Use of DNS in Connection with Trust Registries Panel Discussion

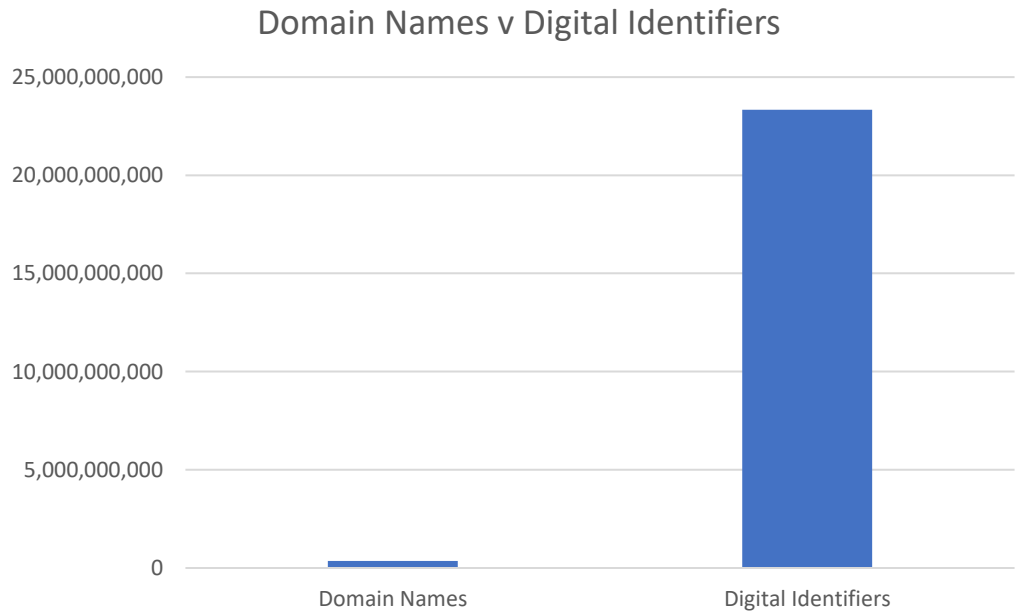
Michael Palage, InfoNetworks
Isaac Henderson, Fraunhofer IAO
Jacques Latour, CIRA

ROW-12
20-June-2023

By the numbers ……

218.3 million gTLDs
135.7 million ccTLDs
354 million domains (total)

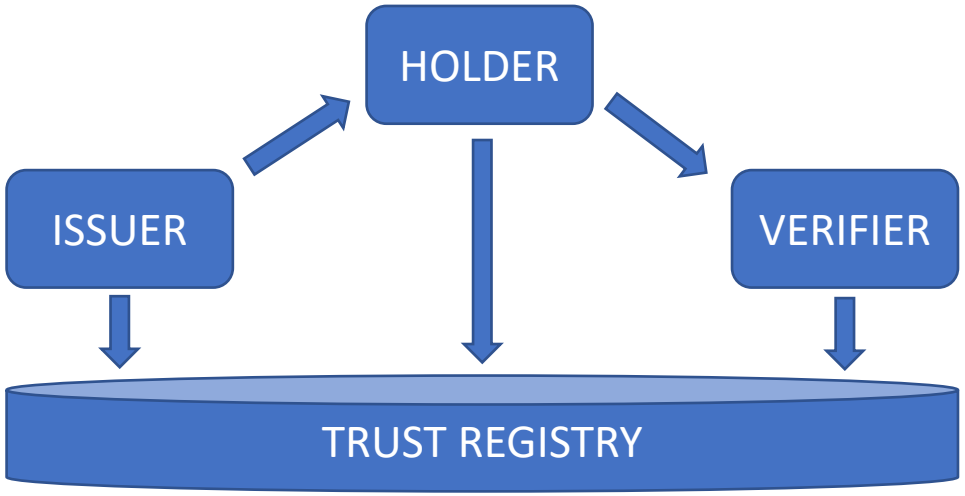
15.4 billion IoT Devices
8.0 billion people
334 million businesses
23.3 billion (total)

