A-SIT Technology
E-Government Innovation Center

27 November 2020 Study · Digital Identity · Mobile Security · 37 min read

DIGITAL ID CARDS

Archived. This content is no longer updated. It remains available for reference.

Source https://technology2.a-sit.at/en/publications/digital-id-cards/

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 a 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.

1. Introduction

Identity cards, such as passports, IDs, bank, or health cards, represent an important asset in our wallet. They serve as an identification means to acquire a service or to gain a certain privilege. Whether we gain driving privileges, bank transactions, medical assistance, or permission to enter a foreign country, it would be impossible to imagine daily workflow without some sort of ID document in our wallet. Among other advantages, identity in a physical world is well defined and structured. The possession of the physical cards is a must-have in a well-organized ecosystem, where each stakeholder knows their role. However, in the last decades, we have witnessed the digital migration of physical identity cards, introducing the term digital identity. Today, digital identity emerged as one of the most significant technology trends in the world [1]. Governments, as well as the private sector, have recognized the potential and benefits and invested in technologies that will be a major part of the digital future. Digital identity plays an important role for citizens by enhancing user experience and providing remote access to public services [2]. On the other side, the e-Government sector is able to provide personalized service to citizens, which eventually would result in increased usability, reduced costs, time and money savings, and better connectivity to citizens.

1.1. E-Government goes mobile

Nevertheless, if we reflect on the trends in 2020, we can observe that digital identity is becoming more and more mobile. With 3.5 billion smartphone users in the world and a forecast to further grow [3], the smartphone era is making demands on the public sector to design and develop a solution that provides access to public services from a smartphone. Mobile IDs, as digital identities that reside on mobile devices, have emerged as a particularly interesting topic for researchers in the E-Government domain. Already in 2015, it is discussed that mobile IDs have a possibility to become a major means of identification; however, it is still a long way from guiding the secure implementation of mobile id solutions that would fulfill standards [4]. It is also pointed out that challenges in terms of regulations and standards still have not been correctly and fully defined.

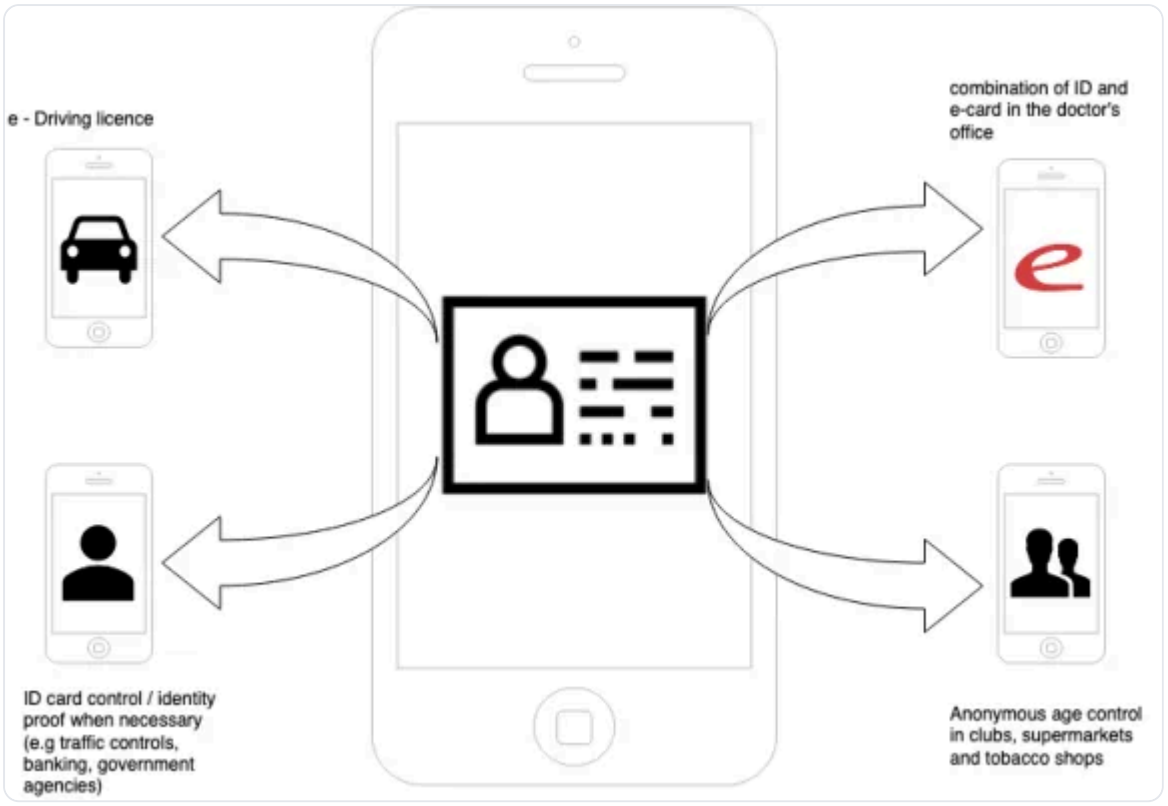


Figure 1. Physical ID cards replaced by a single digital card.

