Fraunhofer FIT

Branch Business & Information Systems Engineering,
Fraunhofer Institute for Applied Information Technology FIT

# Mythbusting Self-Sovereign Identity (SSI)

**Discussion paper on user-centric digital identities**

# Mythbusting Self-Sovereign Identity (SSI)

Discussion paper on digital identities

## Authors

Benjamin Schellinger, Johannes Sedlmeir, Lukas Willburger, Prof. Dr. Jens Strüker and Prof. Dr. Nils Urbach

The Branch Group Business & Information Systems Engineering of Fraunhofer FIT combines the research areas Digital Disruption, Digital Business and Digital Transformation in Augsburg and Bayreuth. Its special characteristics are interdisciplinary expertise in professional and technical topics of business informatics and information management and the ability to combine methodical know-how at the highest scientific level with a customer-, target- and solution-oriented approach.

Fraunhofer Institute for Applied Information Technology FIT
Branch Business & Information Systems Engineering
Wittelsbacherring 10, 95444 Bayreuth

## Acknowledgements

We would like to thank our employees Tobias Guggenberger, Felix Paetzold, Olenka Pankiv, and Fabiane Völter for their active support in preparing this discussion paper.

The German version of this discussion paper was created in cooperation with IBM in the context of the project "Ecosystem of Digital Identities".

## Disclaimer

The Branch Business & Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT has prepared this discussion paper to the best of its knowledge and belief, using reasonable care. Fraunhofer FIT, its legal representatives and/or vicarious agents do not guarantee that the contents of this discussion paper are secure, completely usable for specific purposes or otherwise free of errors. The use of this discussion paper is entirely at the user's own risk. In no event shall Fraunhofer FIT, its legal representatives and/or agents be liable for any damages whatsoever, whether direct or indirect, arising out of the use of this discussion paper.

## Recommended citation

Schellinger, B., Sedlmeir, J., Willburger, L., Strüker J. and Urbach, N. (2022): Mythbusting Self-Sovereign Identity (SSI). Discussion paper on digital identities. Branch Business & Information Systems Engineering of Fraunhofer FIT, Bayreuth.

## Image sources


Self-sovereign digital identities enable users to enjoy a high level of security and convenience while improving control over the disclosure of their verifiable identity data.

# Preface

Last year, the EU Commission presented a framework for the introduction of a European digital identity. The proposal aims to enable citizens and businesses to obtain digital proofs of identity, exchange verifiable documents electronically, and authenticate with internet services across Europe. To manage and use these credentials, the EU aims to provide users with digital wallets.

The introduction of such a self-sovereign identity (SSI) management is intended to provide users with a high level of security and convenience while improving control over the release of their verifiable data. The convenient, privacy-oriented, and efficient management of cross-provider digital identity documents and other proofs is carried out via digital wallets. This is accompanied by numerous possible applications of digital proofs of identity attributes, for instance, password-free login to websites or more efficient interaction with online services of companies and authorities. SSI enables the selective disclosure of identity attributes and the automatic verifiability of digital proofs of an identity by service providers far beyond existing solutions such as the German electronic identities (eID). In addition to the provision of various verifiable documents to individuals, SSI also enables identity proofs for machines and companies, thus extending both existing non-digital and digital identity management systems. Thus, the multi-layered application areas of SSI promise great economic potential.

A European ecosystem of SSI-based digital identities also aims to reduce the risks of large-scale data breaches from digital identity providers and strengthens our independence from US and Chinese identity providers. In this way, SSI should contribute to improving Germany's and Europe's digital sovereignty and enable fair competition in the digital space. Against this background, Germany's government is vigorously pursuing numerous SSI projects, such as four Secure Digital Identities showcase projects and several pilot projects coordinated by the Federal Ministry for Economic Affairs and the Federal Chancellery, respectively.

In this discussion paper, we want to shed light on current debates about the potential and challenges of SSI, digital wallets, and the use of blockchain technology. In this context, we take up current opinions in the public and try to resolve misunderstandings. Then, we summarize the results of the discussion paper and take a glimpse into the future. For an introduction to the topic, we would like to refer to our preceding study, in which we explain the technical foundations, application areas, and potentials of SSI. We hope you enjoy reading this work and kindly invite all readers to enter into a dialogue with us. We are happy to answer questions, discuss issues, and implement suggestions for improvement.

**Prof. Dr. Jens Strüker**

Professor of Information Systems and Digital Energy Management, University of Bayreuth

Head of Fraunhofer Blockchain Lab, Branch Business & Information Systems Engineering of Fraunhofer FIT



**Prof. Dr. Nils Urbach**

Professor of Information Systems, Digital Business and Mobility, Frankfurt University of Applied Sciences

Head of Fraunhofer Blockchain Lab, Branch Business & Information Systems Engineering of Fraunhofer FIT

# Contents

# 1 Motivation and relevance

# 1 Motivation and relevance

The EU has set itself the goal of building an ecosystem of digital identities and connecting them at the European level, in particular, to promote the cross-border recognition of state-issued electronic identities (eIDs). The corresponding foundation is currently being laid with the revision of the proposal for electronic identification, authentication, and trust services for electronic transactions (eIDAS)[1]. The eIDAS regulation aims to facilitate access to public services, regardless of the member state in which the eID was issued. However, European harmonization is still lacking, as EU member states have to submit their identity schemes to a specialist group formed by member states for evaluation as part of a notification procedure to ensure the mutual recognition of the eID system throughout the EU (European Commission, 2021).

Consequently, today each member state creates and implements its own scheme under eIDAS. It is noticeable that the eIDAS regulation focuses in particular on governance aspects but so far does not provide any requirements for a technical implementation[2]. In addition, the scope of currently available proofs of identity is limited to a small amount of basic information, such as data from the ID card. This means that, in particular, documents such as driving licenses, health cards, certificates, training certificates, employment certificates in companies, membership cards in associations, etc., are not currently covered. One of the reasons for the low level of awareness and its use of the eID but also the lack of expansion of the approach to other identity documents is arguably the costly certification process required for the integration of additional organizations. In Germany in particular, the new ID card ("neuer Personalausweis – nPA") is a privacy-oriented and highly secure solution for an eID. However, the corresponding physical (security chip on the ID card) and infrastructural (certification of special parties that are allowed to read data from the nPA) prerequisites may be unreasonably high for many other identity documents where lower or no regulatory requirements prevail. Therefore, these cases demand a more flexible alternative. One indicator of this diagnosis is that while the involvement of the private sector in the use of the eID has been extremely restrained so far, there seems to be great interest in the use of digital proofs of identity in general. In addition, there is still a lack of pressure from the member states for implementation, e.g., the first eIDAS regulation did not include the provisioning of all citizens with an eID as a mandatory component.

In the course of evaluating the functioning of eIDAS 1.0, the associated vulnerabilities mentioned above (European Commission, 2021), and considering the objective of extending it to a much broader range of use cases, the European Digital Identity Framework (eIDAS 2.0) initiative was launched by the European Commission. The proposal particularly aims to promote digital identities for natural and legal persons within the EU and mentions the use of a digital wallet. With the planned introduction of eIDAS 2.0, in contrast to the current eIDAS 1.0 regulation, new services are to be made available that can map any type of digital identity proofs and thus go far beyond the storage of master data provided by a physical ID card. In contrast to the previous regulation, the member states are also obliged to implement this to make the integration and use more attractive for companies and authorities by reaching a "critical mass" more quickly.

The long-term goal is to provide a versatile European identity by means of interoperable digital wallets provided by member states and companies (Austrian Chancellery (AT), 2021). The various SSI projects pursued by the German government and the private sector are already preparing intensively for such a new regulation and are jointly developing a solution that could be implemented across Europe. An expert group from the eIDAS context has published the first draft for a European identity wallet architecture, where var-

[1] See opinion on the regulation on trust services of the Federal Ministry of Economics and Climate Protection.

[2] For technical requirements, the Standards and Specifications of the European Telecommunications Standards Institute (ETSI) apply.

ious use cases, such as online authentication or the cross-border exchange of health data, are considered. Beyond the European Union's efforts to promote an ecosystem of digital identity documents, SSI-based solutions for an eID have already been launched in other countries such as Switzerland (Digital Identity and Data Sovereignty Association (DIDAS), 2021) or Canada (Boysen, 2021).

In addition to expanding the existing technical implementation of eIDAS, SSI is considered a promising concept for achieving a connection between previously fragmented ecosystems based on interoperable standards, thus making various other identity-related documents available for electronic use. Technically, SSI builds on well-known cryptographic techniques such as digital signatures, which are also often used in implementations of the eID. Moreover, implementations of SSI also frequently use zero-knowledge proofs (ZKPs), among other things, for data-minimizing, selective disclosure of verifiable proofs of properties, and authorizations of a specific identity. In doing so, SSI uses established mechanisms for identifying organizations in the form of a public key infrastructure (PKI). Compared to eID, however, the SSI approach is characterized by greater flexibility: Today's state-issued identity documents can be used for use cases that require a very high level of security and must accordingly be designed to be very restrictive in terms of access options, as well as partly requiring a physical carrier (e.g., the security chip in the nPA). The goal of SSI is to go beyond this special case and enable companies and institutions to issue purely digital proofs of identity that users can manage themselves in their digital wallet and freely decide which services they want to reveal this data to. SSI aims to allow users to conveniently use their identity information in different contexts while maintaining a high level of control and privacy, similar to the German nPA. In SSI, certified institutions provide identity credentials, but future use of these credentials should be possible without interacting with these institutions afterwards. In this way, the SSI approach prevents dependencies and the accumulation of identity data across different contexts with large commercial identity providers and states. Additional data protection must be achieved selective disclosure of data enabled by cryptography. A recent study shows that users consider a high degree of self-determination over the use of their identity information to be one of the most important features of a digital wallet (PwC, 2021).

Compared to the currently common forms of digital identity management systems, SSI-based solutions can avoid data silos that contain cross-domain master and transaction data. SSi reduces the risk of data protection incidents with a high number of users and large amounts of individual user data. On the other hand, new governance mechanisms for trustworthy institutions and companies should provide a sufficiently high degree of flexibility for certification and participation even with many new organizations in the identity ecosystem, thus enabling a higher degree of flexibility and adoption. This includes the underlying PKI that requires the reliable assignment and storage of organizations' cryptographic (public) keys. On the Internet, today this is usually done via certificate authorities (CAs) in centralized databases. In the context of SSI, decentralized alternatives such as blockchains are currently being considered and tested for this task.

