H. Roßnagel, C.H. Schunck, S. Mödersheim (Hrsg): Open Identity Summit 2022,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2022 63

eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI

Steffen Schwalm[1], Daria Albrecht[2], Ignacio Alamillo[3]

Abstract: The proposal for review of the eIDAS Regulation from 2021 has opened strong expectations for a deep change in traditional identity models. The user-centric identity model proposed starts with the creation of European Digital Identity Wallets that will enable citizens' control over their data in identification and authentication processes without control by entities providing the identification services. Likewise, with the proposed legal rules for giving legal certainty to electronic ledgers and blockchains, [eIDAS2]opens possibilities to decentralization, especially for the provision and management of user's attributes. The implementation of qualified trust services for attestations or electronic ledgers limits decentralization by requirement of a trusted 3rd party. Standardization will be key in assuring interoperability at the EU level. What are the challenges and opportunities of eIDAS 2.0? And what are the main focuses and needs of (European) standardization? These and other questions will be analysed and discussed in the paper.

Keywords: eIDAS, SSI, self-sovereign identity, identity model, digital wallet, eID

1 Introduction

Unique identification of legal or natural entities as well as their objects – the basement for a digital identity – allows the verification of companies (Do they really exist?), the person acting for the company (Do they really exist?) and their authorization (Is Alice authorized to act for company A?).

Digital identities are currently typically issued by a centralized authority. Despite the widely used but privacy critical social identities, the main electronic identification means of natural entities are government eID issued by member states. While Italian, Danish or Estonian eID are widely used, although notified on different Level of Assurance, the utilization of German eID is still low. Especially in those countries where little us of the government eID is made, many other identification procedures such as BankID (identification by bank and typically one time bank transfer), video identification or fully automated identification always based on a government (mostly notified) eID became popular in the different industries e.g. Finance, Insurance, Health Care or Public Sector. Current government eID and private identification procedures are mainly focused on natural or legal entities. But digital identities contain much more, such as attributes and

[1] msg group, Robert-Bürkle-Str. 1, 85737 Ismaning, Germany
[2] msg group, Robert-Bürkle-Str. 1, 85737 Ismaning, Germany
[3] Universidad de Murcia, C. Campus Universitario, 11, 30100, Murcia, Spain

cbe doi:18.18420/oid2022-05

evidence related to natural or legal entities like vaccination passports, authorization (power of attorney) or diplomas. Those proofs are currently mostly represented by digital documents in pdf or equivalent typically presented via mail, portals etc.

In parallel decentralized digital ecosystems occurred in the context of emergence of distributed ledger technologies. DLT by its distributed design makes it easy to establish decentralized digital business models cross-industry and cross-country between. The technology gains it`s biggest added value in transactions between > 3 parties which don`t trust each other and so trust in a distributed network which is immutable by design [Wer18], [Ko21], [Tr20]. In the context of DLT and decentralized ecosystems also the new paradigm of self-sovereign-identities has to be mtioned. SSI promise identity owner full control over its identity and attributes [Allen]. All identity information is stored decentralized and only the holder should decide whom he`ll give access or transmit identification information. One main postulate is that in DLT based on SSI a trusted 3rd party is not necessary anymore since DLT is used as decentralized PKI and immutable by design – so SSI may be trustworthy by itself [Wer18], [Ko20]. ENISA mentioned in one of it`s last reports that some main initiatives e.g. the strategic Show Case projects in Germany[4], funded by Federal Ministry of Econonmy and Climate Protection use DLT as decentralized PKI and emphasized the privacy advantages due to selective disclosure and Zero Knowledge Proof-Mechanism [ENISA22]. According to ENISA the utilization of DLT may be a step to created trust in SSI.

