Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-SIT

Seidlgasse 22 / 9, 1030 Wien
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

Inffeldgasse 16a, 8010 Graz
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

DIGITAL ID CARDS

Version 2.0 from 20.02.2021
Author – Emina Ahmetovic emina.ahmetovic@egiz.gv.at

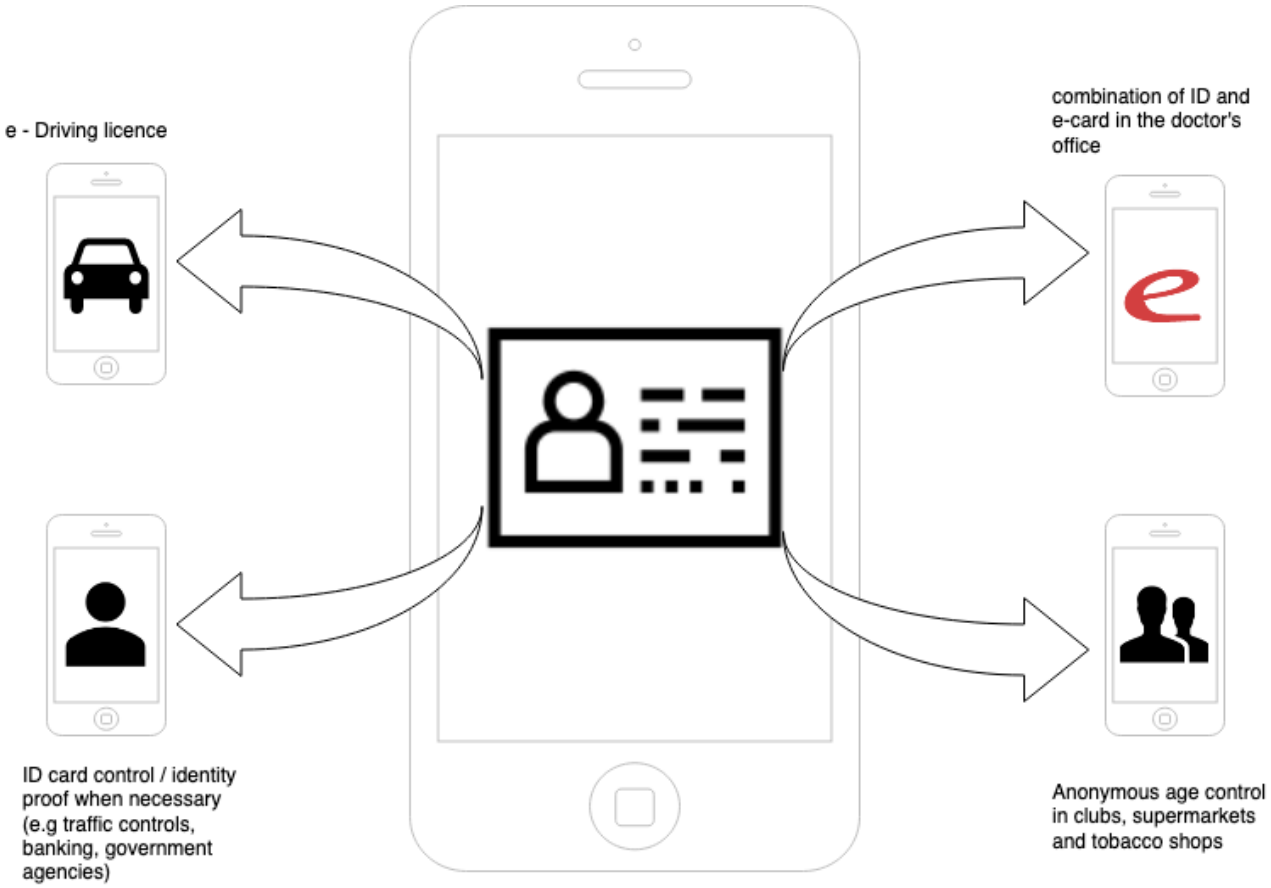
Physical credentials are omnipresent in our everyday lives. Either they are in the form of a bank card, driving license, certificate, health card, passport, or any sort of ID, it is sure they are used on an everyday basis, and that they influence our daily workflow. The use of physical credentials is well structured and defined. However, physical credentials in an electronic or mobile context bring a lot of opportunities, but also come with lot of requirements and challenges. As a part of this project, we aim to give a bigger picture of the mobile solutions that would provide mobile identity verification. We outline the benefits and use cases we would have, and we discuss their security and privacy requirements.

