European Review of Digital Administration & Law - Erdal
2021, Volume 2, Issue 2, pp. 89-108
ISSN 2724-5969 - ISBN 979-12-5994-752-9 - DOI 9791259947529 10

*Self-Sovereign-Identity & eIDAS: a Contradiction? Challenges and Chances of eIDAS 2.0**

Steffen Schwalm
(Principal Consultant & Senior Manager Identity & Trust - Msg systems ag)

Ignacio Alamillo-Domingo
(Researcher - iDerTec - University of Murcia)

ABSTRACT The proposal for review of the eIDAS Regulation published in June 2021 has opened strong expectations for a deep change in traditional identity models. The user-centric identity model proposed takes as point of departure the creation of European Digital Identity Wallets that will enable citizens' control over their data in identification and authentication processes without been controlled by part of the entities providing the identification services. Likewise, with the proposed legal rules for giving legal certainty to electronic ledgers and blockchains, eIDAS 2.0 opens possibilities to decentralization, in particular, for the provision and management of user's attributes. Simultaneously the implementation of qualified trust services for attestations or electronic ledgers limits decentralization by requirement of a trusted third party.

In any case, the success of eIDAS 2.0 relies on the development of common solutions. 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.

1. *Introduction*

Digital identities are the key for trustworthy digital transactions. Only if all actors in a process or ecosystem securely know with whom they are act digital trust will be ensured. Unique identification of legal or natural entities as well as their objects is the basement for a digital identity that allow the verification of companies (Do they really exist?), of the person acting on behalf of that company (Do they really exist?) and of their authorization (Is Alice authorized to act on behalf of company A?).

Currently, digital identities are typically issued by a centralized authority. Despite the widely used (but privacy exposed social identities) the main electronic identification means of natural entities are government eID issued by member states. The current eIDAS Regulation[1] established a coherent and holistic legal framework on digital identities and trust services in the EU and EFTA but was mainly focused on governmental electronic identification schemes and means. The utilisation of notified eID schemes and means differs a lot between the Member States. While Italian, Danish or Estonian eID is widely used although notified on different Level of Assurance and partly beyond, the utilization of German eID or the Spanish eID is still low in comparison to other identification procedures. These governmental eID are less used because of usability issues in comparison to other identification procedures, especially if for every new transaction a re-identification is required as it is e.g. in public services, health care or partly finance sector in Germany[2].

Especially in those countries where the government eID is less used, 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 have become popular in the different industries. This development also depends on industry specific regulation allowing additional digital identities beside notified eID e.g. AML, eHealth etc.

Current government eID and private

* Article submitted to double-blind peer review.

[1] Regulation (EU) n. 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.

[2] J. Anke, T. Ehrlich, D. Richter and M. Meisel, *Self-Sovereign Identity as the Basis for Universally Applicable Digital Identities*, in *HMD Praxis der Wirtschaftsinformatik*, vol. 58, 2021, 247–270, https://doi.org/10.1365/s40702-021-00711-5.

identification procedures are mainly focused on natural or legal entities. Digital identities contain much more such as attributes and evidence related to natural or legal entities like vaccination passports, authorization, or diplomas. Those proofs are currently mostly represented by digital documents. The relationship between the owner/holder of the document might be ensured by metadata or in case of signing by digital signatures but often those evidence exist only as paper, which limits the implementation of fully digital transactions[3].

In parallel decentralized digital ecosystems appeared, especially in the context of the emergence of distributed ledger technologies. DLT makes it possible to establish distributed digital business models in a cross-industry and cross-country fashion. The technology gains its biggest added value in transactions between three or more parties which don't trust each other but trust a distributed network which is immutable by design[4] instead.

In the development of DLT and decentralized ecosystems also the new paradigm of the so-called self-sovereign identities (SSI) occurred. SSI promise identity owners the full control over their identity and linked attributes. All identity information is stored decentralized and only its holder should decide whom he will give access or transmit identity information. One main postulate is that in SSI a trusted third party is not necessary anymore since DLT is used as a decentralized PKI and immutable by design, so SSI may be trustworthy by itself[5].

Currently SSI lacks legal trust because the current eIDAS Regulation is mainly focused on government eIDs not integrating the new SSI-paradigm. Accelerated by the success of DLT and developments like the European Blockchain Services Infrastructure (EBSI) but also because of the limited utilization of existing (centralized) eID, the EU Commission just reviewed the eIDAS Regulation and proposed a re-engineered eIDAS 2 Regulation[6] in June 2021 – recognizing decentralization on one hand and requirement of legal trust on the other one.

Overlooking those regulative requirements on a secure and unique identification of natural and legal entities as well as the fulfilment of burden of proof against third parties or privacy requirements on one hand and decentralized ecosystems on the other hand there's the question on how SSI may fulfil these requirements[7]. Against the background of the new eIDAS Regulation proposal which defines e.g. dedicated requirements on an EU-Digital Wallet, qualified attestation services as approved issuers for the wallet and so trustworthy third parties or trust service providers for electronic ledger the question arises if there may be a contradiction between eIDAS and the promises of decentralized identities and ecosystems.

Based on an introduction about current European regulation, the SSI principles and basic properties of DLT as well as requirements on trustworthy digital transactions, this paper provides an overview about the main changes in in the new eIDAS 2 proposal. In the next sections the authors give a short assessment about possible contradictions between eIDAS 2.0 proposal and the SSI principles. The paper concludes with a possible perspective and recommendations for further research and standardization.

2. *Current European regulation*

2.1. *The eIDAS Regulation*

The eIDAS Regulation which came fully into force in July 2016 provides a Europe-wide mandatory legal framework for digital

[3] J. Sedlmaier, R. Smethurst, A. Rieger and G. Fridgen, *Digital Identities and Verifiable Credentials*, in *Business & Information Systems Engineering*, vol. 63, n. 5, 2021, 603–613, https://doi.org/10.1007/s12599-021-00722.; M. Kubach, C. Schunck, R. Sellung and H. Roßnagel, *Self-sovereign and decentralized identity as the future of identity management*, in H. Roßnagel, C. Schunck, C. H. Mödersheim and D. Hühnlein, *Open Identity Summit 2020*, *Bonn: Gesellschaft für Informatik e.V.*, 2020, 35-47, DOI: 10.18420/ois2020_03.

[4] U. Korte, S. Schwalm, T. Kusber and K. Shamburger, *Criteria for trustworthy digital transactions – Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation*, in *Open Identity Summit 2020. Lecture Notes in Informatics (LNI). Proceedings*, 2020, 49-60.

[5] K. Werbach, *The Blockchain and the New architecture of Trust*, Cambridge, MA, MIT Press, 2018; A. Doerk, *An introduction to self-sovereign identity (SSI),* https://ssi-ambassador.medium.com/aninteroduc-tion-to-self-sovereign-identity-ssi-916eb42f0490.

[6] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 910/2014 as regards establishing a framework for a European Digital Identity. COM/2021/281 final.

[7] U. Korte, S. Schwalm, T. Kusber and K. Shamburger, *Criteria for trustworthy digital transactions – Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation*, 49-60.

identities and trust services. It enables trustworthy digital transactions between public administrations, companies, and citizens. The eIDAS Regulation contains two main parts: digital identities and trust services. Concerning identities, the eIDAS Regulation currently only defines requirements on identity of natural and legal entities. The focus is on government electronic identification schemes and identification means issued by member states. Although the eIDAS Regulation also contains the possibility of identification means issued under mandate of notifying member state or independently of the notifying member state but recognized by this Member State, in practice the issuance by Member States is the majority.

The eIDAS Regulation also focused on the notification of government identification schemes and the core identity of natural and legal entity so e.g. name, surname, address date of birth, place of birth etc. but no more additional attributes such as authorization of individuals, right of representation or further ones like diplomas, licenses etc. Technically those attributes e.g. may be added to digital identities but are currently not regulated under the eIDAS Regulation nor covered by the eIDAS underpinning technical standards, which limits their legal trust and interoperability[8].

The notification leads not only to mutual recognition –so any notified eID has to be accepted by any public administration in Europe– but also reporting obligations on security breaches as well as fully liability for the notifying Member State and therefore to a high level of trust for private and economical users, but only related to notified eID. For non-notified identification schemes and identification means the technical requirements etc. are defined nationally what leads to limitation of their legal and technical interoperability. It also has to be mentioned that the Member State is fully liable for its notified eID scheme as well as eID means based thereof.