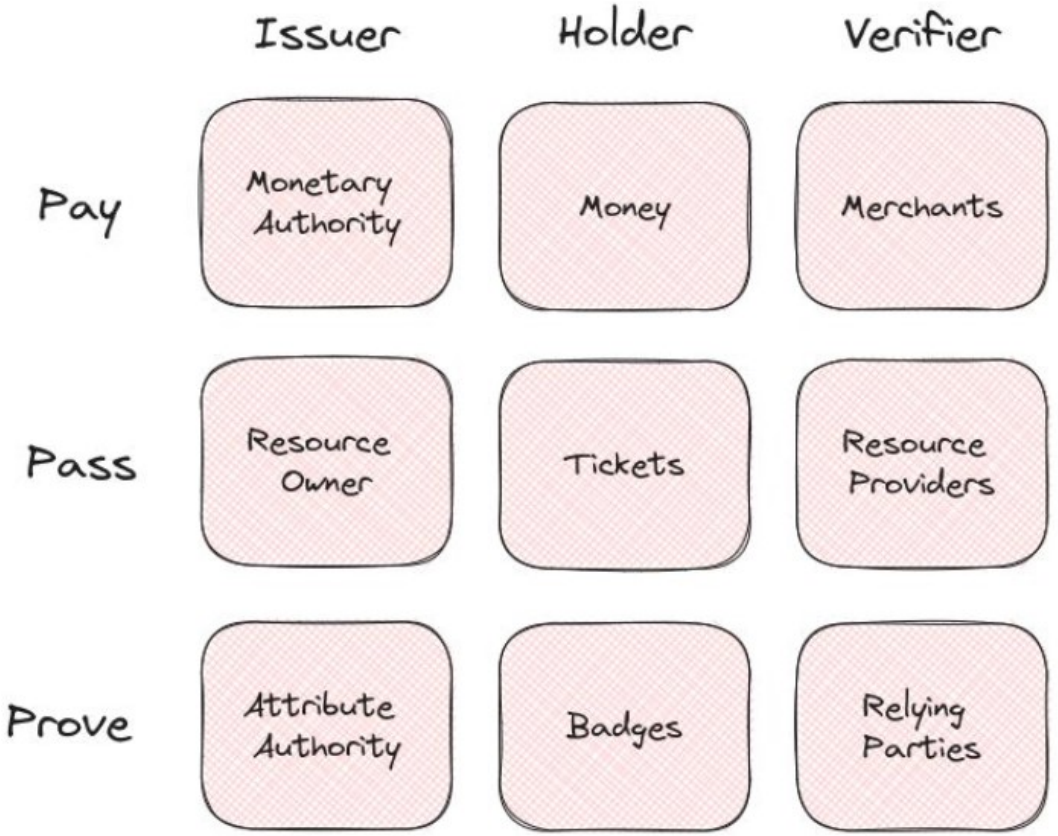


Source: Verisign Domain Name Report Q1-2023

ROW-12
20-June-2023

Trust Triangle

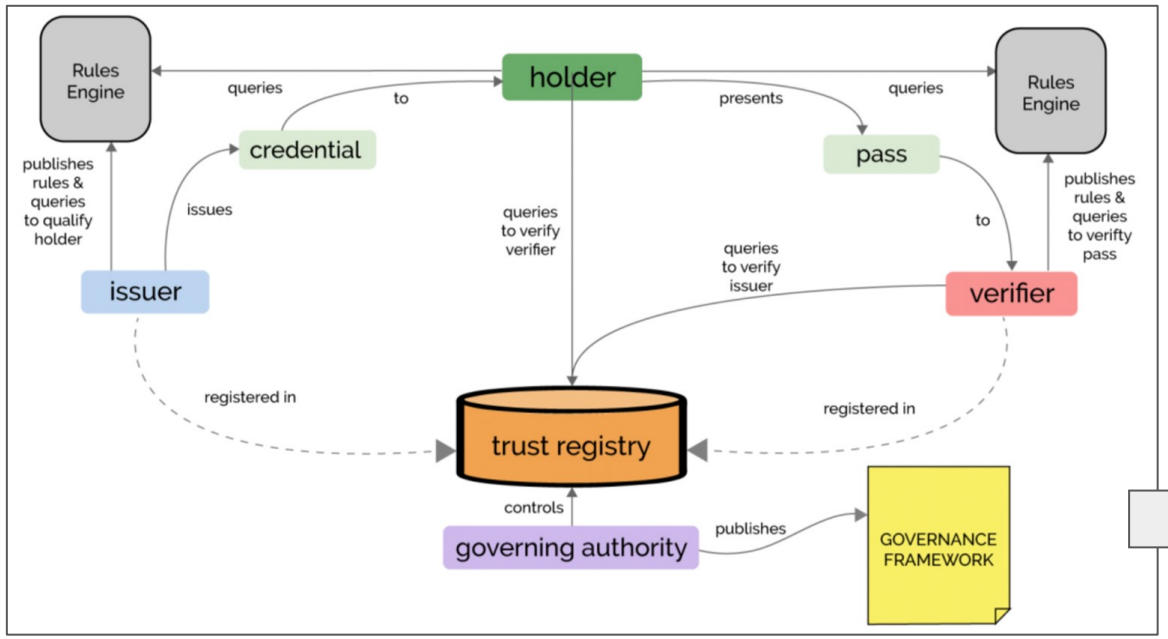


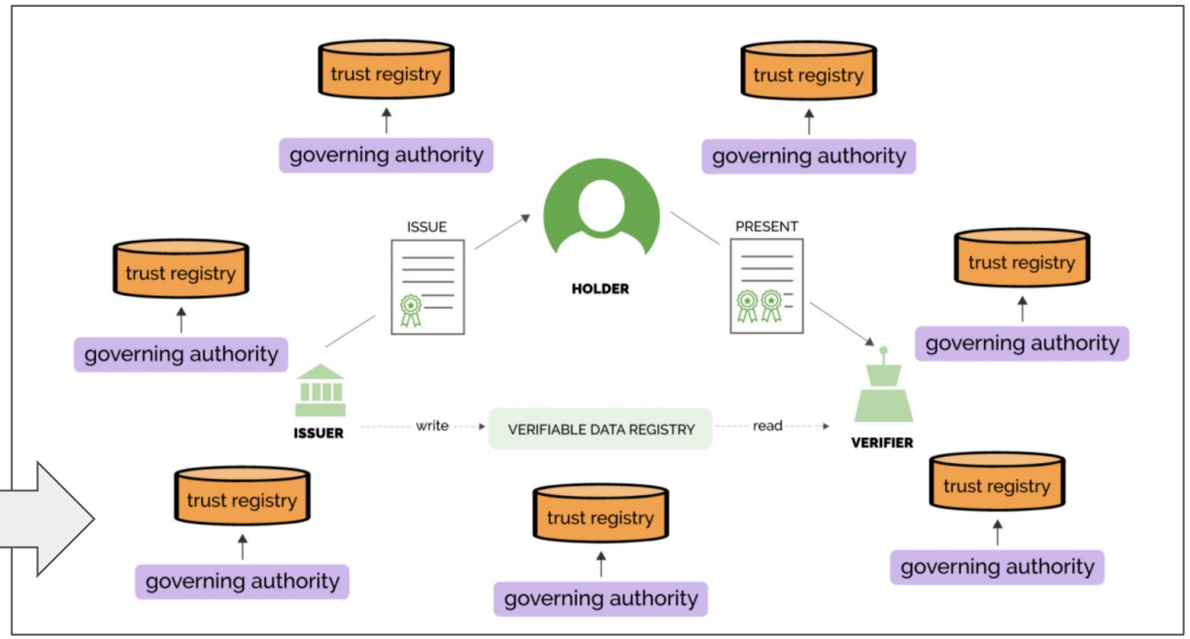


Source: Tim Bouma
Director, Verification and Assessment Digital Governance Council
https://www.linkedin.com/feed/update/urn:li:activity:7075128244047376384/

ROW-12
20-June-2023

Federating Trust Between Ecosystems





- **Trust Challenge 1:** Is the Issuer trustworthy? Is he really who he claims to be? What level of trust?
- **Trust Challenge 2:** Is the Verifier trustworthy? Is this really the Relying Party/verifier or someone stealing my data ("Man in the Middle" attack)?
- **Trust Challenge 3:** Is the Holder wallet trustworthy?

Picture credit: Good Health Pass Interoperability Blueprint

ROW-12
20-June-2023

An Emerging Problem Space

Discoverability	Being able to discover and evaluate services, or a network or ecosystem of services, in a consistent and sustainable manner.
Trust Interoperability	Being able to access and evaluate trusted information about the services and validate certificates/data knowing the technical, policy and business rule frameworks from which they are published.
Technical Interoperability	Being able to technically access, process and verify certificates and/or data regardless of the technical standards used by the services (e.g., data model, schemas, cryptographic signatures).
Semantic Interoperability	Being able to recognize and exchange data in a meaningful way by having knowledge of the data processing and data usage contexts.

TRAIN

TRust Management INfrastructure

ROW-12
20-June-2023

TRAIN Focus: External Verification of the Trust in a Certain Entity

TRAIN is a global trust infrastructure that can be used to verify the trustworthiness of involved parties in an electronic transaction.