Table of Contents

1. Introduction

Credentials in a form of a driving license, passport, plastic cards, and similar, are a major part of our daily life. In a physical world, people need to make certain claims on an everyday basis, whether to get access to a resource or to gain certain privileges. For instance, driving licenses serve as means to convey driving privileges; passports are used to enter foreign countries; student IDs are required when taking an exam. While there are numerous examples, it is sure that the usage of credentials in a physical world is very beneficial for users and well defined.

However, the use of machine-verifiable credentials in an electronic context is shown to be elusive [1]. Moreover, with the prevalence of mobile devices in everyday life, it is quite apparent that electronic verification function should also be available on the smartphone in the future. Providing a digital identity card on a smartphone comes with a lot of opportunities. However, such a solution comes with a lot of challenges. It is required that such a solution is accessible in both offline and online scenarios, interoperable, and enhance usability. For this reason, in the following sections we focus to outline the importance of this work by defining use cases, and security and privacy requirements accordingly.



1.1. Benefits

Mobile technologies in general provide a wide range of benefits for both business and government. Accordingly, providing the functionality of physical cards on a mobile ecosystem gained a lot of attention in the last years. Both public and private sectors are investing in mobile solutions that can be used by a large number of citizens.

In general, the entire concept of digital identity cards provides a wide range of benefits, regardless if they are used as driving licenses, ecards, student IDs, or passports. The Association of European Vehicle and Driver Registration Authorities (EReg Association) summarizes some of the main benefits of the non-physical driving licenses in their technical report [5]:

- **Up-to-date information**. One of the most important features of the mobile identity concept is the ability to always retrieve the latest data. If we take into account mobile driving licenses, this property eventually contributes to increased safety in traffic. If a driving license from a person trying to rent a car has been revoked, this information will be visible to the renting companies who can act accordingly and prevent a person from renting the car. The fact that renting agencies are at the disposal of real-time information can have a significant impact on the overall safety of roads.

- **Increased privacy**. Mobile solutions in general can contribute to enhance privacy and allow users more control over their data. Users are in sole possession of their data and they decide to whom and what data they want to share.

- **Cost and time savings**. In general, mobile as well as electronic services in the e-Government domain provide easier access to public services and therefore make significant time and cost reductions.

- **Environment effect**. One of the additional benefits is that mobile technologies would replace plastic cards and save resources, which leads to fulfilling environmental goals, as one of the urging topics in the world.

1.2. Use cases

A mobile app would replace physical cards or supplement them in the following cases:

- Mobile driving license – required police controls the drivers to validate their driving privileges
- E-card – required when entering a doctor´s office.
- Identification cases – by entering certain facilities, some kind of identification document is required, such as a passport at the border check, hotel check-in, bank visits, and similar.
- Age control – required when entering clubs, buying alcoholic drinks, and similar.

In terms of use cases, we also distinguish:

1. Use digital IDs in F2F: For example, a scenario where police stop you. In this case, we would have:
   - Offline use case: it is not required for a device involved in the transaction to be connected to the Internet.
   - Online use case: requires that devices involved in the transaction are connected to the Internet.

2. Decentralized use case: the digital ID is used as identification means towards an online SP. However, no central identity provider/platform is involved. This corresponds to the self-sovereign identity (SSI) concept.

2. Background

In this section, we outline some of the main concepts for digital IDs We first start with the introduction and current developments in the field of mobile driving licenses, and then we introduce the concepts of verifiable credentials and decentralized identifiers.

2.1. Mobile Driving Licences (mDL)

A driving license, as an official document granting the holder of the document right to operate one or more types of motorized vehicles, is currently owned by 60 percent of population in EU. This number amounts 75% in the UK [2], and 227.5 million of population in the USA [3]. These numbers increase every year and rank driving license as one of the most used official documents.

Nevertheless, a driving license has undergone many development stages. First driving licenses were paper-based with a handwritten text and official stamps, while in the next iterations they were made as polycarbonate cards with physical security features such as ultraviolet ink or holograms [4]. In 2013, a 3rd European Directive on driving licenses (2006/126/EEC) came into force with the aim of aligning driving licenses rules in all EU member states. Publishing driving licenses under uniform EU format and security framework provides more freedom of movement for holders, more safety on road and less frauds. In 2014, traditional licenses evolved into electronic driving licenses in countries such as Croatia [5].

