



Gobernanza de espacios de datos y el papel de Gaia-X

Gaia-X European Association for Data & Cloud AISBL

01

¿Qué es realmente Gaia-X?

¿Qué es realmente Gaia-X?

Gaia-X Trust Framework

Gaia-X Technical Compatibility Specs

- Gaia-X [Architecture doc](#)
- Gaia-X [Data Exchange doc](#)
- Gaia-X [Identity, Credential and Access Mgmt doc](#)
- Gaia-X [Ontology](#)
- Gaia-X Extension Mechanism/ Architecture



**Technical Compatibility Kit (TCK)
& Reference Software Toolkit**

Gaia-X [Compliance Document](#)

- Gaia-X Labels: *Standard Compliance* and *Levels 1 to 3*
- Applicable to ICT services, data exchange services, and Participants

Geog. & Domain rules following the Gaia-X [Extension Fwk](#) or **BYOR**



[Gaia-X Digital Clearing Houses](#)

Gaia-X [Endorsement Programme](#) for

- Gaia-X Qualified Project
- Gaia-X Lighthouse Project
- Gaia-X Lighthouse Ecosystem



Assessment
based on endorsement criteria

¿Qué es realmente Gaia-X?

Gaia-X Trust Framework

Gaia-X Technical Compatibility Specs

- Gaia-X [Architecture doc](#)
- Gaia-X [Data Exchange doc](#)
- Gaia-X [Identity, Credential and Access Mgmt doc](#)
- Gaia-X [Ontology](#)
- Gaia-X Extension Mechanism/ Architecture



Technical Compatibility Kit (TCK)
& Reference Software Toolkit



Gaia-X Digital Clearing Houses

Analogía: La *Gaia-X Tech Compatibility* es el formato de un pasaporte, para que sea legible en diferentes 'Puertos de Entrada'

Gaia-X Endorsement Programme for

- Gaia-X Qualified Project
- Gaia-X Lighthouse Project
- Gaia-X Lighthouse Ecosystem



Assessment
based on endorsement criteria

¿Qué es realmente Gaia-X?

Gaia-X Trust Framework

Gaia-X Technical Compatibility Specs

- Gaia-X [Architecture doc](#)
- Gaia-X [Data Exchange doc](#)
- Gaia-X [Identity, Credential and Access Mgmt doc](#)
- Gaia-X [Ontology](#)
- Gaia-X Extension Mechanism/ Architecture



Technical Compatibility Kit (TCK)
& Reference Software Toolkit



Gaia-X [Compliance Document](#)

- Gaia-X Labels: *Standard Compliance* and *Levels 1 to 3*
- Applicable to ICT services, data exchange services, and Participants

Geog. & Domain rules following the Gaia-X [Extension Fwk](#) or **BYOR**

[Gaia-X Digital Clearing Houses](#)

Analogía: La *Gaia-X Compliance* son las reglas de los visados de entrada y estancia en el país

Gaia-X [Endorsement Programme](#) for

- Gaia-X Qualified Project
- Gaia-X Lighthouse Project
- Gaia-X Lighthouse Ecosystem



Assessment
based on endorsement criteria

¿Qué es realmente Gaia-X?

Gaia-X Trust Framework

Gaia-X Technical Compatibility Specs

- Gaia-X [Architecture doc](#)
- Gaia-X [Data Exchange doc](#)
- Gaia-X [Identity, Credential and Access Mgmt doc](#)
- Gaia-X [Ontology](#)
- Gaia-X Extension Mechanism/ Architecture



Technical Compatibility Kit (TCK)
& Reference Software Toolkit

Gaia-X Compliance Document

- Gaia-X Labels: *Standard Compliance and Levels 1 to 3*
- Applicable to ICT services, data exchange

Analogía: Los sistemas electrónicos de entrada a un país, que leen un pasaporte y generan un sello acorde a las características del visitante y las reglas entre estados

