Gaia-X Federation Services

for

Identity & Trust

Trust Management Infrastructure for Gaia-X Concept Document

Inhalt

List of Figures

List of Tables

1 Motivation

The Gaia-X Trust Framework requires a decentralized, flexible, scalable, and interoperable Trust Model to manage information on trusted entities, federations or participants in the ecosystem. Individual federations have to be able to define and manage their trust anchors in a sovereign way, while at the same time these trust domains have to be interoperable across federations.
Decentralized identity management technology is currently developing fast. At the same time, multiple trust domains exist. It might be overly optimistic to settle on one specific decentralized identity technology and trust domain. Hence, the trust management infrastructure, as defined in this document, aims to be agnostic towards the specific decentralized identity technology, ledger and framework (e.g., EBSI, Indy). Its goal is to bridge different trust domains and to allow individual entities and frameworks to make sovereign trust decisions.

Parts of this document are based on the work of the ICAM Gaia-X Community.

2 Introduction

The trust management infrastructure enables the establishment of a root of trust for entities acting in the Gaia-X ecosystem and credentials issued by these entities. This is achieved through the introduction of trust lists combined with anchoring of pointers in the DNS following the TRAIN (Trust Management Infrastructure) concept. These lists, published by Governance Authorities, 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 Issuers through inclusion in trust lists under a specific trust framework that is administered by a specific governance authority.
Gaia-X Federations and other entities are supported in the sovereign publication and administration of trust lists for specific trust frameworks. This approach addresses the main trust challenges in the standard SSI triangle as sketched in figure 1:

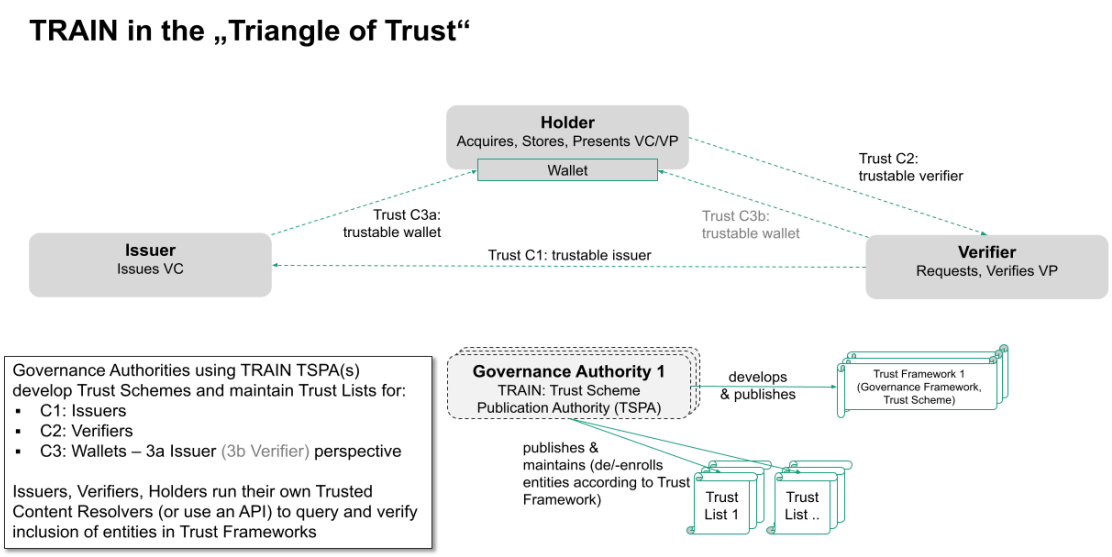

Figure 1 TRAIN in the "Triangle of Trust"

A flexible trust management infrastructure can address the trust challenges as mentioned above. An example for Challenge C1: Trusted issuers is given in figure 2. This approach leverages the well-established global Domain Name Service (DNS and DNSSEC) and combines it with the decentralized Gaia-X SSI approach. To publish and identify the correct trust lists as well as establish a chain of trust, the widely accepted DNS is leveraged.

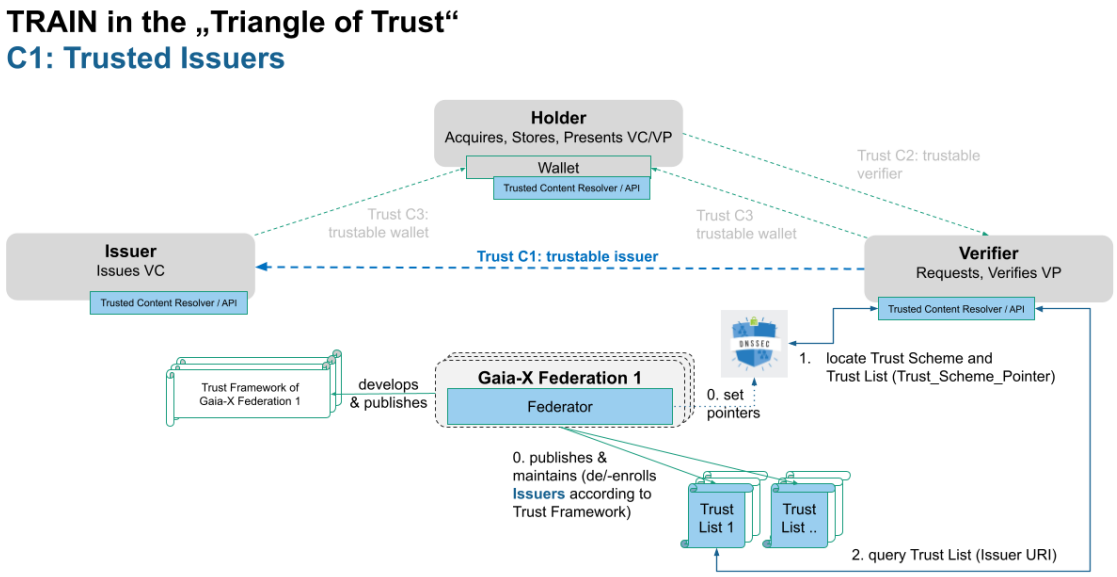

Figure 2 TRAIN in the "Triangle of Trust" – Trusted Issuers

This Trust Management Infrastructure concept is based on the use of Trust Lists for trusted entities. Trust Lists might not be optimal for all use cases and at all levels to ensure trust. This is why the

Chained Credentials Concept[1] is regarded as complementary to the Trust List approach, that is in the focus of this document.

3 Vision

The TRAIN (Trust Management Infrastructure) for Gaia-X will be used to publish lists of trusted entities that are enrolled by a trustable authority. An example could be a specific Gaia-X Federation enrolling its member companies in a member trust list. In the following TRAIN will be abbreviated if this Infrastructure is used.

TRAIN will allow individual entities (e.g., individual companies, federations that are Gaia-X accredited, federations without Gaia-X accreditation) to make trust statements to support individual trust decisions by sovereign entities. At the same time, depending on individual preference, trust decisions can also be delegated between entities.
As an example, companies can decide to trust all enrolled members of a certain (parallel acting) federation. Federations can also link their trust framework to the trust framework of a different federation. To enable this, authorities like the Gaia-X AISBL and individual Gaia-X Federation operators will act as governance authorities that operate trust frameworks and enroll trustable entities in their trust lists.

TRAIN makes use of the DNS(DNSSEC) as a fundamental and well-established anchor to discover and validate trust. In order for an entity to be able to set up a trust list, it has to control a DNS domain to create a Trust Framework (Trust Scheme) in its DNS record and to set pointers to the Trusted Content, specifically the Trust List, in its DNS record. The DNS hostname is then embedded into the meta section (TermsOfUse) of verifiable credentials by entities claiming enrollment in the Trust Framework of a specific Trust Framework operator. Verifying entities use the DNS hostname to resolve trusted content and validate the inclusion of entities in Trust Frameworks - according to their trust requirements, as they can define which Trust Frameworks (via their DNS hostnames) to trust.

For setting up a trust list and enrolling members, the respective Gaia-X Federation performs the following steps[2]:

1. The federation requires a fully qualified domain name (FQDN). This domain name has to be configured using the “Well Known DID” configuration[3] which gives the ability for a DID controller to prove they are the same entity that controls an origin.
2. The DID used for the Well Known DID configuration is published in the DNS URI Resource Record of the domain - it serves as a pointer to resolve the location and key material for the trust list.

[1] As discussed in ToIP:
https://wiki.trustoverip.org/display/HOME/ToIP+Trust+Registry+Protocol+Specification#ToIPTrustRegistryProtocolSpecification-CredentialChaining

[2] For the sake of clarity, some, mainly technical steps have been abbreviated here. They are included in the sequence diagram below.

[3] https://identity.foundation/.well-known/resources/did-configuration/

3. A trust list in JSON format[4] is created.
4. The trust list is published on a Trust List Data store (a web server or the IPFS - depending on the specific requirements).
5. The DIDs of specific member organizations that comply with the requirements of the Trust Framework of this Gaia-X Federation to the federation member are added to that trust list.
6. A Verifiable Credential (VC) with the Location of the Trust List in the credential subject is created.
7. The location of this VC is included as a Service Endpoint in the DID Document for the DID that was associated with the DNS domain.
8. DID document is published (on a web server or ledger - depending on the specific requirements).

The organizational, regulatory/legal, and technical measures to assert trust-relevant aspects for enrollment of companies are defined in the Trust Framework for this Gaia-X federation. Publishing trust lists, setting pointers to trust lists, enrollment, discovery as well as querying of trust lists will be supported by respective components as described in this concept.

Although the TRAIN infrastructure uses the DNS for lookups, the trust frameworks, (optional JSON schemas) and trust lists are distributed on the web (or in the IPFS) and are not stored in the DNS. There can be different instances of trust lists and trust frameworks hosted by different trust framework operators (institutions providing trust frameworks, for example: a Gaia-X Federation operating a Trust Framework for its members. The verifying entity alone can decide which existing trust frameworks and trust lists (for example: the trust framework of Catena-X) to trust.

The overall Vision for TRAIN, over different layers, is described in figure 3.

[4] TRAIN also supports Trust Lists in the Format XML, ETSI TS 119 612 that is used for eIDAS (1.0) Trust Schemes, i.e. https://tl.bundesnetzagentur.de/TL-DE.xml. However, for this document we will focus on trust lists in JSON format resolved via DID / VC.

