Fraunhofer IAO

ROW - 2024

DNS as a bridge to establish interoperable trust across different trust anchors

Isaac Henderson, 04.06.2024

Agenda

- Motivation & Introduction
- TRAIN
- Use Case - The Gaia-X Scenario
- TRAIN in Gaia-X Federation Services (GXFS)
- Unified Signature & Verification Model
- Outlook & Conclusion

Motivation & Introduction

- Managing interoperable trust in cross-domains is essential for the adoption of a decentralized identity ecosystem on a wide scale.
- Verifiable credentials and Decentralized identifiers are currently used in international and European initiatives decentralized identities and for sovereign data sharing.
- A standardized reference framework for interoperability in decentralized identities is lacking, affecting adoption.
- TRAIN introduces a new trust implementation model to enable cross-border and organizational credential interoperability across trust anchors using DNS.
- The proposed model includes a unified signature and verification system, with a detailed use case and integration possibilities with Open ID Federation and EBSI.

TRAIN

Trust Management Infrastructure

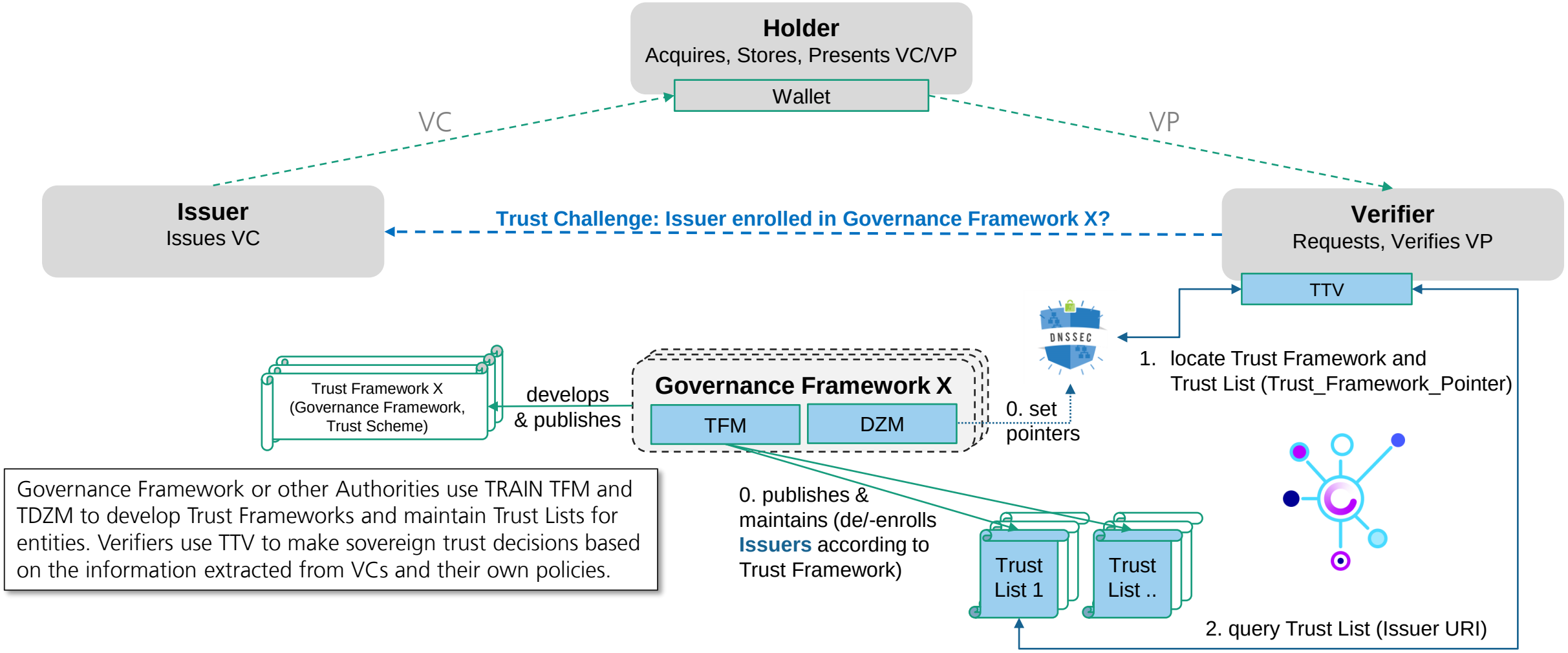
TRAIN supports trust building with trust frameworks by allowing to define and query Trust Anchors / Trustable Authorities as root of trust (e.g., trusted credential issuers)

- Publication and discovery of trust lists through the established DNS infrastructure
- Chain of trust verification leveraging DNS (plus DNSSEC)
- Supports publication and administration of individually defined Trust Lists (e.g., of federation members) for Trust Frameworks maintained by trusted authorities (e.g., Gaia-X federations)
- Technology agnostic ➔ compatible with decentralized VC/ DID-approach as well as with legacy IdM systems

Originated in the EU Project LIGHTest, was developed and piloted further in a number of projects with several partners.