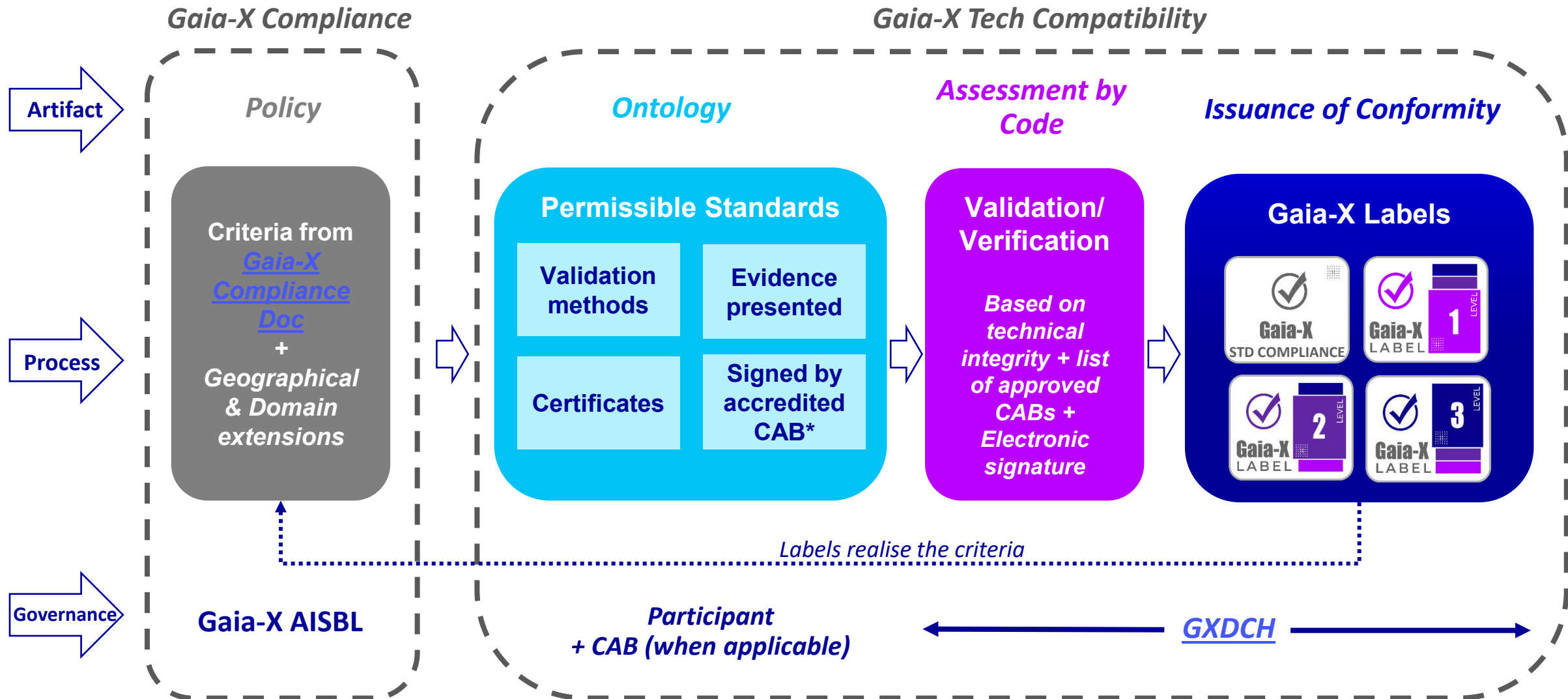
Gaia-X [Endorsement Programme](#) for

- Gaia-X Qualified Project
- Gaia-X Lighthouse Project
- Gaia-X Lighthouse Ecosystem



Assessment
based on endorsement criteria

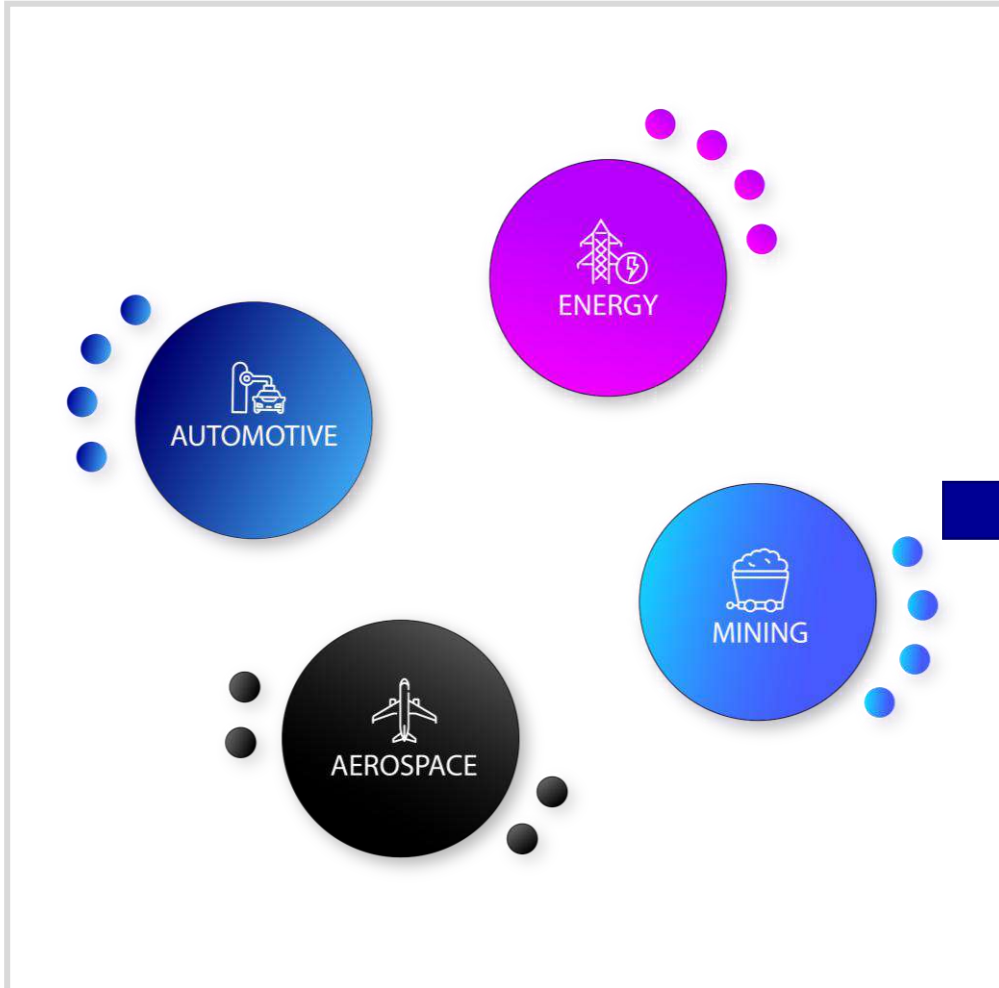
Technical Validation & Verification as a Service