1.2. Opportunities

The potential of the digital ID system in a mobile domain has been recognized early. There are many reasons why both the public and private sectors are more and more interested in designing and developing solutions that support digital identification on mobile devices. First of all, one mobile ID App would replace a lot of physical identification cards and could be used in the following use-cases. Figure 1 depicts the most common use cases:

- e-Driving licenses: The mobile id app would have the potential to either replace physical driving licenses or to supplement them. Either way, the mobile driving license would have the same role as the physical one - as a means for the drivers to convey the driving privileges or as a means to confirm identity [5].

- Identity card: Mobile identity App can be used for identification purposes that are required by entering some institutions, in banks, obtain social services, hotel check-in, voting privileges, and similar.
- In combination with e-card to get an access to medical care, or medical assistance.
- Age control: As purchasing alcohol is restricted only to buyers above a certain age a mobile id application could be used as an age confirmation tool. Similar can be applied to the use case of entering night club.

From the above-defined use cases, we can conclude there are many benefits of having a digital identity functionality on a mobile device. However, the listed use cases are not the only ones, as the true spectrum of use cases is much bigger. For instance, mobile devices are architecturally suitable to serve as a means to electronically sign a document [6], banking activities, and much more.

EReg Association [7] already described some of the key advantages of mobile driving licenses in their technical report. These advantages also represent the overall benefits of replacing physical cards with mobile. As explained in the report, one of the main benefits is the ability to dispose of **up-to-date information** . For example, in a non-physical driving license - mDL, the up-to-date information directly correlates to road safety. 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 significantly impact the overall safety of roads.

Another feature of digital identity solutions residing on mobile devices is certainly an opportunity to **increase users' privacy** . In the following sections, we will further explain privacy properties and their potential and how they can contribute to enhance privacy and allow users more control over their data. Users should be in sole possession of their data, and they decide to whom and what data they want to share. Today, physical cards do not provide opportunities to hide or omit certain kinds of information. For example, when entering night club, it is necessary to prove you are above a certain age, but it is not necessary to disclose your age or any other information. The possibility for implementation of minimal disclosure clearly is one of the biggest advantages of digital solutions compared to physical cards.

Moreover, mobile as well as electronic services in the e-Government domain provide easier access to public services. Utilizing public services leads to the high **cost and time savings** . Citizens are not required to visit administration offices and by simplifying the administration processes and therefore make significant time and cost reductions.

One of the benefits worth outlining is certainly an **environmental effect** . Mobile technologies would replace plastic cards and save resources, leading to fulfilling environmental goals, as one of the world's urging topics.

1.3. Challenges

Credentials are omnipresent in our everyday life. We use different types of cards to assert us in dayto-day activities. Although m-Government, as the mobile transformation of e-Government, is a rising trend, and many countries do recognize the potential of mobile services, the examples of active use cases still remain rare. On the one hand, government agencies find it hard to include a mobile-first strategy on already

existing solutions that are not designed in the manner to support mobile in the first place. On the other hand, although Digital ID brings, without doubt, numerous benefits, governments are also faced with numerous challenges, such as exclusion risks, privacy, and data protection, costs, and sustainability [8]. From a political perspective, creating a digital identity is a task that requires aligned vision and collaboration between multiple stakeholders. It should define the roles, entitlements, and right between multiple parties, which adds to the complexity of the entire process [35]. Many authors agree that assuring privacy and data protection is a key factor for the adoption of digital identities, and they should be based on the legal and technical frameworks.

1.4. Our contribution

In this report, we try to shed light on the current status of digital identities on a mobile device. We argue that mobile ID inevitably responds to the urging demand of citizens to go mobile, brings a lot of benefits, and strongly assumes that mobile will become the preferred means of authentication. However, we also argue that the mobile identity solution will be able to employ its true potential only when the necessary security and privacy requirements are addressed and correctly instantiated. Since the work that has been done so far has not fully addressed the requirements, in this report, we try to pave the path towards a better understanding of this topic. Thus, this report reveals the bigger picture; however, it does not seek to explore the high-level technical details in current implementations.