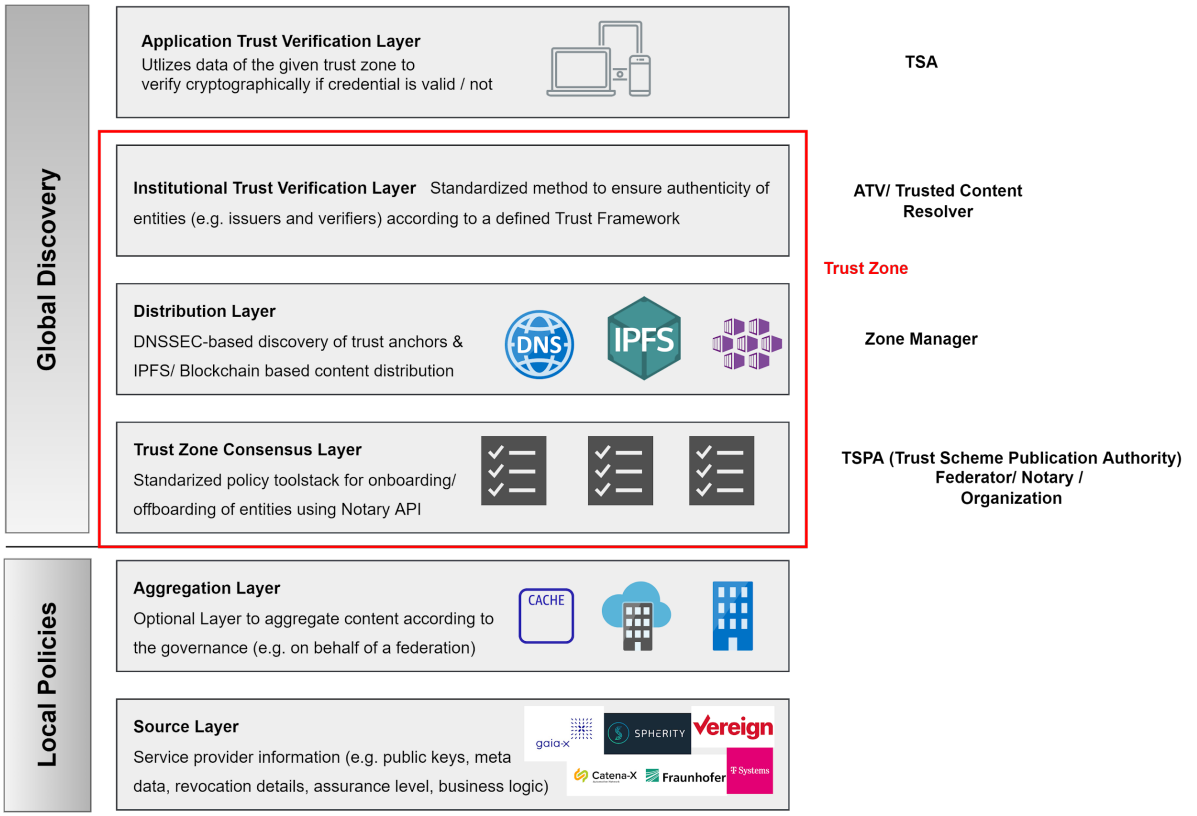

Figure 3 Overall Vision for TRAIN

Any Gaia-X self-sovereign federation controlling a DNS can create their own trust framework and become a trust framework operator e.g., *federation1.com*. Every entity that has to perform trust decisions decides which trust framework operators to trust for which context. Trust framework operators (or delegated Gaia-X Notaries) perform the onboarding/ offboarding of members in the trust framework. An example could be that these companies are members of Federation1 and therefore are trusted to issue VCs of a certain type (e.g., membership credentials) with a certain schema.

The entity operating the trust framework enrolls the members of its trust framework in a trust list. But it can also cross-reference to other trust frameworks. An example could be that a particular trust framework, e.g., *federation1.com*, with trust framework "*example*" may also trust a second trust framework e.g., *"partners"*, of another trust framework operator, e.g., *federation2.de*. It may wish to include the members of this other trust framework as being equivalent to its own members, but avoid having to enroll each of these members to its own trust list. The trust framework operator would therefore add pointer resource records (PTR RRs) to its DNS trust framework entry (as described in detail below) to point to these other equivalent trust frameworks. The use of PTR RRs forms mappings between trust frameworks and trust lists and enables cross-referencing of trust frameworks without individually enrolling entities into trust lists.

4 Assumptions & Side Conditions

The trust management infrastructure makes use of the existing global Domain Name Service (DNS) for discovering information relevant for the validation of trust as described in the concept below. As a

distributed database both in terms of organization of data as well as responsibility for operation and management, the DNS is very suitable for an infrastructure that aims to support integration and interoperation of various trust domains of different Gaia-X Federations that are operationalized through Trust Frameworks and Trust Lists.

The original design of the DNS did not consider a number of attacks allowing miscreants to alter information retrieved via the DNS. It is susceptible to cache poisoning and MITM attacks, which can lead to false results being returned. The Domain Name Service Security Extensions (DNSSEC) have been developed to mitigate this problem. They allow users of the DNS to verify that the data they received is indeed the data intended. This ability for verification is vital for the use of DNS in the context of a trust infrastructure.

Hence, the trust management infrastructure requires acceptance and availability of DNS/DNSSEC as fundamental infrastructure. To ensure an adequate level of security, the use of DNSSEC is required.

5 Concept

For a first overview of the TRAIN concept and its relationships, please refer to the following Archimate diagram. The subsequent sections will cover the main aspects of the concept.

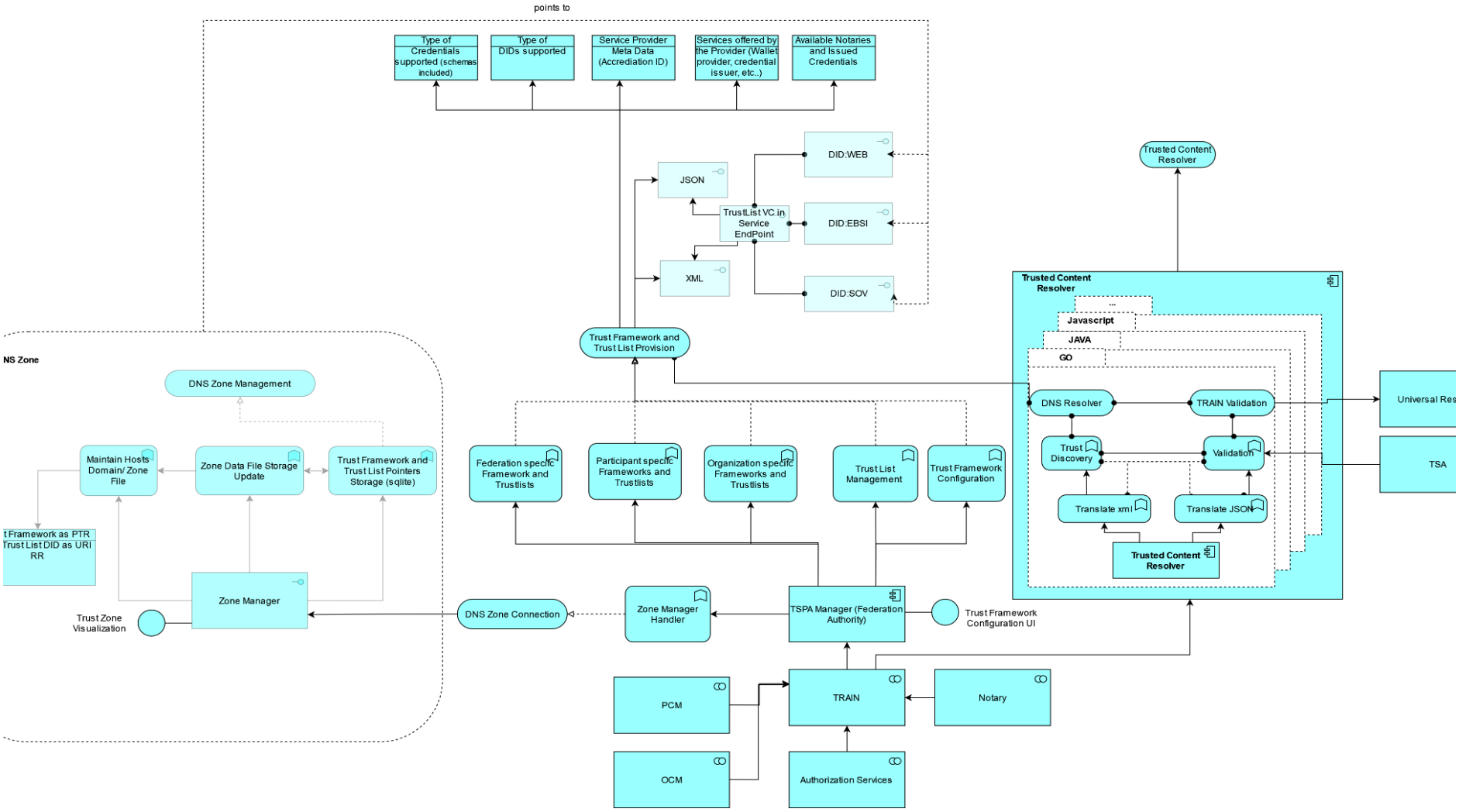

Figure 4 Overview TRAIN Concept

5.1 Role of the DNS/DNSSEC

A Gaia-X Federation controlling a DNS record can set up one or multiple Trust Frameworks with one or multiple trust lists, for example for creating a member trust list. To do this, it performs the following steps:

- The DNS controller creates a DNS entry with the name of its trust framework e.g., *example.federation1.com*., or *partners.federation2.de*..
- Then below this, two further DNS entries named *_trust* and *_scheme* respectively are created. The names of these two entries were specified by the EU Lightest project[5], and TRAIN is following those guidelines. Here, *example* is the name of the Framework, *federation1.com* is the authority responsible for the Trust Framework, and *_scheme._trust* are standardized constant terms used across the TRAIN trust infrastructure.
- The bottom entry, e.g., *_scheme._example.federation1.com*, contains one or more PTR RRs. Each PTR RR points to a DNS entry where the location of a trust list can be found, in a URI RR[6]. This use of PTR RRs allows one Trust Framework to point to several trust lists, for example, one Gaia-X Federation could point to the equivalent trust frameworks of different Gaia-X Federations. It also allows one trust list to be incorporated into multiple trust frameworks.