Currently SSI lacks the legal trust because current [eIDAS1] mainly focused on government eID not integrating the new SSI-paradigm. With the eIDAS Bridge the EU just developed possible legal and technical solution to bridge centralized approach of [eIDAS1] referenced to government eID and (qualified) trust services with decentralized manner of DLT and possibly SSI [Al20]. Accelerated by success of DLT and developments like [EBSI] in Europe but also the limited utilization of existing (centralized) eID, the EU-Commission just revised eIDAS and proposed a re-engineered regulation in June 2021 – recognizing decentralization on one hand and requirement of legal trust on the other one. This paper specifically focuses on whether the [eIDAS2] is complementary or contradictory to the Self-Sovereign-Identity (SSI) concept [Allen], how it may solve the challenge of legal trust in DLT and/or SSI and which challenges and chances the new version of eIDAS offers in respect to the digital identity models in Europe. In first step the main changes of eIDAS 2.0 will be described. Based on the paper discusses possible issue and contradictions between eIDAS 2.0 and SSI. The discussion focus on comparison of EU digital Wallet and the SSI-Principles, the chances and limits of decentralization in eIDAS 2.0 and last but not least the role of DLT in context eIDAS 2.0. The paper finalizes with a perspective on how eIDAS 2.0 and foreseeable underpinning standards should focus on to establish trustworthy self-sovereign identity including legal compliance and trust.

[4] Schaufenster sichere digitale Identitäten

2 Main legal changes in proposed new eIDAS 2.0

2.1 Overview

In June 2021, the European Commission published the proposal on regulation amending [eIDAS1] from 2014 with the aim to establish a framework for a European Digital Identity or, in other words, [eIDAS2]. The main goal of the proposed update is not a replacement but further development of [eIDAS1] in the context of decentralization and the upcoming SSI-paradigm, on one hand, but also the critical assessment and identified areas for improvement in [eIDAS1], on the other hand. The main changes in [eIDAS2] refer to electronic identification. Concerning trust services, only some additional services related to electronic identification were added and some logical gaps where closed.

2.2 Main changes on electronic identification and European Digital Identity Wallet

The main changes in eIDAS [eIDAS2] on electronic identification cover following topics:

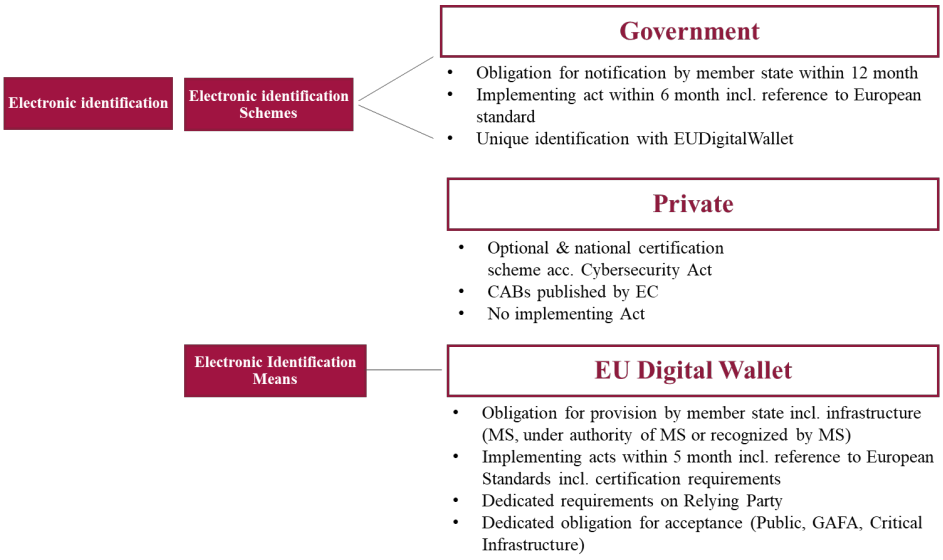

Figure 1: Proposal on [eIDAS2]: Main changes on electronic identification and European Digital Identity Wallet

[eIDAS2] proposal defines in Art. 6a the obligation for every member state to notify one identification within 12 months after the regulation will become applicable. Mandatory implementing acts referencing to European technical standardization shall be published

by European Commission within 6 months after new regulation is published. So, in comparison to [eIDAS1], the new regulation requires that at least one identity scheme from each member states shall be notified (Art. 10 and following). Considering that notification is one pre-condition for mutual recognition of identity, the obligation for notification can be mentioned as step forward in the wider utilization of eID in Europe. The presumable biggest change in [eIDAS2] is the requirements for every member state to provide a European Digital Identity Wallet to its natural entities. The Wallet could be published:

- By the member state
- Under authority of the member state
- Recognized by the member state

