eunomia
Data Spaces for Digital Sovereignty

POLITÉCNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

Enforcing ODRL policy in Data Spaces with the Eunomia DS Agent

Joaquin Salvachúa, Andrés Muñoz, Gabriel Huecas, Carlos Aparicio, Rodrigo Menendez

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Mission

- **Architecting the future of Data Spaces through ODRL, Formal Methods, and Sovereign Governance.**
- **Building trust through open source and interoperable open protocols (including trust and validation via Self-Soveraign Identity and ODRL).**
- Emphasis in interoperability : allow different ways to interact with other data spaces, including existing ones.
- Sematic interoperability via on the fly Ontology compatibility.
- Glue code :DSL automatic generated via Configurable infrastructure
- Develop a dataspace in 60 mins with a prompt as final goal.

Eunomia Interoperability Framework

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: Dataset discovery and policies (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).

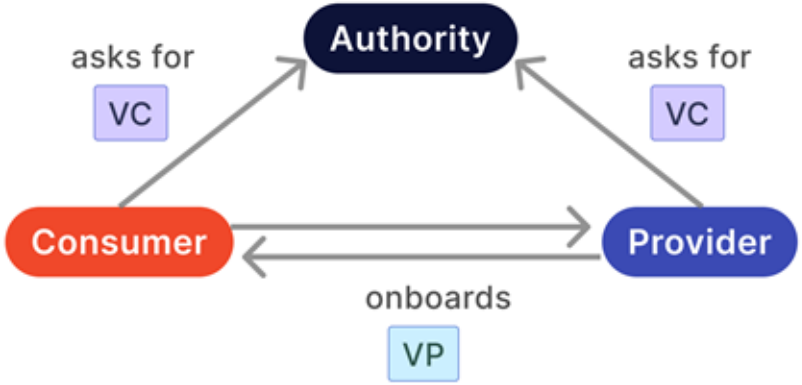
Native SSI Identity

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)

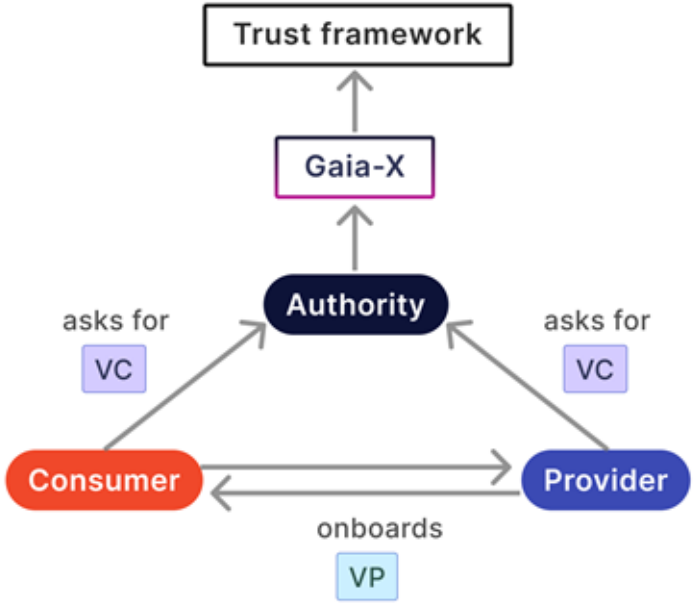
Most connectors solve the bilateral exchange, but not the governance of the ecosystem.

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.