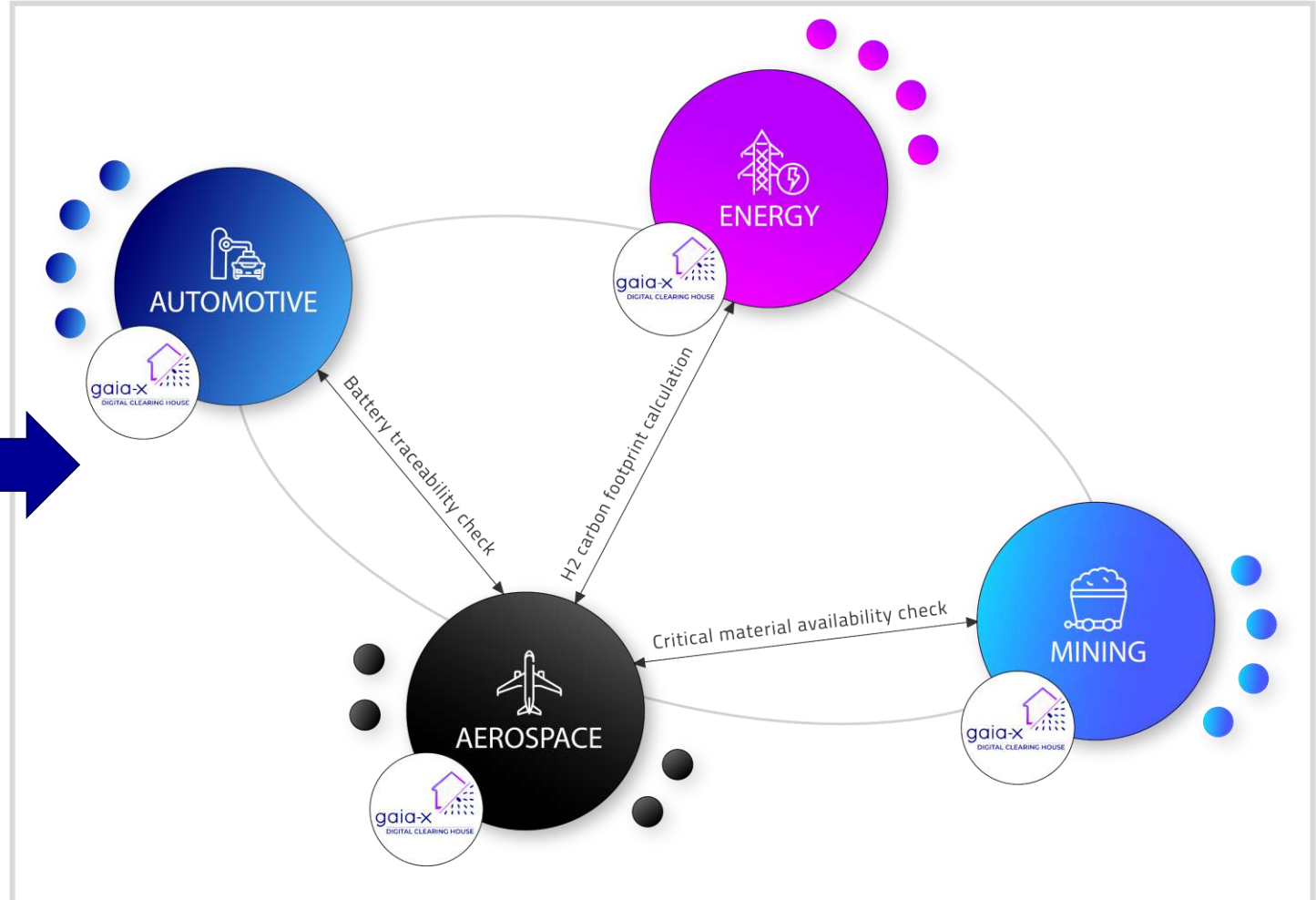
* CAB: Conformity Assessment Body, a type of [Trust Anchor](#)

Interoperable Decentralised Digital Ecosystems

BEFORE= SILOES



AFTER= INTEROPERABLE DOMAINS

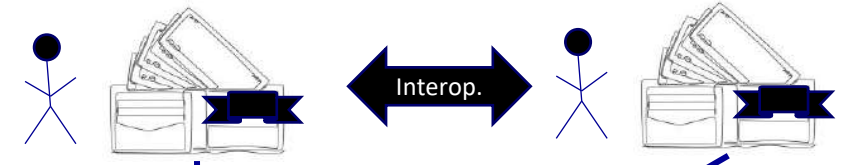
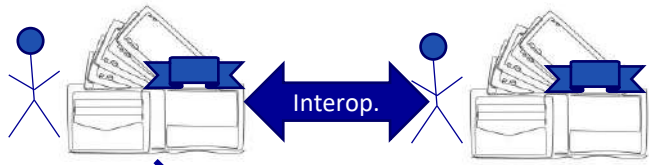