This makes also private wallet possible under the recognition of the member state. The European Digital Identity Wallet will contain the core identity currently covered by government eID as well as additional attributes or verifiable credentials acc. to W3C-standards so driver license, diplomas or the vaccine passport of its holder. This means that [eIDAS2] strictly follows the identity triangular of SSI. Every citizen will become a holder of a European Digital Identity Wallet and should become able to decide on his/her own, to whom he/she releases the identity information. The wallet consolidates core identity and attributes all together, but it must be taken into account that, due to cybersecurity reasons, the government eID will typically be stored on secure hardware components, normally a secure element or an e-sim, and only attributes will be stored in the wallet as a software component [Anke21], [TR03159]. In addition to that, the creation of (qualified) electronic signatures should be possible with the European Digital Identity Wallet. Technical details as well as security requirements for European Digital Identity Wallet will be defined in the ongoing European Standardization at ETSI and CEN. On the other hand, directly corresponding with the European Digital Identity Wallet, the new qualified attestation services acc. Art. 45a-e [eIDAS2] must be taken into account. Only qualified trust services providers offering such qualified attestation services are allowed to access European Digital Identity Wallet. Recognizing this close relationship between qualified attestation services and the wallet, [eIDAS2] contains the same requirements for mandatory implementing acts referring on European Standards for both – wallet and attestation service. Therefore, only the issuer into the European Digital Identity Wallet must be qualified attestation services. Consequently, [eIDAS2] crosses digital identity means and (qualified) trust services – they determine each other. To issue (qualified) attestation the trust service needs access to trust sources provided by member states e.g. public registries which requires their digital availability.

This means, in summary, that the new European Digital Identity Wallet will especially contain interface to qualified attestation service and relying party and shall fulfil LoA high acc. Art. 8 [eIDAS2]. The obligations on acceptance have to be emphasized: Not only public services, also any member of critical infrastructure entities (which means financial sector, utilities, health care etc.) as well as big internet companies such as

Google, Apple, Facebook or Amazon are forced to accept the European Digital Identity Wallet (Art. 12b). Similar to [eIDAS1], the member state is fully liable for providing the European Digital Identity Wallet as well as the eID-Scheme. A qualified attestation service takes the full liability risk like all QTSP, acc. Art. 13. This means that eIDAS limits the risk for users significantly in [eIDAS2] as well. The following picture, oriented on the Architecture Reference Framework [ARF 22] gives an overview on how the different parties may fit together:

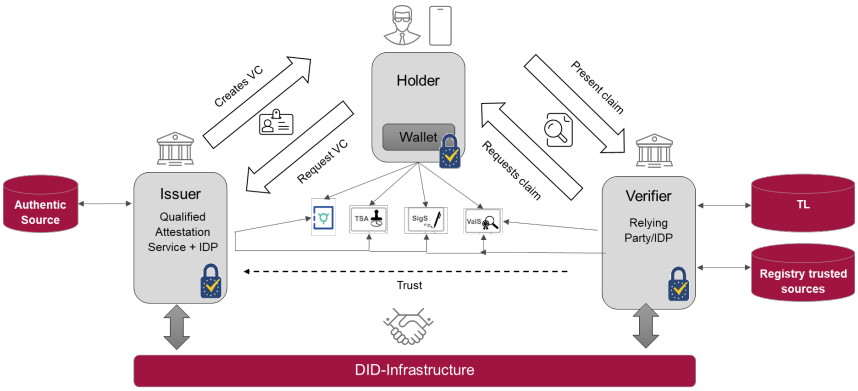

Figure 2: Possible interaction different parties in eIDAS 2.0

2.3 Main changes regarding (qualified) trust services and trust service providers

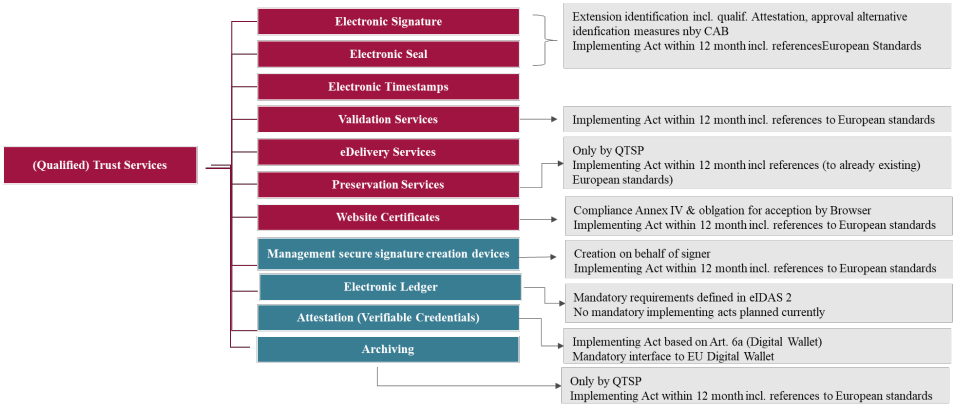

Figure 3: Proposal on eIDAS 2.0: Main changes regarding (qualified) trust services and trust service providers