The notification itself implies a peer review of the proposed identification scheme by other member states against European standardization. The obligation for recognition of notified eID currently only refers to public administration as long as they require them in their public services, but not for private companies[9].

Private identification schemes or means are only implicitly mentioned in the eIDAS Regulation – mainly according to Level of Assurance etc. Some member states also notified private schemes e.g. Italy or Estonia. Interestingly these are the member states with the widest utilization of their notified eID.

The levels of assurance from high to low according to Art. 8 eIDAS and 2015/1502[10] define dedicated security requirements on identity verification procedures (levels of assurance or LoA). They must be recognized by digital service providers to define which LoA is necessary to access the provided service. Such an assessment should be based on a risk management according to ISO 27005[11], comparing possible threats against impact and likelihood including any process of the considered service. This means the LoA defines which identification procedures can be used for a given digital services – the LoA does not depend on notified eID but on all identification procedures, also not notified ones.

Despite the notification of mainly government identification means under an identification scheme on a dedicated LoA the eIDAS Regulation does not contain a formal European wide certification process for identification means against a defined LoA. Only the module certification according to Art. 24 of the eIDAS Regulation allows the audit of identification schemes against LoA

[8] U. Korte, S. Schwalm, T. Kusber and K. Shamburger, *Criteria for trustworthy digital transactions – Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation*, 49-60; M. Kubach, C. Schunck, R. Sellung and H. Roßnagel, *Self-sovereign and decentralized identity as the future of identity management*, 35-47; J. Anke, T. Ehrlich, D. Richter and M. Meisel, *Self-Sovereign Identity as the Basis for Universally Applicable Digital Identities*, 247–270.

[9] U. Korte, C. Berghoff, T. Kusber and S. Schwalm, *Langfristige Beweiswerterhaltung und Datenschutz in der Blockchain*, in *DACH-Security 2018*, 2018, 177-191; D. Hühnlein, T. Hühnlein, G. Hornung and H. Strack, *Towards Universal Login*, in H. Roßnagel, C. H. Schunck, S. Mödersheim and D. Hühnlein (eds.), *Open Identity Summit 2020*, Bonn, Gesellschaft für Informatik e.V, 2020, 193-200, doi: 10.18420/ois2020.

[10] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) n. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[11] ISO/IEC 27005:2018. Information technology — Security techniques — Information security risk management.

substantial or higher, though it is executed nationally based on national regulation and standardization underpinning the eIDAS Regulation and is only valid for qualified trust service providers issuing certificates, but it does not provide a confirmation of a LoA in general. This means e.g. that in Germany the hurdles for certification of identification procedures not based on German eID card such as video-identification or self-identification is significantly higher than in other member states, leading to a competition between Member States regarding security and privacy requirements.

Some Member States have established their own certification schemes to assess public or private identification schemes against LoA despite notification and Art. 24. This contains certifications open for all interested parties but also confirmation procedures like in Germany. Those procedures allow the proof of an LoA beside notified eID and contain currently e.g. mobile identities derived from a (notified) eID, automated identification or BankID.

The certification is valid Europe wide but currently there is no pendant on EU-level: a vulnerability of the current eIDAS limiting the mutual recognition of such certifications as well as the interoperability of the underlying identification procedures.

Along with digital identities eIDAS also defines (qualified) trust services. They contain:

Creation (qualified) certificates for (qualified) electronic signatures, seals and/or timestamps.

Validation of (qualified) electronic signatures, seals and/or timestamps

(qualified) Electronic registered delivery services.

(Qualified) Preservation of (qualified) electronic signatures, seals and/or timestamps

(qualified) website certificates.

Cryptographic electronic signatures or seals make the authenticity and integrity of electronic records evident against third parties, a (qualified) timestamp gives a valid Proof of Existence (PoE) and evidence for the time of transactions. In all cases a successful validation and preservation is necessary. Any at least advanced signature, seal or timestamp from each qualified trust service provider must be accepted and validated by any public administration according to Art. 27 of the eIDAS Regulation[12].

Art. 24 of the eIDAS Regulation requires a unique identification of natural entities applying for a qualified certificate for qualified electronic signatures. The corresponding identification module must be certified by a conformity assessment body (CAB) before being used by qualified trust service provider. Aside from eID or qualified electronic signature, the possible identification procedures are defined nationally. This leads to fundamental differences between member states and competition on the lowest requirements. As a consequence, in Germany the requirements for alternative identification according to Art. 24 Abs. 1 b) are significantly higher than e.g. in Austria or Nordics with the result of competitive disadvantage for German QTSP.

eIDAS was underpinned by mandatory implementing acts. In the context of digital identities especially 2015/1502 has to be mentioned which defines the requirements on Level of Assurance further in the context of trust services 2015/1506[13] should not be forgotten which defines the mandatory signature formats for mutual recognition according to Art. 27 of the eIDAS Regulation.

In summary the current eIDAS Regulation follows the approach of a centralized digital identity *de facto* issued by member state or under its control. This means that eIDAS acts on the assumption of a government trust anchor for each digital identity so that a trustworthy third party issuing the eID is always needed. A digital identity without government trust anchor is not covered by eIDAS[14].

[12] U. Korte, S. Schwalm, T. Kusber and K. Shamburger. *Criteria for trustworthy digital transactions – Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation*, 49-60; Federal Network Agency, *Guideline for digital signature, seal, and timestamp formats as well as technical evidence data (Evidence Record) V1.0*, 2020; A. Zaccaria, M. Schmidt-Kessel, R. Schulze and A. M Gambino (eds.), *EU eIDAS-Regulation: Article-by-Article Commentary*, London, Bloomsbury Publishing, 2020.

[13] Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) n. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[14] D. Hühnlein, T. Hühnlein, G. Hornung and H. Strack, *Towards Universal Login*, 193-200; T. Wich, D. Nemmert and D. Hühnlein, *Towards secure and*

This does not mean the Member States have control over any transaction the owner of the eID is executing with its identity. It only means that the notifying Member State is responsible concerning security and liability – so ensuring government trust anchor. Beside implementing act, the eIDAS Regulation is also underpinned by a common European wide technical standardization framework from the European standardization organizations ETSI and CEN under mandate by European Commission. The standardization framework ensures interoperability of eID and trust services in Europe, in eID e.g. based on results from the STORK[15] project and based on eIDAS nodes and eIDAS minimal data set, regarding trust services through ETSI standards on QTSP and their devices[16].

The picture below shows the relation between legal and technical framework by the example of trust services[17]:

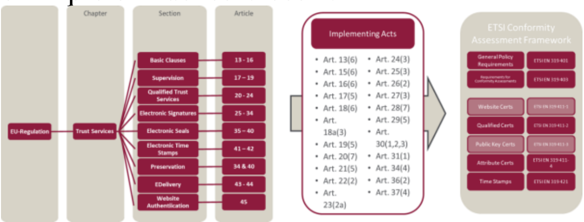

Figure 1: Relationship between the eIDAS Regulation and European standards

Apart from obligation on mutual recognition the utilization of notified identification schemes and identification means based on them is defined by Member States. So e.g. in Germany it is required to use an eID-server and client certified by the Federal Office for Information Security against its Technical Guidelines as well as possession of an authorization certificate to read the German eID-Card. The certificate is issued by Federal Office for Administration in a regulated process. These frame conditions also ensure a secure utilization of core identity data of natural entities by the identity provider so especially that the data are only used for identification in the given service and that no IDP would have an overview where the user will use his eID.

eIDAS created an EU- and EFTA wide trusted space based on trust chains between each of the actors acting as trustworthy 3rd parties. This means as shown at the digital identities that eIDAS always requires a trustworthy 3rd party. There´s no trust by default. Trust only occurs based on European law, supervised by European and national supervisory bodies, accreditation of conformity assessment bodies under European standards, certification of trust services by CAB under supervision of national supervisory bodies and verifiable via European wide trusted lists – so democratically created law, mutual control and certification but also transparent verifiability. The picture below illustrates these trust chains by example of trust services[18]:

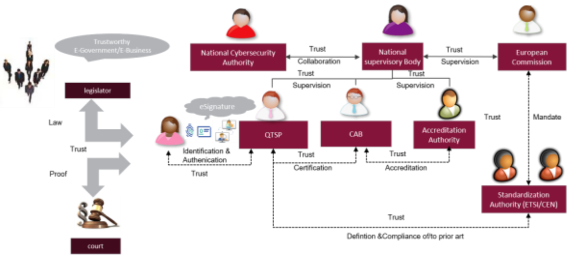

Figure 2: Trust chain in eIDAS

This trust chain also includes the fact that any QTSP is fully liable for its actions and the burden of the proof is on the QTSP (Art. 13 eIDAS); otherwise also the CAB is liable for its conformity assessment, the Accreditation body for accreditation etc. This means that eIDAS limits the liability risk for the user of QTSP significantly.

