Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 254 (2025) 10–19

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Digital Sovereignty (ICDS)

A trust implementation model for cross-domain decentralized identity ecosystems: architecture, use case, and implementation

Isaac Henderson Johnson Jeyakumar[a*], Michael Kubach[a]

[a]*Fraunhofer IAO, Nobelstr. 12, 70569 Stuttgart, Germany*

Abstract

Managing interoperable trust across different domains – as required for a wide adoption of decentralized / self-sovereign identities (SSI) leveraging verifiable credentials – remains a challenge. Verifiable credentials are a part of numerous international and European initiatives like the EUDI Wallet, EBSI, and Gaia-X to enable sovereign data sharing. Nevertheless, a standardized reference framework addressing interoperability challenges around trust in cross-domain environments based on decentralized identities is missing and is one factor hindering wider adoption. To facilitate the interoperability of credentials across borders and organizations this paper proposes a new trust implementation model architecture that enables credentials issued by different entities to be shared and verified in a trustworthy manner. This implementation model architecture also contains a novel unified signature and verification model for the trust list. A use case and implementation details for the model are presented. Furthermore, it discusses potential integration possibilities with existing initiatives using the proposed architecture.

Keywords: decentralized identity, eIDAS, ssi, trust infrastructure, trust registries, verifiable credentials.

1. Introduction

Decentralized identity management technology is currently developing fast, and standards are not yet stable. This is exemplified by the discussions around the development of the Architecture Reference Framework (ARF) for the EU Digital Identity (EUDI) Wallet [1]. At the same time, multiple trust domains (various national trust domains, various

* Corresponding author. Tel.: +49-711-970-2431.
E-mail address: isaac-henderson.johnson-jeyakumar@iao.fraunhofer.de

1877-0509
10.1016/j.procs.2025.02.059

industries etc.) exist and are likely to prevail. It might be overly optimistic to settle on one specific decentralized identity technology and trust domain. Hence, a trust management infrastructure should aim to be agnostic towards the specific decentralized identity technology, ledger, and framework (e.g., EBSI, Indy). It should be able to bridge different trust domains and to allow individual entities and frameworks to make sovereign trust decisions – largely independent of the underlying technology.

Ecosystems building on federated or decentralized identity management technologies (such as self-sovereign identity SSI) require a decentralized, flexible, scalable, and interoperable trust infrastructure to manage information on trusted entities, federations, or participants in the ecosystem. Individual entities or groups of entities (ecosystems) must be able to define and manage their trust anchors in a sovereign way. On the other hand, to ease adoption, it must be possible for individual entities and ecosystems to easily delegate individual trust decisions to trustable authorities and integrate trust anchors according to their requirements. Moreover, it must be possible to connect trust anchors across trust domains to achieve interoperability across federations and eventually bridge ecosystem boundaries.

Different approaches for trust management infrastructures have been implemented and proposed. One is the eIDAS concept of publishing trusted lists of qualified trust service providers in accordance with the eIDAS Regulation [2]. However, such an approach is neither open nor flexible. It is focused on a very specific trust domain and does not allow for the sovereign creation of trust anchors. Hence, with an evolution of the TRAIN (Trust Management Infrastructure) concept, we propose in this paper a flexible and cross-domain trust implementation model with a unified signature and verification model for trust lists that could be used for the EUDI, Gaia-X dataspaces and beyond.

2. Related approaches for trust management: state-of-the-art

Establishing trust in credential ecosystems has remained a challenge despite years of research, regulatory approaches, and numerous proposed solutions. For some credential ecosystems such approaches and solutions are already (or soon to be) used, which could make integration with them advisable. Moreover, they can serve as valuable building blocks and allow for learnings to develop the TRAIN concept further. Hence, in the following, we compare some approaches for trust management that have been proposed and implemented.

2.1. Gaia-X

Gaia-X [3] is a cloud and dataspaces initiative that builds on decentralized identity and verifiable credential (VC) approaches for identity and access management. Dataspaces can be defined as ecosystems for sovereign exchange with the goal of value creation across organizational boundaries. They require a high level of security and trust – but adoption must be easy as well to reach a critical mass of participating entities. The trust implementation model for Gaia-X is in development. Currently, trust is established via the Trust Registry and Compliance Service. Participants, whether individual organizations or federations of companies have to register their X.509 certificate chain in the Trust Registry and receive a compliance credential from the Compliance Service in order to enroll. This credential is used to prove the membership in the Gaia-X ecosystem, an entity possessing the credential complies to the terms of Gaia-X [3]. The current Gaia-X model is relatively centralized via the Trust Registry and Compliance Service. So far, did:web is supported to validate the participant's credential proof. Despite the goal of federations being able to sovereignly define their own trust anchors, the current trust framework supports only did:web and X.509 certificates. Moreover, federations are not able to set up their independent trust registry or anchor on a proprietary blockchain. Also, establishing a chain of trust across organizations, federations, and compliance services in a decentralized way is not possible.

