gaia-x

Tech-X & Hackathon #9

2026 28-29 MAY ATHENS GREECE

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

Agenda | Day 2 (Morning) | 29.05.26

	Time	Slot	Speaker(s)
CONNECTOR	9:30 – 10:15	EDC + OID4VC (+ Gaia-X Credentials)	▪ Bowen Chong (Circular Solutions) ▪ Julien Foliot (Gaia-X)
GAIA-X LAB	10:15 – 10:45	Gaia-X Loire Participant Credential Wizard	Ryan Reychico (Gaia-X Lab)
TECH	10:45 – 11:00	An ODRL Profile to join them all for Data Spaces	▪ Joaquin Salvachua (UPM) ▪ José Muñoz (UPM)
	11:00 – 11:30	Networking Coffee & AR Game	
CONNECTOR	11:30 – 11:45	From Standard to Open Source Stack: Implementing Trusted Data Transaction with the Gaia-X Framework and Data Transfer Agent	▪ Benoit Tabutiaux (IMT) ▪ Frederic Bellaiche (Dawex)
CONNECTOR	11:45 – 12:00	One Connector Many Sovereigns: A Multi-Tenant for Low IT Participants	Sava Stanojevic (MicelioData)
CONNECTOR	12:00 – 12:15	Simpl-Open IAA (Identification, Authentication & Authorization) SSI Tier 2 Implementation: The Gaia-X ICAM Semantic Model in Action+B16:B28	Pietro Bartoccioni (Aruba)
CONNECTOR	12:15 – 12:45	The Eunomia Agentic Connector	▪ Joaquin Salvachua (UPM) ▪ José Muñoz (UPM)
GAIA-X LAB	12:45 – 13:00	Gaia-X CTO Team – Q&A	Gaia-X CTO Team
	13:00 – 14:00	Networking Lunch & AR Game	

#GaiaX #TechX

EDC with OID4VC (+ Gaia-X Credentials)

09:30 – 10:15

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

EDC + OID4VC + Gaia-X Trust Protocol

Necessary Changes

OID4VC

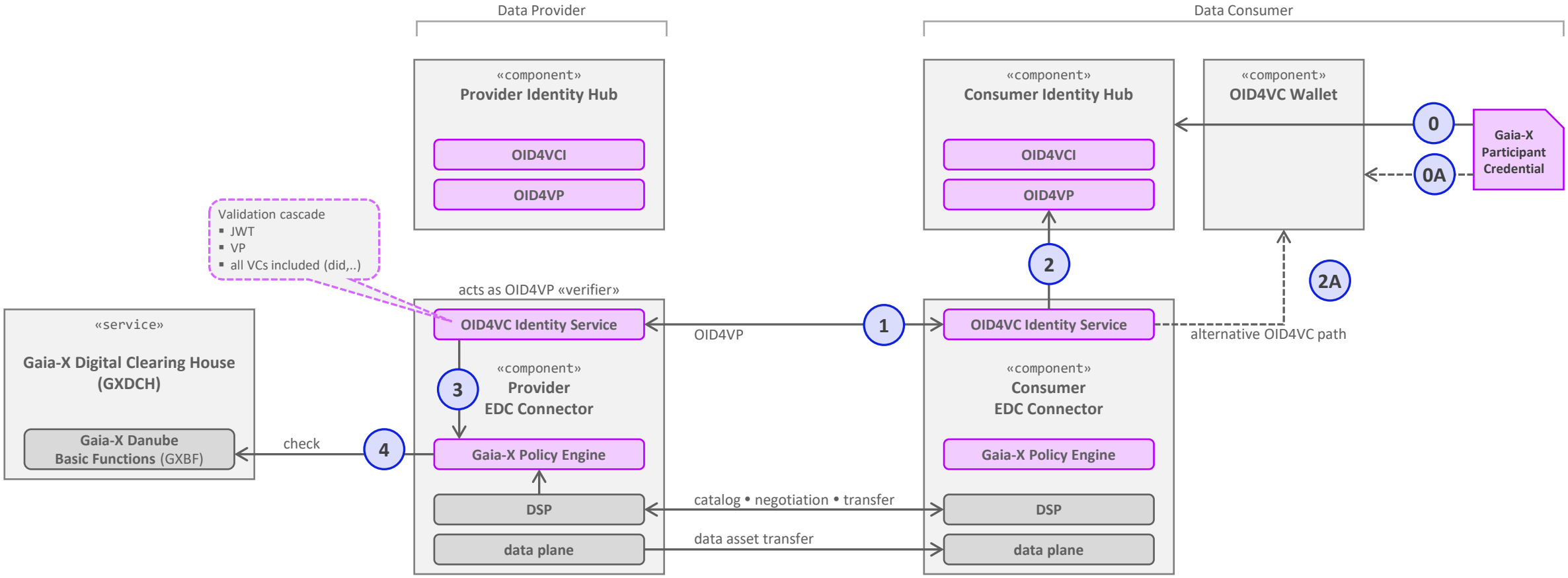
- Identity Hub
  - provide an OID4VC port (like the existing DCP port)
- EDC Connector
  - OID4VC extension ⇔ Identity Hub
  - OID4V extension ⇔ other EDC Connector

Gaia-X Compliance

- EDC Connector
  - “GXDCH-compatible” policy engine

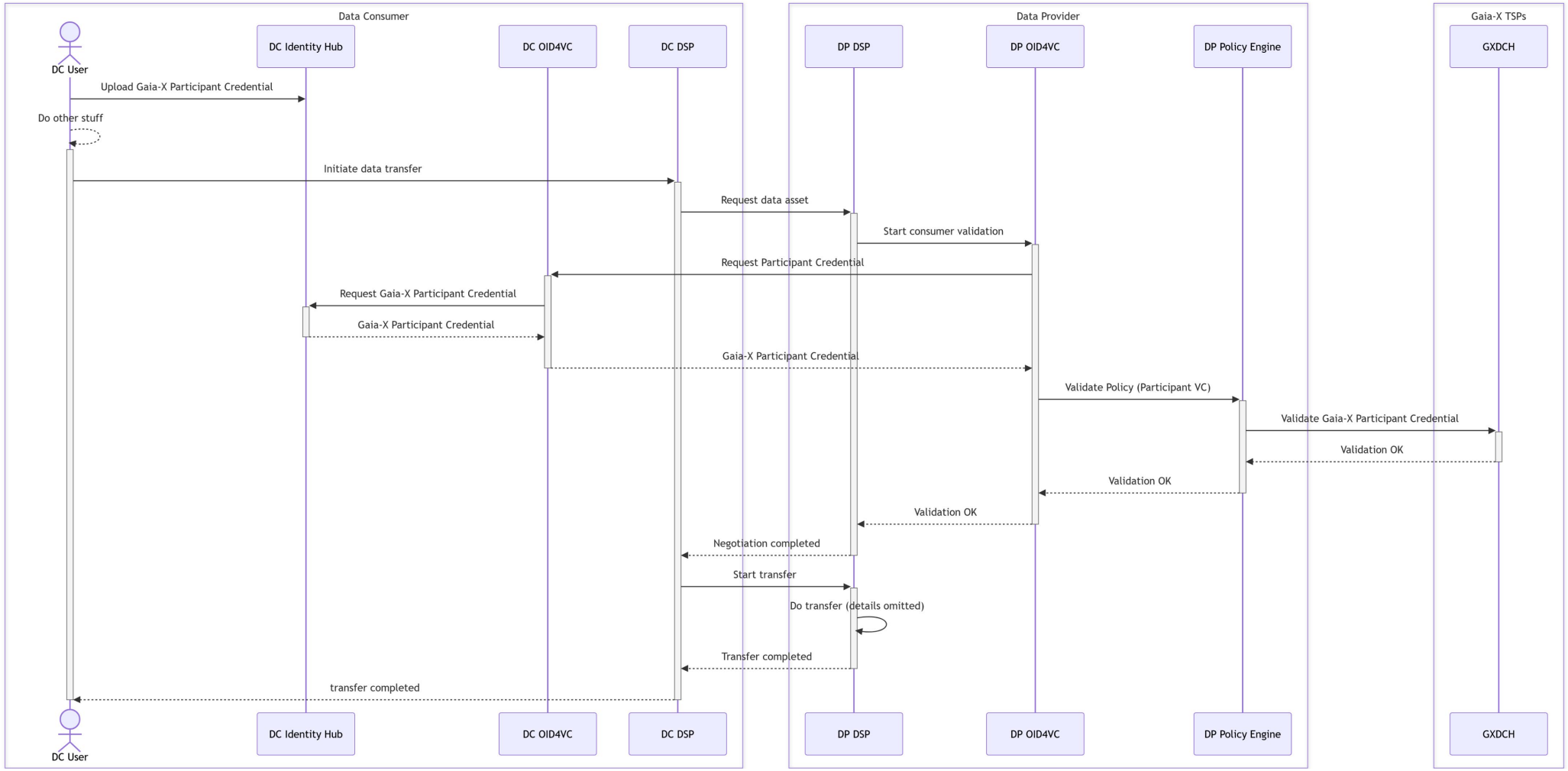
MVD
minimum viable data space

EDC with OID4VC Extension
Architecture



EDC with OID4VC Extensions

Sequence Flow



Thank you!

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

EDC+OID4VC Demonstration

09:30 – 10:15

- **Bowen Chong –** Circular Solutions

In partnership with

EDC + OID4VC Demonstration

gaia-x

9:30 AM CIRCULAR SOLUTION

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

EU is building the wallet ecosystem on OpenID4VC

- eIDAS 2.0 in force since May 2024
- EUDI Wallet (citizens) issued by 2026 - Mandatory acceptance by 2027
- EU Business Wallet (EUBW) - wallet for legal entities, announced under the Commission's Competitiveness Compass (late 2026 target). designed explicitly for industrial dataspaces over DSP
- Both wallet's technical specs and the Commission's reference implementations are built on OpenID4VCI + OpenID4VP

Sources: EUR-lex 2024/1183 - github.com/eu-digital-identity-wallet

EDC ships DCP, not OID4VC

- EDC's identity stack: Eclipse Decentralized Claims Protocol (DCP)
- DCP roadmap: no mention of OID4VC bridge or replacement
- No open EDC issue committing to OID4VC support

> *By 2027, EU relying parties have to accept OID4VC*
> *EDC today cannot speak it.*

Gaia-X already chose OID4VC

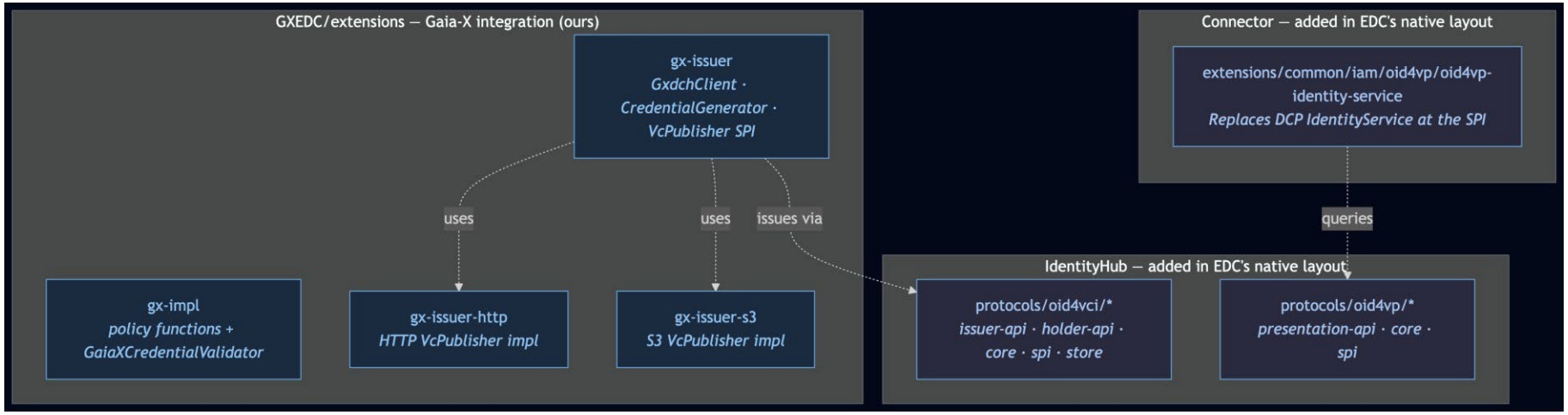
- Gaia-X ICAM Document 25.11 - adopted standards and protocols: “OID4VC, OID4VCI, OID4VP”
- Gaia-X uses OID4VCI for issuance and OID4VP for presentation across user, wallet, GXDCH

> *We are only building the implementation that brings EDC dataspaces into the one Gaia-X already published. not changing the direction*

Use Cases

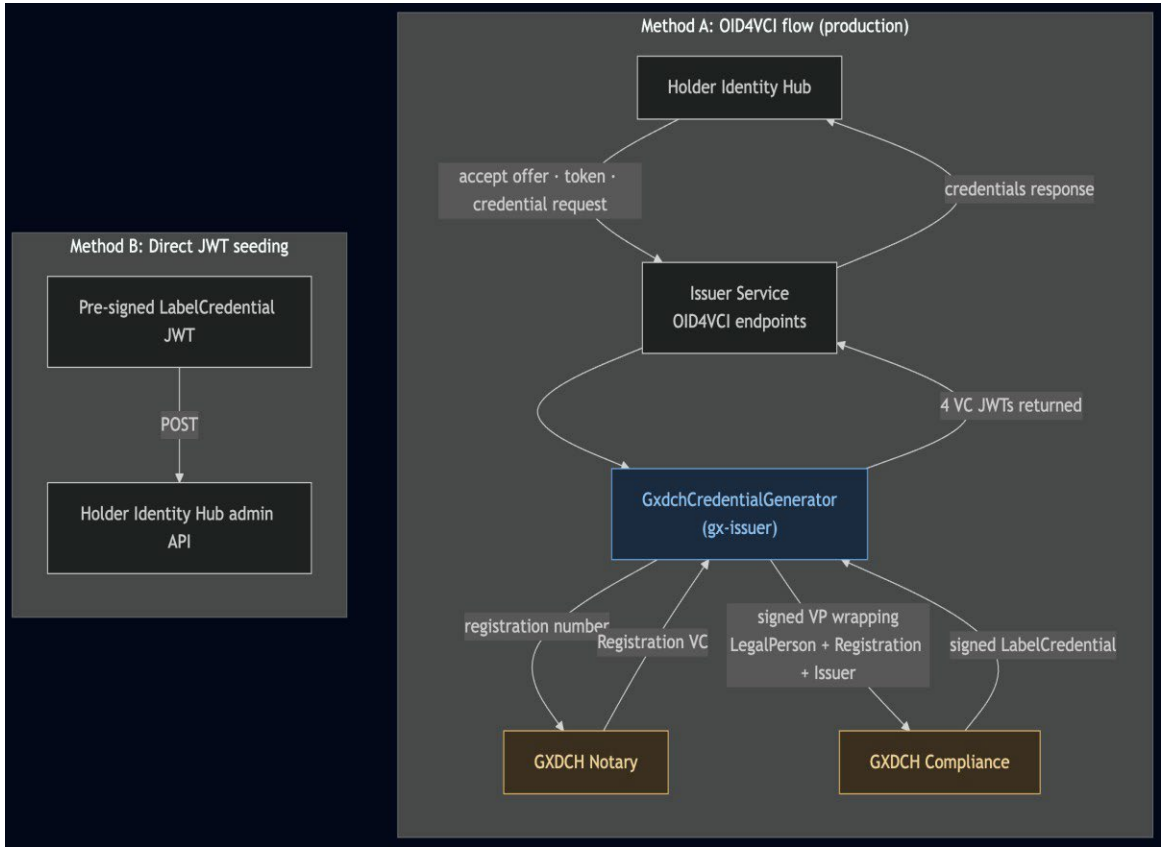
EU Regulatory Alignment	Ecosystem Interop	Sovereign data exchange
eIDAS 2.0 + EUDI Wallet built on OpenID4VC	Any OID4VC compliant wallet or issuer works	Contracts and transfers gated by Gaia-X notarised LEI/VAT
DCP needs a bridge or replacement	No longer stuck in the DCP bubble	OID4VC makes the notary a pluggable issuer (Gaia-X is the trust anchor)

Project Structure



- gx-impl - evaluates VP at every catalog/negotiation. Calls GXDCH Compliance for live verification
- gx-issuer - builds the 3 supporting VCs, wraps them as a signed VP, and calls GXDCH compliance for LabelCredential
- gx-issuer-s3/http - writes vc payloads to operator-owned public locations for runtime policy verification
- Connector (oid4vp-identity-service) - replaces EDC's DCP IdentityService at the SPI boundary
- IdentityHub (protocols)
  - oid4vci - issuer APIs, holder APIs, core, spi and store
  - oid4vp - presentation APIs, core and spi

VC Issuance



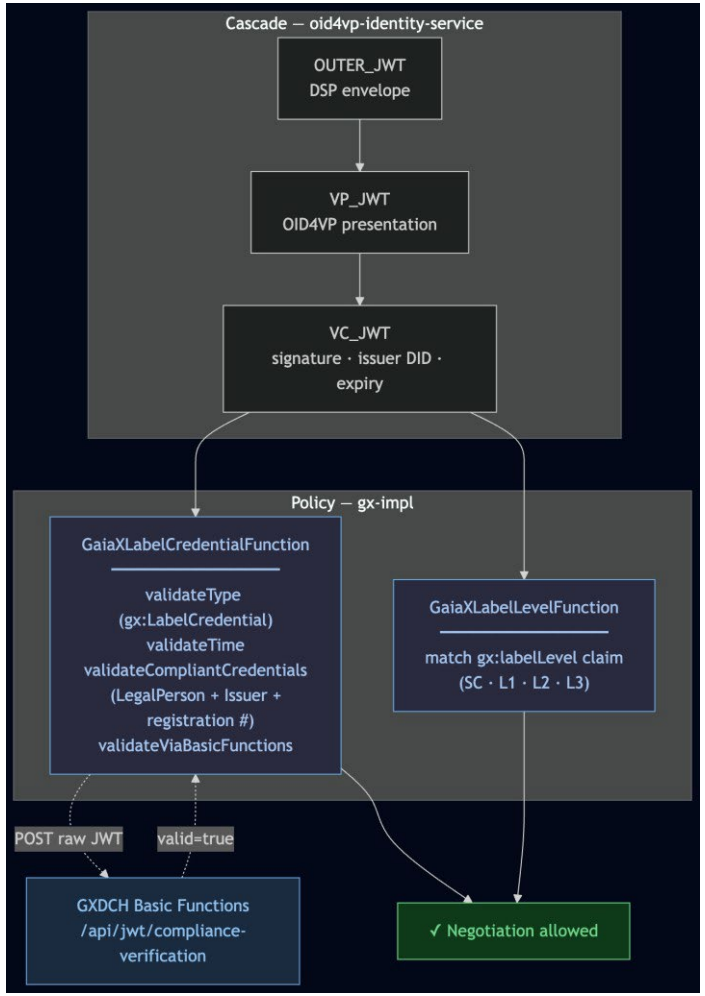
Method A - OID4VCI flow

Holder requests an offer →token → credential. GxdchCredentialGenerator fetches the Registration VC from GXDCH Notary, builds and signs the LegalPerson and Issuer VCs locally, wraps and signs all 3 VC in a VP then POSTs it to GXDCH Compliance. Compliance returns the signed LabelCredential and all 4 VCs flow back through the credentials response and land in the holder's Identity Hub

Method B - Direct JWT seeding

Pre-signed LabelCredential JWT POSTed directly into Holder Identity Hub admin API.