In addition to the new qualified attestation services, [eIDAS2] also introduces the following new trust services for Electronic Ledger, so trust services for DLT (Art. 45g) This means that [eIDAS2] ensures trust in distributed ledger by (qualified) trust service

providers ensuring at least a minimum level of proven security and interoperability. Interestingly, [eIDAS2] does not contain the requirement of mandatory implementing acts referring to European standards only for the electronic ledger. Similar to [eIDAS1] all QTSP take the full liability risks (Art. 13) including the onus at their side – the trust chain is still the same [Ko21], [Zac20].

3 Possible issues and contradictions between [eIDAS2]and SSI

3.1 European Digital Identity Wallet and SSI-Principles

Since [eIDAS2] requires creation of (qualified) electronic signatures in combination with a wallet under the requirement of acceptance, the wallet might become the key tool for trustworthy digital transactions in regulated environments. Regarding the less success of only government issued eID in eIDAS 1.0 one main requirement for the success of EU-digital wallet is the distribution of providers. All possibilities given by eIDAS 2.0 so issued by member state, under authority of member state or recognized by member state should be used by all member states because the foreseeable competition of different public and private providers will ensure diversity according to different users' needs. The fact that EU Digital Wallet has to be issued to every legal or private entity in Europe eIDAS 2.0 achieves principle of representation and equity, the need for certification against European standards ensures it`s interoperability. With their wallet the user decides about relying party he wants to interact – the control of wallet it always on user`s side. eIDAS 2.0 contains obligation for acceptance but not utilization of wallet for the user and at same time opens the ecosystem for all interested parties as long as they fulfil the security requirements on e.g. trust services or relying parties [Al22]. With clear identification and authentication, the new regulation avoids a security findings and vulnerabilities like in German IDWallet where core identity information could be delivered to any unproven relying party without wither any identification nor authentication [FragSt21], [BSI19], [Ko20], [DINTS31648].

The table below gives an example how SSI-principles and [eIDAS2] may fit together:

SSI Principle	**Fulfilment by eIDAS 2.0**
Representation	Notified eID Scheme and European Digital Identity Wallet
Interoperability	Certified European Digital Identity Wallet, conformity assessed QTSP and notified eID as well as eIDAS nodes; Common European standards referenced by implementing acts

SSI Principle	Fulfilment by eIDAS 2.0
Decentralization	European Digital Identity Wallet and proven issuer as well as relying parties
Control and Agency	European Digital Identity Wallet, proven issuer and relying party
Participation	Only obligations for acceptance - no obligation to use the wallet nor the identities
Equity and Inclusion	Equal regulation for whole EU and EFTA
Useability, Accessibility and Consistency	Certified European Digital Identity Wallet and qualified trust service providers based on common European standards proved by accredited CAB
Portability	Any identities or attestation from European Digital Identity Wallet can be moved. Details should be defined in European standards
Security	State of the art security requirements defined in common European standards mentioned by implementing acts. Proved by CAB during certification of wallet, relying party or conformity assessment of QTSP. Trust provable via TrustList
Verifiability and authenticity	Verifiability and authenticity of attestations, signatures, seal, timestamps provable via (qualified) validation services, attestation services etc.
Privacy and minimal disclosure	Ensured by European Digital Identity Wallet and the fact that only holder decides which information he`ll provide but due to fact that relying parties are approved, the holder can really be sure to whom he/she will provide which information. Selective Disclosure and ZeroKnowledgeProof included
Transparency	European-wide regulation with common acts and mandatory European standards

SSI Principle	Fulfilment by eIDAS 2.0
	which are the basement for notification of eID-schemes, certification of European Digital Identity Wallet, relying parties, QTSP and all information published

