



THIRD ECLIPSE TRACTUS-X COMMUNITY DAYS

December 05–06, 2024
STUTTGART



SUPPORTED BY:





The future of EDC and bring your own wallet

December 6th 2024

Christian Lahmer (SSI EG)

Lars Geyer-Blaumeiser (Connectivity EG)



Tractus X





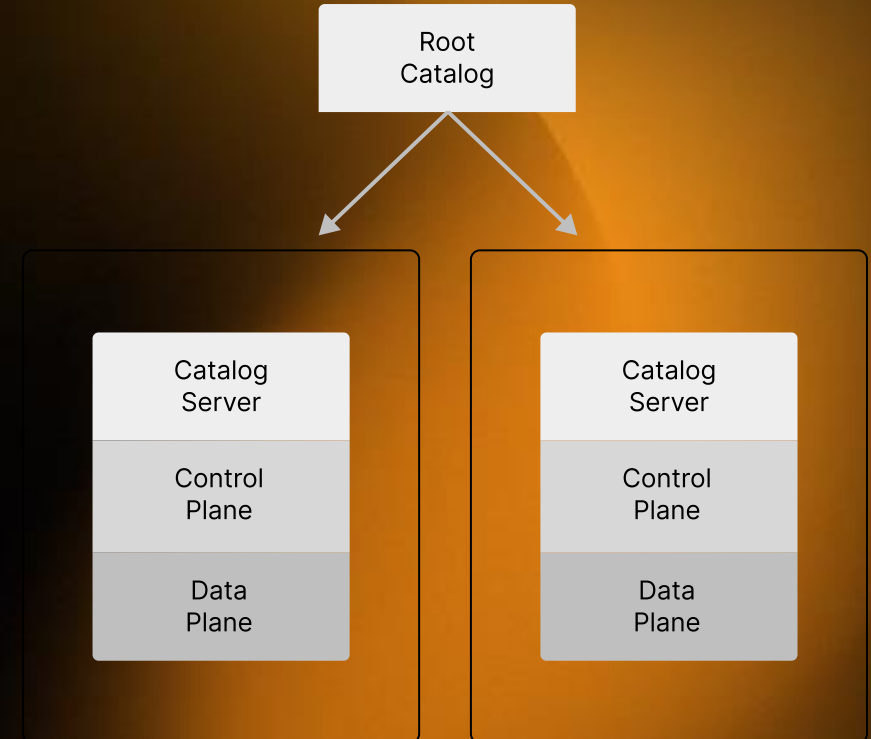
Agenda

- Identifying and addressing assets (Management Domains)
- Identity and EDC discovery
- Bring your own wallet
- Multi-trust issuance



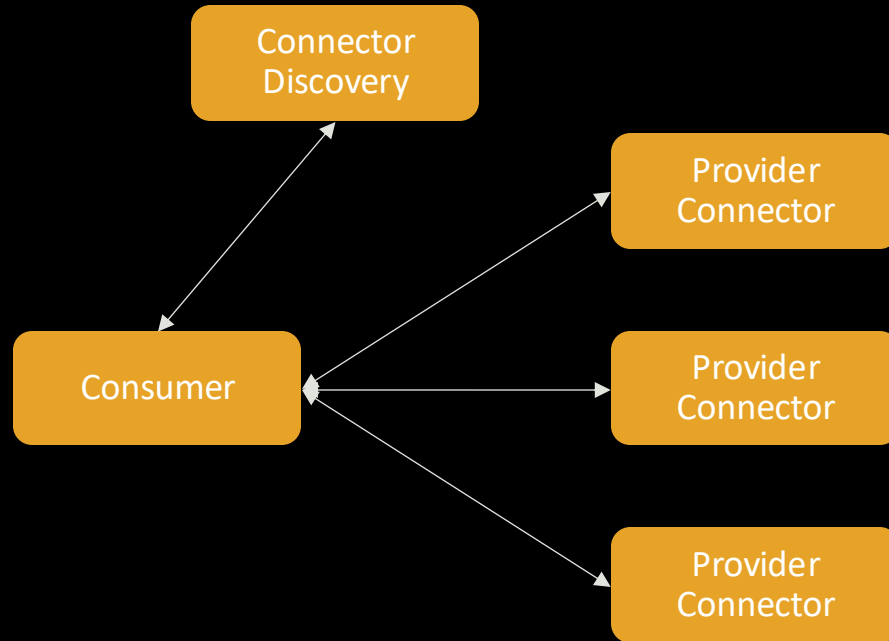
Management Domains

- Hierarchical Structuring of Connectors
- Decoupling of Catalog Service from Control Plane
- Robust Traversal from Root Catalog to Contract Offer





