# Self-sovereign and Decentralized identity as the future of identity management?

Michael Kubach[1], Christian H. Schunck[1], Rachelle Sellung[1], and Heiko Roßnagel[1]

**Abstract:** Blockchain-based Self-sovereign and Decentralized identity approaches are seen by many as the future of identity management. These solutions are supposed to finally bring universally usable, trustworthy, secure, and privacy friendly digital identities for everyone and all use cases. This paper first presents the promises of this technological approach. It then discusses some apparent challenges for this new approach and their potential impact.

**Keywords:** Self-sovereign identity, Decentralized identity, identity management, IT-security, privacy, blockchain, distributed ledger.

## 1 Introduction

Market researchers still foresee a massive growth potential in the digital identity market [Di20a], [Wh19]. Efforts to provide high assurance electronic identities to European citizens date back by more than 20 years. However, from today's perspective one can argue that significant efforts into developing identity solutions with high levels of assurance have only led to very limited adoption: daily (or even monthly) use by citizens and uptake in the private sector is scarce in the vast majority of European member states (with a few exceptions [Ku20]). The private sector is dominated by the single-sign-on solutions that are in the hands of big international platform corporations and that only provide low levels of assurance.

Therefore, it is no surprise that new approaches based on high-impact technologies, such as distributed ledgers and blockchain, have attracted major attention in the last 3-4 years, both in industry and politics. These often called "Decentralized" and "Self-sovereign Identity" (SSI) solutions, claim to bring identity management to the next level.

However, these novel concepts have their own challenges. Many technologies in the identity management sector that were previously hyped as "revolutionary", such as CardSpace, Uprove, and Attribute Based Credentials, have failed miserably on the market [Up20],[Ro16]. So, the question we would like to address in this paper is the following: will Decentralized identities be able to survive the "hype" and truly live up to the high expectations?

This paper will thus explore the current promises and intentions that are associated with SSI based solutions. We conduct an overview analysis by summarizing the challenges for

[1] Fraunhofer IAO, Nobelstr. 12, 70569 Stuttgart, firstname.lastname@iao.fraunhofer.de

identity ecosystems (chapter 2) and by critically reviewing Decentralized and Self-sovereign identity solutions (chapter 3). We identify critical issues and constructively evaluate what is required for SSI to overcome the identified challenges (chapter 4).

## 2 Basic challenges for identity ecosystems

Although the world has become increasingly digital in every aspect of life for the last decades, a major problem remains the transfer of personal identity into the digital world. In this context, many issues have been addressed: privacy, security, data protection, interoperability, and user experience. However, what is substantially lacking is a digital ecosystem with sustainable business models and appropriate incentives for all participating entities that can ultimately drive uptake.

The development of secure and federated digital identities in Europe over the past 20 years was driven forward by initiatives such as the "Large Scale Pilots" Stork [Ta15] and Stork 2.0 funded by the European Commission. The results of these pilots formed an important basis for the eIDAS regulation. In Germany, the development of secure digital identities was primarily promoted by the government through the introduction of the electronic identity card (nPA). Despite eIDAS and the nPA, the everyday and private sector use of digital identities by citizens continues to be dominated by username/password applications and the use of single-sign-on systems controlled by big international platform operators, who offer only lower levels of assurance.

Research efforts regarding government issued eIDs have been ongoing and keep addressing missing building blocks for a potential market uptake. For example, there have been publicly funded projects (e.g. FutureID, SkIDenity [Sh15], [Si20]) that have developed an identity broker, which mediates between different identity and service providers, and thus provides a solution for a federated identity management across sovereign and private service providers. Nevertheless, despite of work that has already been invested by the research community and public sector, there are still major challenges being faced by the digital identity ecosystem and a broad use of eIDs has not materialized (except for niche markets, e.g. Estonia).

The identity market still faces problems associated with a complicated multi-sided market that leads to a “chicken or egg” problem [Zi12]. Creating sustainable and balanced trust relationships between identity providers, relying parties and users has also remained a challenge [Zi12]. From an identity provider perspective, there is still a key problem of generating sustainable business models as pointed out in reference [Ku13].