The uprising popularity of mobile devices is now shaping a new evolution phase for driving licenses. The prevalence of smartphones in everyday life brought a strong demand for mobile solutions. Easily accessible mobile service are not only dominant in private sector; public sector as well is interested into mobile technologies that can be used by majority of population, save time and reduce costs. This leads to the expectation that driving licenses should be available on mobile devices. While it is not likely that mobile driving licenses, or shortly mDL, are supposed to completely replace physical ones, it is sure that a lot of research is directed in empowering mobile driving licenses to be accessible in both offline and online cases, interoperable between different issuing authorities and protect user data.

2.1.1. Stakeholders

In this subsection, we outline some of the stakeholders for the architecture of mDL that has been described in [6]:

- **mDL holder.** An entity that uses mDL with the purpose of confirming identity or gaining driving privileges.
- **mDL**. Mobile driving license. This non-physical driving license complies with the majority of requirements for a traditional driving license described in with ISO/IEC 18013-1; however, it is stored on a smartphone or tablet.
- **mDL reader**. Device that can retrieve mDL data for verification purposes.
- **mDL verifier**. mDL verifier is a person or organization using and/or controlling an mDL reader to verify an mDL.
- **Issuing authority**. Infrastructure under control of the issuing authority.

2.1.2. Use cases

As driving licenses are officially used to permit an individual to operate one or more motorized vehicles, it is not their only purpose. In a lot of cases, a driving license can replace an official ID and serve as an identification document. In the following, we elaborate on the possible use cases that involve a mobile driving license. Thales Group [10] defines four main use cases for mDL:

- **Police control.** Police can stop a driver of a car to check for his identity and his driving privileges. This is one of the most common cases that involve mDL as a means to convey driving privileges.
- **Proof of age.** Vendors of alcohol are allowed to ask for age conformation, as the purchase of alcohol is restricted to individuals more than 18 years in the EU and 21 in the US. For this purpose, a mobile driving license can serve as identity proof.
- **Identity validation or confirmation.** A lot of other institutions are also accepting driving licenses as a means to confirm identity. One of the examples is hotels and many other public facilities.
- **Car rental.** Car rental agencies are another institution that could use mDL.

2.1.3. Standardization

The first steps towards the standardization of the mobile driver licenses have been paved, however, standards are still not fully defined. We outline following documents:

- Digital Driver License -ISO SC17 WG10 –Task Force 14 –Mobile Driver's License (ISO 18013-5) [6]
- Mobile Identity–ISO SC17 WG4 [7]
- AAMVA mDLWorkingGroup –Standards for NorthAmerica [8]
- Digital TravelCredentials–ICAO Compliance group & ISO SC17 WG3 [9]

2.2. Verifiable credentials

Verifiable credentials represent an electronic equivalent to physical credentials. The data model for verifiable credentials is described in the "Verifiable Credentials Data Model 1.0 - Expressing verifiable information on the Web" [1] by the W3C Recommendation published on 19 November 2019. The VCs ecosystem distinguishes four main stakeholders:

- **Holder** - holders are users that can be either students, employees that are in possession of verifiable credentials and want to make verifiable presentations from them.
- **Issuer** – issuers can be governments, corporations, non-profit organizations, and similar. Their role is to assert claims about subjects, to create verifiable credentials from the claim, and to transmit it to a holder.
- **Subject** – subjects can be humans, animals, or things. Claims are made about the subjects, and it can be that a holder of VCs is a subject; however, there are situations when that is not the case; it can happen that a parent is a holder of a verifiable credential of a kid (that is subject in this case).
- **Verifier** - a verifier represents an entity that receives and processes verifiable credentials. Verifiers can be websites, employers, and similar.
- **Verifiable data registry** - is an entity that can be decentralized databases, distributed ledgers, or similar. They represent an entity that mediates the role of creation and verification of data that can require to use verifiable credentials.

To summarize, the issuer creates a claim associated with some subject, while the role of holders is to generate verifiable presentations of the verifiable credentials, and it is up to verifiers to prove the subject possess verifiable credentials with certain characteristics.