Verification Cascade



- Three layers of JWT Verification: Outer →VP →per-VC
- Plus the GXDCH compliance hop as a final external check
- Every step emits an SSE event
- Operators see exactly where any failure happens, in realtime

Demo Items

No.	Item	Action
1	OID4VC Credentials	Test the verification chain with credential variants and observe failures live via verification events
2	Policy Gating	GaiaXLabelCredential and GaiaXLabelLevel policies on a provider asset.
3	End-to-end DSP flow	Standard EDC data exchange

Live Demo

Roadmap

- Contribute to upstream Eclipse EDC - propose the OID4VC modules as contribution into EDC's own iam/oid4vp, protocols/oid4vp and protocols/oid4vci
- Bitstring Status List - vc revocation status checking
- Move VC hosting into the Identity Hub by default (operators no longer need to provision external storage).
- Hardening, spec validation and testing
  - Interop + spec compliance tests with the Gaia-X CTO Team
  - Real-world performance and reliability benchmarks via our platforms

Thank you!

Bowen | bowen.chong@circularsolution.co.kr

- **Main Repository** | https://github.com/Circular-Solution/GXEDC
- **Identity Hub Fork** | https://github.com/yamazhen/IdentityHub
- **Connector Fork** | https://github.com/yamazhen/Connector
- **Email** | bowen.chong@circularsolution.co.kr

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

Gaia-X Loire Participant Credential Wizard

10:15 – 10:45

- **Ryan Reychico –** Gaia-X

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

Key Takeaways What we'll cover today

What you'll learn in this session

1. **Compliance Document:** How the Policy Rules Committee (PRC) defines the rules of the Gaia-X ecosystem.
2. **Participant identity:** What it means to be a recognised as a Gaia-X Participant compliance.
3. **Trust credentials:** The three Verifiable Credentials (VCs) required for compliance.
4. **Decentralised identity:** DIDs, X.509 certificates, and Trust service provider.
5. **Hands-on Wizard:** Generating your Participant Compliance Credential, step by step.

Goal: You will be ready to onboard as a Gaia-X Participant.

Who defines the rules? The Policy Rules Committee (PRC)

The governing authority for compliance

- The Policy Rules Committee (PRC) is the official Gaia-X body that defines what compliance means across the ecosystem.
- It publishes the binding Compliance Document — current version v2.5.0.

Reference: docs.gaia-x.eu/policy-rules-committee/compliance-document/2.5.0/criteria_participant/

What is a Gaia-X Participant Compliance?

The foundational identity in the Gaia-X ecosystem

- A Gaia-X Participant is a legal or natural person formally recognised within the ecosystem.
- Participants can take on multiple roles: consumer, producer, federator, operator, and more.
- To be recognised, a Participant must obtain a Gaia-X Compliance Credential.

The Three Verifiable Credentials Required for Gaia-X compliance

Three credentials. One Compliance Credential:

1. Legal Person: describes the organisation (legal name, headquarters, address), built on the Gaia-X Legal Person ontology.

2. Legal Registration Number (LRN): proves the organisation's legal existence (EORI, VAT ID, LEI Code).

3. Terms & Conditions: the organisation commits to keeping its credentials current and to the integrity of its claims.

→ The three VCs are submitted together to a Clearing House, which issues the Participant Compliance Credential.

The Legal Registration Number Verified by Clearing Houses

How trust is anchored end-to-end

- The LRN VC cannot be self-signed, it must be issued by a trusted registration number notary.
- The registration number notary validates the registration number against official registries (EORI, VAT, LEI).
- The resulting VC is then accepted and validated by the Clearing Houses.
- Clearing Houses only accept credentials anchored to Trust Service Providor (eIDAS, EV SSL certificates).

→ This chain is what makes Gaia-X compliance trustworthy across the entire ecosystem.

What is a DID? And why you need one

gaia-x

Your self-controlled identifier in Gaia-X

- A DID (Decentralised Identifier) is a globally unique, self-controlled identifier.
- Not tied to any central authority, you own it.
- In Gaia-X, your DID Document contains the cryptographic proof under which your VCs are issued and signed.

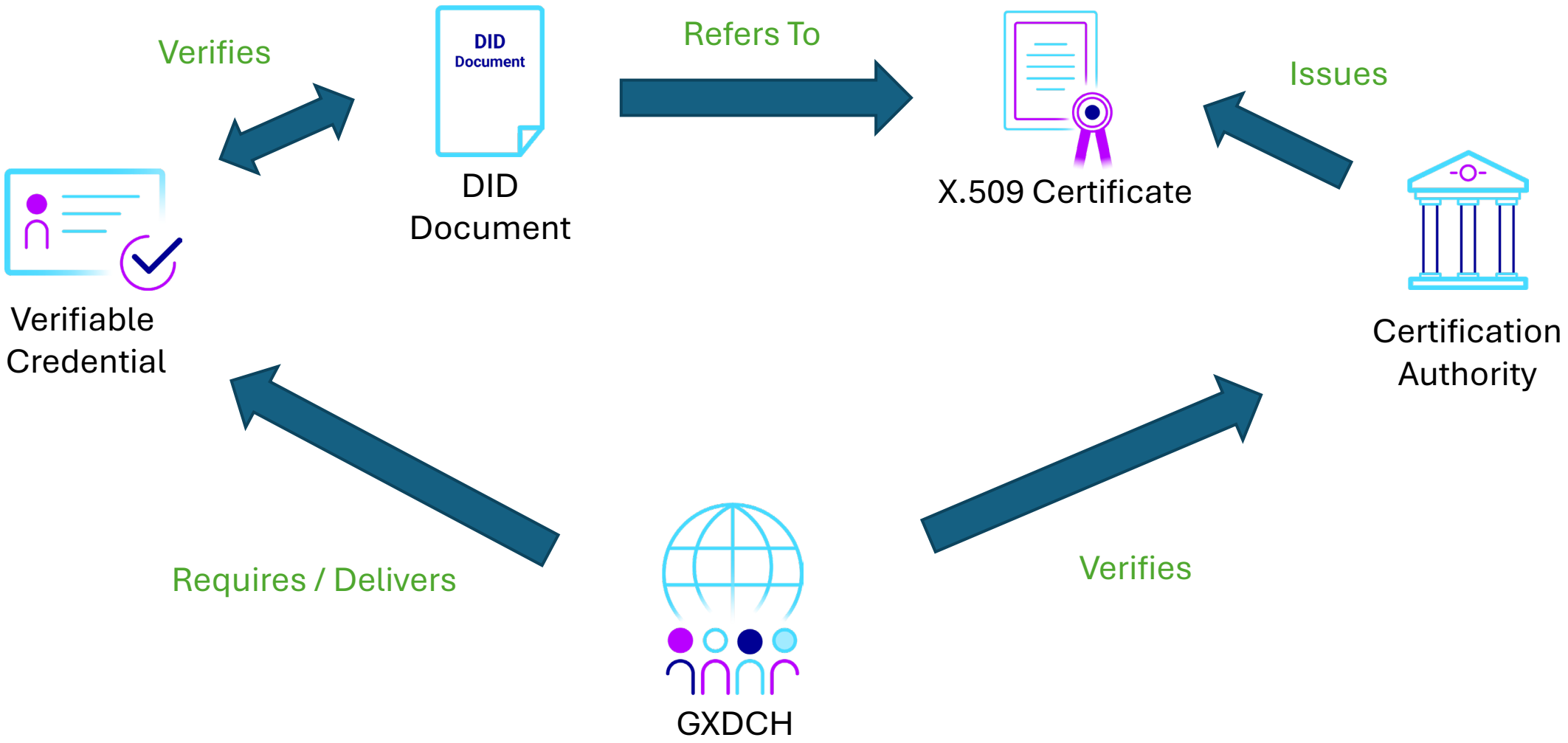
W3C standard: www.w3.org/TR/did-core/

The DID and the X.509 Certificate

Anchoring your DID to a recognised Trust Service Provider

- Your DID document must reference an X.509 certificate (and public key).
- What is an X.509 certificate? A digital certificate issued by a trusted Certificate Authority (CA) that binds a public key to an identity, the same technology used by HTTPS.
- In Gaia-X, the certificate must come from a Trust Service Provider recognised by the PRC (eIDAS qualified certificates, EV SSL, etc.).

→ This certificate is what gives your DID, and every VC you sign, its trustworthiness in the eyes of the Clearing Houses.


Verifies
DID Document
DID Document
Refers To
X.509 Certificate
Issues
Certification Authority
Verifiable Credential
Requires / Delivers
GXDCH
Verifies

You're ready Let's use the Wizard

gaia-x

Everything is in place, time to run the Wizard.

Prerequisites checklist

- ✓ Your private key
- ✓ Your DID (hosted and resolvable)
- ✓ Your X.509 certificate (linked to your DID)
- ✓ Your Legal registration number (EORI / VAT / LEI)

LIVE DEMO

Gaia-X Participant Credential Wizard

Useful Links Documentation and references

Resources to go further

- Live Wizard wizard.lab.gaia-x.eu/
- PRC Compliance Document v2.5.0 docs.gaia-x.eu/policy-rules-committee/compliance-document/2.5.0/
- Participant Criteria docs.gaia-x.eu/.../criteria_participant/
- W3C DID Standard www.w3.org/TR/did-core/
- Gaia-X Trust Anchors docs.gaia-x.eu/.../Gaia-X_Trust_Anchors/

Q&A

Your turn.

Happy to take any questions on the Wizard, the credentials, or the wider Gaia-X workflow.

https://wizard.lab.gaia-x.eu/

Thank you!

Ryan REYCHICO| ryan.reychico@gaia-x.eu

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

An ODRL Profile to join them all for Data Spaces

10:45 – 11:00

- **Joaquin Salvachua & José Muñoz** – Polytechnic University of Madrid

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

An ODRL Profile to join them all for Data Spaces

Joaquín Salvachúa
Andres Muñoz

Universidad Politécnica de Madrid

UNIVERSIDAD POLITÉCNICA DE MADRID

Information Processing and Telecommunications Center

In partnership with

Mission

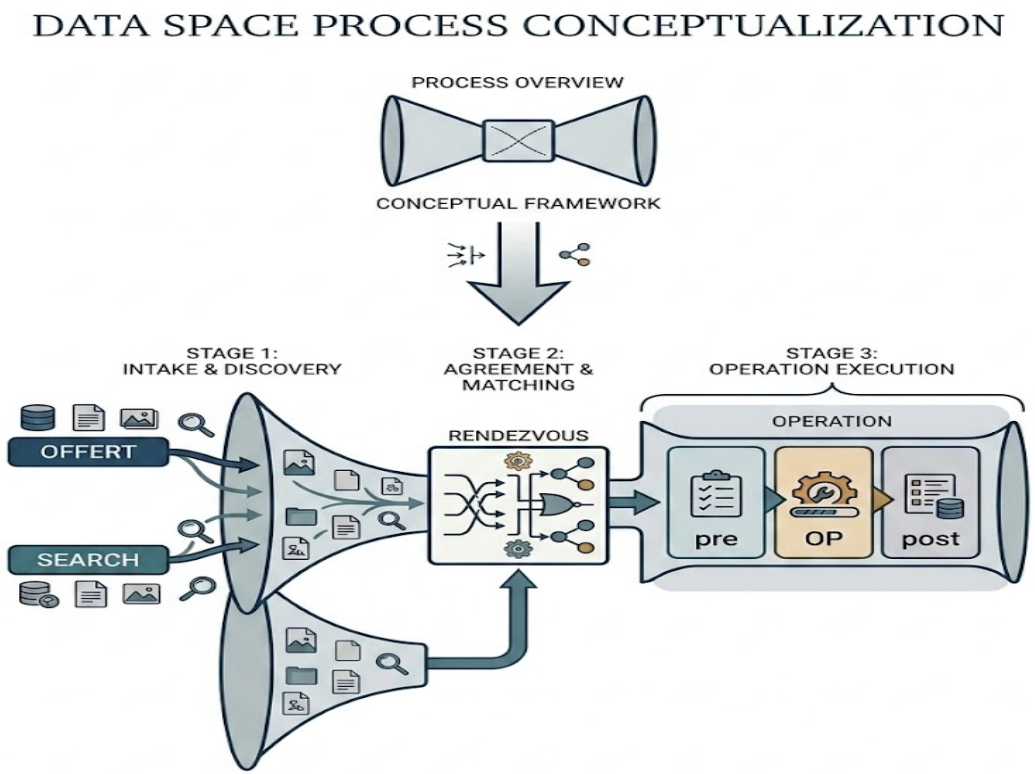
- Data Spaces has a complex workflow, that could be slightly different on each implementation.

- Have a profile that serves as container for all the different uses of ODRL that may be involved into data spaces.

- More to come (catalog searching and others).

- https://w3c.github.io/odrl/profile-bigdata/
- (note big data was the initial name since they do not know about data spaces)

One profile to bind them all
Serving as container for a given dataspace



DataSpace offering to be publish in catalog

ODRL with RDF serialization is NOT for normal Humans.

Proposals

- ODRL4H : arrow notation
- Graphical notation based on Blockly (ongoing work)
- Set notation to indicate all posible offering + semantic anotation:
  - Must / May /Maybe on the offers ODRL statements.

ODRL4H

Use arrows -> to indicate action and prohibitions.

- # Permission with condition
- DataOwnerX -> Permit -> Action(Read) -> Asset(Report_2026) -> Condition(<= "2026-12-31")
- # Prohibit Action
- DataOwnerX -> Prohibit -> Action(Anonymize) -> Asset(Report_2026)
- # Obligation
- DataOwnerX -> Oblige -> Action(Read) -> Asset(Report_2026)

The Sidecar Pattern (policy-env.yaml)

All the URL needed for rdf. So ODRL4H.txt + policy-env.yaml

https://github.com/EunomiaUPM/Odrl4Humans

Set notation

The ODRL4H language maps directly to the ODRL 2.3 Information Model. We define the vocabulary of the language using the following discrete mathematical sets:

- $\mathbb{P} = \{p_1, p_2, \ldots, p_n\}$: The set of all valid **Parties** (e.g., *Assigners* and *Assignees* resolved via the environment lookup).
- $\mathbb{R} = \{\text{Permit}, \text{Prohibit}, \text{Oblige}\}$: The strict, finite set of core **Rule Types**.
- $\mathbb{A} = \{\text{Action}(a_1), \text{Action}(a_2), \ldots\}$: The set of all executable **Actions**.
- $\mathbb{E} = \{\text{Asset}(e_1), \text{Asset}(e_2), \ldots\}$: The set of all target **Assets** (Entities).
- $\mathbb{C} = \{\text{Condition}(c_1), \text{Condition}(c_2), \ldots\}$: The set of all logical **Constraints** mapping to ODRL leftOperand, operator, and rightOperand.
- $\mathbb{D} = \{\text{Duty}(d_1), \text{Duty}(d_2), \ldots\}$: The set of all subsequent **Duties** (Obligations) attached to a permission.

$$\Sigma \equiv p_{src} \xrightarrow{\text{MAYBE}} r \xrightarrow{\text{MUST}} a \xrightarrow{\text{MUST}} e \xrightarrow{\text{MAY}} p_{dst} \xrightarrow{\text{MAY}} c \xrightarrow{\text{MAYBE}} d$$

We must go to the rendezvous

After searching in the catalog the DCAP-AP metadata must include an offer like ODRL.

We must instantiate it with a rendezvous negotiation

Semantics should be more formal specified (also on what may be the compensations and are one or a process).

After this we transform the Set notation in the normal ODRL profile

Operations

Pre conditions :

Previous to start working what must be fullfilled

What trust framework/model are we using.

Part of the Access control : Use Rebac (Google zanzibar) model in order to specify what data you could connect with:

Translate into ETL commands that do not Access data no allowed.

Ongoing stremming datra dycamically restrain data produced to be transmited.

Operations

Normal conditions just enforced

Data usage control :: impact on data sovereignty

- Use / Process: Performing computations or algorithmic transformations on the dataset without modifying the primary source.
- Aggregate: Combining the dataset with other third-party sources to generate synthetic metrics or insights.
- Anonymize / Pseudonymize: Redacting or altering identifiers in real-time before data lands in secondary environments.

Post operation

Post conditions

Related to ensure some actions are done:

- Copy / Store: Writing the data to local persistent storage (caches, databases, file systems).
- Share or transmitting the data provider's assets to a third-party actor outside the initial transaction boundary.
- Delete / Purge: Cryptographically shredding or erasing the data from all consumer-controlled environments.

Studing the relationship with a posible governance layer (actions and events between both layers). Ongoing work.

The key is how to ensure this in the platform => produce a detector for this environment as agent.

Ongoing work on the W3C ODRL group

First version about to be publish on june.

ODRL group temporal closing and reopening to add the full specification of the proposal specification.

Reopen the sub specificacions in september.

Input for the forecoming future of ODRL brainstorming meeting.

Future work

Develop all the sub profiles (some are done, while others are ongoing).

Check the proper integration of different transpilation process.

Offer an Open Source tool that integrates this with data spaces (Eunomia) :: END SEPTEMBER.

Thank you!

