A novel approach to establish trust in verifiable credential issuers in Self-Sovereign Identity ecosystems using TRAIN

Isaac Henderson Johnson Jeyakumar[1], David W Chadwick[2] and Michael Kubach[3]

Abstract: Self-sovereign identity (SSI) promises to bring decentralized privacy friendly identity management (IdM) ecosystems to success. Yet, trust management in SSI remains challenging. In particular, as it is lacking a holistic approach that combines trust and governance frameworks. A practical and scalable mechanism for verifiers to the external verification of trust in credential issuers is missing. This paper illustrates how TRAIN (Trust mAnagement INfrastructure), an approach based on established components like ETSI trust lists and the Domain Name System (DNS), can be used as a trust registry component to provide a holistic approach for trust management in SSI ecosystems. TRAIN facilitates individual trust decisions through the discovery of trust lists in SSI ecosystems, along with published credential schemas, so that verifiers can perform informed trust decisions about issued credentials.

Keywords: Self-sovereign identity, SSI, digital identity, decentralized identity, identity management, trust registry, trusted issuers, trust lists, IdM.

1 Introduction

The concept of Self-sovereign identity (SSI) [1] is currently widely debated in the digital identity community, among practitioners, politicians, as well as academics. It promises to put the end user (citizen) in total control of revealing their identity. The end user's credentials are managed by themselves and directly presented to verifiers (service providers) without the involvement of third parties. The issuers of the credentials (i.e., identity providers) are not involved in the process of presentation.

Some pursue SSI hoping to achieve their vision of an independent citizen identity. Others see SSI in the context of the political project of data sovereignty that the European Union (EU) is pushing forward, among other aspects with the revision of eIDAS [2]. SSI has been called the next evolutionary step in the world of digital identity, the future of digital identity, and more [3], [4].

However, despite the high hopes that are connected to SSI, the technology still has to

[1] University of Stuttgart, Institute of Human Factors and Technology Management IAT, Allmandring 35, Stuttgart, 70569, Isaac-Henderson.Johnson-Jeyakumar@iat.uni-stuttgart.de.

[2] Crossword Cybersecurity, Capital Tower, 91 Waterloo Rd, South Bank, London SE1 8RT, david.chadwick@crosswordcybersecurity.com

[3] Fraunhofer IAO, Nobelstr. 12, 70569 Stuttgart, Germany, michael.kubach@iao.fraunhofer.de

overcome certain significant challenges before it can become widely adopted in the market and live up to the expectations of its proponents [5]. One fundamental hurdle that has already been widely discussed but has not yet been fully solved in practice is trust management in these decentralized identity ecosystems that SSI is creating [6]. This is where our paper contributes. In the following sections, we first elaborate a bit further on the trust and governance challenges that current SSI systems are facing. Subsequently, in section 3 we present related work and initiatives, as this topic has of course been picked up by other researchers and developers as well. In section four we then present the general TRAIN approach to trust management for SSI that we have developed further over the last year. Section 5 then gives more details on how TRAIN enables verifier-centric trust decisions to establish trust in issuers. In section 6 we give an outlook on future work, before we conclude the paper in section 7.

2 Trust and governance challenges in self-sovereign identity

SSI claims to solve the trust issues in identity management systems by focussing on Decentralized identifiers (DIDs), distributed ledgers, crypto key rotations, and Zero-knowledge proofs. However, those architectural elements only address “technical” trust, which is only one part of the overall trust in IdM system. On the other side is “institutional” trust which addresses and defines criteria for relying parties to be accepted as a legitimate actors in the ecosystem. Unless institutional trust is ensured, every issuer can claim to be legitimate which can lead to different security attacks in the ecosystem. For example: A framework for institutional trust defines that only certain governmental institutions are entitled to issue Identity Document (IDs) to citizens of a country. If everyone would be eligible to issue citizen IDs then there might be a lot of fake IDs circulating.