We will look at the current deployment of mobile identity card solutions. As a part of this report, it is crucial to encourage the adoption of such a solution by outlining the advantages and opportunities they bring for both the public and private sectors. We discuss different case studies and we review the current state-of-the-art solutions for a digital identity on a mobile device.

1.5. Outline

This report is structured as follows: In the section 2, we discuss the related work and we also give a short summary of the general requirements. In the section 3, we discuss requirements for the implementation of the digital identities in mobile domain, while the section 4 introduces the most relevant technologies that can be used in designing and implementing such a solution. In addition, in section 4 we also provide a matrix of relevant use cases in domain of mobile identities. Lastly, in section 5 we outline the practical study cases from four implementations.

2. Related work

Mobile identity solution has been a topic of scientific interest for many years now, especially since the success story of smartphones and mobile connectivity as a key enabler on a global scale for a digital transformation plays an important role [9]. In [10], the authors state that the government and private sector would benefit from an electronic identity system that provides easily accessible identification for both electronic ids and physical ids. They also express the urging demand of governmental institutions and businesses for mobile id solutions, anticipating that the demand will have an upward trend. They propose a solution for digital representation of id documents in Austria, and they follow a centralized approach, outlining the disadvantages of decentralized use cases. Furthermore, other solutions show the use cases where mobile identity applications can improve a health care system, leveraging the current Austrian health card infrastructure with extended functionality by introducing an equivalent of a patient's physical health cards on a mobile device [11].

The mobile application has a great potential to serve as a social-economic enabler. Mobile communication that can establish a citizen's identity discloses a full range of benefits for public service and poses an important social and economic factor. Governments would benefit from costefficiency since digital, compared to paper, is economically more efficient [12]. They would also provide better security by applying correct cryptographic mechanisms and better flexibility by managing identities remotely. Lastly, it would provide better connectivity, as the citizens could access services anytime and anywhere with minimum requirements.

One of the countries that have a pioneering role in establishing digital and mobile eID is Austria. The Austrian eID was first introduced in 2003. One of the core components in the Austrian e-Government processes is the Citizen Card Concept, a concept for transferring a user's identity into electronic identity and enabling users to authenticate themselves against the remote service. One of the implementations of the Citizen Card Concept is the Mobile Phone Signature. The Mobile Phone Signature, or Handy-Signatur, represents a usable alternative to the traditional approaches that rely on additional hardware such as smartcards and tokens. One of the major benefits of the solution is that a mobile device can easily be used as a tool that provides access to a wide range of e-services, enables qualified signing of documents in a legal manner, and offers a high-level of security and usability [30].

Estonia [13] is another example of countries with well-developed digital identity system. By now, every Estonian can authenticate himself without physical documents by using a national issued digital id that provides access to e-services. In the Estonian experience, mobile ID allows people to use a mobile phone as a form of secure digital ID, meaning that mobile device can be used to access secure e-services and digitally sign documents, but on the other hand, it not requiring a card reader. For this purpose, a special mobile SIM card is issued for the citizens that stores private keys, along with a small application delivering the authentication and signature functions.

However, many authors agree that mobile solutions cannot exist by default, meaning that they cannot fully replace traditional solution, but rather they would serve as a supplement that can enhance user experience and provide a response to the demand of the smartphone era [14], [15].

2.1. General requirements

In contrast to the pilot projects and production roll-outs, we aim to assess how well the existing solutions conform with the general mobile id requirements. To do so, we first need to define requirements for a mobile equivalent of a physical card. We start defining general requirements, and in the upcoming sections, we show great interest in evaluating the security and privacy properties. With the world becoming more and more digitalized, there is an obvious need for verifying digital identities. However, digital identification can also jeopardize our privacy in an incorrect setting, so it is crucial to discuss the privacy and security implementation in digital identification [16].

3. Requirements

The use of public service on a mobile device accompanies the mass adoption of smartphones; however, the requirements for transferring a digital identity into a mobile device is a topic that has been neglected. The benefits of such a solution are quite outlined and stressed; we still need to analyze and derive requirements for such a solution, which is especially important for privacy and security requirements. We have gathered the most common requirements through the literature that we split into three groups:

privacy, security, and technical. It should be noted, however, that these not exclusively belong to one or the other group. It should also be noted that they are connected and dependent on each other. Due to their nature, some of the requirements were deliberately defined on a rather high level of abstraction.