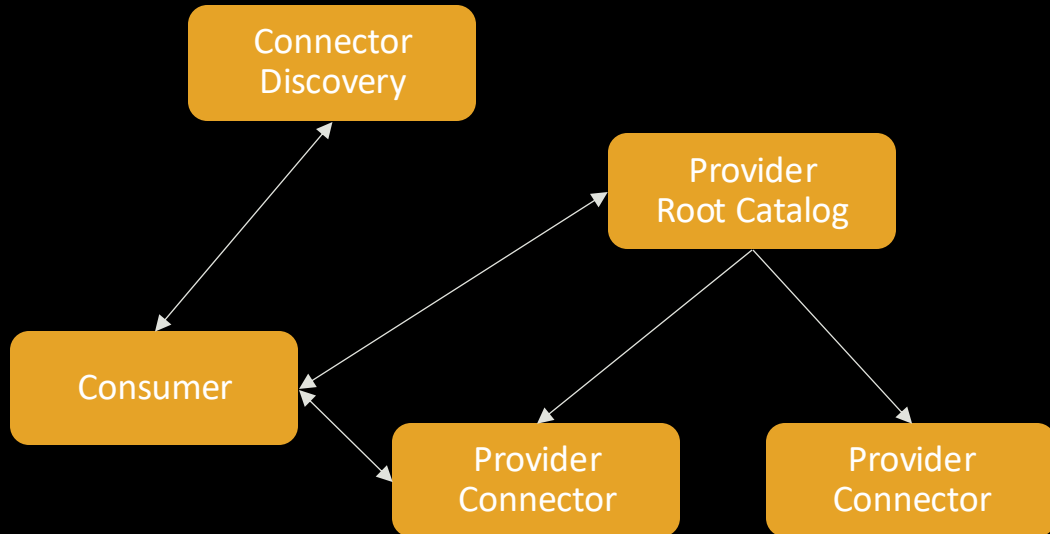
Asset Identification Today



- Provider register multiple connectors
- Consumer
 - receive list of connectors from connector discovery
 - retrieves catalogs from all registered connectors
 - identifies relevant asset from the right catalog
 - assumes the catalog connector to be also the asset connector
 - negotiates with the relevant provider connector for a contract