2.2. *GDPR*

Furthermore, the General Data Protection Regulation GDPR [Re16] has to be recognized to ensure the confidentiality of personal data in digital transactions. The

standard-compliant implementations of the PSD2 Directive, in L. Fritsch, H. Roßnagel and D. Hühnlein (eds.)*, Open Identity Summit 2017*, Bonn, Gesellschaft für Informatik e.V, 2017, 63-80.

[15] http://science2society.eu/content/stork-20.

[16] Vv.Aa., *eIDAS und der ECM-Markt Elektronische Identifizierung und Vertrauensdienste als Chance für die Digitalisierung*, Berlin, Bitkom, 2020; D. Hühnlein, J. Schwenk and T. Wich, *Moderne Vertrauensdienste für vertrauenswürdige Transaktionen: Ergebnisse des Forschungsprojektes "FutureTrust"*, in *Datenschutz und Datensicherheit – DuD*, vol. 43, n. 4, 214-219; D. Hühnlein *et al*, *Future trust-services for trustworthy global transactions*, in *Open Identity Summit, OID*, 2016.

[17] U. Korte, S. Schwalm, T. Kusber and K. Shamburger, *Criteria for trustworthy digital transactions – Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation*, 49-60.

[18] U. Korte, S. Schwalm, T. Kusber and K. Shamburger, *Criteria for trustworthy digital transactions – Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation*, 49-60.

technical and organizational measures to ensure confidentiality of personal data acc. to GDPR[19] can also be used to keep trade and business secrets to achieve a holistic management of protective records. In Art. 6 GDPR, the obligation for information (Art. 13+14 GDPR [Re16]) as well as the rights of the affected person are in focus so right of access, right of rectification, right to erasure and right of data portability. These obligations and rights require not only organizational and technical measures included in a well-defined data protection management system but also the technical ability of the applied IT-system to change, export or delete personal data as well as a defined access management or functionalities to decrease amount of the processing of personal data.

Taking into account retention periods for decades as well as existing documentation obligations and burden of proof the GDPR reflects the ensuring, preservation and evidence of the significant properties of electronic records: authenticity, integrity and reliability (e.g. evidence for consent, obligation of information, access, data portability), availability (e.g. rectification, erasure, portability). This means if DLT is used in processes where personal data are collected, managed and stored, the requirements of GDPR have to be fulfilled[20].

2.3. *Further regulation*

Besides eIDAS and GDPR different industry specific laws require a unique identification of legal or natural entities as well as evidence for authenticity and integrity of digital transactions against 3rd parties. Typical examples are AML-and PSD2-regulation[21] in financial sector, EASA Part 21[22] for aerospace, FDA[23] or GxP for pharma and life sciences of national regulation in health care or public sector.

The main focus of these regulations is the documentation and traceability of digital transactions to ensure burden of proof against 3rd parties like regulative authorities, courts, auditors etc. The authenticity, integrity etc. is afterwards ensured by utilization of secure digital identities and trust services according to eIDAS whose qualified electronic signature for instance makes non-repudiation and so authenticity and integrity of digital documents evident against third parties such as courts, regulative authorities, etc[24].

3. *Trustworthiness of digital transactions and records management*

Trustworthiness of digital transactions and records means that the process and the (authoritative) records created in the transaction are really what they seem to be and that this is provable by independent 3rd parties. Currently there is no regulation defining technology or institution as trustworthy by themselves. This means subsequently that there´s no trust by self-proclaiming only by proof. Trustworthy digital transactions ensure the unique and lossless evidence of authenticity, integrity, reliability of the electronic records which are created, received, stored and managed during the life cycle of transaction against independent 3rd parties as long as they are needed so until the end of the defined retention periods based on and compliant to existing laws (between 2 & 110 years or permanent)[25].

In accordance with applicable law and international standardization e.g. ISO 15489[26]

[19] 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).

[20] M. Weber, W. Krogel, S. Schwalm and T. Vogt, *Records Management acc. ISO 15489. Introduction and Guideline*, Berlin, Beuth Verlag GmbH, 2018.

[21] Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015, on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) 1093/2010, and repealing Directive 2007/64/EC.

[22] EASA: Part 21 - Airworthiness and Environmental Certification, https://www.easa.europa.eu/acceptable-means-compliance-and-guidance-material-group/part-21-airworthiness-and-environmental.

[23] CFR: Title 21 - Part 11 Electronic Records; Electronic Signatures. 21CFR11. 2019.

[24] M. Weber, W. Krogel, S. Schwalm and T. Vogt, *Records Management acc. ISO 15489.*

[25] U. Korte, S. Schwalm, T. Kusber and K. Shamburger, *Criteria for trustworthy digital transactions – Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation*, 49-60; U. Korte, K. Shamburger, T. Kusber and S. Schwalm, *Records Management and Long-Term Preservation of Evidence in DLT*, in H. Roßnagel, C. H. Schunck and S. Mödersheim (eds.), *Open Identity Summit 2021*, Bonn, Gesellschaft für Informatik e.V., 2021, 131-142.

[26] ISO 15489-1:2016. Information and documentation — Records management — Part 1: Concepts and principles.

or ISO 30300[27] a valid records management, with or without SSI and/or DLT, provides the necessary processes, roles and responsibilities, governance and technical solutions for the management of electronic records which provide the evidence for business transactions. Essential characteristics are the authenticity, integrity and traceability of electronic records as well as their availability and transferability. These inherent properties have to be ensured and preserved as long as the records are needed. This requires the availability and transferability of the records – so their evidence based on the records themselves and their useability acc. to retention requirements e.g. readability, analysability etc. Records fulfilling these requirements are called authoritative records and their authoritativeness, so their authenticity, integrity and traceability, has to be preserved until the end of the retention period. A system creating, capturing, storing records until disposition, is called record system[28]. So, if DLT is used in high-regulated industries where typically a valid records management is necessary, it acts as a record system and so it has to fulfil the requirements on record systems and records management.

Main pre-condition to ensure authenticity of the records is a unique identification and authentication of the natural or legal entity and their objects involved in the transaction not matter if for executing or signing transaction or record. Additionally, the integrity has to be ensured and made evident. Another main pre-condition are the availability as well as the protection of the confidentiality of records protection including privacy of involved natural and legal entities. The authoritative records contain content, metadata and transaction (process) data. The basic preconditions to be able to proof evidence of authoritativeness of records so their authenticity and integrity is their transferability[29] which the evidence will be proven based on the records themselves so the named requirements and in consequence the evidence value of a record are significant properties of the electronic record itself[30].

The utilization of cryptographic measures, e.g. qualified e-signatures, seals and time stamps according to eIDAS, enables users to make authenticity and integrity of their electronic records evident against third parties without losing the transferability of the records[31]. In this context it has to be taken into account that (qualified) electronic signatures, seals acc. to eIDAS require secure digital identities on at least LoA substantial.

As the consequence digital identities are not only necessary for secure access to digital services but especially one main measure to ensure burden of proof and documentation requirements and so trustworthiness of digital transactions until end of retention period of the related authoritative records[32]. Despite digital identities which are in focus of this paper one main pre-condition is the establishment of a valid records management and preservation of evidence[33]. This includes established policies, roles & responsibilities, processes as well as appropriate functionalities in business-IT to managing records properly during their whole life-cycle from the creation or receiving over utilisation and storage until archiving and disposition[34].

[27] ISO 30300:2020. Information and documentation — Records management — Core concepts and vocabulary.

[28] ISO 15489-1:2016. Information and documentation — Records management — Part 1: Concepts and principles; ISO 30300:2020. Information and documentation — Records management — Core concepts and vocabulary; M. Weber, W. Krogel, S. Schwalm and T. Vogt, *Records Management acc. ISO 15489*.

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

[30] U. Korte, D. Huehnlein and S. Schwalm, *Standards for the preservation of evidence and trust*, in *Proceedings Archiving 2014*, 2014, 9-14.; M. Weber, W. Krogel, S. Schwalm and T. Vogt, *Records Management acc. ISO 15489*.

[31] U. Korte, D. Huehnlein and S. Schwalm, *Standards for the preservation of evidence and trust*, 9-14.