Addressing trust challenge in digital identities using TRAIN

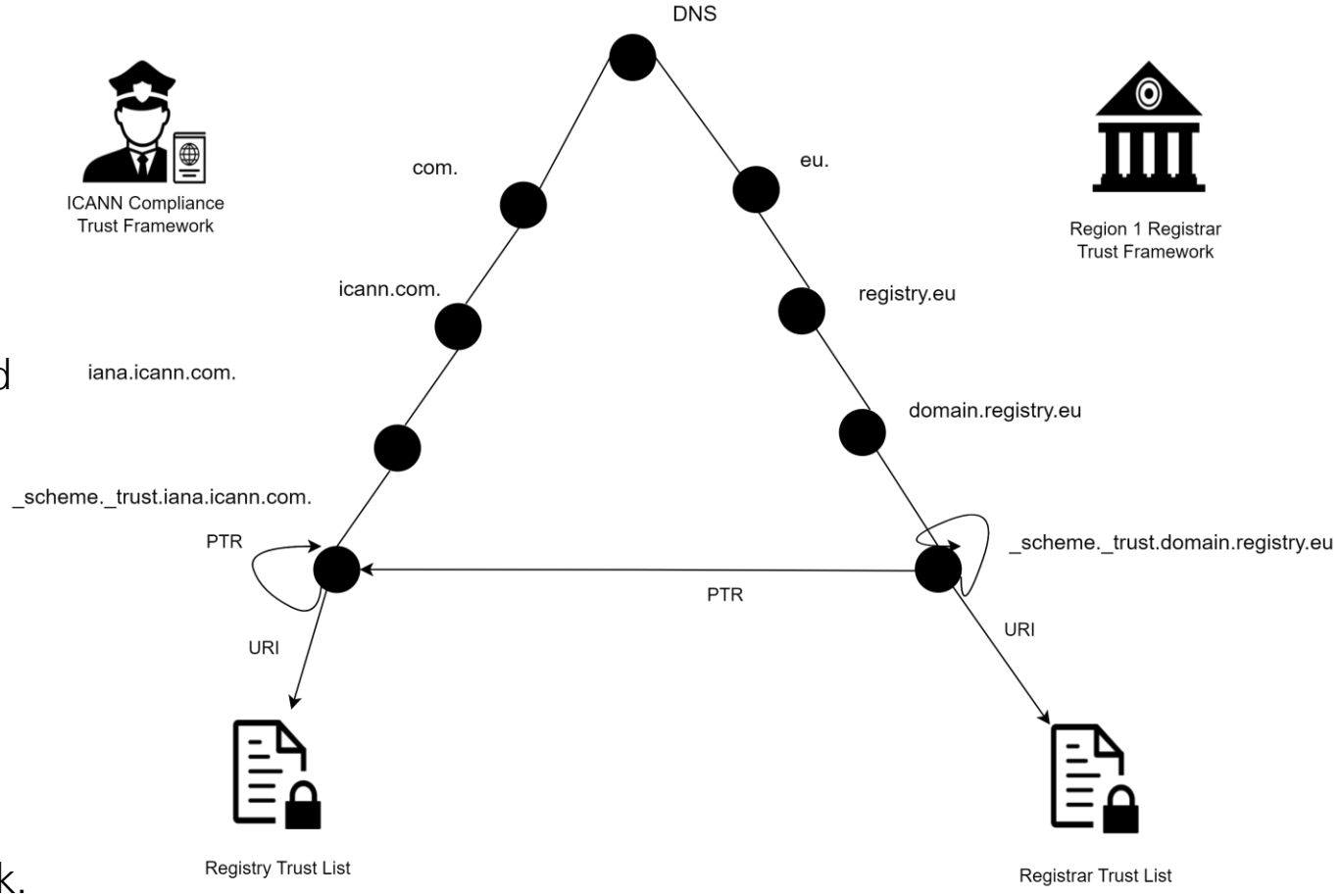
Overview



Governance Framework or other Authorities use TRAIN TFM and TDZM to develop Trust Frameworks and maintain Trust Lists for entities. Verifiers use TTV to make sovereign trust decisions based on the information extracted from VCs and their own policies.