02


Gaia-X en la práctica: Automated Compliance

Scenario 1: Ecosystem Rulebook


→ Badges mean participants fulfils a given ecosystem rulebook




Domain A
Defines
Policy Rules
schema, Trust
anchors,
Validation methods



 Provide validation and verification

Domain B
Defines
Policy Rules
schema, Trust
anchors,
Validation methods





 Provide validation and verification

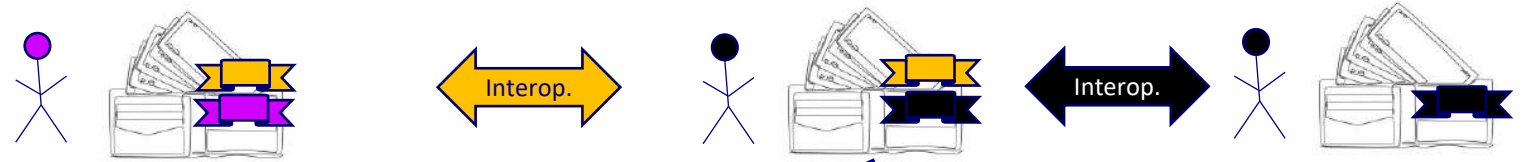
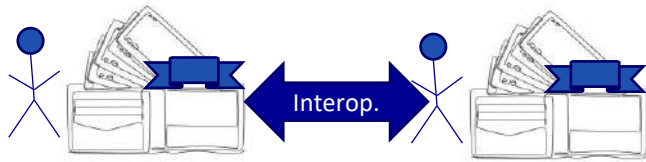
Domain C
Defines
Policy Rules
schema, Trust
anchors,
Validation methods

 Provide validation and verification


 Participants
 Gov. Authority

Scenario 2: Cross-Ecosystem Rulebook


- Fulfils a given ecosystem rulebook ( ,  , )
- ⋯→ Fulfils rulebook agreed  between two ecosystems



Domain A
 Defines
 Policy Rules
 schema, Trust
 anchors,
 Validation methods


 Provide validation and verification


Domain B
 Defines
 Policy Rules
 schema, Trust
 anchors,
 Validation methods



 Provide validation and verification

Need agree
 on (some)
 common
 Schema,
 Trust Anchors









Domain C
 Defines
 Policy Rules
 schema, Trust
 anchors,
 Validation methods

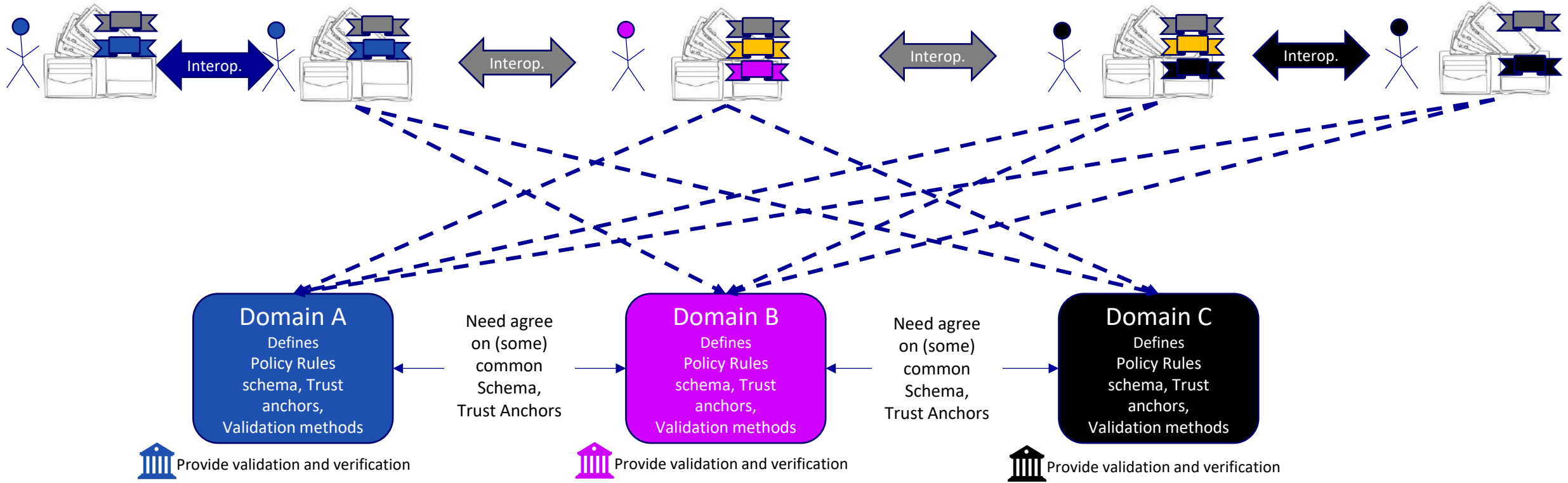
 Provide validation and verification


 Domain-specific
 (e.g. compliance to specific
 regulation or standards)


 Participants
 Gov. Authority



Scenario 3: Global Rulebook

-  Fulfils a given ecosystem rulebook (, , )
-  Fulfils rulebook agreed  between two ecosystems
-  Fulfils global rulebook 