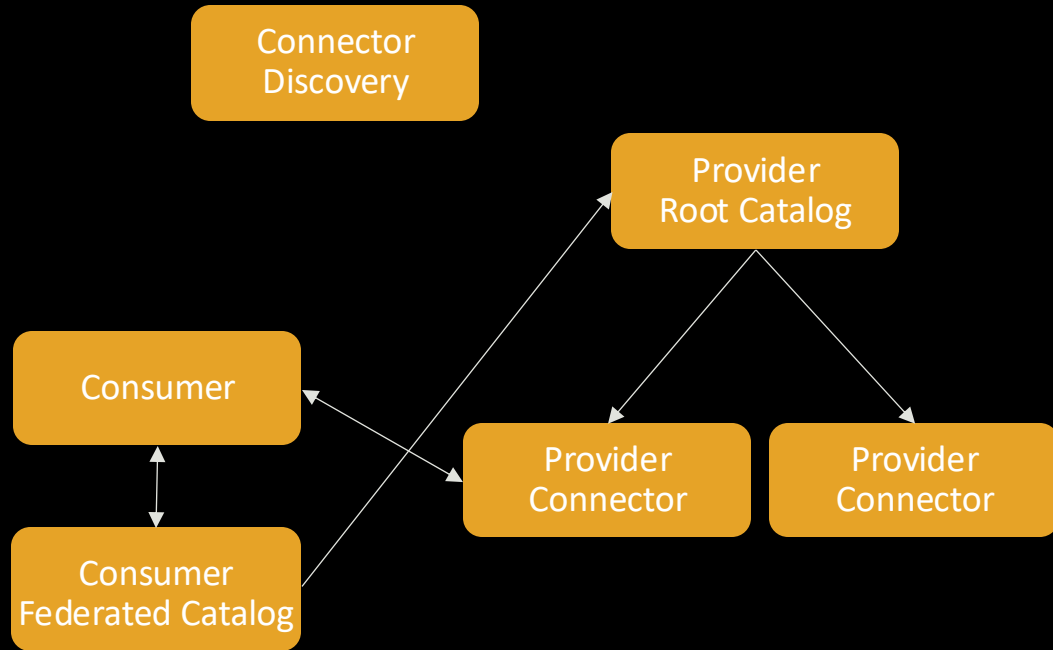
Management Domain Concept



- Provider register root catalog connectors
- Consumer
 - receive access to root catalog server
 - traverse hierarchical catalog entries in root catalog
 - identifies relevant asset from the final catalog
 - gets control plane uri for asset from the catalog
 - negotiates with the relevant provider control plane for a contract
- Multi-level hierarchies possible
- Catalog entries contain metadata to identify right path
- Decoupling of catalog and control plane
 - Other topologies possible



Federated Catalogs



- Provider register root catalog connectors
- Consumer
 - configures Federated Catalog cache to crawl provider catalog
 - retrieves a catalog from the local Federated Catalog cache (appropriate filtering applied)
 - identifies relevant asset from the cached catalog
 - gets control plane uri for asset from the catalog
 - negotiates with the relevant provider control plane for a construct
- Continuous crawling of relevant root and sub catalogs
 - Configured by the consumer
- Remote interaction starts with contract negotiation
- Disadvantages
 - Catalog crawling creates constant traffic (e.g., every 10 minutes)
 - Small window of unavailability



Management Domains – Conclusions

- Improved management of provider connectors
- Improved robustness of contract negotiations
- Less search effort for assets
- Better alignment to mainstream Dataspace Protocol

- Federated Catalogs as booster for response times

- Consumer application changes required

- Concepts for a mixed mode operation required
 - Keep all connectors registered at the connector discovery
 - Potentially change connector discovery to handle root catalogs specially

