context of official documents: the physical passport or ID card can be used as a secure trust anchor. In the case of emergency documents however, this original identity must be transferred to the smartphone in other ways, as temporary replacement of the document has taken place due to the loss of the original document.

What's even more interesting is the question about the location of the data. Two very different options present themselves here: the smartphone and the cloud. If the data is stored locally, precautions must naturally be taken to ensure that the data can only be read for legitimate purposes. Secure storage systems such as secure elements or smart cards (SIM cards), which are usually installed in smartphones, could be used for this purpose. Similarly, storing the identity in the cloud also requires cryptographic protection, typically using an asymmetric encryption key that requires special protection. In addition, you can combine the two methods and store parts of the data in the smartphone's secure memory and parts in the cloud. The choice of storage location then raises new questions, e. g. how an identity can be restored if the mobile device is lost or destroyed. One solution is My Identity App (MIA): a smartphone-based mobile ID implemented by Österreichische Staatsdruckerei [Tr16].

Just as interesting is the question of which interfaces should be used to read the data. In the context of official documents, the NFC interface offers a possible solution. This is similar to the ISO / IEC 14443 interface used for smart cards so that parts of it can continuously be used. However, there are also other interfaces under discussion, such as Bluetooth or QR codes. Deutsche Bahn uses a QR code for its tickets as a relatively robust interface between the traveller's smartphone and the ticket inspector's reader, for instance. The topic of mobile identities first became popular in the field of electronic driving licences. The standardisation groups that operate in this environment – such as ISO SC17 WG10 – have been working on the question of how to store physical driver's

licence data securely on a smartphone for several years. Since these mechanisms are not limited to driving licences, the technical requirements and proposed solutions are currently being discussed generically in working groups such as ISO SC17 WG3 or the New Technology Working Group (NTWG).

2 Related work

2.1 Cryptographic Service Provider

A fundamental basis for identification and authentication on a substantial level of assurance according to [EP14] is a Secure Element (SE). The SE is capable of hosting various third party applets, e.g. for identification, authentication, public transport, payment, etc. The installation itself of such an applet by a Trusted Service Manager (TSM) is independent from the concrete applet. The administration of applets (loading, installation, deletion and personalisation) can be implemented based on Trusted Service Management Systems (TSMS). Generally the security mechanisms of the applet hosted by the SE can also be proven by security certification. Usually Common Criteria demands a composite certification of the applet in conjunction with the underlying Protection Profile of the underlying SE. To allow installation of CC-certified applets without the need of a Composite Certification of the applet on top of each type of SE, the cryptographic functionalities are encapsulated in a Cryptographic Service Provider (CSP), providing secure cryptographic services to the applet. Since the CSP's security services are logically separated and provided through well-defined external interfaces, the operational environment cannot affect the security and correctness of the CSP. Consequently, the security functionalities of the applet can be certified independently. All functionalities can be implemented on the SE itself or alternatively the SE can provide a key store/management back end for a CSP implemented outside of the SE. In both cases, the Secure Element itself must be certified on at least Assurance Level EAL4+AVA_VAN.4. [Kü20]

2.2 ISO/IEC 23220

This standard series provides building blocks for mobile eID System infrastructures and normalizes protocols, interfaces and services for mobile eID Apps and mobile verification applications. This is done by specifying generic system architectures of mobile eID Systems, generic transaction flows of mobile eID Systems and generic lifecycle phases of mobile eID Systems. One important part of this standard is the secure area of a secure device which can be implemented by several types of secure elements, e.g. embedded universal integrated circuit card (eUICC), embedded secure elements (eSE) or Trusted Execution Environments (TEE) [ISO20].

3 Current projects around the world

3.1 Mobile Driving Licence

The mobile Driving Licence (mDL) was the first popular initiative transferring an ID onto a smartphone. Based on existing chip-based electronic driving licences standardized in ISO/IEC 18013 [ISO18] a mobile driving licence is specified in this series now. The purpose of this standard is to standardize interface specifications for the implementation of a driving licence in association with a mobile device. It standardizes the interface between the mDL and mDL Reader, and the interface between the mDL Reader and the issuing authority infrastructure. Key functionality is the access to the security anchor of the smartphone. To authenticate the origin of the mDL data and to verify the integrity of the mDL data, it is necessary to get access to the secure element that is used in the smartphone. Therefore, the mDL uses protocols that are standardized in ISO/IEC 23220.

3.2 Digital Travel Credentials

In 2016 the ICAO New Technologies Working Group (NTWG) established a specialised subgroup in cooperation with the International Organization for Standardization (ISO) to standardise digital travel credentials (DTC). Such credentials can be issued or applied in a digital format, e.g. on smart devices or on servers. A DTC could temporarily or permanently substitute a conventional passport by a digital representation of the traveller's identity. To assure security and convenience a DTC has to provide similar functionality and security features that are comparable to those of a current eMRTD. The role of ICAO is to define policies and use cases in this context; the role of ISO is to specify technical guidelines.

One important advantage of an eMRTD is the digitisation of the traveller's biographic and biometric data stored in a chip embedded in the document. The chip data already offers many benefits, including the verification of the passport holder's identity through facial recognition and providing authorities with the tools to verify and to authenticate the ePassport. Therefore, the eMRTD is the template and the reference for the idea of digital travel credentials. The ICAO has defined several core principles for DTC in [IA18]:

- The DTC must be at least as secure as an eMRTD.
- The information contained in the DTC must be derived from the Travel Document Issuing Authority's data, and may come directly from the eMRTD.
- The lifecycle management of the DTC must not necessarily be dependent on the lifecycle management of the eMRTD.
- Incompatible changes must not be required in the current eMRTD standards or in the current process of issuing eMRTDs.