3.1. Privacy requirements

Mobile driving license standardization [17] follows Privacy by Design goals that can be achieved following ISO/IEC 29100 Privacy Framework—2011, and that can be easily applied to general solutions in the domain of mobile identities. In this work, we derive mobile driving license privacy considerations that are also applicable to mobile digital identity solutions. As GDPR regulations provide a set of privacy regulations and consequences for violating them, it is recommended for every entity participating in this system to implement them. In this section, we summarize the most general privacy properties; however, the concrete implementation of these properties strongly depends on the use cases.

- **Consent and Choice** . - Consent and choice as privacy property refer that a data holder or a user of service allows that her data is going to be collected. Moreover, the user should also be fully aware for what purpose the collection of her data is used and to have a choice to give the data. 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 their personal data. In addition, users need to have a choice of giving access to their personal data. One of the examples is that users give consent that their data is used for different kinds of survey or research purposes.

- **Purpose Specification** . - Users should be fully aware of the purpose their personal data is being processed. The collected data from data holders should be associated with the concrete purpose, and data holders should know at any moment why their data has been processed [18]. In addition to this, the data holder's attributes should be directly and reasonably connected to the purpose for which they are being collected. In general, the aim for sensitive data such as ethical, political, religious orientation should be minimized to the maximal extend.

- **Collection Limitation.** - User data should be collected only for a specific purpose, and data collectors should collect only data necessary for the transaction purpose. The attributes that are required for a specific purpose should be necessary to the maximum extend, and no other data than the absolutely necessary ones should be asked from data holders. For instance, for entering a night club it is required to prove you are older than 18, and this is the only necessary data attribute. Collection of any other personal information, for example, an address, would not make sense in this case and should not be required. On the other hand, data holders should only respond with data that has been asked of 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. Verifiable Credentials Data Model [19] defines data minimization as an action of limiting the context of

the data attribute to the minimum required by data collectors for a specific use, as privacy violation can happen when information associated within one context leaks into another.

- **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. Data attributes collected for a specific use should be retained only for the period of time sufficient until they serve the purpose of their collection.
- **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. In addition to this, data attributes should be easily accessible and available for data holders, and users should be able, by need, to check who used their data and for what purpose.
- **Individual Participation.** - Users should be involved in the collection, consent, processing, and storage management of their personal data. Users could also challenge and question the conclusions that have been made from their attributes.
- **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 [20], 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 the case of different transactions with a different set of attributes, it should not be possible to link them to the previous ones. Linked information should be shared with third parties only when this is necessary, and they should be stored only for the time they fulfill the purpose of collecting.

3.2. Security 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 that 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.

- **Confidentiality** - a property that information is not made available or disclosed to unauthorized individuals, entities, or processes [21]. 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 [21]. 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 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 [22].

- **Authentication** - property of recognizing a user's identity. Authentication represents 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 a 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 [23].

3.3. Technical requirements

One of the main technical requirements that is highly important for the mobile ID system is certain **interoperability** . Interoperability is defined as an ability of a system to manage and share information between different devices. For a mobile ID system, interoperability means that the solution should work even in the cases when users have different devices or when different applications are offered by different vendors.

4. Technologies

4.1. The ISO/IEC 18013-5 mDL standard

The ISO 18013-5 mDL standard [17] defines an interface for implementing a physical driving license on a mobile device. This way, the mobile device would be able to replace the mobile document fully and would serve as a valid identification tool. Its development started in 2014 by the members of the International Organization for Standardization with the aim of supporting and building the mDL ecosystem with privacy-preserving, high-level security, and interoperability features. In this subsection, we outline some of the common parties described in the architecture of mDL, while the core security and privacy features will be discussed in separate sections.

- **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 purpose.
- **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.

Principle	CoI2	Mechanism
Consent and Choice	✔	Supports the implementation of two modes: pre-consent and transaction-time consent. Pre-consent allows users to configure with which verifier they have trust, so that verifier can access data without transaction-time consent. Transaction-time consent is just-in- time consent required during the processing time.
Purpose specification	✔	
Collection Limitation	✔	Provides “intent to retain” to fulfill collection limitation. Disclosing additional data is permitted only to fulfill the purpose of the request.
Data minimization	✔	Supports privacy-preserving attributes where data groups are divided into data elements. By transaction, only specific data elements are requested. Data minimization should be applied to metadata as well.
Use, Retention, and Disclosure Limitation	✔	
Openness and Transparency	✔	
Individual Participation	✔	Individual participation is enabled through the sequence of “Device Engagement, secure connection, Request, Response, Repeat” that allows pre-consent and transaction-time consent.
Information Security	✔	Signing data and using digital certificates assures data integrity and authenticity.
Privacy Compliance, Accountability and Auditing	✔	
Anonymity and Unlinkability	✔	Data minimization for metadata should be applied; Ephemeral keys from mDL and mDL Reader should be destroyed after use; Rotation of public keys is recommended; The online token exchanged between holder and verifier should be short-lived and used only once, this way, the replay attacks could be mitigated.