Table 1: Possible match eIDAS 2.0 and SSI-Principles

3.2 Decentralization and its limits in eIDAS 2.0

[eIDAS2] defines the main legal framework for trustworthy digital transactions with centralized and decentralized digital identities and in the consequence a valid records management in Europe. The regulations take into account that SSI is not implemented on a green field but in an existing environment where centralized digital identities are established, widely used and, in regulated industries, fulfil the legal requirements [Ko18], [Ko20] [Anke21]. If SSI should be a sustainable alternative instead of centralized digital identities, legal compliance and trust are main pre-condition and trust given by notified eID-Scheme, certified EU-DigitalWallet and verifiable credentials by certified and supervised qualified attestation services which are fully liable. This means [eIDAS2] ensures a trustworthy decentralization with the entanglement of legal requirements in the law and its implementing act with mandatory European standardization. Clear and proven liability, security and interoperability of trust services and identity enable legal certainty of SSI with the disadvantage that a full decentralization with self-created credentials independent from any trusted 3rd party is not possible. In parallel, [eIDAS2] ensures with its mandatory implementing acts the achievement of SSI-principles on interoperability, security and so participation, equity and inclusion. The reason is that the implementing acts will reference common European standards for all member states and ensure same technical framework for each European Digital Identity Wallet and SSI in Europe in accordance with the SSI-Principle of representation [Ku20].

The fact that [eIDAS2] requires notification of government issued eID (or recognized/under authority of/by member state) as well as certification of private identification scheme by CAB – same with European Digital Identity Wallet the new regulation limits the decentralization of SSI because a trustworthy 3rd party is always necessary under eIDAS, but also to fulfil burden of proof in any regulated industry [We18], [DINTS31648]. However, this apparent disadvantage is one main added value of eIDAS 2.0, because for the first-time self-sovereign-identities gain legal trust and become usable in regulated environments with its needs for burden of proof and documentation requirements which must be made evident in non-repudiated manner against trusted 3rd parties. [eIDAS2] ensures a legally compliant verifiability and proven security and makes execution of SSI principles on security, authenticity and verifiability possible. Without legal compliance SSI would remain academic [Al20], [Sedl21],

[Ko20]. By ensuring trust in SSI, [eIDAS2] also limits its decentralization and therefore creates the boundaries of decentralization and SSI principle of participation evident. If there should be reliability that the legal or natural entity is really what it seems to be, a verified and secure identification is essential. This procedure, however, would set an entry requirement for the participation in the ecosystem.

3.3 DLT in the context of eIDAS 2.0

Basically [eIDAS2] is technology neutral. Neither for the (qualified) attestations, nor the identification scheme nor the identification means a concrete infrastructure is required. No DLT is mandatorily needed to implement Self-Sovereign-Identity. SSI is much more an identity and access management concept where on one hand the identity holder decides to whom he will give which part of his identity information and on the other hand does not have to give the full identity information in all cases but only the needed parts. Technically no DLT is mandatorily needed for SSI – the attestations may also be created in a centralized PKI which would recognize the fact that a centralized authority – the qualified attestation service issues the attestation based on (typically centralized trusted sources provided by member states) [Co20]. Nevertheless, some SSI proposals make use of functions supported by DLTs, such as DID-anchoring (of information of the qualified attribute attestations) or revocation information propagation [Sedl21], [Ku20].

DLT currently lacks a clear and legally compliant identification of parties taking part in the network, as well as unique evidence for authenticity and integrity of its transactions. Regarding the fact that DLT is immutable by design this main property is in contradiction to privacy law e.g. GDPR and its rights of the affected person (e.g. right for erasure, right for correction). Same with lack of standards for interoperable data exchange of on-chain data what limits the right for data portability according to GDPR [Ko20], [DINSPEC4997]. Similar vulnerabilities are the less long-term crypto stability, preservation of evidence and Proof of Existence which is critical for utilization in regulated environments with their often-complex documentation requirements, burden of proof until the end of the common decade long retention period [We18], [Sa17], [Ko21]. Without fulfilling basic criteria for trusted transactions and records management DLT is not feasible to be used in regulated environments [DINTS31648]. With QTSP for DLT the eIDAS 2 ensures legal trust in DLT because the QTSP will foreseeably act as de facto gatekeeper. The other advantage is that [eIDAS2] just solve the liability problem in DLT. According to Art. 13 eIDAS every QTSP is fully liable for its business. Since Art. 13 was not changed, this also applies to QTSP for Electronic Ledger and implies a Public or Private Permissioned DLT to ensure that there is always a provider operating and providing the DLT-network. With this approach [eIDAS2] ensures proven security in DLT. Because DLT might be used as decentralized PKI for SSI especially the EBSI it`s difficult to understand why the [eIDAS2] proposal does not contain the requirements for mandatory implementing acts referencing European Standards for QTSP for Electronic Ledger.