A relying party’s interest focuses on gaining more users or customers that are using a service provided [Zi12]. It favors identity solutions that provide easy onboarding of new customers, and a reasonable security at low cost. As for the relationships between relying parties and users, the challenge remains that these are influenced by indirect network effects and thus difficult to establish top-down.

The main determinant for uptake on identity schemes is still the number of applications and services where they are accepted.

In regards to the user, there have been many claims and assumptions to what features users would like to have in regards to privacy and security. However, these claims often neglect that privacy and security are just two among many other requirements user balance when making decisions and detailed user studies on those claims are often lacking. A study in relation to users' willingness to pay and their preferences regarding identity management systems [Ro14], finds that the users' willingness to pay is generally low and preferences of convenience often overtake privacy and security concerns. Overall, digital identity ecosystems continue to face the issue of generating sustainable business models for identity providers, and of addressing indirect network effects between key players of the identity ecosystem. These issues continue to hamper the uptake and reusability of digital identities.

## 3 Decentralized identity management and Self-sovereign identity

After describing some key challenges for any digital identity ecosystems, we are now focusing on what is being marketed as the future of digital identity management [Si18],[Ar17]. It promises the key to empower users to reclaim control over their data [Je19],[Al16], and to break the dominance of the platform giants in web identity management, e.g. through making identities easily portable [Va19],[Wa20]. In the following, we will first clarify necessary fundamental terms of Decentralized identity management and Self-sovereign identity concept before turning to the potential that is associated with the concept. Finally, we will take a brief look at current approaches implementing the concept.

### 3.1 Fundamental terms

A number of particular terms are frequently used in the context of Decentralized and blockchain-based identity management. To avoid misconceptions, we will briefly define the key terms without going into further detail – acknowledging that this is an evolving field and definitions are not universally established yet.

In traditional identity management, every service provider (or relying party) stores credentials of each user and enables them to authenticate directly to the business. However, this also means that the user needs to separately register and authenticate with each individual service they wants to use. Federated identity management simplifies this process for the user. Here, an identity provider or credential service provider as intermediary manages user credentials and enables the user to register and sign on to various service providers. Most blockchain-based identity management approaches, however, follow a user-centric model of identity management. This is supposed to address interoperability, security, and privacy concerns, given the privileged position of the

identity provider. In this model, the user controls their identity data and interacts directly with the service providers – without relying on a trusted intermediary. Verifiable information – credentials that the user received from credential issuers – are being shared by the user on a need-to-know basis. The blockchain as such is mainly used an integrity-protected "bulletin board" for a public key infrastructure (PKI) that supports the mapping of keys to identifiers [Le20]. Following the characterization of a blockchain as a Distributed Ledger Technology (DLT), this concept to manage public keys has been described as Decentralized Public Key Infrastructure [Mü18], [Al15].

Self-sovereign Identity (SSI) is a frequently used term for blockchain-based identity management approaches. The term is not always used consistently, but according to [Mü18], a few key properties of the concept have emerged. Those can be summarized as that a Self-sovereign identity management system allows users to fully own and manage their identity without having to rely on a third party. This can be traced back to the so called *Ten Principles of Self-sovereign Identity* proposed by [Al16] that apply a strong user focus to identity management. Parts of these principles had already been included in the *Seven Laws of Identity* proposed by [Ca05]. [Le20] characterize Self-sovereign identity as a bottom-up approach, where no single entity acts as central authority that has control over identifier origination and/or credential issuance. Identifiers and credentials are solely managed by the users, without requiring any permissions. This is contrasted by the top-down approach that is on the other side of a spectrum of possible organizational structures. In this approach, a central authority controls identifier origination and/or issuance while power may be delegated hierarchically through roles. Here, an owner of the system with control of its governance exists. However, as [Ku19] shows in a survey of blockchain-based IdM systems, the term SSI is used by solutions that do not completely follow a bottom-up approach as well.