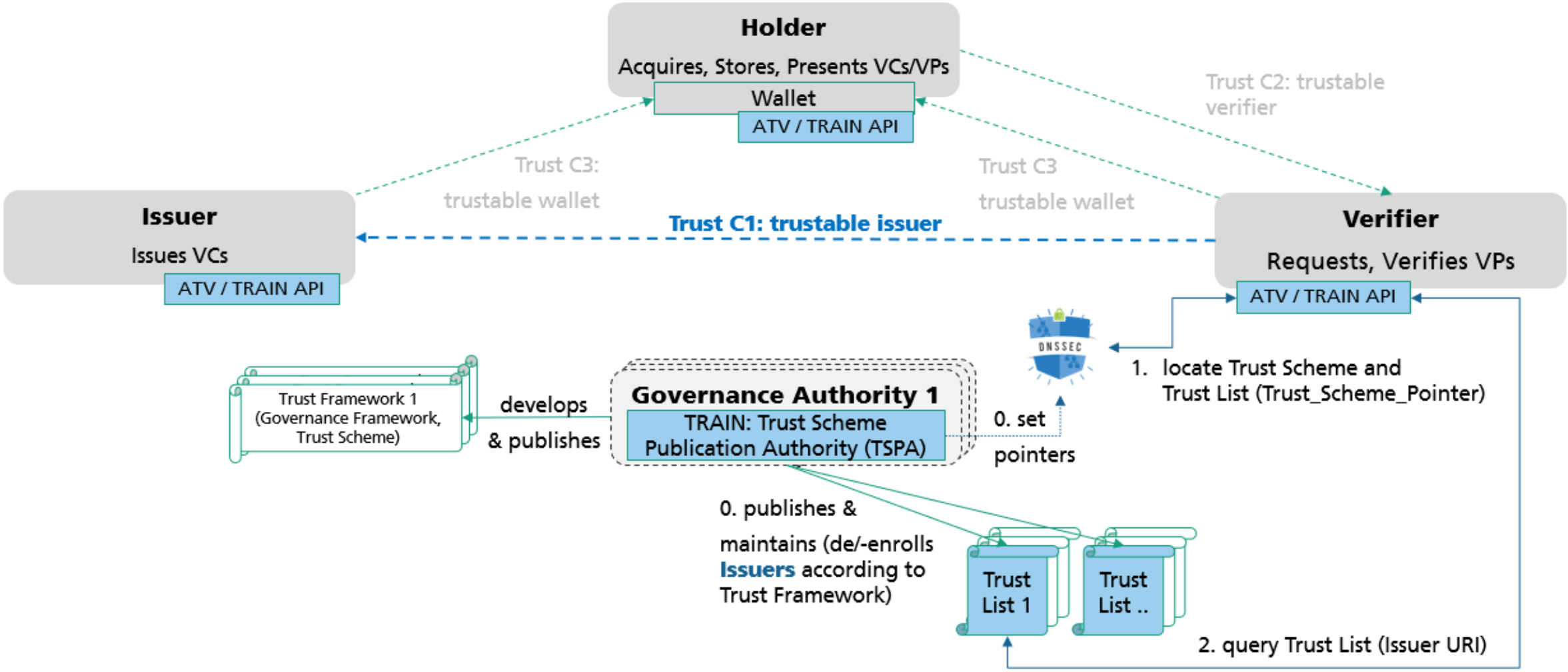
TRAIN is an approach to trust lists (trust registries):

- Supports publication and administration of individually defined Trust Lists for Trust Frameworks (Trust Schemes) that can be maintained trusted authorities
- Supports Verifiers in examining the trustworthiness of Issuers through inclusion in trust lists
- Enables considering Trust Framework memberships (eg. eiDAS, business registers) of entities with different Trust Anchors as root of trust
- Developed in EU Projects LIGHTest and NGI ESSIF LAB

"...TRAIN enables secure, trustable digital interactions. A classical hierarchical Certificate Authority (CA)-type structure is avoided - so is fraud, chaos and the pure dominance of the economically strongest actors in the system...TRAIN will provide a decentralized framework for the publication and querying of trust information..."

ROW-12
20-June-2023

TRAIN in the „Triangle of Trust“



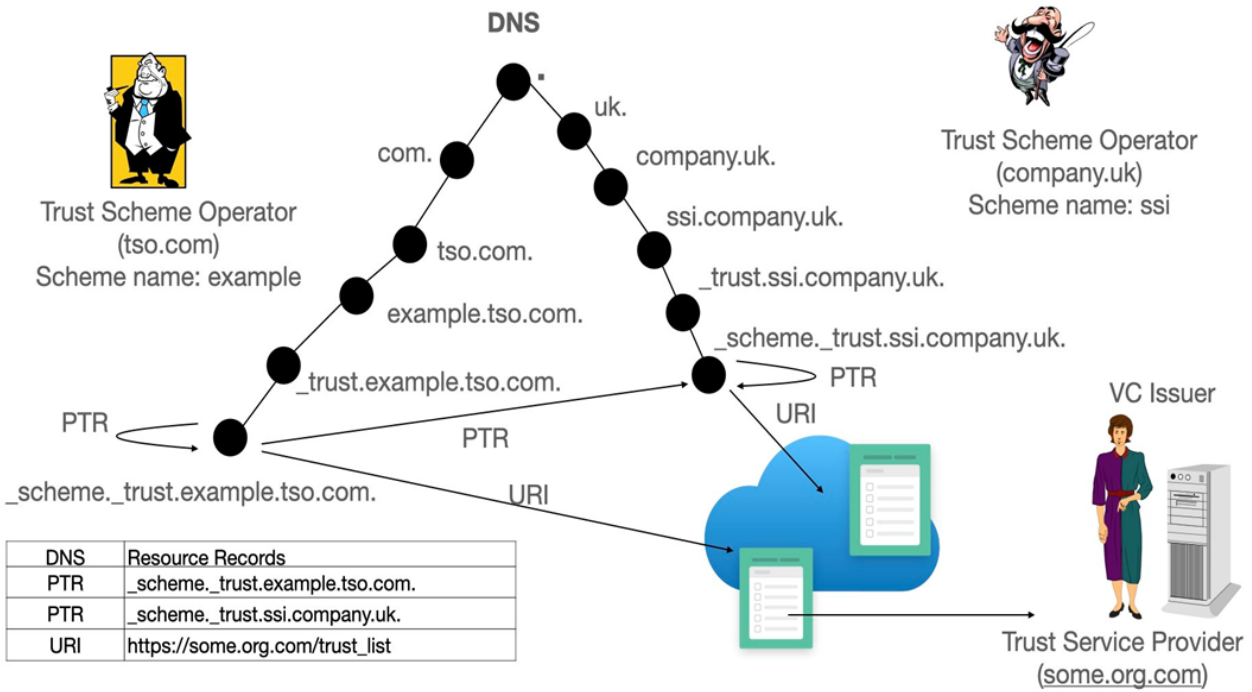
ROW-12
20-June-2023

TRAIN Technical Overview

TRAIN makes use of the Internet Domain Name System (DNS) with its existing global infrastructure, organization, governance and security standards.