[32] U. Korte, D. Huehnlein and S. Schwalm, *Standards for the preservation of evidence and trust*, 9-14; S. Schwalm, *A service for the preservation of evidence and data – a key for a trustworthy & sustainable electronic business*, in *Open Identity Summit 2017*, Bonn, Gesellschaft für Informatik e.V., 2017, 131-144; ETSI: TS 119 511 - V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques, 2019.

[33] ISO 15489-1:2016. Information and documentation — Records management — Part 1: Concepts and principles; ETSI: TS 119 511 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques, 2019; U. Korte, K. Shamburger, T. Kusber and S. Schwalm, *Records Management and Long-Term Preservation of Evidence in DLT*, 131-142.

[34] M. Weber, W. Krogel, S. Schwalm and T. Vogt, *Records Management acc. ISO 15489*; ISO 15489-

These basic burdens of proofs and requirements on trustworthy digital records and transactions are independent from used IT-system, organization or process.

4. *Decentralization, DLT and SSI*

4.1 *DLT*

After the bitcoin crash in 2019 first doubts about the real capacity of DLT occurred. In this context standardization on DLT increased and industry as well as public sector used the chance to enable the technology for high-regulated industries with corresponding requirements on records management and trust[35].

Basically, DLT is a decentralized distributed peer-to-peer network of technical nodes for data exchange and transaction execution. According to ISO 22739[36] a distributed ledger is in this case shared across a set of DLT nodes and synchronized between the DLT nodes using a consensus mechanism. The consensus mechanism ensures that all transactions are valid and unaltered. Its manner depends on the type of DLT so that the well-known prejudice that DLT implies unacceptable high energy need is only valid for some consensus mechanisms e.g. Proof of Work, other ones are much more efficient especially those ones in DLT with restricted access rights e.g. BFT, Proof of Authority, Proof of Stake etc[37]. DLT networks allow the transfer of data or value from one party to another without having intermediates involved. Once written to the ledger the transactions are immutable, mainly based on hash protection of data stored on the chain. Any transaction can reliably be tracked on the chain[38]. If the factual distributed data set or transactions are bundled in sequential linked blocks it is called a blockchain – a special kind of DLT. The blocks can also include the hash of the previous block and so build the mentioned hash-protection and a so called "timestamp".

This DLT-"timestamp" as well as DLT "signatures" have currently to be differentiated from timestamps defined in eIDAS and related standards[39] due to its lack of a trustworthy source of time, missing creation and validation of digital signatures by trust service provider and missing Proof of Existence created by a third party instead of the system, here DLT, itself. The hash-based integrity protection of each block is based on Merkle-trees[40]. In comparison to the original ideas of blockchain, DLT does not mandatorily require the elimination of an operator or consortium providing the distributed network, this depends on the kind of DLT which can be distinguished regarding the access rights and transparency of the transactions. In public DLT everybody can view all transactions and data so there is full transparency, in private DLT only authorized users are allowed, similar conditions apply concerning execution of transactions. In permissionless DLT every user is allowed to validate and persist transactions, in permissioned DLT it depends on the access rights who has the authorization to do so. Furthermore, DLT is differentiated concerning data storage, on chain if data are stored on the ledger or off-chain if data are only represented by hash in DLT. At minimum the transaction documented by ledger records or referred records acc. to ISO 30300[41] are stored on chain together with hash values of the related off-chain records.

Due to performance limitations and privacy reasons e.g. GDPR[42] off-chain storage is

1:2016. Information and documentation — Records management — Part 1: Concepts and principles.

[35] V. Lemieux, *Trusting records: is Blockchain technology the answer?* in *Records Management Journal*, vol. 26, 2016, 110-139.

[36] ISO 22739:2020. Blockchain and distributed ledger technologies — Vocabulary.

[37] ISO 22739:2020. Blockchain and distributed ledger technologies — Vocabulary.

[38] U. Korte, S. Schwalm, T. Kusber and K. Shamburger, *Criteria for trustworthy digital transactions – Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation*, 49-60; ISO/WD TR 24332 Information and documentation - Blockchain and DLT and records management: Issues and considerations, 2021; ISO/DIS 23257 Blockchain and distributed ledger technologies — Reference architecture, 2021.

[39] ETSI EN 319 421 v1.1.1. Electronic Signatures and Infrastructures (ESI) Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. Electronic Signatures and Infrastructures (ESI);
Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[40] U. Korte, S. Schwalm, T. Kusber and K. Shamburger, *Criteria for trustworthy digital transactions – Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation*, 49-60; X. Xu, I. Weber and M. Staples, *Architecture for Blockchain Applications*, Cham, Springer, 2019.

[41] ISO 30300:2020. Information and documentation — Records management — Core concepts and vocabulary.

[42] 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

currently widely used[43]. In summary, DLT can be characterized as distributed system which derives its trust from the immutability due to cryptographic protection and integrity, as well as the consistency (not completeness) check by the consensus mechanism so that any unauthorized alteration will be transparent and, at best, no central authority or intermediary is needed. This also means that DLT is typically only useful in distributed ecosystems with more than two parties involved where distribution is reasonable and the parties typically do not trust each other, so that trust in the technology seems to be necessary[44].

Currently the European Union is improving the European Blockchain Service Infrastructure as a pan-European DLT-network with a focus on use cases like e.g.:

- Notarization or data validation.
- Digital proofs or evidences.
- Electronic registries and tokenization.
- Cross-industry trade platforms or data exchange platforms.

Summarising, DLT can boost decentralized digital ecosystems. In the context of digital identities especially the development of self-sovereign identities must be mentioned. This new paradigm gives the user the control of all its identity information – those ones covered by government eID but also attributes or proofs.

4.2. *SSI-Principles*

There are nearly 10 up to 12 SSI-principles which summarize the main requirements from a decentralization perspective the requirements on an ideal decentralized and self-sovereign identity[45]:

Principle	Meaning
Representation	An SSI ecosystem shall provide the means for any entity—human, legal, natural, physical or digital—to be represented by any number of digital identities
Interoperability	An SSI ecosystem shall enable digital identity data for an entity to be represented, exchanged, secured, protected, and verified interoperably using open, public, and royalty-free standards
Decentralization	An SSI ecosystem shall not require reliance on a centralized system to represent, control, or verify an entity's digital identity data
Control and Agency	An SSI ecosystem shall empower entities who have natural, human, or legal rights in relation to their identity ("Identity Rights Holders") to control usage of their digital identity data and exert this control by employing and/or delegating to agents and guardians of their choice, including individuals, organizations, devices, and software
Participation	An SSI ecosystem shall not require an identity rights holder to participate
Equity and Inclusion	An SSI ecosystem shall not exclude or discriminate against identity rights holders within its governance scope
Useability, Accessibility and Consistency	An SSI ecosystem shall maximize usability and accessibility of agents and other SSI components for identity rights holders, including consistency of user experience
Portability	An SSI ecosystem shall not restrict the ability of identity rights holders to move or transfer a copy of their digital identity data to the agents or systems of their choice
Security	An SSI ecosystem shall empower identity rights holders to secure their digital identity data at rest and in motion, to control their own identifiers and encryption keys, and to employ end-to-end encryption for all interactions
Verifiability and authenticity	An SSI ecosystem shall empower identity rights holders to provide verifiable proof of the authenticity of their digital identity data
Privacy and minimal disclosure	An SSI ecosystem shall empower identity rights holders to protect the privacy of their digital identity data and to share the minimum digital identity data required for any particular

of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation). GDPR, 2016.

[43] U. Korte, T. Kusber, C. Berghoff and S. Schwalm, *Langfristige Beweiswerterhaltung und Datenschutz in der Blockchain*, 177-191.

[44] K. Werbach, *The Blockchain and the New architecture of Trust*; J. Strueker, N. Urbach, T. Guggenberger, J. Lautenschlager, N. Ruhland, V. Schlatt, J. Sedlmeir, J-C. Stoetzer and F. Voelter, *Self-Sovereign Identity - Foundations, applications, and potentials of portable digital identities*, Bayreuth, Fraunhofer Institute for Applied Information Technology, 2021.

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

	interaction
Transparency	An SSI ecosystem shall empower identity rights holders and all other stakeholders to easily access and verify information necessary to understand the incentives, rules, policies, and algorithms under which agents and other components of SSI ecosystems operate

Table 1: SSI-principles

Beside these ideal principles it must be assessed on how DLT and SSI may achieve the requirements on trustworthy digital transactions.