DNS as a bridge to establish trust across different trust anchors

- To set up their trust framework an organization/entity should use their DNS at e.g., federation1.eu.
- The DNS RR holds the PTR for the trust framework and the URI to obtain the Trust List.
- A trust framework operator, e.g. ,icann.com, with framework name “iana” may also chose to trust the trust framework e.g., “domain”, of another trust framework operator, e.g., registry.eu.
- The trust framework operator would therefore add pointer resource records (PTR RRs) to its DNS trust framework entry to point to this other trust framework.
- Allows for hierarchical structure of trust frameworks

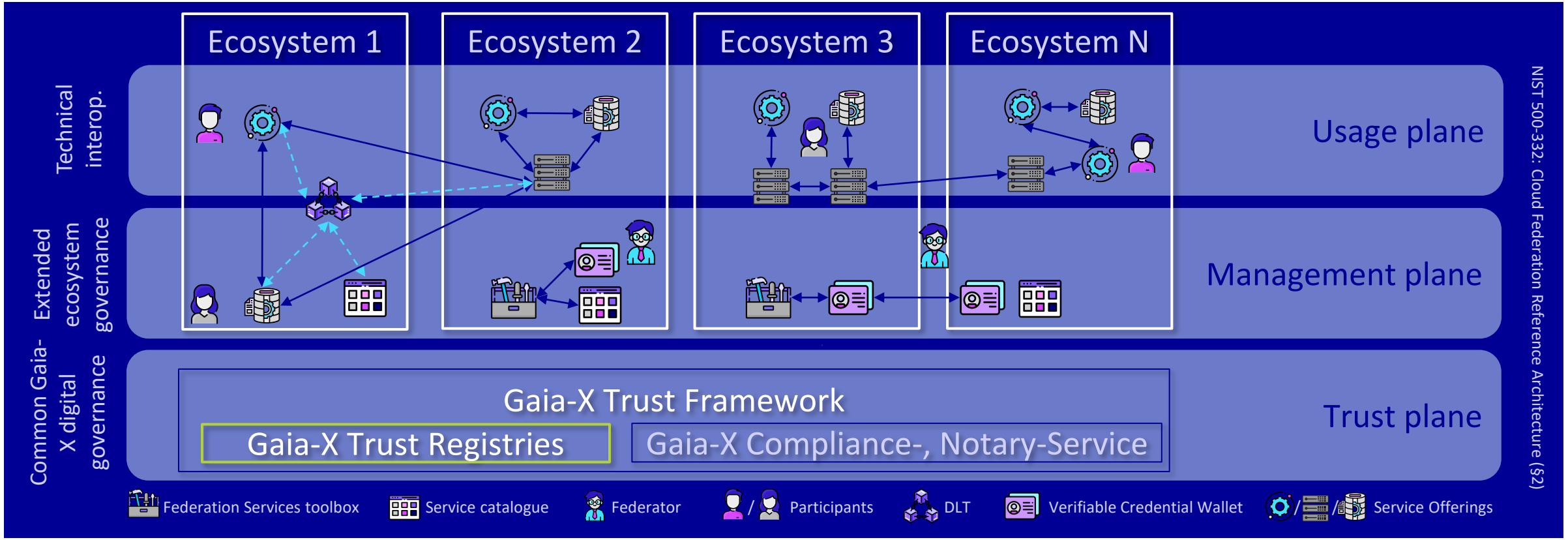


DNS	Resource Records
PTR	_scheme._trust.iana.icann.com.
PTR	_scheme._trust.domain.registry.eu
URI	https://some.org/trust_list / did:ebsi: xyz...

Use Case - The Gaia-X Scenario

Working towards decentral, federated, interoperable, autonomous ecosystems

Gaia-X Ecosystem: the virtual set of Participants, Service Offerings, Resources fulfilling the requirements of the Gaia-X Trust Framework



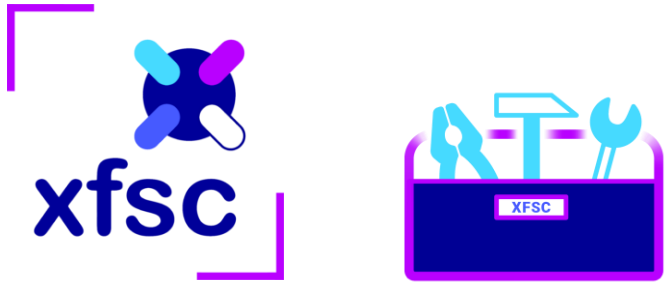
Based on work by Berthold Maier, XFSC Lead IdM & Trust, T-Systems International

The Gaia-X Federation Services (GXFS),

… and the Cross Federation Service Components (XFSC) Toolbox

A project funded by the German government. Aim of the project is to support the development of decentralised digital ecosystems. As part of GXFS, freely accessible, open source-based software components were developed for the creation of federated digital ecosystems.

https://www.gxfs.eu/set-of-services/



The Cross Federation Service Components (XFSC) toolbox was developed as part of GXFS. It comprises the GXFS federation services and offers free and open source code for all interested parties. The XFSC toolbox was officially handed over to the Eclipse Foundation as a community project in late summer 2023. This opens up the project work completely to development contributions from the community.

https://eclipse.dev/xfsc/

TRAIN in GXFS

The Gaia-X Trust Implementation Model requires a decentralized, flexible, scalable, and interoperable Trust Model to manage information on trusted entities, federations, and participants in the ecosystems.