Highlighted TRAIN Technical features:

- Can use DNSSEC (Domain Name System Security Extensions) to secure and verify the chain of authenticity and to locate the Trust List
- Provides agnostic support for all types of 'Root of Trust' architecture, e.g. X.509, DID.
- Adopts pattern from the ETSI 119 612 TS scheme for trust lists
- Provides an API for discovery and verification of trusted endpoints
- Open Source Apache 2.0 License



DNS	Resource Records
PTR	_scheme._trust.example.tso.com.
PTR	_scheme._trust.ssi.company.uk.
URI	https://some.org.com/trust_list

ROW-12
20-June-2023

TRAIN in Verifiable Credentials

W3C Verifiable Credentials Data Model

Terms of Use Feature (https://www.w3.org/TR/vc-data-model/#terms-of-use)
"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. This specification defines a termsOfUse property for expressing terms of use information"

➔ TRAIN Information is placed in the Terms of Use of a Verifiable Credential

```
"termsOfUse": [{
"type":"https://gitlab.grnet.gr/essif-lab/infrastructure/fraunhofer/train-source-code",
"id": "https://train.trust-scheme.de/info",
"trustScheme": ["ehic.europe.train.trust-scheme.de"]
}]
```

Exemplary Credential

1

```
{
"@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://essif-lab.pages.grnet.gr/interoperability/eidas-generic-use-case/contexts/ehic-v1.jsonld",
    "https://essif-lab.pages.grnet.gr/interoperability/eidas-generic-use-case/contexts/cades-signature.jsonld"
    "https://essif-lab.pages.grnet.gr/interoperability/eidas-generic-use-case/contexts/train-trustScheme.jsonl
],
"id": "https://ec.europa.eu/credentials/83627465",
```

2

```
"type": [
    "VerifiableCredential",
    "EuropeanHealthInsuranceCard"
],
"issuer": "Ministry of Social Security & Inclusion",
"name": "European Health Insurance Card",
"description": "Example of a European Health Insurance Card",
"expirationDate": "2029-12-03T12:19:52Z",
"institutionID": "09999 - INSS Madrid",
"issuanceDate": "2021-05-27T10:09:34.175Z",
"cardNo": "80756099990000034111",
"personalID": "09999 111999",
"credentialSubject": {
    "id": "did:key:z6MkjRagNiMu91DduvCvgEsqLZDVzrJzFrwahc4tXLt9DoHd",
    "type": [
        "EuropeanHealthInsuranceHolder",
        "Person"
    ],
    "familyName": "Muster",
    "givenName": "Maria",
    "birthDate": "1958-07-17"
},
```

3

```
"termsOfUse": [{
    "type": "https://train.trust-scheme.de/info",
    "trustScheme": [
        "ehic.europe.train.trust-scheme.de"
    ]
}],
"proof": [{…
```

4

```
"proof": [{
        "verificationMethod": "did:sov:staging:BJX4adKceDv9D4qmztEN3F#key-1",
        "proofPurpose": "assertionMethod",
        "type": "Ed25519Signature2018",
        "created": "2021-05-27T10:09:38Z",
        "jws": "eyJhbGciOiAiRWREU0EiLCAiYjY0IjogZmFsc2UsICJjcml0IjogWyJiNjQiXX0..9kPrEo_j-3lqvcqsFfXCXwsDun4uKlvT_lFkbI9gSCLYrrSpkEEA7NOQBF63mKSsL
    },
    {
        "type": "CAdESRSASignature2020",
        "created": "2021-05-27T10:09:40Z",
        "verificationMethod": "did:sov:staging:BJX4adKceDv9D4qmztEN3F#MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAziPjJZebqdAhKZI0zUqd7439PGAlGY/M
        "proofPurpose": "assertionMethod",
        "cades": "-----BEGIN PKCS7-----MIIKmwYJKoZIhvcNAQcCoIIKjDCCCogCAQExDzANBglghkgBZQMEAgEFADBPBgkqhkiG9w0BBwGgQgRAxqU6KyRyuEpX/UP59TOlkSt9uwr
    }
]
```

