A lightweight trust management infrastructure for self-sovereign identity

Michael Kubach[1] and Heiko Roßnagel[1]

Abstract: Decentralized approaches towards digital identity management, often summarized under the currently popular term Self-sovereign identity (SSI) are being associated with high hopes for a bright future of identity management (IdM). Numerous private, open source as well as publicly funded research initiatives pursue this approach with the aim to finally bring universally usable, trustworthy, interoperable, secure, and privacy friendly digital identities for everyone and all use cases. However, a major challenge that so far has been only rudimentary addressed, is the trust management in these decentralized identity ecosystems. This paper first elaborates this problem before presenting an approach for a trust management infrastructure in SSI ecosystems that is based on already completed work for trust management in digital transactions.

Keywords: Self-sovereign identity, SSI, digital identity, decentralized identity, identity management, IdM, trust, trust frameworks, trust schemes, trust lists, IT-security, eID, eIDAS

1 Introduction

Despite of years of research and development, the availability of different technical approaches and eIDAS creating a stable EU level regulatory framework, establishing trust for secure digital identities remains a challenge in practice. With a few exceptions (e.g., Austria, Estonia), the wider adoption (including by private sector service providers) of identity solutions with high levels of assurance has remained limited. Instead, the market is dominated by web and cloud identities with low assurance levels, mainly provided by big transatlantic platform corporations. Worries exist, that this lack of secure digital identities could slow down the digitalization of the European society and economy. Moreover, there is the real risk that European digital sovereignty is in danger if big international platform corporations take over control of digital identities and trust management as they have done in such areas as smartphone operating systems, social media platforms, web search and cloud services. Solving the challenge of trust and secure digital identities is therefore an important task for the digital sovereignty and the cohesion of the European single market. The increasing importance of digital identities for things/devices only tightens the situation. This analysis is reflected in several initiatives that have been brought on track in the recent months, such as the European Commission's vision for a European Digital Identity [ON20, St20] and similar initiatives by the German government [DI20].

Regarding the technological basis for secure digital identities, so-called Self-sovereign

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

identity approaches are favoured by many, calling them "the next evolutionary step in the development of digital identities" [DE20], the future of digital identity [Si18] etc. and marketed as easy to roll out and ready for productive use (e.g. [PR20]). All four R&D projects that were recently selected for the final phase of the German "Schaufenster Sichere Digitale Identitäten" (Showcase Secure Digital Identities), receiving in total over 40 million EUR in governmental funding, build mainly on SSI [SH21].

Surfing the wave of the blockchain hype, the term and respective projects have emerged from blockchain/Distributed Ledger Technology (DLT)-based and other decentralized identity solutions. While not always used consistently, these approaches usually aim to allow users to fully own and manage their digital identity without having to rely on a third party. The DLT is used to build a decentralized Public Key Infrastructure (PKI). End users usually manage keys and credentials for their digital identities in smartphone application "wallets" [Le20, Mü18]. The privacy-focused vision and term SSI are rooted in the *Ten Principles of Self-sovereign Identity* postulated by [Al16]. It can be noted, however, that SSI has since been gradually emancipating itself from the blockchain context and there have been proposals for SSI-approaches not relying on blockchain/DLT [Sm21].

However, despite the high hopes that are placed in SSI-technology, it still has to overcome significant challenges before a wide adoption seems possible. Some of these apply to all types of IdM solutions. Those are the complicated multi-sided market with non-interoperable solutions that leads to a "chicken or egg" problem, the creation of sustainable and balanced trust relationships between identity providers, relying parties and users [ZR12], and creating sustainable business models in IdM ecosystems [Ku13] with generally low willingness to pay of users and preferences of convenience often overtaking privacy and security concerns [Ro14]. Most IdM solutions have so far not been particularly successful in solving these challenges. In addition to that, SSI, due to its particular approach and still relative immaturity, faces some distinct challenges. In a previous paper [Ku20] we have summarized those as into four main aspects: (1) Immaturity of the technology without established standards: Building solutions while SSI technologies and standards are still under development and evolving rapidly, (2) Usability and User Experience: Self-administration of digital identities and private keys for non-technical users, (3) Transparency vs. unlinkability: Reliable and transparent revocation of SSI based credentials and claims, and (4) Trust management: Absence of a natural trust anchor for DLT-based digital identities. Those four challenges and the aforementioned general ones coincide well with the eight challenges identified by [DT20] in a recent review of decentralized identity systems.