2.2. EBSI trust registries

The European Blockchain Service Infrastructure (EBSI) is a public sector-driven initiative of the European Blockchain Partnership (EBP) that aims to provide cross-border public services using blockchain technology. The EBSI framework includes an SSI model leveraging verifiable credentials (based on the W3C standard) and decentralized identifiers (did:ebsi) [4]. The EBSI Trust Model makes use of the EBSI Ledger. In a nutshell, the EBSI Issuer Trust Model defines Trusted Accreditation Organizations (TAOs) that are responsible for accrediting Trusted

Issuers in a certain domain of trust to issue certain VCs. An example given is the Ministry of Education of a country accredits a university to issue diplomas in the form of VCs. The EBSI ledger acts as a public registry of TAOs and Trusted Issuers, their DID, DID document and additional information. This Trusted Issuers Registry (TIR) stores information in a smart contract. The structure of the trust model is hierarchical: an EBSI member states requests a TAO to be authorized by the EBSI Help Desk who is a gatekeeper that issues the verifiable authorization associated with the DID of a TAO. This is the root accreditation that starts a new trust chain. The TAO then also can accredit sub-TAOs. TAOs accredit trusted issuers. An API allows to interact with the public TIR smart contract [5].

By design, the EBSI trust implementation model is focused on the EBSI ecosystem with its use cases. The infrastructure is provided by the public permissioned EBSI ledger and there are gatekeepers with the Member States and the EBSI Help Desk. The structure of the trust model is hierarchical, and the trust relevant information is stored in one place: on the ledger (replicated over the EBSI nodes). Retrieving the trust information is fundamentally open for other domains of trust that want to integrate this information into their ecosystem and/or use cases. However, not everyone can or would want to set up their own EBSI-based trust chain for their domain of trust. The reason could be that it might not be in their interest to be dependent from an accreditation EBSI Member States/the EBSI Help Desk or that these gatekeepers have no interest in accrediting them – for example for use case ecosystems beyond the initial scope of EBSI, outside of Europe, very small ones etc. While the flexibility of this trust model and its applicability is limited, it has support from the European Commission and member states and could certainly act as a valuable trust anchor for certain credentials.

2.3. Legal person and organization identifiers

Different approaches towards identifiers for legal persons and organizations have been proposed. The verifiable LEI (vLEI) is such an identifier and comes in the form of a verifiable credential. It is issued by the Global Legal Entity Identifier Foundation (GLEIF). GLEIF is a supra-national non-profit organization that oversees the Legal Entity Identifier (LEI) [6]. The LEI references key information about an entity via a 20-character, alpha-numeric code. Originating in the financial sector, it aims to also cover entities in other sectors. The vLEI is the counterpart of the LEI and that can be automatically verified. It is based on the decentral KERI protocol and the Trust over IP Authentic Chained Data Container (ACDC) specification. The vLEI is agnostic towards the blockchain or decentralized key management platform underlying a specific identity system. Qualified vLEI Issuers (QVIs) issue the vLEI for organizations and then persons representing organizations can receive vLEI Role Credentials. The vLEI has been in productive use since the end of 2022. The ultimate root of the vLEI trust in this implementation model is GLEIF as governing authority. From there a hierarchical structure emerges. If the vLEI of a QVI gets revoked by GLEIF, all vLEIs issued by this QVI get revoked as well [6]. This model is clearly advantageous for ecosystems that integrate well with the scope of GLEIF and accept it as governing authority but limits the approach for use cases beyond.

DID ETSI Legal person Semantic Identifier Method Specification (did:elsi) is a DID method for legal persons. It aims to bridge the world of the eIDAS regulation with that of W3C VCs for use cases that require with high levels of legal certainty and compliance. did:elsi gives legal persons possessing an advanced or qualified signature or seal according to eIDAS a DID identifier, leveraging the already existing eIDAS trust framework [7]. Hence, the complex task of creating a new trust framework can be skipped and for ecosystems and use cases where eIDAS legal compliance is relevant, this is a huge advantage. However, it also limits the scope of this trust implementation model to these use cases. Internationally and in many use cases the eIDAS framework might be not acceptable and not flexible enough.

2.4. Open ID Federation

The Open ID Federation 1.0 specification [8] from OpenID Connect provides an automated determination whether an OpenID relying party (RP) and an OpenID provider (OP) can trust one another, given one or more shared trust anchors. It also assists in the discovery, policing and updating of RP and OP metadata, federation wide. Moreover, it provides features for the registration of RPs as clients at OPs, saving costly human administration. The trust resolution

takes place as a two-step process, namely obtaining the trust chain and validating the trust chain. The trust chain with its metadata is published under /.well-known/openid-federation. A json-based data format is used for publishing the meta data and trust chain [8]. The OpenID Connect Federation 1.0 trust chain is similar to a X.509 certificate chain. Both types of chains can be used to assert and verify that a named entity owns a given public key, by defining a data structure for authorities to sign the public keys of subjects. X.509 thus enables the creation of a public key infrastructure, to secure communications over the Internet. Currently, the approach has also been used in the Proof of Concept (PoC) of the GAIN project [9].