1) Contents
2) Credentials
3) Terms of Use - TRAIN
4) ProofsContent

ROW-12
20-June-2023

TRAIN Use Cases

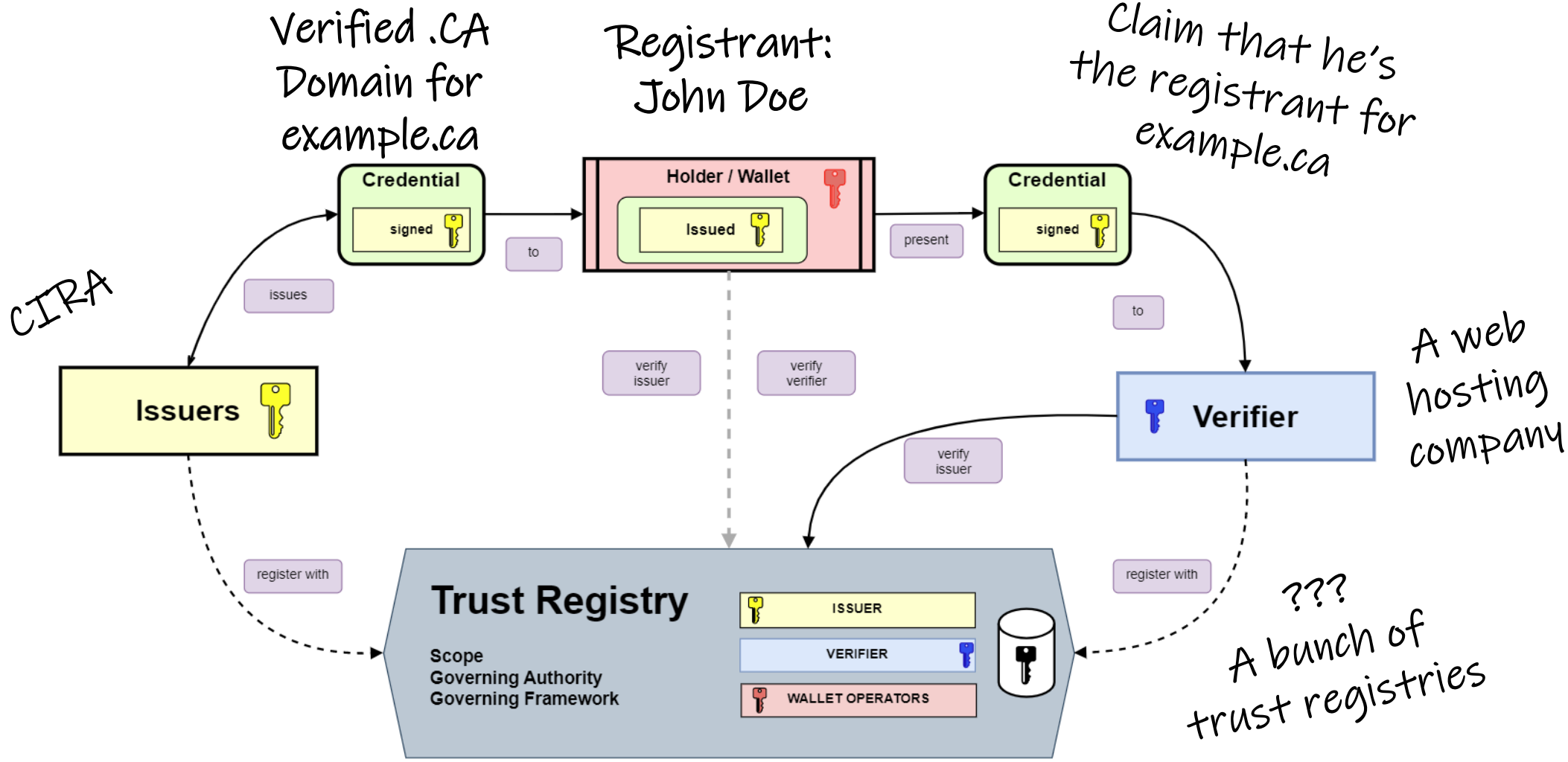
- Regi-TRUST at UNDP
- European Project: Gaia-X
- Next Generation SSI Standards

TRAIN is a flexible approach to trust management that can be combined with other approaches (e.g. eIDAS 1.0 trusted lists, EBSI trusted issuer registry, etc.)

DANCE

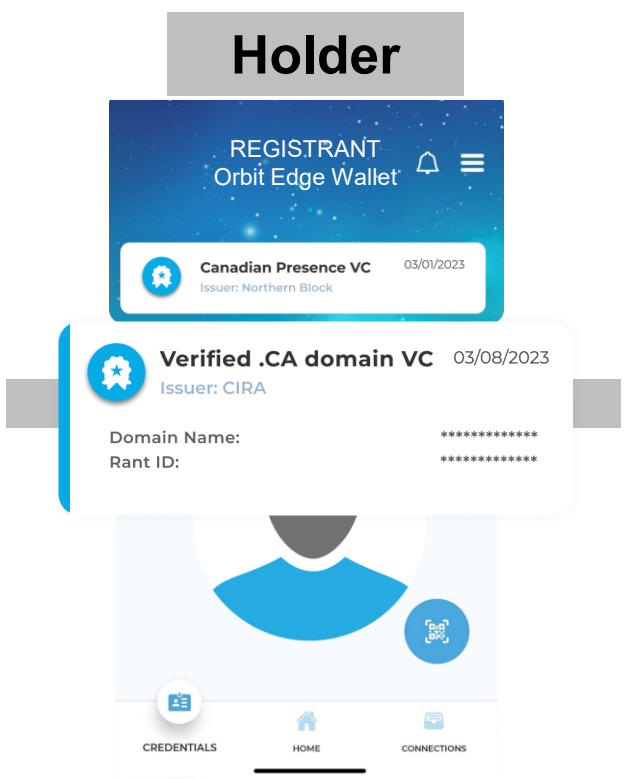
ROW-12
20-June-2023

Interoperability of Digital Credential Ecosystem



ROW-12
20-June-2023

ISSUING A *VERIFIED .CA DOMAIN* DIGITAL CREDENTIAL



Offers
Verified .CA Domain
Digital Credential
to Registrant

CIRA as an Issuer

Issuer domain: verified.cira.ca

ROW-12
20-June-2023

Digital Trust is about verifying
< Authenticity, accuracy and authority >
The DNS enables unique identifiers
DNSSEC enables authenticity in DNS transactions

When an entity is presented with a verifiable claim, there are three things they will want to ensure:

1. **That a claim hasn't been altered/falsified at any point in time**
   (Cryptographic proof verifiability, TLSA records)
2. **That a claim has accurate representation**
   (Authentication, DID Discovery/mapping within DNS)
3. **That a claim has authority**
   (Authorization, Trust Registries/trust lists, TLSA records)

DEFINITION OF A TRUST REGISTRY

AKA Member Directory, Repository or Trust Hubs, Trust Lists…

The purpose of a Trust Registry is to provide participants of a Digital Identity Ecosystem the means to verify in that ecosystem that other digital participants are trustworthy

Governance, Operations and Registration Management

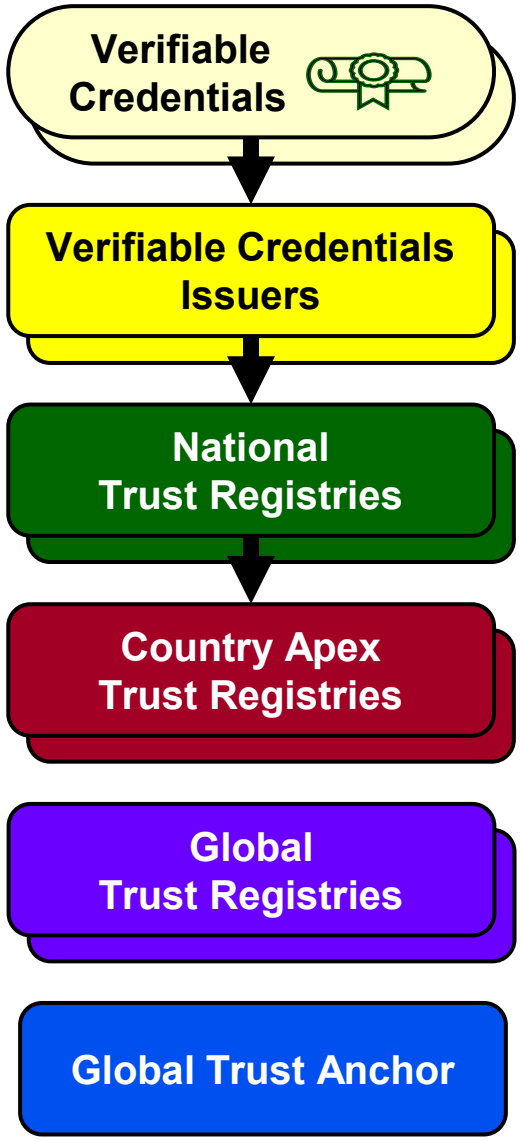
I made this up ☺

Trust Registry: (i.e. Ecosystem: All Country Code Top Level Domain (ccTLD) Operators)