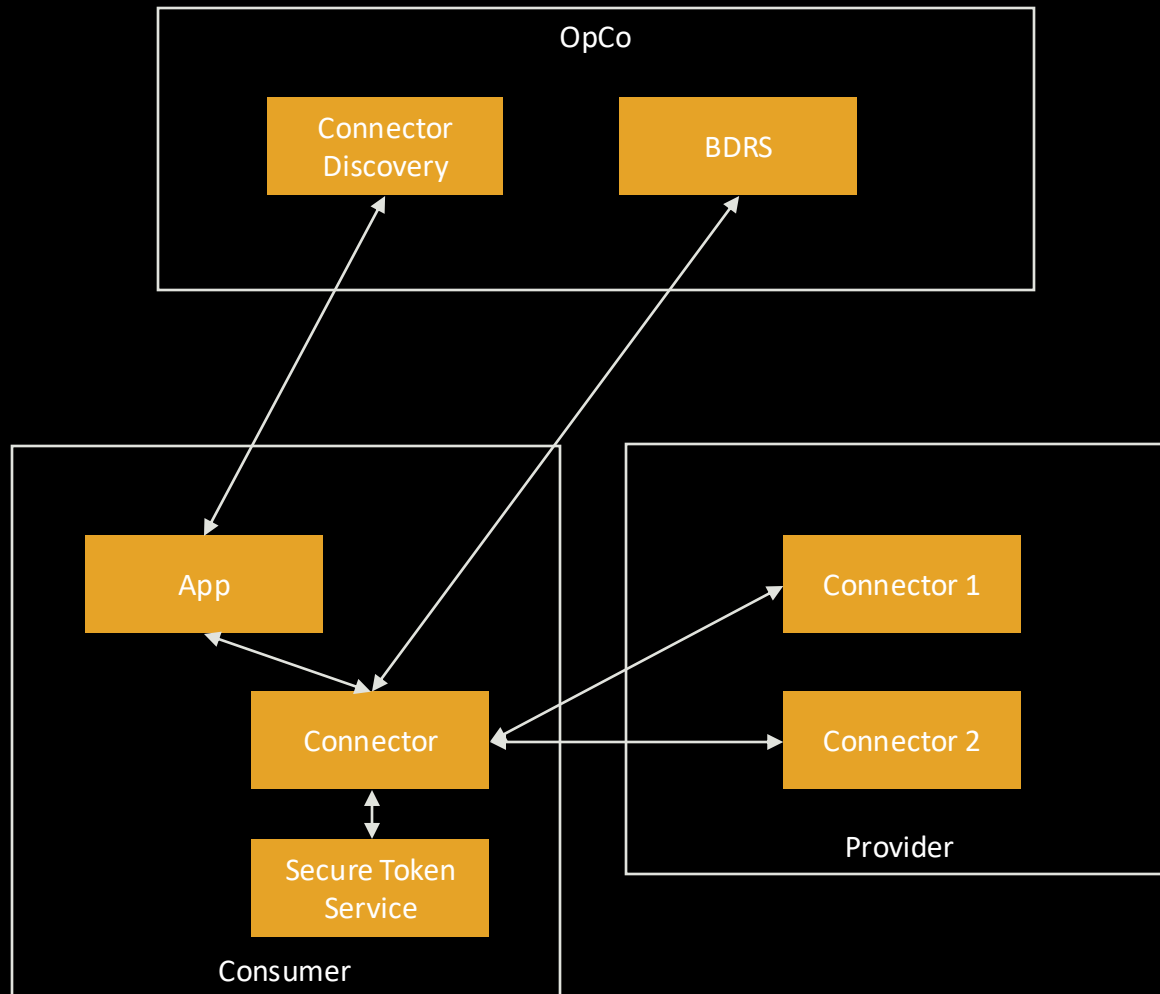


Harmonization of Technical Identity

- Catena-X data space development has a history
 - Parallel developments of concepts
 - Fundamental changes of concepts with legacy leftovers
 - Result:
 - Semantically questionable interaction of concepts, e.g., identities
 - Catena-X uses the Dataspace Protocol based technologies in a niche interpretation
 - Potentially higher maintenance efforts
- Goal: Harmonize concepts on the technical/protocol layer
 - Implement a semantically sound concept
 - Optimize decentralization
 - Get back to mainstream interpretation on how to apply the Dataspace Protocol



Current Flow



Start point: BPN of the Provider

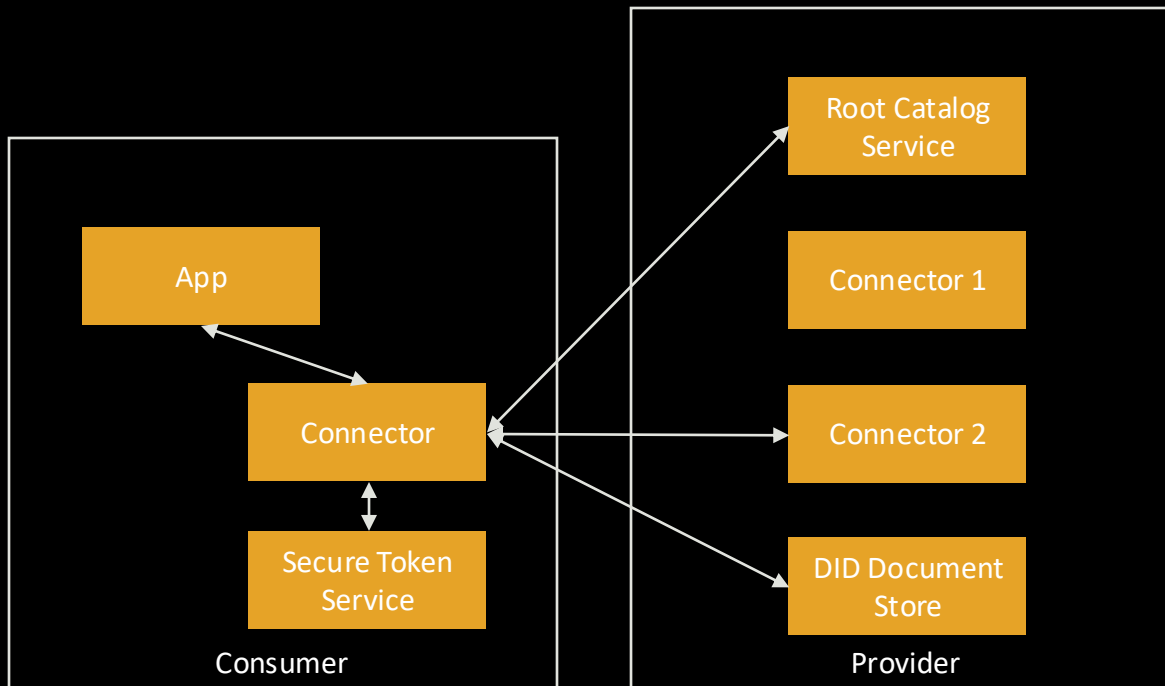
- Known by direct relationship
- Retrieved by BPN Discovery