Two technical concepts that are an essential part of most blockchain-based identity approaches are Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). Both are currently being developed by the World Wide Web Consortia (W3C), which also illustrates the ongoing standardization efforts around Decentralized identity management.

Recently, a working draft v1.0 for Decentralized Identifiers (DIDs), has been presented [De19]. DIDs are identifiers that can be used for credential exchange and authentication. Ownership of a DID is proven by demonstrating the possession of the private key associated with the public key bound to the DID [Le20]. According to the W3C, the term DID refers' only to the *Uniform Resource Identifier (*URI) with the format *"did:"<did-method-name>":" <method-specific-id>*, for example: *did:example:123ABCdef*. Other elements of the specification are the DID scheme, which is the formal syntax of a DID and the DID method that defines how to implement a specific scheme. This includes information on how to create, update, and deactivate DIDs. A DID resolver returns the DID document for a given DID that contains associated data describing the DID subject, such as public keys, other attributes and metadata [De19]. A universal resolver is currently in development by the Decentralized Identity Foundation (DIF). It is envisioned to enable interoperability between different Decentralized identity management solutions [De20].

The W3C recommendation for Verifiable Credentials (VCs) v1.0 [Ve19] defines a format for credentials that are key element in many blockchain-based identity architectures (but could be used in other architectures as well). A VC is a tamper-proof statement about the subject that is cryptographically signed by its issuer. Besides the statement, it contains metadata linking to the issuer, validity period, cryptographic schemes etc. The VC concept also needs to include a revocation mechanism, which needs to balance privacy aspects with effective revocation. This challenge can be approached in various ways and is one significant difference between the W3C's proposal for VCs and alternative implementations. While in an on-chain claims registry, such as proposed for Ethereum-based IdM systems, issuers can directly add and revoke claims [To17b], the W3C approach does not utilize such a registry. Here, the blockchain is only used to map identifier and authentication method. The W3C approach is more privacy-focused, but makes revocation more difficult and brings challenges regarding collusions between the issuer of claims with the claim holder as described in [Mü18]. Due to the problems associated with the storage of personally identifying information contained in claims on an immutable blockchain that result from regulations such as the GDPR, Ethereum-based IdM proposals are recently moving away from on-chain to off-chain claims as well [Br19]. Therefore, while the concrete implementation of VCs may differ, the fundamental concept of VCs is that of a cryptographically signed credential that is usually under the control of the user and can be passed on to a service provider/relying party. Using different cryptographic techniques, the service provider can check who issued the credential, whether it has not been revoked and to whom it has been issued. This is achieved without the issuer of the credential being directly involved in the process.

Private keys and credentials are usually managed by the user in a so-called wallet application. This is also the application to interact with other entities, e.g. to sign in for new services, and receive credentials. This application is often implemented on a smartphone, but can reside on other edge devices, such as a desktop computer, too [Le20], [So19]. Wallets can also be located on cloud computing infrastructure as cloud wallets or be provided by third parties as so-called custodial wallets. Then they establish a stable, always available endpoint for other services [Le20], [So18], [Ha19] and might also be used to recover credentials if a wallet on an edge device is no longer available. Finally, hardware wallets (USB sticks or smart cards) and paper wallets (private key and/or seed phrases and/or QR-Codes that are printed out on paper) serve as alternative options to back up and recover private keys [Le20], [So19], [Bl18].

### 3.2 Associated Potential

As mentioned earlier, the Decentralized approach is seen by many as the future of identity management [Si18],[Ar17]. Decentralization is often used as a "synonym for a better architecture: less monopoly/oligopoly, more control for the end user, more room for the market forces, etc." [Ku19]. However, to critically analyze the real potential it seems advisable to break this argument down.