4.3. *DLT, SSI and requirements on trustworthy digital transactions*

Overlooking requirements for trustworthy digital transactions mentioned in section 3 some adjustments must be done to use DLT regulated environments.

To utilize DLT for trustworthy digital transactions, the identities of the participants have to be known unambiguously. This is necessary to make transactions and their records evident against third parties, to fulfil burden of proof and documentation needs to be compliant to prior art for records management and trustworthy digital transactions[46]. To attain this, DLT inherent functions must be enhanced with addition of eIDAS compliant identification in appropriate level of assurance. This can be achieved with self-sovereign-identity[47].

In this case only the anonymized or pseudonymized data are stored on-chain. The identity data itself is stored off-chain in order to ensure compliance to GDPR. Decentralized identifiers (DID) based on W3C standard[48] are suitable to be integrated for this purpose and maintain compliance to privacy regulations as no identifying data is stored on chain. In fact the holder of the DID has complete control over the DID and there is no central authority needed to implement it. The inclusion of identities provides the basis for assignment of permissions to these identities further improving security of the system. At same time the trustworthiness of the verifiable credentials as well as their issuers has to be considered, what requires the unique identification of the issuer but also provable authenticity and integrity of the credentials themselves. Same with the verifier or relying party to avoid sending personal data to unproven or non-trustworthy parties and so ensure data sovereignty. It should be carefully considered which participant should be allowed to execute what type of actions within the system[49].

A trusted authority in role of gatekeeper assigns permissions to nodes operated by trusted identities thus defining the actions these are allowed to execute. This approach is currently executed e.g. by ESSIF[50] and EBSI[51] in EU, but also several other initiatives around Europe like the eIDAS Bridge on DLT[52].

Furthermore, DLT inherent functions have to be enhanced with addition of eIDAS compliant identification in appropriate level of assurance and by trust services[53]. Especially the trust services for creation of qualified electronic signatures, seals (X.509 based or token based using content of X.509 envelope) and timestamps are needed to provide genuine verifiability of digital processes using DLT authenticity, reliability and integrity of transactional data by keeping provability by independent third parties. This means in fact that a trusted "gatekeeper" could enable the DLT with secure digital identities and trust

[46] Weber, W. Krogel, S. Schwalm and T. Vogt, *Records Management acc. ISO 15489*; U. Korte, S. Schwalm, T. Kusber and K. Shamburger, *Criteria for trustworthy digital transactions – Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation*, 49-60.

[47] W3C: Decentralized Identifiers (DIDs) v1.0. 2020.

[48] W3C: Decentralized Identifiers (DIDs) v1.0. 2020.

[49] eIDAS Bridge specification https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/document/ssi-eidas-bridge-use-cases-and-technical-specifications; DIN TS 31648:2021: Criteria for Trusted Transactions — Records Management and Preservation of Evidence in DLT/Blockchain. 2021; I. Alamillo-Domingo, *SSI eIDAS Legal Report. How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market*, Brussels, European Commission, 2020.

[50] ESSIF, European Self-Sovereign Identity Framework, https://www.eesc.europa.eu/en/news-media/presentations/european-self-sovereign-identity-framework.

[51] EBSI, European Blockchain Services Infrastructure, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI.

[52] eIDAS Bridge specification, https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/document/ssi-eidas-bridge-use-cases-and-technical-specifications.

[53] U. Korte, S. Schwalm, T. Kusber and K. Shamburger, *Criteria for trustworthy digital transactions – Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation*, 49-60; DIN/TS 31648:2021: Criteria for Trusted Transactions — Records Management and Preservation of Evidence in DLT/Blockchain.

services acc. to eIDAS to be used for trustworthy digital transactions[54].

DLT may act as decentralized PKI or anchoring layer where the personal data will mostly be stored off-chain, only anonymized or pseudonymized equivalents e.g. Public DIDs in SSI are on-chain. Most famous protocols for DLT in case of SSI are Ethereum, Alastria ID, or Hyperledger Indy[55]. The European Self-Sovereign-Identity Framework defined frame conditions and first standards for decentralized digital identities[56].

In summary it can be stated that without appropriate measures it is currently not possible to use DLT for trustworthy digital transactions. Same with SSI as long as there is no source of trust and verifiable authenticity of its credentials. There is no trust by default only by proof in European legislation. The proposal of the new eIDAS regulation took this background as well as the developments in ESSIF, EBSI etc. into account. The main changes in the proposal are mentioned in next section.

5. *Main legal changes in proposed new eIDAS Regulation*

5.1. *Overview*

In June 2021 the European Commission published the proposal of a Regulation amending eIDAS with the aim to establish a framework for a European Digital Identity; in other words, eIDAS 2.0[57]. The main goal of the proposed update is not a replacement but further development of eIDAS in the context of decentralization and the upcoming SSI paradigm on one hand but also the critical assessment and identified areas for improvement in eIDAS 1.0[58] on the other hand. The main changes in eIDAS 2.0 refer to electronic identification. Concerning trust services only some additional services related to electronic identification where added and some logical gaps where closed.

5.2. *Electronic Identification*

eIDAS 2.0 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 eIDAS 1.0 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 te obligation for notification can be mentioned as step forward in the wider utilization of eID in Europe. This applies even more due to the fact that any notified eID-scheme has to ensure the possibility of unique identification with the also proposed EU-Digital Wallet (Art. 11a).

Beside government eID-schemes relevant for notification the new eIDAS-proposal also introduces in Art. 12a private identification schemes together with the possibility for a national certification against level of assurances mainly. The certification scheme shall be based on EU cybersecurity Act and done by dedicated Conformity Assessment Bodies listed transparently by the EC. An implementing act is currently not stipulated what runs the risk of different national interpretations and standards of Cybersecurity act and at the end a possible competition concerning certification requirements for member states as well as identity providers.

The presumable biggest change in eIDAS 2.0 is the requirements for every Member state to provide an EU-Digital Wallet to its natural entities. The Wallet could be published:

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

This makes also private wallet possible under the recognition of a Member State. The EU-Digital 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 vaccine passport of its holder. This mean that eIDAS 2.0 strictly follows the identity triangular of SSI. Every

[54] U. Korte, S. Schwalm, T. Kusber and K. Shamburger, *Criteria for trustworthy digital transactions – Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation*, 49-60.

[55] J. Bernabe, R. Torres Moreno, D. Martin and A. Crespo, *An Overview on ARIES: Reliable European Identity Ecosystem*, in J. Bernal Bernabe and A. Skarmeta (eds.), *Challenges in Cybersecurity and Privacy - the European Research Landscape*, Gistrup, River Publisher, 2019, 231.

[56] European Self-Sovereign-Identity Framework.

[57] Proposal for a Regulation of the European Parliament And of the Council amending Regulation (EU) 910/2014 as regards establishing a framework for a European Digital Identity {SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}.

[58] See section 2.1.

citizen will become holder of EU-Digital Wallet and decides for its own to whom they release their identity information. The wallet consolidates core identity and attributes all together, but it must be taken into account that acc. to cybersecurity requirements core identity so the government eID will typically be stored on secure hardware normally the secure element or e-sim – only the attributes will be stored in the wallet as a software component. Also, the creation of (qualified) electronic signatures should be possible with the EU Digital Wallet. Technical details as well as security requirements for EU-Digital Wallet will be defined in the ongoing European Standardization at ETSI and CEN.

Directly corresponding with the EU-Digital Wallet the new qualified attestation services acc. Art. 45a-e eIDAS 2.0 must be taken into account. Only qualified trust services providers providing such qualified attestation services are allowed to access EU-DigitalWallet. Recognizing this close relationship between qualified attestation services and the wallet eIDAS 2.0 contains the same requirements for mandatory implementing acts referring on European Standards for both – wallet and attestation service. So only the issuer into the EU-Digital Wallet must be qualified attestation services. In the consequence eIDAS 2.0 crosses digital identity means and (qualified) trust services – they determine each other.