- **Defined Scope** (i.e. The trusted list of all ccTLDs that issue digital credentials)
- **Governing Authority** (i.e. The **ccNSO** verified credential committee)
- **Governance Model** (i.e. All **registered** ccTLDs)

This is an example only

ROW-12
20-June-2023



ALIGNMENT OF EMERGING IDENTIFIERS TECHNOLOGIES

Unique “Digital Credentials Issuer” identifiers enables global interoperability

Now is the time to think on having:

- **A global interoperable network of digital identity ecosystem via trust registries**
- **Global unique identifiers for digital credential issuers**
- **And leverage DNS and DNSSEC:**
  - **to ensure the uniqueness and authenticity of credential issuers**
  - **To enable lookup of trust registry affiliation**

ROW-12
20-June-2023

Thank You

Michael Palage
InfoNetworks
mpalage@infonetworks.global
https://www.linkedin.com/in/michaelpalage

Isaac Henderson
Fraunhofer IAO / University of Stuttgart
isaac-henderson.johnson-jeyakumar@iao.fraunhofer.de
https://www.linkedin.com/in/isaac-henderson-76171a68/

Jacques Latour
CIRA
Jacques.Latour@cira.ca
https://www.linkedin.com/in/jacqueslatour/

Annex – Miscellaneous Slides

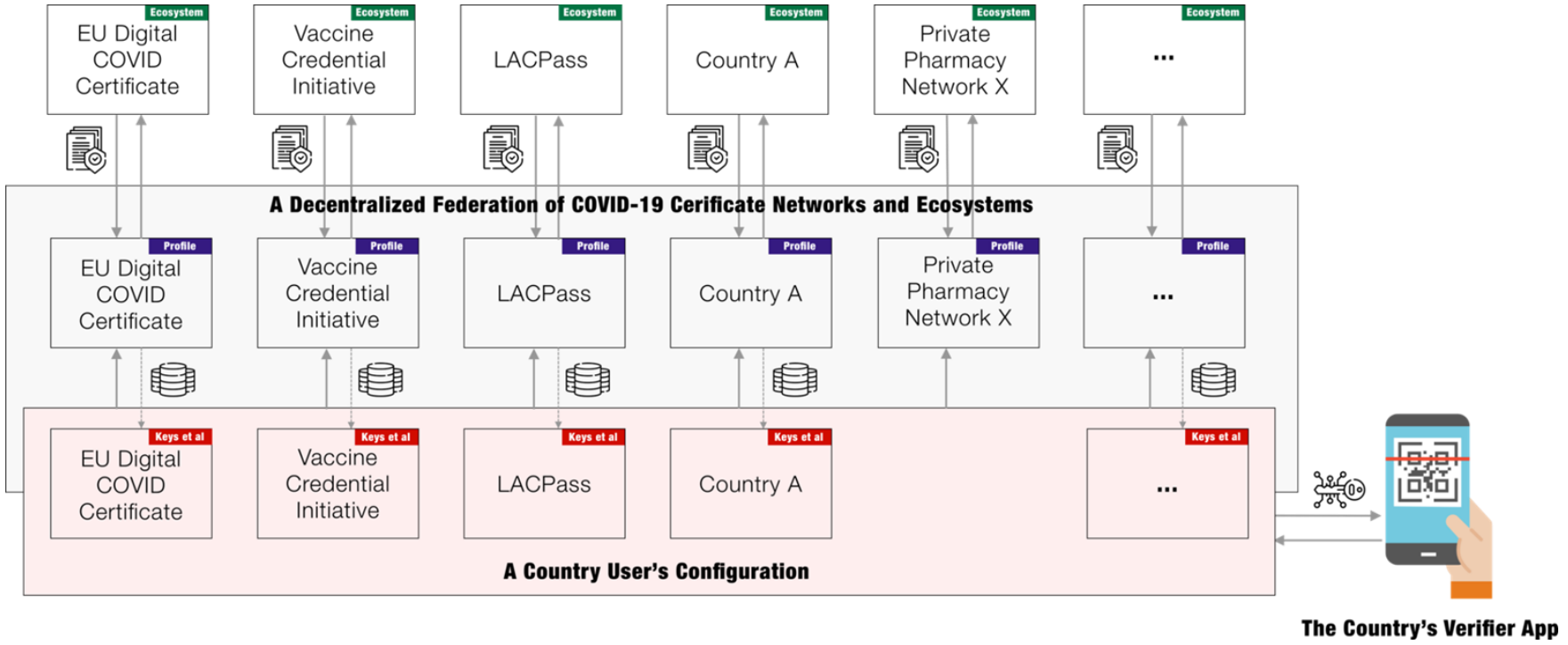
Attributes of TRAIN Trust Lists

- **Trust Lists** used by TRAIN follow the **ETSI TS 119 612 standard** and list all the enrolled entities (Issuers) in a specific data file/format certified by the issuing authority.
- Every trusted VC issuer's details are described under the attribute *<TrustServiceProvider>.*
- The ID of the issuer is under the attribute *<IssuerName>.*
- Each VC issuer in the trust list has a Service Type Identifier under the attribute *<ServiceTypeIdentifier>*. This is a URL, and the web page that it points to should contain the JSON schema (including the @context property) for the VCs that are issued for this Service Type.

```
<TrustServiceProvider>
 <TSPInformation>
  <TSPName>
   <Name xml:lang="en">BGE</Name>
  </TSPName>
  <IssuerName>
   <Name xml:lang="en">https://vc.bge.verifiablecredentials.net</Name>
  </IssuerName>
  <TSPTradeName>
   <Name xml:lang="en">VATES-11111111</Name>
  </TSPTradeName>
  <TSPAddress>
   <PostalAddresses>
   <ElectronicAddress>
  </TSPAddress>
  <TSPInformationURI>
   <URI xml:lang="en">https://www.inclusion.gob.es/en </URI>
  </TSPInformationURI>
 </TSPInformation>
 <TSPServices>
  <TSPService>
   <ServiceInformation>
                <ServiceTypeIdentifier>
     https://train.trust-scheme.de/schema/gasBill-schema.json</ServiceTypeIdentifier>
   <ServiceName>
                <Name xml:lang="en">Gas Bill</Name>
   </ServiceName>
   <ServiceDigitalIdentity>
                <DigitalId>
                                    <X509Certificate>...</X509Certificate>
  <DID>DID:WEB... </DID>
                </DigitalId>
   </ServiceDigitalIdentity>
                <ServiceStatus>
  http://ehic.essif.trust-scheme.de/ServiceTypes/Servicestatus/granted </ServiceStatus>
       <StatusStartingTime>2021-05-11T00:00:00Z</StatusStartingTime>
   </ServiceInformation>
  </TSPService>
 </TSPServices>
</TrustServiceProvider>
```