DNS	**Resource Records**
PTR	_scheme._example.federation1.com.
PTR	_scheme._partners.federation2.de.
URI	https://some.org/trust_list / did:web:xyz…

Table 1 DNS & Resource Records

5.2 Functional Roles and Components in TRAIN

The table below compares roles and components in TRAIN with other trust concepts currently being developed.

Description	**Term in Gaia-X**	**Term in EBSI**	**Terms in other Concepts**
Organizational authority certifying trustworthiness of entities and enrolling them into the list of trusted entities,	Trust Framework Operator: - Gaia-X AISBL - Federator of a specific Gaia-X	Trusted Accreditation Organisation (TAO)	Governance Authority, Trust Scheme Provider

[5] Wagner, S.; Kurowski, S.; Laufs, U.; Roßnagel, H.: A mechanism for discovery and verification of trust scheme memberships: the LIGHTest Reference Architecture, in Open Identity Summit 2017 - Proceedings, Lecture Notes in Informatics (LNI), Bonn: Köllen Druck + Verlag GmbH, pp. 81–92, 2017.

[6] This step is abbreviated here. Both, a URL or a DID can be used as URI to point to the trust list. In case of the DID the trust list will be resolved via a verifiable credential that is located over the DID.

maintaining the list(s)/ registrie(s) and organizational framework	Federation		
Defined organizational, regulatory/legal, and technical measures to assert trust-relevant attributes for enrolled entities (in a certain domain)	Gaia-X Trust Framework, Trust Frameworks of specific Federations	Use-case Policies	Trust Framework, Trust Scheme, Governance Framework
List of trusted entities in specific data file / format certified by a maintaining authority	Trust List (JSON or XML following ETSI TS 119 612)	Registry of Issuers (on EBSI Ledger) as Smart Contract	Trust Registry, List of Trusted Entities (Issuers etc.)
Formalized set of rules to automate trust decisions for individual transactions	(Trust) Policy (REGO)	Not defined or unknown	n/a

Table 2 Comparison: Roles and Components in TRAIN with other trust concepts

5.3 Integration with Verifiable Credentials

Every VC that is issued by an entity that claims to be in a certain Trust Framework must contain a standard Terms of Use property (according to W3C Verifiable Credentials Data Model 1.0). The Terms of Use contains the DNS names of the trust framework(s) that the issuer claims to be a member of. For this, there must at least be one "trustScheme" defined, as in the following example: `"trustScheme": ["example.federation1.com", "partners.federation2.de"].`

If schemas are also to be included in the trust framework, the credential must also contain a standard credentialSchema property listing the URL where the schema can be found, along with the syntax of the schema. As with claimed trust framework memberships, these could be true or false statements. In any case, the Verifier will check the claims using TRAIN. What counts in the end is the actual inclusion of the details into the trust list of the Trust Framework Operator as defined in the enrollment process. An example for the format of the TRAIN Terms of Use property is given below:

```
"termsOfUse": [{
    "type": "train",
    "id": "https://train.trust-scheme.de/info",
    "trustScheme":                          ["example.federation1.com",
"partners.federation2.de"]
}]
```

Optional reference to a credential schema:

```
"credentialSchema": {
    "id": "https://train.trust-scheme.de/schema/membershipCredential-schema.json",
    "type": "JsonSchemaValidator2018"
    }
```

5.4 Unified Signature & Verification Model for Trust Lists via DID and VC

The Unified Signature & Verification model for Trust List via DID and VC allows trust lists across trust domains to be signed and verified uniformly using Verifiable Credentials (VC). This is achieved by enveloping the storage location of the Trust List (Trusted Data Store, e.g., https url or IPFS) in the credential subject of a Verifiable Credential. The entity operating the trust framework (the Federator) is responsible for signing the VC with its proof.

The signature approach is as follows:

1. A *DID* is created and associated with the DNS domain under the control of the trust framework operator (the Federator) following the Well Known DID configuration approach[7].
2. The DID is stored in the *DNS PTR record URI*
3. A *DID Document* is created for the DID and stored on a ledger/IPFS/https URL resource. The DID document defines a *Service End Point* with the URI to a Verifiable Credential / Presentation
4. The *Verifiable Credential / Presentation* is created so that it can be resolved via the URI in the DID Document. The *Credential Subject of the VC/VP* contains the URI to resolve the Trust List. The VC/VP is signed so that it can be validated with the public key from the DID Document.
5. The *Trust List* is stored at the Trusted Data Store at the location (IPFS/https web resource) defined in the Credential Subject of the VC

The verification process is described in the next section.

5.5 Trust Verification

To verify the inclusion of an entity in a specific trust framework, minimum two specific inputs are required:

1. The trust framework reference (Trust Framework Pointer), that is embedded as a DNS name in the termsofUse object of the VC (see section “Trusted Content Resolving” below).
2. 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 or it could also be a UUID.

[7] https://identity.foundation/.well-known/resources/did-configuration/

The TRAIN trust verification is not restricted by the backend technology behind the VC in the respective SSI ecosystem used in Gaia-X.

If a user needs a certain service-specific information they can restrict it by adding additional parameters to the inputs. For example: If a Trust Verifier needs to process only DID requests, the user can include an input called ServiceDigitalIdentity: "DID". Thereby the verifier after verification process will return only those identities specific to the DID as output.

The trust verification is performed by a trust verification component denoted "Trusted Content Resolver" (see also the Sequence Diagram below, in TRAIN also called ATV: Automatic Trust Verifier). The registration/enrolment process is also elaborated in the respective section further below. The "TSPA/Federator" is located at the authority operating the trust framework, e.g., a specific Gaia-X Federation. The trust list is detailed further below in the respective section.

Based on the Trust Framework Pointer as DNS name in the termsOfUse, the Trusted Content Resolver will first attempt to connect to the DNS name server that holds the entries of the trust framework operator using DNSSEC. This provides an unbroken chain of trust from the root DNSKEY RR set to the Trust Framework's DNS entries. However, if DNSSEC is not available, it will use standard DNS. *The use of DNS without DNSSEC is not recommended as described in the Security Considerations below.* The reason for this is that support for DNSSEC might not be within the control of the Trust Framework Operator. If participants still prefer to use TRAIN and are willing to accept the risks, they can use TRAIN with only DNS and are not forced to wait until DNSSEC is available to them. We recognize that this leaves the trust framework open to certain attacks, such as DNS MITM and cache poisoning, but Trust Framework Operators and verifiers can perform this risk assessment before deciding to use TRAIN without DNSSEC.

The verification process is as follows:

1. The Trusted Content Resolver will read the *PTR RRs of the DNS domain* resolved from the trust framework reference (Trust Framework Pointer).
2. There the Trusted Content Resolver dereferences the *URI RRs*, and expects to find a *DID*.
3. The Well Known DID configuration verification is performed.[8]
4. From the DID the Trusted Content Resolver resolves a *DID Document* which via its *Service Endpoint* leads to a *Verifiable Credential/Verifiable Presentation*.
5. The *proof of the VC/VP* is validated against the public keys of the DID Document.
6. The *Credential Subject of the VC/VP* is ready to obtain the URI of the Trust List (at a https URL or IPFS resource).
7. The trust list is resolved and the Trusted Content Resolver checks if the specific entity is listed in the trust list. If this is the case, the Trusted Content Resolver will return that the claimed entity is a member of the trust framework operated by this "DNS name".
8. Likewise, the VC schema can be checked.

[8] https://identity.foundation/.well-known/resources/did-configuration/

Hence, it does not matter whether the entity was telling the truth when it claimed membership of a certain trust framework. The Trusted Content Resolver and the DNS controller/trust framework operator establish the root of trust.

The source code for a sample implementation of the Trusted Content Resolver component is available under Apache 2.0 (developed in the ESSIF-TRAIN Project and called ATV: Automatic Trust Verifier). The Trusted Content Resolver can be automated through policy languages (the ATV implementation supports TPL - Trust Policy Language) or other languages like REGO as foreseen for GXFS. Trusted Content Resolvers can be run by any entity, so that there can be multiple distributed copies of this service running in clouds as backup services or completely locally under sovereign control. The existing Trusted Content Resolver (ATV) implementation also offers a "TRAIN API" allowing to initiate the trust verification process using the POST API Service and to return the result to the verifier.[9]

An overview of TRAIN and the integration with GXFS is given in the Archimate Diagram in figure 5. Integration with other GXFS components is described in further details in the sections below.

5.6 Sequence Diagram: Trust List Initialization, Trust List Enrolment and Update, Trust Discovery and Validation

The sequence diagram in figure 5 summarizes what was described above and gives an overview of the central steps to:

- initially set up of a Trust List (Trust List Initialization)
- update the Trust List, e.g., to add new entities (Trust List Enrolment and Update)
- discover the correct Trust List and validate the trust (Trust Discovery and Validation)