Name| email

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

Networking Coffee/AR Game
11:00 – 11:30

From Standard to Open Source Stack: Implementing Trusted Data Transactions with the Gaia-X Framework and the Data Transfer Agent

Benoît TABUTIAUX, PhD, CTO at Teralab - IMT Transfert

Frédéric BELLAICHE, PhD, VP Research & Technology at Dawex

In partnership with

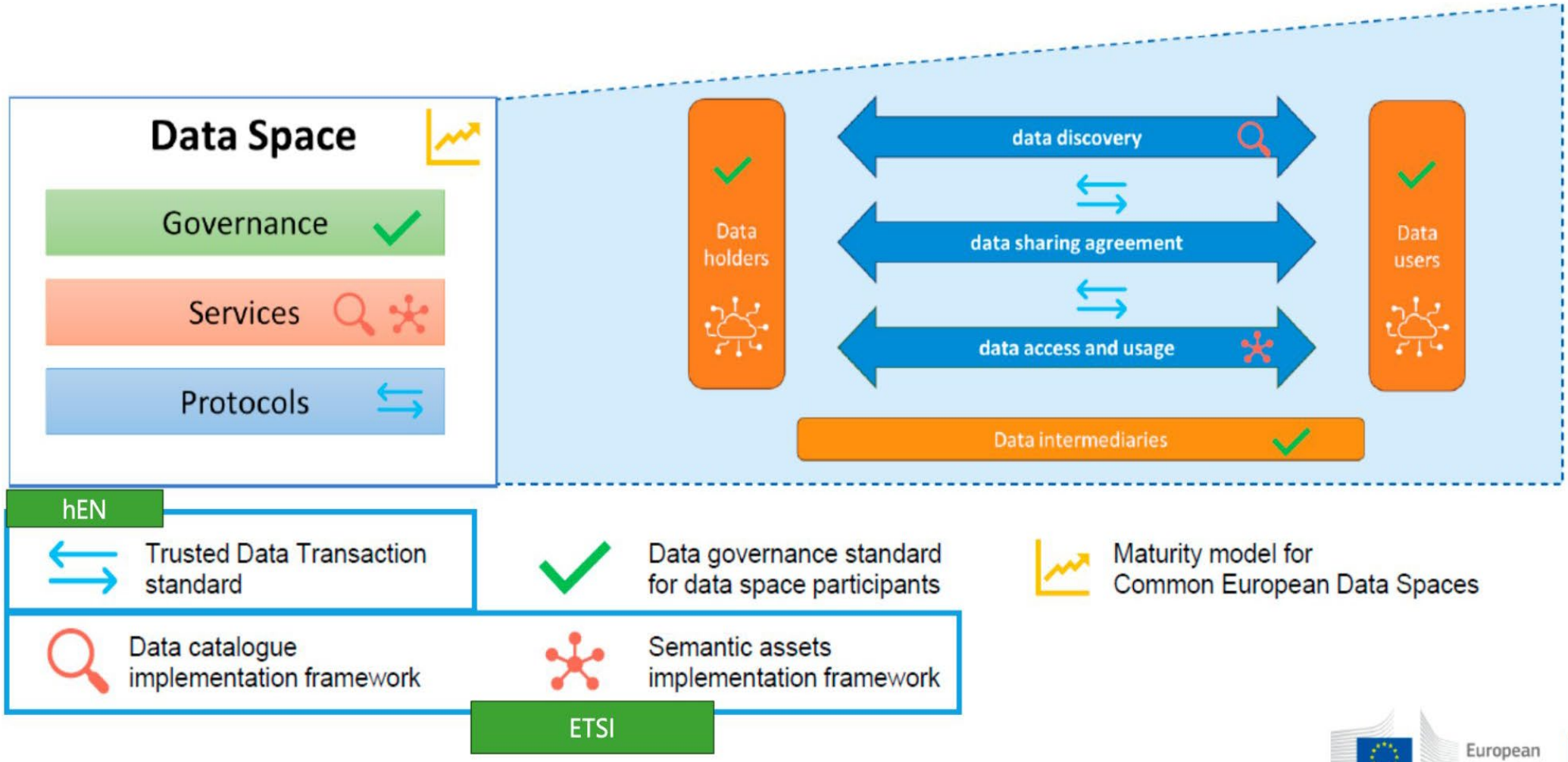
gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

Friday 29 May – 11:30

gaia-x

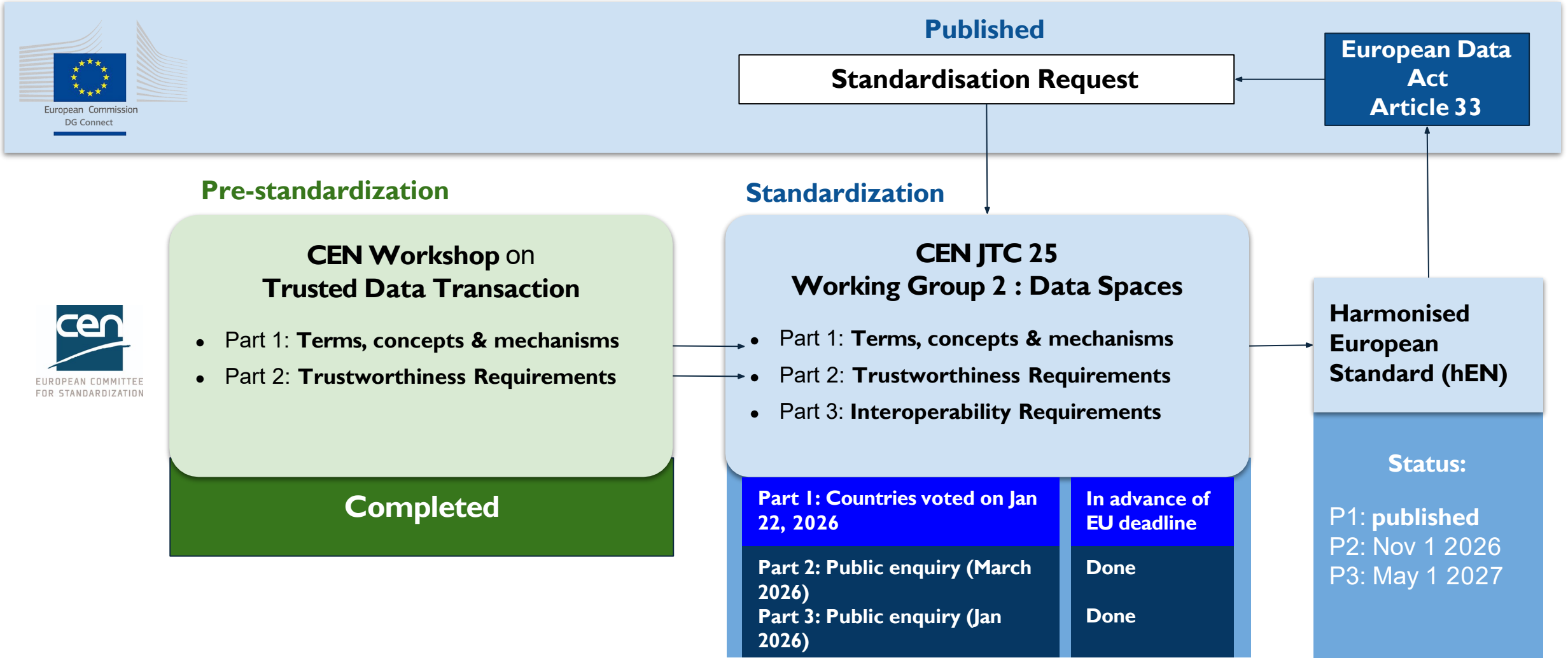
European Trusted Data Framework



Presumption of conformity

STANDARDISATION REQUEST

Harmonised European standard Trusted Data Transactions



Harmonised European standard Trusted Data Transactions

A trusted data transaction is an exchange of data between participants in which trust is established at every phase - from granting rights through publication, discovery, negotiation, exchange, and access & usage - by means of verifiable identities, policies, claims and evidence reconciled within an agreed legal, operational and technical trust framework.

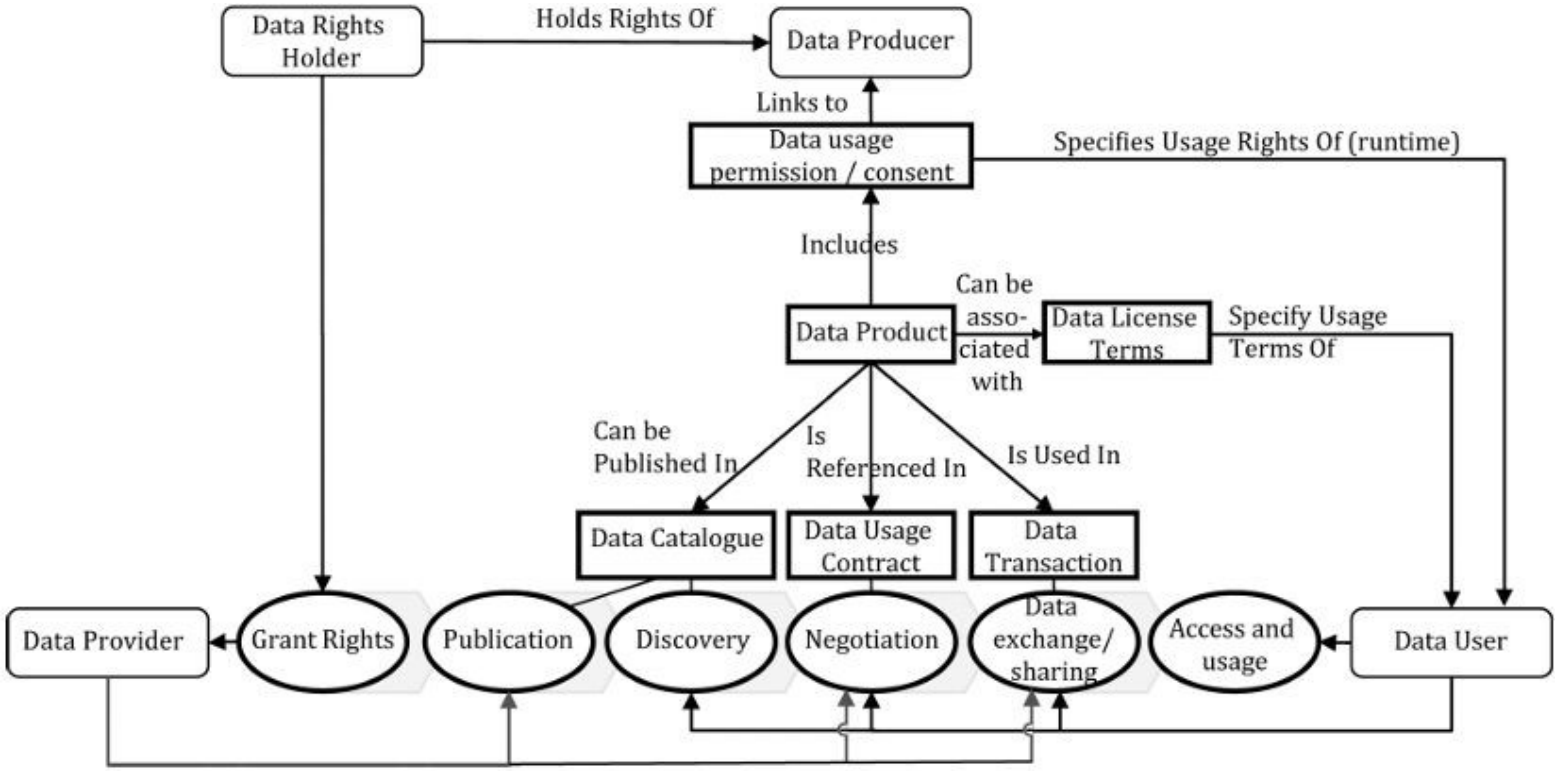


Figure1 — Scope of data transaction

Six phases defined in EN 18235-1:2026 (terminology)

General Principles & General Requirements

§ 4 · Foundational Principles

Apply across every phase of a trusted data transaction

- **Six-phase trust** Trust must be established at every phase of the transaction.
- **Data rights & data products** Rights holders retain control; products bundle data + metadata over the lifecycle.
- **Data quality** Multi-dimensional (accuracy, integrity, completeness, fitness for purpose), described in metadata.
- **Provenance & lineage** Tamper-resistant record of origin, transformations and derivations.
- **Observability & traceability** Monitor, log and audit transactions for accountability and non-repudiation.
- **Data spaces & interoperability** Common rulebook governed by a DSGA; interoperable policies enable cross-space sharing.
- **Trust frameworks · 3 dimensions** Legal · Operational · Technical — separated for reuse, combined to deliver trust.

§ 5.2 · General Requirements

Apply to ALL phases of a trusted data transaction

- **Identification of participants**
  Each participant SHALL hold a valid digital identifier from a recognised identity provider; evidence machine-readable, references issuer, uniquely identifies the participant.
- **Policies · claims · evidence**
  Issuer identifiable; each item uniquely identified; content integrity verifiable; validity verifiable (dates, revocation); machine-readable presentation.
- **Reconciliation & legal enforceability**
  Participants SHALL reconcile policies/claims/evidence — including those of data intermediaries — and ensure they are legally valid and enforceable.
- **Trust framework definition**
  A trust framework SHALL define allowed identification methods, taxonomy of policy/claim/evidence types, and the semantic model(s) used to describe them.
- **Data Space Governance Authority**
  DSGA SHALL validate claims at onboarding, provide a mechanism to verify membership, and validate claims from other federated data spaces.

Source: CWA 18245:2025 (Trusted Data Transaction - Part 2)

Summary of requirements for each data transaction phase

1 Grant Rights
§ 5.3

- Traceable records of delegation (legal docs)
- Metadata: data products, allowed users, purposes, prohibited uses
- Provenance / lineage info; consent for personal data

2 Publication
§ 5.4

- Verify publication rights before listing
- Catalogue metadata: machine-readable, up-to-date, access methods
- Use restrictions, licence terms, provenance, lineage, quality

3 Discovery
§ 5.5

- Service only exposes products it has rights to surface
- Access control by user group / data-space membership
- Results enable assessment of relevance, quality, licence terms

4 Negotiation
§ 5.6

- Provider evidences authority to license the product
- Contract recorded in machine-readable form, undisputable
- Mandatory elements, unambiguous product reference, agreed standard

5 Data Sharing / Exchange
§ 5.7

- Verify identity of data user before exchange
- Evaluate authorisations; validate consent for personal data
- Comply with agreed observability mechanisms (optional 3rd party)

6 Access & Usage
§ 5.8

- Re-verify authorisations on EACH access (may have expired)
- Provider can stop supply if user breaches the contract
- User verifies permissions/consent before each use; observability applies

Across every phase: identity verification, policy/claim/evidence reconciliation, observability and traceability all apply continuously.

Six phases defined in EN 18235-1:2026 (terminology) - trustworthiness requirements specified in Part 2, §5.3–§5.8.

What the Gaia-X Trust Framework already covers

Gaia-X Trust Framework can provide a foundation for many of the requirements.

✓ COVERED BY GAIA-X TODAY

- **Identity of participants · § 5.2.2**
  Participant Self-Descriptions signed via eIDAS; W3C Verifiable Credentials carry machine-readable, issuer-referenced identity evidence.
- **Claims & evidence model · § 5.2.3**
  VCs + linked-data graph give identifiable issuer, unique IDs, cryptographic integrity, and validity / revocation handling.
- **Trust anchors & notaries · § 5.2.5**
  Gaia-X Registry lists endorsed issuers; trust anchors underpin claims that would otherwise be self-declared.
- **Grant rights phase · § 5.3**
  Evidence of delegated rights when rights holder ≠ provider.
- **Continuous compliance · § 5.2 / general**
  Gaia-X Digital Clearing House (GXDCH) automates ongoing validation of credentials across the ecosystem.
- **Federated catalogue · § 5.4 / § 5.5**
  Self-Descriptions for Service Offerings + federated catalogue enable findability, access control, discovery.
- **Extensibility for data spaces · § 4.10**
  Federations (data spaces) can add criteria, select trust anchors, and combine trust frameworks on top of Gaia-X.

⚠ STILL TO BE ADDRESSED

- **Data-product metadata · § 5.4**
  Provenance, lineage, quality.
- **Machine-readable contracts · § 5.6**
  Negotiation phase: undisputable, data usage contracts.
- **Runtime authorisation & observability · § 5.7–5.8**
  Per-transaction identity check, policy enforcement, audit trails.
- **Reconciliation · § 5.2.4.4**
  Reconciling policies, claims.

Covering the gaps

⚠ STILL TO BE ADDRESSED	✓ ON GOING GAIA-X WORK	BY WHOM?
Data-product metadata · § 5.4 Provenance, lineage, quality	**Mostly covered. New ontologies need to be introduced and added to the Data Product Model**	Data Exchange Services ICAM Service Characteristics
Machine-readable contracts · § 5.6 Negotiation phase: undisputable, data usage contracts.	**Specification of Data Usage Contracts**	Data Exchange Services
Runtime authorisation & observability · § 5.7–5.8 Per-transaction identity check, policy enforcement, audit trails.	**Observability framework has to be defined**	Architecture Document Data Exchange Services
Reconciliation · § 5.2.4.4 Reconciling policies, claims.		

To fully cover the gaps, Data Spaces need adjustments to Gaia-X specifications as well as a **Data Transfer Agent** that can **operationalise** trusted data transactions.

Data Transfer Agent (DTA)

DTA is a **lightweight** software component that comes into play after two parties have agreed on a **data transaction**

Carries out the **verifications** and **operationalise trusted data transactions** within a **Data Space**

- Participants, Data Products and DAC's management
- Policy enforcement and granting access to the data
- Transfer and stream data
- Observability

The component implements the **Gaia-X Trust Framework** and **OIDC4VC/OIDC4VP openID Standards**.

Covering the missing gaps with Data Transfer Agent

MISSING GAPS CAN BE COMPLETED WITH DTA	✓ Data Transfer Agent
Machine-readable contracts · § 5.6 Negotiation phase: undisputable, data usage contracts.	DTA enables the implementation (needs Gaia-X specification)
Runtime authorisation & observability · § 5.7–5.8 Per-transaction identity check, policy enforcement, audit trails.	DTA enables the implementation (needs Gaia-X specification)
Reconciliation · § 5.2.4.4 Reconciling policies, claims	Already covered

Gaia-X and DTA as a foundation to implement TDT for Data Spaces

✓ COVERED BY GAIA-X TODAY

Identity of participants · § 5.2.2
Participant Self-Descriptions signed via eIDAS; W3C Verifiable Credentials carry machine-readable, issuer-referenced identity evidence.

Claims & evidence model · § 5.2.3
VCs + linked-data graph give identifiable issuer, unique IDs, cryptographic integrity, and validity / revocation handling.

Trust anchors & notaries · § 5.2.5
Gaia-X Registry lists endorsed issuers; trust anchors underpin claims that would otherwise be self-declared.

Grant rights phase · § 5.3
Evidence of delegated rights when rights holder ≠ provider.

Continuous compliance · § 5.2 / general
Gaia-X Digital Clearing House (GXDCH) automates ongoing validation of credentials across the ecosystem.

Federated catalogue · § 5.4 / § 5.5
Self-Descriptions for Service Offerings + federated catalogue enable findability, access control, discovery.

Extensibility for data spaces · § 4.10
Federations (data spaces) can add criteria, select trust anchors, and combine trust frameworks on top of Gaia-X.

✓ COVERED BY GAIA-X (2026) and DTA

Data-product metadata · § 5.4
Provenance, lineage, quality, licence terms at the data-product level.