In this paper we want to focus on just the set of challenges that is related to trust management. This is not meant to disregard the importance of the others, but for trust management we can build on previous work in a research project for a different, but similar use case to propose an approach that might be valuable for SSI.

The remainder of the paper is structured as follows. Next, we will analyse the trust-related challenges in SSI in greater detail (chapter 2) and address relevant related work on these topics (chapter 3). Then, we will present our approach to trust management in SSI (chapter 4), before concluding the paper.

2 Some trust-related challenges in Self-sovereign identity approaches

SSI approaches put a high emphasis on the user's control over their data. In the Principles of Self-sovereign identity [Al16], the interests of other stakeholders of the identity ecosystem are not considered. Data is to be freed from the siloes of service providers and dependence on trusted third parties is to be minimized. It is expected that this is going to foster trust into the technology by end users and eventually foster adoption of the technology through them. To achieve this, the most prominent SSI approaches only store non-personal data on public blockchains and build on components such as Decentralized Identifiers (DIDs) [DE21], Verifiable Credentials (VCs) [VR20] with Zero Knowledge Proofs that allow for highly privacy-friendly solutions [Le20]. While this is certainly an important aspect for the adoption, we certainly cannot dismiss the trust requirements of the other relevant stakeholders in the identity ecosystem that are also essential for the adoption of an identity technology [ZR12]. Here, the relying parties (RP) also known as service providers (SP) are of particular importance, as they offer services that end users might want to access with a somehow provided and managed digital identity. In the following, we address trust-related challenges of SSI that are especially relevant from a service provider's perspective. First, we will turn to the challenge of the root of trust in SSI solutions. Second, we will focus on the challenge to manage complex trust-relationships between multiple actors/ organizations on different levels in an automated manner, so that the solution is scalable in practice.

2.1 Absence of a natural trust anchor

Establishing a chain of trust in SSI approaches remains a major challenge. How can it be assured that the credential issuing entity is in fact the entity that it claims to be? How can partners in a digital interaction be certain that a public key really belongs to the claimed entity? This challenge is illustrated in the simplified example depicted in Figure 1. In this SSI architecture, following basic SSI principles, credentials can be issued by anyone: any *Bank* or *Fake Bank* can issue a credential about the solvency of Tom (holder)[2]. It is cryptographically easy to verify for *Web Shop* (service provider/relying party/verifier) whether the solvency credential was really issued from *Bank* or *Fake Bank* to Tom and

[2] The "solvency credential" here simply serves as a handy example for this illustrative use case. There are certainly other ways for *Web Shop* to ensure to get paid. However, this use case example aims to illustrate how there is a need for identity attributes or credentials to be issued by parties that can be trusted by service providers and how this trust can be established in a scalable manner while leaving the trust decision with the verifiers.

has not been tampered or revoked.

The credential issuers *Bank* or *Fake Bank* are not involved in the proof of solvency by Tom to the *Web Shop*, so the privacy of Tom is protected. The question that remains is what happens if *Fake Bank* is a fraudulent service posing as *Bank* that just issues solvency credentials to anyone? How can the *Web Shop* assess the trustworthiness of the issuing *Bank* and/or the Level of Assurance of the Credential? How can this process be automated so that it is scalable?