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.

Different domains of trust are existing and currently developing (e.g., eIDAS, EBSI etc.):
the Trust Implementation Model must be able to incorporate and bridge them

Challenges

- How to manage Trusted entities/ Federations/ Participants in a decentralized way?
- Practical Example: How to verify that a credential is issued by a trusted (e.g., from a certain federation) issuer?
- How does interoperability/discovery of federations/participants/entities happen?
- How to integrate different Trust Anchors (e.g., eIDAS, EBSI, sovereignly defined)?

TRAIN Architecture

TRAIN DNS Trustzone Manager (DZM)

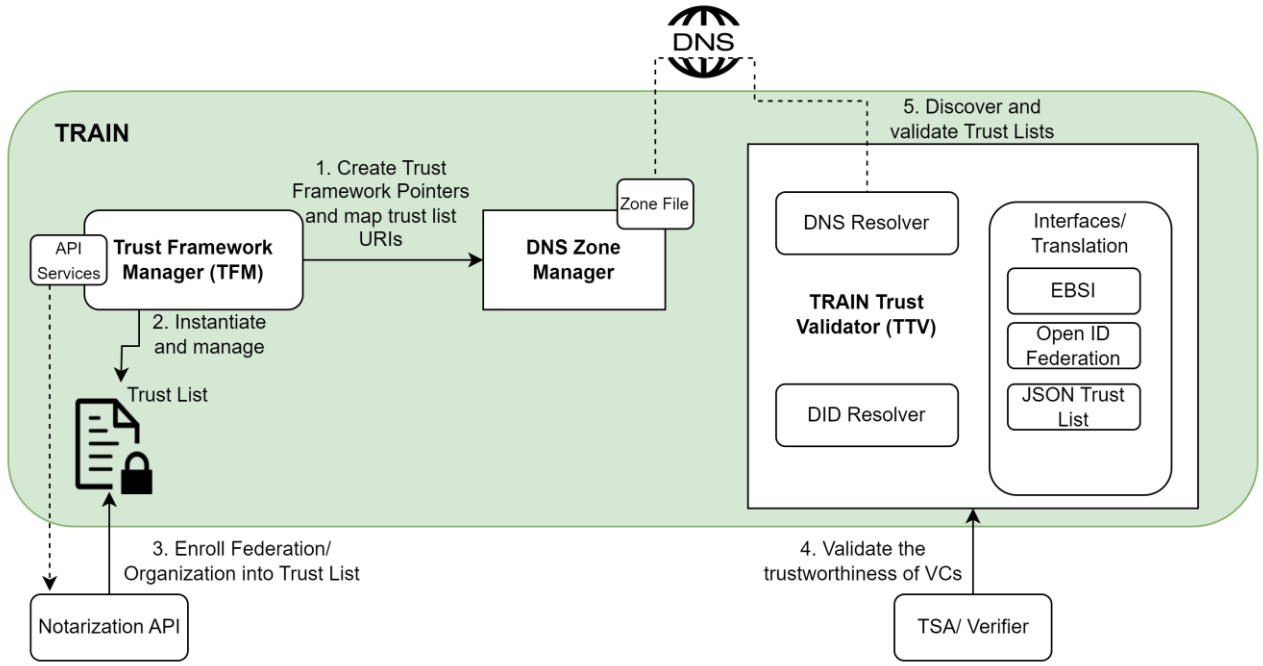
- Anchoring a Trust Framework in the DNS Pointer Resource Record (PTR RR)
- Trust List URI DID is anchored in DNS URI Resource Record (URI RR)
- Global discovery through DNS and DNSSEC for chain of trust

TRAIN Trust Framework Manager (TFM)

- Setup and Configuration of a Trust Framework
- Trust List Management: de-/enrollment of entities etc.
- Provides Federation/organization/participant specific Trust Lists in different formats