The most prominently mentioned potential of Decentralized identity management is certainly to give users the ultimate control over their data. Ideally, portability lets users take their data out of the siloes of service providers and dependence on (trusted) third parties as intermediaries for the use of identity data is eliminated. This goes with a high level of privacy, which is particularly emphasized by the proposed solutions and plays a major role in the case for Decentralized identity management [Si18], [Ai18], [Je19], [Wa20], [Le20], [To17a]. The Decentralized, user-centric approach is also seen as a way to reduce the risk associated with large aggregated sets of identity data – both regarding hacks/leaks (e.g. Equifax) as well as misuse/manipulation (e.g. Facebook/Cambridge Analytica) [Go19a], [Va19], [So18]. Moreover, the solutions often integrate cryptographic schemes such as zero-knowledge proofs. Those enable the use of verifiable credentials with selective disclosure so that users can disclose identity data directly to service providers on a need-to-know basis, thus protecting the user's privacy even further [Le20], [So18], [Ab17].

Privacy, however, might not be a sufficient feature for the broad adoption of Decentralized identity management. Therefore, following the user-centric approach further, usability aspects are frequently stressed as well. Several Decentralized or Self-sovereign identity solutions promise to eliminate the username/password problem. They promise to achieve this via single-sign on (SSO) and/or logins via their smartphone wallet as well as biometrics [Ku19], [So18]. As all identity data is managed at the user side, it should be easy for them to keep data updated with all the services that they uses. Moreover, signing up for new services becomes easier if no forms have to be filled out as already existing identity data can be simply shared. On the other hand, this should also be attractive to service providers as it reduces friction from customer onboarding. If verified identity data is easily accessible, this could be used to reduce fraud and fulfil compliance requirements too e.g. from Know Your Customer/Anti-Money Laundering (KYC/AML) regulations. As the identity data could be shared directly from the user with the service provider, the service provider would not be dependent on a third-party identity provider that might profit from this relationship and/or constitute a point of failure [Go19b]. At the same time, businesses would not have to manage the user information themselves. Hence, they could be relieved from the associated costs and risks (e.g. for infrastructure, security) [Le20].

Finally, Decentralized identity management systems might have a potential to provide the ID-infrastructure for currently over one billion people lacking valid identity information that are thus excluded from even basic societal and business services. This can be refugees, stateless persons or people in areas lacking proper infrastructure [Je19], [Wa20]. Several initiatives are promoting digital identities to address this issue, for example the ID2020 Alliance [Di20b] and the World Bank's Identification for Development (ID4D) Initiative [Id20]. A number of proof of concept projects are/have been practically evaluating the use of blockchain based identity management for this use case [Wa20], e.g. the World Food Programme (WFP) in refugee camps and reported promising results [Bu20].

### 3.3 Approaches to Decentralized identity management

Blockchain-based, Decentralized identity management can be implemented in various ways. Three recently published papers analyze the different approaches, so that we refer to them at this point. Without analyzing actual projects, [Le20] discuss different approaches on a generic level according to the organizational structure (top-down vs. a bottom-up), different models for identifier and credential management, presentation disclosure, general system architecture design and the use of public registries. [Mü18] survey essential components of a Self-sovereign identity, highlighting differences in specifications and in actual projects/designs. In his extensive survey of market offerings for blockchain-based identity management, [Ku19] analyses 43 approaches with different levels of maturity and availability. The three papers show that despite these promises, the technology is still in a quite early stage with a number of questions unanswered. While standards are slowly forming, there is a significant number of competing approaches that are not necessarily interoperable.

## 4 Critical analysis of centralized identity management

As discussed in the previous section Decentralized identity management has created high expectations. Here we identify a number of critical challenges this approach is facing and that will need to be addressed in the future. An important driving force behind the development of SSIs was to enhance privacy and control for users by taking advantage of a distributed architecture and thus avoiding single points of failure as well as single points of control that exist in the conventional identity schemes based on PKIs and/or large-scale, international, platform based identity providers and brokers. However, privacy is merely one requirement among others and for broad user adoption ease-of-use, cost, reliability, and convenience are important criteria, which cannot be implemented without trade-offs. Even addressing the privacy protection goals by themselves requires trade-offs for example between transparency and unlinkability [Zi19].