Global Project: Regi-TRUST at UNDP

Digital TRUST Infrastructure for Discovery and Validation (Regi-TRUST) is a digital infrastructure project hosted by the United Nations Development Programme (UNDP). The project is built on TRAIN to develop and provide a suite of tools to enable scalable 'network of networks' models for discovery and validation of trusted services across networks/ecosystems. It was initially started at the Linux Foundation in 2021 as the Global COVID Certificate Network (GCCN) to address the interoperability challenges that exist between the siloed COVID certificate ecosystems.



Global Project: Regi-TRUST at UNDP

Regi-TRUST in the long run aims to provide the 'network of networks' infrastructure that enable:

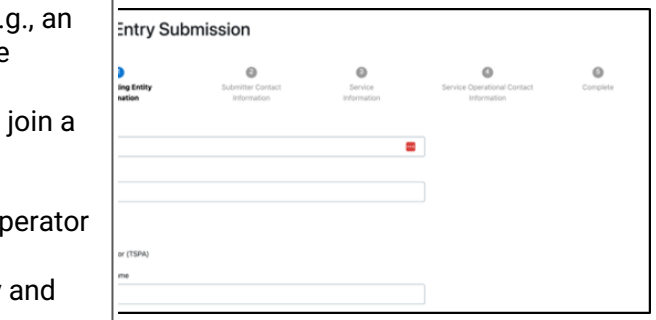
- Inter-governmental organizations to implement and operate decentralized federations of digital ecosystems and services and facilitate interoperability and trusted interactions among them.
- Governments and organizations at large to participate in ecosystems of digital services at local, regional, national, or global level without having to compromise on their own governance/policies.
- Consumers, both individuals and organizations, to be able to easily discover and validate public and private services in need and access relevant service information/endpoints in a secure and trusted manner.

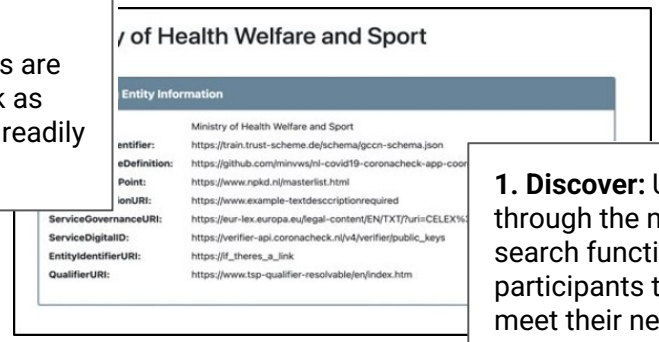
Participating

1. Apply: Participants (e.g., an existing COVID certificate ecosystem) provide the requested information to join a network

2. Vetted: The network operator vets the submitted data, validating its authenticity and legitimacy

3. Published: Participants are published onto a network as vetted and active entries readily discoverable





1. Discover: Users browse through the network or use search function to identify participants that potentially meet their needs and criteria.

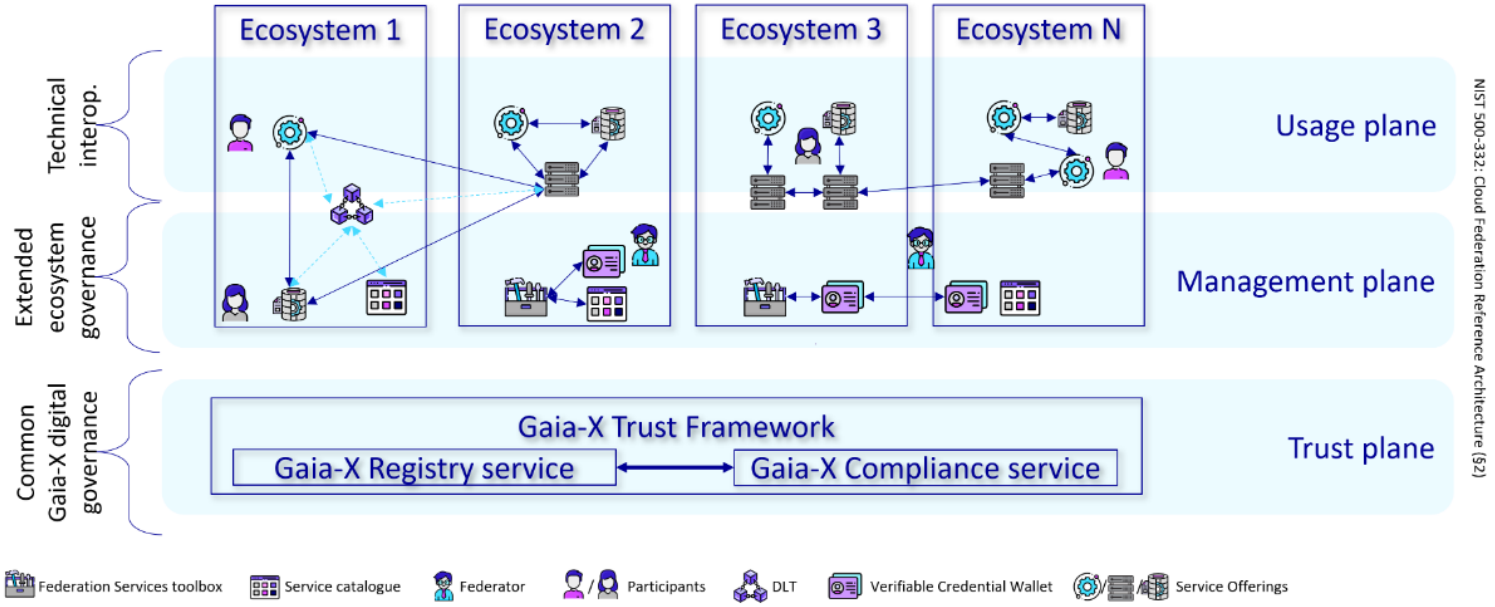
2. Build Trust: Users review vetted information of discovered participants, determining who they want to