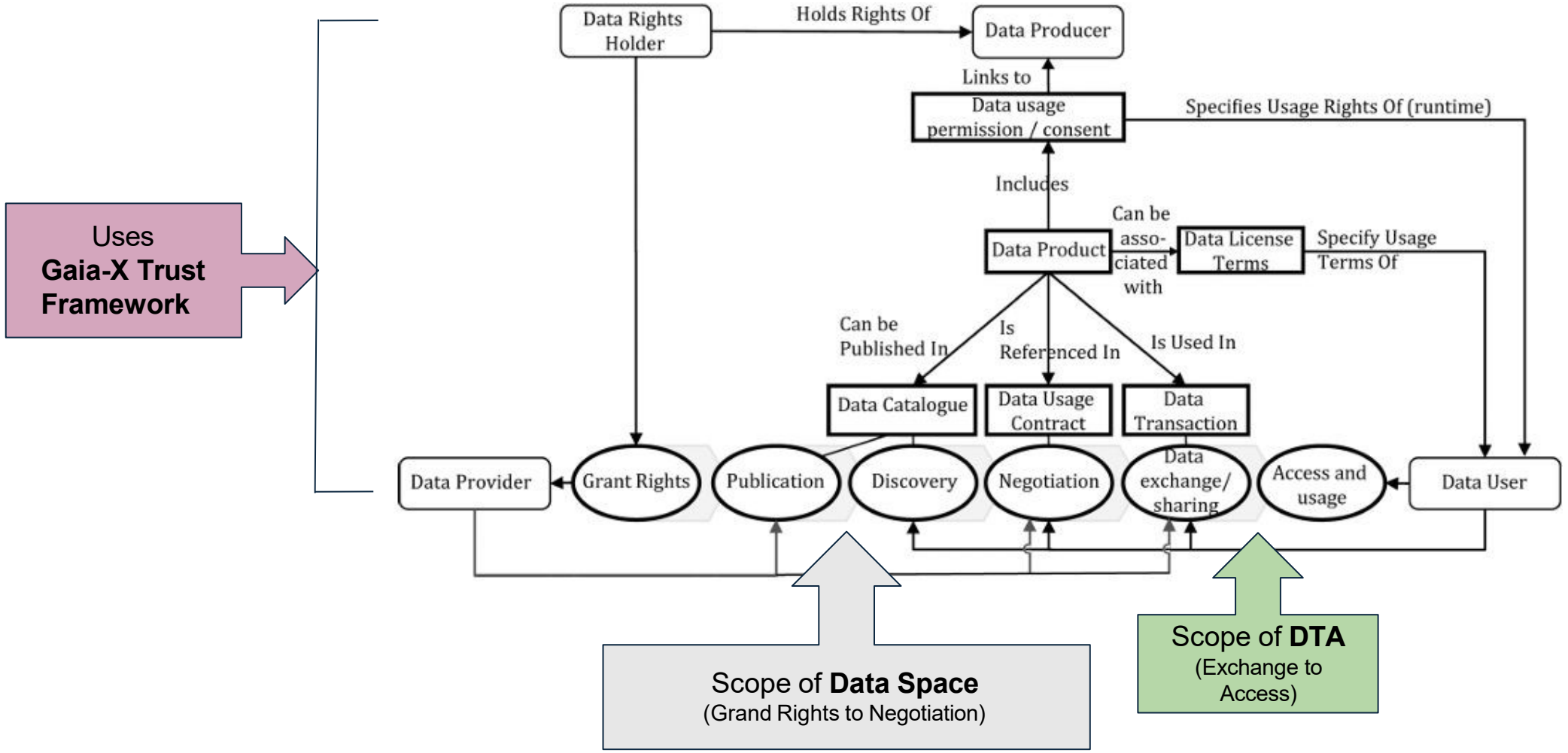
Machine-readable contracts · § 5.6
Negotiation phase: undisputable, data usage contracts.

Runtime authorisation & observability · § 5.7–5.8
Per-transaction identity check, policy enforcement, audit trails.

Teconciliation · § 5.2.4.4
Reconciling policies, claims.

With adjustments to Gaia-X and TDT, Data Space will be able to cover all requirements of TDT

The scopes of Gaia-X, DTA and Data Space



Addressing concrete needs. Not just another component

Ecosystems require:

- Traceability
- Integrity
- Availability
- Production Grade Software

From the **Trust Framework**, … but also from **all components implementing Trust**

Why developing as a community tools?

Trustable component for Trust Ecosystem

- Peer Review
- Audits (Code Verification & Code Review)
- Sustainability (reduce single points of failure)
- Shared conformity assessment
- Versioning and support

- Aligned with the sprint « software components Labels » from the PRC.
- Reference implementation for Gaia-X Specifications.
- Allow co-development with Gaia-X Labs teams.

What are the next steps to implement TDT for Data Spaces?

Gaia-X specifications (WG level)

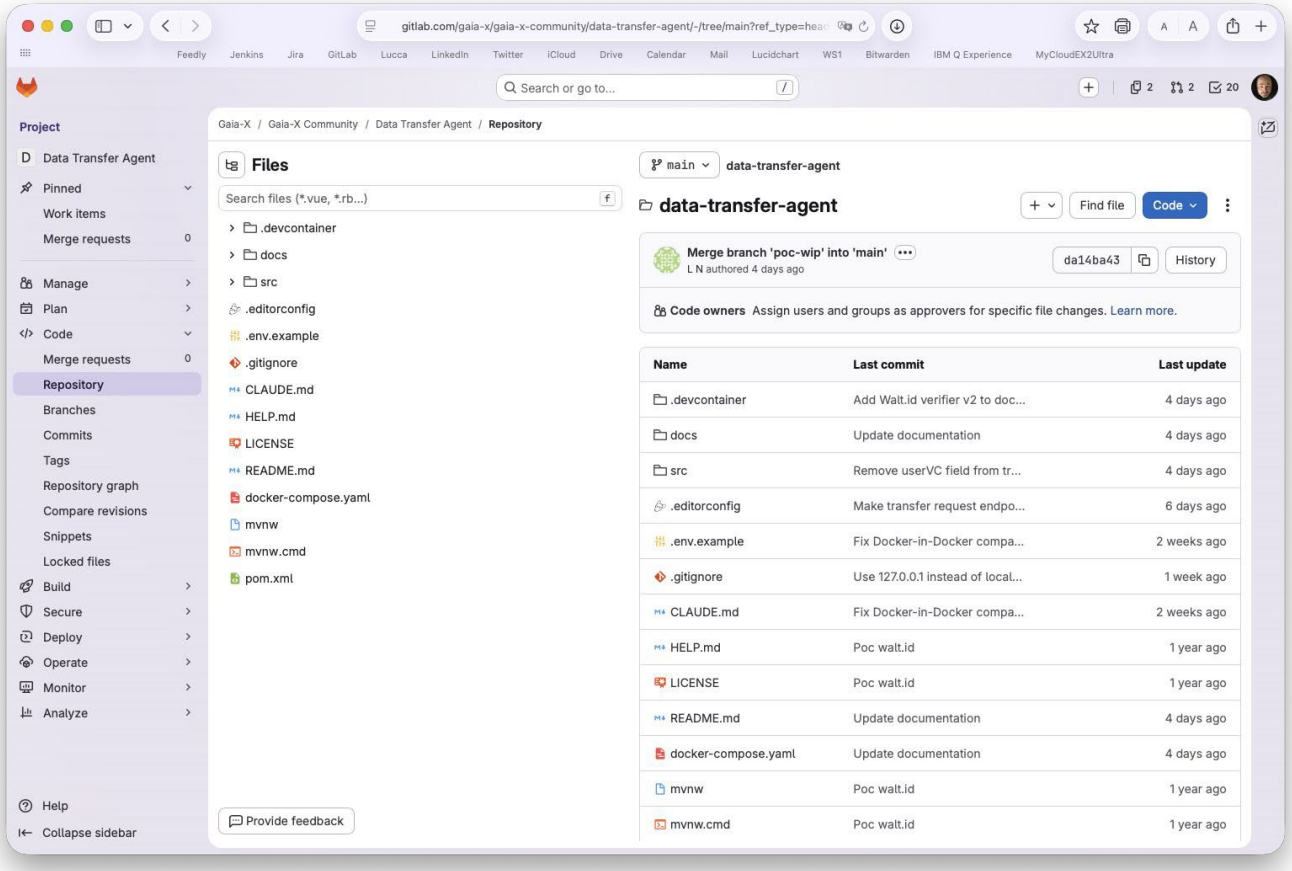
- Implement missing ontologies (party credentials, DAC, etc.)
- Complete specifications (DAC, Observability)

Gaia-X implementation (OSS Community level)

- Build a **strong OSS community** around Gaia-X
- Provide tools and **implementations** for Data Spaces

Join the collective effort to implement European Trusted Data Framework with Gaia-X!

Contributing to Data Transfer Agent (DTA)



- Code source is **available** on **Gaia-X Gitlab**
- Code is moving **fast**
- Apache 2.0 licence

Thank you!

Benoit Tabutiaux | benoit.tabutiaux@imt.fr
Frédéric Bellaiche | frederic.bellaiche@dawex.com
Christoph Strnadl | christoph.strnadl@gaia-x.eu

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

One Connector Many Sovereigns: A Multi-Tenant for Low IT Participants

11:45 – 12:00

- **Sava Stanojevic –** MicelioData

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

ONE CONNECTOR MANY SOVEREIGNS

Time: 15 minutes

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

#GaiaX #TechX26

MicelioData

First data space in the textile industry

HOW DO WE CONNECT PARTICIPANTS TO A DATA SPACE WHEN OFTEN STATE-OF-THE-ART IS PEN AND PAPER?

WORK IN PROGRESS

DEPLOYMENT IN PROGRESS

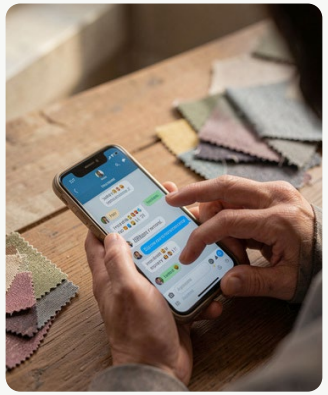
EDC-V · DSP · GAIA-X

~95% Of SMEs excluded from dataspaces

~70% Of textiles are exported to the EU from Asian countries

2028 EU Digital Product Passport for textiles
Every supply chain tier must comply

BANGLADESH: HOW SUPPLY CHAINS ACTUALLY OPERATE



MOBILE-FIRST OPERATIONS

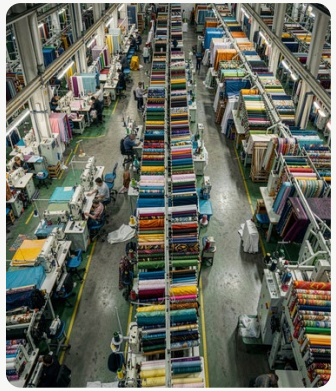
- Factory operations often run from a single mobile phone
- Orders and updates are managed via WhatsApp
- Quality checks rely on photos and voice notes

PAPER-BASED RECORDS

- Production and chemical records are often handwritten
- Most factories operate without digital backups
- Critical operational data remains offline and fragmented

CONTRACTS BY HANDSHAKE

- Supplier agreements negotiated verbally.
- No formal contracts, no digital signatures, no audit trail.

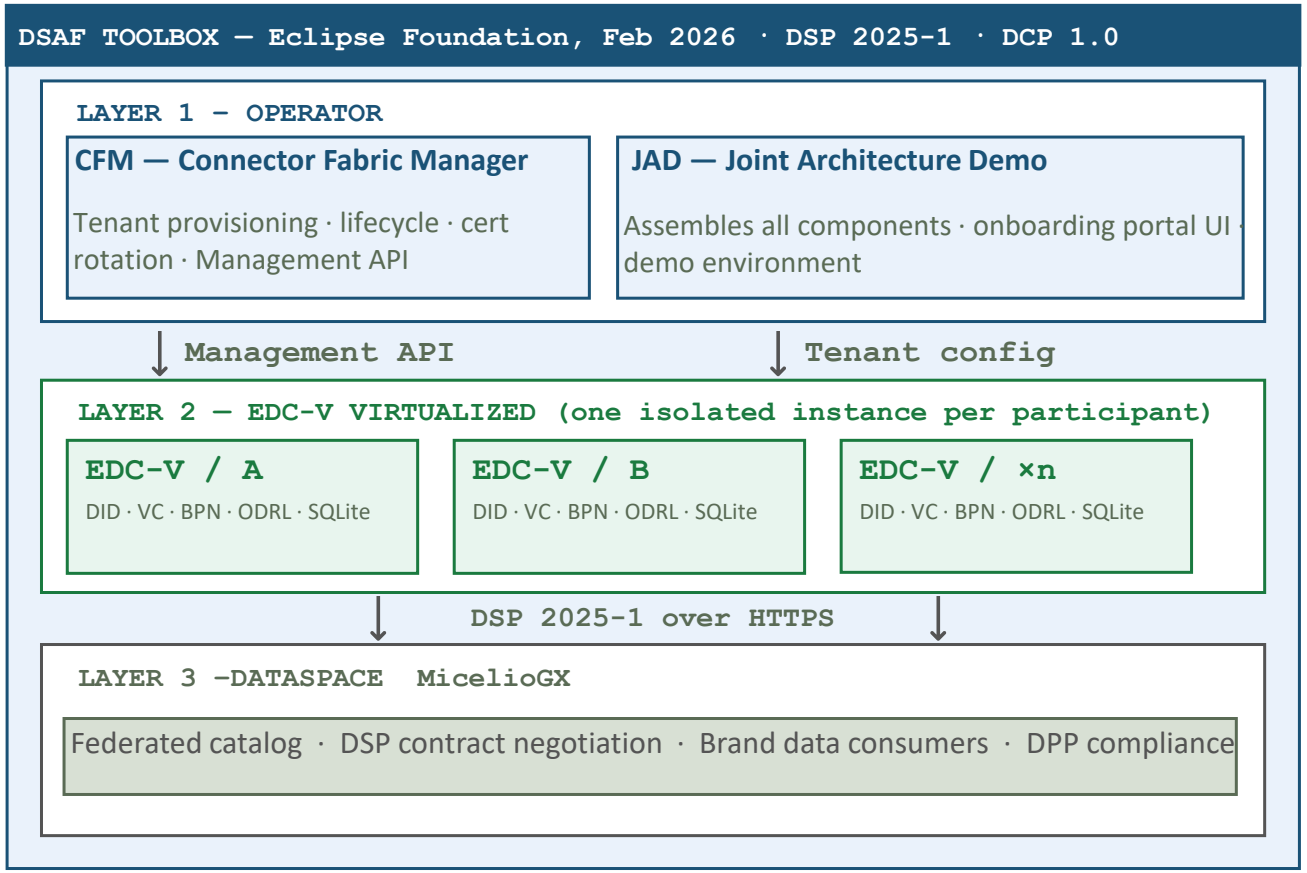


ZERO TECHNICAL INFRASTRUCTURE

- No ERP, no server, no IT department
- Low technological literacy
- Unstable internet and power connection

EU Digital Product Passport (2028) demands verified, machine-readable data from every tier of the supply chain

THE INFRASTRUCTURE PROBLEM IS SOLVED. THE PARTICIPATION PROBLEM IS NOT.



WHAT THE TOOLBOX SOLVES:

- ✓ Multi-tenant provisioning at scale via CFM
- ✓ Cloud-native EDC variant (EDC-V) for MSPs
- ✓ Automated lifecycle management
- ✓ Pluggable data planes for compatibility

CRITICAL ASSUMPTION REMAINS

- ✗ The tenant must have some technical knowledge
- ✗ They must be able to store their credentials
- ✗ They have some technical entity understanding the process
- ✗ They must have their data digitized and stored

Our participants have none of this. They are the majority of the SMEs and they are mandatory to ensure traceability

SUPPLIERS WITH ZERO IT: THE LAST STEP

Identity Wallet

DIDs · BPN · Verifiable Credentials — provisioned, hosted and rotated by intermediary. Supplier never touches it.

Standardised & Interoperable Data

Raw data from paper/WhatsApp transformed into DPP, CSRD, EUDR compliant structured data assets.

Secure Sovereign Storage

Encrypted per-participant data store. Intermediary operates but cannot co-mingle with other tenants.

ODRL Policies → Plain Language

Machine-readable access policies derived from plain-language agreements the supplier can read and understand.

Contract Negotiation

EDC-V contract negotiations run live on every transaction — even when we operate both sides. This is our governance record.

SUPPLIER INTERACTION

WhatsApp · CSV · Web form · Photo

Zero technical knowledge required

↓

GATEWAY LAYER

MIA — Micelio Intelligence Agent

Extract · Normalise · Derive ODRL · Route identity

↓

ORCHESTRATION

Eclipse CFM + Kubernetes

Provision · Lifecycle · Certificates · Auto-deploy

↓

DATASPACE CONNECTOR

EDC-V — per-participant virtualized

DID · BPN · VC · ODRL · SQLite — structurally isolated

↓

DATASPACE

MicelioGX

Each participant = independent sovereign actor

MIA: TECHNICAL ARCHITECTURE FOR ZERO-IT PARTICIPANTS

MicelioData — Allowing the participations of participants with zero technical literacy

LAYER 1 — MIA (Micelio Intelligence Agent)

UI/UX Interface
- WhatsApp-native
- Mobile web form
- Photo/doc upload
- Voice + multilingual

ML/LLM Engine
- MD-SE semantic extraction
- Unstructured → DPP/CSRD
- LLM data matching
- Schema validation

Policy Translator
- Plain language → ODRL
- Policy store per tenant
- Consent provenance log
- Human-readable terms

Identity Broker
- DID provisioning
- VC issuance + mgmt
- BPN held in trust
- Key lifecycle mgmt

↓ DSP API calls via Management API

LAYER 2 — EDC-V (Eclipse Dataspace Components — Virtualised, DSAF / Eclipse Foundation)

Control Plane
- Contract negotiation (DSP)
- Catalog management
- Policy enforcement
- Management API

Data Plane
- Asset transfer
- EDR token refresh
- Pluggable connectors
- Encrypted data flows

CFM Orchestration
- Per-tenant provisioning
- K8s lifecycle mgmt
- Cert rotation
- Health monitoring

Identity Layer
- DCP 1.0 · DID resolver
- VC presentation
- IDSA Rulebook compliant
- DSP 2025-1 certified

↓ Dataspace Protocol (DSP 2025-1) over HTTPS

LAYER 3 — MicelioGX | Gaia-X / IDSA compliant dataspace | Federated catalog · DSP · Brand data consumers

THANK YOU!

Sava Stanojevic | sava.stanojevic@miceliodata.eu

Connect with me!

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

Simpl-Open IAA (Identification, Authentication & Authorization) SSI Tier 2 Implementation: The Gaia-X ICAM Semantic Model in Action

12:00 – 12:15

- **Pietro Bartoccioni** – Aruba

In partnership with

Simpl-Open **SSI** Tier 2 Implementation
The ICAM Semantic Model in action

gaia-x

29 May 2026 Time: 12:00

Pietro Bartoccioni
Sovereign-X

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

What is Simpl?