Standardization and interoperability are arguably the most relevant governance challenges for SSI [7]. Currently, an increasing number of initiatives are trying to implement SSI or SSI-like solutions and contribute to standardization efforts in order to achieve interoperability between the different ecosystems under development. SSI today is in a stage similar to the early days of the transmission and network protocols before the internet, i.e., TCP/IP protocols, were firmly established. Isolated SSI islands with proofs of concepts in different use cases prevail. It will be necessary to achieve a widespread adoption of standards in order to achieve global interoperability.

At this point, for example, the international W3C consortium has launched efforts for standards such as DIDs and Verifiable Credentials (VCs), aiming to standardize SSI data models [8], [9]. But so far, protocols are out of their scope. These efforts are supported by the Open ID Foundation, which is enhancing the OpenID Connect (OIDC) protocol to support W3C VCs and DIDs [10]. In addition, the Trust over IP Foundation (ToIP) has committed itself to building a holistic architecture for digital trust on the Internet [11]. In particular, its desire to support the ability to port VCs between different networks will be crucial for the widespread adoption of person-based SSI. Likewise, the number of

providers will initially be decisive to reach a broad mass of users.

The European Union Agency for Cyber Security (ENISA) in its recent report regarding leveraging the self-sovereign identity concept to build trust [12] mentioned the requirement of Governance frameworks in Certification of Wallets, Audit, and Oversight of DID Controllers, VC Issuers, DIDs, and VC registries.

3 Related work and initiatives

In recent months, the requirement of a trust registry and trust anchor has been recognized as a challenge by different working groups in the SSI space. The Trust Over IP Foundation has recognized the need to address the trustworthiness of the parties involved in the SSI ecosystem. Hence, a trust registry specification working group [13] has been established, which addresses the challenges pertaining to trust and governance in the SSI ecosystem and aims to develop a trust registry framework specification.

Moreover, the GAIA-X Federation Services (GXFS) in the GAIA-X initiative, aiming to build their IdM on SSI components, has acknowledged this challenge as well. The project that is developing a federation of data infrastructures and service providers for Europe have presented the requirement for trust anchors as a part of trust services in one of their recent publications [14].

Finally, in the current pandemic situation, many governments have begun designing and implementing Covid certificate systems. With the EU Digital Covid Certificate, the lack of a global trust architecture and ready-to-deploy tools to build compatible systems in other countries could not be clearer. Consequently, the Linux Foundation for Public Health (LFPH) has launched the Global Covid Credential Network (GCCN) [15] to address this gap by adapting and operationalizing the Interoperability Blueprint of the Good Health Pass Collaborative, an industry coalition that has defined principles and standards for Covid certificates. GCCN has also established a special working group called GCCN Trust Registry Network, which also addresses the requirement of the trust registry component.

4 The role of TRAIN in the SSI ecosystem

TRAIN stands for "**TR**ust m**A**nagement **IN**frastructure". It was a subproject run by Fraunhofer-Gesellschaft in the EU NGI eSSIF-Lab project [16]. The basic conceptual approach of TRAIN as a lightweight trust infrastructure has been first published in [6].

TRAIN makes use of the global, well-established, and trusted infrastructure of the Internet Domain Name System DNS (using DNSSEC) as its root of trust. Its basic technology had been developed and validated in several pilots of the EU LIGHTest project (for the general context of trust for digital transactions). For the reference architecture of this approach please refer to [17].

TRAIN addresses the issue of establishing trust into certain institutions in the SSI ecosystem beyond what is achieved through mainly technical means, i.e., cryptography. An example would be the verification of the credibility of credential issuers, e.g., to find out whether the credential issuers really are who they claim to be. At the state of writing this paper in February 2022, there are around 113 different registered DID methods (and probably many more unregistered ones) [18]. Each method might have a different technical backend implementation. But irrespective of the technical infrastructure behind a certain SSI infrastructure, verifying the institutional trust between different components still remains an open issue. This is where TRAIN steps in. Using TRAIN, the verifier has the possibility of subscribing to one or several trust schemes that can be defined by trustworthy institutions, thereby giving the verifier the opportunity to verify the credibility of issuers, regardless of their technical infrastructure.