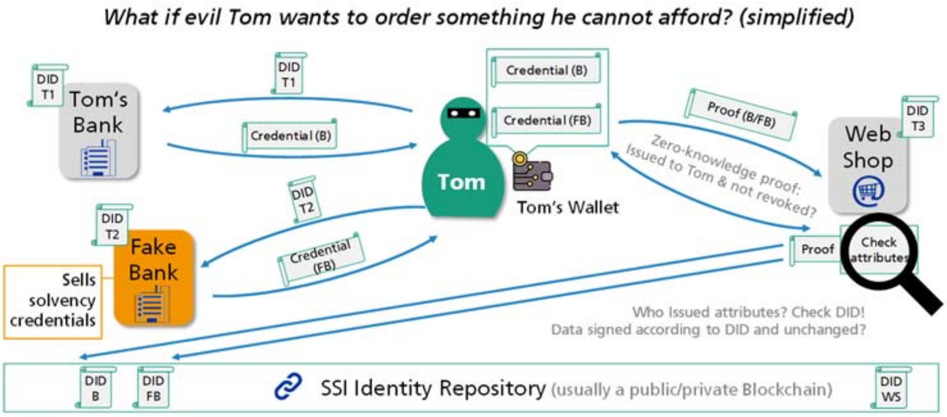
What if evil Tom wants to order something he cannot afford? (simplified)
DID T1
Tom's Bank
DID T1
Credential (B)
Credential (B)
Credential (FB)
Tom
Tom's Wallet
Proof (B/FB)
Zero-knowledge proof: Issued to Tom & not revoked?
DID T3
Web Shop
DID T2
Credential (FB)
DID T2
Fake Bank
Sells solvency credentials
Proof
Check attributes
Who Issued attributes? Check DID!
Data signed according to DID and unchanged?
DID B
DID FB
SSI Identity Repository (usually a public/private Blockchain)
DID WS

Figure 1: The Challenge of the Root of Trust in SSI solutions

2.2 Automated trust management

Digital identity and associated trust information is increasingly exchanged between organizations. This follows from several developments that are likely to take off even more in the future. People work on premise and increasingly remotely in project-teams consisting of members of multiple organizations, assisted by smart Internet of Things (IoT)-devices, and linear production chains have evolved into complex value networks. Identity and trust information is needed to secure these processes, protect intellectual property etc. SSI seeks to support this by opening up identity and data silos between separate organizations and independent platforms. This requires technical interoperability through standards, but also advanced trust management capable of dealing with different trust levels and roots of the participating entities in a scalable manner.

Hence, automatization of trust management processes could be an important step to achieve efficient trust management in many use cases and might be actually a requirement to leverage the full potential of SSI. Otherwise, scalability would be limited as efforts to manage trust manually raise too fast when trust domains, organizations, devices etc. increase beyond a certain simple level. This requires however, that trust policies can be expressed in a formalized way and it requires tools that can verify transactions against those policies in an automatic fashion.

3 Previous and related work

So far, SSI approaches do not explicitly contain trust management approaches. The current focus is more on technical interoperability through standardization of interfaces and protocols (Decentralized Identifiers (DIDs) [DE21], Verifiable Credential types [VR20] etc.). Work on trust of verifiers focuses on the trust of verifiers in the cryptographic integrity of credentials while preserving the holder's privacy [Yo21] – certainly an important aspect, but not enough. Nevertheless, some approaches are worth considering, could be built on previous work from other contexts and are increasingly being recognized by important SSI players such as the Trust over IP Foundation and EBSI ESSIF.

One approach to trust in SSI would be to introduce centralized governance layers and trust frameworks with trust anchors and/or trust intermediaries. This could potentially increase trust in certain use cases. However, such would contradict the decentralized aspect of SSI and one of its main arguments, moving from an open ecosystem to one with a dominant stakeholder (or cartel) acting as gatekeeper. Hence, we would fall back to the reliance on central trusted third parties.

A different approach could be to just stick to a decentral model and reliance on the market to decide about the trustworthiness of actors. One could expect that in the long term, trustable actors would prevail – if they are able to build a sustainable business model. However, we would have to face re-occurring problems with fraudulent actors in this model – as illustrated in the example above. Fake banks could always re-enter the market[3]. Automation of processes would become quite difficult. And in the end, we could end up with few powerful players dominating the market. Quite similar to the current situation regarding web identity management. The market approach could therefore lead to a low level of trust and/or promote an oligopoly that is hostile to innovation (as it makes it very difficult for new small players/start-ups to gaining a foothold in the market).

A compromise between these two extreme approaches could be to rely on traditional hierarchical solutions for trust management such as hierarchical PKIs. There, a trust root issues certificates for certification authorities who again issue certificates to customers. This forms a chain of trust from the root of trust to the leave certificates. However, the process of certification usually requires substantial time and effort, might not be scalable and flexible enough for the large number of entities in future use cases (i.e., Internet of Things) while also lacking advanced automated management functions needed for large scale interorganizational or cross domain/region etc. application areas. Furthermore, this approach requires that both parties (holder and verifier) accept the same trust root.

[3] It would even be possible to automate the re-entry process, which would allow the Fake Bank to register a new DID every time their old on is exposed and removed.