Issues in Current Flow:

- Multiple requests, one for each registered connector to retrieve catalog
- Mixture of identities on technical level (BPN in request, DID in Token)
- Limited flexibility: A connector that shows an asset in its catalog also serves it
- Flow deviates from mainstream Dataspace Protocol interpretations on identity
- Additional central services required in data exchange workflows
 - Non-optimal decentralization
 - Potential data space disturbances due to bottlenecks



Target Flow



Start point: DID of the Provider

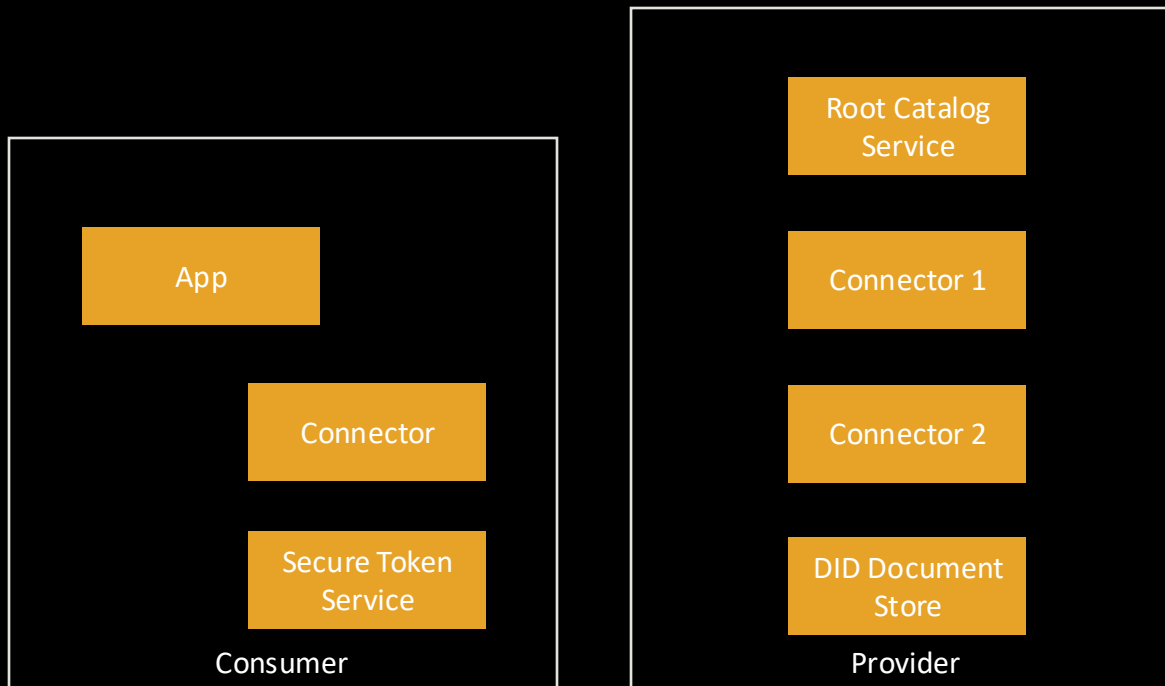
- Known by direct relationship
- Retrieved by BPN Discovery
- Retrieved from still available BDRS