Simpl Essentials

open-source means built-in trust & security, flexibility to deploy, simplicity to customise

middleware are software suites that enable applications and databases to work seamlessly together and provide a flawless user experience

Simpl is the open-source smart middleware that enables cloud-to-edge federations and all major data initiatives funded by the European Commission

cloud-to-edge federations put together resources across cloud and edge computing environments as a cohesive system, creating a seamless integrated infrastructure that combines the strength of both cloud and edge computing

all major data initiatives, in particular the development of **Common European Data Spaces** in a modular and interoperable way

Simpl is made of three products

Simpl Essentials

The open-source smart middleware that enables cloud to edge federations enabling major data initiatives.

Simpl-Open

Playground environment for Simpl-Open
+
Interoperability test for existing data spaces

Simpl-Labs

Distinct instances of Simpl-Open software stack deployed for specific sectoral data spaces/initiatives.
European Commission plays an active role in their management.

Simpl-Live

Simpl-Open 2 Tier IAA Architecture

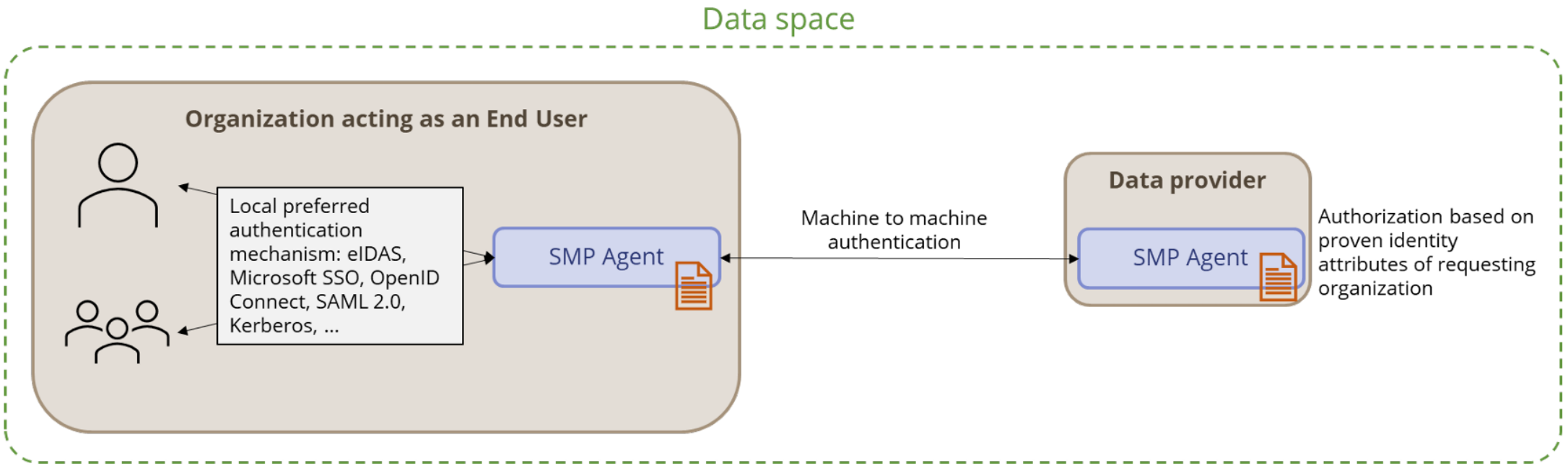


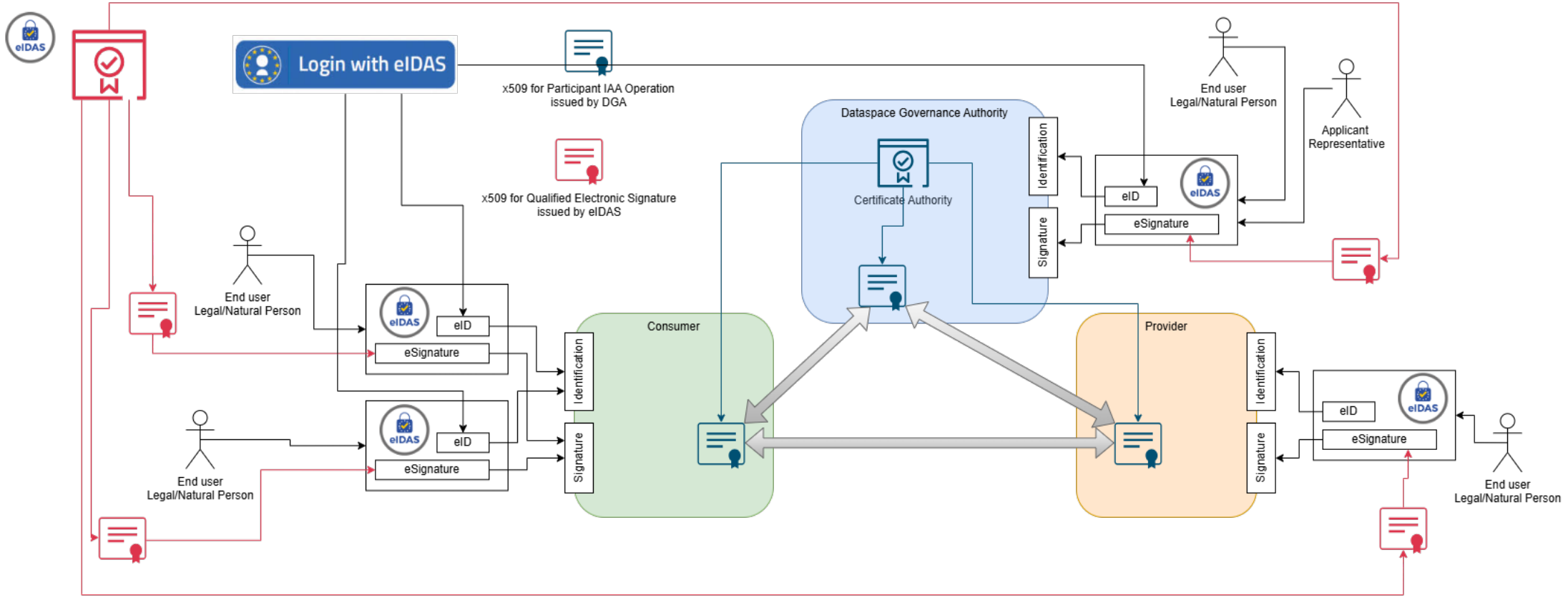
Figure 11. Visual illustration of the two-tier IAA

Extracted from the **Architecture Vision** of Simpl-Open tender documentation
Note that in this diagram, **End User** means **Consumer**

Simpl-Open Tier 1

where End-Users are First-class Citizens

Tier 1 is not only local IDPs but also eIDAS Framework integration using eID and eSignature building blocks



Extracted from the presentation **«Simpl-Open eIDAS Integration»** done last year at the **Gaia-X Architecture** meeting, available in the Simp-Open academy

Tier 2 - where Participant's Agents securely communicate

The Simpl-Open Zero Trust Architecture of Tier 2 IAA and the 3 Options

1. X.509 certificates with embedded identity attributes
2. X.509 certificates with dynamic identity attributes provisioning
3. Self-Sovereign Identity with a distributed ledger

All the above options rely on the **mTLS Authentication** to ensure that all communications are from/to a trusted and active Simpl-Open data space participant agent, and also across data space federations

NOTE: Even if in the Architecture Vision document, there was no explicit mention of IDSA RAM, we stick to it in fact:

- Option 1 and Option 2 are implementations of **Identities for Devices** (removing the tracking info from the DAT)
- Option 3 will be an implementation of **Identities for Participants**

As described in the 4.1 Security Perspective → 4.1.2 Identity and trust management section

IDSA RAM 4.0 - 4.1.2 identity and trust management - identities for devices and 4.1.2 identity and trust management - identities for participants

The Tier 2 - where Participant's Agents securely communicate

Simpl-Open Option 1 and Option 2 are a Production Grade implementation of Identities for devices

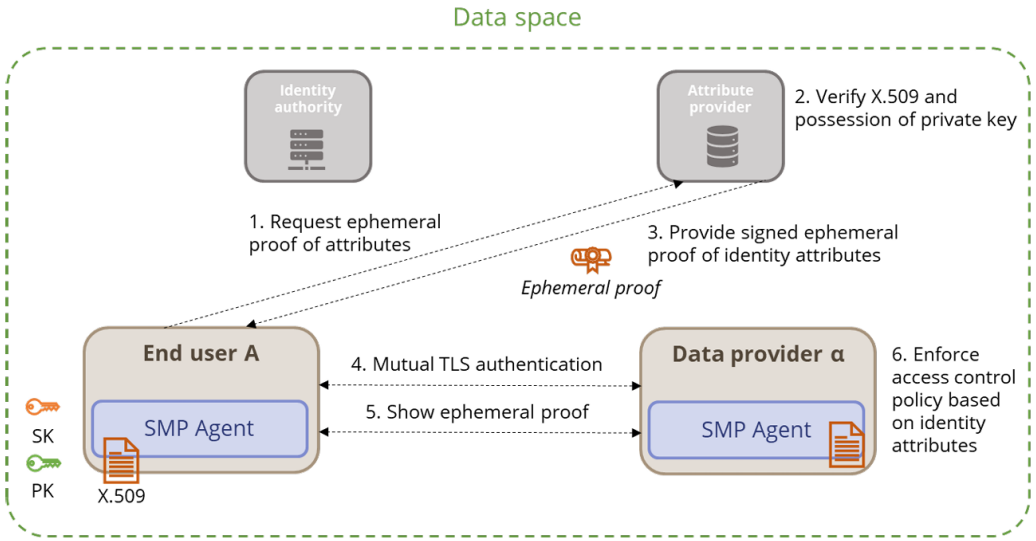
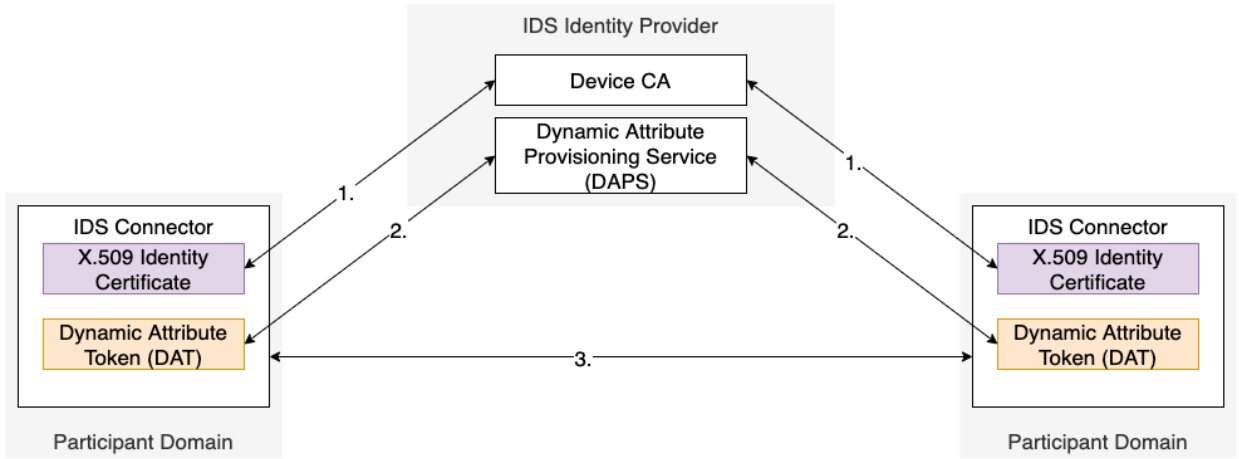


Figure 16. End user requesting access in the second option for SMP IAA

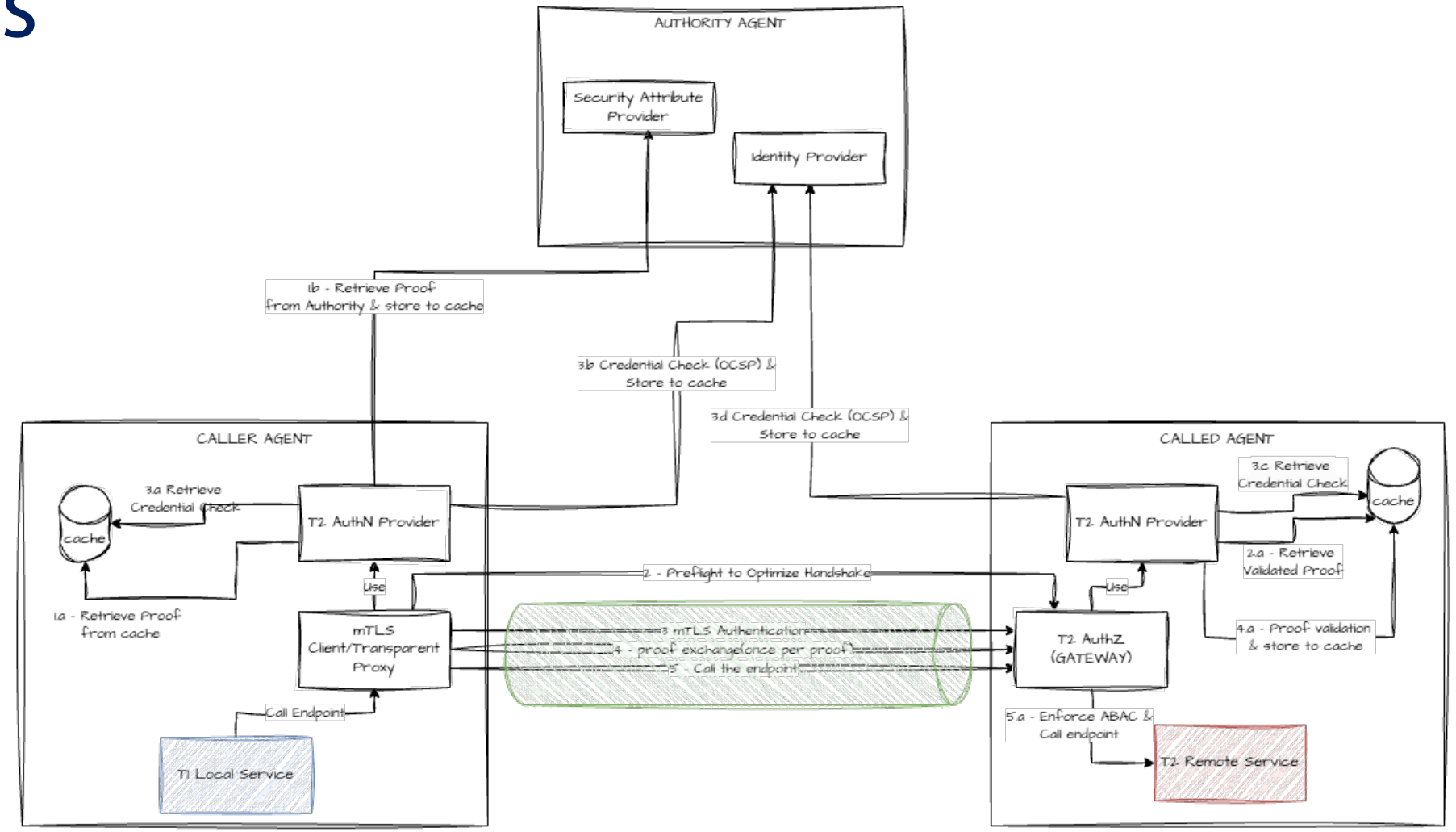
INTERNATIONAL DATA SPACES ASSOCIATION

Identities for Devices



IDSA RAM 4.0 - 4.1.2 identity and trust management - identities for devices

The Tier 2 – deep dive into technical details



Option 3 – Self-Sovereign Identity

The initial requirements for SSI – Agent-To-Agent Communications

The high-level overview of the Option 3 original requirement

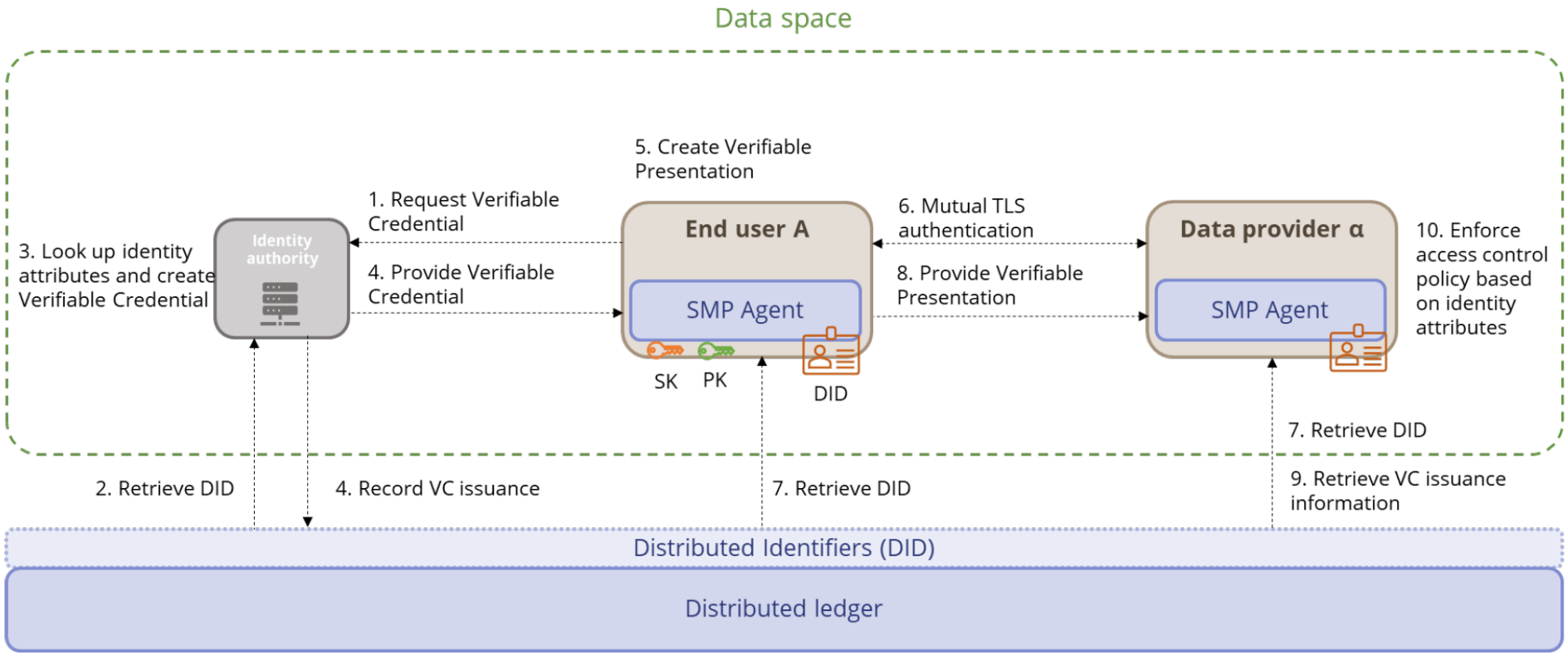


Figure 20. End user requesting access in the third option for SMP IAA

Extracted from the Architecture Vision of Simpl-Open tender documentation
Note that in this diagram, End User means Consumer