During our work over the last two years, we have repeatedly identified the following challenges, without making a claim for completeness:

1. Building solutions while SSI technologies and standards are still under development and evolving rapidly
2. Self-administration of digital identities and private keys for non-technical users
3. Reliable and transparent revocation of SSI based credentials and claims
4. Absence of a natural trust anchor for DLT-based digital identities

### 4.1 Building solutions while SSI technologies and standards are still under development and evolving rapidly

There is currently a strong desire to demonstrate that SSI technologies are useful and can

live-up to their promise. A high number of demonstrators and prototypes have been presented, but existing solutions are still on a low to medium TRL (technology readiness level) with the highest being around a TRL6 (technology demonstrated in relevant environment) [Ho17].This considers that wallet applications found in App stores are still missing important functions, so that the solutions are not applied in productive environments. Therefore, developers are encouraged to rapidly customize and deploy SSI based solutions using the existing frameworks, such as Hyperledger Indy, Aries and Ursa. However, due to still ongoing rapid developments, the existing releases are not yet very stable and undergo frequent changes. For example, it might be challenging to reliably assess and certify the "level of assurances" (LoAs) of these solutions. While we believe that these issues will be resolved eventually, the development of production level applications is currently risky and could require expensive re-developments as technologies and standards are adjusted.

### 4.2 Self-administration of digital identities and key management for non-technical users

Self-sovereign management of digital identities implies that users manage their digital identities without the need to rely on third parties. To achieve the highest degree of privacy, users must thus take care of key management entirely by themselves. In this case, also key-recovery becomes the sole responsibility of the user with all associated risks and inconveniences in case of permanent loss. For most users, an appropriate balance between privacy and convenience needs to be achieved and thus third parties will need to get involved in key management and recovery.

For this reason, mechanisms like Decentralized Key Management Systems (DKMS), a global interoperable standard for portable digital wallets, which hold the user's private keys are being developed. DKMS shall enable users to rely on a third-party application to manage their digital wallets, and in particular aid with key recovery.

A completely Self-sovereign approach resembles users keeping their cash (credentials) in a safe at home, while using a third-party digital wallet application is similar to opening a bank account. DKMS then standardizes key recovery procedures (both offline and social) and ensures that users can easily move their accounts to another bank (portability) if they wish to do so.

However, standardization will not be sufficient. As banks underlie regulatory oversight, there will emerge a need for governance bodies that oversee the certification of portable wallet providers to ensure that these adhere to the DKMS standard.

Further, development, maintenance and certification of portable digital wallets will incur costs. Currently, it is unclear if users' willingness to pay will be sufficiently high to cover these costs, or whether new sustainable business models can emerge, that do not attempt to monetize user data.

Finally, advocates of SSI based solutions stress that "portability" is a truly unique concept that does not exist in traditional identity solutions. However, portability could easily be ensured via regulation in all traditional solutions as well. In both approaches, governance bodies are required to ensure adherence to standards and regulation.

### 4.3 Reliable and transparent revocation of SSI based credentials and claims

Most SSI schemes spend significant effort to achieve "unlinkability" (one of the six privacy protection goals [Ha15]: no one, neither the credential issuer nor verifiers, should be able to monitor credential use by the owner. The revocation of SSI based credentials and claims is thus not trivial since the "phone home" problem must be avoided: a credential verifier should not need to contact the credential issuer ("phone home") to verify that the credential has not been revoked. Mechanisms to circumvent this "phone home" problem have been developed in several SSI schemes [Ve19], [To18] and are currently being implemented.

However, there is another important privacy protection goal that is often in conflict and thus needs to be balanced with unlinkability: transparency. This gives rise to an important, so far unsolved problem: as all SSI schemes focus on unlinkability it has become impossible to monitor and audit credential use – even for the credential owner. This becomes problematic if a wallet is compromised: an intruder can just copy the associated private keys and then use the respective credentials. The credential owner might never become aware of the compromise since the key is not "missing". The complete absence of an audit log and thus of transparency regarding credential use prevents any systematic approach for credential owners to detect improper use by another party.