Table 1.The table depicts the privacy requirements and the technical opportunities to implement these requirements in the ISO/IEC 18013-5 mDL standard.

4.2. Verifiable Credentials and DIDs

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" [19] 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.

Decentralized identifiers (DIDs) are identifiers that are used to create verifiable, decentralized digital identity [24]. 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.

4.3. Self-Sovereign Identity

The SSI concept emerged as a combination of Distributed Ledger technologies (or Blockchain), Decentralized Identifiers and Verifiable Credentials. The SSI data are data that we own on our digital identity wallet. One of the key feature of this concept is that SSI credentials are completely under our control, they are tamper-proof, and thanks to the peer-to-peer communication between verify, issuer and holder, nobody knows when the credentials have been exchanged [25]. The concept is based on the sovereignty principle, defined as the supreme power without outside factors. For an identity management system, SSI is seen as a next step of evolution [26] that assures following:

- **Full control over data** . User has a full access to the stored identity data, in addition to the logs, and user is free to add, delete, revoke any of her identity attributes.
- **Security, privacy and integrity of data** . Data need to be secured, integrity can be achieved using Blockchain technologies and privacy needs to be preserved.
- **Portability of data** . Users should be able to use their identity data whenever needed.
- **No dependency on a central authority** . Trust to the central authority is not required.
- **Interoperability** . This means that for verifying identities we can use different system and platforms.

The SSI concept emerged as an alternative to physical and digital cards. It is known that physical identification cards kept in our pocket are often being stolen or impersonated with the cases of ID theft. Moreover, the process of getting physical cards is often cumbersome, time-consuming, and costly. One clear disadvantage of physical cards is the fact they can be destroyed in natural disasters and extreme situations like wars, where the right authority would not have an option to retrieve them. When it comes to privacy issues, many of the privacy properties cannot be applied, as minimal disclosure, since we always have to show the entire card to the authorities. The biggest advantage of the SSI is that users have control over their data, with who and what they share it, nevertheless, there are some disadvantages of the technology that will be more elaborated in the following sections. One of the technologies that is used for preserving privacy of users are Zero-KnowledgeProofs (ZKP), a cryptographic method where an entity can prove to another entity that they know a certain

Principle	Col2	Mechanism
Consent and Choice	✔	Users must deliberately agree to the use of their identity. Sharing personal data is established only when a user provides a consent. A consent must be well understood.
Purpose specification	✔	The EBSI/ESSIF is a concrete example of purpose specification implementation, where the requester has to state why he needs the requested attributes.
Collection Limitation	✔	Collection limitation can be achieved in the SSI, however depends on a concrete project.
Data minimization	✔	Disclosed claims should be minimal to satisfy the purpose. Data minimization is supported by the implementation of zero knowledge proofs, range proofs, and selective disclosure.
Use, Retention, and Disclosure Limitation	✔	Protection of user data and rights is one of the principles of SSI.
Openness and Transparency	✔	The systems for managing a network of identities must be open. Algorithms should also be transparent; without dependencies on a particular architecture they should be free and open-source. Users can monitor how their information has been used and stored.
Individual Participation	✔	One of the principles of the SSI is that the users are in control of their data, meaning they can choose with who they will share it. Also, access to their data is guaranteed by the principle of SSI.
Information Security	✔	Data integrity of identity data is secured through the signature on these data.
Privacy Compliance, Accountability and Auditing	✔	Privacy compliance is possible in SSI; for auditing and accountability the Blockchain could be utilized.
Anonymity and Unlinkability	✔	Can be achieved, however, depends on a specific project.

Table 1.The table depicts the privacy requirements and the technical opportunities to implement these requirements in the SSI.

value without disclosing the actual value. This way the verifier has zero knowledge about the information except its validity. One of the challenges of SSI concept poses offline verification. When users provide credentials to verifiers, they need to be able to verify whether the credentials are valid, invalid or revoked. This validity information, however, can be obtained when checking the database, but the posing question is what to do in the offline case. This case assumes the verifier does not have an internet connection to check the status of a credential.