The initial requirements for SSI – Data space Federation

The high-level overview of the Option 3 original requirement

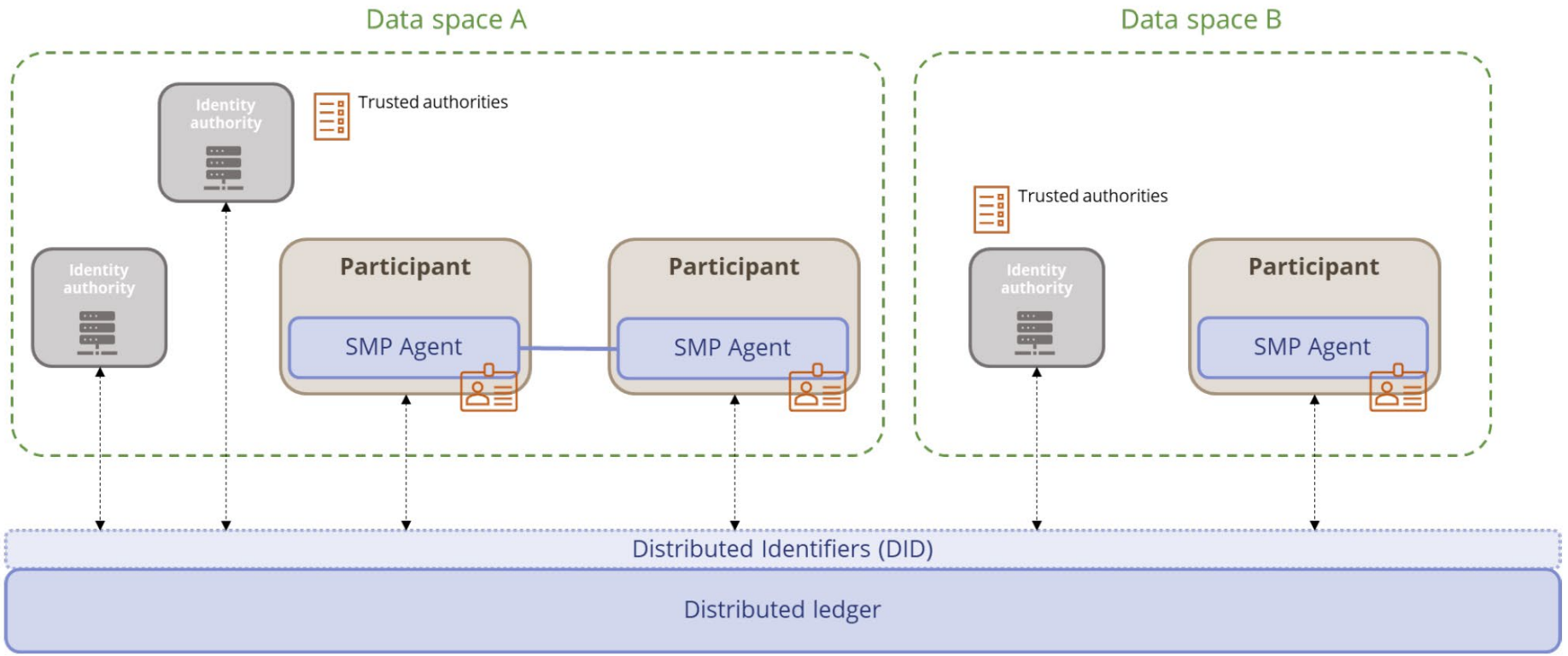


Figure 21. Federation of trust in the third option of SMP IAA

Extracted from the Architecture Vision of Simpl-Open tender documentation

Option 3 – Self-Sovereign Identity Implementation

Simpl-Open using Gaia-X ICAM Semantic Model enables RAM Identities for Participant

The high-level overview

Simpl-Open

The ICAM Semantic Model

The IDSA - RAM Identities for Participants

adopts

gaia-x

enabling

INTERNATIONAL DATA SPACES ASSOCIATION

Using Gaia-X ICAM Semantic Model to enable SSI in data spaces and federations

The Semantic Model in Simpl-Open Data Space

Simpl-Open will use a specialisation of the PartyCredential to implement the **Simpl Participant Credential** that is issued by the Data Space Governance Authority to all Participants, the main used properties (claims) are:

- **identityAttributes** - which contains all the Identity Attributes assigned to the participant and used in ABAC (Attribute-Based Access Control) in Agent-to-Agent communication.
- **holder** – which identifies the **verificationMethod** bound to the public key of the current agent-controlled keypair (also used in mTLS)
- **publicKeyDigest** – the hash (as defined in the Subresource Integrity) of the public key retrieved using the **holder** property. This is used to **strongly bind** the credential to the public key of the holder and check the proof of possession during Verifiable Presentations
- **credentialStatus** to ensure almost real-time and privacy-preserving control over the issued credentials using the Bitstring Status List

Using Gaia-X ICAM Semantic Model to enable SSI in data spaces and federations

The Semantic Model in Simpl-Open Data Space Federations

- Simpl-Open will use the TrustScopeCredential to implement the **Simpl DataSpace Credential.**

- This credential is self-issued by all the Data Space Governance Authorities and can be trusted by any other Data Space Governance Authorities that want to establish a **Trust Relation.**

- As described in the ICAM document (section 6.1.2), the Trust Relation is monodirectional, and Bidirectional (or full) federation can be achieved by combining two opposite Trust Relations.

- Simpl-Open needs a **Simpl TrustRelation Credential** to define fine-grained mapping of Identity Attributes

What Next?

What becomes possible in Simpl-Open after SSI Implementation is in place

Integration and embedding in Simpl-Open of other SSI-based IAA solutions, like:

- **Decentralised Claim Protocol (DCP)** → using IdentityHub + implementing SimplDidResourceStore, SimplCredentialResourceStore, and SimplKeyPairResourceStore
- **OpenID Connect for Verifiable Credentials (OIDC4VC)** → providing access to Simpl-Open DID, Verifiable Credentials, and KeyPair

Federation with Non-Simpl-Open Data Spaces:

- Adopting the ICAM Semantic Model (TrustScope + TrustRelation Credentials) for Monodirectional and Bidirectional Federations
- Extending the existing Zero-Trust mTLS Agent-to-Agent secured communication to external participants, developing a lightweight agent (Gateway, Transparent Outbound Proxy)

gaia-x

Website

Visit our website for Simpl documentation, requirements and latest news.

Social Media

Join and engage with our growing community!

Forum

Keep a look out for topics on Simpl's forum!

Simpl Newsletter

Subscribe to stay up-to-date with Simpl!

Code Repository

Check out and review the code!

Webinars & Workshops

Join technical and business sessions, online and in person.

NEW

#GaiaX #TechX

Thank you!

Pietro Bartoccioni | pietro.bartoccioni@staff.aruba.it

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

The Eunomia Agentic Connector

12:15 – 12:45

- Joaquin Salvachua – Polytechnic University of Madrid
- José Muñoz – Polytechnic University of Madrid

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

The Eunomia Agentic Connector

Joaquín Salvachúa
Andres Muñoz

Universidad Politécnica de Madrid

UNIVERSIDAD POLITÉCNICA DE MADRID

POLITÉCNICA

iptc Information Processing and Telecommunications Center

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

Mission

- Architecting the future of Data Spaces through ODRL, Formal Methods, and Sovereign AI Governance. Building trust through open source and interoperable open protocols.
- Emphasis in interoperability : allow different ways to interact with other data spaces.

- Agentic capabilities : DSL middleware capable of been generated by LLM/SLM.
- Glue code generated via Configurable infrastructure
- Develop a dataspace in 10 mins with a prompt

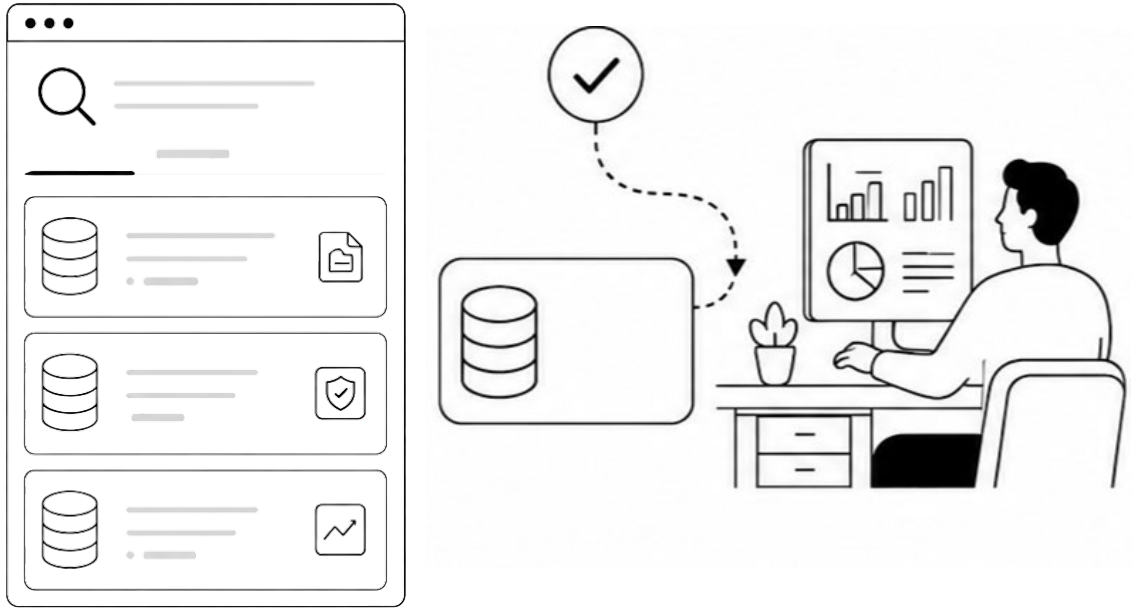
Eunomia Framework Interoperabilidad

The Standard: Dataspace Protocol

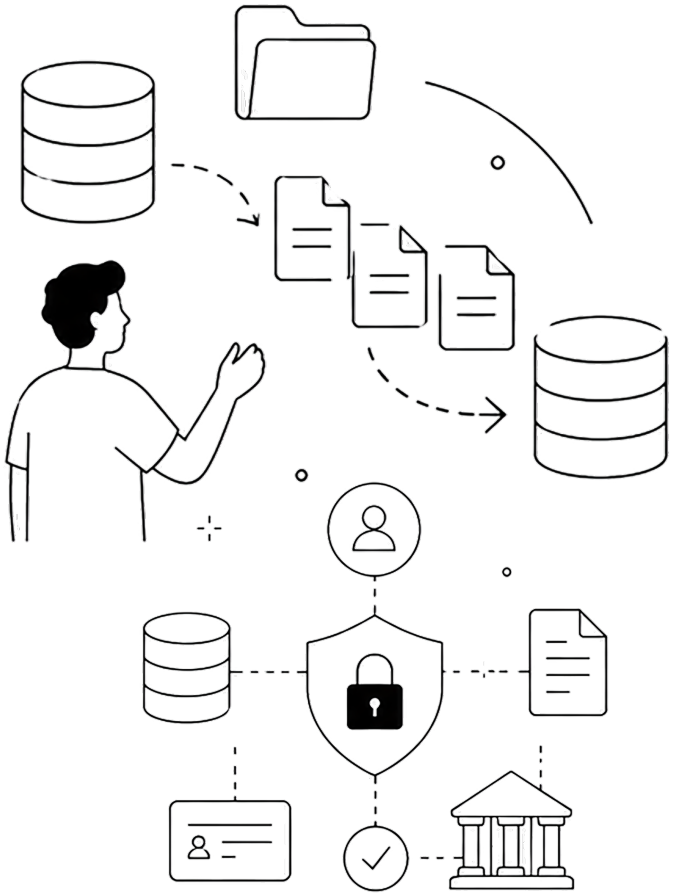
Protocol published by IDSA and standardized on the Eclipse Foundation. It defines three sub-protocols that cover the complete data sharing cycle:

Catalog: descubrimiento de datasets y políticas (DCAT + ODRL)

- **Contract negotiation:** structured dialogue until a formal Agreement is generated
- **Transfer:** coordination of the actual exchange (push/pull, finite/non-finite) DSP is implementation agnostic: any connector that implements it can participate in the data space. Current Version: 2025-1 (Release Candidate), Path to Eclipse Specification.



Eunomia: Complete Framework for Data Spaces



Eunomia is an open-source framework developed by UPM that provides all the necessary components to create a data space from scratch. It's not just a connector: it's an ecosystem of components that covers identity, governance, negotiation, and transfer. Main components:

- **Eunomia DS-Agent:** Agent for Negotiation, Transfer and Governance Proxy
- **Eunomia Heimdall:** authority, clearing house, credential issuance
  Implements DSP ensuring interoperability with other connectors in the ecosystem (EDC, FIWARE DSC).

Focused on innovation and interoperability(DEPLOYTOUR)

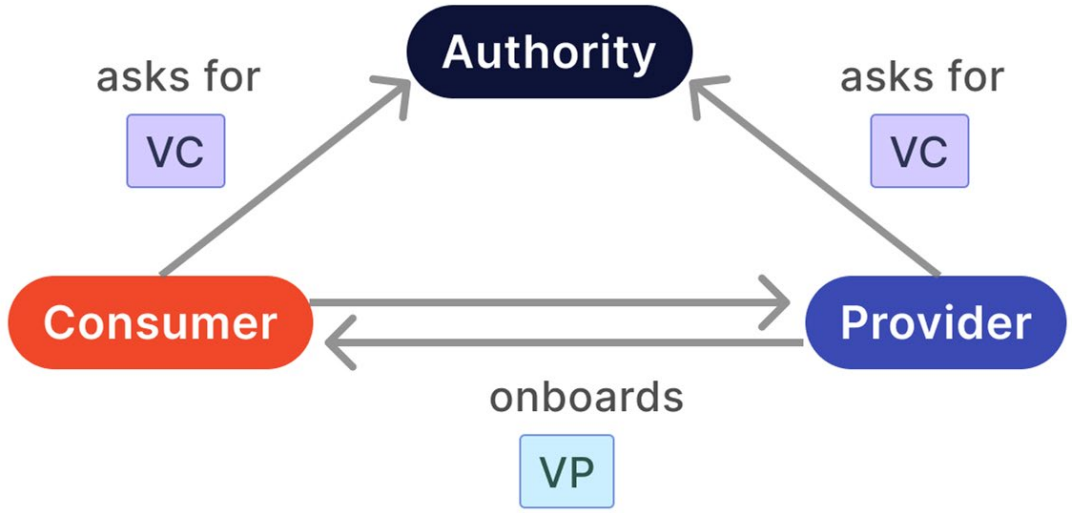
Native SSI Identity

While other connectors treat identity as external integration, Eunomia has it as an architectural pillar.

Each participant has a DID and verifiable credentials managed in their own wallet.

Onboarding works like this: you request to join the space by presenting a certificate (eIDAS / Fabrica Moneda y Timbre), the Authority issues you a VC. To operate with a provider, you present proof of your VP and receive an access token.

No central identity platform, no shared passwords, no single point of failure. Did:web compatible for GAIA-X (optional)



Integrated Governance (Heimdall)

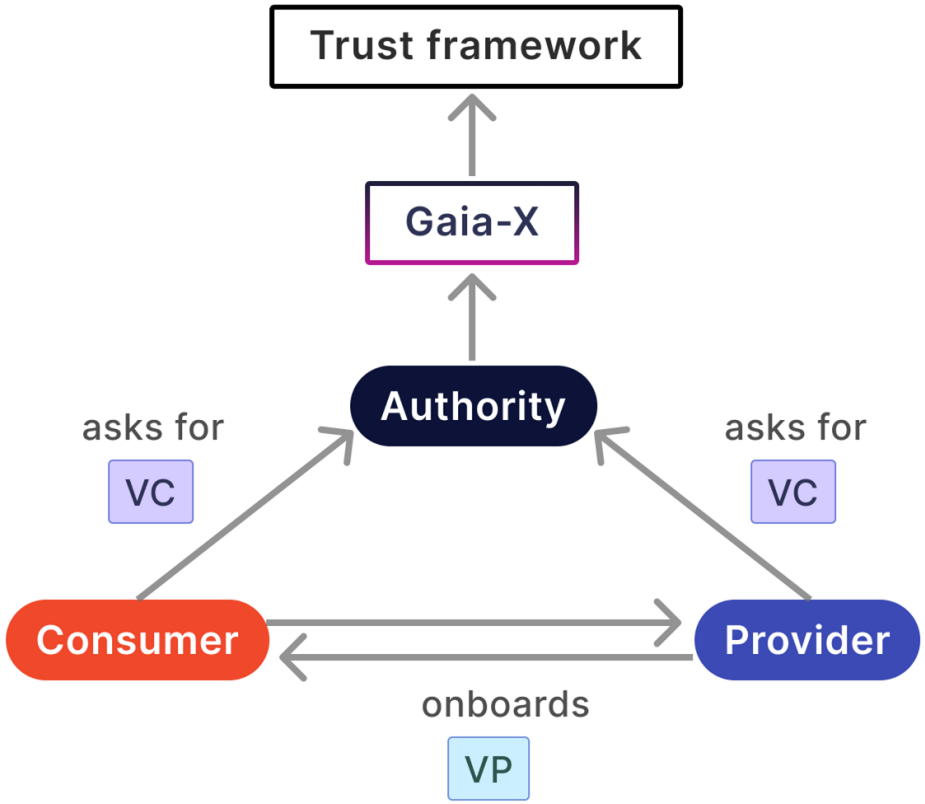
Most connectors solve the bilateral exchange, but not the governance of the ecosystem.

Heimdall fills that gap as a dedicated component of Authority that defines and enforces the rules of the data space: which credentials are accepted, which trust anchors, which policy profiles and catalogs. (more to come)

It functions as a clearing house (compliance validation), legal authority (issuance of legal-level credentials), and service registry.

Compatible with GAIA-X Trust Framework.

A data space without governance is just an API gateway.



Programmable data plane

The DSP standardizes the control plane (negotiation, coordination), but leaves the data plane out of reach.