OpenID Connect Federation 1.0 is not bound to OpenID Connect use cases only. It could be suited for other domains as well, for instance with OAuth 2.0 / 2.1, Internet of Things, and wallets / verifiable credentials. However, the currently specified trust chain approach does not provide details regarding the support of other cross-domain trust frameworks.

2.5. eIDAS trusted lists

In the EU, the eIDAS regulation on electronic identification and trust services for electronic transactions in the internal market provides a regulatory environment for electronic identification and trust services. In 2024 a revision that is informally called eIDAS 2.0 [10] was passed by the European Parliament and of the Council, whereas the initial eIDAS regulation [11] is referred to as, eIDAS Version 1. Already in Version 1 eIDAS defines so called trusted lists that are established, maintained, and published by the member states for qualified trust the service providers (and their services) for which the country is responsible. Non-qualified trust service providers can be included as well. It is important to note that trust service providers can offer their services in the whole EU market – not only in the country that is responsible for them. The idea was to create a free EU market for trust services. Qualified trust services are added to the Trusted List by the member states according to a defined process. The trusted lists indicate the status of service providers and of the services at the moment of supervision and follow ETSI TS 119 612 [11].

The EU Commission provides a List of Trusted Lists (LOTR) that contains the national Trusted Lists. Hence, we can observe a hierarchical structure of this trust implementation model. eIDAS gives a clear trust framework that is transparent and founded in accepted regulation. However, this framework is clearly focused on the EU market which might not make it suitable for use cases that involve actors beyond. Moreover, new trust anchors and trusted lists for specific use cases cannot be flexibly created. All this was simply not in the initial scope of eIDAS. According to the latest available version of the Architecture Reference Framework [1], it is envisioned that trusted lists and a LOTR will play an role for the trust framework of the EUDI Wallet. However, the details are still under development.

2.6. TRAIN

TRAIN (TRust mAnagement INfrastructure) originates from a subproject of the EU NGI eSSIF-Lab initiative [12], while its basic technology had already been developed and validated in several pilots of the EU LIGHTest project [13]. The conceptual approach of TRAIN as a lightweight trust infrastructure for decentralized identity uses the global, well-established, and trusted infrastructure of the Internet Domain Name System DNS as its root of trust, leveraging DNS's ubiquitous use and recognition [14]. The security extensions of DNS (DNSSEC) ensure that the results returned from DNS queries are authentic and have not been tampered with. Consequently, TRAIN uses DNSSEC whenever available. TRAIN uses trust lists to store information on trusted entities. For this it builds on the work of eIDAS Trusted Lists and therefore adopted the format described in ETSI TS 119 612 [15]. These lists are published by governance authorities (this can be basically anyone who controls a DNS record), include entities that are certified according to a certain trust framework that is maintained by the respective governance authority. This, for example, supports verifying entities in examining the trustworthiness of credentials originating from issuers through their inclusion in the trust list under a specific trust framework.

To integrate with verifiable credentials for the establishment of trust in credential issuers, TRAIN uses the termsOfUse attribute of the W3C VC Data model (VCDM) [16]. EBSI Trusted Lists follow a similar approach in using termsOfUse for verifiable accreditations. Moreover, it has been demonstrated how it can be leveraged to establish trust in verifiers [17]. Currently, TRAIN is specified to be used as a base architecture to provide decentralized governance of the federation services [18] of Gaia-X.

The TRAIN trust implementation model is highly flexible: individual entities can define their own trust anchors and policies, manage, and apply them. Individual entities or federations (industry organizations, manufacturer-supplier-networks, NGOs, etc.) can define for themselves the trust standards they require, establish trust frameworks, and publish trust lists of entities adhering to their trust framework. Cross-referencing of trust frameworks is possible. No central authority is established, anyone can issue certificates/credentials and set up their own trust frameworks, but TRAIN facilitates individual trust decisions through the defined discovery of trust lists via the established and widely accepted mechanism of the DNS. However, the first evolutionary stages of the architecture of TRAIN, as described in the resources above, were limited to ETSI trust lists in XML format. Different formats of trust lists and combination with decentralized identifier and wrapping in verifiable credentials had not yet been explored.

