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

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

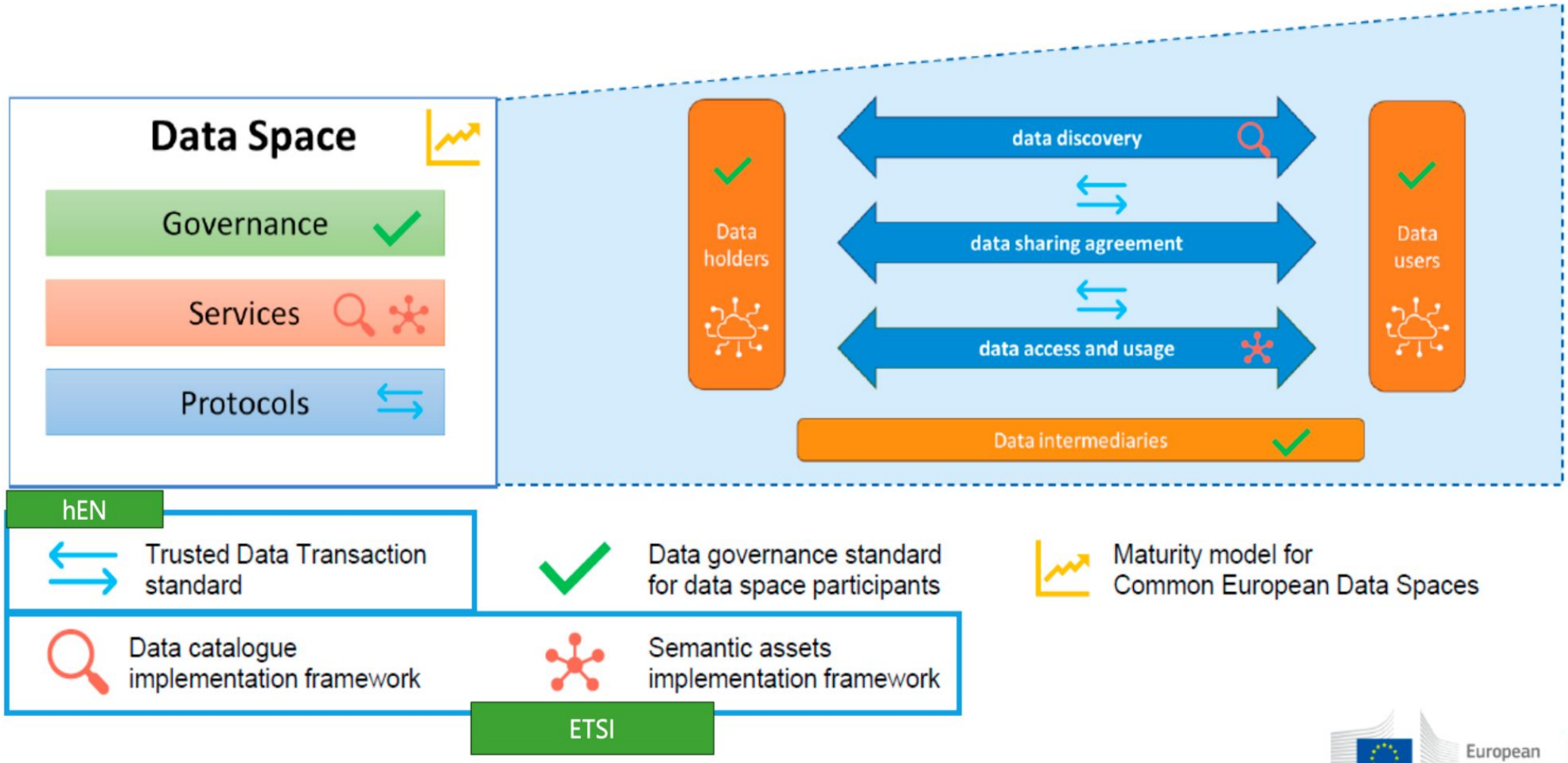
In partnership with

gaia-x Hub Greece

LMS Laboratory for Manufacturing Systems & Automation

Friday 29 May – 11:30

European Trusted Data Framework



Harmonised European standard Trusted Data Transactions

European Commission
DG Connect

EU Trusted Data Framework

Published

Standardisation Request M/614

European Data Act Article 33

Pre-standardization

CEN Workshop on Trusted Data Transaction

- Part 1: **Terms, concepts & mechanisms**
- Part 2: **Trustworthiness Requirements**