### 4.4 Absence of a natural trust anchor for DLT-based digital identities.

An important problem that SSI-based credentials must address is: How can one trust that the credential issuing entity is in fact the entity that it claims to be? If, for example, anyone could issue credentials in the name of "Harvard University" one clearly runs into a trust problem if someone presents a "Harvard University" Self-sovereign degree certificate.

Thus – if certificates should retain their value – SSI must deal with the very same problems that were addressed with centralized PKIs and Decentralized Webs of Trust years ago: to ensure that a public key is really issued by the entity that claims to have issued it. One might argue that one can eventually implement DLT based consensus schemes that implement mechanisms via which a community agrees on what is trustworthy. However, it is unclear if their speed and the associated costs to prevent attempts to introduce bias can compete with the ease at which fake accounts can be created at close to zero cost.

Therefore, most SSI schemes introduce centralized governance layers and trust frameworks with trust anchors and/or trust intermediaries to address this problem. However, those approaches destroy one of the main arguments for SSI, moving from an

open ecosystem to one with a dominant stakeholder (or cartel) acting as gatekeeper. Moreover, the developers (programmers) of the SSI components (crypto libraries, wallets etc.) still possess significant power, which requires users to trust them for being honest and competent (this aspect is mitigated by an open source strategy that is pursued by many solutions). As of the time of this writing, we are not aware of solutions that take a unique advantage of DLT architecture to develop a game changing new answer to this fundamental problem for identity management frameworks.

## 5 Conclusion

How game-changing will SSI be for digital identity management? SSI does not have an inherent answer to the problem of creating and managing trust anchors. The lack of audit trails for credential use and thus transparency can create severe problems for detecting compromised user accounts even for the legitimate account owners. Finally, efficient and convenient key management requires users to rely (to a varying degree) on cloud service providers. Approaches to build SSI Ecosystems for example according to the REAL framework [Bo19] show that Decentralized ledger technologies just dominate layer one out of four layers: the Self-sovereign aspects get increasingly diluted as the ecosystems are constructed. This is by itself not necessarily a negative outcome, but the question is whether such systems could not been built as well using conventional technologies without a DLT layer.

Apart from architectural/technological issues relating to the functional performance of the technology and at least as important is the question of adoption and economic sustainability of the innovation. So far it has not been demonstrated how the chicken and egg problem of attracting enough service providers/relying parties can be solved. Moreover, sustainable business models for such a Decentralized identity ecosystem that emphasizes privacy and data minimization still seem to be missing.

In addition, the focus on providing privacy in the form of unlinkability might actually not be the most pressing need for users of such systems. According to [Ro14], users do not value unlinkability (in form of privacy preserving credentials) as much as researchers often assume. In fact, the majority of the sample showed less willingness to pay compared to centralized solutions [Ro14].

Great attention should be paid to the new trust frameworks that are suggested. Rather than building completely new frameworks like SOVRIN, that slowly need to attract recognition and could suffer from a lack transparency, more conventional approaches, including the incorporation of Web of Trust technologies, should be considered. An interesting approach has been explored by the EU-funded project LIGHTest: LIGHTest has built a Global Trust Infrastructure based on the DNS system, which not only allows to easily check which public key belongs to which entity, but also to certify this entity according to which "trust scheme" (e.g. eIDAS) [Ro17]. With a non-binding and extremely lightweight integration of LIGHTest with DLT-based identities, an unwanted introduction of a PKI through the

back door can be avoided. The advantage of such approaches is that one can already rely on a trust root that is globally well established.

So, what is the ultimate advantage of DIDs and SSI? Without doubt, SSI brought a lot of new movement into the digital identity sphere. Businesses, governments and supranational bodies are paying attention and share the hope associated with this a novel approach. New possibilities emerge to overcome the challenges that hampered the successful and sustainable development of conventional digital identity ecosystems. This brings entrenched stakeholders with sometimes conflicting interests back together to the table, which could lead to solutions previously impossible. One important aspect that could drive success is that the DLT layer is not controlled by a single entity. This can encourage businesses to take advantage of market opportunities without being afraid to ultimately just support the growth of a platform operator. In this context, it remains to be seen whether sustainable business models for credential issuers, wallet operators, certification, and governance bodies will emerge.