Currently, several use cases, especially for digital personal identities, such as for a hotel check-in, a digital proof of driving license or the opening of an online bank account, are being developed and tested by the German Federal Government with cooperating organizations on an SSI basis. Some of these solutions are already in pilot operation. In addition, self-sovereign digital identities for companies are being tested for their feasibility and added value, for example, at the Bavarian State Office for Taxes (LfSt) in the context of tax administration for merchants, but also for machine identities, for example, as part of the Blockchain Machine Identity Ledger (BMIL) project by the German Energy Agency (Guggenberger et al., 2021). In general, companies and public institutions are jointly designing and testing different use cases in four large

consortia (ID-Ideal, IDunion, ONCE and SDIKA)[3] In addition to preparing for the eIDAS 2.0 regulation, which aims to give citizens more security and enable faster processes, the numerous projects are intended to ensure companies' competitiveness in the ongoing digital transformation. SSI should facilitate the interaction between users and other organizations, thus, enhancing efficiency particularly for small and medium-sized enterprises.

As a result, these projects marked the start for a comprehensive ecosystem of digital identities for citizens, companies, authorities, and machines. The development and launch of these use cases have provoked both positive and negative reactions from the general public and IT security specialists. For example, the premature launch of the German digital driver's license in the ID wallet app shortly before the German elections in September 2021 garnered a lot of criticism from IT specialists, politicians, company representatives, the media, and users. Media coverage has often given the impression that the SSI projects pursued by the German Federal Government and the private sector are completely unnecessary, fundamentally conceptually ill-conceived, and insufficiently coordinated with other identity projects. Therefore, it is assumed that these projects cannot contribute to a sustainable added value for Germany and Europe.

Overall, we believe that there has been a lack of comprehensive discussion so far on assessing the advantages and drawbacks of a SSI-based identity management and differentiating between the current status quo of implementation and the conceptual strengths and challenges of this approach. In addition, many of the backgrounds and advantages of SSI projects in Germany and the technological foundations do not seem to be sufficiently known yet. Thus, in this discussion paper, we want to contribute to the general understanding of SSI-based digital identities and credentials, take up and critically reflect on current discussions in public, and clarify prevailing prejudices. We identify seven myths in a multitude of contributions and discussions in the context of SSI should serve to dispel misunderstandings and create the basis for discussing the added value of the technologies used in an informed way. We then summarize the results of this discussion paper and venture a look into the future.

[3] See Selection of Use Cases of the Federal Ministry for Economic Affairs and Climate Protection.

# 2 Seven myths about SSI-based digital identities

## 2 Seven myths about SSI

Before we deep dive into the myths, we will present a working definition of SSI, which will hopefully help readers to understand our argumentation later on. There exist already a few definitions of SSI, which can be found, for example, in the ten principles of SSI by Christopher Allen (Allen, 2016) or the "12 Principles of SSI" of the Sovrin Foundation, which are based on them (Sovrin Foundation, 2021). Accordingly, the essential characteristics of SSI are user-friendliness, independence, and data minimization:

- *User-friendliness*: The simple use of identity documents from different contexts in one (or a few) but freely selectable apps. In particular, it should also be possible to combine identity documents from different contexts, such as the name from an ID card and an authorization from an employee badge.
- *Independence*: Avoiding lock-in effects and the accumulation of identity information with individual identity service providers across different contexts. In particular, communication should be bilateral: Verifiable digital identity documents are transmitted from the issuer to users and the identity proofs generated are sent directly to verifying parties. There is no need to repeatedly communicate with the issuing institution or a third party after bootstrapping.
- *Data minimization*: The purely bilateral communication of identity information between users and verifying organizations is already a major privacy benefit from a user's perspective. For instance, it protects against the tracking of user activities in the context of identity management by companies or authorities. Moreover, especially when information from multiple identity documents is required, only the information necessary for a process should be transmitted to avoid that additional data is stored and analyzed. This includes the selective disclosure of attributes, such as showing the name of an ID card. Furthermore, this includes using one-time pseudonyms instead of repeated unique identifiers for persons and presented identity proofs (see also myths 2 and 4).

Based on this definition of SSI, we find that the implementation of the eID in Germany has many features that provide user-friendliness, independence, and data minimization. However, in our view, the eID alone does not yet offer SSI-based identity management, as it only covers a very specific context (proof of identity from the ID card). In addition, access to corresponding proofs of identity is severely restricted by the required certification of the parties involved: The higher the required level of assurance, the more restrictions must be placed on which parties a user may present a credential to. Due to the implementation employing a chip in the ID card and the special restrictions on readability, the purely digital implementation and, thus, the applicability of the technical infrastructure in many other contexts is currently also difficult to imagine. For this reason, we see the eID or its future development into the Smart eID, which no longer requires a physical smart card, as an extreme point in the spectrum from less strongly regulated proofs of identity (e.g., tickets or gym memberships) to strongly regulated proofs of identity. Therefore, the goal of SSI is complementary to that of the eID: to create technically unified digital credentials that are more easily accessible to both issuers and verifying parties, also outside domains with the highest level of assurance needs, and to empower users to conveniently manage their digital identity in their digital wallet app. This makes password-based login, the repeated manual filling of forms, and the tedious scanning and highly error-prone manual verification of physical documents obsolete.

SSI thus promises to significantly improve existing digital identity management. Nonetheless, SSI is still accompanied by some challenges, so the public discourse on this topic is currently not always benevolent. To promote an SSI-based digital identity ecosystem in Europe, it is essential to critically

examine and better understand its characteristic advantages and disadvantages – especially in comparison with established and alternative technical implementations of digital identity management – as well as its significance for society, the economy, and politics.

By means of seven selected myths on different topics around SSI-based digital identities, we will discuss current topics of discourse and illuminate the value that corresponding technologies can potentially add from a scientific perspective. In the following, we present and analyze these myths. Table 1 summarizes the individual myths.

| # | **Myths** |
|---|---|
| 1. | Current digital identity management solutions are sufficient. |
| 2. | A digital wallet does not address users' needs. |
| 3. | Regulatory requirements are not met with an SSI-based solution. |
| 4. | The SSI concept exhibits fundamental technical security issues. |
| 5. | SSI can only be implemented using blockchain technology. |
| 6. | In SSI, personal data is stored on a blockchain. |
| 7. | SSI-based identity solutions are inefficient and consume much energy. |

Table 1: Overview of the seven myths about SSI.

## Myth 1

Current digital identity management solutions are sufficient.

## Myth 1: Current digital identity management solutions are sufficient.

In the internet age, citizens use many different accounts and passwords to access digital services, marketplaces, and platforms. Often, a username and password combination is used to access online services. In addition to the need to repeatedly store identity information in accounts, which can be burdensome for users to provide and for service providers to verify, managing passwords poses a major challenges for users. On average, users now have over 100 different digital accounts and often reuse or do not update their passwords. This can lead to significant security problems.

To make the management of users' many digital identities in the form of their accounts more convenient, US technology companies, in particular, offer single sign-on services (SSO) and act as "identity providers". Service providers then interact with these identity provider every time a user proves his or her identity. Experience shows that big tech companies not only gain a competitive advantage from being an identity provider but also analyze and monetize the data at their disposal (Lapienytė, 2021). Beyond individuals, also the dependency of European organizations and companies on SSO provided by corporations to enable employees and customers to interact efficiently and securely on the internet is critical. Many European organizations and enterprises use platform-provided SSO to enable efficient and secure interactions for employees and customers. Furthermore, centralized systems are vulnerable to network failures as they represent a single point of failure. The recent case of Meta Group, where Facebook, Instagram, and WhatsApp went down worldwide for hours at the end of 2021, not only partially eliminating critical communication, but also the ability to log in to other services using Facebook's SSO solution, shows that a failure of highly centralized infrastructure can have a significant impact and lead to losses for other companies (Zivadinovic, 2021).

Furthermore, centralized solutions can enable states to monitor their citizens and companies more closely. In China, for example, the Social Credit System uses big data to record and analyze the behavior of citizens and companies (Liang et al., 2018). The state's intentional surveillance of society and organizations contradicts the European Union's fundamental values to leave control and sovereignty over their (digital) identity to the users. Although SSO appears comfortable in users' perception and the protection of privacy does not play an overriding role for many, the listed disadvantages are not to be neglected.