The Trust over IP foundation has also recognized the need for “strong evidence of the credibility and authority of the issuer making claims” [IN20]. They propose to rely on the chain of trust that results from hierarchical approaches, but instead of setting up a new PKI for the identity system, they promote the use of existing already established Trust Schemes and Trust Ecosystems. This is a very pragmatic approach, that only requires that the verifier considers the trust root of the used trust scheme/ecosystem to be authentic and trustworthy.

The SSI eIDAS Bridge could be seen as one such instance of the proposal by Trust over IP and a hierarchical PKI. It is an approach to make eIDAS available as a trust framework for the SSI ecosystem. On the one hand it assists the issuer in signing a verifiable credential. On the other hand, the verifier is assisted by verifying the issuer’s advanced or qualified electronic signature (if the issuer is a natural person) or seal (if the issuer is a legal person) that are s attached to the verifiable credential in form of a linked data signature. This approach is currently developed in an EU H2020 NGI ESSIF Lab project [ES21c]. However, it has to be noted that this specific approach follows a quite narrow goal: it can only integrate SSI with one trust framework which is eIDAS. eIDAS is just one of several existing trust frameworks (others for example being the Pan Canadian Trust Framework, the Trust Scheme of Turkey etc.) and eIDAS is focused on the trust domain of national legal electronic identification and trust services in the European context. The relevance of eIDAS for the private sector has so far been rather limited. Other trust domains and the private context cannot be integrated through the SSI eIDAS Bridge (which is of course also not its goal).

The EU-funded project LIGHTest takes this idea one step further. Initially focused on electronic transactions in general, they provide a standardized way that allows operators of trust schemes to publish all the relevant information about their trust scheme using DNSSEC [Wa17]. This provides a great advantage, because it allows the verifier to also check the identity of the trust scheme operator following the DNSSEC chain of trust up to the already established and globally accepted trust root of DNSSEC. LIGHTest also provides the means to automatically verify transactions using a so-called Automated Trust Verifier (ATV), that collects all relevant information and verifies transactions against the trust policy of the verifier. Therefore, it is possible for the verifier to more easily integrate new trust domains and to verify transactions in an automatic fashion. Section 4 describes how this approach can be leveraged to establish trust in SSI ecosystems.

Automation of trust management in supporting verifiers of verifiable credentials and interoperability between trust domains is also being picked up. The Policyman Project in the EU H2020 NGI ESSIF Lab [PO21] is developing a middleware with APIs for verifiable credential issuers, holders, and verifiers. The policy management tool should allow service providers to specify policies for access to their resources using a graphical interface. Moreover, a publicly accessible policy registry is envisioned to store different syntactic policies and a conversion server to convert policies between different syntactics of various SSI ecosystems.

4 Proposing the TRAIN approach as a lightweight trust management infrastructure for Self-sovereign identity

The situation and challenges as described in section two, that are currently not fully addressed by the related work, as described in the previous section, can be summarized as:

1.) Credentials can basically be issued by anyone. Every service provider/verifier can individually decide for him/herself whether the issuer is deemed trustworthy given the information available. No intermediary, other third party or gatekeeper is required in this process. This is an important and aspired aspect of the decentralized, open architecture.
2.) In some, more or less sensitive use cases (e.g. online shopping, employers reviewing diplomas), verifiers highly profit from support when having to decide whether certain credential issuers are trustworthy.
3.) Certain schemes and standards, for example regarding the Levels of Assurance (LoA) behind certain credentials would allow for automated decision making and could ease the handling of credentials from different issuers and more trustable.

In the following, we present an approach to address these challenges. It is based on the work of the EU H2020 research project LIGHTest [LI21] that is currently being developed further for the application in the SSI context in the EU H2020 NGI ESSIF Lab[4] project TRAIN (TRust mAnagement INfrastructure) [ES21b].