2.7. Comparison of existing approaches

Due to space limitations, only some of the approaches to trust management assessed while developing TRAIN could be presented above. Additionally, IRMA (Yivi) Schemes [19], VICAL [20], and TrustyDID [21] were considered as well. Comparing of these approaches allows to highlight some important commonalities, differences, and open aspects (see Table 1). Most of the approaches focus on a specific trust domain (e.g., Gaia-X, IRMA (Yivi), eIDAS, EBSI) and are not generic, flexible, or designed to incorporate other domains like TRAIN. This is also related to the specific authority governing the trust framework. It is usually fixed as well, for example with the Trust Registry/Compliance Service (Gaia-X), EBSI Help Desk, IRMA, eIDAS/EU Commission / Member States, GLEIF (vLEI). TRAIN and TrustyDID however, allow for the flexible specification of trust authorities. Most approaches are focused on a specific type of credential or certificate, e.g., EBSI, vLEI, OpenID Federation, Gaia-X (to be extended), while others aim to be more technology agnostic in this regard. The situation is similar when it comes to the DID methods that are supported. Many approaches only support their own proprietary methods (e.g., EBSI, ELSI) and sometimes did:web (e.g., Gaia-X) – others do not support DID at all (e.g., IRMA, VICAL). TRAIN on the other hand aims to be flexible in this regard as well. Finally, the maturity of the different approaches differs greatly. While eIDAS has been in use for years now (with limited adoption), most exist mainly as specifications, demonstrators and PoCs.

Table 1: Comparison of different trust management approaches

Trust Management Approach	Structure	Interoperable Support of Different Trust Anchors	DID Support	Support of X.509	Root of Trust	Support of Extendable Metadata
Gaia-X	Centralized	No	Yes	No	Distributed Authority using Clearing Houses	Yes
EBSI	Decentralized	No	Yes	No	EBSI	Yes
GLEIF LEI	Centralized	No	No	Yes	GLEIF Foundation	No
OpenID Federation	Federated	No	Yes	No	CA Certificates	Yes
eIDAS v1 LOTL	Centralized	No	No	Yes	CA Certificates / EU Commission	No
TRAIN	Decentralized	Yes	Yes	Yes	DNS	Yes
trustyDID	Decentralized	No	Yes	No	DNS	Yes
VICAL	Centralized	No	No	Yes	CA Certificates	No
IRMA Schemes	Decentralized	No	No	No	Community-based	Yes

3. Evolution of the TRAIN trust implementation model

As described in section 2, TRAIN has been developed and implemented for different use cases. It gives the flexibility to sovereignly set up specific trust frameworks. So far, the integration of existing trust frameworks or trust registries and the use of different trust list formats with different identifiers were not part of the existing architecture

(beyond the integration of eIDAS Trusted Lists, that had already been possible in LIGHTest, the predecessor project to TRAIN). Therefore, we will describe how TRAIN could accommodate different trust list formats as well as integrate other trust registries. Hence, in this paper we propose a novel unified signature & verification model for trust lists via decentralized identifiers (DIDs) and verifiable credentials as an evolution of the existing TRAIN architecture.

3.1. Unified signature and verification model for trust lists

The Unified signature and verification model for trust list via DID and VC allows trust lists across trust domains to be signed and verified uniformly leveraging decentralized identifiers and verifiable credentials. This is achieved by enveloping the storage location of the Trust List (Trusted Data Store, e.g., a https URL or Interplanetary File System - IPFS) in the credential subject of a VC. The entity operating the trust framework is responsible for signing the VC with its proof. To make the enveloped VC universally resolvable it is anchored in the service endpoint of the DID document in its instantiation process. The DID used for resolving the enveloped VC will further be anchored in the DNS URI RR. An example for an enveloped xml trust list is given below.

```
{ "@context": [
          "https://www.w3.org/2018/credentials/v1",
          "https://w3id.org/security/suites/jws-2020/v1",
          "https://schema.org"],
  "type": ["VerifiableCredential"],
  "id":"did:web:company1.com#issuer-lists",
  "issuer": " did:web:company1.com ",
  "issuanceDate": "2023-03-21T12:00:00.148Z",
  "credentialSubject": {
  "hash": "Qma9obqf2eXvbQmhtUu9Av6NYaykB25rXqXRziE3Qq7LnK",
    "id": "uuid:2632367287r82729",
    "trustlisttype": "XML based Issuer Lists",
    "trustlistURI":"https://company1.com/trust-list/federation.xml" },
  "proof": {
    "type": "JsonWebSignature2020",
    "created": "2023-07-20T07:42:14.094Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "did:web:company1.com#owner",
    "jws":"eyJhbGciOiJQUzI1NsImI2NCI6ZmFsc2UsImNyaX"  }}
```

This could also be extended to JSON formats and user-defined data models. By using this approach, the requirement of individual signature suites for specific data model can be avoided (xades, jades). In the initial TRAIN approach (see section 2), the DNS URI RR references directly to the trust list via its URI. Now, to make the system more technology agnostic and at the same time provide support for ledger-based systems, a DID is placed in the URI RR. At the same time, the integrity of the DID with the DNS can be verified using the Well Known DID Configuration [22] approach, enhancing the security of the architecture further. In the following section, we illustrate the new trust implementation model with a concrete use case.