2.3. Decentralized Identifier (DID)

Decentralized identifiers (DIDs) are identifiers that are used to create verifiable, decentralized digital identity [14].

The important feature of DIDs is that they are separated from the centralized registries - A DID identifies any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) that the controller of the DID decides to, which distinguishes this model from the traditional federated identifiers. DIDs are defined as URLs that associate a DID subject with a DID document.
Some components of the DID architecture are:

- **DIDs and DID URLs.** Decentralized Identifiers or DIDs represent a URL consisting of:
  1. A scheme “did:”
  2. A method identifier
  3. Unique method-specific identifier that is generated by a DID method. DID URL represents an extension of the basic DID syntax that includes the ability to include other URI components such as path, query, and fragment. This logic is necessary, for instance, for locating some services external to the DID document or public keys inside the DID document.

- **DID Subject.** The entity identified by DID is a DID subject. DID subject can be a person, organization, group, logical or physical thing, etc.

- **DID Controller.** Entity (person, organization, or autonomous software) that has the capability defined by a DID method to make changes to the DID document is a DID controller. Such a capability is typically defined by the cryptographic keys control on software that the controller is using. It is important to note that DID can have more than one controller. Also DID subject can be the DID controller.

- **Verifiable Data Registries.** DIDs are recorded on Verifiable Data Registries that can be either systems or networks, such as decentralized file systems, peer-to-peer networks, databases, etc. Whatever underlying technology is used, Verifiable Data Registries should be able to record DIDs and return any data necessary to produce DID documents.

- **DID documents.** DID documents contain metadata related to DIDs. DID documents can also be expressed as verification methods (such as public keys) and services necessary for the interaction with the DID subject.

- **DID methods.** Creating, resolving, updating, and deactivating DIDs of a particular type and related DID documents in a verifiable data registry is defined by DID methods.

- **DID resolvers and DID resolution.** DID resolver represents a software or hardware component that based on an input DID (and related metadata), creates an output DID document (with related metadata). Such a process is called DID resolution.

- **DID URL dereferencer and DID URL dereferencing.** A DID URL dereferencer represents a software or a hardware component that based on an input DID URL (and related metadata), creates an output resource (with related metadata). Such a process is called DID URL dereferencing.

3. Requirements

Public services aim to provide high-level security and privacy-preserving solutions without sacrificing usability. However, moving the application ecosystem to a mobile device comes with a lot of challenges. One of the main tasks of this project is to define security, and privacy features should be considered when designing a solution for mobile solutions. The requirements are diving into two categories that are the topic of our interest; however, they are not the only ones. In this section, we provide an abstract high-level definition of requirements to encapsulate the wider focus.

3.1. Security requirements

- **Confidentiality** – a property that information is not made available or disclosed to unauthorized individuals, entities, or processes [11]. In other words, confidentiality as a security property assures that only authorized users can gain access to data. A failure in complying with this feature leads to a breach, a state where access to private data has been compromised and where someone gained access to unauthorized data.

- **Integrity** - property of accuracy and completeness [11]. Integrity refers to security property where the source of information is genuine, and information has not been altered. Alteration of the document is only allowed by the authorized users.

- **Availability** - data are available to authorized users. Availability, as one of the security properties, assures that your data can be accessed on demand at any time. Availability, as well as integrity and confidentiality, plays an important role in providing public services since one of the pillars of e-Government is data accessibility 24/7 [13].

- **Authentication** - property of recognizing a user's identity. Authentication represents a proving an assertion. In contrast to the identity, where a person claims it is someone, the authentication represents a process of verifying that identity. The process of verifying includes representing personal identification documents, such as IDs, or it can be creating digital signatures.

- **Authorization** - the process of giving someone permission to access something or have something. Authorization can be defined as a security mechanism used to determine the privileges of a user, or access level to specific resources. Authorization is usually followed by user authentication and proving the alleged identity.

- **Non-repudiation** - Non-repudiation is the assurance that someone cannot deny the validity of something. This means that the sender of data has proof of delivery and the recipient of data is provided with proof of the sender’s identity, so neither of them can later deny having processed the data [12].

3.2. Privacy requirements

Mobile driving license standardization extensively describes privacy recommendations [6] that can be easily applied to general solutions in the domain of mobile identities. It should be noted that in this section, we summarize the most general privacy properties; however, the concrete implementation of these properties strongly depend on the use cases.