- The revocation of a DTC may result in a revocation of the eMRTD associated with this DTC at the discretion of the issuing State.
- The revocation of the eMRTD must automatically revoke all underlying DTCs.
- The DTC must be issued by a Travel Document Issuing Authority.

3.2.1 Form factor of DTC

A number of different form factors for storing a DTC have been evaluated by ICAO, and at the end the preferred one is a hybrid model that would consist of a virtual component (DTC-VC) and a physical component (DTC-PC). The virtual component acts like a credential that is linked to at least one physical component (authenticators). The technical specifications are developed by ISO SC17 WG3 and contain protocols, data structures and PKI [IA19].

The benefit of a hybrid travel credential is the combination of a virtual and a physical travel credential in a way that the advantages of both approaches are merged while the disadvantages are minimised.

To achieve this, a virtual travel credential is linked to one or more physical devices that perform additional active authentication or chip authentication of the credential when required for increased security. A hybrid travel credential may be used as virtual travel credential alone where cloning protection may be arranged differently. In use cases where a stronger binding is required, it may additionally be verified that a linked physical token (the eMRTD) is in possession of the traveller, e.g. through biometrics.

Today an eMRTD can already be considered as a hybrid travel credential using the logical data structure (LDS) as virtual travel credential and active authentication or chip authentication implemented on the chip as the physical token. The virtual credential may also consist of the data stored in a remote system, e.g. a database or a web service, with the physical authenticator being a smart device (e.g. a smartphone) that can be used to retrieve the data from the remote system by authenticating the holder of the physical credential to the remote system.

This is preferred as the credential is already linked to the issuer by passive authentication. The physical token allows the verifier to select the correct virtual credential, with the added benefit of this being potentially provided in advance. It also provides the verifying authority with the flexibility to decide whether the virtual credential is sufficient or the physical authenticator is additionally required for authentication.

The following matrix explains the mapping between the three options defined in the mentioned policy paper and the specifications contained in the technical report:

	DTC-VC data identical to existing eMRTD	DTC-VC data not tied to any existing eMRTD
No separate DTC-PC	Self-Derived	(Not defined)
DTC-PC tied to DTC-VC	Authority Derived	Authority Issued

Tab. 1: Mapping of eMRTD and DTC

3.2.2 Interesting use case

A digital representation of an emergency travel document could be a first use case for the DTC. This solution allows a flexible process to support travellers who lost their ePassport and who are now in need of urgent travel documents yet in a location where delivery of a standard ePassport is either impossible or unfeasible.

In an emergency case a traveller could apply for an urgent renewal enabling the issuing authority to issue a hybrid DTC: essentially a virtual credential with a linked verified physical authenticator provided remotely to the smartphone of the traveller. The citizen could then travel back home or to a location where the ePassport could be collected. This way requires that the DTC is acceptable for travelling (exit and entry for all crossed borders) without the physical passport in the traveller's possession.

The following first projects have started where DTC are used:

- Known Traveller Digital Identity (KTDI) funded by World Economic Forum [KT20]
- New Zealand and Australia are using biometric and logical data structures in a frequent traveller program
- IATA One ID: Document-free process at airport based on identity management and biometric recognition [OI20]

3.3 OPTIMOS 2

OPTIMOS 2 aims at creating an open, usable and secure identity ecosystem for mobile services. Goal of the project is to supply a platform for eID-providers and enable them to offer mobile eID services at eIDAS level "substantial". Another goal is to offer service providers - relying on a certain security level - a secure, privacy friendly platform for mobile services. To assure this security level, access to a secure element of the smart device is essential. The derived holder data (in this case derived from the German ID card) is securely stored in the secure element of the smartphone. A Trusted Service Manager (TSM) grants access to the secure element and allows secure and authentic storing of holders data.

4 Outlook

This list of outstanding projects in the context of mobile ID shows the importance of this topic. Today it is already possible to store eID data on a smartphones with eIDAS level “substantial”. As soon as the standards are finalized and officially released they will be the base for several projects and new use cases for mobile identities. The use case “emergency travel document” might be the first milestone in the area of travelling with derived credentials stored on smartphones.

Bibliography

[Fe19] Federal Office for Information Security (BSI): Technical Guideline TR-03159 Mobile Identities, August 2019

[Eu14] European Parliament, Council of the European Union: Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[Kü20] Kügler, Dennis (BSI): Identities Go Mobile - The Future of Electronic Identification. In: Omnisecure Proceedings 2020, Berlin

[IA18] ICAO: Policy paper – Digital Travel Credentials, 24.10.2018

[IA19] ICAO: Technical Report – Digital Travel Credentials, Version 0.7, 13.08.2019

[ISO18] ISO: Information technology - Personal identification - ISO-compliant driving licence, 2018

[ISO20] ISO: Card and security devices for personal identification - Building blocks for identity management on mobile devices, 2020

[KT20] Website: Known traveller digital identity: https://ktdi.org/ (last accessed 06.04.2020)

[OI20] Website: IATA One ID: https://www.iata.org/en/programs/passenger/one-id/ (last accessed 06.04.2020)

[Tr16] Terbu, Oliver. et.al.: One mobile ID to secure physical and digital Identity. In (D. Hühnlein, H. Roßnagel, C. Schunck, M. Talamo, ed.): Open Identity Summit 2016, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016