[9] https://essif.trust-scheme.de/swagger_train/

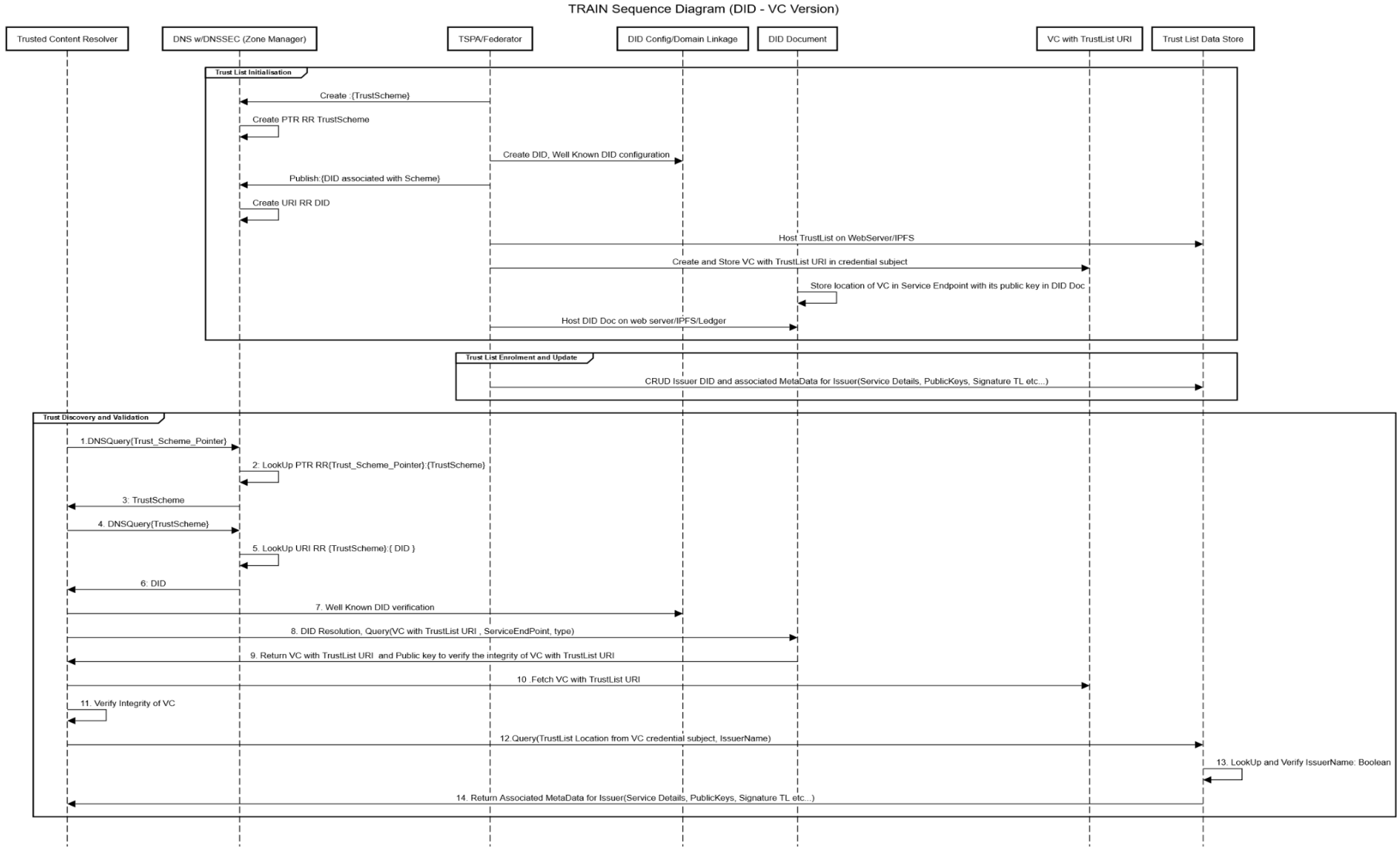

Figure 5 TRAIN Archimate Diagra

5.7 Initial Integration into Trust Framework Memberships

For an entity to be enrolled into a specific trust framework, the DID and potentially additional relevant information for the entity (see exemplary trust lists below) must be added to the Trust List of this trust framework. For this, the TSPA/Federator performs CRUD operations on the Trust List located on the Trust List Data Store.

The initial integration into Trust Framework Memberships is being triggered via the Notary. Please refer to the Section “Integration with Notary” for details.

5.8 Cross-Referencing of Trust Framework Memberships

The entities operating a Trust Framework are able to cross reference other Trust Framework Memberships using the PTR record. Hence, the DNS record of Trust Framework 1 will hold the DNS hostname pointer for Trust Framework 2 that is being trusted by Trust Framework 1. This would then imply that a verifier trusting Trust Framework 1 will automatically also trust the entities that are enrolled in Trust Framework 2. This way, Trust Framework 1 will not have to individually enroll all entities enrolled in Trust Framework 2 but can simply cross-reference to the other framework. An example is given by the figure 6 and table 3.

Moreover, during Verifiable Credential issuance, entities can include multiple Trust Framework membership pointers in the termsOfUse (e.g., `"trustScheme": [“example.federation1.com”, “partners.federation2.de”]`) to claim memberships in multiple trust frameworks.

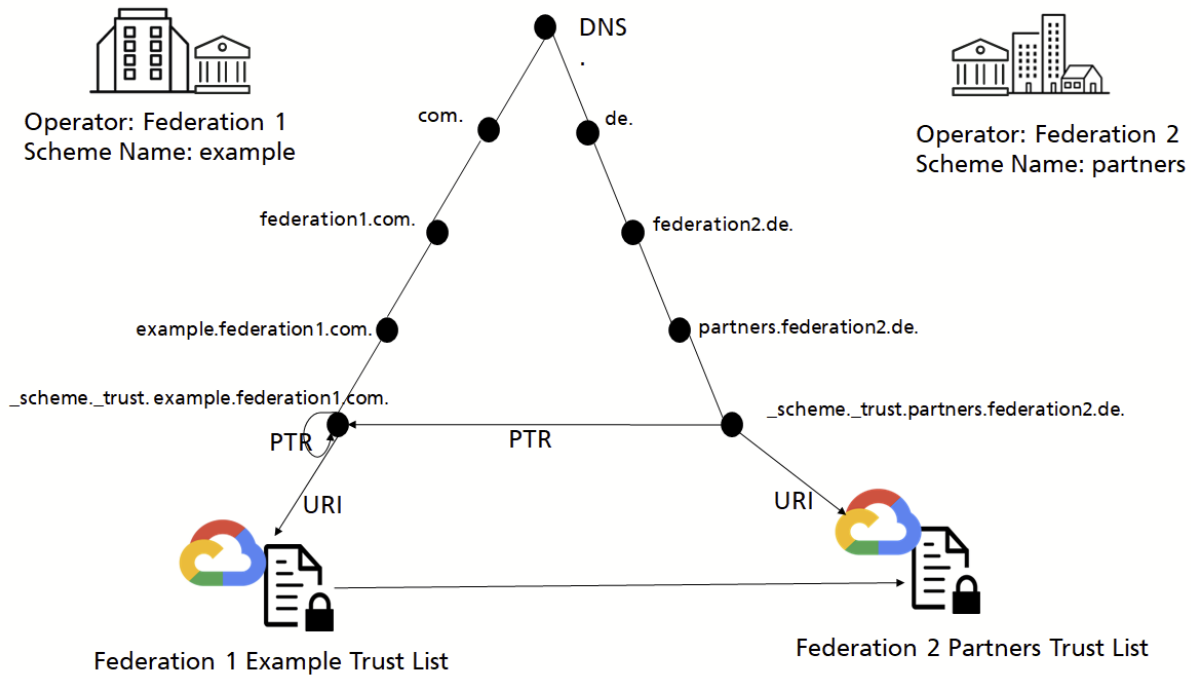

Figure 6 Cross-Referencing of Trust Framework Memberships

DNS	Resource Records
PTR	_scheme._example.federation1.com.
PTR	_scheme._partners.federation2.de.
URI	https://some.org/trust_list / did:web:xyz…

Table 3 Cross-Referencing of Trust Framework Memberships: DNS and Resource Records

5.9 Integration into a New Trust Framework with existing Credentials

Using TRAIN, the enrollment of an entity into a new Trust Framework is immediately reflected and does not require an update of already issued credentials. This can be achieved by leveraging the PTR record cross-referencing of Trust Frameworks as explained above to enroll into a new Trust Framework.

This could be illustrated as follows:

1. An exemplary "Federation X" maintains a trust list of members for the Trust Framework "Members Federation X" and gives out VCs. In their terms of use, these VCs include the DNS hostname pointer `"trustScheme": ["members.federationX.com"]` to claim membership in the Trust Framework "Members Federation X".
2. Federation X is not a member of the Trust Framework of the "Example-Dataspace" (with the Trust Framework identified by the DNS hostname `accredited.exampleDataspace.com`) as it has not been accredited.
3. A validating entity that has configured their Trusted Content Resolver to trust VCs issued under the Trust Framework `members.federationX.com` will be able to validate these credentials as trustworthy. However, if a validating entity has configured their Trusted Content Resolver to only trust VCs issued under the Trust Framework `accredited.exampleDataspace.com`, it will not be able to validate these credentials as trustworthy.
4. Now, Federation X gets accredited according to the Trust Framework of Example-Dataspace. Example-Dataspace will therefore add a PTR record pointer to `members.federationX.com` right into their DNS under `accredited.exampleDataspace.com` to reference the Trust Framework of Federation X as trustworthy.
5. A validating entity that receives the DNS hostname pointer `"trustScheme": ["members.federationX.com"]` that has configured their Trusted Content Resolver to trust VCs issued under the Trust Framework `accredited.exampleDataspace.com` will now be able to follow the PTR record pointer to `members.federationX.com` under the PTR record of `accredited.exampleDataspace.com` and validate these credentials as trustworthy - without any changes in the initially issued credentials.

5.10 Integration with TSA

The Trust Services API (TSA) can integrate the Trusted Component Resolver Libraries to verify the institutional trust of the verifiable credentials.

5.11 Integration with OCM

The Organization Credential Manager (OCM) can use the TSA to validate the trust of the organizational verifiable credentials (via the Trusted Component Resolver Libraries) before storing them in the wallet.

5.12 Integration with Notary

The Notary uses the TSPA Connector to enroll trusted entities into the trust framework and add them via the TSPA/Federator to the Trust List.