Changes to current flow

- App requests root catalog from Consumer connector with DID as only parameter
- Consumer connector retrieves root catalog endpoint from DID Document
- Consumer connector uses Management Domain concept to retrieve catalog



Target Flow



Applied Concepts for Target Flow

- DIDs as technical identifiers
- Management Domains to organize multiple connectors

Advantages:

- Flow follows mainstream implementation of Dataspace Protocol
 - Improved interoperability
 - Improved future maintainability
- No central services in the data exchange
 - Improved decentralization
- Reduced number of requests with Providers that maintain many connectors
 - Further improvement potential with Federated Catalogs
- Semantical soundness concerning technical identity of partners
- Improved robustness by using the catalog endpoint reference for asset



Harmonized Identities – Consequences

- Consumer application changes required
 - Awareness of DID as technical identifier to initiate data transfers
 - No knowledge of connector endpoints is required, as this is resolved via the DID document
 - Support Management Domain concept to find the right asset in a connector hierarchy
 - Use of contract offer information to identify asset endpoint url
- Connector discovery will become obsolete, as the DID is the only element needed to initiate contact
- Adaptations to the BPN discovery to return DIDs
- Usage of the still available BDRS to retrieve DID for a BPN, now on application level
- DID to BPN mapping based on membership credentials required to support
 - BPN based authentication of data planes
 - Legal requirements concerning identity which is based on BPNs
- Concepts for a mixed mode operation of BPN and DID based connectors required
 - Identification of protocol of opposite connector
 - Internal mapping of BPN and DIDs for new connectors to enable interaction with BPN based connectors



Self-sovereign Identity (SSI) Evolution

Where did we come from?

- Central IdP setup with DAPS
- Companies didn't have
 - SSI wallets
 - attested SSI identity

Self-sovereign Identity (SSI) Evolution

Current State

- Decentral SSI setup with a single cloud wallet offering
 - BYOW is not possible
 - Each participants gets a new SSI wallet which can only be used in Catena-X
- Credentials issued from the operating company are injected to the holder wallet with a proprietary API
- EDC uses SSI for identification of communication partners
- Only one wallet implementation available (no open-source solution)
- Trust list with a single issuer
- Single operating company

Self-sovereign Identity (SSI) Evolution

Short Term Target

- Enable **BYOW**
 - Onboarding with an existing DID
- Enable the issuer to distribute verifiable credentials based on a **standard protocol**
 - DCP issuance
- Trust list with multiple issuers



The Future!

The journey is not over yet more exiting things are on the horizon and have to be evaluated:

- Company identities with EIDAS
 - Additional DID methods
 - Multiple issuers (operating company, ISO certificates, tax numbers)
- More Manufacturing-X projects are building on top of Catena-X
- Common trust list for multiple issuers
- Expansion to other regions (China, US)



Extension of the Onboarding Process

Participants should have the possibility to

- enter their already **existing DID**
- **identify** with existing verifiable credentials



Extension of the Issuer Component

The issuer should

- use a **common protocol** to transfer verifiable credentials to the holder
- **publish the credential types** that can be requested
- provide the possibility to **offer credentials** to a holder (revocation of the signing key)

EXAMPLE 10: IssuerMetadata

```
{
  "@context": [
    "https://w3id.org/dspace-dcp/v0.8",
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "type": "IssuerMetadata",
  "credentialIssuer": "did:web:issuer-url",
  "credentialsSupported": [
    {
      "type": "CredentialObject",
      "credentialType": [
        "VerifiableCredential",
        "CompanyCredential"
      ],
      "offerReason": "reissue",
      "bindingMethods": [
        "did:web"
      ],
      "cryptography": [
        "JsonWebSignature2020", "eddsa-rdfc-2022", "eddsa-jcs-2022", "..."
      ],
      "issuancePolicy": {
        "permission": {
          "action": "use",
          "constraint": {
            "and": {
              "leftOperand": "CredentialPrereq",
              "operator": "eq",
              "rightOperand": "active"
            }
          }
        }
      }
    }
  ]
}
```