3.2. Gaia-X use case

As presented in section 2.1, Gaia-X aims to enable dataspaces that are currently facilitated by a trust implementation model leveraging a compliance service. However, the current approach restricts the sovereignty of federations and is centralized on the trust registry. The development of the trust implementation model of Gaia-X is still in progress. This gives the opportunity to take the Gaia-X ecosystem as an exemplary use case and demonstrate how TRAIN could be leveraged to implement trust in the Gaia-X ecosystem in a flexible way, giving more autonomy to the federations.

To make the use case concrete, we consider three entities of the Gaia-X trust ecosystem: (1) the compliance service, (2) a federation, and (3) an organization in the federation. In Gaia-X, individual federations can be established, which are then responsible for enrolling organizations. As an example: Catena-X is a dataspace initiative, an automotive federation where car makers and suppliers can get enrolled to exchange data in a trustworthy manner. Such a federation has to be enrolled in the Gaia-X compliance service in order to be part of the Gaia-x ecosystem.

Now, complementing the existing architecture of Gaia-X, the trust implementation model of TRAIN enables the Gaia-X compliance service, federation and organizations to act autonomously and flexible while at the same time maintaining an established chain of trust (see Fig. 1). To achieve this, PTR and URI RRs of the DNS are used to reference other trustable trust frameworks. Moreover, URI RRs contain DIDs resolvable for the enveloped trust list.

When a federation enrolls in the compliance service, the federation's meta data is added to the trust list of the compliance service. On successful enrollment to the compliance service the federation sets an additional PTR RR in its own trust framework ((_scheme._trust.notary.federation1.eu). So now the trust framework (notary.federation1.eu) has two PTR RR, one referring to its own and the other pointing to compliance service. RR pointing to the federation's trust framework (_scheme._trust.notary.federation1.eu). The same applies when an organization is enrolled in the trust framework of a federation it sets an additional PTR RR in its own trust framework (_scheme._trust.trust.organization1.eu). The trust implementation model provides the flexibility and autonomy for compliance service, federation and organization to have their trust lists anchored in e.g., did:web, did:ebsi, or did:sov. With this, Gaia-X can integrate participants following conventional identity management (e.g. did:web) as well as DLT-based (e.g. did:ebsi) technologies.

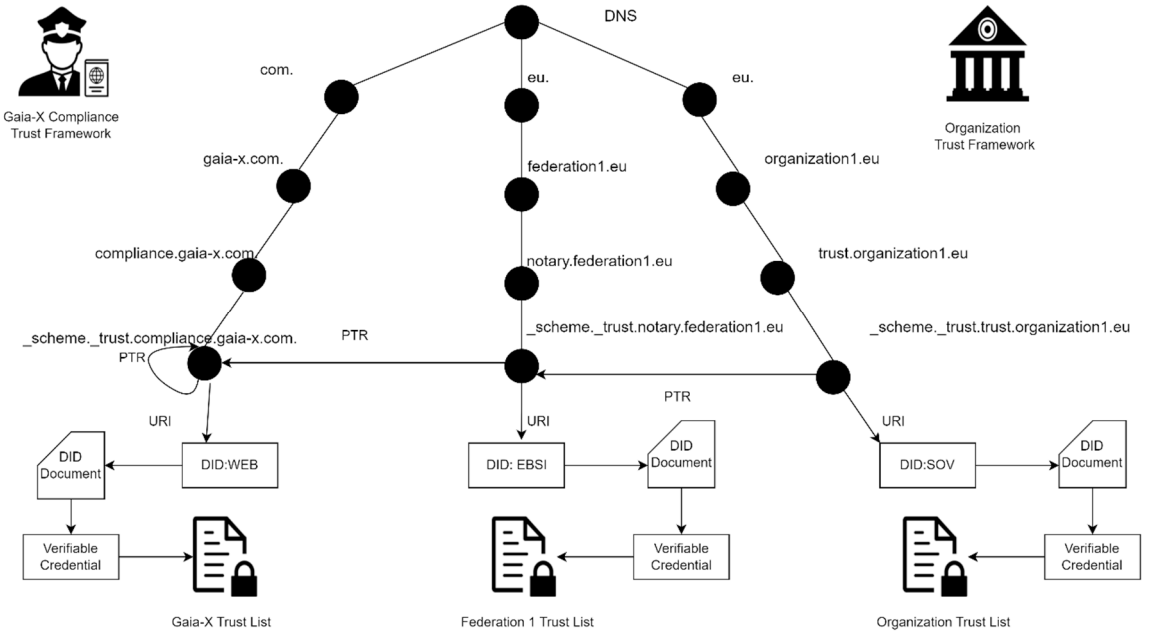

Fig. 1. Chain of trust and trust references in the Gaia-X use case with TRAIN

To verify the trust chain, the trust framework details are included in the termOfUse object of a self-description, or the VCs issued by the compliance service or federations. Hence, a credential issued by a federation, must contain a reference to its own framework and the compliance service trust framework in the termsOfUse as shown below.

```
"termsOfUse": [{
"type": "train",
"id":"https://train.trust-scheme.de/info",
    "trustScheme": ["notary.federation1.eu", "compliance.gaia-x.com"]}]
```

Similarly, the credential issued by an organization will contain in the termsOfUse the trust framework pointers of its own organizational trust framework, those of its federation and compliance service.