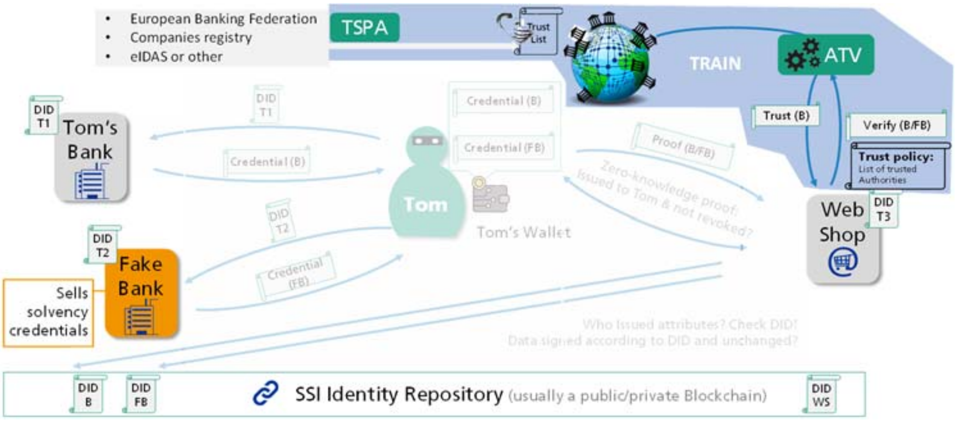
European Banking Federation
Companies registry
eIDAS or other
TSPA
Trust List
TRAIN
ATV
DID T1
Tom's Bank
DID T1
Credential (B)
Credential (B)
Credential (FB)
Tom
Tom's Wallet
Trust (B)
Verify (B/FB)
Trust policy: List of trusted Authorities
Proof (B/FB)
Zero-knowledge proof: Issued to Tom & not revoked?
Web Shop
DID T3
DID T2
DID T2
Fake Bank
Sells solvency credentials
Credential (FB)
Who issued attributes? Check DID!
Data signed according to DID and unchanged?
DID B
DID FB
SSI Identity Repository (usually a public/private Blockchain)
DID WS

Figure 2: TRAIN as a lightweight trust management infrastructure for Self-sovereign identity

Figure 2 gives an overview of the architecture. It illustrates how the TRAIN component is introduced into the simplified SSI architecture already known from the scenario in section

[4] eSSIF-Lab is an EU-funded project and aims at advancing the broad uptake of Self-Sovereign Identities (SSI) as a next generation, open and trusted digital identity solution for faster and safer electronic transactions via the Internet and in real life (https://essif-lab.eu/).

2.1. The TRAIN project is currently working to integrate it into the more sophisticated EBSI ESSIF Framework [ES21a].

Using TRAIN, *Web Shop* as verifier can decide to seek external support to assess the trustworthiness of solvency credentials issued by banks not known to him. Thus, the verifier defines in a Trust Policy one or multiple trusted authorities to accept for certain transactions – e.g., over a certain financial threshold. Based on the Trust Policy, the Automatic Trust Verifier (ATV) component verifies if any Bank that has issued the solvency credential is listed in one of the corresponding Trust Lists of Trusted Authorities accepted by the Web Shop. Such a list could for example be published by a banking federation or another industry association. These are the so-called Trust Scheme Publication Authorities (TSPAs) that operate standard DNS Name Servers with DNSSEC extension. Such a server can publish multiple trust lists under different sub-domains of the authority's domain name. Alternatively, the Web Shop could require eIDAS certificates and refer to eIDAS Trusted List.

As mechanism for the discovery and verification of trust scheme memberships, TRAIN makes use of the global, well-established and trusted infrastructure of the internet Domain Name System DNS (using DNSSEC) as trust root. This approach has been developed and validated in several pilots of the LIGHTest project (for the general context of trust for digital transactions). For the reference architecture of this approach please refer to [Wa17].

Compared to the alternative approaches sketched out above in section 3, TRAIN still follows a decentral approach. The final trust decision remains with the verifiers that can decide whether to rely on other authorities to transparently support them. Central gatekeepers are avoided and everyone still being able to issue credentials, just as everyone can easily publish their own trust lists as TSPA. While allowing for this, TRAIN introduces a transparent and trustable infrastructure that supports participants of the SSI ecosystem to define which issuers they deem trustable – or who can support them in this decision and under which circumstances and automate this process. Verifiers are supported in setting up self-defined Trust Policies that define certain credentials/certificates that are issued by specific entities that are incorporated in specific trust lists are deemed trustworthy. Hence, the focal point of trust remains with the verifier. The trust lists are published by TSPAs that operate Trust Schemes. A Trust Scheme comprises the organizational, regulatory/legal, and technical measures to assert trust-relevant attributes about enrolled entities in a given domain of trust. Thus, it is transparent how issuers got included in the Trust List of a certain Trust Scheme. TSPAs can be governmental institutions, but also any other organizations like businesses or other non-governmental institutions. Thus, if a verifier decides that external support for a trust decision is needed, it refers to the TSPA of its preference. Moreover, issuers can signal their trustworthiness by committing to a certain Trust Scheme to be included into certain Trust Lists. Finally, credential holders profit from a trustable and still dynamic ecosystem with low barriers for new entrants. TRAIN adds a flexible trust layer to SSI, enables scalable and automated trust management and is fully in line with the open and decentral SSI approach.