## 6 References

[Ab17] Abraham, A.: Self-sovereign Identity: Whitepaper about the Concept of Self-sovereign Identity including its Potential. E-Government Innovationszentrum, Graz, 2017.

[Ai18] Forbes, https://www.forbes.com/sites/rogeraitken/2018/01/07/blockchain-to-the-rescue-creating-a-new-future-for-digital-identities/, accessed: 05.02.2020.

[Al15] Github, https://github.com/WebOfTrustInfo/rwot1-sf/blob/master/draft-documents/Decentralized-Public-Key-Infrastructure-CURRENT.md, 2015.

[Al16] GitHub, https://github.com/ChristopherA/Self-sovereign-identity, accessed: 05.02.2020.

[Ar17] Security intelligence, https://securityintelligence.com/reimagining-the-future-of-identity-management-with-blockchain/, accessed: 05.02.2020.

[Bl18] Blockchain Bundesverband, https://bundesblock.de/de/new-position-paper-self-sovereign-identity-defined/, accessed: 11.02.2020.

[Bo19] Medium, https://medium.com/@trbouma/Self-sovereign-identity-making-the-ecosystem-real-v2-536345a10738, accessed: 24.02.2020.

[Br19] GitHub, https://github.com/ethereum/EIPs, accessed: 06.02.2020.

[Bu20] World Food Programme, https://innovation.wfp.org/project/building-blocks, accessed: 13.02.2020.

[Ca05] Microsoft, https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf., 2005.

[De19] W3C, https://www.w3.org/TR/did-core/, accessed: 06.02.2020.

[De20] Identity, https://identity.foundation/, 2020.

[Di20a] MarketsandMarkets, https://www.marketsandmarkets.com/Market-Reports/digital-identity-solutions-market-247527694.html, accessed: 21.02.2020.

[Di20b] ID2020, http://id2020.org/, accessed: 13.02.2020.

[Go19a] Goodell, G.; Aste, T.: A Decentralized Digital Identity Architecture. Frontiers In Blockchain, Volume 2, 2019

[Go19b] Evernym, https://www.evernym.com/blog/5-ways-Decentralized-identity-will-cut-costs-and-grow-revenues/, accessed: 13.02.2020.

[Ha15] Hansen, M.; Jensen, M.; Rost, M.: Protection Goals for Privacy Engineering. In: 2015 IEEE Security and Privacy Workshops, San Jose, CA, p. 159-166, 2015.

[Ha19] GitHub, https://github.com/hyperledger/aries-rfcs, accessed: 11.02.2020.

[Ho17] European Commission, http://ec.europa.eu/research/participants/data/ref/h2020/other/wp/2016-2017/annexes/h2020-wp1617-annex-ga_en.pdf., accessed: 13.02.2020.

[Id20] World Bank, https://id4d.worldbank.org/, accessed: 13.02.2020.

[Je19] Accenture-insights, https://www.accenture-insights.nl/en-us/articles/identity-management-on-blockchain, accessed: 05.02.2020.

[Ku15] Kubach, M.; Leitold, H.; Roßnagel, H.; Schunck, C.; Talamo, M.: SSEDIC.2020 on Mobile eID. In: Lecture Notes in Informatics, Open Identity Summit 2015, Berlin, Germany, Bonn: Köllen, p. 29–41, 2015.

[Ku13] Kubach, M.; Rossnagel, H.; Sellung, R: Service providers' requirements for eID solutions: Empirical evidence from the leisure sector, In: Lecture Notes in Informatics, Open Identity Summit, Stuttgart, Germany, Bonn: Köllen, p. 69-81, 2013.

[Ku19] Kuperberg, M.: Blockchain-Based Identity Management: A Survey from the Enterprise and Ecosystem Perspective. IEEE Transactions on Engineering Management, p. 1–20, 2019.