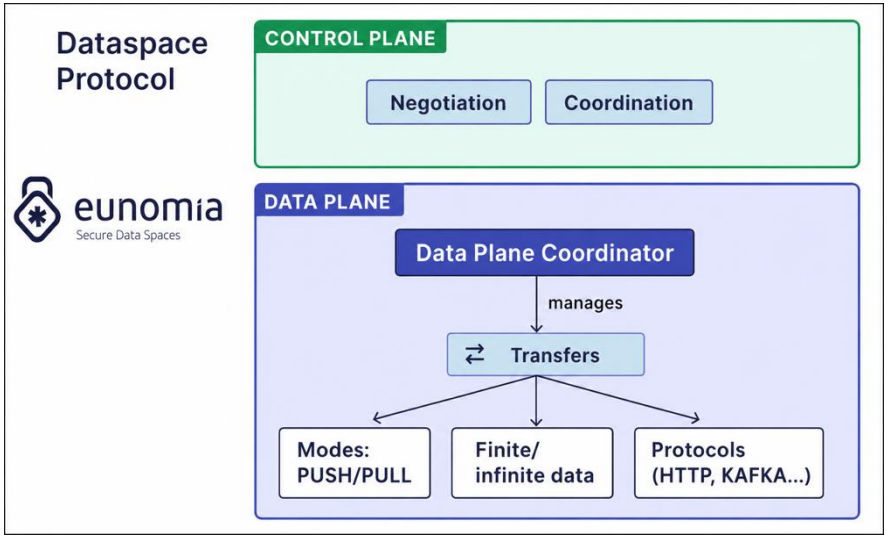
Programmable data plane

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



Ecosystem Players

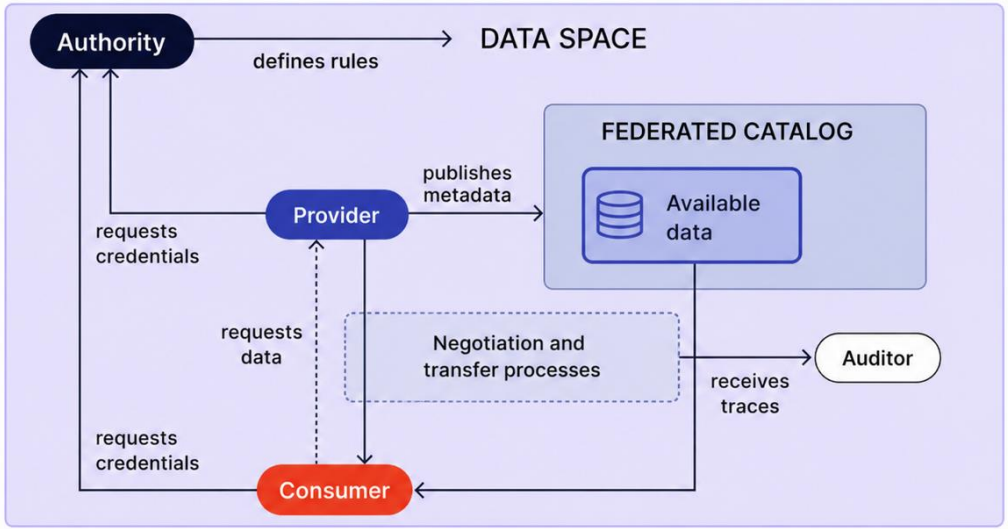
Provider: organization with available data that wants to be part of the data space. It has end systems (APIs, streaming).

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.

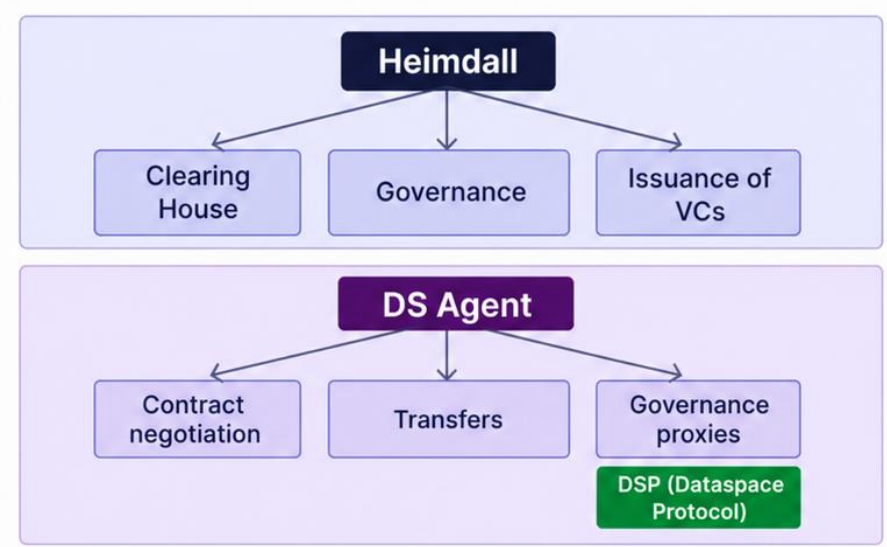
Auditor: receives traces of negotiation and transfer, persists them on Blockchain for audit.



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.



ODRL enforcement

Define a DataSpace full ODRL profile (w3c)

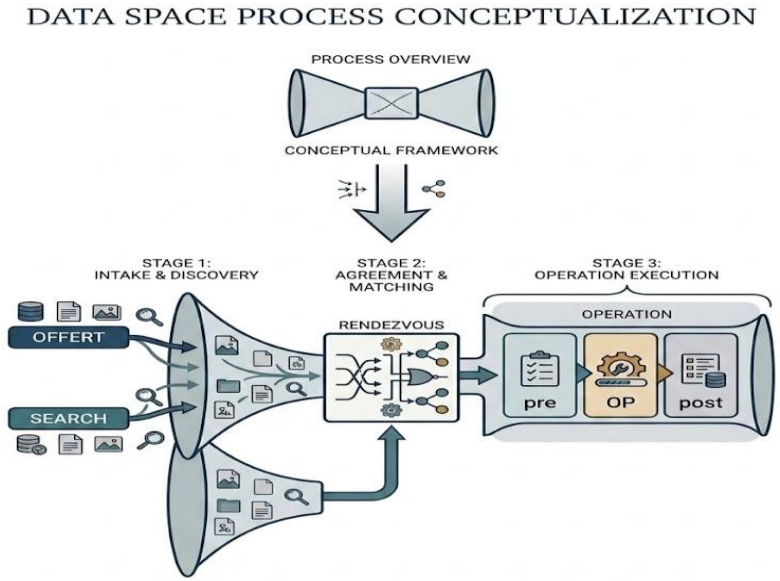
- Data Spaces has a complex workflow, that could be slightly different on each implementation.
- The behaviour for a data space may be defined using the Data Space Definition Language (RFC been developed).