Completed

Standardization

CEN JTC 25 Working Group 2 : Data Spaces

- Part 1: **Terms, concepts & mechanisms**
- Part 2: **Trustworthiness Requirements**
- Part 3: **Interoperability Requirements**

Part 1: published EN 18235-1:2026	In advance of EU deadline
Part 2: Public enquiry (comments resolution)	Done
Part 3: Public enquiry (May 28 2026 > Aug 22 2026)	Started

Presumption of conformity

Harmonised European Standard (hEN)

Status/Targets:

P1: **published**
P2: Nov 1 2026
P3: May 1 2027

EUROPEAN COMMITTEE FOR STANDARDIZATION

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.

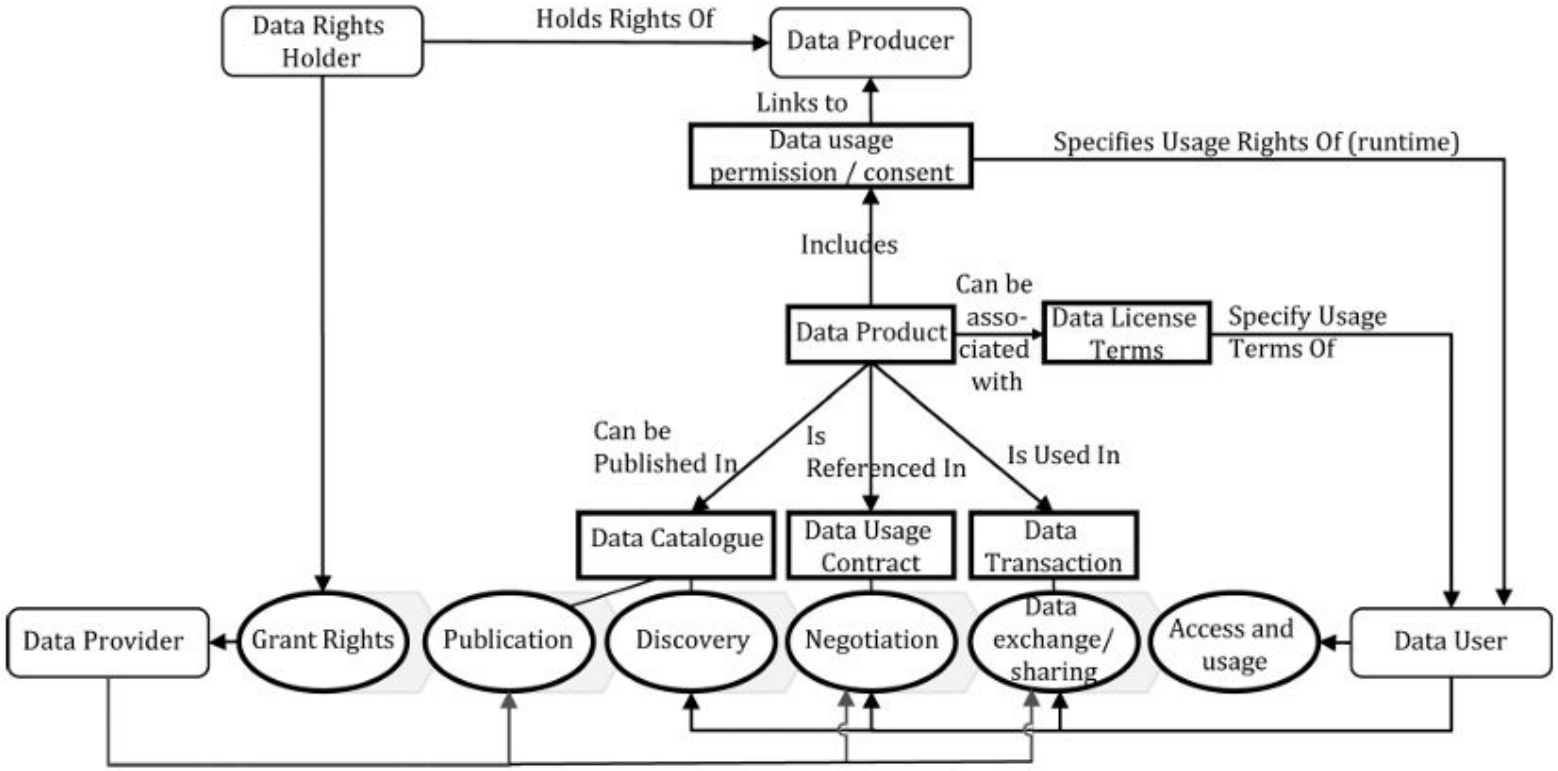


Figure1 — Scope of data transaction

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 metadata 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.

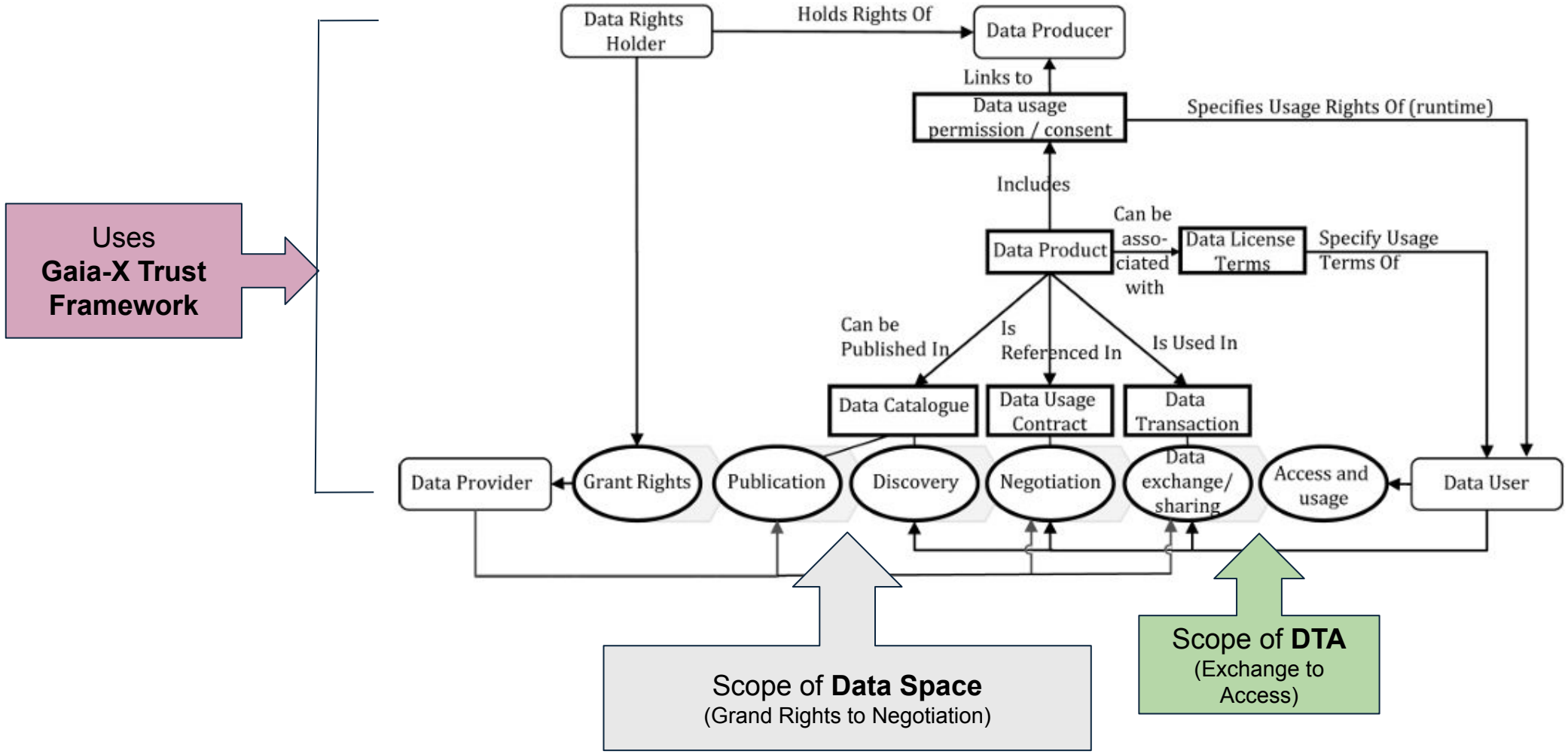
Machine-readable contracts · § 5.6
Negotiation phase: undisputable, data usage contracts.