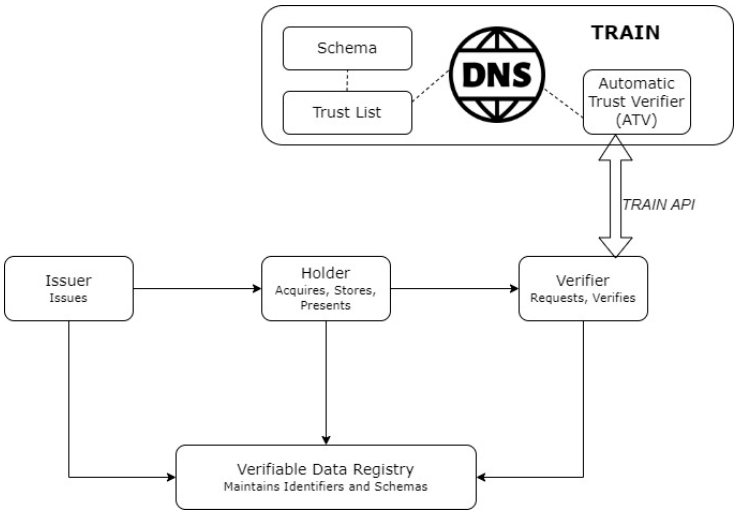

Figure 1 Integration of TRAIN into W3C VC SSI ecosystem

The architecture and integration of TRAIN into the W3C VC SSI ecosystem is shown in **Fehler! Verweisquelle konnte nicht gefunden werden.**. Although the TRAIN infrastructure uses the DNS for lookups, the trust schemes, JSON schemas and trust lists are distributed on the web and are not stored in the DNS. There can be different instances of trust lists and trust schemes hosted by different trust scheme operators (institutions providing trust schemes), and the verifier alone can decide to trust other existing trust schemes, trust lists (for example: eIDAS) or create their own trust schemes depending on their requirements. Verifiers can define policies using a policy language on how trust decisions are to be made. Anyone can decide to set up and provide their own trust scheme. The TRAIN API acts as a bridge between the SSI ecosystem and the TRAIN infrastructure. The TRAIN ATV component can be deployed as a cloud service but can be operated by the verifiers themselves in their own infrastructure as well.

5 Enabling individual and distributed trust decisions based on TRAIN

TRAIN assists verifiers in making trust decision about VC issuers. In essence, a VC issuer can make any statement it wishes (true or false) about the trust schemes it is a member of, and the verifier uses the TRAIN infrastructure to determine whether any statement is true or not.

5.1 Creation and publication of trust schemes

Any DNS owner can create their own trust scheme and become a trust scheme operator e.g., tso.com. Similarly, every VC verifier decides which trust scheme operators to trust. Trust scheme operators decide which VC issuers are members of its trust scheme and therefore are trusted to issue VCs of a certain type with a certain schema. The trust scheme operator publishes the members of its trust scheme in a trust list that is based on the ETSI standard TS 119 612 (see section 5.2). A trust scheme operator, e.g., tso.com, with scheme "example" may also trust the trust scheme e.g. "ssi", of another trust scheme operator, e.g., company.uk. Consequently, it may wish to include the members of another trust scheme as being equivalent to its own members. The trust scheme operator would therefore add pointer resource records (PTR RRs) to its DNS trust scheme entry (as described below) to point to these other equivalent trust schemes. The use of PTR RRs forms mappings between Trust Schemes and Trust Lists. TRAIN offers the flexibility to create different trust schemes mapped to different trust lists according to the requirements of a certain trust framework.