This means in summary that the new EU-Digital Wallet will contains following interfaces and main properties:

- Interface to QTSP for Attestation
- Interface to relying party
- User interface
- Ensuring that qualified trust service provider for qualified attestation only access the wallet for issuing or verification of attributes
- Fulfilment of LoA “high” acc. Art. 8 eiDAS
- Based on eID-Scheme notified on LoA “high” acc. Art. 8 eIDAS
- Integration of strong authentication measures acc. cyber security act for relying party before sending the necessary credentials
- Secure storage of identity information of natural entities

The fulfilment of these requirements will be certified by conformity assessment bodies based on a further defined certification scheme which as to be compliant to EU Cybersecurity Act (Art. 6c). The responsibility for the assessment itself is at the issuing member state, typically the national cybersecurity agency. The CAB themselves are mentioned to the EC by the member states. Within 6 months, mandatory implementing acts will define the necessary requirements by referencing the relevant European standards. A list of all certified EU Digital Wallets will be published by the European Commission, like a Trust List for the EU Digital Wallet.

In guidance on the SSI triangle, the eIDAS 2.0 Regulation also contains in Art. 6b requirements on the verifier – the relying party. They must notify their start and to fulfil European standards which will be mentioned in mandatory implementing acts – achievement will be proven by conformity assessment bodies. Unfortunately, the certification requirements are defined nationally acc. to eIDAS 2.0 proposal including the strong authentication of the verifier. This approach contains the risk of competition about lowest standards and so privacy risks for holders.

Equivalent to the dedicated requirements on the EU-Digital Wallet, the qualified attestation services as well as the identification schemes eIDAS 2.0 also defines concrete obligation on acceptance of the wallet. Not only public services, also any member of critical infrastructure (which means financial sector, utilities, health care etc.) as well as the big internet companies such as Google, Apple, Facebook, or Amazon are forced to accept the EU-Digital Wallet (Art. 12b).

Similar to eIDAS 1.0 the member state is fully liable for the provided EU-Digital 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 also in eIDAS 2.0.

5.3. *Trust Services*

Additionally, to the new qualified attestation services eIDAS 2.0 also introduces the following new trust services:

- Electronic Ledger, so trust services for DLT (Art. 45g)
- Management of secure signature creation devices (Art. 29a)
- Archiving (Art. 45h)

This means that eIDAS 2.0 now covers the whole life-cycle of authoritative electronic records from creation and signing until preservation and archiving so keeping their availability, authenticity and integrity as long as they are needed. It also ensures trust in distributed ledger by (qualified) trust service providers ensuring at least a minimum level of proven security and interoperability. Interestingly only for electronic ledger eIDAS 2.0 does not contain the requirement of mandatory implementing acts referring to European standards. Like eIDAS 1.0 all QTSP take the full liability risks (Art. 13) including the onus at their side – the trust chain mentioned in chap. 2.1 is still the same.

There are also some changes in existing trust services. Art. 24 will be expanded so that identification with EU-Digital Wallet and qualified attestation are possible which is consequently if the wallet should also be used to create qualified electronic signatures. Alternative identification measures acc. to Art.24 paragraph 1 letter d) will in future be approved by a CAB – so a module certification only. Because eIDAS 2.0 also requires mandatory implementing acts referring to European standards a Europe-wide harmonization is foreseeable. Mandatory implementing acts always linked to European standards are currently required for any other trust service in the eIDAS 2.0 proposal.

The proposed eIDAS 2.0 Regulation is particularly interesting because it includes, among its contents, an electronic legder regulation, in line with the proposal contained in the SSI eIDAS Legal Report, developed under EBSI V2.0.

The need to establish this legal regime is mentioned in the memorandum accompanying the proposed eIDAS 2.0, which explains that electronic ledgers provide users with proof and an unchanging audit trail for the sequencing of transactions and data records, protecting the integrity of the data. Among the cases of use that are cited we find its usefulness for the sharing of data from decentralised sources, for self-sovereign identity solutions or for the attribution of ownership in digital assets, among others.

The proposal also emphasises that, to prevent fragmentation, it is necessary to define a single pan-European framework allowing cross-border recognition of trust services that support the operation of e-books, which is particularly relevant when the technical approach is that of a DLT or Blockchain.

The legal challenges of DLTs are very important. From the perspective of its regulatory regulation, it is not the first time that attempts to regulate DLT technology have been established, as happened in Spain with the pioneering initiative of the Aragon regional legislation, or in Italy with Decree-Law 135/2018 (validated by Law 12/2019) giving these technologies legal effect equivalent to the electronic time stamp, or in Andorra with the recent Law 29/2021, of 29 April.

But it is the first time that a comprehensive vision is proposed, with a neutral approach that also includes centralised solutions, including the definition of the concept, the establishment of requirements and the legal effect. The important thing here is, first, that any electronic ledger will benefit from the principle of non-discrimination, but that, if it is qualified, it will enjoy a presumption of the uniqueness and authenticity of the data it contains, the accuracy of its date and time, and its sequential chronological order within the ledger.

The definition of the electronic ledger contained in the Proposal refers to an electronic record of tamper-proof data, which provides authenticity and integrity of the data they contain, accuracy of their date and time, and their chronological order, in a technologically neutral approach, allowing centralised and distributed systems, such as DLT/Blockchain.

This legal framework may help overcoming some of the problems that are preventing the deployment of SSI and DLT/Blockchain solutions, especially from the perspective of the use of Blockchain as a legal evidence instrument, thus allowing the transfer of legal responsibility.

It seems that the European Commission's proposal aims at facilitating the uptake of these technologies through their regulation as a trust service, and the establishment of the corresponding legal presumptions.

In this sense, Article 45h of the Proposal establishes the legal effects of the electronic ledger, based on the principle of non-discrimination, under which an electronic ledger shall not be denied legal effect and admissibility as evidence in court proceedings solely because it is in electronic form or does not comply with the requirements of qualified electronic ledgers; but adding that a qualified electronic ledger shall enjoy the presumption of the uniqueness and authenticity of the data contained therein, the accuracy of its date and 6.2. time, and its sequential chronological order within the ledger, which really facilitates the adoption of these technologies for all types of operations.

The regulation of the electronic ledger is an imperative for its reliable adoption, especially because of the replacement of proof of work-based consensus protocols with other protocols that are not based on intensive mathematical tests, such as proof of authority or proof of stake.

In this regard, it is very interesting that Article 45i of the Proposal has set out the requirements to be met by any electronic ledger, including its creation by one or more qualified trust service providers, the guarantee of the uniqueness, authenticity and correct sequence of data entries recorded in the general ledger; ensuring the correct sequential chronological order of the data in the ledger and the accuracy of the date and time of data entry; and record data in such a way that any subsequent change in data is immediately detectable.

In summary eIDAS 2.0 lead to Europe-wide harmonization and interoperability solving the national differences and disadvantages from eIDAS 1.0.

6. *Possible Issues and contradictions between eIDAS 2.0 and SSI*

6.1. *E Digital Wallet and SSI-Principles*

The EU Digital Wallet combines core identity as well as attestation decentralized in the control of the citizen and so ensures its data sovereignty. Because eIDAS 2.0 requires creation of (qualified) electronic signatures also with the wallet together with the comprehensive obligations for acceptance it 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. Same with private identification schemes – the possibilities of eIDAS 2.0 should be used to extend option for natural and legal entities but also mobile and cloud wallet. Only requirement should be that the wallet fulfils the technical standards for the EU-Digital Wallet certified by an accredited CAB – so in the established approach of eIDAS. If the EU-Digital Wallet will be provided by member states themselves only and also remain the only ones so no private wallets possible this will limit their portability and control of its owner due to dependency on government and its political decisions.

The fact that eIDAS 2.0 requires notification of government issued (or recognized/under authority of/by member state) as well as certification of private identification scheme by CAB – same with EU Digital Wallet the new regulation limits the decentralization of SSI because a trustworthy 3rd party is always necessary under eIDAS. By ensuring trust in SSI eIDAS 2.0 also limits its decentralization and so makes the boundaries of decentralization and SSI principle of participation evident. If there should be reliability that the legal or natural entity is really what they seem to be – a verified and secure identification is essential but at same time sets an entry requirement to take part in the ecosystem.

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 have to be made evident in non-repudiated manner against trusted third parties. eIDAS 2.0 ensures a legal compliant verifiability and proven security and makes execution of SSI principles on security, authenticity, and verifiability possible. Without legal compliance SSI would remain academic.

With the requirement on strong authentication of de facto certified relying parties eIDAS 2.0 ensures that SSI security and accessibility principles can be achieved. With clear identification and authentication requirements, the new regulation avoids a security finding and vulnerability like in German IDWallet, where core identity information could be delivered to any unproven relying party without any previous identification nor authentication[59].