5 Conclusion

To fulfill the promise for a bright future of identity management, SSI solutions urgently need to solve the trust management issues that we outlined in section 2, particularly regarding the trust anchor and automation. The emphasis of SSI on protecting the privacy of the holder and the overall decentralized approach have created a situation in which the verifier can find itself in a disadvantageous situation. However, the verifier is a stakeholder that also has to be motivated to adopt SSI as identity solution – as has the user. Hence, the valid interests of the verifier as provider of valuable service cannot be neglected.

In the currently limited SSI approaches, the verifier might be forced to make a decision on whether or not to trust a credential presented by the holder without the means to verify if this credential is reliably and trustworthy. As outlined in section 2, cryptographical verification is not enough, if you are not able to assess if the source is genuine and trustworthy. Approaches to address this issue range from central governance layers with dominant stakeholders as gatekeepers to approaches that fully rely on the market to govern itself. Hierarchical approaches could be a viable compromise between these extremes but require all parties to accept a common root of trust – which is not a realistic scenario in many cross-domain and/or international use cases. This particular drawback, however, can solved by leveraging existing trust schemes and ecosystems and by providing a standardized way to publish their trust-relevant information. The TRAIN project follows such an approach to provide a trust management infrastructure for SSI. This is an important first step for providing the necessary credibility to make SSI also attractive for relying parties.

The TRAIN approach is currently working to transfer knowledge and components developed and focused in LIGHTest to the SSI ecosystem. Currently, it focuses on fundamental interaction with verifiers and is developing the respective API. However, the SSI ecosystem is in dynamic development and standards are only currently forming and there is currently no universal interface to issuers available. In general, TRAIN faces the challenge of achieving enough momentum for being picked up by enough issuers and verifiers. Here, it faces a two-sided market with network effects. If enough verifiers would integrate the solution, it would also be attractive for issuers – and vice versa. Making it as easy as possible for both sides to integrate the solution by building on the emerging standards in SSI and also facilitating the enrolment process of issuers through a respective API, making it easy for verifiers to formulate policies by adjusting the policy authoring tool developed in LIGHTest [WO21], sharpening the value position and making the approach more known in the SSI ecosystem – e.g. through further work in EBSI ESSIF – will be important next steps on the roadmap for TRAIN.

6 References

[Al16] Allen, C.: The Path to Self-Sovereign Identity., https://github.com/ChristopherA/self-sovereign-identity, accessed: 05/02/2020.

[De20] INATBA: Decentralized Identity: What is at Stake? INATBA Position Paper : INATBA Identity Working Group, 2020.

[De21] W3C: Decentralized Identifiers (DIDs) v1.0. https://www.w3.org/TR/did-core/. - accessed: 09/02/2021.

[Di20] Bundesregierung: Digitale Identität - Personalausweis im Smartphone und mehr. https://www.bundesregierung.de/breg-de/aktuelles/digitale-identitaet-1824658. - accessed:0802/2021.

[DT20] Dib, O.; Toumi, K.: Decentralized identity systems: Architecture, challenges, solutions and future directions. In: Annals of Emerging Technologies in Computing Bd. 4, Nr. 5, pp. 19–40, 2020.

[Es21a] EBSI ESSIF Lab: eSSIF-Lab Functional Architecture | eSSIF-Lab. https://essif-lab.pages.grnet.gr/framework/framework/docs/functional-architecture. accessed: 23/02/2021.

[Es21b] ESSIF Lab Project: eSSIF-TRAIN by Fraunhofer-Gesellschaft | ESSIF-LAB. https://essif-lab.eu/essif-train-by-fraunhofer-gesellschaft/. accessed: 23/02/2021.