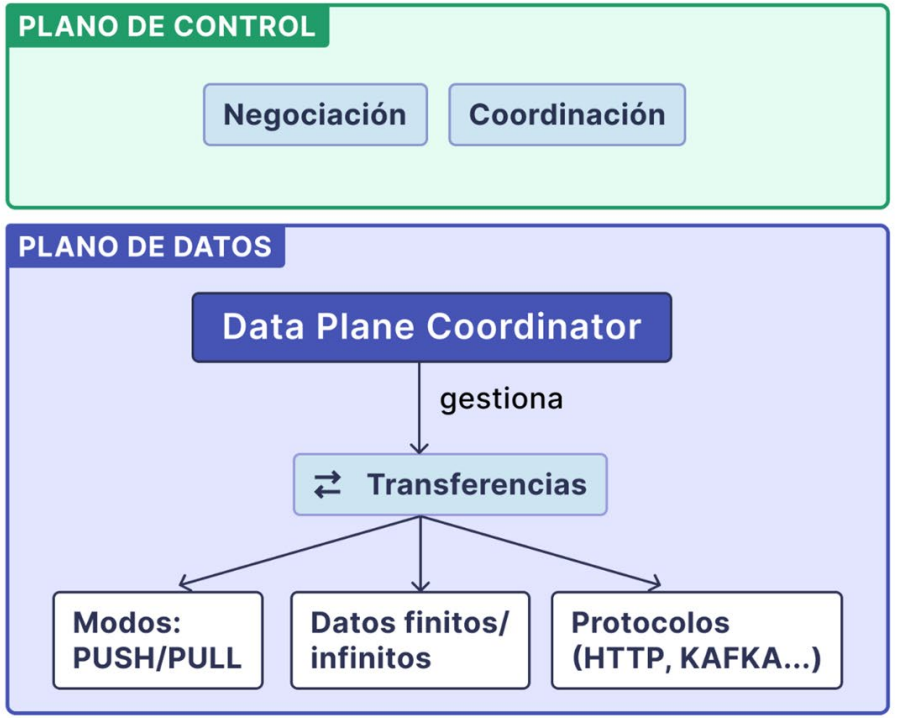
Eunomia addresses it with a Data Plane Coordinator that manages the actual transfer: pull (consumer download) and push (provider sends) modes, finite and infinite data (streams), and multiple transport protocols (HTTP, with roadmap for S3, Kafka, gRPC).

The DS-Agent acts as a governance proxy: every byte that passes is backed by a verifiable Agreement.

Efficient RUST Implementation: Microservices or Monolith

Dataspace Protocol

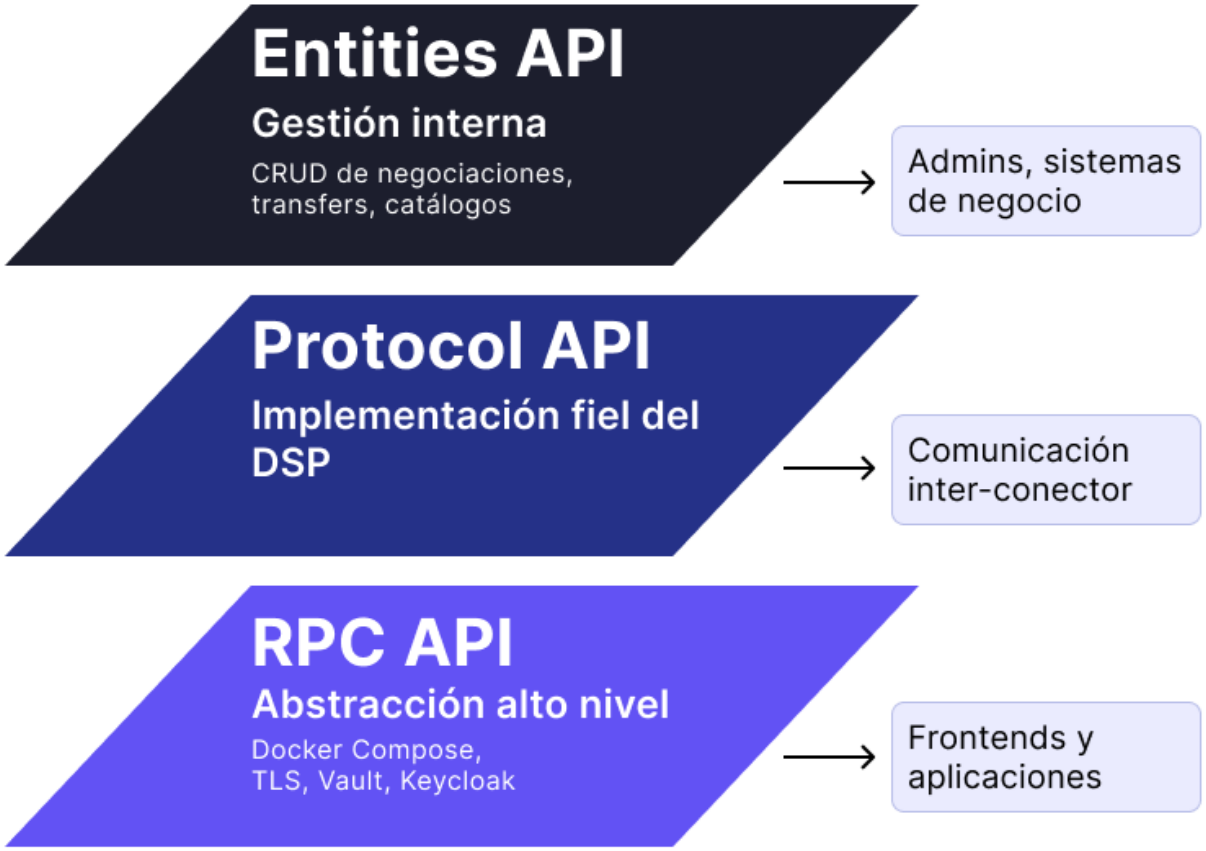
eunomia
Secure Data Spaces



Experiencia de desarrollador

Un problema recurrente en conectores DSP es la complejidad de integración. Eunomia resuelve esto con tres capas:

- **Entities API:** internal management (CRUD of negotiations, transfers, catalogues). For admins and business systems.
- **Protocol API:** faithful implementation of the DSP. For inter-connected communicationr.
- **RPC API:**high-level abstraction. A single call executes an entire DSP flow. For frontends and applications. In addition: Ready-to-use SPA, Mini deployment (Docker Compose, 5 minutes) and Production (TLS, Vault, Keycloak). Open source GPL-3.0.API CRED + Evolution to Declarative API



Ecosystem Players

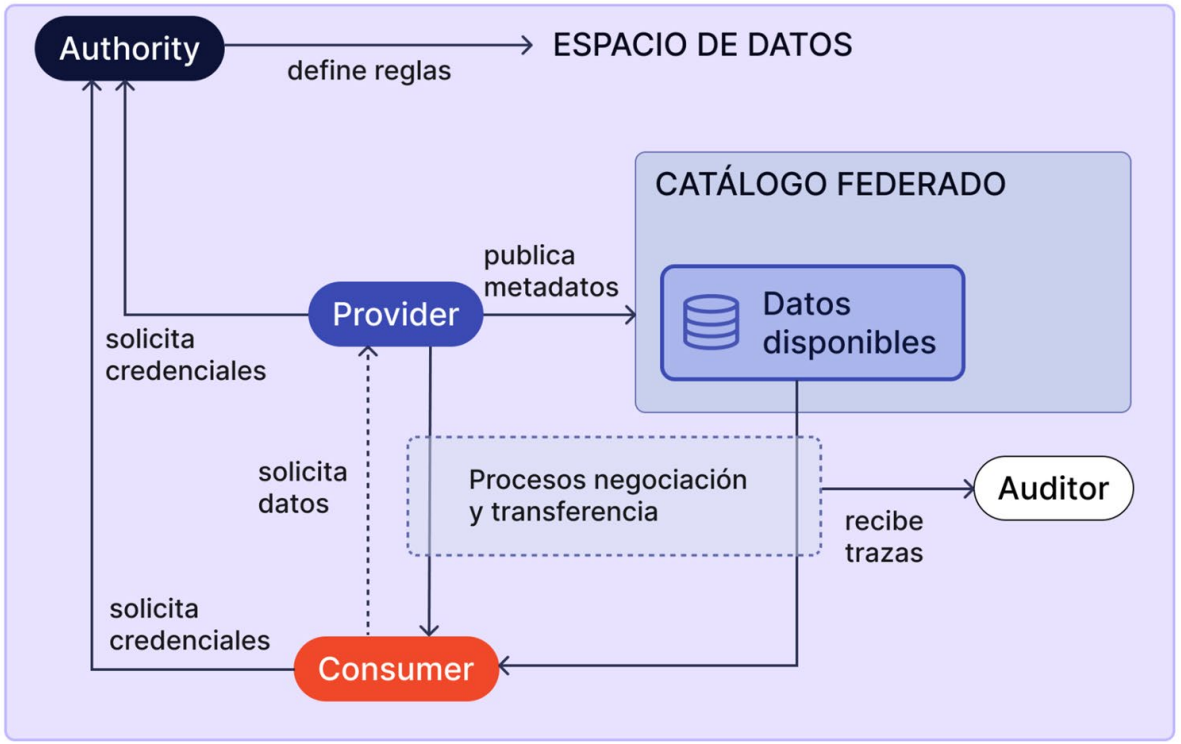
Provider: organization with available data that wants to be part of the data space. It has end systems (APIs, streaming).

Consumer: organization that wants to consume data from providers. Orchestrate requests or receive streams.

Authority: A consortium that defines the rules of the space (accepted credentials, trust anchors, policy profiles, and catalog). Service Registration.

Catálogo federado: Catalog where participants register offers. Enable discovery.

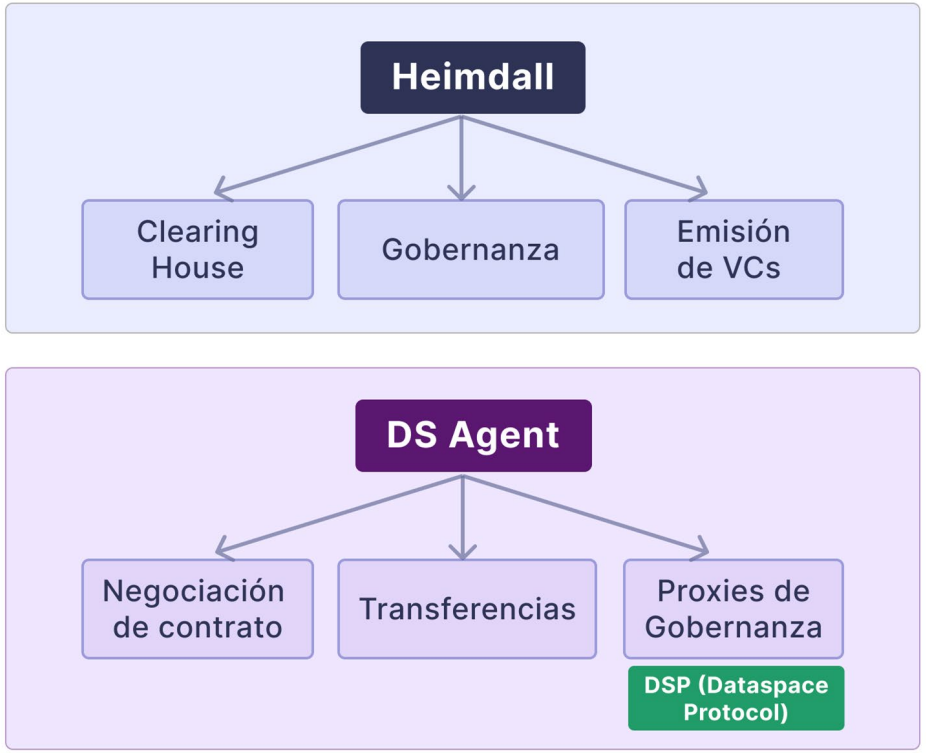
Auditor: receives traces of negotiation and transfer, persists them on Blockchain for audit.



Eunomia Framework

Component framework to generate a data space from scratch. Main components:

- **Eunomia Heimdall:** software for the Authority (clearing house, governance, VC issuance, etc.)
- **Eunomia DS-Agent:** agents for contract negotiation, transfer, and governance proxies for data exchange Implements DSP (Dataspace Protocol) to ensure interoperability between different component vendors.

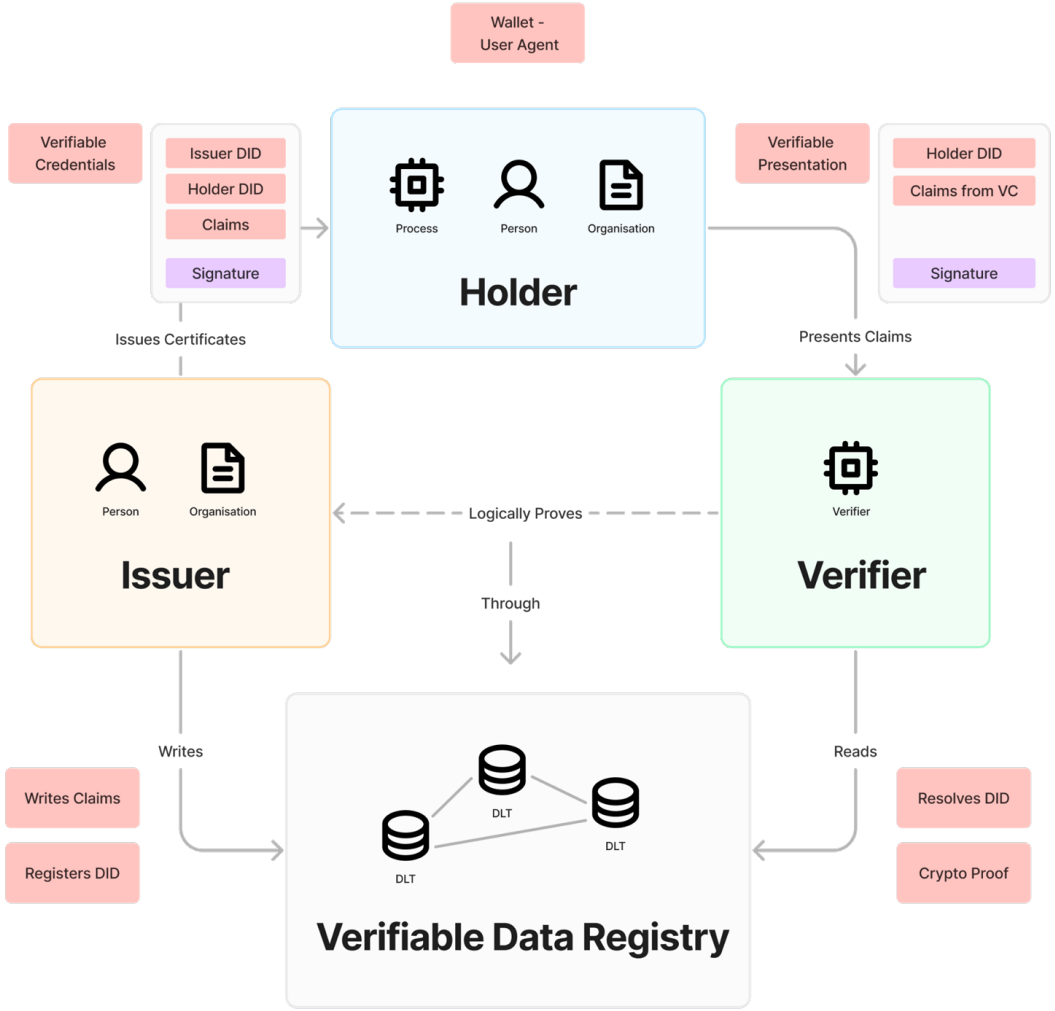


Demostration (video)

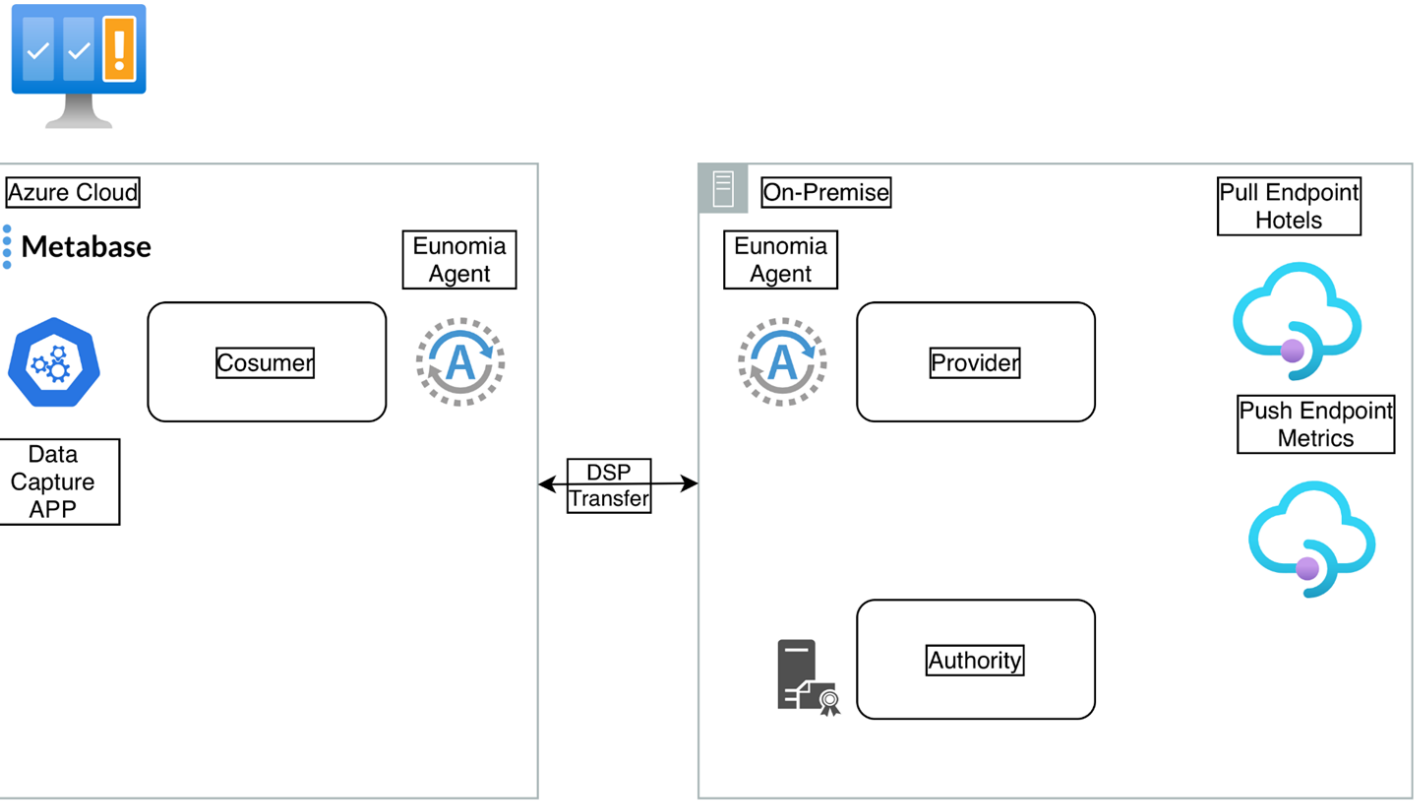
Data Space Authoriry

Onboarding

- Data Space AUthority manages:
  - **Onboarding process (wallet)**
  - **Get Credential based on certificates**
  - **Get VC**
  - **Present VC**
  - **Approve participants**