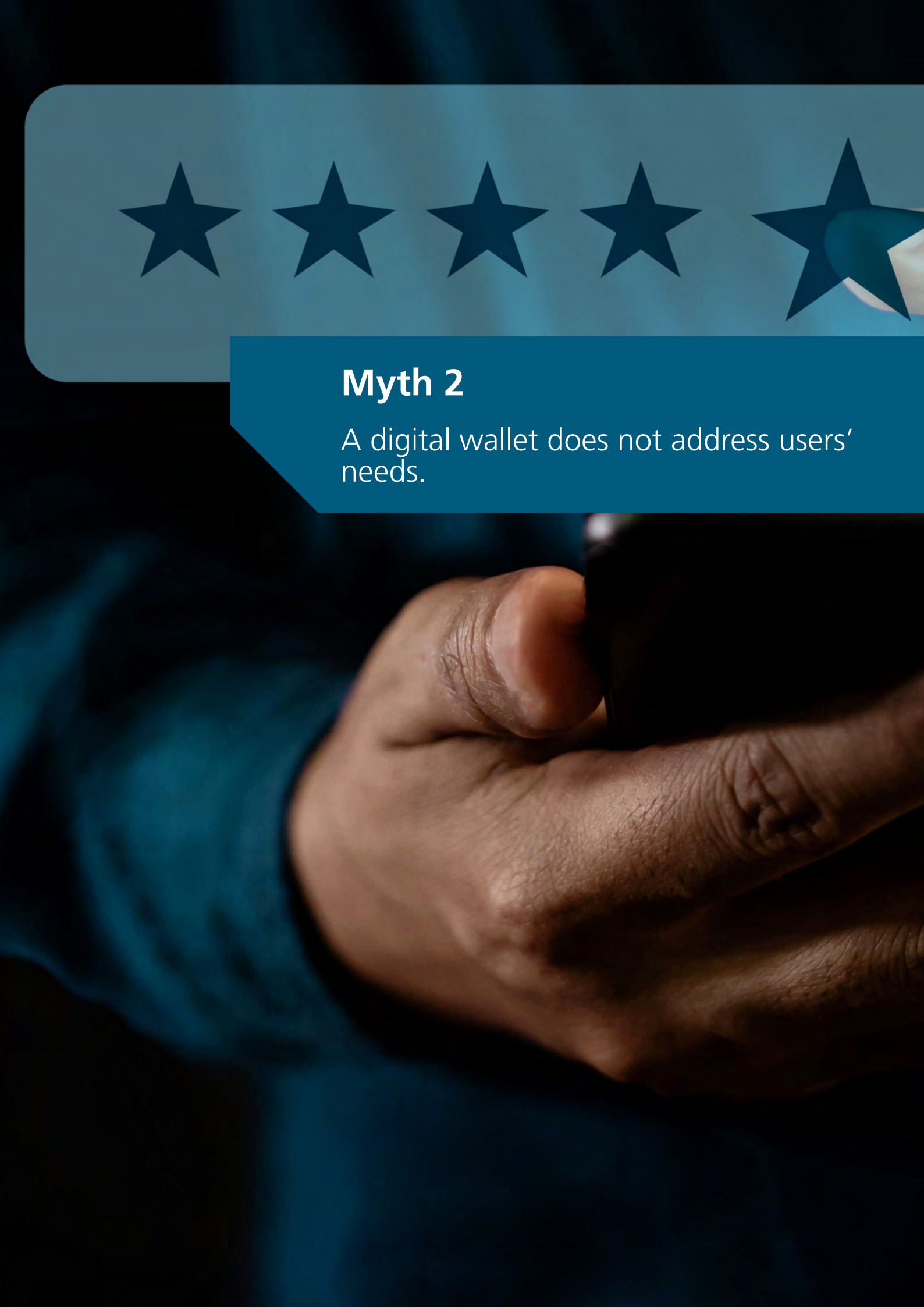
Nonetheless, it is not only identity providers' centralized databases that can represent rewarding targets for cybercriminals because the effort to steal a large amount of data is relatively low per record. Even certificate-based solutions that do not require the continuous interaction between end users, service providers and identity providers can be compromised. For instance, issuing forged certificates with a valid signature also poses a high risk for potential data theft. Such problems arose in this regard during the Corona pandemic when forged Covid-19 digital vaccination certificates were issued by individual pharmacy staff (BR 24 Redaktion (Frank Jordan), 2021). Such certificates are correctly created from a cryptographic's perspective and, therefore, not readily recognizable as forgeries. The lack of possible recall of forged certificates has been a major problem with Covid vaccination certificates, among others (Wolf and Nabben, 2021).

As mentioned above, SSI considerations and developments stem from the problems of centralized solutions for digital identities, such as government surveillance, aggregated data silos, and digital identity theft. There are even more problems, such as compromised certificate authorities. In contrast to the aforementioned centralized identity solutions of large companies, control can be returned to the hands of the users with decentralized concepts. Against this background, the German Federal Government is setting the framework for developing and testing SSI-based identity solutions: The goal includes the development of an overarching, less

proprietary ecosystem of digital identities for citizens, companies, and machines. This is intended to keep pace with the advancing digital transformation, which is represented in particular by the increasing range of digital products and services.

SSI-based identities within the EU require open standards, interoperability, and scalability. Therefore, it is important to understand SSI in the overall context and develop a Europe-wide, compatible, scalable solution for digital identities of all kinds and different target groups. Through the German Federal Government's commitment to developing digital identities based on the SSI approach, German and European competitiveness, in particular, should be promoted by building the infrastructure of a digital ecosystem (German Chancellery (DE), 2021).

This approach will support the European economy and reduce dependence on large technology companies outside Europe. In this context, a possible introduction of eIDAS 2.0 should promote digital identities for natural and legal persons within the EU. In addition, any type of proof should be supported by an SSI solution. Users, on the other hand, should be confident that no central authority can track their interactions, provided that they trust a (state-certified and/or open-source) wallet.



## Myth 2

A digital wallet does not address users' needs.

## Myth 2: A digital wallet does not address users' needs.

In the analog world, identity documents and other certificates serve as proofs for the authenticity of personal data and attributes. They are usually issued on plastic cards or in the form of special paper documents. When showing these proofs, for example, during a police check, when applying for a loan, or when proving one's vaccination status, it is often impossible to reveal only the data required for the application and hide the information that is not relevant. When using these proofs of identity in the digital realm, there is typically also no opportunity for citizens to show parts of their identity in a privacy-protecting way. In the course of advancing the digital transformation, there is an increasing need for such digital versions of proofs of identity, such as an ID card or driving license, as well as the opportunity to disclose identity attributes selectively (Government, 2021).

Even common certificate systems such as the digital vaccination passport have not yet eliminated these weaknesses, as they require an ID card for making sure that the holder of the certificate is authentic through a comparison of names – an SSI-based approach could address this weakness (Rieger et al., 2021). Generally, when certificates are checked, all information about holders is disclosed. On the other hand, the selective disclosure of attributes is possible with solutions that rely on secure hardware, such as the German electronic ID card (Tsakalakis et al., 2016). However, this approach requires the use of a physical smart card with a security chip as well as the involvement of a third party that reads in and forwards all requested attributes of the respective proof of identity (Slamanig et al., 2014). [4] An SSI solution that supports a variety of digital proofs of identity should also enable selective disclosure purely on a software basis and be able to prove the revealed attributes directly bilaterally to the service provider. Similar to physical ID documents and certificates, individuals should be able to store their verifiable proofs in a digital wallet on their smartphone, in the cloud, or on another trusted system, to manage them, and to show them when needed in a data-minimizing manner without having to obtain authorization from a third party. Therefore, the local and decentralized storage of personal information in an SSI solution ensures the security and protection of the data. Users can thus use verifiable credentials for identification, authentication, and authorization on their own (Sporny et al., 2019).

When verifying identity attributes, only the data requested by the verifying party via a proof request and explicitly revealed by users through a verifiable presentation, i.e., data to be transmitted to the verifying authority, is transmitted. Furthermore, selective disclosure enables individual attributes of an identity to be selectively confirmed when presented. This is an advantage over existing certificate-based approaches and analog identity management, where certificates and cryptographic identifiers must be transmitted completely and recognizably (Sporny et al., 2019). Unlike common certificates based on JSON Web Tokens or X.509, SSI-based certificates can prove that a trusted issuing entity has signed the specified values in the verifiable presentation, without transmitting the verifiable credential (certificate) itself.

This is made possible – unless, as with the nPA, there is a hardware-based security chip – by ZKPs, which verifiably reveal the minimum amount of information required for the interaction. ZKPs are cryptographic protocols that convince a verifying party that a (mathematical) statement about the data is correct, without revealing the information itself (Goldwasser et al., 1989). It should be emphasized that ZKPs are rarely used for anonymity reasons, as relatively unique identity characteristics often need to be transmitted. However, ZKPs make it possible to mathematically guarantee that no more information than necessary is transferred. This ensures that verification does not involve the transmission of unique identifiers or attributes that

[4] While the Smart-eID allows the ID card to be fully digitally replicated on the mobile phone, so far, only individual Samsung models have been certified by the German Federal Cyber Security Authority (BSI) for the highest level of assurance.

are not required. In general, the verifiable credential never leaves the user's wallet. In addition, SSI offers the opportunity to use range proofs to prove that numerical values, such as birth or issue date are below or above a specific threshold, without revealing the information itself (Camenisch et al., 2008; Dingle, 2020).

In general, it should be emphasized that SSI puts great emphasis on maintaining the confidentiality of sensitive information, and even exceeds regulatory requirements in this regard. This is reflected in the avoidance of cross-domain data silos with particularly far-reaching consequences in the event of data breaches and the possibility of selective disclosure of information. However, the development of verifiable proofs is still at an early stage and thus does not represent a legally binding end product. For example, in this context, the basic ID of the Federal Chancellery's SSI pilots does not yet represent an official identity document owing to its prototype status. Consequently, the basic ID can initially only be used where the legislator does not require an electronic ID card or passport, or a smart eID, e.g., for car-sharing or rental car providers (Wölbert, 2021). In the long run, citizens should be able to store, manage, and present their verifiable proofs of identity, such as driving licenses, birth certificates, or diplomas, in a self-determined manner in digital wallet app on their smartphone. The draft of eIDAS 2.0 is intended to advance the recognition of such documents considerably.

There are already promising open-source solutions for the technical implementation of digital wallets, such as the Hyperledger Indy software development kit (SDK). However, from users' point of view, further usability improvements should be sought before large-scale use because of the limited experience with wallet apps for identity documents (Sartor et al., 2022). In this context, large-scale studies on user-friendliness are advised (Rieger et al., 2022).

The German Federal Government is already promoting domestic competition to develop digital wallets in this context. Although the implementation of digital wallets involves many technological components, the work required at companies, consortia, and research institutes for the integration of SSI solutions is primarily procedural. Thus, only a few interfaces need to be adapted to integrate a digital wallet. This is particularly about testing these solutions, gaining experience, and building up technology knowledge. Furthermore, under the current proposal for eIDAS 2.0, the EU member states would be obliged to provide or promote a digital wallet solution for their citizens within one year.

In summary, digital wallets are an indispensable component in the overall SSI ecosystem. They have many features that can bring significant benefits and efficiencies from the user's perspective, not only in purely digital interactions.

## Myth 3

Regulatory requirements are not met with an SSI-based solution.

## Myth 3: Regulatory requirements are not met with an SSI-based solution.

Most identity documents and, in particular, sovereign documents, such as a basic ID or a digital driving license, contain personal data of natural persons that are subject to Art. 1 par. 1 General Data Protection Regulation (GDPR). In using SSI, data is only exchanged bilaterally between users and verifying parties after the initial issuance of cryptographically signed and verifiable credentials. The issuance of these credentials is executed using a secure, bilateral communication channel between the users and the issuing institutions, hindering third parties to see the data flows. This "Privacy by Design" approach allows to comply with the strict requirements of the GDPR for natural persons in the EU: The limitation of the exchange of personal information to the parties directly involved and to the minimum necessary reflects, for example, the principle of "data minimization" (cf. Article 1 (1) of the GDPR) as well as "purpose limitation" (cf. Article 5 (1b) and (1c) GDPR). In addition, in the case of a proof request, the release of individual attributes must always be actively confirmed by the user ("transparency" and "control"). The storage of verifiable credentials in a digital wallet also facilitates portability (cf. Article 20 of the GDPR) and the independent deletion of identity information by users ("right to be forgotten", cf. Article 17 of the GDPR).