5.1 DNS structure

The DNS controller creates a DNS entry with the name of its trust scheme e.g., example.tso.com., or ssi.company.uk. Then below this, two further DNS entries named _trust and _scheme respectively are created as shown in Figure 2. The names of these two entries were specified by the EU Lightest project [17], TRAIN is following those guidelines. Here, *example* is the scheme name, *tso.com* the authority responsible for the scheme, and *_TRUST* a standardized constant word used across the trust infrastructure. The bottom entry, e.g., _scheme._trust.example.tso.com contains one or more PTR RRs. Each PTR RR points to a DNS entry where the location of an ETSI trust list can be found, in a URI RR. This use of PTR RRs allows one trust scheme to point to several ETSI trust lists, for example, each located in a different country of the EU. It also allows an ETSI trust list to be incorporated into multiple trust schemes.

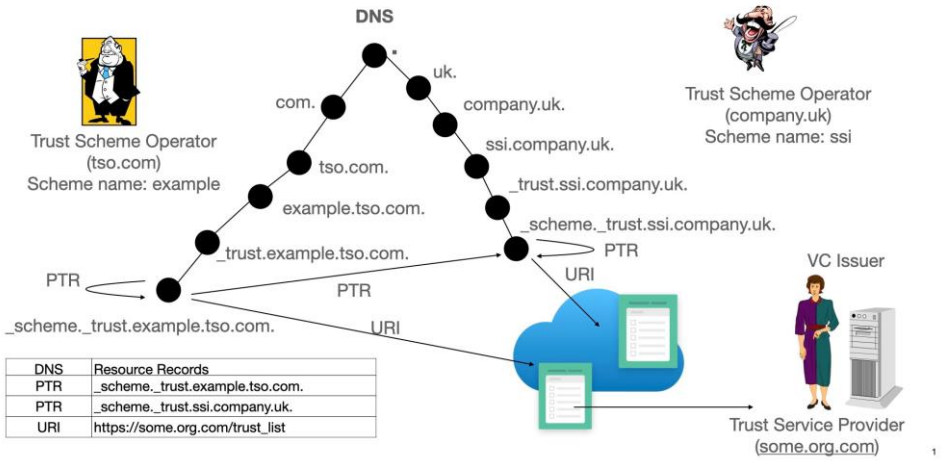

Figure 2. TRAIN use of the DNS

5.2 Trust lists and JSON schema formats

Trust Lists used by TRAIN follow the ETSI TS 119 612 standard [19] and list all the enrolled entities (Issuers) in a specific data file/format certified by the issuing authority. An exemplary trust list is given in the following:

```
<TrustServiceProvider>
 <TSPInformation>
  <TSPName>
   <Name xml:lang="en">BGE</Name>
  </TSPName>
  <IssuerName>
   <Name
xml:lang="en">https://vc.bge.verifiablecredentials.net</Name>
  </IssuerName>
  <TSPTradeName>
   <Name xml:lang="en">VATES-11111111</Name>
  </TSPTradeName>
  <TSPAddress>
   <PostalAddresses>
   <ElectronicAddress>
  </TSPAddress>
  <TSPInformationURI>
   <URI xml:lang="en">https://www.inclusion.gob.es/en </URI>
  </TSPInformationURI>
 </TSPInformation>
 <TSPServices>
```

```
  <TSPService>
   <ServiceInformation>
          <ServiceTypeIdentifier>
     https://train.trust-scheme.de/schema/visa-
schema.json</ServiceTypeIdentifier>
   <ServiceName>
    <Name xml:lang="en">Visa Credit</Name>
   </ServiceName>
   <ServiceDigitalIdentity>
    <DigitalId>
          <X509Certificate>...</X509Certificate>
    </DigitalId>
   </ServiceDigitalIdentity>
    <ServiceStatus>
  http://ehic.essif.trust-
scheme.de/ServiceTypes/Servicestatus/granted_</ServiceStatus>
      <StatusStartingTime>2021-05-
11T00:00:00Z</StatusStartingTime>
   </ServiceInformation>
  </TSPService>
 </TSPServices>
</TrustServiceProvider>
```