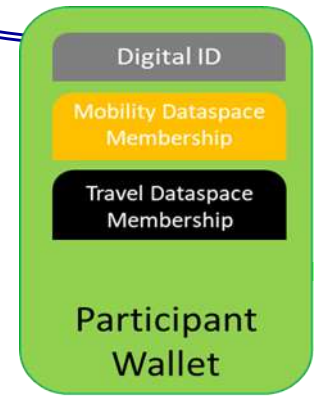
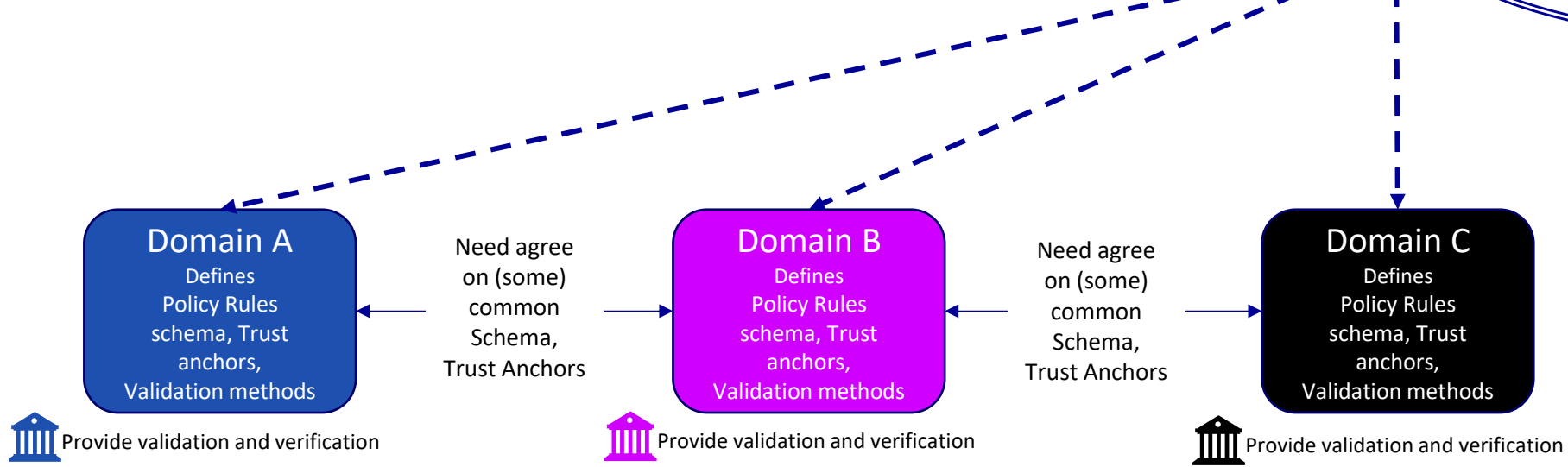
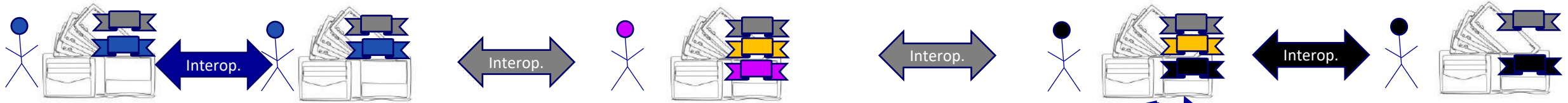
 Common
(e.g. availability of a digital ID)

 Domain-specific
(e.g. compliance to specific regulation or standards)


 Participants
 Gov. Authority


Ecosystem Trust Federation

-  Fulfils a given ecosystem rulebook (, , )
-  Fulfils rulebook agreed  between two ecosystems
-  Fulfils global rulebook 



Key feature is that participants bring their own credentials, stored within their wallets

 Common (e.g. availability of a digital ID)

 Domain-specific (e.g. compliance to specific regulation or standards)

A single (operational) model allows to present & verify the same credentials across different ecosystems

This leads to automated onboarding and scalable organisational interoperability

03

Rulebooks como elemento clave en espacios de datos

¿Qué es un espacio de datos?

- Un ecosistema donde diferentes participantes **comparten** datos (y servicios) de forma controlada y descentralizada
- Basado en la confianza, bajo unas reglas claras y la creación de valor mutuo
- No es sólo tecnología, sobre todo es **colaboración estructurada**

Creación de (nuevo) valor

- Permiten nuevos casos de uso *data-driven*
- Mejoran la eficiencia, la transparencia y la toma de decisiones
- Activan nuevas oportunidades en torno a la economía del dato

El ecosistema es la clave

- Los participantes definen (sistémicamente) el valor del espacio de datos
- Sus roles, relaciones y dinámicas son el punto de partida
- **¡Sin ecosistema, no hay espacio de datos!**

Gobernanza en Espacios de Datos

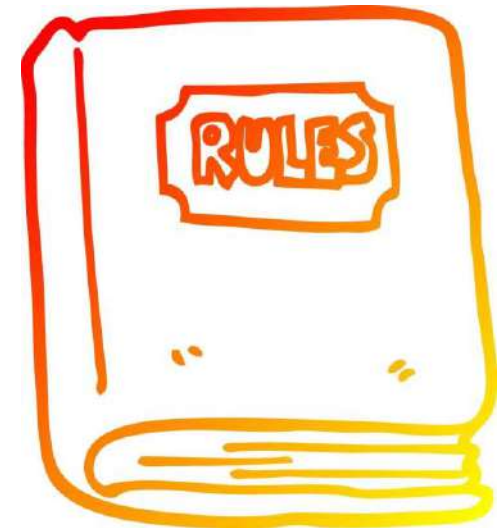
Gobernanza: El habilitador estratégico

- La **gobernanza** define cómo se comparten los datos, entre quiénes, quién tiene derecho a usarlos y para qué finalidad, y cómo
- Reduce riesgos legales, operativos y competitivos
- Hace posible la confianza entre los participantes