First and foremost, SSI-based solutions are subject to the same regulatory requirements as, for example, other electronic proofs of identity. However, a differentiation must be made between the use cases to fulfill the applicable regulatory requirements. This differentiation applies, among others, to the SSI projects of the Federal Chancellery, e.g., for the Basic ID (Identity Card Act) or the Bavarian State Tax Office's VAT certificates (money laundering and know-your-customer requirements). Owing to the purpose of these identities, there are different legal and regulatory requirements. Regarding data protection requirements, as in the GDPR, SSI could fulfill the strict requirements to a high degree through its privacy by design approach (see Myth 2).

For the creation of uniform surrounding conditions in the cross-border use of electronic identification means and trust services, the eIDAS regulation provides the regulatory framework (see section 1, Motivation and Relevance). To make eIDAS trust services available as an anchor in the European SSI ecosystem, the European Commission designed the eIDAS Bridge, which assists issuing institutions in signing a verifiable credential (Alamillo-Domingo, 2020). It also assists to identify the issuing party (a legal entity in the context of this project) by its public key. Hence, through the eIDAS Bridge, a verifiable credential could potentially be classified as trustworthy and legally usable (Alamillo-Domingo, 2020).

A conclusive assessment of whether current SSI projects meet relevant regulatory requirements is not possible at this stage. Among other things, SSI-based identity solutions would have to be recognized under a possible eIDAS 2.0 regulation to be introduced. In addition, interoperability with existing certificate systems must be established, e.g., by connecting existing public key infrastructures with the verifiable credentials used in the pilot projects of the Federal Chancellery or with the use of general-purpose ZKPs in connection with X.509 certificates (Delignat-Lavaud et al., 2016).

The SSI-based use cases that are implemented in the context of the showcase projects, show already complementary approaches with other technological standards, e.g., a digital ID card (electronic proof of identity (eID)) and a digital driving license (ISO/IEC 18013-5:2021). While the latter standard is tailored to a specific use case and the eID specifies both a regulatory and technical implementation, SSI aims to provide a broader, more general basis suitable for various use cases with the associated functional legal components.

The German eID infrastructure can currently only be used to represent the ID card and therefore only show the owner's master data. From a technical

perspective, the Enhanced Role Authentication Protocol is intended to allow additional identity information from other „attribute providers" to be presented together with the eID. So far, however, this functionality has not passed the status of conception and it is not yet known how the protocol will be integrated into the national eID system or even the Europe-wide eIDAS ecosystem. The actual retrieval of the data stored on the ID card is not done directly from the smartphone but from a BSI-certified eID service, which communicates directly with the ID card after the user's confirmation. The eID service then forwards the retrieved data to the requesting website. The smartphone only serves to establish an encrypted communication channel and cannot decrypt the transmitted information. Even if the involvement of a third party contradicts the purely bilateral interaction between users and verifying parties, this approach can be useful for ensuring the requirements of the highest level of trust. This mechanism prevents multiple attack vectors, such as a man-in-the-middle attack. In such an attack the authenticity of transmitted data is compromised or a security hole in the operating system that leaks personal information to malicious third parties. The integration of Secure Elements into smartphones makes it possible to store and present document data in a tamper-proof manner. However, a lengthy certification process is required for smartphones and access for relying parties is severely restricted, making an ecosystem of providers and verifying parties difficult.

On the other hand, documents in everyday use cases are often also acceptable at a slightly lower security level. Accordingly, in the SSI context, these proofs can be stored and used directly in a freely chosen wallet without involving a trusted third party. It should be noted that the two approaches are not mutually exclusive and can be operated in parallel. A hybrid approach makes it possible to keep the existing eID system with its high security and proven governance structures while exchanging workday identification documents with lower security requirements in an environment with fewer restrictions. This flexibility reduces entry barriers for end users, companies, and authorities. It offers the opportunity for new fields of application without jeopardizing the security level of critical, government-issued identification documents. Since the level of assurance ***high*** specified in the eIDAS regulation is required for sovereign documents, such as a digital ID card or a potential digital driving license, special security requirements must be met for the credential to be recognized. For example, for an SSI solution, implications can be derived from the security and governance mechanisms based on the eID architecture. Since, according to German Federal Office for Information Security (2021), SSI cannot map this level of assurance on its own at this point, technological approaches are useful to facilitate a solution for both lower and higher-level credentials.

It should be emphasized that SSI-based systems use cryptographic primitives that are not yet certified by the BSI (see also Myth 6). Even if no specific security vulnerabilities are currently known for these methods, an end-to-end audit is indispensable for a high level of security. Accordingly, it is the basic prerequisite for a complete regulatory assessment and regulation. Since cryptographic methods can be seen as a chicken-and-egg problem, an initial review and assessment of the cryptographic components used should be sought for the further course of the Secure Digital Identities showcase projects. If these aspects are successively addressed, the prevailing challenges can be gradually removed.

Overall, properly designed SSI solutions could well meet all legal requirements in the long term. While many developers and supporters of SSI plausibly argue that more decentralized governance is necessary or helpful for a highly scaled ecosystem of digital identities, an evaluation can probably only be done through practical implementation. Accordingly, further research should consider how to keep the opportunity for both centralized and decentralized approaches open with little effort.

## Myth 4

The SSI concept exhibits fundamental technical security issues.

## Myth 4: The SSI concept exhibits fundamental technical security issues.

In Germany, the introduction of a digital representation of the driving license led to criticism because of its premature stop (Wittmann, 2021; Muth, 2021). Within the framework of technical analyses, justified questions were raised about the implementation and its security mechanisms. As with any public software architecture, malicious actors must be expected at any time in an SSI-based system. Thus, extensive penetration tests must be carried out before the launch to exclude attack points. The fact that the name (and possibly an image) of the requester can be freely selected when verifying a credential in the context of a proof request received criticism. Consequently, the identity of the verifying party cannot be confirmed beyond doubt. In addition, the security of complex cryptographic procedures such as ZKPs and blockchains as well as the suitability of smartphones for storing sensitive identity information were also controversially discussed (Kahlo, 2021; Chaosradio, 2021)[5]. We address the raised concerns in the following.

First, it is at the heart of a self-sovereign identity to determine to what degree data is disclosed and to whom. Comparing this scenario to handing over the information of physical identity to a stranger in the real world, the same due diligence has to be done. This can raise a problem in the digital world to that extent that end users in digital interactions cannot visually verify the identity of verifying parties. This is problematic because sensitive information can fall into the wrong hands.

A much more far-reaching attack scenario, which was not prevented during the implementation of the digital driving license, is a man-in-the-middle attack (Wittmann, 2021; Lissi, 2021). In such an attack, a third party can read the communication between the verifying party and wallet users unnoticed by pretending to be the verifying party for the owner of a wallet and the wallet's owner for the verifying party. In addition to reading sensitive information, there may be use cases where newly issued proofs of identity can be made directly usable for attackers in the interaction. The consequences can be far-reaching for both wallet owners and verifying parties, as they rely on the authenticity of the counterpart.

This problem is often encountered in digital identity management solutions and has been discussed in the SSI community. Various possible solutions have been proposed. One solution that seems to make sense, especially for sovereign documents, is to restrict the disclosure of sovereign credentials, comparable to the eID system, and to allow a digital wallet to present credentials only to certified entities (Lissi, 2021)(Lissi, 2021). Such considerations can also be found in the first architectural sketch for the European implementation of digital wallets (eIDAS Expert Group, 2022): Accordingly, registers for trusted parties are required. In addition, the digital wallet should be able to identify the verifying party so that users can make informed decisions[6]. However, strong restrictions can only enforce compliance with these restrictions – in the case of the eID, for example, in the security chip of the ID card itself. However, certification of digital wallets to ensure that corresponding rules are observed seems sufficient for use cases outside the "high" assurance level. Nevertheless, it is conceivable that, depending on the use case, also different security levels for the identification of the verifying party or their permission to process the corresponding data are checked differently, for example, by different registers of trustworthy verifying parties. This measure can be implemented, for example, by depositing the public keys of a verifying organization in a trust register, which can be managed centrally or decentrally (see myth 5). Depending on the sensitivity of the data or the level of security required, end users can then be sure that it will only be passed on to authorized organizations and not to malicious actors. Otherwise they will receive a recommendation from their wallet app and can ignore it if necessary.

[5] For the BSI's position on ZKPs in general, see Study of the BSI on secure blockchains.

[6] "To ensure informed actions from the user and adequate security levels, the EUDI Wallet shall implement mutual authentication capabilities."

Verifying the identity of the relying party is thus easy to implement, can use existing mechanisms for identifying organizations on the internet, such as SSL certificates and qualified website certificates, and are to some extent already implemented in the ID Wallet. On the other hand, for many interactions, this approach also represents a possibly too strong restriction of users, for example, if they are sure they want to transmit information to an uncertified but trustworthy party. Especially if the information involved is not very sensitive or is strongly anonymized using ZKPs, users should be able to ignore the warning sent by the wallet app. This could make sense, for example, in the case of proving one's age of majority or one's vaccination status without disclosing sensitive information, such as a full name. Further discussions on different scenarios, under which conditions which approaches are suitable and how fine-grained these possibilities have to be differentiated are still necessary.

In addition to classic certificate authorities (CA), which form the PKI of today's internet, signature keys can also be allocated and published via decentralized registers using distributed ledger technology (DLT), such as blockchain technology[7]. In the context of the Secure Digital Identities showcase projects, the management of this cryptographic material is done in a distributed manner by several trusted parties, i.e., node operators[8]. The nodes of a blockchain, such as Hyperledger Indy, are operated by companies or public authorities in their infrastructure. Overall, a network must be sufficiently protected against failure in its design, as a distributed system can only exist with a limited amount of failing or compromised nodes before consensus is lost or the entire network fails. In this context, a system with inherent tolerance for failed or compromised nodes can provide much higher integrity and security guarantees than a centralized design, given appropriate governance.