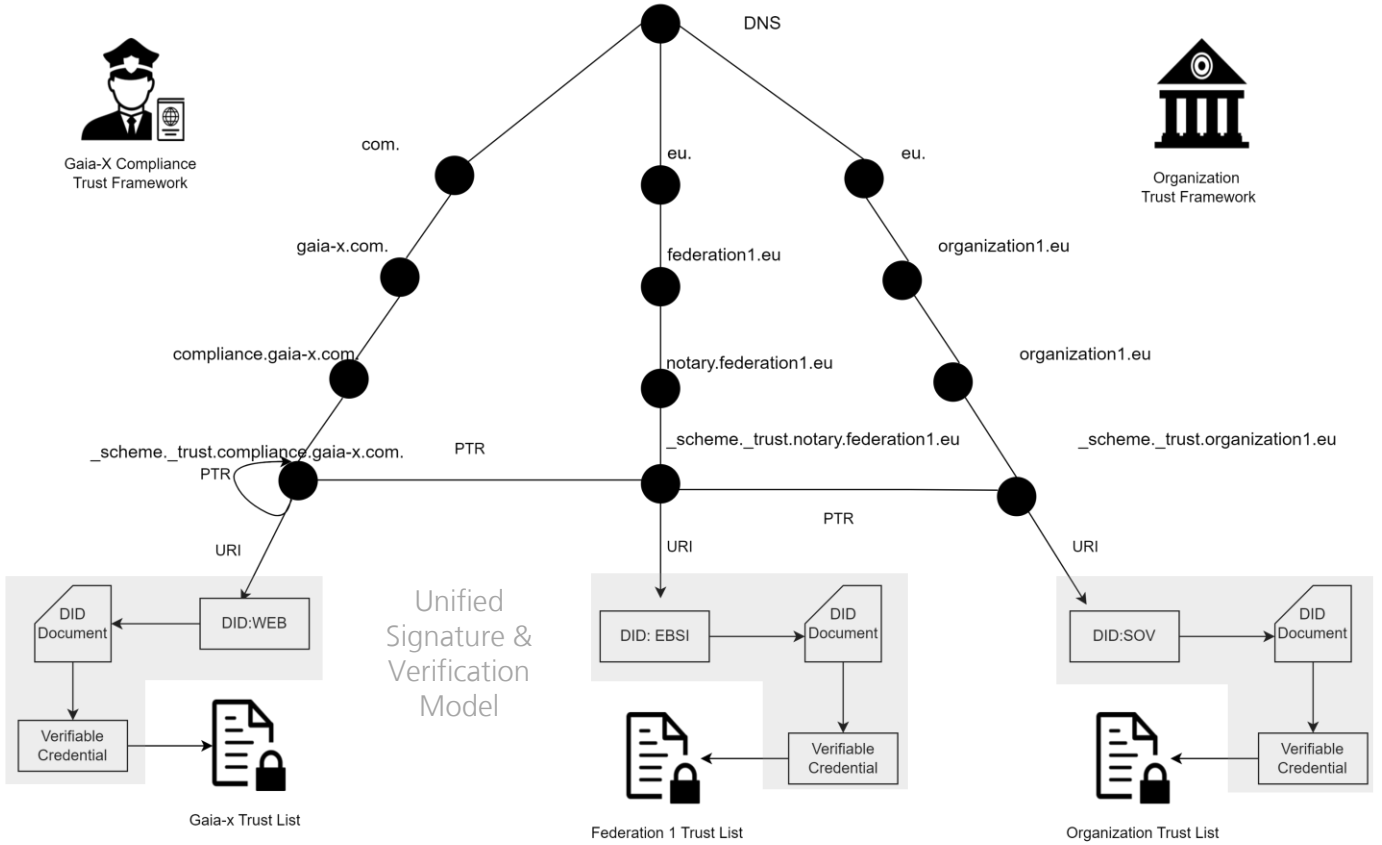
TRAIN Trust Validator (TTV)

- Supports external validation of trust through integration in a Trust Framework
- Global Discovery of Trust Frameworks through DNS Resolver
- Verification of issuer details of the credential with the information of the trust list



Leveraging DNS for creation, publication, and cross referencing of trust frameworks

- To set up their trust framework a federation can use their DNS at e.g., federation1.eu.
- The DNS RR holds the PTR for the trust framework and the URI to obtain the Trust List DIDs
- A trust framework operator, e.g. ,gaia-x.com, with scheme “compliance” may also chose to trust the trust framework e.g., “notary”, of another trust framework operator, e.g., federation1.eu.
- The trust framework operator would therefore add pointer resource records (PTR RRs) to its DNS trust framework entry to point to this other trust framework.
- Allows for hierarchical structure of trust frameworks



DNS	Resource Record	Function
PTR	_scheme._trust.compliance.gaia-x.com	Trust Framework Pointer
PTR	_scheme._trust.notary.federation1.eu	Trust Framework Pointer
URI	http://some.org/trust_list / did.example…	Trust List Location URI

Trust Lists

XML Example

- TRAIN Trust Lists are based on the ETSI TS 119 612 standard and list all the enrolled entities in a specific data file/format certified by the Trust Framework Provider
- JSON-LD and XML currently supported
- Stored on web server or IPFS
- Every trusted VC issuer's details are described under the attribute <TrustServiceProvider>
- The ID (for example URI, DID or UUID) of the issuer is under the attribute <ServiceTypeIdentifier>