El *Rulebook* (Libro de Reglas) como pieza central

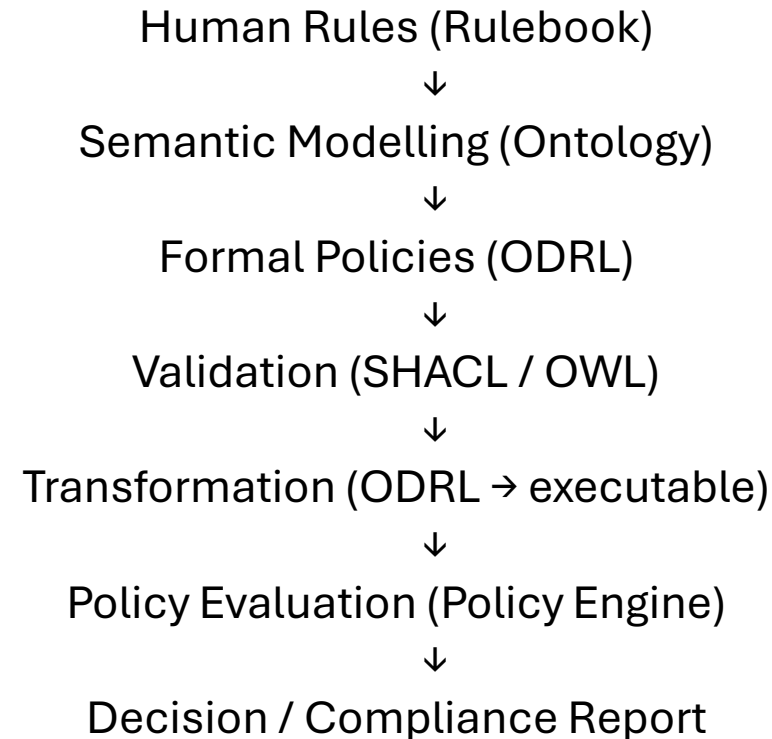
- Materializa la gobernanza de dicho espacio de datos
- Convierte acuerdos en reglas claras, que dan forma a una ontología
- Es la base para los acuerdos contractuales
- También para la plataforma tecnológica, basa en componentes software



Espacios de datos: Pipeline de '*compliance-as-code*'



Cómo pasar de reglas humanas (*rulebooks*) → reglas *machine-readable* → *compliance* automatizado



From Rulebook to Automated Compliance



Fase	Input	Output	Tecnologías
0. Rulebook	Texto humano	Reglas estructuradas	—
1. Ontología	Reglas	Modelo semántico	OWL, RDF
2. ODRL	Ontología	Policies	ODRL, JSON-LD
3. Enrichment	Policies	Policies + contexto	VC, JSON-LD
4. Validación	Policies	Policies válidas	SHACL
5. Transformación	ODRL	Reg / ejecutable	OPA
6. Evaluación	Request	Decision	PDP/PEP
7. Compliance	Logs	Reporte	RDF, SPARQL

OWL: Web Ontology Language
RDF: Resource Description Framework
ODRL: Open Digital Rights Language
VC: Verifiable Credential
JSON-LD: JavaScript Object Notation for Linked Data
SHACL: Shapes Constraint Language
OPA: Open Policy Agent
PDP: Policy Decision Point
PEP: Policy Enforcement Point
SPARQL: SPARQL Protocol and RDF Query Language

El Rulebook como Punto de Partida



La Gobernanza como elemento **estratégico**, no sólo técnico:

El *rulebook* no es documentación: es el mecanismo que convierte un conjunto de organizaciones en un **sistema coordinado capaz de generar valor**.

Alineamiento de valor

Pregunta clave: ¿por qué participa cada actor?

El *rulebook*:

- define el valor esperado
- evita desequilibrios
- hace explícito el ‘win-win’

Modelo de gobernanza

Pregunta clave: ¿quién decide qué?

El *rulebook*:

- define autoridad
- define procesos
- define evolución

Reglas de interacción

Pregunta clave: ¿cómo interactúan los actores?

El *rulebook* define:

- acceso
- uso
- responsabilidades

Confianza

Pregunta clave: ¿por qué confiar?

El *rulebook* introduce:

- accountability
- auditabilidad
- enforcement

Gobernanza de Espacios de Datos en la Práctica



Caso de uso (análisis de procesos):

Regla de gobernanza

Lenguaje común (ontología)

Arquitectura espacio de datos

El OEM está autorizado a utilizar los **datos de** inventario y capacidad de producción compartidos por el Proveedor **exclusivamente para** el cálculo de sus algoritmos internos de Planificación de Requerimientos de Materiales (MRP) y optimización de Just In Time (JIT), con una **periodicidad máxima** de actualización de 24 horas. Su uso para el desarrollo de algoritmos de Process Mining **no está permitido**

- ¿**Qué datos** se pueden compartir?
- ¿**Para qué** finalidades?
- ¿Bajo qué **condiciones**?