The integration with the Notary is illustrated in figure 7:

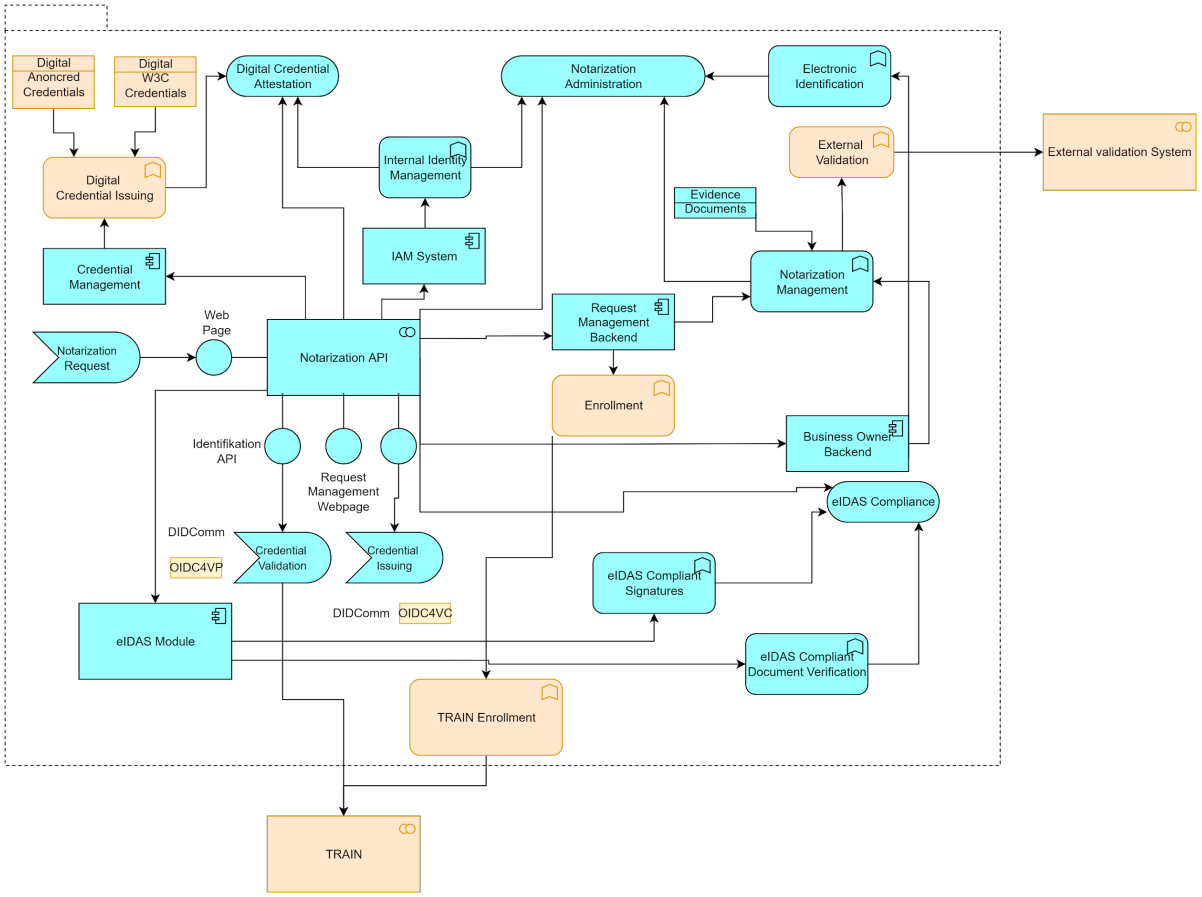

Figure 7 TRAIN integration with the Notary

5.13 Required Trust Lists for Gaia-X

Certain trust aspects will be covered through the use of chained credentials. For others, trust lists are more efficient. Hence, the following trust lists are foreseen:

- **One Gaia-X Federations Trust List** (one single Trust List *operated by Gaia-X AISBL* for the Gaia-X Federations that are conformant to the general Gaia-X Trust Framework)

- **Trust List of Notaries operated by Gaia-X AISBL** (one single Trust List *operated by Gaia-X AISBL for the Notaries* that are conformant to the general Gaia-X Trust Framework)
- **Multiple Federation Participants Trust Lists** (one Trust List *operated by each Federation*, listing the participants of this Federation that are conformant to its Trust Framework)
- **Multiple Trust Lists of Notaries operated by Federations** (one Trust List *operated by each Federation*, listing the Notaries that are trusted by each Federation and their services offered and credentials issued)
- **Multiple Participant Trust Lists** (one Trust List *operated by each Participant*, listing the services offered and credentials issued by each participant)
- **Multiple Participant Notaries Trust Lists** (one Trust List *operated by each Participant*, listing the Notaries that are trusted by each Participant and their services offered and credentials issued)

Further Trust Lists for additional entities or application scenarios are possible.

5.14 Trust List Formats

Trust Lists used by TRAIN contain all the enrolled entities (e.g., Members of a Gaia-X Federation) in a specific data file/format certified by the Trust Framework authority (e.g., the respective Gaia-X Federation operating the Trust Framework). Trust lists for Gaia-X are referenced from a VC (the location is embedded into the credential subject) and the content can be in JSON-LD or in XML-Format. An exemplary trust list in XML Format (following the ETSI TS 119 612 standard, a JSON example is shown after this) is given in the following:

```
<TrustServiceStatusList                                          xmlns="http://uri.etsi.org/02231/v2#"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#"             xmlns:ns3="http://uri.etsi.org/01903/v1.3.2#"
xmlns:ns4="http://uri.etsi.org/02231/v2/additionaltypes#"
xmlns:ns5="http://uri.etsi.org/TrstSvc/SvcInfoExt/eSigDir-1999-93-EC-TrustedList/#"
xmlns:ns6="http://uri.etsi.org/01903/v1.4.1#" TSLTag="http://uri.etsi.org/19612/TSLTag">
     <SchemeInformation>
              <TSLVersionIdentifier>5</TSLVersionIdentifier>
              <TSLSequenceNumber>1</TSLSequenceNumber>
              <TSLType>http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUgeneric</TSLType>
              <SchemeOperatorName>
                       <Name xml:lang="en">Federation 1 Notary</Name>
              </SchemeOperatorName>
              <SchemeOperatorAddress>
                       <PostalAddresses>
                                <PostalAddress xml:lang="en">
                                         <StreetAddress>Lichtstraße 43h</StreetAddress>
                                         <Locality>Köln</Locality>
                                         <PostalCode>50825</PostalCode>
                                         <CountryName>DE</CountryName>
                                </PostalAddress>
                       </PostalAddresses>
                       <ElectronicAddress>
                                <URI xml:lang="en">mailto:mail@federation1.com</URI>
                                <URI xml:lang="en">https://www.federation1.com</URI>
                       </ElectronicAddress>
              </SchemeOperatorAddress>
              <SchemeName>
                       <Name xml:lang="en">DE:TRAIN</Name>
              </SchemeName>
              <SchemeInformationURI>
                       <URI xml:lang="en">https://dl.gi.de/handle/20.500.12116/38702</URI>
              </SchemeInformationURI>

     <StatusDeterminationApproach>http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EUappropriate
</StatusDeterminationApproach>
              <SchemeTypeCommunityRules>
```

```
                        <URI                                    xml:lang="en">https://train.trustscheme.de
/schemerules/ngi.train.trustscheme.de </URI>
                </SchemeTypeCommunityRules>
                <SchemeTerritory>GLOBAL</SchemeTerritory>
                <PolicyOrLegalNotice>
                        <TSLLegalNotice xml:lang="en">This is an experimental list for the GXFS Federation
Notary.</TSLLegalNotice>
                </PolicyOrLegalNotice>
                <HistoricalInformationPeriod>65535</HistoricalInformationPeriod>
                <ListIssueDateTime>2022-09-27T00:00:00Z</ListIssueDateTime>
                <NextUpdate>2022-12-27T00:00:00Z</NextUpdate>
        </SchemeInformation>
        <TrustServiceProviderList>
                <TrustServiceProvider>
                        <UID>
                                <Name xml:lang="en">2325</Name>
                        </UID>
                        <TSPCurrentStatus>
                                <Name xml:lang="en">Active</Name>
                        </TSPCurrentStatus>
                        <StatusStartingTime>
                                <dateTime>2022-11-22T00:00:00Z</dateTime>
                        </StatusStartingTime>
                        <TSPInformation>
                                <TSPName>
                                        <Name xml:lang="en">Notary 1</Name>
                                </TSPName>
                                <TSPTradeName>
                                        <Name xml:lang="en">NTRUK-SC090312</Name>
                                        <Name xml:lang="en">Notary Federation 1 </Name>
                                </TSPTradeName>
                                <TSPAddress>
                                        <PostalAddresses>
                                                <PostalAddress xml:lang="en">
                                                        <StreetAddress>Lichtstraße 43h</StreetAddress>
                                                        <Locality>Köln</Locality>
                                                        <PostalCode>50825</PostalCode>
                                                        <CountryName>DE</CountryName>
                                                </PostalAddress>
                                        </PostalAddresses>
                                        <ElectronicAddress>
                                                <URI
xml:lang="en">mailto:mail.notary1@federation.com</URI>
                                        </ElectronicAddress>
                                </TSPAddress>
                                <TSPInformationURI>
                                        <URI xml:lang="en">https://notary1.info/TRAIN/info</URI>
                                </TSPInformationURI>
                                <TSPCertificationList>
                                        <TSPCertification xml:lang="en">
                                                <Type>LEI</Type>
                                                <Value>1234567</Value>
                                                <Scope></Scope>
                                        </TSPCertification>
                                        <TSPCertification xml:lang="en">
                                                <Type>Gaia-X Compliance</Type>
                                                <Value>1234567</Value>
                                                <Scope></Scope>
                                        </TSPCertification>
                                        <TSPCertification xml:lang="en">
                                                <Type>eidas</Type>
                                                <Value>1234567</Value>
                                                <Scope></Scope>
                                        </TSPCertification>
                                </TSPCertificationList>
                        </TSPInformation>
                        <TSPServices>
                                <TSPService>
                                        <ServiceInformation>

        <ServiceTypeIdentifier>https://participant.membership.notary1.federation.com</ServiceTypeIdentifie
r>
                                                <ServiceName>
                                                        <Name    xml:lang="en">Federation    Participant
Membership Credential</Name>
                                                </ServiceName>
```

```
                                        <ServiceDigitalIdentity>

    <x509>242364735r6347856348573489573495873954739573957395739324587 43rz3ufgf3hrfv3hfv3hfv3hfv3hf</x5
09>
                                                <did>did:web:notary.federation1.com</did>
                                        </ServiceDigitalIdentity>

    <ServiceStatus>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</ServiceStatus>
                                        <StatusStartingTime>2022-09-
29T22:00:00Z</StatusStartingTime>
                                        <ServiceSupplyPoints>

    <ServiceSupplyPoint>https://participant.membership.notary1.federation.com</ServiceSupplyPoint>
                                        </ServiceSupplyPoints>
                                        <TSPServiceDefinitionURI>
                                                <URI>https://notary1.info/schema/V-2022-
1/participant_membership.json</URI>
                                        </TSPServiceDefinitionURI>
                                        <AdditionalServiceInformation>
                                                <ServiceCredentialTypes>
                                                        <CredentialType>X.509</CredentialType>

    <CredentialType>did:web</CredentialType>
                                                </ServiceCredentialTypes>
                                                <ServiceGovernanceURI>https://eur-
lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953</ServiceGovernanceURI>