<ServiceTypeIdentifier>did:key:z6MkkVNPqpURtWDdy9Tx…</ServiceTypeIdentifier>

```
<TrustServiceProvider>
 <UUID>1144355</UUID>
 <TSPName>Automotive Federation</TSPName>
 <TSPTradeName>Automotive Federation e.V.</TSPTradeName>
 <TSPInformation>
    <Address>
       <ElectronicAddress>notary@autofed.de</ElectronicAddress>
       <PostalAddress>
          <City>Stuttgart</City>
          <Country>DE</Country>
          <PostalCode>70563</PostalCode>
          <StreetAddress1>Heilbronner Straße 1</StreetAddress1>
       </PostalAddress>
    </Address>
    <TSPCertificationList>
       <TSPCertification>
             <Type>ISO:9001</Type>
             <Value>9386546745</Value>
       </TSPCertification>
       <TSPCertification>
             <Type>EU-VAT</Type>
             <Value>DE988889999</Value>
       </TSPCertification>
    </TSPCertificationList>
    <TSPEntityIdentifierList>
       <TSPEntityIdendifier>
             <Type>LEI</Type>
             <Value>334701983XD71E4FBC41</Value>
       </TSPEntityIdendifier>
    </TSPEntityIdentifierList>
    <TSPInformationURI>https://autofed.de/informationuri</TSPInformationURI>
 </TSPInformation>
 <TSPServices>
    <TSPService>
       <ServiceName>Notary Auto Federation</ServiceName>
       <ServiceTypeIdentifier>did:key:z6MkkVNPqpURtWDdy9TxYuKVgSMfTu7kcAEwQfrkyiWqqrKV</ServiceTypeIdentifier>
       <ServiceCurrentStatus>active</ServiceCurrentStatus>
       <StatusStartingTime>2023-12-15T00:00:00Z</StatusStartingTime>
       <ServiceDefinitionURI>string</ServiceDefinitionURI>
       <ServiceDigitalIdentity>
          <DigitalId>
             <X509Certificate>123example</X509Certificate>
             <DID>did:web:notary.autofed.de</DID>
          </DigitalId>
       </ServiceDigitalIdentity>
       <AdditionalServiceInformation>
          <ServiceBusinessRulesURI>https://notary.autofed.de/business</ServiceBusinessRulesURI>
          <ServiceGovernanceURI>https://notary.autofed.de/governance</ServiceGovernanceURI>
          <ServiceIssuedCredentialTypes>
             <CredentialType>
                <Type>Participant Credential</Type>
             </CredentialType>
             <CredentialType>
                <Type>Principal Credential</Type>
             </CredentialType>
          </ServiceIssuedCredentialTypes>
          <ServiceContractType>https://notary.autofed.de/contract</ServiceContractType>
          <ServicePolicySet>https://notary.autofed.de/policy</ServicePolicySet>
          <ServiceSchemaURI>https://notary.autofed.de/schema</ServiceSchemaURI>
          <ServiceSupplyPoint>https://notary.autofed.de/sp</ServiceSupplyPoint>
```


Integration with Verifiable Cedentials

via TermsOfUse (W3C VCDM)

- VCs by issuers enrolled in a trust framework via TRAIN must contain a **termsOfUse** property
- Terms of Use contain the **Trust Scheme Pointers** (DNS names) of the trust frameworks(s) that the issuer claims to be a member of

W3C VCDM v1.1 / 2.0 (Candidate Recommendation Draft 03/03/2024):
"Terms of use can be utilized by an issuer or a holder to communicate the terms under which a verifiable credential or verifiable presentation was issued. The issuer places their terms of use inside the verifiable credential. The holder places their terms of use inside a verifiable presentation."


```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "
    https://identity.foundation/EcdsaSecp256k1RecoverySignature2020/lds-ecdsa-
    secp256k1-recovery2020-0.0.jsonld"
  ],
  "issuer": {
    "id": "did:key:z6MkkVNPqpURtWDdy9TxYuKVgSMfTu7kcAEwQfrkyiWqqrKV"
  },
  "credentialSubject": {
    "id": "did:key:z6MkkVNPqpURtWDdy9TxYuKVgSMfTu7kcAEwQfrkyiWqqrKV",
    "type": [
      "Participant Credential",
      "Entity Credential"
    ],
    "OrganizationName": "Fraunhofer IAO",
    "OrganizationAddress": "Nobelstrasse 12",
    "OrganizationLocation": "Stuttgart",
    "OrganizationCountry": "DE"
  },
  "termsOfUse": {
    "type": "train",
    "id": "https://train.trust-scheme.de/info",
    "trustScheme": [
      "notary.federation1.de",
      "compliance.gaia-x.eu"
    ]
  },
  "issuanceDate": "2024-01-18T11:09:10.497Z",
  "type": [
    "VerifiableCredential"
  ],
  "proof": {
    "type": "Ed25519Signature2018",
    "created": "2024-01-18T11:09:10Z",
    "verificationMethod":
    "did:key:z6MkkVNPqpURtWDdy9TxYuKVgSMfTu7kcAEwQfrkyiWqqrKV#z6MkkVNPqpURtWDd
    y9TxYuKVgSMfTu7kcAEwQfrkyiWqqrKV",
    "proofPurpose": "assertionMethod",
    "jws":
    "eyJhbGciOiJFZERTQSIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..wqaMMxzw8vpOnHg
    ZfoFkrvF0fuJTu14hV4Q-yaf-YTFaec1T418qUBrQDPTYFOpxeZ-CckZt1lVsYmez01ebCA"
  }
}
```