- **Data product**: datos de inventario y capacidad
- **Purpose**: Algoritmos MRP/ JIT/ *Process Mining* **Algorithms prohibido**
- **Constraint**: periodicidad máxima de 24 h/

- Política activa en el conector
- Acceso permitido solo para los usos definidos
- Cumplimiento automático (*compliance by design*)



Principios de uso, control y cumplimiento normativo



La regla se hace explícita y compartida



Negocio, legal y tecnología hablan de lo mismo



La regla se ejecuta, no se interpreta

Gobernanza ejecutable:

Las decisiones no se quedan en un documento, se convierten en comportamiento del sistema

De Reglas Humanas a Reglas *Machine-Readable*



Rule (humano)



Ontología (lenguaje común)



ODRL (política ejecutable:
rule machine-readable)



Dataspace Connector

R-01 – Permitted Use of process XYZ Data in Supply Chain ABC

El OEM está autorizado a utilizar los datos de inventario y capacidad de producción compartidos por el Proveedor exclusivamente para el cálculo de sus algoritmos internos de Planificación de Requerimientos de Materiales (MRP) y optimización de Just In Time (JIT), con una periodicidad máxima de actualización de 24 horas. Su uso para el desarrollo de algoritmos de *Process Mining* no está permitido

```
DataProduct
└─ TechnicalDataXYZ

Purpose
├─ AITraining
├─ MRPPanning
├─ JustInTimeOptimization
└─ ProcessMiningAlgorithms (X
prohibited)
```

```
Constraint
└─ Update_frequency
```

```
ActorRole
├─ DataProvider
└─ DataConsumer
```

El DataProduct = TechnicalData puede ser usado **solo si** Purpose ∈ {AITraining, MRPPanning, JITOptimization} and Update_frequency ≤ 24 y **nunca** si Purpose = ProcessMining.

```
{
  "@context": "http://www.w3.org/ns/odrl.jsonld",
  "@type": "Policy",
  "uid": "policy-dataXYZ-ai-only",
  "permission": [{
    "target": "urn:dataprodut: technical-dataXYZ",
    "action": "use",
    "constraint": [{
      "leftOperand": "purpose",
      "operator": "isAnyOf",
      "rightOperand": [
        "AITraining",
        "MRPPanning",
        "JustInTime"
      ]
    }
  ]
}],
  "prohibition": [{
    "target": "urn:dataprodut:technical-dataXYZ",
    "action": "use",
    "constraint": [{
      "leftOperand": "purpose",
      "operator": "eq",
      "rightOperand": "ProcessMining"
    }
  ]
}]
}
```

¿Qué ocurre en tiempo de ejecución?

1. Un participante solicita acceso al *data product*
2. La solicitud incluye:
 - identidad verificada
 - *purpose* declarado
3. El *Policy Engine* del conector evalúa la política ODRL:

Purpose declarado	Resultados
AITraining	Acceso concedido
MRPPanning	Acceso concedido
ProcessMining	Acceso denegado

Rulebook Mínimo Viable (y Conexión con CRED)

Propósito del Libro de Reglas

0. Aprobación y mantenimiento del Libro de Reglas

A. Contexto y alcance del Espacio de Datos

1. Forma organizativa y objetivos
2. Marco legal, contractual y regulatorio

B. Reglas específicas del Espacio de Datos

3. Principios y objetivos de gobernanza
4. Órganos de gobernanza, comités y estructura de toma de decisiones
5. Participantes, roles y responsabilidades
6. Reglas de compartición, acceso y uso de datos

C. Operación

7. Ciclo de vida de participación
8. Resolución de disputas, reclamaciones y sanciones
9. Monitorización, auditoría y rendición de cuentas
10. Cumplimiento y validación ética
11. Comunicación y Transparencia Institucional

D. Implementación

12. Relación con los elementos técnicos del espacio de datos



Data Spaces & Gaia-X: The real challenge



Data space initiatives are not failing because of technology — they are failing because of **lack of clarity on roles, responsibilities and value creation.**

Projects often:

- Look for an **end-to-end solution**
- Expect **Gaia-X to ‘solve everything’**
- Struggle to **operationalize governance and trust**

This leads to a fundamental confusion:

A data space is not a system to deploy — it is an ecosystem to design.

Gaia-X and Data Spaces



Data Space Projects

When a sponsor/orchestrator approaches Gaia-X, they typically look for:

- a way to **build their data space**
- a solution to **onboard participants**
- tools to **exchange data**
- mechanisms to **ensure compliance**
- support to **create business value**

In other words, they are looking for a **complete ecosystem solution**.

The problem:

Gaia-X is often perceived as something that could (or should) cover all of this.

Reality: Gaia-X Has a Very Specific Role

Gaia-X operates in a **very precise layer of the ecosystem**: provides **the mechanisms to establish, verify and reuse trust across participants, services and ecosystems**.

This role is:

- transversal (used across the lifecycle)
- foundational (everything depends on it)
- but **not end-to-end**

Roles & Responsibilities across Data Space Planes



Plane	Purpose	Key Stakeholders	Core Responsibilities	Gaia-X Role	Data Space journey
ECOSYSTEM PLANE	Define value & governance	Custodians	Business model, Rulebook, incentives	✗ No direct role	Design → Growth
USAGE / CONTROL PLANE	Define & enforce usage	Orchestrators, Users, Providers	Policies, access conditions	Enables	Design → Access → Operation
DATA PLANE	Enable data exchange	Providers	APIs, exchange, interoperability	Supports	Exchange → Operation
TRUST PLANE	Establish trust	Gaia-X members, issuers, federators	Identity, compliance, verification	✓ Core (Gaia-X Trust Framework)	Onboarding → Access → Federation

- A data space is a multi-plane system - Responsibilities are **distributed**
- Gaia-X is **not everywhere**
- Gaia-X is **critical in one plane: trust** (Gaia-X does not build data spaces - it enables trust across them)