                                                <ServiceBusinessRules>https://eur-
lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953</ServiceBusinessRules>
                                        </AdditionalServiceInformation>
                                </ServiceInformation>
                        </TSPService>
                        <TSPService>
                                <ServiceInformation>

    <ServiceTypeIdentifier>https://principal.membership.notary1.federation.com</ServiceTypeIdentifier>
                                        <ServiceName>
                                                <Name     xml:lang="en">Federation     Principal
Credential</Name>
                                        </ServiceName>
                                        <ServiceDigitalIdentity>

    <x509>242364735r6347856348573489573495873954739573957395739324587 43rz3ufgf3hrfv3hfv3hfv3hfv3hf</x5
09>
                                                <did>did:web:notary.federation1.com</did>
                                        </ServiceDigitalIdentity>

    <ServiceStatus>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</ServiceStatus>
                                        <StatusStartingTime>2022-09-
29T22:00:00Z</StatusStartingTime>
                                        <ServiceSupplyPoints>

    <ServiceSupplyPoint>https://verifier.research.identiproof.io/</ServiceSupplyPoint>
                                        </ServiceSupplyPoints>
                                        <TSPServiceDefinitionURI>
                                                <URI>https://notary1.info/schema/V-2022-
1/participant_membership.json</URI>
                                        </TSPServiceDefinitionURI>
                                        <AdditionalServiceInformation>
                                                <ServiceCredentialTypes>
                                                        <CredentialType>X.509</CredentialType>

    <CredentialType>did:web</CredentialType>
                                                </ServiceCredentialTypes>
                                                <ServiceGovernanceURI>https://eur-
lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953</ServiceGovernanceURI>
                                                <ServiceBusinessRules>https://eur-
lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953</ServiceBusinessRules>
                                        </AdditionalServiceInformation>
                                </ServiceInformation>
                        </TSPService>
                        <TSPService>
                                <ServiceInformation>

    <ServiceTypeIdentifier>https://consumer.membership.notary1.federation.com</ServiceTypeIdentifier>
                                        <ServiceName>
```

```
                                                        <Name     xml:lang="en">Federation     Consumer
Credential</Name>
                                                </ServiceName>
                                                <ServiceDigitalIdentity>

     <x509>242364735r6347856348573489573495873954739573957395739573932458743rz3ufgf3hrfv3hfv3hfv3hfv3hf</x5
09>
                                                        <did>did:web:notary.federation1.com</did>
                                                </ServiceDigitalIdentity>

     <ServiceStatus>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</ServiceStatus>
                                                <StatusStartingTime>2022-09-
29T22:00:00Z</StatusStartingTime>
                                                <ServiceSupplyPoints>

     <ServiceSupplyPoint>https://verifier.research.identiproof.io/</ServiceSupplyPoint>
                                                </ServiceSupplyPoints>
                                                <TSPServiceDefinitionURI>
                                                        <URI>https://notary1.info/schema/V-2022-
1/participant_membership.json</URI>
                                                </TSPServiceDefinitionURI>
                                                <AdditionalServiceInformation>
                                                        <ServiceCredentialTypes>
                                                                <CredentialType>X.509</CredentialType>

     <CredentialType>did:web</CredentialType>
                                                        </ServiceCredentialTypes>
                                                        <ServiceGovernanceURI>https://eur-
lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953</ServiceGovernanceURI>
                                                        <ServiceBusinessRules>https://eur-
lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953</ServiceBusinessRules>
                                                </AdditionalServiceInformation>
                                        </ServiceInformation>
                                </TSPService>
                                <TSPService>
                                        <ServiceInformation>

     <ServiceTypeIdentifier>https://resource.membership.notary1.federation.com</ServiceTypeIdentifier>
                                                <ServiceName>
                                                        <Name     xml:lang="en">Federation     Resource
Credential</Name>
                                                </ServiceName>
                                                <ServiceDigitalIdentity>

     <x509>242364735r6347856348573489573495873954739573957395739573932458743rz3ufgf3hrfv3hfv3hfv3hfv3hf</x5
09>
                                                        <did>did:web:notary.federation1.com</did>
                                                </ServiceDigitalIdentity>

     <ServiceStatus>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</ServiceStatus>
                                                <StatusStartingTime>2022-09-
29T22:00:00Z</StatusStartingTime>
                                                <ServiceSupplyPoints>

     <ServiceSupplyPoint>https://resource.membership.notary1.federation.com</ServiceSupplyPoint>
                                                </ServiceSupplyPoints>
                                                <TSPServiceDefinitionURI>
                                                        <URI>https://notary1.info/schema/V-2022-
1/participant_membership.json</URI>
                                                </TSPServiceDefinitionURI>
                                                <AdditionalServiceInformation>
                                                        <ServiceCredentialTypes>
                                                                <CredentialType>X.509</CredentialType>

     <CredentialType>did:web</CredentialType>
                                                        </ServiceCredentialTypes>
                                                        <ServiceGovernanceURI>https://eur-
lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953</ServiceGovernanceURI>
                                                        <ServiceBusinessRules>https://eur-
lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953</ServiceBusinessRules>
                                                </AdditionalServiceInformation>
                                        </ServiceInformation>
                                </TSPService>
                                <TSPService>
                                        <ServiceInformation>
```

```
        <ServiceTypeIdentifier>https://onboarding.membership.notary1.federation.com</ServiceTypeIdentifier
    >
                                                    <ServiceName>
                                                            <Name    xml:lang="en">Federation    Onboarding
    Credential</Name>
                                                    </ServiceName>
                                                    <ServiceDigitalIdentity>

        <x509>242364735r6347856348573489573495873954739573957395739573932458743rz3ufgf3hrfv3hfv3hfv3hfv3hf</x5
    09>
                                                            <did>did:web:notary.federation1.com</did>
                                                    </ServiceDigitalIdentity>

        <ServiceStatus>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</ServiceStatus>
                                                    <StatusStartingTime>2022-09-
    29T22:00:00Z</StatusStartingTime>
                                                    <ServiceSupplyPoints>

        <ServiceSupplyPoint>https://onboarding.membership.notary1.federation.com</ServiceSupplyPoint>
                                                    </ServiceSupplyPoints>
                                                    <TSPServiceDefinitionURI>
                                                            <URI>https://notary1.info/schema/V-2022-
    1/participant_membership.json</URI>
                                                    </TSPServiceDefinitionURI>
                                                    <AdditionalServiceInformation>
                                                            <ServiceCredentialTypes>
                                                                    <CredentialType>X.509</CredentialType>

        <CredentialType>did:web</CredentialType>
                                                            </ServiceCredentialTypes>
                                                            <ServiceGovernanceURI>https://eur-
    lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953</ServiceGovernanceURI>
                                                            <ServiceBusinessRules>https://eur-
    lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953</ServiceBusinessRules>
                                                    </AdditionalServiceInformation>

                                            </ServiceInformation>
                                    </TSPService>
                            </TSPServices>
                    </TrustServiceProvider>
        </TrustServiceProviderList>
    </TrustServiceStatusList>
```