4.4. Use cases

When we explain the use cases, it is crucial to categorize the digital identity model. In this report, we will focus on three types of digital identity model:

- **Centralized model** . In centralized system, user data are stored at identity provider (IdP). To access some service, user needs to authenticate herself at IdP and then the identity data are transferred to the service provider (SP). Technologies that can be used for authentication purposes are either combination of username and password or multifactor authentication. One of the major drawback of this approach is that a user is not in a control of her data. In addition, a user also needs to remember quite a large set of passwords, and lastly centralized storages are often a target for an attack.

- **Semi-centralized or federated model.** As the first model showed some of the disadvantages in terms of a user experience, the federated identity model was designed as an alternative that is based on the principle of distributing identity data across multiple IdPs. This way, personal data are not stored on one central place and access to a service is provided by multiple parties that work together in federation. One of the technologies of federated system is Single Sign On. As with previous centralized, and in general every identity system, federated system is also at the risk of data breaches.

- **Decentralized model.** One of the key features of decentralized system is that a user is in a sole possession of her identity data and no central identity provider infrastructure is needed. One of the implementations of decentralized system is SSI. Even though it is very promising, SSI would reach its full potential when some of the following challenges are addressed [35]:

o **Offline availability –** Using digital identities in offline use cases is one of the biggest issues that needs to be tackled. In digital identity management system, it is crucial to provide an answer to the question if the credentials are valid or revoked, which in the offline case represents a challenge.

o **Key management –** In the SSI infrastructure, key management is also one of the challenges, as the loss of private keys could be problematic for the users.

o **Adoption of a new ecosystem –** SSI would reach its full potential when a large ecosystems adopt this technology, which is still a work in progress.

o **The freshness of data.** One of the issues in the model is the disposal of up-to-date information that has not been revoked.

o Achieving different **levels of assurance** for authentication is another challenge.

Furthermore, based on the data retrieval mode, we distinguish:

- **Offline use case** : In offline use case, devices that are participating in the transaction are not connected to the Internet, or at least one device in the communication is not connected.
- **Online use case** : requires that devices involved in the communication are connected to the Internet, or the same network.

When it comes to interaction method, we have following use cases:

- **Device-to-device.** One of the possible scenarios for device to device communication is routine police control.
- **Device-to-SP.** In this case, a digital ID is used as an identification means towards an online service provider.

Mapping between these cases is shown on the following table.

Use case	Description of the use case	Actors	Col4	Transmission method	Support	Col7
Use case	**Description of the use case**	Name	Description	Description	User's device	Verifier's device
Offline	Devices that are participating in the communication are not connected to the Internet, or at least one device in the communication is not connected to the Internet.	Device-to-device	A user's mobile device interacting with a verifier's mobile device, e.g., police control	BLE	Must support at least one of the transmission methods	Mandatory
Offline	Devices that are participating in the communication are not connected to the Internet, or at least one device in the communication is not connected to the Internet.	Device-to-device	A user's mobile device interacting with a verifier's mobile device, e.g., police control	NFC	NFC	Mandatory
Offline	Devices that are participating in the communication are not connected to the Internet, or at least one device in the communication is not connected to the Internet.	Device-to-device	A user's mobile device interacting with a verifier's mobile device, e.g., police control	QR CODE	QR CODE	Mandatory
Offline	Devices that are participating in the communication are not connected to the Internet, or at least one device in the communication is not connected to the Internet.	Device-to-device	A user's mobile device interacting with a verifier's mobile device, e.g., police control	WIFI Aware	WIFI Aware	Mandatory

Use case	Description of the use case	Actors	Col4	Transmission method	Support	Col7
Online	Requires that devices involved in the transaction are connected to the Internet.	Device-to-device	A user's mobile device and a verifier's mobile device or a user's mobile device in the interaction with terminal, e.g., bank payment	Internet protocols	Mandatory	Mandatory
Online	Requires that devices involved in the transaction are connected to the Internet.	Device-to-Service Provider	Mobile device from a user is interacting with online service	Mobile device from a user is interacting with online service	Mobile device from a user is interacting with online service	Mobile device from a user is interacting with online service

Table 2. The table depicts the mapping between different categories of use cases.

5. Case study

In this section, we reflect on some of the solutions that introduce mobile ID service.