Gaia-X en el Journey *From Rulebook to Automated Compliance*

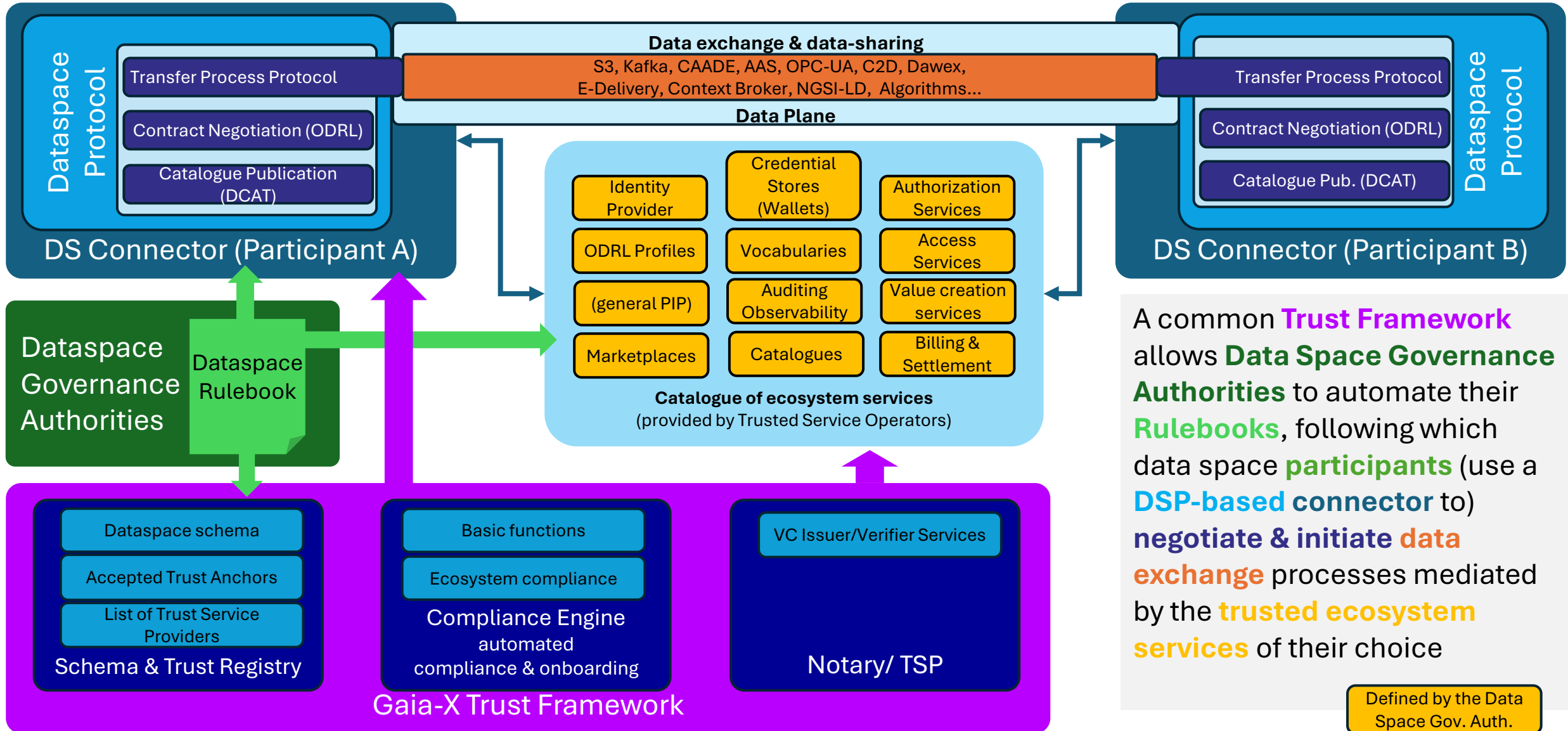


Fase	Input	Output	Tecnologías	Rol de Gaia-X	Componentes Gaia-X
0. Rulebook	Texto humano	Reglas estructuradas	—	No interviene directamente	—
1. Ontología	Reglas	Modelo semántico	OWL, RDF	✓ Proporciona vocabulario base	Gaia-X Ontology
2. Policy formalization	Ontología	Policies	ODRL	✓ Define enfoque de policies	ODRL + Gaia-X profiles
3. Enrichment	Policies	Policies + contexto	JSON-LD, VC	✓ Añade identidad verificable	Verifiable Credentials
4. Validation	Policies	Policies válidas	SHACL, OWL	✓ Define compliance rules	Gaia-X Compliance Rules
5. Transformation	ODRL	Policies ejecutables	OPA / Rego	Parcial	Policy Reasoning
6. Evaluation	Request	Decision	PDP/PEP	✓ Núcleo de Gaia-X	Gaia-X Digital Clearing House
7. Compliance	Logs	Reporte	RDF, SPARQL	✓ Verificación de cumplimiento	Compliance Services

OWL: Web Ontology Language
 RDF: Resource Description Framework
 ODRL: Open Digital Rights Language
 VC: Verifiable Credential
 JSON-LD: JavaScript Object Notation for Linked Data

SHACL: Shapes Constraint Language
 OPA: Open Policy Agent
 PDP: Policy Decision Point
 PEP: Policy Enforcement Point
 SPARQL: SPARQL Protocol and RDF Query Language

The Gaia-X Trust Framework for Data Spaces



Follow us on:



[@gaiax_aisbl](https://twitter.com/gaix_aisbl)



www.linkedin.com/company/gaia-x-aisbl



www.youtube.com/@gaia-x5188