Compromised nodes can also be removed from the network with the help of majorities of the remaining nodes. As long as a significant proportion (usually 1/3) of the nodes in the network are not compromised, the takeover of the network by these mechanisms is not possible. To proactively counteract this attack surface, the entire network should be continuously monitored to detect such threats at an early stage and, in the event of a takeover, to exclude suspicious nodes from the consensus and finally remove them from the network. Compared to centralized software architecture, the advantage is that the entire infrastructure is not immediately at risk from an attack. However, the attack surface is distributed among several stakeholders, thus enabling a flexible response. Thus, it is no longer sufficient to penetrate only one organization. Because of the underlying consensus building, at least the majority of nodes must be attacked or a considerable share of a scarce resource such as computing power of the overall system must be reached. Overall, this results conceptually in demonstrably high availability and robustness against attackers. The Hyperledger Indy-based distributed ledger used in the context of the ID Wallet uses a consensus mechanism that builds on concepts known mathematically for more than 20 years. It is provably secure as long as less than 1/3 of the nodes are attacked or fail (Castro and Liskov, 2002; Aublin et al., 2013; Naik and Jenkins, 2021). However, the implementation so far remains complex and unproven in terms of security and performance over long periods (see myth 5).

Concerning the smartphone wallet, in an IT security context, the question should be raised about how to ensure that cryptographic keys and certificates cannot be extracted via cyber-attacks or physical access to the locked device. Research suggests that while smartphones could achieve a high level of security in protecting, e.g., cryptographic keys, corresponding mechanisms are often insufficiently deployed (Lovejoy, 2021; Zinkus et al., 2021). Overall, this topic should receive more attention in the discussion since private companies, for example, such as the NSO Group in the case of the Pegasus spyware (Munzinger, 2021), can attack smartphones in a targeted and unnoticed manner. Considera-

[7] In the following, we use the terms blockchain and DLT synonymously.
[8] See, for instance, Governance at IDunion.

tion should also be given to the dependence of manufacturing companies on smartphones and their operating systems but also ensuring that they cannot track activity in the wallet. Perfect security is very difficult to achieve and abandoning a smartphone application would probably also go hand in hand with considerable restrictions in user-friendliness. Therefore, well-founded trade-offs must be achieved between the different realization options of a digital identity. In addition, with the direct linking of the operating system and digital wallets, it is questionable to what extent the authorities of the individual countries can intervene or adapt since the proofs are stored in the respective integrated wallet solution. Here, the trade-off must be made between generalization via a standard and deviations in specific cases. However, this applies analogously to all mobile digital identity solutions.

Furthermore, using a digital wallet app raises the question to what extent security requirements of secure access for users are met. In this context, two-factor authentication is very important to ensure the security of users in the management of personal information. In addition, it is important to prevent unnoticed theft of credentials, for example, by connecting them to the mobile device. In order to increase the practical utility of a digital wallet app and to meet security-related requirements, it is crucial to enable the recovery of identity documents and cryptographic keys, for example, via backups. In this light, users should be able to regularly back up their data to restore it in case of a loss or theft. Some digital wallets on the market have an integrated facility for automated encrypted backups to cloud services. Once the app is installed, a recovery key is initially generated that is required to decrypt the backup, e.g., via cloud providers or wallet providers' services. The keys can be stored offline, outsourced to a trusted person or distributed across several devices (multi-device recovery). It should be noted that backups for keys in secure key stores may not be feasible. However, it is conceivable that only the digital ID card has device binding. In the event of theft or loss, the old (digital) ID card would have to be revoked and a new one created, just as in the analog case. On the other hand, the remaining identity documents can be restored via backups but simultaneously inherit the new device binding of the ID card by presenting it in conjunction with the ID card if required in a use case with high level of assurance requirements.

In addition to storing cryptographic keys in the wallet app, a particularly strong device binding can be used, which, in contrast to the operating system's key store, uses a special chip – i.e., the Secure Element – whose sole purpose is the secure storage of cryptographic material. This approach can virtually prevent verifiable copying of credentials and associated keys to another smartphone. This ensures that use is only possible on one mobile device and makes sharing credentials more difficult. It should be noted that the ZKPs used in existing SSI implementations are not yet able to provide proof of control over keys in the Secure Element without leaving a unique trace. However, the feasibility of reconciling security and data minimization in this case has already been demonstrated using X.509 certificates (Delignat-Lavaud et al., 2016) and it is desirable to make this happen in the SSI implementations used as well.

## Myth 5

SSI can only be implemented using blockchain technology.

## Myth 5: SSI can only be implemented using blockchain technology.

In many SSI pilot projects, the use of blockchain technology is being tested for the allocation and publication of signature keys. However, central alternatives can also be considered for this purpose. In general, one or more verifiable and publicly available data registers must assign (public) signature keys to organizations. The assignment usually serves as a basis for verifying organizations to classify the trustworthiness of identity documents.

Distributed and synchronized data storage in a blockchain-based solution enables wide acceptance and referencing of a common basis for the use of sovereign and other credentials. In this context, organizations can generate their own public decentralized identifier (DID) and issue credentials based on it. Users can manage digital identity credentials together with other credentials in an ecosystem of SSI-based identities and use them in combination in one process. Individuals and organizations should be able to dispose of their digital identity without depending on a third party. This is important because DIDs can form the basis of any identity and communication system because, without them, there are no relationships, transactions and messages between entities (Sabadello, 2017). In addition, new schemas for verifiable identities can be easily registered in the network and thus made referencable and usable for issuing institutions in credential definitions.

Another advantage comes with revoking issued credentials, which can prevent correlation of users through the use of tails files and accumulators and thus protect privacy despite public availability[9]. A blockchain-based revocation registry enables improvements in the availability of revocation information and empowers users to prove the validity of their identity credentials without contacting the issuing parties again. In contrast, PKI-based identity solutions work with interactive services that check the validity of the certificates when requested and thus enable the correlation of the users. Another advantage of blockchain-based SSI architecture is the immutability and transparency of the transaction history, which, among other things, allows the addition of new schemas, credential definitions or entries in the revocation register, as well as the adjustment of rights and roles, to be stored in a publicly visible manner. Furthermore, points of attack or failure can be reduced for blockchains. If individual DIDs or nodes are compromised, this only affects a few issuer services but not the entire system (see myth 4).

However, using a blockchain increases the complexity and thus offers potential for attacks. In particular, the applicability of revocation possibilities via blockchain-based registers involves a high degree of complexity. In this case, cryptographic concepts are applied that requires a profound understanding and sophisticated security system. Access-restricted blockchain-based systems such as Hyperledger Indy do often have major challenges in terms of write operations performance (Sedlmeir et al., 2021). However, when the blockchain is used correctly – predominantly for reading for which horizontal scaling is possible – these do not pose significant problems in the case of SSI. In particular, the performance issues of the mobile digital driver's license in the ID wallet is unrelated to the blockchain component[10].

In addition to implementing a revocation register, fundamental questions arise regarding the governance of such a network. Careful evaluation is required as to which entities can be trusted to operate each node on the network. If node operators harbor malicious intent, they could potentially attack the network and take over the entire system. Consequently, this would lead to a loss of trust in the system and the organizations involved. Furthermore, it is crucial to define an overarching governance system in advance regarding the management of roles and rights, for example, to allocate the necessary access and write rights for changes on the blockchain ledger to the corresponding organizations. Compared to established CA and PKI

[9] See the documentation on Tails Files and Accumulator.

[10] For the performance of the Hyperledger Indy blockchain used, see Sedlmeir et al. (2021).

structures, blockchain technology is still at an early stage and must first prove itself in practice as an alternative decentralized trust anchor and guarantee authentication at an appropriate level for all applications over a longer period (German Federal Office for Information Security, 2021).

As mentioned above, a centralized solution using CAs and PKI could also assign, manage and authenticate public keys to a person or organization on the Internet. Especially if applications are to achieve an increased level of security, which for example, require eIDAS-compliant authentication. In this event, PKI-based solutions should be considered (German Federal Office for Information Security, 2021). Moreover, PKIs lend themselves when a high level of trust in centralized entities already prevails. However, the question arises as to who this trusted entity should be in a centralized scenario. In Germany, legally defined requirements for digital certificates and qualified electronic signatures apply according to the Trust Services Act[11]. The CAs are subject to the supervision of the Federal Network Agency, which guarantees the integrity of the certificates in legal transactions.

On the other hand, verification bodies may be composed of several entities, especially if governance is considered in the bigger European picture. Similar to the International Civil Aviation Organisation (ICAO), there are already overarching standards for issuing and verifying e-passports. In this context, each country establishes a national root certification authority for signing (CSCA[12]) as a trusted authority. The national CSCA creates the root certificates (CSCA certificates) and signs certificates required for signing data on (ID) documents. These document signer certificates can then be used, for instance, by passport manufacturers. Subsequently, the digital signature on a passport can be verified against the CSCA's root certificate.[13]. This approach hence provides a practically, decentralized, and standardized alternative to a blockchain infrastructure at European level, as the involvement of a national certification authority can be hardly contested.

Overall, blockchain technology is experiencing great momentum in the industry, various countries, and in different SSI projects (e.g., Hyperledger Indy), which can contribute to a cross-border ecosystem of compatible digital wallets with innovative privacy-protecting features and well-resolved revocation capabilities. In the future, however, there may also be SSI-based ecosystems that allow multiple different registries on a centralized and decentralized level for the allocation and verification of cryptographic keys.

[11] See Gesetzestext.
[12] see example on Country Signing Certification Authority (CSCA).
[13] See Explanation of the BSI.

## Myth 6

In SSI, personal data is stored on a blockchain.

## Myth 6: In SSI, personal data is stored on a blockchain.

With a blockchain-based SSI solution, just like with the use of centralized alternatives (e.g., CAs), data protection requirements must be met. The big difference between blockchain-based systems and centralized alternatives is the immutability of the transaction history and the replication of data on multiple nodes with a blockchain-based registry. Due to the characteristics of blockchain in terms of transparent and unchangeable data entries stored on many nodes, challenges arise in dealing with data protection regulations, such as the GDPR (Sedlmeir et al., 2022).

In other use cases in which personal data is processed on a blockchain, upstream pseudonymization is usually carried out to enable subsequent anonymization and thus deletion of the personal reference. A good anonymization method, however, is characterized by the fact that it can only be removed with disproportionate effort using technical aids[14]. It should also be noted that users can revoke their consent to data processing at any time[15]. Due to the immutability, data on blockchain-based systems can usually no longer be changed afterward. In this context, it is very difficult for users to exercise their right to adjust incorrect data or to delete data on blockchains.