Fraunhofer IAO

TRAIN Trust Validator (TTV)

TTV is integrated in the TSA (Trust Services API) for external verification of trust via TTV Libraries

- Issuer: Taken from issuer of the VC – can also be a URI (e.g. DID)
- trustSchemePointers: taken from termsOfUse of the VC
- endpointTypes: Service Endpoints from the DID documents, to specify specific trust lists [optional]

TTV returns the details of the respective Trusted Service Provider from the Trust List (if present), e.g. public keys, contracts, policies, business rules (see Trust List Example).

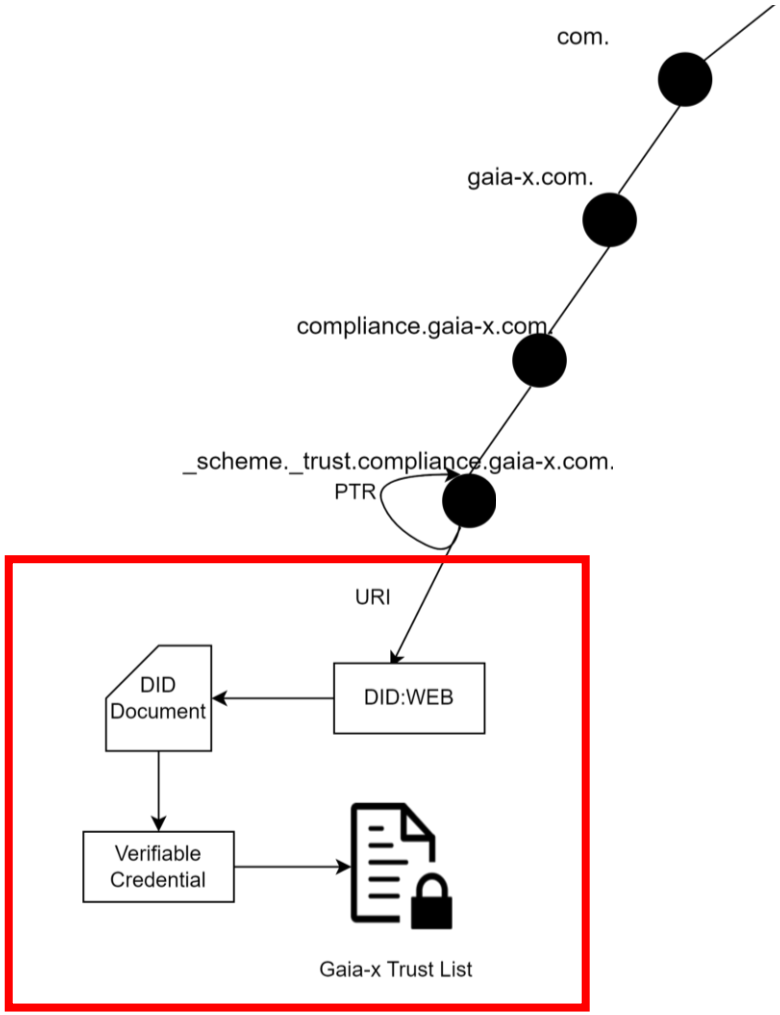
With these details a specified trust policy can be executed


```
  "issuer":
"did:key:z6MkkVNPqpURtWDdy9TxYuKVgSMfTu
7kcAEwQfrkyiWqqrKV",
  "trustSchemePointers": [
    "notary.federation1.de"
  ],
  "endpointTypes": [
    ""
  ]
}
```


Unified Signature & Verification Model

Trust Lists via DID and VC

Allows trust lists across trust domains with different trust list formats (json, XML) to be signed and verified uniformly using Verifiable Credentials (VC).