The current version of the compliance service just verifies the hash of the VC against the X.509 certificate chain, which is registered in the registry service. Moreover, federations' sovereignty to define their own trust anchors is limited due to the centralized trust registry approach. Hence, TRAIN based trust implementation model could offer decentralized governance and interoperability which can be used to enhance the flexibility and autonomy of federations in the Gaia-x use case and beyond.

3.3. High level TRAIN architecture

After introducing the TRAIN trust implementation model with a potential use case, the different TRAIN components with its architecture can be presented in more detail. Fig. 2 gives an overview of the architecture before we address the main components. The component *TRAIN Trust Framework Manager* (*TFM)* is responsible for configuring and managing trust frameworks with its corresponding trust lists. It handles the hosting of the trust list and the enveloping the trust list as VC. Moreover, it anchors the enveloped VC storage URI in the service end points of the DID Document. Finally, it transfers the data that is anchored in the DNS using the Zone Manager. The detailed data flow diagram for the Trust Framework and Trust List Provision can be found in the following link [23].

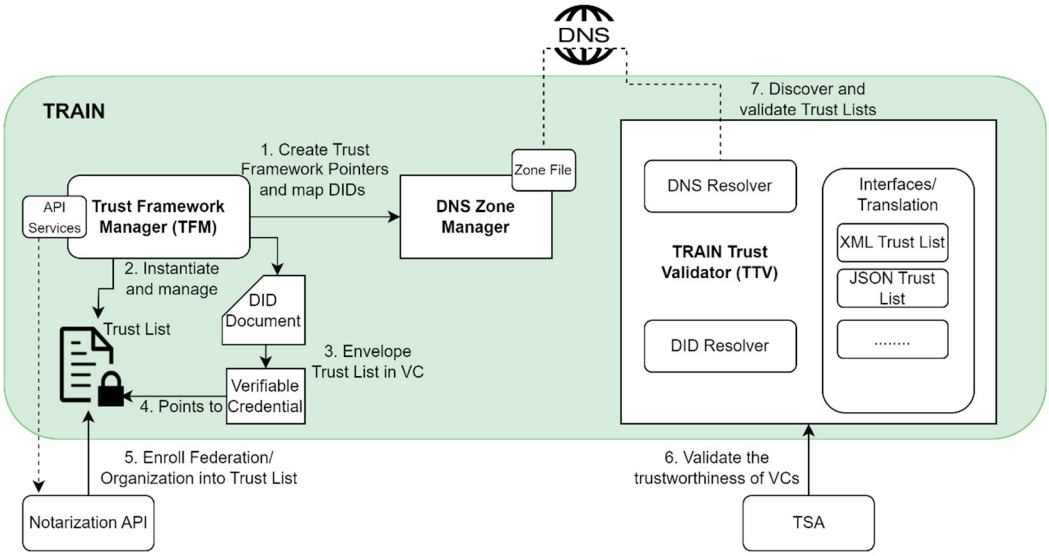

Fig. 2. High-Level Architecture of TRAIN for Gaia-X Use Case

The *DNS Zone Manager* is responsible for managing the DNS zone file and used to anchor the trust framework DID information into the DNS zone file. It also for re-signs the zone file for DNSSEC for every new update.

The *TRAIN Trust Validator (TTV)* performs the trust verification. It is responsible for the trust discovery and validation based on the input from the VC / Verifiable Presentation. The trust discovery process is realized via the DNS Resolver and the Universal DID Resolver. And the detailed data flow diagram can be found in the following link. Currently, the TTV validates the trust list to verify that issuer of the VC /VP is present in the trust list. But SSI Verifiers can have additional policies to validate different attributes of the trust list. The detailed data flow diagram of the trust discovery and validation process can be found in the following link [23].

Depicted in Figure 2 while not part of the TRAIN architecture but rather components of the Gaia-X Federation Services (GXFS) used for creating and issuing participant credentials to participants/organizations are Notarization API and Trusted Services API (TSA). Using the TRAIN TFM, a notary service or institution can use the Notarization API to onboard trusted participants to the trust list. The TTV enables the TSA to perform trustworthiness validation of credentials. This in turn enables decentralized onboarding and validation of credentials issued across federations.

3.4. Implementation details

This section provides insights into the implementation specifics for the components delineated in Section 3.3. Their

production-ready source code, complete with Helm charts, is available in the GXFS GitLab repository [27].