The details of every entity enrolled in the trust list are described under the attribute *<TrustServiceProvider>.* The ID of the entity is under the attribute *<IssuerName>.*

Each entity in the trust list can have 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 entity is trusted to issue. This trust list also offers the flexibility to the service provider to add different services with different schemas.

An example for a trust list in JSON format would look as follows:

```
{
 "TrustServiceStatusList": {
  "SchemeInformation": {
   "HistoricalInformationPeriod": "65535",
   "ListIssueDateTime": "2022-09-27T00:00:00Z",
   "NextUpdate": "2022-12-27T00:00:00Z",
   "PolicyOrLegalNotice": {
    "TSLLegalNotice": {
     "#text": "This is an experimental list for the GXFS Federation Notary.",
     "@xml:lang": "en"
```

```
  }
 },
 "SchemeInformationURI": {
  "URI": {
   "#text": "https://dl.gi.de/handle/20.500.12116/38702",
   "@xml:lang": "en"
  }
 },
 "SchemeName": {
  "Name": {
   "#text": "DE:TRAIN",
   "@xml:lang": "en"
  }
 },
 "SchemeOperatorAddress": {
  "ElectronicAddress": {
   "URI": [
    {
     "#text": "mailto:mail@federation1.com",
     "@xml:lang": "en"
    },
    {
     "#text": "https://www.federation1.com",
     "@xml:lang": "en"
    }
   ]
  },
  "PostalAddresses": {
   "PostalAddress": {
    "@xml:lang": "en",
    "CountryName": "DE",
    "Locality": "K\u00f6ln",
    "PostalCode": "50825",
    "StreetAddress": "Lichtstra\u00dfe 43h"
   }
  }
 },
 "SchemeOperatorName": {
  "Name": {
   "#text": "Federation 1 Notary",
   "@xml:lang": "en"
  }
 },
 "SchemeTerritory": "GLOBAL",
 "SchemeTypeCommunityRules": {
  "URI": {
   "#text": "https://train.trustscheme.de /schemerules/ngi.train.trustscheme.de",
   "@xml:lang": "en"
  }
 },
 "StatusDeterminationApproach": "http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EUappropriate",
 "TSLSequenceNumber": "1",
 "TSLType": "http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUgeneric",
 "TSLVersionIdentifier": "5"
```

```
  },
  "TrustServiceProviderList": {
   "TrustServiceProvider": {
    "StatusStartingTime": {
     "dateTime": "2022-11-22T00:00:00Z"
    },
    "TSPCurrentStatus": {
     "Name": {
      "#text": "Active",
      "@xml:lang": "en"
     }
    },
    "TSPInformation": {
     "TSPAddress": {
      "ElectronicAddress": {
       "URI": {
        "#text": "mailto:mail.notary1@federation.com",
        "@xml:lang": "en"
       }
      },
      "PostalAddresses": {
       "PostalAddress": {
        "@xml:lang": "en",
        "CountryName": "DE",
        "Locality": "K\u00f6ln",
        "PostalCode": "50825",
        "StreetAddress": "Lichtstra\u00dfe 43h"
       }
      }
     },
     "TSPCertificationList": {
      "TSPCertification": [
       {
        "@xml:lang": "en",
        "Scope": null,
        "Type": "LEI",
        "Value": "1234567"
       },
       {
        "@xml:lang": "en",
        "Scope": null,
        "Type": "Gaia-X Compliance",
        "Value": "1234567"
       },
       {
        "@xml:lang": "en",
        "Scope": null,
        "Type": "eidas",
        "Value": "1234567"
       }
      ]
     },
     "TSPInformationURI": {
      "URI": {
```

```
      "#text": "https://notary1.info/TRAIN/info",
      "@xml:lang": "en"
     }
    },
    "TSPName": {
     "Name": {
      "#text": "Notary 1",
      "@xml:lang": "en"
     }
    },
    "TSPTradeName": {
     "Name": [
      {
       "#text": "NTRUK-SC090312",
       "@xml:lang": "en"
      },
      {
       "#text": "Notary Federation 1",
       "@xml:lang": "en"
      }
     ]
    }
   },
   "TSPServices": {
    "TSPService": [
     {
      "ServiceInformation": {
       "AdditionalServiceInformation": {
        "ServiceBusinessRules": "https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953",
        "ServiceCredentialTypes": {
         "CredentialType": [
          "X.509",
          "did:web"
         ]
        },
        "ServiceGovernanceURI": "https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953"
       },
       "ServiceDigitalIdentity": {
        "did": "did:web:notary.federation1.com",
        "x509": "242364735r6347856348573489573495873954739573957395739573932458743rz3ufgf3hrfv3hfv3hfv3hfv3hf"
       },
       "ServiceName": {
        "Name": {
         "#text": "Federation Participant Membership Credential",
         "@xml:lang": "en"
        }
       },
       "ServiceStatus": "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted",
       "ServiceSupplyPoints": {
        "ServiceSupplyPoint": "https://participant.membership.notary1.federation.com"
       },
       "ServiceTypeIdentifier": "https://participant.membership.notary1.federation.com",
       "StatusStartingTime": "2022-09-29T22:00:00Z",
       "TSPServiceDefinitionURI": {
```

```
      "URI": "https://notary1.info/schema/V-2022-1/participant_membership.json"
     }
    }
   },
   {
    "ServiceInformation": {
     "AdditionalServiceInformation": {
      "ServiceBusinessRules": "https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953",
      "ServiceCredentialTypes": {
       "CredentialType": [
        "X.509",
        "did:web"
       ]
      },
      "ServiceGovernanceURI": "https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953"
     },
     "ServiceDigitalIdentity": {
      "did": "did:web:notary.federation1.com",
      "x509": "242364735r6347856348573489573495873954739573957395739573932458743rz3ufgf3hrfv3hfv3hfv3hfv3hf"
     },
     "ServiceName": {
      "Name": {
       "#text": "Federation Principal Credential",
       "@xml:lang": "en"
      }
     },
     "ServiceStatus": "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted",
     "ServiceSupplyPoints": {
      "ServiceSupplyPoint": "https://verifier.research.identiproof.io/"
     },
     "ServiceTypeIdentifier": "https://principal.membership.notary1.federation.com",
     "StatusStartingTime": "2022-09-29T22:00:00Z",
     "TSPServiceDefinitionURI": {
      "URI": "https://notary1.info/schema/V-2022-1/participant_membership.json"
     }
    }
   },
   {
    "ServiceInformation": {
     "AdditionalServiceInformation": {
      "ServiceBusinessRules": "https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953",
      "ServiceCredentialTypes": {
       "CredentialType": [
        "X.509",
        "did:web"
       ]
      },
      "ServiceGovernanceURI": "https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953"
     },
     "ServiceDigitalIdentity": {
      "did": "did:web:notary.federation1.com",
      "x509": "242364735r6347856348573489573495873954739573957395739573932458743rz3ufgf3hrfv3hfv3hfv3hfv3hf"
     },
     "ServiceName": {
```

```
      "Name": {
       "#text": "Federation Consumer Credential",
       "@xml:lang": "en"
      }
     },
     "ServiceStatus": "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted",
     "ServiceSupplyPoints": {
      "ServiceSupplyPoint": "https://verifier.research.identiproof.io/"
     },
     "ServiceTypeIdentifier": "https://consumer.membership.notary1.federation.com",
     "StatusStartingTime": "2022-09-29T22:00:00Z",
     "TSPServiceDefinitionURI": {
      "URI": "https://notary1.info/schema/V-2022-1/participant_membership.json"
     }
    }
   },
   {
    "ServiceInformation": {
     "AdditionalServiceInformation": {
      "ServiceBusinessRules": "https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953",
      "ServiceCredentialTypes": {
       "CredentialType": [
        "X.509",
        "did:web"
       ]
      },
      "ServiceGovernanceURI": "https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953"
     },
     "ServiceDigitalIdentity": {
      "did": "did:web:notary.federation1.com",
      "x509": "242364735r6347856348573489573495873954739573957395739573932458743rz3ufgf3hrfv3hfv3hfv3hfv3hf"
     },
     "ServiceName": {
      "Name": {
       "#text": "Federation Resource Credential",
       "@xml:lang": "en"
      }
     },
     "ServiceStatus": "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted",
     "ServiceSupplyPoints": {
      "ServiceSupplyPoint": "https://resource.membership.notary1.federation.com"
     },
     "ServiceTypeIdentifier": "https://resource.membership.notary1.federation.com",
     "StatusStartingTime": "2022-09-29T22:00:00Z",
     "TSPServiceDefinitionURI": {
      "URI": "https://notary1.info/schema/V-2022-1/participant_membership.json"
     }
    }
   },
   {
    "ServiceInformation": {
     "AdditionalServiceInformation": {
      "ServiceBusinessRules": "https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953",
      "ServiceCredentialTypes": {
```

```
            "CredentialType": [
              "X.509",
              "did:web"
            ]
           },
           "ServiceGovernanceURI": "https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953"
          },
          "ServiceDigitalIdentity": {
           "did": "did:web:notary.federation1.com",
           "x509": "242364735r6347856348573489573495873954739573957395739573932458743rz3ufgf3hrfv3hfv3hfv3hfv3hf"
          },
          "ServiceName": {
           "Name": {
            "#text": "Federation Onboarding Credential",
            "@xml:lang": "en"
           }
          },
          "ServiceStatus": "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted",
          "ServiceSupplyPoints": {
           "ServiceSupplyPoint": "https://onboarding.membership.notary1.federation.com"
          },
          "ServiceTypeIdentifier": "https://onboarding.membership.notary1.federation.com",
          "StatusStartingTime": "2022-09-29T22:00:00Z",
          "TSPServiceDefinitionURI": {
           "URI": "https://notary1.info/schema/V-2022-1/participant_membership.json"
          }
         }
        }
       ]
      },
      "UID": {
       "Name": {
        "#text": "2325",
        "@xml:lang": "en"
       }
      }
     }
    }
   }
}
```


6 Trusted Content Handling

Trust lists and pointers to the trust lists will be summarized under the term “Trusted Content” in the following.

6.1 Trusted Content Locations

Pointers to trust frameworks will be placed as in the DNS of the Trust Framework Operators. Depending on requirements of the specific use case, trust lists can be placed on https web servers or in the IPFS. To maintain auditability and security against manipulation, it is recommended that the Trust List is published in the IPFS.

DID Documents can be placed on Ledgers, the IPFS or https web servers.
The Verifiable Credential with the Trust List URI can also be published on the different locations as mentioned.

6.2 Enrolment Process of Entities in Trust Lists

The Notarization API will cover the enrolment of entities in trust lists. The requirements that have to be fulfilled for enrolment are dependent on the Trust Framework of the respective context, i.e., the Gaia-X Trust Framework, the Trust Framework of a certain Federation, etc. The technical process is triggered by the notary and executed by the TSPA/Federator performing CRUD operations on the trust list that is located on the Trusted Data Store.

6.3 Trusted Content Resolving

Resolving trusted content via trust list involves trust discovery and trust validation processes. In order to resolve the trusted content, the following data model is to be followed:

{
"IssuerDetails": "did:web:company.de"
"Trust Framework Pointer": ["federation1.com", "gaia-x.eu"],
"ServiceContentType": "gx-trust-list-issuer"
}

The term:

- *"IssuerDetails"* describes the DID or URI of the issuer credential
- *"Trust Framework Pointer"* describes the trust frameworks mentioned in the termsofUse of the verifiable credential
- *"ServiceContentType"* is set by the Resolver to resolve the corresponding trust list. For example: gx-type-list-issuer contains the information of a trusted issuer trust list but if the resolver needs information regarding schema then it can point to "gx-trust-list-schemas". The following are minimum set of trusted content service types for TRAIN in Gaia-X:
    - gx-trust-list-issuer (format: Verifiable credentials, JSON)
    - gx-trust-list-schemas
    - gx-trust-list-policies
    - gx-trust-list-apps
    - gx-trust-list-verifier
    - gx-trust-list-authorities

It is foreseen that a further analysis of the specific requirements of the concrete use cases is performed. This analysis will define if a specific type is needed and/or if further types will have to be added, as well as the specific format and content of the types.

Please refer to the sections "Trust Verification" and "Unified Signature & Verification Model for Trust Lists via DID and VC" which describe in detail the discovery process of the trust list and the step-by-step validation.

6.4 Trusted Content Auditing

Depending on the requirements for auditability, different procedures are recommended for the anchoring of trusted content:

Requirement	Procedure
Trusted Content must be auditible up to Enrollment	Anchor all items into an audible, tamper-proof system (e.g., IPFS, Ledgers)
Trusted Content Creator must be audible	Anchor the DID in the DNS Zones (default)
Trusted Content Location must be anchored	Anchor the URL in the DNS Zones

Table 4 Procedures for auditability requirements

Other options remain possible.

6.5 Setup Process for Trust Verification

An entity performing trust verification, i.e., to check whether a certain company is indeed a member of the specific Gaia-X Trust Framework that it claims to be, the entity has to configure the DNS names of the trust frameworks that it trusts in the Trusted Content Resolver [10]. So, if it would choose to trust the Trust Framework "Example" of the Gaia-X Federation "Federation1" it would configure the Trusted Content Resolver for "*example.federation1.com*." And if it also trusts the Trust Framework "Partners" of "Federation2" it would also add "*partners.federation2.de."*

Additionally, the Trusted Content resolver can also configure what type of trust lists needs to be resolved, as different types of trust lists can be configured in the DID Document using service type. Examples are: *gx-trust-list-issuer*, *gx-trust-list-verifier*, *gx-trust-list-schemas*, *gx-trust-list-apps*, *gx-trust-list-authorities*.

When the verifying entity receives a VC, it extracts the asserted trust framework claims made by the issuer in the Terms of Use property. If it trusts any of the claimed trust frameworks, it calls the Trusted Content Resolver, passing it the URI of the issuer (taken from the VC, e.g., "*did:example:123456789abcdefghi*") and the DNS name of the trusted trust framework that the VC Issuer purports to be a member of (e.g., "Trust_Scheme_Pointer": "*example.federation1.com*").