Every trusted VC issuer's details are described under the attribute <*TrustServiceProvider*>. The ID of the issuer is under the attribute <*IssuerName*>. Each VC issuer in the trust list has a Service Type Identifier under the attribute <*ServiceTypeIdentifier*>. This is a URL, and the web page that it points to should contain the JSON schema (including the @context property) for the VCs that are issued for this Service Type. In this way the verifier can find out which attributes the issuer is trusted to issue. This trust list also offers the flexibility to the service provider to add different services with different schemas. An example of such a JSON Schema follows:

```
{
    "description": "this is the web page published by the trust
federation pointed to by one of its Service Type IDs",
    "vctype": "",
    "@contexts": ["https://www.w3.org/2018/credentials/v1"],
    "schema": {
        "$schema": "https://json-schema.org/draft/2019-
09/schema",
        "description": "",
        "title": "",
        "type": "",
        "definitions": {
            "credentialSubject": {
                },
        "properties": {
            "credentialSchema": {
            },
            "termsOfUse": {
```

```
                    "type": "array",
                    "items": {
                        "type": "object",
                        "properties": {
                            "trustScheme": {
                                "type": "array",
                                "items": {
                                    "type": "string"
                                }},"id": {
                                "format": "uri-template",
                                "type": "string"
                            },"type": {
                                "format": "uri-template",
                                "type": "string"
                            }},
                        "required": [
                            "type",
                            "trustScheme"
                        ]}},
                "issuanceDate": {
                },
                "credentialSubject": {
                    "$ref": "#/definitions/credentialSubject"
                },id": {
                },"type": {
                    "type": "array",
                    "items": {
                        "type": "string"
                    }},
                "issuer": {
                    "format": "uri-template",
                    "type": "string"
                },
                "expirationDate": {
                                }
            },
            "required": [
                "id",
                "issuer",
                "issuanceDate",
                "expirationDate",
                "type",
                "credentialSubject"
            ],}
    }
```

5.3 TRAIN ATV

The TRAIN Automatic Trust Verifier (ATV) is designed to verify the trustworthiness of

a VC issuer given minimal information. It only requires two inputs to execute the trust policy defined by the verifier: one is the trust scheme name, that is embedded as a DNS name in the VC (see section 5.4), and the other one is the URI of the VC issuer, obtained from the VC. The URI of the issuer is flexible and may depend on the backend technology being used by the VC ecosystem. For example: the URI can be a DID that could be anchored in a blockchain/distributed ledger, but it could also be a https URL from a PKI. The TRAIN ATV is not restricted by the backend technology behind the VC in the SSI ecosystem.

The TRAIN ATV will read the PTR RRs, dereference the URI RRs, and expect to find an ETSI trust list published at this https URL. It will then check if the VC Issuer is listed in this DNS named trust list, and if so, will tell the verifier that the issuer is a trusted member of this trust scheme operated by this "DNS name". In this way it does not matter whether the issuer was telling the truth or not. The TRAIN API and the DNS controller/trust scheme operator establish the root of trust.

The source code of the ATV is freely available under Apache 2.0 [16]. ATVs can be run by anyone, so there can be multiple distributed copies of this service running in clouds or locally, and verifiers only need to keep pointers to one or more of them to provide them with backup services or completely under their own control.

5.4 Configuration at the issuer side

Every VC that is issued by any issuer that supports the TRAIN trust scheme must contain a standard Terms of Use property containing the DNS names of the trust scheme(s) that the issuer is a member of. These of course could be true or false statements. In any case as the Verifier will check them using the TRAIN API – what counts in the end is the actual inclusion into the trust list of the trust scheme operator. This enrolment is another process that is beyond this paper. The exact format of the TRAIN Terms of Use property is given below:

```
"termsOfUse": [{
    "type": "https://train.trust-scheme.de/info",
    "trustScheme": ["example.tso.com", "ssi.company.uk"]
}]
```

According to the W3C VC recommendation, each Terms of Use must have a globally unique type, and we have reserved the value "*https://train.trust-scheme.de/info*" to refer to the TRAIN Terms of Use type.