4 Perspectives of eIDAS 2.0 and necessary standardization

The proposal on new eIDAS-regulation proposes the first regulation on trustworthy self-sovereign-identities gaining legal trust and compliance. With the obligation for member states to provide one notified eID-Scheme but also European Digital Identity Wallet for their member states, the new eIDAS ensures a secure digital identity for each citizen. The close combination of wallet and (qualified) attestation services ensure legal trust not only in self-sovereign-identities and verifiable credentials but also actual data sovereignty and proven security for the user due the notification of eID-Scheme, certification of the wallet as well as certification of the qualified trust service provider. The risk for the user of a European digital identity is limited because member states and QTSP take the full risk for their schemes, European Digital Identity Wallet and attestation. It´s positive that [eIDAS2]is technology neutral and does not require DLT as infrastructure for SSI but also mentions QTSP for Electronic Ledger and, in this way, achieves proven security and trust for DLT. The extensive requirements on mandatory implementing acts linked to European standards enable the technical harmonization and limit national specifics. The creation of coherent and comprehensible European standardization framework gains as more importance as the standards will be referenced by the mainly mandatory implementing acts acc. to eIDAS 2.0 proposal. Against this background the standardization should especially focus on eID-schemes, EU-DigitalWallet and Attestation services first. Delegated authentication protocols like OIDC and OAuth2 are established and so interoperability is not a challenge currently [Hue19]. In W3C the work concerning DID-resolver is ongoing [Resolv] – a collaboration would be meaningful to identify relevant subjects for Europe and ensuring international feasibility of European SSI-standardization [Bast22]. The standardization may also focus on interoperability between centralized and decentralized digital identities to ensure comprehensive digital transactions notwithstanding if the natural or legal entity owns wallet or stored their identities at a centralized identity provider and only shares them with a relying party. Standardization supporting eIDAS 2.0 shall avoid reinventing the wheel. There are established and feasible standards e.g. for creation or preservation of signature, seal, timestamps; thus, only the gaps should be closed [ESI].

Currently, [eIDAS2] and related standardization mainly focus to store core identity information based on notified identity scheme on hardware of mobile devices and only the attestation in the wallet software itself [TR03159]. This means that core identity information of European citizens will be stored in non-European hardware whose specification are not disclosed or completely open source. Necessary European standards should focus on appropriate security measures for a fully hardened but also interoperable wallet which technical specifications and implementations are open source and therefore completely provable for 3rd parties [BSI19], [Al20], [Ko20], [Ko21]. The ongoing work on eIDAS Toolbox should consider this. It is also worth mentioning that some critical issues should be considered in the final version. For instance, a clearer statement for the certification and acceptance of wallets provided by private companies against the requirements of European Digital Identity Wallet to avoid restrictions on competition

should be provided. Since DLT may be used as infrastructure for SSI, there also should be mandatory implementing acts in eIDAS with references to European standards to ensure technical harmonization. Regarding the SSI-principles, it can be stated that there is no fundamental contradiction with the [eIDAS2]to be seen. The [eIDAS2] makes it possible for SSI-principles to become reality recognizing that decentralization has to be restrained to an acceptable level for achieving legal trust and data sovereignty. If a holder can`t trust an identity, issuer or verifier, he cannot act self-sovereign.

Bibliography

[Al20] Alamillo Dr. I-: SSI eIDAS Legal Report. How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market. Brussels 2020.