[Le20] Lesavre, L.; Varin, P.; Mell, P.; Davidson, M.; Shook, G.: A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems. National Institute of Standards and Technology, 2020.

[Mü18] Mühle, A.; Grüner, A.; Gayvoronskaya, T.; Meinel, C.: A survey on essential components of a Self-sovereign identity. Comput. Sci. Rev, Volume 30, p. 80–86, 2018.

[Ro14] Roßnagel, H.; Zibuschka, J.; Hinz, O.; Muntermann, J: Users' willingness to pay for web identity management systems, European Journal of Information Systems, Volume 23, p. 36–50, 2014.

[Ro16] Roßnagel, H.; Zibuschka, J.; Hinz, O.; Muntermann, J.: Zahlungsbereitschaft für Föderiertes Identitätsmanagement. In (Hornung, G.; Engemann, C. eds.): Der digitale Bürger und seine Identität, Baden-Baden: Nomos Verlagsgesellschaft, p. 225-245, 2016.

[Ro17] Roßnagel, H.: A Mechanism for Discovery and Verification of Trust Scheme Memberships: The Lightest Reference Architecture. In: Lecture Notes in Informatics,

Open Identity Summit 2017, Karlstadt, Sweden, Bonn: Köllen, p. 81-92, 2017.

[Sh15] Cordis.europa, https://cordis.europa.eu/project/id/318424, accessed: 21.02.2020.

[Si18] Microsoft, https://www.microsoft.com/en-us/microsoft-365/blog/2018/02/12/Decen tralized-digital-identities-and-blockchain-the-future-as-we-see-it/, accessed: 05.02.2020.

[Si20] SkIDentity, https://www.skidentity.de/, accessed: 21.02.2020.

[So18] Sovrin Foundation, https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf., accessed: 06.02.2020.

[So19] Soltani, R.; Nguyen, T.; An, A.: Practical Key Recovery Model for Self-sovereign Identity Based Digital Wallets. In: 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress, Japan, p. 320–325, 2019.

[Ta15] European Commision, https://ec.europa.eu/digital-single-market/en/content/stork-take-your-e-identity-you-everywhere-eu, accessed: 21.02.2020.

[To17a] Sovrin Foundation, https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-sovereign-Identity.pdf., accessed: 11.02.2020.

[To17b] GitHub, https://github.com/ethereum/EIPs/issues/780, accessed: 06.02.2020.

[To18] Tobin, A.: Sovrin: What goes on the Ledger? Sovrin, Evernym, 2018.

[Up20] Microsoft, https://www.microsoft.com/en-us/research/project/u-prove/?from=https%3A %2F%2 Fresearch.microsoft.com%2Fen-us%2Fprojects%2Fu-prove, accessed: 25.03.2020.

[Va19] Van Bokkem, D.; Hageman, R.; Koning, G.; Nguyen, L.; Zarin, N.: Self-sovereign Identity Solutions: The Necessity of Blockchain Technology, Delft, 2019.

[Ve19] W3C, https://www.w3.org/TR/vc-data-model/, accessed: 06.02.2020.

[Wa20] Wang, F.; De Filippi, P.: Self-sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. Frontiers in Blockchain, Volume 2, p. 1–22, 2020.

[Wh19] McKinsey Global Institute, https://www.mckinsey.com/~/media/McKinsey/Business %20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%2 0key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx, accessed: 21.02.2020.

[Zi12] Zibuschka, J.; Rossnagel, H: Stakeholder Economics of Identity Management Infrastructures for the Web. In: Proc. 17th Nord Work Secure IT, Karlskrona, 2012.

[Zi19] Zibuschka, J.; Kurowski, S.; Roßnagel, H.; Schmuck, C.; Zimmermann, C.: Anonymization Is Dead–Long Live Privacy. In: Lecture Notes in Informatics, Open Identity Summit 2019, Garmisch-Partenkirchen, Germany, Bonn: Köllen, p. 71-82, 2019.