5.1. GET Group North America

In 2019 Get Group North America, a mobile technologies development group, has introduced their mobile ID and mobile DL that fully supports ISO 18013-5. The solution has been successfully evaluated in terms of international standards for security, privacy, and functionality. The ISO 18013-5 enabled GET Mobile ID Digital Identity Solution [34] supports NFC for data transmission for both Android and iOS [33]. According to the GET Group, the mobile solution provides cross-platform solution on the market for both Android and iOS. The solution represents a mobile application that can replace a physical ID card or driving license and serve as a quick and convenient solution for different identity services. In addition, it also fully implements ISO/IEC 18013-5 Standard for mDL and complies with AAMVA guidelines. It supports different data transport protocols, such as NFC, QR Code, Bluetooth, Wifi Aware, and Internet protocols.

5.2. Kosovo case study by Veridos

Another case study worth mentioning is the mobile driving licence in Kosovo based on the Veridos VeriGO DriveID solution [36]. Users can opt for a mobile application that fully replaces a physical driving licence and serves to prove driving privileges. On the other side, the authorities can verify the driving licence using another verification application. There are two steps in using the app. The first one is the activation, where a user is prompt to scan a code from the authorities to activate the app. In the second verification phase, a user can use the app by generating a QR code that is scanned by the authorities. The app provides,

according to [36], reflects on the ISO/IEC 1801, and also provides a secure and usable application for both Android and iOS that is based on the security standards and up-to-date data. In addition, the application can also be expanded to include different kinds of digital ID, such as health cards.

5.3. Thales solution

In the state of Florida, Thales, a technology leader that is engaged with many driving licence projects [38], is delivering a mobile driver´s licence solution to the citizens that can use the service to prove the driving rights, as age and identity verification. According to [37], this will be the first state in the US that offers mobile driving licence solution that meets standards provided by the American Association of Motor Vehicle Administrators and the International Organization for Standardization allowing to operate nationally and internationally. In addition, the solution also serves as an authentication tool against numerous online services. To use the service, users are first required to activate the application and select the verification type. This way, the app is not required ever to leave the users and remains easy to use. Thales also delivers a digital driving licence solution to Queensland, Australia, that fully meets the International ISO-Compliant Mobile Driving Licence Standard [39]. The solution represents a privacy-enhancing solution that offers easy access to the online service from a smartphone and provides users control over their data so that they can decide what data and with whom they will share it.

5.4. My Identity App

The Austrian State Printing House [40] offers a portable and mobile replacement for the physical cards. The *My Identity App* (or *MIA*) [39] represents a unique solution for mobile identities that integrates physical documents and eID cards on one smartphone. MIA provides a highly secure, easy-to-use, and efficient tool for identification, authentication, and authorization that can also be used in face-to-face scenarios, such as police roadside control. Outlining the disadvantages of the decentralized approach, such as recovery when a user loses credentials, MIA is built upon the centralized model, where data are retrieved from a central unit [10]. Security of the application doesn't rely on the hardware elements but rather on the secure process, which mitigates additional requirements of users such as support of NFC or smartcard readers. Regarding the app's privacy features, the MIA application can disclose only a set of claims rather than the entire document, which enhances the privacy of users in many use cases. In general, the MIA app can be used for a variety of services, for gaining driving privileges, as a health insurance card, and as an asset for different identity verification purposes.

6. References

[1] 2019 Thales Group, https://www.thalesgroup.com/en/markets/digital-identity-andsecurity/government/identity/digital- identity-services/trends

[4] Kubach, M., Leitold, H., Roßnagel, H., Schunck, C. H., Talamo, M. (2015). SSEDIC. 2020 on Mobile eID. Open Identity Summit 2015.

[6] Ahmetovic, Emina. "Signatures to Go: A Framework for Qualified PDF Signing on Mobile Devices." 17th International Conference on Security and Cryptography. 2020.

[2] CEF eID SMO. Trends in electronic identification: Embracing mobile identity for eGovernmentMay2020, https://ec.europa.eu/cgital/wiki/display/EIDCOMMUNITY/Embracing+mobile+identity+for+eGovern ment

[3] 2020 Statista, https://www.statista.com/statistics/330695/number-of-smartphone-usersworldwide/

[7] EReg Association (AISBL ACG/47039-001) Non-physical driving licences - going mobile. May 2018, www.ereg-association.eu

[5] AAMVA. MOBILE DRIVER'S LICENSE FUNCTIONAL NEEDS WHITE PAPER 2019, http://www.aamva.org

[10] Terbu, Oliver, Stefan Vogl, and Sebastian Zehetbauer. "One mobile ID to secure physical and digital Identity." (2016).