Process

1. TFM provides endpoints for trust list initialization with different formats
2. On successful instantiation, the trust list is stored on IPFS/web server, their signature along with a hash is enveloped as VC and stored separately
3. The URI location of the VC can be resolved via a service endpoint of a DID Document

Integration of TRAIN with other GXFS Components

Trust Services API

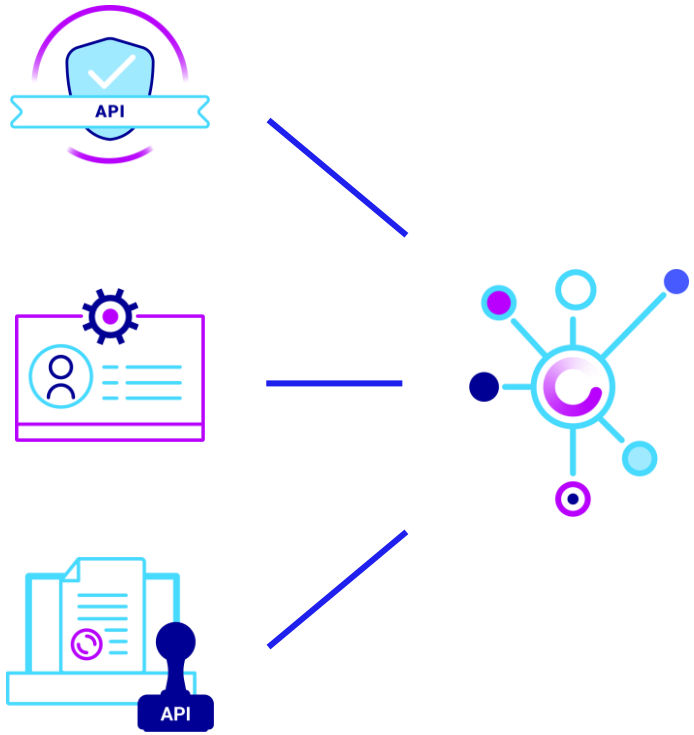
can integrate the TRAIN Trust Validator Libraries to verify the institutional trust of verifiable credentials

Organizational Credential Manager

can use the TSA to validate the trust of the organizational verifiable credentials (via the TRAIN Trust Validator Libraries) before storing them in the wallet

Notarisation Services API

uses the TRAIN Trust Framework Manager Connector (Rest API Endpoints) to enroll trusted entities / trusted service providers into the Trust List via the TRAIN Trust Framework Manager (TTFM)



Outlook & Conclusion

- Managing interoperable trust across diverse ecosystems is challenging due to the rapid evolution of identity technology and emerging new standards.
- Current trust management systems are mostly centralized and effective within specific domains that recognize a single authoritative entity.
- The TRAIN model supports diverse credential formats, aiming to serve as a universal trust model for various initiatives like Gaia-X and EUDIW.
- The Unified Signature and Verification model has been implemented in the Gaia-X Federation Services and tested with two trust list formats.

That's it – so far

Next Steps

- Standardization in Gaia-X and beyond
- UNDP Regi-TRUST as global pilot
- Evaluate the use of Ethereum Name Service (ENS) as a DLT-based alternative to DNS
  (a first concept exists for the GNU Name System)
- Future enhancements include extending the TRAIN implementation to support Open ID Federation Trust Lists and the EBSI Trusted Issuers Registry.

Check out TRAIN in the XFSC Toolbox: https://gitlab.eclipse.org/groups/eclipse/xfsc/train/

There is also a demo with documentation that lets you experiment with TRAIN locally:
https://gitlab.eclipse.org/eclipse/xfsc/train/TRAIN-Documentation/-/tree/main/demonstration

Contact

Isaac Henderson
Team Identity Management

www.hci.iao.fraunhofer.de
Phone +49 711 970-2431
isaac-henderson.johnson-jeyakumar@iao.fraunhofer.de
0000-0001-9397-1321
https://www.linkedin.com/in/isaac-henderson-76171a68/

Fraunhofer Institute for Industrial Engineering IAO
Nobelstr. 12 | 70569 Stuttgart, Germany
Hardenbergstr. 20 | 10623 Berlin, Germany

Unified Signature & Verification Model

Validation Process

Required:

Trust Framework Pointer (embedded as a DNS name in the termsofUse object of the VC) and URI (DID, URL, UUID) of the VC issuer (obtained from the VC)

1. TTV reads the PTR RRs of the DNS domain resolved from trust framework pointer,
2. dereferences the URI RRs, and expects to find a DID,
3. Well Known DID configuration verification,
4. DID document is resolved from the DID,
5. Service endpoint of DID document leads to VC,
6. Proof of the VC is validated against public keys of the DID Document
7. Credential subject of VC contains URI to the trust list and hash of the trust list
8. Trust list is resolved, integrity of trust list is checked against the hash from the VC
9. validation is performed (simple case: issuer URI included in the trust list – or complex policy)