This makes also clear that the full avoidance of any trustworthy third-party ensuring fulfilment of state-of-the-art security in SSI prevent the achievement of same main SSI-principles like security, privacy, verifiability as well as control and agency. If personal data is transferred from the holder to unproven relying party, there is no control of its identity for the holder anymore and a privacy breach foreseeable. If there is no authenticity provable independently from the infrastructure, so independent from DLT, a non-repudiation of verifiable credentials and so no evidence possible.

Currently eIDAS 2.0 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[60]. 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. Unknown backdoors causing cyberattacks and data loss can`t be fully eliminated. Consequently, the EU Digital Identity Wallet should require that all identity information are stored in the wallet, so the software itself to ensure fully data sovereignty as well as portability of digital identities of European citizens. Necessary European standards should focus on appropriate security measures for a fully hardened but also interoperable wallet whose technical specifications and implementations are open source and so completely provable for third parties.

6.2. *Decentralization and its limits in eIDAS 2.0*

EU Digital Identity Wallet and especially the need for qualified attestation services to issue legally provable verifiable credentials based on trusted sources but also qualified trust services for electronic signatures, seals, timestamps and their validation or preservation towards approved relying parties eIDAS 2.0 enables and at the same time limits decentralization by ensuring legal trust on SSI, Verifiable Credential and DLT with the need of trusted third party. As defined in current standardization, there's no trust by default only by prove – so also in SSI and DLT. eIDAS 2.0 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 takes 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. For SSI to be an alternative, legal compliance and trust are main pre-conditions 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 eIDAS 2.0 ensures a trustworthy decentralization with the entanglement of legal requirements in the law and its implementing act with mandatory European standardization. Clearly 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 third party is not possible. In parallel, eIDAS 2.0 ensures with its mandatory implementing acts the achievement of SSI-principles on interoperability, security and so participation, equity and inclusion. Reason is that the implementing acts will reference common European standard for all member states and so ensures same technical framework for each EU Digital Wallet and SSI in Europe in accordance to the SSI Principle of representation.

Entanglement of EU Digital Wallet & qualified attestation services & Member states (obligation to provide trusted sources for attestations) mandatorily tied together reach trusted decentralization because full liability of QTSP ensures their independence & credibility of the attestation themselves – economical competition ensures UX & user-

[59] https://fragdenstaat.de/anfrage/id-wallet-des-bundeskanzleramts-ein-projekt-der-bundesregierung-datenschutzrechtliche-aspekte/#nachricht-643462.

[60] ETSI TS 103 732 V1.1.1. CYBER; Consumer Mobile Device Protection Profile; 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; Technical Guideline TR-03159-2. Mobile Identities. Amendment A – Provisionierung und Personalisierung. Version 1.0.0 Draft 4. November 2020. Federal Office for Information Security. Bonn 2020.

friendly services, close to SSI Principles on useability and accessibility.

6.3. *DLT in the context of eIDAS 2.0*

Basically eIDAS 2.0 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 or, based on Zero Knowledge Proof, only the information that the needed identity statement is true (e.g. fulfilment of age limit, existence of valid driver license etc.). 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). 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.

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[61].

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 periods[62].

Without fulfilling basic criteria for trusted transactions and records management DLT is not feasible to be used in regulated environments. Secure digital identities as well as (qualified) trust services are some main keys to enable DLT. In DIN TS 31648[63] Germany just defined provable criteria and needed outcome documents to use DLT in trusted transactions as well as a mapping which trust service might be used to fulfil which requirements on authoritative records acc. current records management standardization[64].

With its requirements on identity schemes, the EU-Digital Wallet as well as qualified attestations on one hand but also qualified trust service providers for creation, validation, preservation of electronic signatures eIDAS creates the basic legal framework to fulfil basic criteria for utilization of DLT in environments with high requirements on burden of proof and so records management. The mainly mandatory implementing acts referring to European standards ensure interoperability also for DLT-native solutions. As explained, identification schemes and means as well as the qualified trust services acc. eIDAS (2.0) are pre-condition to use DLT for trusted and to provide proof in on-chain transactions – from onboarding to signature until the preservation of evidence[65].

If SSI is not fully based on DLT it would be much easier to use it also in transactions in a DLT network – because no additional

[61] Federal Office for Information Security, *(BSI): Towards Secure Blockchains. Concepts, Requirements, Assessments*, 2019; U. Korte. T. Kusber, S. Schwalm and K. Shamburger, *Criteria for trustworthy digital transactions*, 49-60; U. Korte, K. Shamburger, T. Kusber and S. Schwalm, *Records Management and Long-Term Preservation of Evidence in DLT*, 131-142; DIN SPEC 4997: Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology, 2020.

[62] U. Korte. T. Kusber, S. Schwalm and K. Shamburger, *Criteria for trustworthy digital transactions,* 49-60; U. Korte, K. Shamburger, T. Kusber and S. Schwalm, *Records Management and Long-Term Preservation of Evidence in DLT*, 131-142; M. Sato and S.'i Matsuo, *Long-Term Public Blockchain: Resilience against Compromise of Underlying Cryptography*, in *ICCCN: 26th International Conference on Computer Communications and Networks (ICCCN)*, Vancouver, IEEE, 2017, 1–8.

[63] DIN TS 31648:2021: Criteria for Trusted Transactions — Records Management and Preservation of Evidence in DLT/Blockchain. 2021.

[64] ISO 15489-1:2016. Information and documentation — Records management — Part 1: Concepts and principles; ISO 30300:2020. Information and documentation — Records management — Core concepts and vocabulary.

[65] U. Korte, K. Shamburger, T. Kusber and S. Schwalm, *Records Management and Long-Term Preservation of Evidence in DLT*, 131-142.

interoperability standards needed between e.g. Hyperledger Indy and ARIES or Ethereum as main DLT-protocols for SSI and Corda or Hyperledger Fabric as some main protocols in DLT-networks. In this case SSI would also not depend on the mentioned disadvantages of DLT regarding records management and burden of proof. SSI might be supported by functions provided by DLT-networks, such as revocation information propagation, but also by centralized ecosystems which are currently much more established than decentralized ones.

The evidence for authenticity or integrity does not need DLT, but qualified electronic signatures, seals and timestamps which are established since decades independently from DLT.

SSI based on centralized PKI or KERI[66] would make it as well, together with the other trust services easier to ensure evidence and burden of proof as well as interoperability (not only) with conventional identification schemes and means without losing advantages of decentralized DLT-based ecosystems because in this case is does not owe the disadvantages of DLT concerning privacy or cryptostability[67]. There are some examples of SSI without DLT especially used for vaccine passports[68].

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 eIDAS 2.0 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 eIDAS 2.0 ensures proven security in DLT.

Because DLT might be used as decentralized PKI for SSI it may be difficult to understand why the eIDAS 2.0 proposal does not contain the requirements for mandatory implementing acts referencing European Standards for QTSP for Electronic Ledger. Especially concerning the lack of interoperability, vulnerabilities in security and long-term crypto stability in DLT the mandatory implementing acts seem to be constraining pre-conditions to rely on DLT as infrastructure for SSI on one hand or network for trusted transactions on the other hand.

7. *Needed standardization according to eIDAS 2.0*

European standardization related to eIDAS 2.0 is divided between ETSI and CEN. While ETSI is mainly focused on trust services especially creation, validation and preservation of electronic signature, seal, timestamps (ETSI ESI) or DLT (ETSI PDL), the emphasis for CEN is e.g. secure signature creation devices, decentralized identity management so the basics of SSI and wallet (CEN-CLC/JTC 19) or archiving (CEN TC 468). The European standardization is embedded in international pendants at ISO TC 307 (DLT) ISO-IEC/JTC1/SC 27 (information security) or ISO TC 46 SC 11 (records management) and so also participates from developments at ISO. Some examples are ISO TR 23649[69] or ISO TR 23644[70], which are directly related to European standards in the context of eIDAS 2.0 and lead by European experts also creating the framework in Europe.

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. This means that the referenced technical standards will de facto become legal requirements to fulfil the regulation itself. Against this background the Standardization

[66] S. M. Smith, *Key Event Receipt Infrastructure (KERI) design*, v2.54, 2020.

[67] Federal Office for Information Security, *(BSI): Towards Secure Blockchains. Concepts, Requirements, Assessments*, 2019; U. Korte. T. Kusber, S. Schwalm and K. Shamburger, *Criteria for trustworthy digital transactions*, 49-60; U. Korte, K. Shamburger, T. Kusber and S. Schwalm, *Records Management and Long-Term Preservation of Evidence in DLT*, 131-142; DIN TS 31648:2021: Criteria for Trusted Transactions — Records Management and Preservation of Evidence in DLT/Blockchain, 2021.