[Allen] Allen, C.: https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md

[Anke21] Anke J. et al: Self-Sovereign Identity as the Basis for Universally Applicable Digital Identities. HMD 58, 247–270 (2021)

[ARF22] European Digital Identity Architecture and Reference Framework. Outline. 2022

[BSI19] Federal Office for Information Security (BSI): Towards Secure Blockchains. Concepts, Requirements, Assessments. 2019

[Co21] Corici A. et. al: Towards Interoperable Vaccination Certificate Services. 17th International Conference on Availability, Reliability and Security (ARES 2021) mGov4EU - Mobile Cross-Border Government Services for Europe 08 2021

[eIDAS1] Regulation (EU) No 910/2014 of the European Parliament and of the Council - of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. eIDAS, 2014.

[eIDAS2] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity {SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}

[ENISA22] DIGITAL IDENTITY. Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust. European Union Agency for Cybersecurity.2022

[ET20b] ETSI Group Report 003. Permissioned Distributed Ledger (PDL). Application Scenarios

[ET21b] ETSI TS 103 732 V1.1.1. CYBER; Consumer Mobile Device Protection Profile.2021

[GDPR] Regulation (EU) 2016/ 679 of the European Parliament and of the Council - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/ 46/ EC (General Data Protection Regulation). GDPR, 2016.

[Hue18] Huehnlein D.: Towards Universal Login. In: Roßnagel, H., Schunck, C. H.,

Mödersheim, S. & Hühnlein, D. (Hrsg.), Open Identity Summit 2020. Bonn: Gesellschaft für Informatik e.V.. (193-200). DOI: 10.18420/ois2020_18

[IS20a] ISO 22739:2020: Blockchain and distributed ledger technologies - Terminology, 2020.

[Ko20] Korte, U. et. al.: Criteria for trustworthy digital transactions – Blockchain/ DLT between eIDAS, GDPR, Data and Evidence Preservation. OpenIdentity Summit 2020. Lecture Notes in Informatics (LNI). Proceedings. Bonn 2020 S. 49-60

[Ko21] Korte, U. et. Al.: Records Management and Long-Term Preservation of Evidence in DLT. In: Roßnagel, H., Schunck, C. H. & Mödersheim, S. (Hrsg.), Open Identity Summit 2021. Bonn: Gesellschaft für Informatik e.V.. (131-142)

[Ku20] Kubach M. et. al.: Self-sovereign and Decentralized identity as the future of identity Management?. In: Roßnagel, H., Schunck, C. H., Mödersheim, S. & Hühnlein, D. (Hrsg.), Open Identity Summit 2020. Bonn: Gesellschaft für Informatik e.V.. (S. 35-47). DOI: 10.18420/ois2020_03

[Me80] Merkle, R. C.: Protocols for Public Key Cryptosystems. In: 1980 IEEE Symposium on Security and Privacy. IEEE, Oakland, CA, 1980. S. 122-134.

[OE17] OECD Digital Economy Outlook 2017. Organisation for Economic Co-operation and Development OECD, Paris, 2017.

[Resolv] https://github.com/decentralized-identity/universal-resolver

[Sedl21] Sedlmaier J., Smethurst R., Rieger A.: Digital Identities and Verifiable Credentials. Business & Information Systems Engineering 5/202

[TR03159-1] Technical Guideline TR-03159. Mobile Identities Part 1: Security Requirements for eIDAS LoA “substantial” Version 1.0 Draft 2 26. August 2019, Federal Office for Information Security. Bonn 2019

[Sa17] Sato, M.; Matsuo, S.'i.: Long-Term Public Blockchain: Resilience against Compromise of Underlying Cryptography. In ICCCN: 26th International Conference on Computer Communications and Networks (ICCCN) July 31-August 3, 2017, Vancouver, Canada. IEEE, Piscataway, NJ; 2017, S. 1–8

[Tr20] Treiber, K. Die Blockchain als zentrale Schnittstelle führt zur Verschmelzung unterschiedlicher Branchen. In: Die Zukunft ist dezentral. Frankfurt School of Finance & Management. Frankfurt 2020

[UN17] UN United Nations Commission on International Trade: UNCITRAL model law on electronic transferable records. United Nations, New York, 2017

[We18a] Weber, M. et al.: Records Management nach ISO 15489. Einführung und Anleitung. Beuth Verlag, Berlin, 2018.

[Wer] Werbach, K.: The Blockchain and the New architecture of Trust. Massachusetts Institute of Technology. 2018

[Zac20] Zaccharia et. al.: EU eIDAS-Regulation: Article-by-Article Commentary. Brussels 2020