Scenario Overview



1 Provider

1 Consumer

1 Authority

2 Servers:

1 Azure

1 UPM On Premise

Transport protocol

DSP Interation for transfer

Dataflow scenario

For pull and push includes:

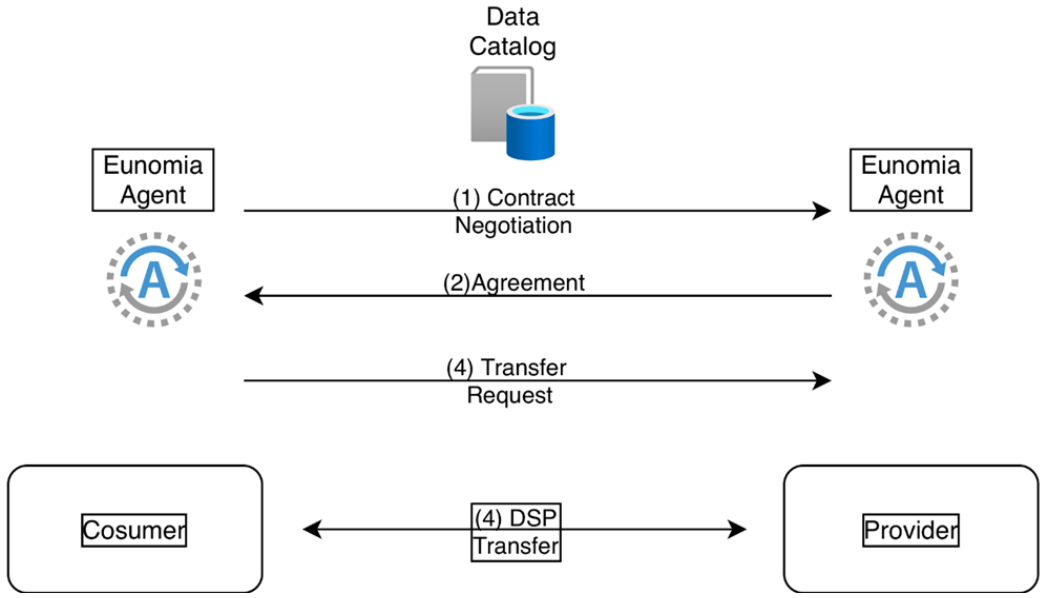
Contract Negotiation

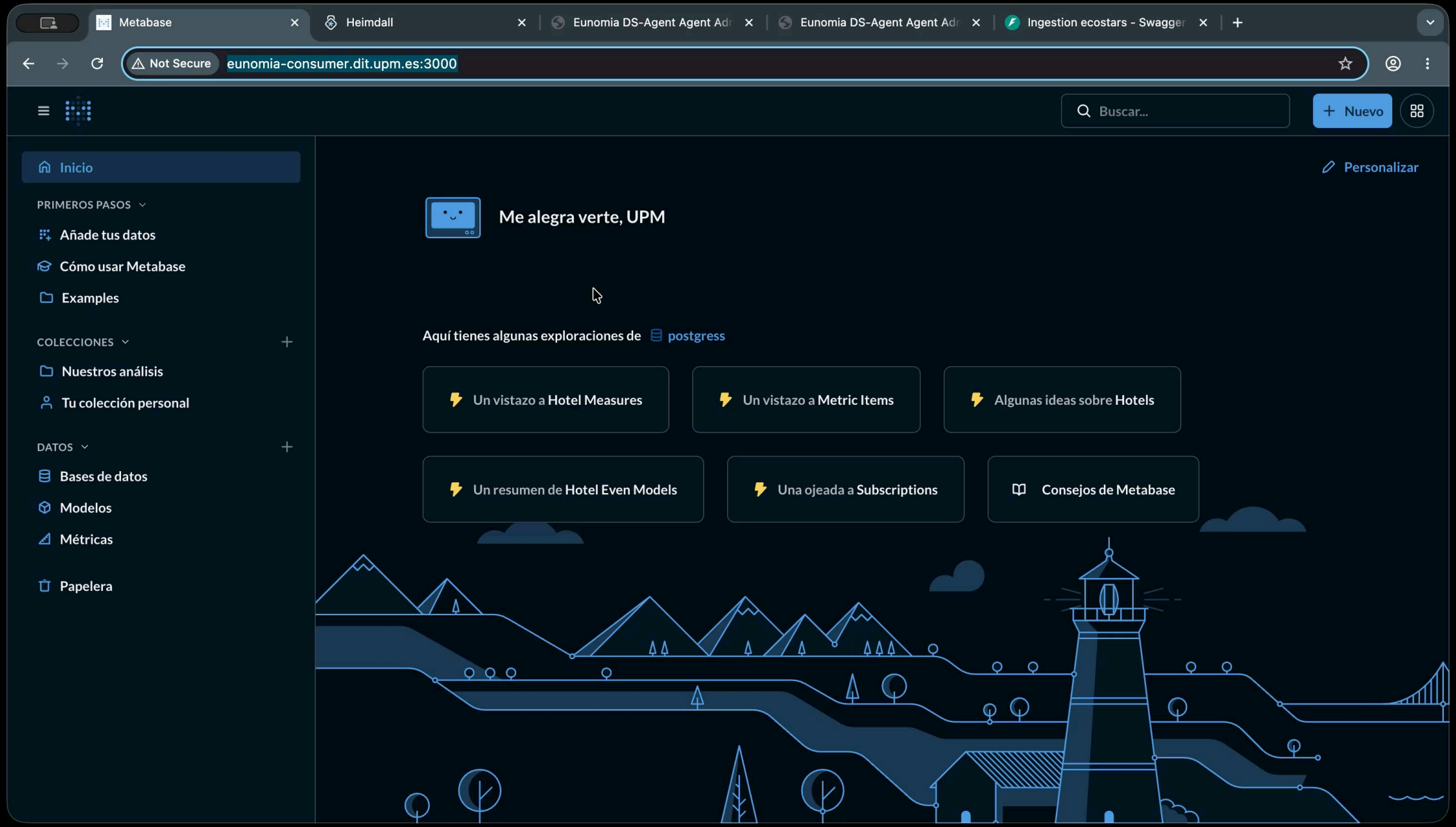
Agreement

Transfer Request

Start Transfer

End to End includes the data visualization on the consumer side using Metabase




Metabase
Heimdall
Eunomia DS-Agent Agent Ad
Eunomia DS-Agent Agent Ad
Ingestion ecostars - Swagger
Not Secure
eunomia-consumer.dit.upm.es:3000
Buscar...
Nuevo
Inicio
PRIMEROS PASOS
Añade tus datos
Cómo usar Metabase
Examples
COLECCIONES
Nuestros análisis
Tu colección personal
DATOS
Bases de datos
Modelos
Métricas
Papelera
Personalizar
Me alegra verte, UPM
Aquí tienes algunas exploraciones de postgress
Un vistazo a Hotel Measures
Un vistazo a Metric Items
Algunas ideas sobre Hotels
Un resumen de Hotel Even Models
Una ojeada a Subscriptions
Consejos de Metabase

New things in the works

ODRL Execution Approach

- Different subprofiles
  - Translation (transpilation) into different technologies
  - openFGA Access Control (REBAC)
  - Access Usage Control with Apache Flink Complex Event Processing

- Behavior Detection/ prohibitions.
  - Translation to CSP (Communicating Secuential Process) Formal Process algebra.
  - Compiler to Go/Gorrutines (CSP-based).
  - Certain prohibition checks with Model Checking (TLA+).

- Implementation of the proposed W3C ODRL Profile

Interoperability Pathway Data space definition language

- Data Space Definition Language (to
  - YAML declarative
  - PDDL Workflow of steps to be carried out.

- Actuals experiments allow to generate it via prompts (“gemma 4”).
- Integration with Apache Camel for data injection / modification.
- Policy enforcement via Apache Flink CEP capabilities.

- Conformance test suit and service
  - Tests based on the interoperable Europe compatibility frameworks.
  - Existing for the DSP currently.
  - Extensible to the entire operation of the Data Space.
  - Validation prior to interconnection and operation.

Advanced data space Protocol (ongoing work)

- Expanding the different planes
  1. Communication (firewalls and complex deployments)
  2. Data (Advanced Interconnect +
  3. Trust – ODRL
  4. Governance – Data lineage.
  5. Payments and consideration
  6. TRUST and SSI
  7. Advanced Control

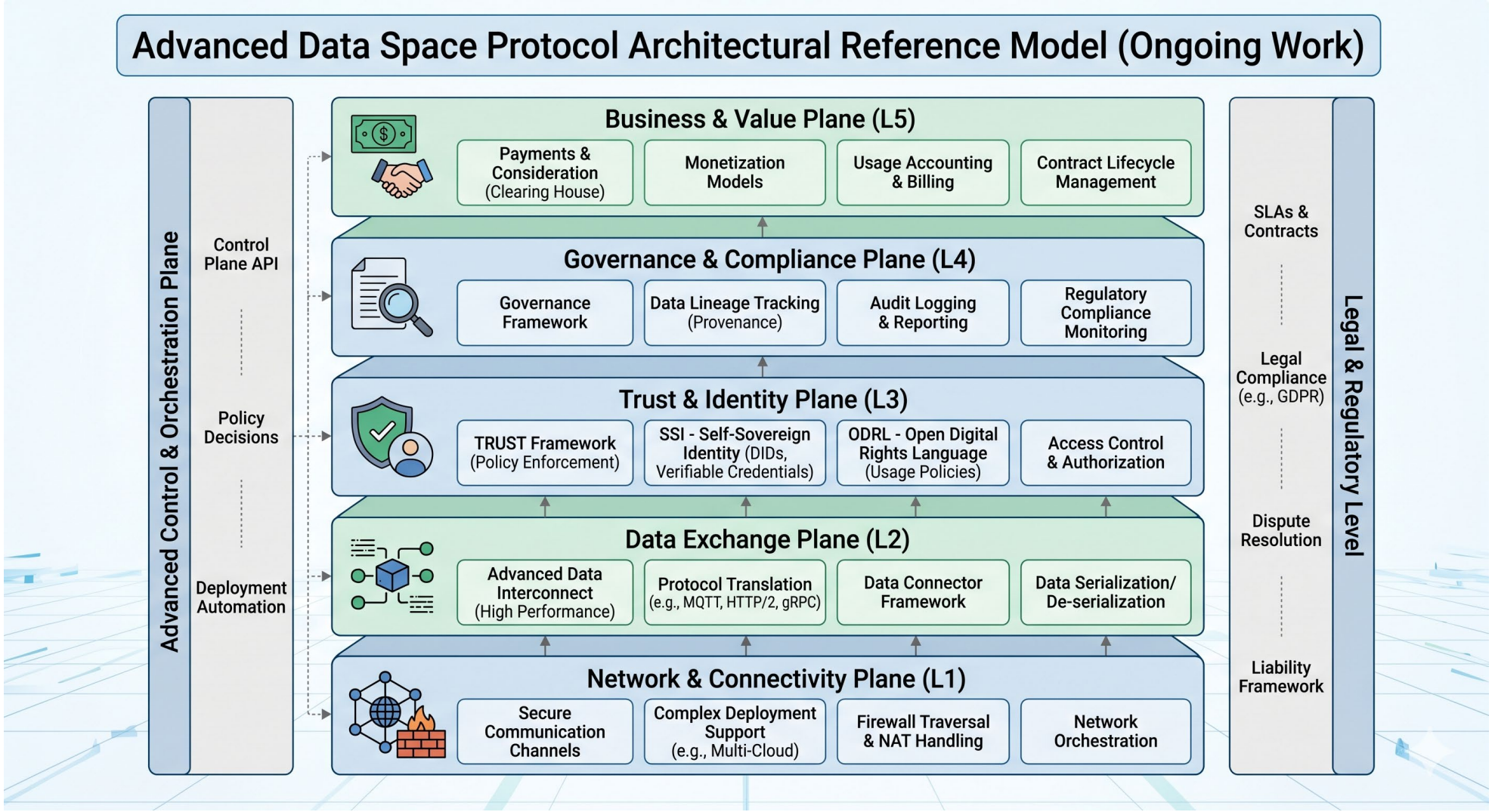
  8. Legal level.

Simplification of complementary operating modes and specification Advanced deployment

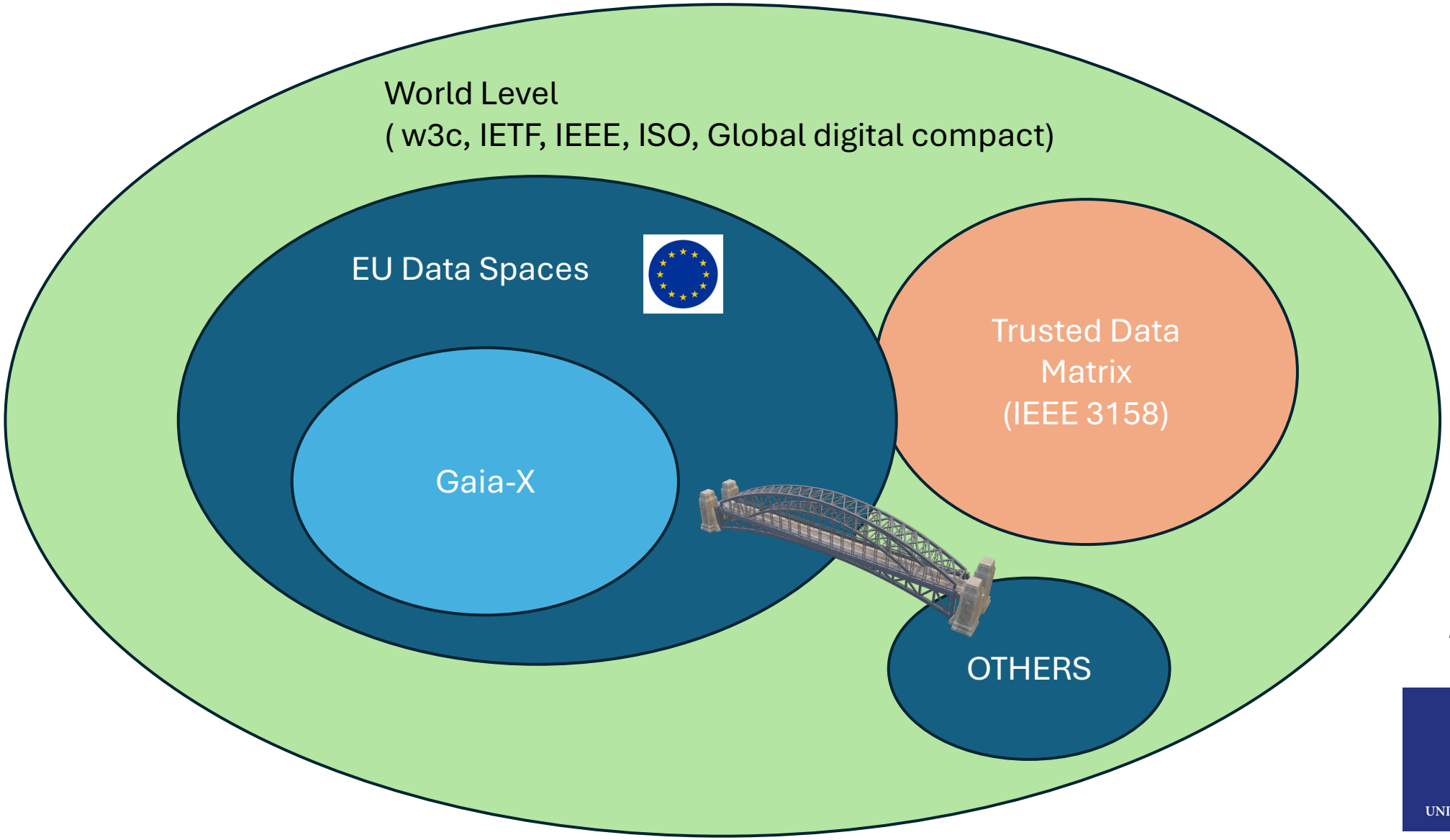
Federated / distributed catalog implementation

Trust Distributed Model : integration persona project

Easy API exposed (declarative mode).



#GaiaX #TechX26



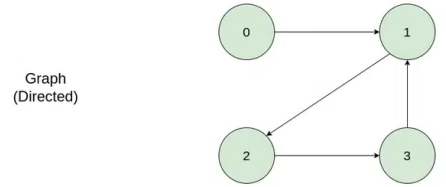
Fuzzy logic
Trust model

UNITED FEDERATION of PLANETS

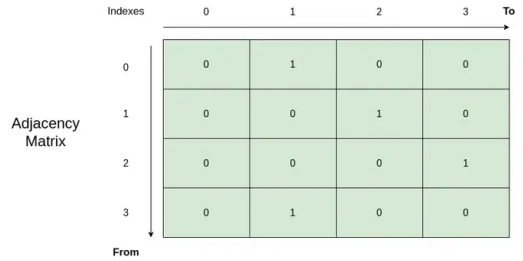
#GaiaX #TechX26

Eficient implementation for RDF

Love/hate with most of the graph implementations



- Ongoing solution
  - A graph is a matrix
  - Producing a shacl verificator based on matrix implenta
  - Slow to produce, very fast to execute.



- First experiences looks fine.

Thank you!

Name| email

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

Q&A

12:45 – 13:00

- **Gaia-X CTO Team**

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

Networking Lunch/AR Game
13:00 – 14:15

Agenda | Day 2 (Afternoon) | 29.05.26

Time	Slot	Speaker(s)
14:15 – 14:30	Hackathon Winner Announcement	Christoph F. Strnadl (Gaia-X)
14:30 – 14:45	Hackathon Presentation – 3rd Winner	
14:45 – 15:00	Hackathon Presentation – 2nd Winner	
15:00 – 15:15	Hackathon Presentation – 1st Winner	
15:15 – 15:30	Closing Tech-X	▪ Kosmas Alexopoulos LMU Uni Patras & Gaia-X Hub Greece ▪ Christoph F. Strnadl Gaia-X

Hackathon Winner Announcement

14:15 – 14:30

- **Christoph F. Strnadl –** Gaia-X

In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

Closing Tech-X

15:15 – 15:30

- **Christoph F. Strnadl –** Gaia-X
- **Kosmas Alexopoulos –** Laboratory for Manufacturing Systems & Automation (LMS), University of Patras; Coordinator Gaia-X Hub Greece

In partnership with