The Trusted Content Resolver will then check if the VC issuer is a member of any of the trust lists pointed to by this trust framework, and if so, return the Service Type URL to the Verifier. The verifier can check that this URL is identical to the one in the credentialSchema property, and if it is, use the schema contained at this URL to validate that the attributes in the received VC match the schema for this Service Type.

[10] If an API is used, the URL(s) of the TRAIN API(s) to call to verify the membership lists have to be set up as well.

6.6 Packages for Programming Languages

The Trusted Content Resolver will be developed for the following programming languages:

- Java
- Javascript
- Go

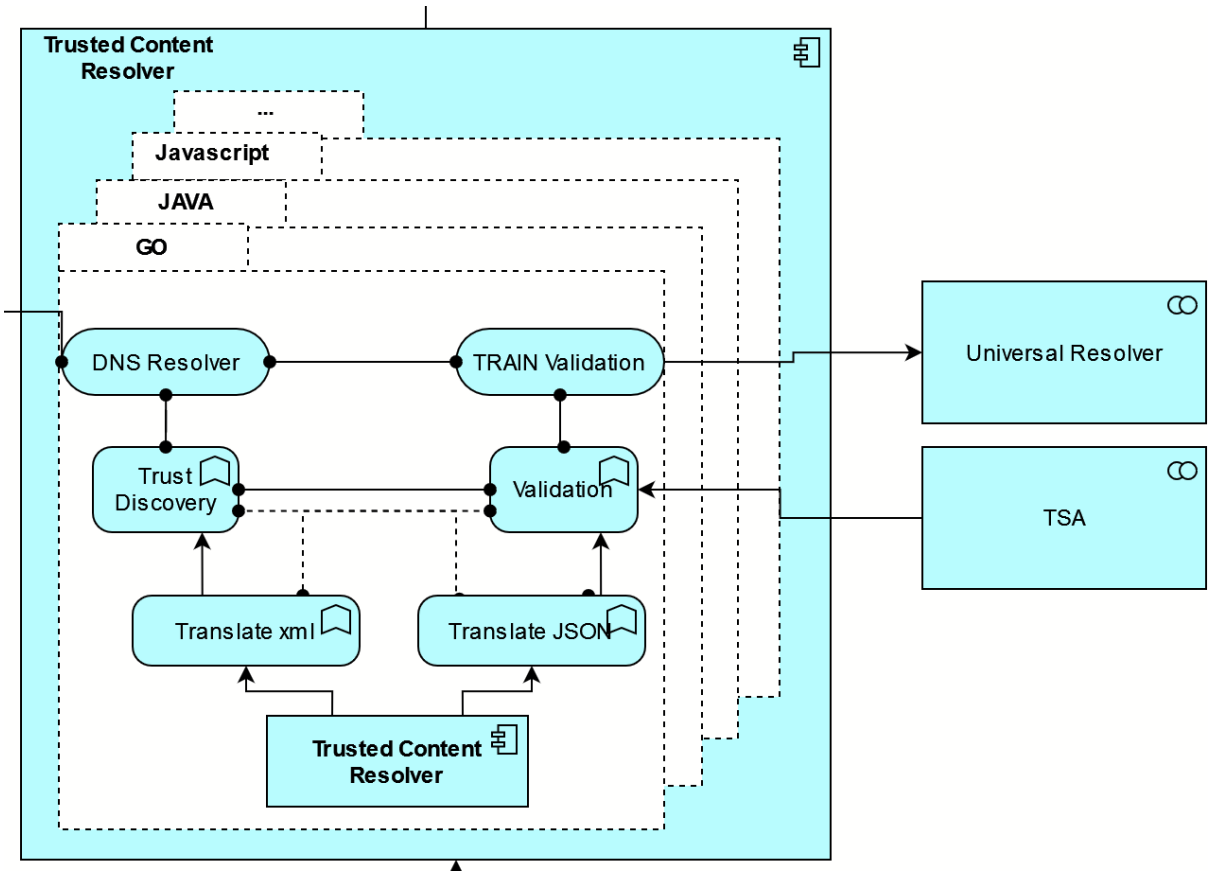

Figure 8 Trusted Content Resolver

7 Conclusion and Consequences

7.1 Security consolidations and implications

As a distributed database both in terms of organization of data as well as responsibility for operation and management, the DNS is very suitable for an infrastructure that aims to support integration and interoperation of various trust frameworks across federations. The original design of the DNS did not consider a number of attacks allowing miscreants to alter information retrieved via the DNS. The Domain Name Service Security Extensions (DNSSEC) have been developed to mitigate this problem. They allow users of the DNS to verify that the data they received is indeed the data intended. This ability for verification is vital for use of DNS in the context of a trust infrastructure.

However, this also means that the secure control of the DNS is essential for a trust framework provider in TRAIN. Hence, TRAIN requires secure organizational governance of the DNS processes at the DNS controller responsible for creating the Trust Schemes/Trust Frameworks and setting the pointers to locations of the Trust Lists.

7.2 Advanced Concepts

7.2.1 Integration with the Ethereum Name Service (ENS)

A potential for further development would be to evaluate further the use of Ethereum ledger based DIDs as pointers to the Trust Lists. This could leverage the trust of Smart Contracts and a decentralized consensus mechanism. The Ethereum Name Service (ENS) is a distributed, open, and extensible naming system based on the Ethereum blockchain.[11] ENS supports text records as well as reverse resolution. Hence, there is a potential for TRAIN to use ENS complementary to DNS/DNSSEC. However, the ENS is not as mature and established as DNS/DNSSEC and this approach would need further research.

7.2.2 Establishment of Trust against Man-in-the-Middle Attacks: PCM and OCM

Further investigation would be required in order to evaluate how Trust Lists can be leveraged to protect against Man-in-the-Middle Attacks between different components. This would be particularly important for interactions between Personal Credential Manager (PCM) and Organizational Credential Manager (OCM).

7.2.3 Verification of the Verifier from the Holder

The following figure shows how TRAIN can be used to establish trust into the verifier. To enable this, a certain authority, such as a specific Gaia-X Federation, has to develop a Trust Framework that specifies how a verifier can be trustworthy (and potentially which verifiers can be trusted to receive which information). Verifiers complying with these requirements will be enrolled via their DID to the trusted verifiers trust list of this Gaia-X Federation.

Now, before a VC is exchanged, the verifier passes the Trust_Scheme_Pointer in the presentation request to the holder. With this, the verifier claims membership in a certain verifier trust framework/scheme. It follows a validation process as described above - only that it is initiated from the holder. After this validation is successful, the requested data can be passed to the verifier.

[11] https://docs.ens.domains/

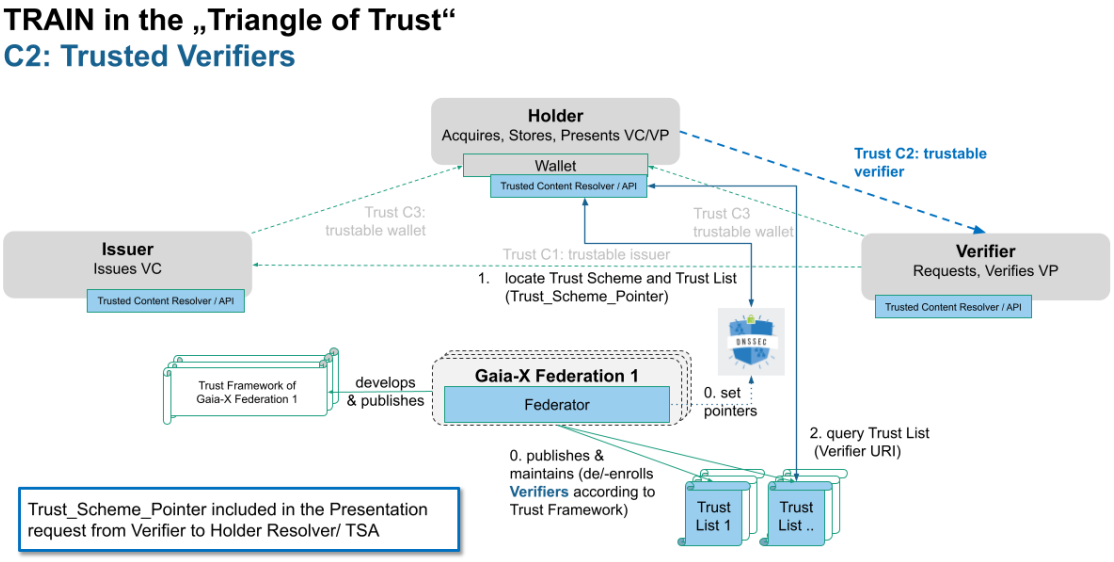

Figure 9 TRAIN in the "Triangle of Trust": Trusted Verifiers

7.2.4 Support of Federation Membership Verification in the OIDC4VP Standard

The following section is for information purposes. The use of TRAIN is explicitly referenced in the implementation considerations of the OIDC4VP at: https://openid.net/specs/openid-connect-4-verifiable-presentations-1_0.html#name-implementation-consideratio

It is written there: "Trust schemes that conform to the TRAIN trust scheme are identified by the type https://train.trust-scheme.de/info. Individual federations are identified by their DNS names.An example claims parameter containing a presentation_definition that filters VCs based on their federation memberships is given below."

```
{
    "vp_token": {
        "presentation_definition": {
            "id": "32f54163-7166-48f1",
            "input_descriptors": [
                {
                    "id": "federationExample",
                    "purpose": "To pick a UK university that is a member of
the UK academic federation",
                    "constraints": {
                        "fields": [
                            {
                                "path": [
                                    "$.termsOfUse.type"
                                ],
                                "filter": {
                                    "type": "string",
                                    "const":          "https://train.trust-
scheme.de/info"
```

```
                                    }
                                },
                                {
                                    "path": [
                                        "$.termsOfUse.federations"
                                    ],
                                    "filter": {
                                        "type": "string",
                                        "const": "ukuniversities.ac.uk"
                                    }
                                }
                            ]
                        }
                    }
                ]
            }
        }
}
```

This example will choose a VC that has been issued by a university that is a member of the ukuniversities.ac.uk federation and that uses the TRAIN terms of use specification for asserting federation memberships.