The TFM facilitates backend processes with API endpoints designed to manage trust lists and trust service providers, as well as to anchor trust frameworks and DIDs via the Zone Manager. It offers users and organizations the ability to configure various storage types, such as IPFS or local storage, and trust list formats, including XML and JSON. The TFM's modular design allows for the integration of both internal and external VC signers. For instance, the TSA Signer component, developed within the GXFS framework, was adopted as an external signer. When enrolling DIDs through the TFM endpoints, the system is designed to perform validation checks. For instance, for the enrollment of a `did:web`, the system verifies the presence and authenticity of the DID Document as well as the existence of a corresponding well-known configuration file for the domain. Customizable rules can be established for various DID methods to align with the interests of users or organizations. Moreover, all endpoints are secured with JSON Web Tokens (JWT), and there is an option to configure different OpenID Connect (OIDC) servers. The API endpoints provided by the TFM are documented at the following link [24].

The *DNS Zone Manager Service*, leveraging Name Server Daemon (NSD), has been implemented as an extension to the LIGHTest repository [25]. While LIGHTest was originally limited to anchoring trust list URIs within DNS, the now enhanced version accommodates DID anchoring. Additionally, a Docker-based implementation of the Zone Manager was developed to facilitate easier deployment and configuration of various domains.

The *TTV* is tasked with validating the trustworthiness of VCs and Verifiable Presentations (VPs) by examining issuer details and termsOfUse information. This process involves more than just examining the content within trust lists; it also verifies the trust chain from DNSSEC to the integrity of the trust list. The TTV further examines various service endpoints specified within the DID Document. The resolve and validate endpoints provided by the TTV can be accessed at [26].

4. Conclusion

Managing interoperable trust across diverse ecosystems presents a considerable challenge, as the landscape of identity technology rapidly evolves, and new standards continue to emerge. This paper has provided a comprehensive overview of existing and proposed approaches for trust management. Centralized trust management systems prevail in the current paradigm, suitable mostly within domains where participants are willing to acknowledge a single authoritative entity as the gatekeeper. Such systems, however, are often also constrained by their affiliation to specific credential formats or technological solutions, limiting their applicability across different ecosystems further.

In response to these limitations, we have proposed an advancement to the TRAIN trust implementation model, predicated on a thorough examination of prevailing trust management approaches. The proposed model introduces a unified signature and verification mechanism for trust lists, facilitating the sovereign deployment of specific trust frameworks. The versatility of the TRAIN's concept transcends the confines of particular credential or DID formats, positioning it as a potentially universal trust model for initiatives such as Gaia-X, other data spaces, and the European Digital Identity Wallet (EUDIW), thereby bridging geographic and sectoral domains of trust. The presented unified signature and verification model has been successfully implemented recently within the GXFS [28] and has undergone testing with two distinct trust list formats. However, while TRAIN leverages established standards such as the W3C VCDM and the ETSI guidelines for Trust Lists, the model itself has yet to attain standardization. It is presently referenced in the implementation considerations to establish trust among federations in Gaia-X, and ongoing efforts within the W3C Community Group on Verifiable Issuers and Verifiers [29] are indicative of the need for further standardization efforts in this domain. Moreover, as our future work it is planned to extend the implementation to accommodate Open ID Federation based trust lists and the EBSI Trusted Issuers Registry. Due to the limited space available, the current paper focuses on the general architecture and high-level comparison with alternative approaches. A more detailed security analysis and implementation details will be subject to a future paper.

Disclaimer: The authors did not use any AI-assisted tool for improving English or enhancing language accuracy, including spelling, grammar, and punctuation. The author accepts full responsibility for the originality of the final content of this publication.

References

[1] eIDAS Expert Group, "EUDI Wallet - Architecture and reference framework 1.4.1." Accessed: Sep. 30, 2024. [Online]. Available: https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.4.0/

[2] European Commission, "eIDAS Dashboard: EU/EEA Trusted List Browser." Accessed: Jul. 20, 2023. [Online]. Available: https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home

[3] Gaia-X, "Gaia-X / Data-Infrastructure Federation Services / AuthenticationAuthorization · GitLab," GitLab. Accessed: Mar. 15, 2023. [Online]. Available: https://gitlab.com/gaia-x/data-infrastructure-federation-services/authenticationauthorization

[4] EBSI, "What is EBSI," What is EBSI. Accessed: Jul. 20, 2023. [Online]. Available: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi

[5] EBSI, "Issuers trust model - Accreditation of Issuers, EBSI Specifications." Accessed: Jul. 20, 2023. [Online]. Available: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Issuers+trust+model+-+Accreditation+of+Issuers

[6] GLEIF, "Introducing the verifiable LEI (vLEI) - vLEI," Introducing the verifiable LEI (vLEI) - vLEI – GLEIF. Accessed: Jul. 14, 2023. [Online]. Available: https://www.gleif.org/en/vlei/introducing-the-verifiable-lei-vlei/