Consequently, when using a blockchain infrastructure, care must be taken to avoid personal references of data as well as the disclosure of internal company and machine data as a matter of principle (Schlatt et al., 2021; Sedlmeir et al., 2022). It is important to determine whether the data is personal data. For example, the legal evaluation of the SSI prototype of the Bavarian State Office for Taxes, which was implemented based on blockchain technology, shows that a legally compliant design appears possible. However, not all data protection risks in the use of blockchain technology can be evaluated in this project, as there is currently still a lack of clear legislation in this regard (Guggenberger et al., 2021).

In the context of the SSI pilots of the Federal Chancellery, data protection requirements are complied with when issuing and verifying credentials in the digital wallet (see myth 3). The use of blockchain technology in this pilot project only serves to store public key material (public keys and DIDs) of issuing parties and as a decentralized verification infrastructure. No personal data is written to the blockchain ledger during the issuance or the verification process. In particular, individuals' identity attributes and public keys are never written to a blockchain but are stored in the users' digital wallets and shared bilaterally with verifying parties. Moreover, as discussed in Myth 5, the use of ZKPs in a blockchain-based revocation registry does not allow any inferences to be made about individuals by correlation. It should be noted that credential issuing institutions have a natural interest in data due to the use case requirements which also comes with legal consequences, e.g., information about the expiry date of an ID card or a revoked driver's license. Thus, issuing entities always process and control personal data in their own databases – regardless of whether a blockchain is used or not.

One exception where exclusive local storage by end users is not possible is for managing revocation. Many SSI implementations choose to store revocation-related information in a revocation registry on a publicly accessible blockchain. This revocation registry on the ledger always refers to an existing credential definition and contains compressed and anonymized information about the currently revoked or valid credentials in the form of a cryptographic accumulator. This accumulator does not allow third-parties (beyond the credential holder) to derive information about the credentials whose validity the accumulator represents. It also contains the URI of the tails files and its hash value. When a credential is issued, users receive the index value and a key figure (the product of all other accumulator values in the tails files), i.e., the witness. On the ledger, the issuing organization's

[14] cf. Article 4 sentence 5 GDPR.
[15] cf. Article 7, sentence 3, GDPR. Except for Article 6, sentences 1b) to f).

new accumulator value is updated periodically and globally in the revocation register to revoke credentials that have in the meantime been found to be erroneous or stolen. When the credential is presented, a corresponding delta between the previous and the new witness is derived via the updated accumulator value. The index value in the tails files does not change. During the verification process, users prove that they have valid credentials by cryptographically proving that they know a certain entry in the tails files with the help of the public accumulator value stored on the blockchain. In this process, users do not need to reveal information about their credential that would allow a verifying party to track previous or future usages or revocation-related events associated to this credential. Verifying parties are not required to contact issuing institutions or check a black list. With this approach, users can hence demonstrate the validity of their credentials in an innovative and privacy-compliant way.

## Myth 7

SSI-based identity solutions are inefficient and consume much energy.

## Myth 7: SSI-based identity solutions are inefficient and consume much energy.

In general, the development of SSI is intended to address the weaknesses of existing digital identity management systems. The principles of controllability, portability and security of SSI identities must be taken into account in order to release the potential of an overarching SSI ecosystem (Allen, 2016). Overall, an SSI-based solution should make digital identities convenient, privacy-protecting, and manageable across various providers using a digital wallet. Users are free to choose a digital wallet app from a specific provider, which the German Federal Government promotes through open competition. In this light, fostering competition avoids a lock-in effect as with SSO services.

Despite the complex and innovative technical infrastructure, users can be guided through the issuing and verification process in their wallet app in a very user-friendly way if it has been designed to such an extent (see myth 2). For example, users are actively notified by verifiers of what data is requested and can agree or decline to share data with just a few clicks. However, given potential man-in-the-middle attacks by unauthorized verifying organizations, any risk mitigation measures should be considered and implemented during development (see myth 4). Ultimately, users manage their identity documents together with other credentials in one hand – digitally and decentrally on the smartphone. Moreover, issued credentials can be used throughout Europe and save routine administrative procedures, e.g., when moving at home or abroad, or identification procedures, e.g., when opening (bank) accounts (Schlatt et al., 2021). In this respect, an SSI solution is not a complex system for end users and can be very practical in everyday use (see myth 2).

For software developers, on the other hand, the cryptographic primitives used, the interaction of innovative, sometimes immature open-source software components provided by communities, and compliance with the associated technical standards can lead to difficulties. In this context, for example, compared to the simple verification of digital signatures, ZKP are much more innovative and complex and, for this reason, can pose greater security risks (Kahlo, 2021). However, the currently used ZKPs have been mathematically known for 20 years and have been used successfully for a long time, especially in blockchain applications, without any known security problems.

The ZKP procedures currently used in common implementations also require special signature procedures, which results in limited flexibility for future adaptations and a lack of compatibility with secure key stores. On the other hand, there are currently great advances in much more general ZKPs that can address these two challenges. Further research is needed for a conclusive evaluation. In addition to ZKPs, adding a blockchain as a decentralized key allocation and verification authority can increase the degree of complexity (see myth 5). This raises further questions concerning governance as well as legal and security aspects. However, a blockchain is not immediately noticeable to users, as it functions as an infrastructure in the background. Nevertheless, due to the numerous, excessively positive reservations about blockchain technology in particular and negative reservations due to misconceptions such as those just described, researching the implications of using a blockchain on user acceptance might be meaningful.

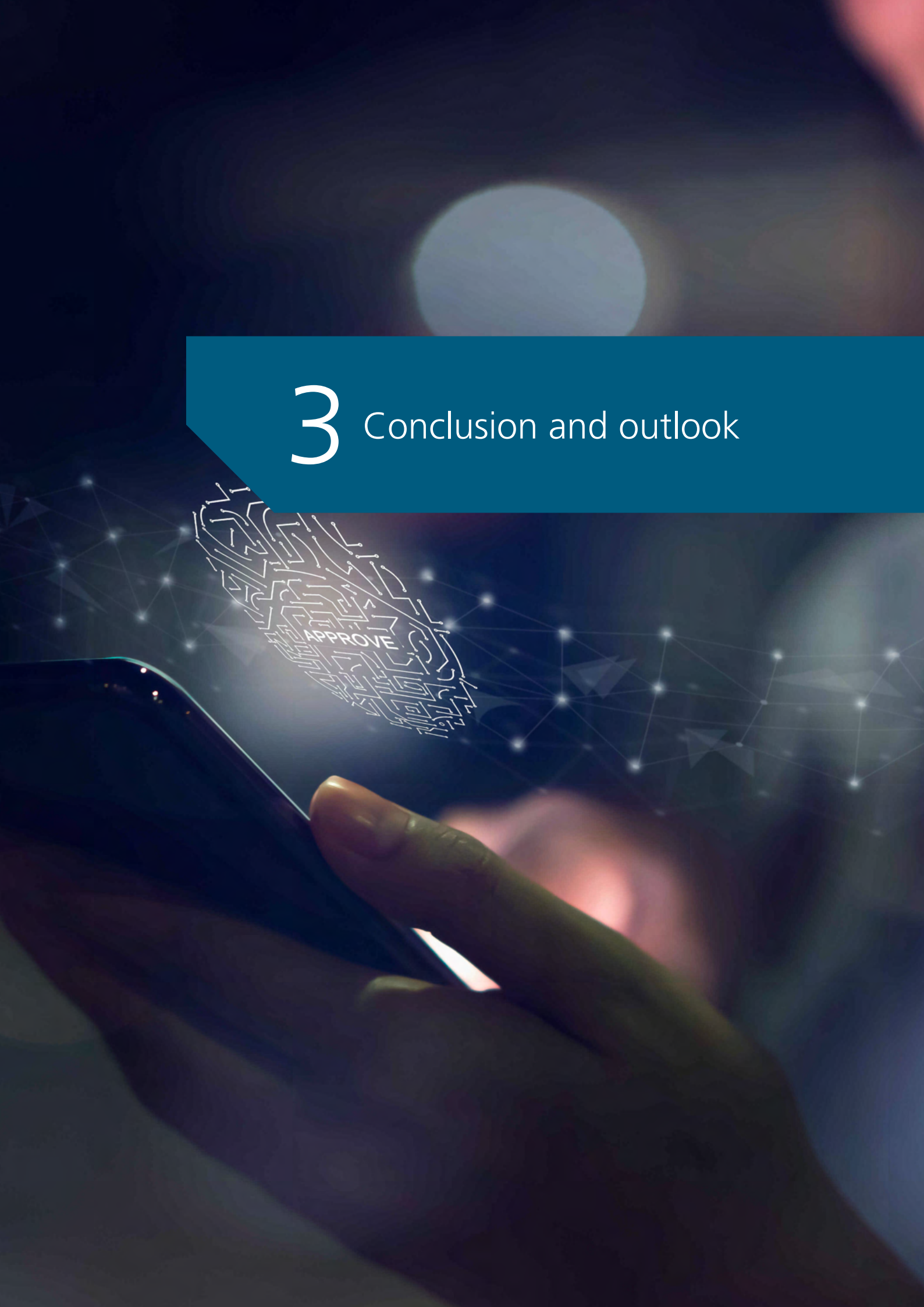
Considering the energy demand for the production of (special) paper and mobility, it can be assumed that the energy demand for issuing or verifying credentials will be lower than the previous paper-based identity management, which often requires presence. However, it is doubtful that a digital representation would make physical documents obsolete for many sovereign identity documents in short to medium term. However, the portability of credentials would at least eliminate the need for multiple (and sometimes paper-based) issuance, such as certified copies. Handling identity management by employing an SSI solution across different systems could also save costs through redundant administration, data storage and (paper-based) processes

at the state and private-sector organizations. In particular, the low error rate and time intensity of a fully automated cryptographic verification come into play (Schlatt et al., 2021). Furthermore, the increased data quality as well as data availability can considerably increase efficiency in different application areas and processes without entailing negative aspects such as lack of transparency and control over the transmission of sensitive data as described above with established identity management approaches (Strüker et al., 2021).