5.5 Configuration at the verifier side

All the verifier has to do is configure the DNS names of the trust schemes that it trusts, and the URL(s) of the TRAIN ATV API(s) to call to verify their membership lists. When it receives a VC, it extracts the asserted trust schemes made by the issuer in the ToU

property, and if it trusts any of the listed trust schemes, it calls the TRAIN API, passing it the URI of the issuer (taken from the VC) and the DNS name of the trusted trust scheme that the VC Issuer purports to be a member of. The TRAIN API will then check if the VC issuer is a member of any of the trust lists pointed to by this trust scheme, and if so, return the Service Type URL to the Verifier. The verifier can use the schema contained at this URL to validate that the attributes in the received VC match the schema for this Service Type.

```
{
   "Issuer": "https://vc.bge.verifiablecredentials.net",
   "Trust_Scheme_Pointer": "ssi.company.uk"
}
```

6 Future work

The integration of TRAIN with VC issuers and verifiers has been described in this paper, but the integration of TRAIN with other components like the VC holder still remains to be done. This work is currently being specified by the OpenID Foundation and the Decentralised Identifier Foundation (DIF). DIF is defining presentation definitions, as part of the presentation exchange specification [20], which allows a verifier to indicate to a holder, which VCs it should return in a verifiable presentation. OpenID Connect is being enhanced so that it can transfer presentation definitions from the verifier to the holder, and verifiable presentations from holders to verifiers, using the OIDC SIOPv2 protocol [21]. The latest draft [10] contains informative implementation guidelines describing how issuers, holders and verifiers can utilise the TRAIN trust scheme approach.

Further work describing how to incorporate both Public Key Infrastructure (PKI) and DID public keys in ETSI Trust lists is planned, thereby offering the possibility of integrated trust lists. Currently ETSI Trust Lists only support PKI public keys.

Moreover, TRAIN is being developed further towards an architecture that could accommodate DIDs as trust-scheme pointers besides DNS HostNames. This would enable a TRAIN trust infrastructure that does not rely on the DNS System, but could rely on alternative trust anchors, such as blockchains or other distributed ledgers.

7 Conclusion

In order to accomplish the promise of a bright future for identity management, SSI solutions need to address some fundamental trust and governance challenges. Although the current SSI offers modern cryptographic trust to enhance the privacy of users, the challenge of institutional trust still needs to be addressed. Without institutional trust, it is impossible for a relying part to verify the credibility of a VC issuer.

The TRAIN approach leverages the DNS, an already proven and universally accepted trust anchor, to provide a trust management infrastructure for SSI in a distributed manner. This is an important first step in providing the necessary credibility to make SSI also attractive for relying parties.

Bibliography

[1] C. Allen, "The Path to Self-Sovereign Identity," *GitHub*, Apr. 26, 2016. https://github.com/ChristopherA/self-sovereign-identity (accessed Feb. 05, 2020).

[2] EU Commission, "A cybersecure digital transformation in a complex threat environment — Brochure," *Shaping Europe's digital future*, Jan. 28, 2021. https://digital-strategy.ec.europa.eu/en/library/cybersecure-digital-transformation-complex-threat-environment-brochure (accessed Feb. 18, 2022).

[3] INATBA, "Decentralized Identity: What is at Stake?," INATBA Identity Working Group, Nov. 2020. Accessed: Feb. 08, 2021. [Online]. Available: https://inatba.org/news/inatba-identity-working-group-publishes-position-paper-on-decentralised-identity/

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

[5] M. Kubach, C. H. Schunck, R. Sellung, and H. Roßnagel, "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, pp. 35–47.