3. Verify: Verifier apps configured by users check if incoming certificates/data are from trusted parties

Using

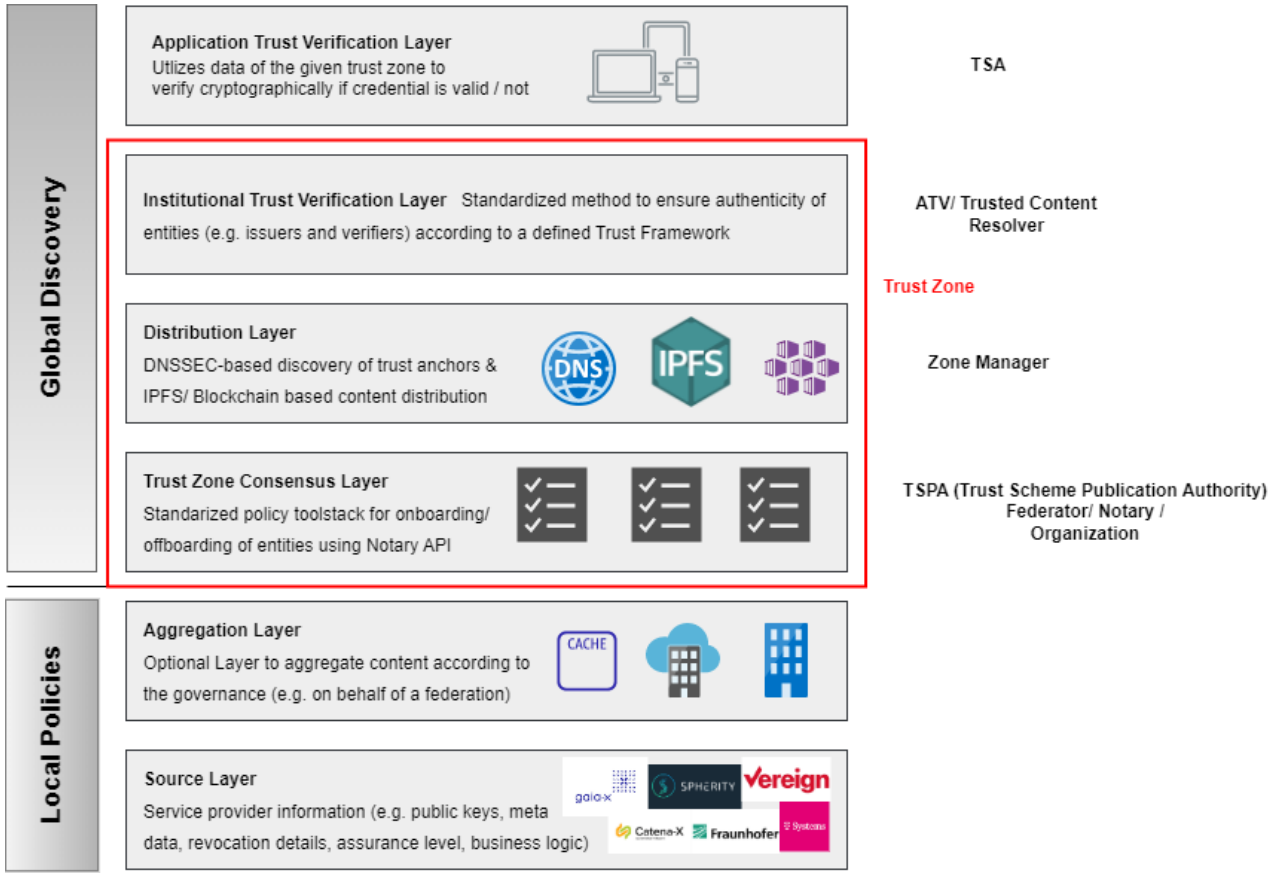
European Project: Gaia-X

- The Gaia-X Ecosystem is the virtual set of Participants, Service Offerings, Resources fulfilling the requirements of the Gaia-X Trust Framework.
- Gaia-X enables Interoperability between independent autonomous ecosystems.
- The three planes represent three levels of interoperability and match the planes as described in the NIST Cloud Federation Reference Architecture chapter 2.



TRAIN as Trust Implementation Model for Gaia-X

- DNS(SEC) as a trust anchor and to locate trust frameworks/ trust registries
- **Multiple Trust Frameworks** can be set up under the Trust Infrastructure to scale globally and to cater to different domains of trust (etc: EBSI, eIDAS...)
- Federations or groups (industry organizations, NGOs, etc.) of entities have the flexibility to define themselves the trust standards they require
- Provides technical components* supporting entities in:
    1. Publication and administration of trust lists
    2. Verification of trust list membership using Trusted Content Resolver



Transatlantic Project: Next Generation SSI Standards

- The aim of the project was to perform interworking experiments between Europe and the USA, and also report our results to the relevant Standards Development Organizations.
- The partners in this project are CROSSWORD CYBERSECURITY LTD, FRAUNHOFER FHG AND SPRUCE SYSTEMS, INC.
- **The interworking tests covered the following features:**
  a. credential issuing and presentation using the latest OpenID4VCs drafts;
  b. using JWT proofed VCs, which are ambiguously specified in the current W3C Verifiable Credentials Data Model v1.1, so we needed to resolve these ambiguities;
  c. using TRAIN infrastructure for trust scalability;
  d. using eIDAS LoAs, when RPs require different LoAs before accepting VCs from users.

TRAIN Status and Ongoing Work

TRAIN is a flexible approach to trust management that can be combined with other approaches (e.g. eIDAS 1.0 trusted lists, EBSI trusted issuer registry, etc.).

Demonstrated with TRAIN:

- Verification of Issuers, Schemas and Verifiers

Ongoing work:

- ONCE, BMWK Showcase Secure Digital Identities („Schaufenster Sichere Digitale Identitäten“) Piloting TRAIN for the Trust Framework of the municipal ID-credential („Kommunale Datenkarte“)
- Fed2SSI for Gaia-X/Dataspaces, Developing a bridge for policy-based transformation of federated credentials to SSI credentials with TRAIN as trust anchor
- Verification of Wallets, other aspects, such as GDPR conformance of entities/components
- Integration of TRAIN components into web-agents and more wallets
- Policies for verifying entities
- Working Groups in Rebooting Web of Trust, W3C, Gaia-X ICAM, German Showcase Projects, IDlab Community of Practice, etc. towards standardization etc.