If a blockchain-based SSI solution is used, it cannot be compared with open, proof-of-work-based blockchain systems such as Bitcoin or Ethereum in terms of its energy consumption in the case of a restricted-access blockchain. It is important to distinguish between the design parameters and consensus mechanisms used for blockchains (see myth 4). In particular, access-restricted blockchain-based systems, where trusted entities operate nodes, have a significantly lower energy overhead than non-access-restricted blockchains, such as Bitcoin or Ethereum (Sedlmeir et al., 2020). If an open system is chosen, the aim should be to select a blockchain with a low-energy consensus mechanism, e.g., Proof of Stake, to ensure low energy requirements for this scenario.

The numerous publicly funded SSI projects of Germany's Federal Government and private industry use blockchains as a highly available and performant data storage to provide trust-inspiring data, providing a highly efficient synchronization mechanism. Using 30 nodes, one can estimate the energy demand to be about 30 times that of a central server, although central systems usually also have some inefficiencies due to backups. As a result, such a blockchain does not consume significantly more energy than conventional, centralized IT systems (Sedlmeir et al., 2020).

# 3 Conclusion and outlook



# 3 Conclusion and outlook

In this discussion paper, we presented opinions from the controversial public discourse on the topic of SSI and taken up, questioned, and discussed arguments that have been put forward. In doing so, we examined the added value of the concepts and technologies used from a scientific perspective and highlighted existing challenges. The myths examined in this context are primarily intended to help decision-makers in business and politics, IT specialists, and citizens to gain a better understanding of SSI and to support them in classifying the resulting opportunities and risks. We explore the topic from a multidimensional perspective with regard to the complex interrelationships between adoption barriers, data protection, and security, considering technical, governance-related, research-related, regulatory, and general aspects.

Germany is taking a pioneering role in the EU in developing an SSI-based digital identity ecosystem that comprises numerous projects in the public and private sector. Especially against the backdrop of a potential introduction of the eIDAS 2.0 regulation, Germany is setting the course early on for an interoperable SSI solution that could be implemented across Europe. To support and accelerate this process, Germany's Federal Government is acting as a pacemaker for an ecosystem of secure digital identities, which are defined by predetermined framework conditions, particularly those of the European Commission. In doing so, the Federal Government wants to enable fair competition in the digital economy. However, the practical opportunities for application are currently limited to mainly test and pilot status. In addition, the regulatory requirements in many domains must be adapted to enable the legally effective and widespread use of digital wallets. At the latest when the eIDAS 2.0 regulation comes into force, this step could be taken promptly at the national and European level.

Overall, SSI promises great economic potential through an increased level of security, flexibility, and privacy. In addition, SSI-based digital identities for companies and machines can increase efficiency in exchanging master data. This approach is already being tested in various pilot projects of the German Federal Government, and arguably relevant also beyond core identity-related applications, for instance, in the context of Industry 4.0 and personal $CO_2$-accounting. The development and adoption of an SSI-based identity solution can significantly accelerate the digital transformation in Germany and Europe and help to achieve goals such as those of the German Online Access Act ("Onlinezugangsgesetz")[16]. A European ecosystem of decentralized digital identities could also reduce the risks of centralized systems and strengthen independence. In this way, SSI could contribute to the digital sovereignty of Germany and Europe.

However, to develop such an ecosystem and realize the potential of SSI, several challenges still need to be addressed. SSI is highly dependent on a thriving ecosystem with many different use cases, as the added value of an identity solution scales with the number of possible uses. Especially when developing further use cases, the basic ID should be considered the fundamental digital credential for personal identities. With the help of a secure digital identity, users can have other proofs and identity documents issued quickly and efficiently and use them in everyday life in a self-determined manner. A high fragmentation of different solutions for digital identities, such as existing competing PKI solutions, can strongly limit the possible adoption of SSI. On the other hand, the interaction of existing eID systems for state-issued, highly regulated documents with SSI-based attestations for all remaining cases in a single digital wallet is also a realistic implementation option. An interoperable and scalable ecosystem of digital identities requires at least the pan-European standardization of technical components, such as the technical design of verifiable proofs and the corresponding fundamental trust structures. Here, the implementation of eIDAS in the past has already created a great foundation, which SSI-based approaches should take into ac-

[16] The Onlinezugangsgesetz obliges the federal, state, and local governments to make nearly 600 administrative services available in purely digital form by the end of 2022. Further information can be found here.

count and leverage. We also want to emphasize that the described advantages of an SSI-based identity solution, especially from the user's perspective, are only substantial and reliable using end-to-end encryption without any backdoor. In this sense, policy-makers in Germany and the EU level should be encouraged to define the framework conditions for such a solution. Improvements to the user experience of existing digital wallets are also still required and demand large-scale studies (Rieger et al., 2022; Sartor et al., 2022)

Furthermore, the implementation of digital identities must meet many requirements, especially from a regulatory, technical, and governance perspective. Many pilot projects in Germany are testing the applicability and practical fit of SSI in different use cases, using agile software engineering approaches. However, these SSI pilots' rapid and continuous development should not be at the expense of security. Technical standards and requirements must be met at all times. An SSI-based solution and its components must withstand the demands of production quality. In addition, technology assessments must be carried out continuously when designing and implementing new features or applications to identify potential risks at an early stage and use the associated opportunities of SSI in a more targeted manner. In any case, an open-source development of the components is desirable to allow a broad community of developers and experts to participate, test, and thoroughly examine the system.

A candidate for a regulatory framework for SSI has already been initiated with the eIDAS 2.0 proposal. In our opinion, an SSI-based approach could fulfill the legal requirements under eIDAS 2.0 very well and be a useful complement to existing eID implementations in less regulated areas. In this context, the German Federal Government must provide its citizens with a digital wallet within one year – another positive indicator for an SSI-based solution under eIDAS 2.0. We conclude that SSI offers the opportunity for an open technical system with easy onboarding that enables and promotes a European ecosystem of user-managed digital identities in which small and medium-sized organizations can also participate. Regulatory and technical aspects are heavily intertwined and must be considered in an integrative way.

# References


Alamillo-Domingo, N. (2020). ***SSI eIDAS Legal Report – How eIDAS Can Legally Support Digital Identity and Trustworthy DLT-Based Transactions in the Digital Single Market***. URL: https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf (visited on 05/07/2022).

Allen, C. (2016). ***The Path to Self-Sovereign Identity***. URL: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (visited on 05/07/2022).

Aublin, P.-L., S. B. Mokhtar, and V. Quéma (2013). "RBFT: Redundant Byzantine Fault Tolerance". In: ***33rd International Conference on Distributed Computing Systems***. IEEE, pp. 297–306. DOI: https://doi.org/10.1109/icdcs.2013.53.

Austrian Chancellery (AT) (2021). ***Schaffung einer digitalen Identität für alle Europäerinnen und Europäer***. URL: https://www.bundeskanzleramt.gv.at/themen/europa-aktuell/schaffung-einer-digitalen-identitaet-fuer-alle-europaeerinnen-und-europaeer.html (visited on 05/07/2022).

Boysen, A. (2021). "Decentralized, Self-Sovereign, Consortium: The Future of Digital Identity in Canada". In: ***Frontiers in Blockchain*** 4, p. 11. DOI: https://doi.org/10.3389/fbloc.2021.624258.

BR 24 Redaktion (Frank Jordan) (2021). ***Hunderte digitale Impfpässe gefälscht – Festnahme in München***. URL: https://www.br.de/nachrichten/bayern/hunderte-digitale-impfpaesse-gefaelscht-festnahme-in-muenchen (visited on 05/07/2022).

Camenisch, J., R. Chaabouni, and A. Shelat (2008). "Efficient Protocols for Set Membership and Range Proofs". In: ***International Conference on the Theory and Application of Cryptology and Information Security***. Springer, pp. 234–252. DOI: https://doi.org/10.1007/978-3-540-89255-7_15.

Castro, M. and B. Liskov (2002). "Practical Byzantine Fault Tolerance and Proactive Recovery". In: ***ACM Transactions on Computer Systems*** 20.4, pp. 398–461. DOI: https://doi.org/10.1145/571637.571640.

Chaosradio (2021). ***ID Wallet CR272 Wie die Union ihren Internetführerschein verlor***. URL: https://chaosradio.de/cr272-id-wallet (visited on 05/07/2022).

Delignat-Lavaud, A., C. Fournet, M. Kohlweiss, and B. Parno (2016). "Cinderella: Turning Shabby X.509 Certificates into Elegant Anonymous Credentials with the Magic of Verifiable Computation". In: ***Symposium on Security and Privacy***. IEEE, pp. 235–254. DOI: https://doi.org/10.1109/SP.2016.22.

Digital Identity and Data Sovereignty Association (DIDAS) (2021). ***Eine E-ID auf Basis SSI — welche regulatorischen Voraussetzungen müssen geschaffen werden?*** URL: https://www.didas.swiss/de/2021/12/17/eine-e-id-auf-basis-ssi-welche-regulatorischen-voraussetzungen-muessen-geschaffen-werden/ (visited on 05/07/2022).

Dingle, P. (2020). ***Advancing Privacy with Zero-Knowledge Proof Credentials***. URL: https://techcommunity.microsoft.com/t5/identity-standards-blog/advancing-privacy-with-zero-knowledge-proof-credentials/ba-p/1441554 (visited on 05/07/2022).

eIDAS Expert Group (2022). ***European Digital Identity Architecture and Reference Framework – Outline***. URL: https://cloud.eid.as/index.php/s/DQ5aRjyzJDNKXpW (visited on 05/07/2022).

European Commission (2021). ***Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EU) n° 910/2014 as Regards Establishing a Framework for a European Digital Identity***. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021SC0124&from=EN (visited on 05/07/2022).

German Chancellery (DE) (2021). ***Digitale Identität – Wie ein Ökosystem digitaler Identitäten zu einem selbstbestimmten und zugleich nutzerfreundlichen Umgang mit dem digitalen Ich beitragen kann***. URL: https://www.bundesregierung.de/resource/blob/992814/1898280/d9819a40553a9543b9e8f3acb620b0c2/digitale-identitaet-neu-download-bundeskanzleramt-data.pdf (visited on 05/07/2022).

German Federal Office for Information Security (2021). ***Eckpunktepapier für Self-sovereign Identities (SSI) unter besonderer Berücksichtigung der Distributed-Ledger-Technologie (DLT)***. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.pdf;jsessionid=0EE03D850260A455ECF294A830E0FB3E.internet462?__blob=publicationFile&v=2 (visited on 05/07/2022).