- **Consent and Choice.** - No user data should be shared with any other party without informed consent. Informed Consent dictates that the data holder will be given sufficient informed just-in-time notice about the data being requested, the entity requesting the data, and the purpose for the request. Users must consent to the processing of her personal data. In addition, users need to have a choice of giving the access to their personal data.

- **Purpose Specification.** - Users should be fully aware of the purpose their personal data is being processed.

- **Collection Limitation.** - User data should be collected only for a specific purpose, and data collectors should collect only data necessary for the transaction purpose. On the other hand, data holders should only respond with data that has been asked from them and not disclose more.

- **Data Minimization.** - Processing of data should be minimized for the purpose specified. Additional data can be disclosed only in the case that disclosing minimal data was not enough to fulfill the requirements of the first use case. Additionally, data groups need to be separated into individual blocks to ease data transmission and comply with data minimization.

- **Use, Retention, and Disclosure Limitation.** - Personal data of the user should not be used except for the purposes specified and consistent with these other principles.

- **Openness and Transparency.** - Users should be aware of how and what data is being processed. Users or data holders should always be given the ability to consent to the sharing of that data and be informed of the onward storage of that data. The consent would contribute to the higher transparency of the used data.

- **Individual Participation.** - Users should be involved in the collection, consent, processing, and storage management of their personal data.

- **Information Security.** - Personal data should be protected by security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.

- **Privacy Compliance, Accountability and Auditing.** - Data processors should be accountable for all aspects of processing personal data.

- **Anonymity and Unlinkability** - According to ISO/IEC 29100 [16], anonymity is defined as a "characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly". In practice, this means that in case of different transactions with different set of attributes, it should not be possible to link them to the previous ones.

4. Discussion

In this document, we tend to cover a wider range of privacy and security properties. However, it should be noted that some of the privacy considerations need to be taken into account. The concrete instantiation of the properties strongly depends on the use case. For this reason, privacy and security properties could be defined on a different spectrum, from those that are considered non-correlated to those considered highly-correlated. This means that for entering a night club, probably the only information required to be delivered is whether the holder is above 18 or not. The same could apply for buying alcoholic drinks in retails, and in these cases, it is desired that information, such as name or similar, remains undisclosed. However, it should also be noted that for other scenarios, such as for acquiring medical insurance policy, more user data need to be disclosed. Hence, we can conclude that there is no single approach that would satisfy every use case for privacy and security properties, but that it strongly depends on a use case. The metric between a concrete use case and privacy properties should be covered as a part of the future work. Moreover, future research should focus on analyzing current market rollouts and research done so far.

5. Bibiliography

[1] Verifiable Credentials Use Cases - W3C Working Group Note 24 September 2019 https://www.w3.org/TR/vc-data-model/

[2] RAC Foundation 2020. https://www.racfoundation.org/motoring-faqs/mobility

[3] https://www.statista.com/statistics/191653/number-of-licensed-drivers-in-the-us-since-1988/

[4] 2020 The Silicon Trust. https://silicontrust.org/2019/11/22/mobile-driving-license-vs-electronic-driving-license-replacement-or-supplement/

[5] EReg Association of European Vehicle and Driver Registration Authorities. https://www.ereg-association.eu/media/2024/finl-report-tg-xix-on-non-physical-driving-licences.pdf

[6] ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application https://www.iso.org/standard/69084.html

[7] ISO/IEC JTC 1/SC 17 Cards and security devices for personal identification https://www.iso.org/committee/45144.html

[8] American Association of Motor Vehicle Administrators. https://www.aamva.org/mDL-Resources/

[9] ICAO. https://www.icao.int/Meetings/TRIP-Symposium-2019/PublishingImages/Pages/Presentations/Digital%20Travel%20Credentials.pdf

[10] 2019 Thales Group. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/driving-licence/digital-driver-license

[11] ISO. https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en:term:2.61

[12] National Institute of Standards and Technology NIST. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf

[13] Abraham, A., Hörandner, F., Zefferer, T., & Zwattendorfer, B. (2020). E-Government in the Public Cloud: Requirements and Opportunities. *Electronic Government*, *16*.

[14] W3C. Decentralized Identifiers (DIDs) v1.0 https://www.w3.org/TR/did-core/

[16] ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework https://www.iso.org/standard/45123.html