[source](#)



Credential Request triggered from a Holder

Holders should

- have the possibility to **request verifiable credentials** from the issuer
- processes credential offers of a known issuer
- Have the possibility to select an open-source wallet implementation

Identity hub

Request Verifiable Credentials from an Issuer



Only for visualization

Credentials Select an application Issue Import **Request**

Received **Created**

Search

CO2 Footprint
Certificate of CO2 Footprint

Type: CO2Footprint
Issued: Sep 25, 2024, 6:51:00 PM
Expires: Nov 25, 2024, 5:51:00 PM
Assigned to: **Continental-App**

CO2 Footprint
Certificate of CO2 Footprint

Type: CO2Footprint
Issued: Sep 25, 2024, 6:51:00 PM
Expires: Nov 25, 2024, 5:51:00 PM
Assigned to: **Continental-App**



Request Credential

Application: Catena-X

Issuer: Cofinity-X (did:web:cofinity-x.com)

Type: VerifiableCredential BPN x Membership x

Request Cancel



Multiple Trusted Issuers

The trust list should be extended

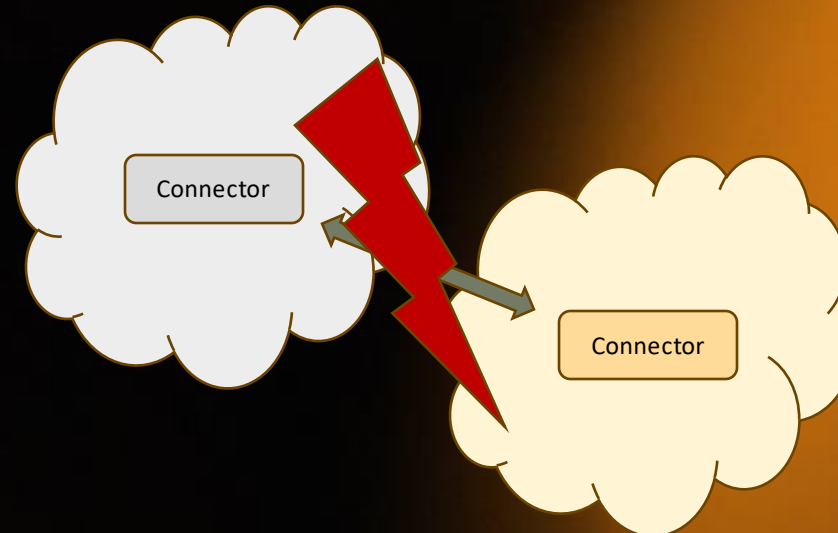
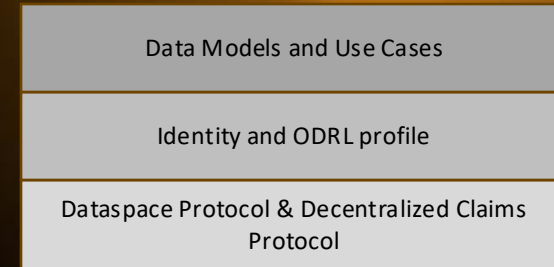
- to support more than one entry
- to be distributed to multiple EDCs, wallets



Interoperability

- Interoperability of data space not distinguishable from multi-issuance
 - Direct interoperability requires compatibility on all layers
 - Given that, the data spaces merge and differ only on issuers
- If some stack layer is incompatible, a connector
 - technically acts in two different data spaces
 - following two different operation stacks
- Interoperability not targeting the whole stack will require
 - Bridge solutions
 - Contractual agreements on identity acceptance
 - E.g., Ouranos case

Interoperability Stack:





Where do we go tomorrow?

- Further decentralization of data exchange
- Greater decoupling from core services
- Improved consistency in network services
- Better alignment in technology stack to improve interoperability
- Compatibility with other SSI initiatives
- Availability of Open-Source Wallet implementation