[7] J. Ruiz, "DID ETSI Legal person Semantic Identifier Method Specification (did:elsi)," DID:ELSI Method. Accessed: Jul. 21, 2023. [Online]. Available: https://alastria.github.io/did-method-elsi/

[8] R. Hedberg et.al, "OpenID Connect Federation 1.0 - draft 29." Accessed: Aug. 14, 2023. [Online]. Available: https://openid.net/specs/openid-connect-federation-1_0.html#name-federation-policy

[9] "OpenID Connect Federation 1.0 explained | Connect2id."Accessed:Aug.14,2023.[Online].A: https://connect2id.com/learn/openid-connect-federation

[10] European Parliament and the Council. (2024) "Regulation (EU) No 2024/1183 of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework."

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

[12]ESSIF-LAB, "eSSIF-TRAIN by Fraunhofer-Gesellschaft | eSSIF-Lab." Accessed: Feb. 11, 2022. [Online]. Available: https://essif-lab.eu/essif-train-by-fraunhofer-gesellschaft/

[13] Wagner, Sven, Sebastian Kurowski, Uwe Laufs and Heiko Roßnagel. (2017) "A mechanism for discovery and verification of trust scheme memberships: the LIGHTest Reference Architecture," in *Open Identity Summit 2017*, *LNI*, pp. 81–92.

[14] Kubach, Michael and Heiko Roßnagel. (2021) "A lightweight trust management infrastructure for self- sovereign identity", *Open Identity Summit 2021, LNI,* pp. 155-166.

[15] 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, 2016. [Online]. Available: http://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.01.01_60/en_319401v020101p.pdf.

[16] Johnson Jeyakumar, Isaac H., David W. Chadwick and Michael Kubach. (2022) "A novel approach to establish trust in verifiable credential issuers in Self-sovereign identity ecosystems using TRAIN," *Open Identity Summit 2022, LNI*, Bonn, pp. 27–38.

[17] Chadwick, David W., Michael Kubach, Ioram Sette and Isaac H. Johnson Jeyakumar. (2023) "Establishing Trust in SSI Verifiers," *Open Identity Summit 2023, LNI,* pp. 15–26.

[18]GXFS, "Gaia-X Federation Services (GXFS) werden erweitert," GXFS.eu. Accessed: Jul. 12, 2023. [Online]. Available: https://www.gxfs.eu/de/ausschreibung-identity-trust/

[19]yivi, "yivi.app," Yivi: a product by SIDN. Accessed: Jul. 21, 2023. [Online]. Available: https://www.yivi.app

[20]ENISA, "Digital Identity Standards," ENISA, Jul. 2023. Accessed: Jul. 21, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/digital-identity-standards

[21]CIRALabs, "TrustyDID." Accessed: Jul. 21, 2023. [Online]. Available: https://github.com/CIRALabs/TrustyDID/tree/main

[22]Buchner et.al, "Well Known DID Configuration." Accessed: Jul. 21, 2023. [Online]. Available: https://identity.foundation/.well-known/resources/did-configuration/

[23]"TRAIN Data Flow Diagrams." Accessed:Feb.12,2024.[Online]. Available: https://essif.iao.fraunhofer.de/files/paper/Data-flow-Diagrams.pdf

[24]"TRAIN / Train Trust Framework Manager · GitLab," GitLab. Accessed: Feb. 16, 2024. [Online]. Available: https://gitlab.eclipse.org/eclipse/xfsc/train/tspa

[25]H2020LIGHTest/ZoneManager. (Nov. 10, 2022). Python. Horizon 2020's LIGHTest. Accessed: Feb. 16, 2024. [Online]. Available: https://github.com/H2020LIGHTest/ZoneManager

[26]"Open API TCR," GitLab. Accessed: Feb. 23, 2024. [Online]. Available: https://gitlab.eclipse.org/eclipse/xfsc/train/trusted-content-resolver/-/tree/main/deploy/helm/tcr-service/templates?ref_type=heads

[27]"TRAIN / Train Trust Validator · GitLab," GitLab. Accessed: Feb. 16, 2024. [Online]. Available: https://gitlab.eclipse.org/eclipse/xfsc/train/trusted-content-resolver/-/tree/main?ref_type=heads

[28]eco and GAIA-X, Software Requirements Specification for Gaia-X Federation Services Trust Management Infrastructure IDM.TRAIN, 2023. Accessed: Aug. 10, 2023. [Online]. Available: https://www.eco.de/wp-content/uploads/2023/07/srs_idm.train_.pdf

[29]"Verifiable Issuers and Verifiers v0.1," Draft Community Group Report 05 January 2023. Accessed: Aug. 10, 2023. [Online]. Available: https://w3c-ccg.github.io/verifiable-issuers-verifiers/