Goldwasser, S., S. Micali, and C. Rackoff (1989). "The Knowledge Complexity of Interactive Proof Systems". In: ***SIAM Journal on Computing*** 18, pp. 186–208. DOI: https://doi.org/10.1137/0218012.

Government, G. F. (2021). ***Ökosystem Digitale Identitäten: Nachweise für die digitale Brieftasche***. URL: https://www.bundesregierung.de/breg-de/suche/e-id-1962112 (visited on 05/07/2022).

Guggenberger, T. et al. (2021). ***SSI@LfSt: Einsatz der Blockchain-Technologie in der Steuerverwaltung***. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT. URL: https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Whitepaper_SSI@LfSt.pdf (visited on 05/07/2022).

Kahlo, C. (2021). ***Blockchain + SSI = ID?*** URL: https://medium.com/@ckahlo/blockchain-ssi-id-d7e51d98d050 (visited on 05/07/2022).

Lapienytė, J. (2021). ***Tech Giants Endlessly Exploit our Data. Who Will Put an End to It?*** URL: https://cybernews.com/editorial/tech-giants-endlessly-exploit-our-data-who-will-put-an-end-to-it/ (visited on 05/07/2022).

Liang, F., V. Das, N. Kostyuk, and M. M. Hussain (2018). "Constructing a Data-Driven Society:

China's Social Credit System as a State Surveillance Infrastructure". In: ***Policy & Internet*** 10.4, pp. 415–453. DOI: https://doi.org/10.1002/poi3.183.

Lissi (2021). ***Diskussion über die Sicherheit von Wallets für digitale Identitäten***. URL: https://lissi-id.medium.com/diskussion-%5C%C3%5C%BCber-die-sicherheit-von-wallets-f%5C%C3%5C%BCr-digitalen-identit%5C%C3%5C%A4ten-d1c6218fef66 (visited on 05/07/2022).

Lovejoy, B. (2021). ***Johns Hopkins Security Researchers 'Shocked' at Android and iOS Vulnerabilities***. URL: https://9to5mac.com/2021/01/14/johns-hopkins-ios-vulnerabilities/ (visited on 05/07/2022).

Munzinger, H. (2021). ***Pegasus auf die Schliche kommen***. URL: https://www.tagesschau.de/investigativ/report-muenchen/impfzertifikate-101.html (visited on 05/07/2022).

Muth, M. (2021). ***Nutzlos, unsicher und schon wieder kaputt***. URL: https://www.sueddeutsche.de/wirtschaft/fuehrerschein-digital-id-wallet-1.5425432 (visited on 05/07/2022).

Naik, N. and P. Jenkins (2021). "Sovrin Network for Decentralized Digital identity: Analysing a Self-sovereign Identity System Based on Distributed Ledger Technology". In: ***International Symposium on Systems Engineering***. IEEE. DOI: https://doi.org/10.1109/ISSE51541.2021.9582551.

PwC (2021). ***Der Online-Ausweis auf dem Smartphone und die digitale Brieftasche. PwC-Studie 2021: Bevölkerungsbefragung zum Online-Ausweis (Smart eID) und Self Sovereign Identities (SSI)***. URL: https://www.pwc.de/de/branchen-und-markte/oeffentlicher-sektor/pwc-studie-der-online-ausweis-auf-dem-smartphone-und-die-digitale-brieftasche.pdf (visited on 05/07/2022).

Rieger, A., T. Roth, J. Sedlmeir, and G. Fridgen (2021). "The Privacy Challenge in the Race for Digital Vaccination Certificates". In: ***Med*** 2.6, pp. 633–634. DOI: https://doi.org/10.1016/j.medj.2021.04.018.

Rieger, A., T. Roth, J. Sedlmeir, L. Weigl, and G. Fridgen (2022). "Not Yet Another Digital Identity". In: ***Nature Human Behaviour*** 6.3, p. 3. DOI: https://doi.org/10.1038/s41562-021-01243-0.

Sabadello, M. (2017). ***A Universal Resolver for self-sovereign identifiers. On any blockchain or other decentralized system***. URL: https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c (visited on 05/07/2022).

Sartor, S., J. Sedlmeir, A. Rieger, and T. Roth (2022). "Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets". In: ***Proceedings of the Thirtieth European Conference on Information Systems***.

Schlatt, V., J. Sedlmeir, S. Feulner, and N. Urbach (2021). "Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity". In: ***Information & Management***, p. 103553. DOI: https://doi.org/10.1016/j.im.2021.103553.

Sedlmeir, J., H. U. Buhl, G. Fridgen, and R. Keller (2020). "The Energy Consumption of Blockchain Technology: Beyond Myth". In: ***Business & Information Systems Engineering*** 62.6, pp. 599–608. DOI: https://doi.org/10.1007/s12599-020-00656-x.

Sedlmeir, J., J. Lautenschlager, G. Fridgen, and N. Urbach (2022). "The Transparency Challenge of Blockchain in Organizations". In: ***Electronic Markets***. DOI: https://doi.org/10.1007/s12525-022-00536-0.

Sedlmeir, J., P. Ross, A. Luckow, J. Lockl, D. Miehle, and G. Fridgen (2021). "The DLPS: A New Framework for Benchmarking Blockchains". In: ***Proceedings of the 54th Hawaii International Conference on System Sciences***. 54th Hawaii International Conference on System Sciences, pp. 6855–6864. DOI: https://doi.org/10.24251/hicss.2021.822.

Slamanig, D., K. Stranacher, and B. Zwattendorfer (2014). "User-centric Identity as a Service-Architecture for eIDs with Selective Attribute Disclosure". In: ***Proceedings of the 19th ACM Symposium on Access Control Models and Technologies***, pp. 153–164. DOI: https://doi.org/10.1145/2613087.2613093.

Sovrin Foundation (2021). ***12 Principles of SSI***. URL: https://sovrin.org/principles-of-ssi/ (visited on 05/07/2022).

Sporny, M., D. Longley, and D. Chadwick (2019). ***Verifiable Credentials Data Model 1.0: Expressing Verifiable Information on the Web***. URL: https://www.w3.org/TR/vc-data-model (visited on 05/07/2022).

Strüker, J. et al. (2021). ***Self-Sovereign Identity — Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten***. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, Bayreuth. URL: https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Fraunhofer%5C%20FIT_SSI_Whitepaper.pdf (visited on 05/07/2022).

Tsakalakis, N., S. Stalla-Bourdillon, and K. O'Hara (2016). "What's in a Name: The Conflicting Views of Pseudonymisation under eIDAS and the General Data Protection Regulation". In: ***Open Identity Summit***. Gesellschaft für Informatik eV.

Wittmann, L. (2021). ***Mit der ID-Wallet kannst Du alles und jeder sein, außer Du musst Dich ausweisen.*** URL: https://lilithwittmann.medium.com/mit-der-id-wallet-kannst-du-alles-und-jeder-sein-au%5C%C3%5C%9Fer-du-musst-dich-ausweisen-829293739fa0 (visited on 05/07/2022).

Wölbert, C. (2021). ***E-Perso: Der Personalausweis kommt in drei Varianten aufs Smartphone***. URL: https://www.heise.de/news/E-Perso-Der-Personalausweis-kommt-in-drei-Varianten-aufs-Smartphone-6194859.html (visited on 05/07/2022).

Wolf, S. and B. Nabben (2021). ***Handel mit falschen Nachweisen nimmt zu***. URL: https://www.tagesschau.de/investigativ/report-

muenchen/impfzertifikate-101.html (visited on 05/07/2022).
Zinkus, M., T. M. Jois, and M. Green (2021). ***Data Security on Mobile Devices: Current State of the Art, Open Problems, and Proposed Solutions***. URL: https://arxiv.org/abs/2105.12613 (visited on 05/07/2022).
Zivadinovic, D. (2021). ***Der Facebook-Ausfall und die ungeahnten Folgen***. URL: https://www.heise.de/news/Der-Facebook-Ausfall-und-die-ungeahnten-Folgen-6221349.html (visited on 05/07/2022).

## Branch Business & Information Systems Engineering

The Branch Business & Information Systems Engineering of Fraunhofer FIT combines the research areas of Digital Disruption, Digital Business, and Digital Transformation in Augsburg and Bayreuth. Its special features are interdisciplinary expertise in professional and technical topics of business and information systems engineering and information management and the ability to combine methodological know-how at the highest scientific level with a customer-and target- and solution-oriented approach. Our team currently consists of around 90 researchers and more than 140 research assistants. Our research activities are thematically bundled in various areas, which gives us extensive expertise in different areas of business informatics. This enables us to transfer current research results into practical solutions in applied research projects with numerous companies from different industries, thus creating long-term "win-win situations". In addition, we can incorporate the knowledge gained into our numerous lectures to provide our students with theoretically sound and practically relevant and up-to-date content. Our goal is to continue synergizing our range of topics with suitable research areas in the future.

## Fraunhofer Blockchain Lab

Based on these principles, the Fraunhofer Blockchain Lab was founded, which is characterized by the interdisciplinary combination of economic, legal, and technical competencies. Blockchain solutions are conceptualized, developed, and evaluated at the Blockchain Lab, which has become known far beyond national borders. Together with numerous partners from business and science, we are working intensively to comprehensively investigate the potential of blockchain technology and make it accessible. At our location in Bayreuth, we have supported companies and public sector institutions in several applied research projects and accompanied the development of individual and needs-based solutions in blockchain technology from a scientific perspective since our foundation in 2016. Even though blockchain technology became known through its first application as the basis of the cryptocurrency Bitcoin, it quickly became apparent that the actual potential of blockchain reaches much further. For example, in addition to business logic mapped by so-called smart contracts, user-friendly, independent, and privacy-oriented digital identities can also be implemented today with the support of blockchain. In 2016, we were one of the first organizations in Germany to publish a study in which we examined the basics, possible applications, and economic potential of blockchain technology as well as the role of intermediaries in various contexts. We have also received several awards for our work – including the Innovation Award Reallabore (Sandboxes) from the Federal Ministry for Economic Affairs and Energy and the eGovernment Award for our project with the Federal Office for Migration and Refugees. In 2021, we published a study on the SSI paradigm.