[68] A. Corici, T. Huehnlein, D. Huehnlein and O. Rode, *Towards Interoperable Vaccination Certificate Services. 17th International Conference on Availability, Reliability and Security (ARES 2021)*, 2021, mGov4EU - Mobile Cross-Border Government Services for Europe 08 2021 DOI: 10.1145/3465481.3470035 https://zenodo.org/record/5253578; https://medium.com /decentralized-identity/keri-for-every-did-a-microledger -f9457fa80d2d.

[69] ISO TR 23649 Overview of existing DLT systems for identity management.

[70] ISO TR 23644 Overview of trust anchors for DLT-based identity management (TADIM).

should especially focus on identification schemes, the EU-Digital Wallet as well as the qualified attestation services and requirements on relying parties, so the apparent core components of eIDAS 2.0. Technically the interoperability of SSI especially when based on W3C-specification should be one focus, beside security and privacy requirements as well as user experience.

Today there are more than 80 different DID-methods and n-different DLT-protocols as decentralized PKI for SSI, creating interoperability issues not yet resolved. Delegated authentication protocols like OIDC and OAuth2 are established and so interoperability is not a challenge currently[71]. In W3C the work concerning DID-resolver is ongoing[72] – a collaboration would be meaningful to identify relevant subjects for Europe and ensuring international feasibility of European SSI-standardization.

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. Some open subjects beside the wallet etc. are DLT-native signatures, seals or timestamps which would make utilization and deployment on-ledger much easier, or those ones created based on the wallet as required in eIDAS 2.0. Other fields for optimization are the new trust services for electronic ledger. In this case a close collaboration with ISO Tc 307 concerning the technical subjects as well as ISO Tc 46 Sc 11 JWG 1[73] regarding records management seems to be useful to ensure worldwide acceptance and interoperability but also fulfilment of burden of proof.

Beside interoperability European standardization in the context of eIDAS 2.0 should focus on information security as well as long-term preservation and archiving of qualified attestation in correspondence with the authoritative records they are related to. If we are not able to fulfil burden of proof as long as the records are needed also with SSI and/or DLT – the EU Digital Wallet, Self-Sovereign-Identity & DLT will remain buzzwords. With preservation services acc. Art. 34 and 40 eIDAS as well as ETSI TS 119 511 and 512 solutions for preservation already exists and usable also for SSI and DLT[74]. Archiving services are foreseen by eIDAS 2.0 and in this context well-proven standards already exist[75].

In this subject it should be taken into account that qualified attestations only make it evident that e.g. Alice owns a valid driver license or company A has the confirmation to produce a new airplane but the attestation won`t make the documentation as basement for application and following confirmation obsolete nor the driver license itself. Otherwise, standardization for SSI and attestation must replace established and well-proven standards on data formats, metadata structures etc. for each industry and data type from documents to research data, from construction data for ships, airplanes until vaccines or maintenance of nuclear plants – a complex and impossible endeavour.

Qualified attestations as unique evidence for a property of natural or legal entities as well as their objects may be preserved in adoption of existing preservation and archiving approaches. Just storing the necessary validation information and certificate equivalent information in self-contained information packages as defined in ETSI TS 119 511, 512 as well as ISO-14721 and protecting them with cryptographic measures like Merkle Hashtrees and Evidence Records according to RFC 4998[76] as widely used cross-industry. The BSI TR-03125[77] of

[71] D. Hühnlein, T. Hühnlein, G. Hornung and H. Strack, *Towards Universal Login*, 193-200.

[72] https://github.com/decentralized-identity/did-resolver.

[73] ISO WD/TR 24332. Information and documentation — Blockchain and DLT in relation to authoritative records, records systems, and records management.

[74] U. Korte. T. Kusber, S. Schwalm and K. Shamburger, *Criteria for trustworthy digital transactions*, 49-60; U. Korte, K. Shamburger, T. Kusber and S. Schwalm, *Records Management and Long-Term Preservation of Evidence in DLT*, 131-142; M. Sato and S.'i Matsuo, *Long-Term Public Blockchain: Resilience against Compromise of Underlying Cryptography*, 1-8.

[75] ISO 14721:2012. Space data and information transfer systems — Open archival information system (OAIS) — Reference model.

[76] Evidence Record Syntax (ERS), IETF RFC 4998, 2007.

[77] Federal Office for Information Security, *(BSI), BSI Technical Guideline 03125, TR-ESOR – Preservation of*

German Federal Office for Information Security contains well-proven standard for preservation products to achieve long-term verifiability of authenticity, integrity in a transferrable manner of authoritative electronic records including related attestations. In newest version the Technical Guideline also ensures long-term preservation of DLT.

In this case also independence from the DLT as decentralized PKI must be ensured, in case of SSI based on DLT, since there are still no standardized measures to ensure long-term archiving in DLT itself[78].

Preservation and archiving of qualified attestations and decentralized digital identities shall be object of further standardization and research to ensure long-term burden of proof and fulfilment of documentation requirements for decade long retention periods. Otherwise, SSI and attestation will not be feasible in highly regulated industries.

8. *Conclusions and perspectives*

The proposal of new eIDAS-regulation contains a 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 EU-Digital 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, and certification of wallet as well as the qualified trust service provider. The fact that the liability requirements were not changed in eIDAS 2.0 the risk for the user of EU digital identity is limited because member states and QTSP take to full risk for their schemes, EU Digital Wallets or attestation. Referring to the comprehensive obligation for recognition of EU Digital Wallet the proposal prepares the digital single market for EU digital identity and so ensures foreseeable broad utilization possibilities at digital services. It´s positive that eIDAS 2.0 is technology neutral and not requires DLT as infrastructure for SSI but also mention QTSP for Electronic Ledger and so achieve proven security and trust for DLT too. The extensive requirements on mandatory implementing acts linked to European standards enables a technical harmonization and limits national specifics.

It also must be mentioned that some critical subjects should be solved in the final version. These are especially clearer statement for the certification and acceptance of wallets provided by private companies against the requirements of EU-Digital Wallet to avoid restrictions on competition. 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’s no fundamental contradiction but more the fact that eIDAS 2.0 makes it possible that SSI-principles become a reality recognizing that decentralization should be restrained to an acceptable level to achieve legal trust and data sovereignty.

The table below gives an example how SSI-principles and eIDAS 2.0 may fit together.

Principle	**eIDAS 2.0**
Representation	Notified eID Scheme and EU Digital Wallet
Interoperability	Certified EU-Digital Wallet, conformity assessed QTSP and notified eID as well as eIDAS nodes Common European standards referenced by implementing acts
Decentralization	EU-Digital Wallet and proven issuer as well as relying parties
Control and Agency	EU-Digital 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 EU-Digital Wallet and qualified trust service providers based on common European standards proved by accredited CAB.
Portability	Any identities or attestation from

Evidence of Cryptographically Signed Documents v. 1.2.2, https://www.bsi.bund.de/EN/tr-esor, 2019.

[78] U. Korte. T. Kusber, S. Schwalm and K. Shamburger, *Criteria for trustworthy digital transactions*, 49-60; U. Korte, K. Shamburger, T. Kusber and S. Schwalm, *Records Management and Long-Term Preservation of Evidence in DLT*, 131-142; DIN TS 31648:2021: Criteria for Trusted Transactions — Records Management and Preservation of Evidence in DLT/Blockchain, 2021.

	EU Digital Wallet can be moved. Details defined in European standards.
Security	State-of the art security requirements defined in common European standards which will be mentioned by implementing acts. Proved by CAB during certification of wallet, relying party or conformity assessment of QTSP. Trust provable via Trust List.
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 EU Digital 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'll provide which information. Selective Disclosure and Zero Knowledge Proof included.
Transparency	European wide regulation with common and via implementing acts mandatory European standards which are basement for notification of eID-schemes, certification of EU-Digital wallet, relying parties, QTSP and all notifications and certification/successful conformity assessment published.

Table 2: SSI-principles matching on eIDAS 2.0

European standardization should now set up the technical framework for eIDAS 2.0 and a trustworthy self-sovereign European Identity but also decentralized digital ecosystems and records management with or without DLT. Only with a holistic technical basement the promises of the regulation may become usable. eIDAS 2.0 gives Europe the chance to establish a trustworthy and legally compliant decentralized digital identity and ecosystem with or without DLT as one of the first ones in the world and be a model worldwide.