[Es21c] SSI eIDAS Bridge Project: ESSIF-Lab / infrastructure / VALIDATED-ID / SEB_project_summary. https://gitlab.grnet.gr/essif-lab/infrastructure/validated-id/seb_project_summary. accessed: 01/03/2021.

[In20] Trust over IP Foundation: Integration with Established Trust Ecosystems - Guidance Deliverable, 2020.

[Ku13] Kubach, M.; Roßnagel, H.; Sellung, R.: Service providers' requirements for eID solutions: Empirical evidence from the leisure sector. In: Hühnlein, D.; Roßnagel, H. (Hrsg.): Open Identity Summit 2013 - Lecture Notes in Informatics (LNI) - Proceedings. Bonn, pp. 69–81, 2013.

[Ku20] Kubach, M. et.al.: Self-sovereign and Decentralized identity as the future of identity management? In: Open Identity Summit 2020 - Lecture Notes in Informatics (LNI) - Proceedings. Bonn: Köllen Druck + Verlag GmbH, 2020, publisher: Gesellschaft für Informatik eV, pp. 35–47, 2020.

[Le20] Lesavre, L. et.al.: A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems: National Institute of Standards and Technology, 2020.

[LI21] LIGHTest. https://www.lightest.eu/. accessed: 23/02/2021.

[Mü18] Mühle, A. et.al.: A survey on essential components of a self-sovereign identity. In: Computer Science Review Bd. 30, pp. 80–86, 2018.

[On20] DG CONNECT: Online European Digital Identity Roundtable: Clear message in favour of a secure e-Identity for all Europeans!. https://ec.europa.eu/digital-single-market/en/news/online-european-digital-identity-roundtable-clear-message-favour-secure-e-identity-all. accessed: 08/02/2021.

[PO21] Policyman Project: ESSIF-Lab / business / PolicyMan / PolicyMan_project_summary. https://gitlab.grnet.gr/essif-lab/business/policyman/policyman_project_summary. -

accessed: 01/03/2021.

[Pr20] Products - Evernym’s Verifiable Credential Platform. https://www.evernym.com/products/. - accessed: 09/10/2021.

[Ro14] Roßnagel, H. et.al.: Users’ willingness to pay for web identity management systems. In: European Journal of Information Systems Bd. 23, Nr. 1, pp. 36–50, 2014.

[Sh21] Showcase programme “Secure Digital Identities”. https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/sichere_digitale_ident.html. accessed: 28/02/2021.

[Si18] Simons, A.: Decentralized digital identities and blockchain: The future as we see it. https://www.microsoft.com/en-us/microsoft-365/blog/2018/02/12/decentralized-digital-identities-and-blockchain-the-future-as-we-see-it/. accessed: 05/02/2020.

[Sm21] Smith, S. M.: Key Event Receipt Infrastructure (KERI). In: arXiv:1907.02143, 2021.

[St20] Stolton, J.: EU leaders to call for an EU electronic ID by mid-2021. https://www.euractiv.com/section/digital/news/eu-leaders-to-call-for-an-eu-electronic-id-by-mid-2021/. accessed: 08/02/2021.

[VR20] W3C: Verifiable Credentials Data Model 1.0. https://www.w3.org/TR/vc-data-model/. - accessed: 06/02/2020.

[Wa17] Wagner, S. et.al.: A mechanism for discovery and verification of trust scheme memberships: The LIGHTest Reference Architecture. In: Open Identity Summit 2017, Lecture Notes in Informatics (LNI), Lecture Notes in Informatics (LNI). Bd. P277. Bonn: Köllen Druck + Verlag GmbH, pp. 81–92, 2017.

[WO21] Weinhardt, S.; Omolola, O.: Usability of Policy Authoring Tools: A Layered Approach. In: 2021 — ISBN 978-989-758-359-9, pp. 301–308, 2021.

[Yo21] Young, K.: Verifiable Credentials Flavors Explained, Linux Foundation Public Health: Linux Foundation Public Health, 2021.

[ZR12] Zibuschka, J.; Roßnagel, H.: Stakeholder Economics of Identity Management Infrastructures for the Web. In: Proceedings of the 17th Nordic Workshop on Secure IT Systems (NordSec 2012). Karlskrone, Sweden, 2012.