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)

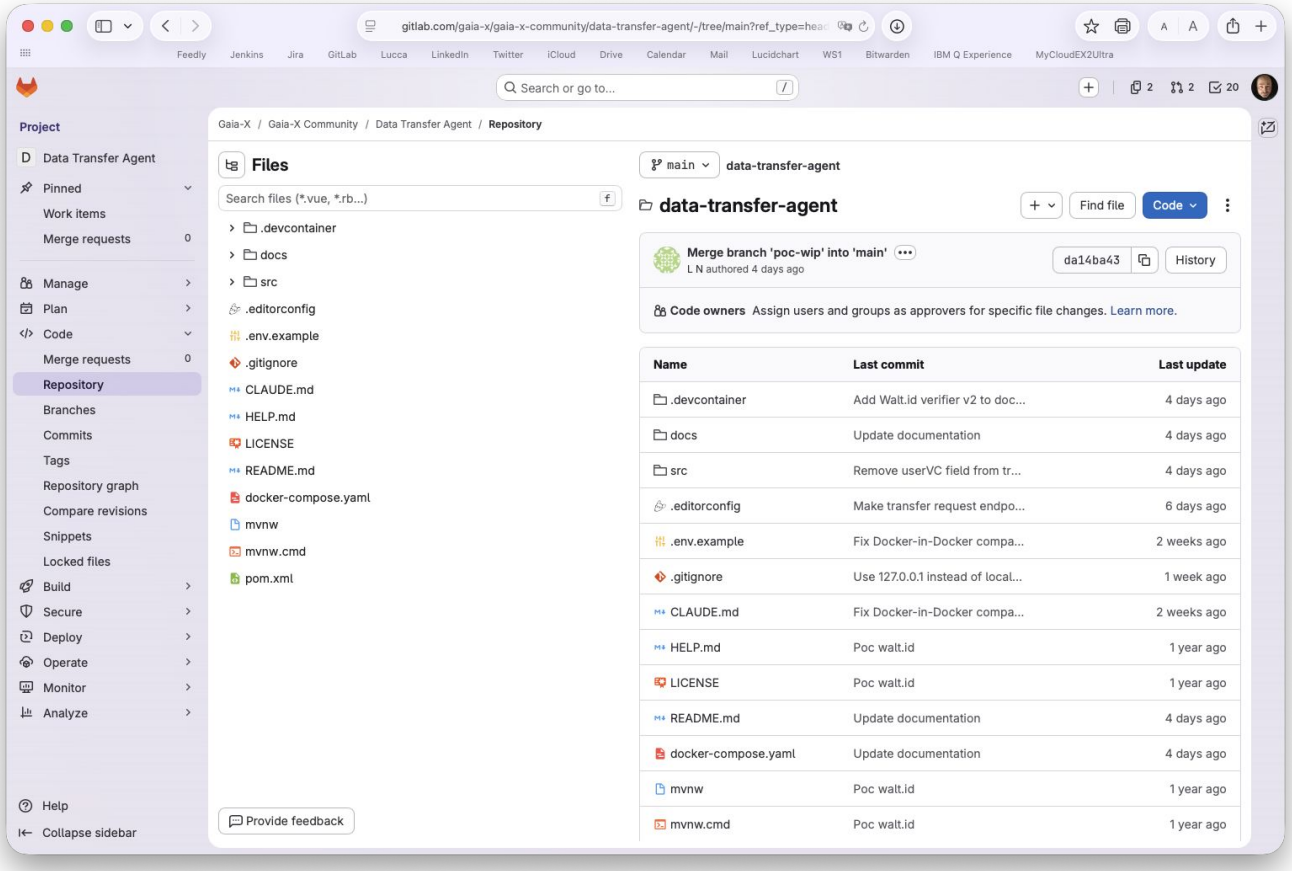
- Implement missing metadata (party credentials, DAC, etc.)
- Complete specifications (DAC, Observability)

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