[11] Goraczek, Malgorzata Zofia, et al. "Mobile Health ID Card." Federation of International Conferences on Software Technologies: Applications and Foundations. Springer, Cham, 2017.

[12] Huy, Ngu Phuc, and Loc H. Khuong. "Mobile identity as social economic enabler." 2012 7th International Conference on Computing and Convergence Technology (ICCCT). IEEE, 2012.

[13] E-Estonia Mobile ID, https://e-estonia.com/solutions/e-identity/mobile-id/

[26] Abraham, Andreas. "Self-sovereign identity." Styria. EGIZ. GV. AT (2017).

[9] IDEMIA 2020, https://www.idemia.com/news/why-mobile-network-operators-are-keysuccess-trusted-digital- identity-2020-07-17

[14] 2020 The World Bank Group, https://id4d.worldbank.org/guide/mobile-id

[15] 2020 The Silicon Trust, https://silicontrust.org/2019/11/22/mobile-driving-license-vselectronic-driving-license-replacement- or-supplement/

[22] Abraham, A., Hörandner, F., Zefferer, T., Zwattendorfer, B. (2020). E-government in the public cloud: requirements and opportunities. Electronic Government, an International Journal, 16(3), 260-280.

[35] Abraham, Andreas, et al. "Revocable and Offline-Verifiable Self-Sovereign Identities." Proceedings-19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2020. 2020.

[16] Electronic Frontier Foundation 2020. Digital Identification Must Be Designed for Privacy and Equity https://www.eff.org/deeplinks/2020/08/digital-identification-mustbe-designed-privacy-and-equity-10

[8] Natarajan, Harish, Mandepanda Sharmista Appaya, and Sriram Balasubramanian. G20 Digital Identity Onboarding. No. 129861. The World Bank, 2018.

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

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

[25] 2021 Tykn. https://tykn.tech/self-sovereign-identity/

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

[18] Ayed, Ghazi Ben, and Solange Ghernaouti-Hélie. "Privacy requirements specification for digital identity management systems implementation: Towards a digital society of privacy." 2011 International Conference for Internet Technology and Secured Transactions. IEEE, 2011.

[19] World Wide Web Consortium (W3C) 2019. Verifiable Credentials Data Model 1.0. https://www.w3.org/TR/vc-data-model/introduction

[17] ISO/IEC DIS 18013-5 2020 Personal identification—ISO-compliant driving licence—Part 5: Mobile driving licence (mDL) application https://www.iso.org/standard/69084.html

[35] 2016 International Bank for Reconstruction and Development / The World Bank. Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation A joint World Bank Group – GSMA – Secure Identity Alliance Discussion Paper http://documents1.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB- GSMA-SIADigitalIdentity-WEB.pdf

[24] World Wide Web Consortium (W3C) 2019. Decentralized Identifiers (DIDs) v1.0 https://www.w3.org/TR/did-core/

[30] 2021 Federal Ministry for European and International Affairs https://www.bmeia.gv.at/en/travel-stay/living-abroad/meeting-point-austrians-abroad/handysignature-mobile-phone-signature/

[33] 2021 GlobeNewswire, Inc. https://www.globenewswire.com/fr/newsrelease/2019/07/15/1882887/0/en/GET-Group-North- America-Announces-Near-field-Communication-NFC-Support-on-iOS-for-mDL-and-Mobile-ID-Transactions-at-Pointof-Sale.html

[34] 2021 Global Enterprise Technologies Corp. https://getgroupna.com/solutions/mobileid/

[36] Veridos Gmbh, 2020 https://www.veridos.com/files/assets/downloads/pdf/Flyer_DriveID-Kosovo_US_A4_2020-06- 09_download.pdf

[39] 2021 Business Wire, Inc. https://www.businesswire.com/news/home/20200107005628/en/Thales-to-Deliver-Digital-Licence- Solution-to-Queensland-Australia

[37] 2021 Thales Group https://www.thalesgroup.com/en/thales-provide-mobile-driver-licenses-state-florida

[38] 2021 Thales Group https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/driving- licence/digital-driver-license

[39] 2021 YOUNIQX IDENTITY AG https://www.youniqx.com/en/mia-my-identity-app/

[40] OeSD 2021 Österreichische Staatsdruckerei GmbH https://www.staatsdruckerei.at/en/news-en/my-identity-app-mia/