[6] M. Kubach and H. Roßnagel, "A lightweight trust management infrastructure for self-sovereign identity," in *Open Identity Summit 2021 - Lecture Notes in Informatics (LNI) - Proceedings*, H. Roßnagel, C. H. Schunck, and S. Mödersheim, Eds. Bonn: Köllen Druck + Verlag GmbH, 2021, pp. 155–166.

[7] Strüker, J., Urbach, N., Guggenberger, T., Lautenschlager, J., Ruhland, N., Schlatt, V., Sedlmeir, J., Stoetzer, J.-C., Völter, F., "Self-Sovereign Identity - Foundations, applications, and potentials of portable digital identities." Project Group Business & Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT, Bayreuth., 2021.

[8] W3C, "Decentralized Identifiers (DIDs) v1.0," *W3C Working Draft 08 February 2021*, Feb. 08, 2021. https://www.w3.org/TR/did-core/ (accessed Feb. 09, 2021).

[9] W3C, "Verifiable Credentials Data Model 1.0," *W3C Recommendation 19 November 2019*. https://www.w3.org/TR/vc-data-model/ (accessed Feb. 06, 2020).

[10] "OpenID Connect for Verifiable Presentations." https://openid.net/specs/openid-connect-4-verifiable-presentations-1_0-07.html (accessed Feb. 11, 2022).

[11] "Trust Over IP - Defining a complete architecture for Internet-scale digital trust," *Trust Over IP*. https://trustoverip.org/ (accessed Feb. 18, 2022).

[12] ENISA, "Digital Identity: Leveraging the SSI Concept to Build Trust," European Union Agency for Cybersecurity, Athens, Heraklion, Jan. 2022. [Online]. Available: https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust

[13] *ToIP TSS0001>: Trust Registry Specification*. Trust over IP Foundation, 2021. Accessed: Jan. 12, 2022. [Online]. Available: https://github.com/trustoverip/tswg-trust-registry-tf

[14] “Gaia-X Federation Services (GXFS) White Paper - Gaia-X Ecosystem Kickstarter.” GAIA-X, Feb. 12, 2021. [Online]. Available: https://gaia-x.eu/sites/default/files/2021-12/GXFS_1.pdf
[15] “Global COVID Certificate Network (GCCN),” *Linux Foundation Public Health*. https://www.lfph.io/global-covid-certificate-network/ (accessed Jan. 12, 2022).
[16] ESSIF-LAB, “eSSIF-TRAIN by Fraunhofer-Gesellschaft | eSSIF-Lab.” https://essif-lab.eu/essif-train-by-fraunhofer-gesellschaft/ (accessed Feb. 11, 2022).
[17] S. Wagner, S. Kurowski, U. Laufs, and H. Roßnagel, “A mechanism for discovery and verification of trust scheme memberships: the LIGHTest Reference Architecture,” in *Open Identity Summit 2017, Lecture Notes in Informatics (LNI)*, Bonn, 2017, vol. P277, pp. 81–92.
[18] W3C, “DID Specification Registries,” *W3C Working Group Note 02 November 2021*, 2021. https://www.w3.org/TR/did-spec-registries/#did-methods (accessed Feb. 18, 2022).
[19] ETSI: Electronic Signatures and Infrastructures (ESI), “General Policy Requirements for Trust Service Providers.” ETSI, Sophia Antipois Cedex, France, European Standard ETSI EN 319 401, 2016. [Online]. Available: http://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.01.01_60/en_319401v020101p.pdf.
[20] “DIF Presentation Exchange.” https://identity.foundation/presentation-exchange/ (accessed Feb. 11, 2022).
[21] OpenID Connect, “openid-connect-self-issued-v2-1_0-07,” *Self-Issued OpenID Provider v2*, Jan. 28, 2022. https://openid.net/specs/openid-connect-self-issued-v2-1_0.html