- 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).

- Will be ”an umbrela” profile that Will connect with several more.

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
  - Ex: “DataOwnerX -> Permit -> Action(Read) -> Asset(Report_2026) -> Condition(<= "2026-12-31")”

- Graphical notation based on Blockly (ongoing work)

- Set notation to indicate all posible offering + semantic anotation:
  - Must / May /Maybe on the offers ODRL statements.

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.

This Will be publish into the federated distributed catalog and may be signed using VC.

DEPLOYTOUR: Ongoing requirements develop by use cases + partners

- Woking on interoperability in DEPLOYTOUR Project : interoperability between 5 current projects to provide a common Tourism Data Space.

	Policy	Description
Access policies	Access Policy	Information that indicates whether the data product is publicly accessible, has access restrictions or is not public.
	Participant Conditions	Eligible categories of organizations
Contract Policies	Data Delivery Method (API/File download, Streaming, etc)	Specifies the technical mechanism to transfer data between participants.
	Payment	Pricing plan.
	Duration (days)	Specifies for how long this price (or price component) will be billed.
	Geography Restriction	Geographic restrictions on the use of this products based on the consumer's origin.
Usage policies (permitted / prohibited actions)	Usage Permitted	Specifies the exact operations the consumer is authorized to perform with the data product. Any actions not explicitly selected are strictly prohibited for the consumer of this data product.
	Purpose	Scope of use

Operations

Pre conditions :

- Previous to start working what must be fullfilled
- What trust framework/model are we using. : requirementes about SSI-VC + what requirements (Trust Framework for GAIA-X AISBL

- Part of the Access control : Use Rebac (AWS Cedar - 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.

- Conceptually is a Data DDL algebra SubQuery : the result is the data that you could query or transmit (working on specify this).

$$Q' = \pi_{A \cap A_{cedar}}(\sigma_{C \wedge C_{cedar}}(R))$$

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.

ODRL Execution Approach :
multiple transpilation approach for each workflow step

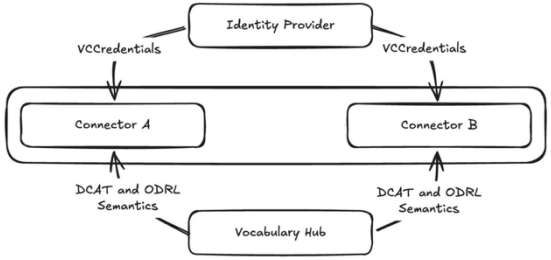
- Different subprofiles
  - Translation (transpilation) into different technologies
  - openFGA Access Control (REBAC) + REGO generation if required
  - Access Usage Control with Apache Flink Complex Event Processing

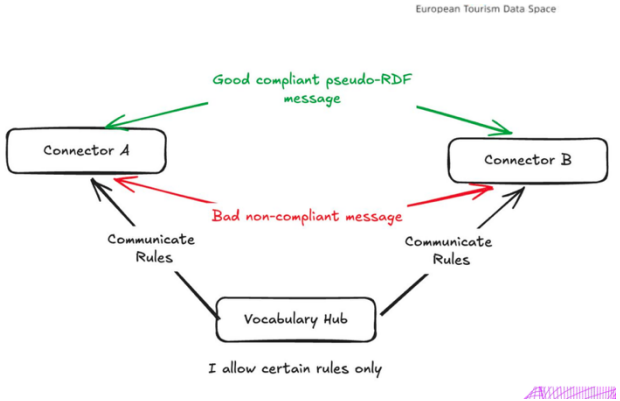
- Behavior Detection/ prohibitions. PDP/PXP
  - Translation to CSP (Communicating Secuential Process) Formal Process algebra.
  - Compiler to Go/Gorrutines (CSP-based).
  - Ongoing work.

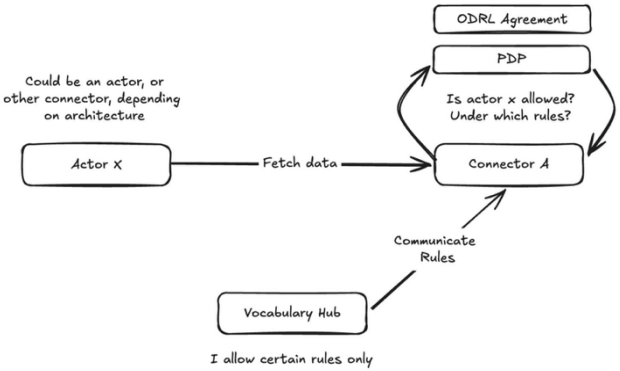
- Interaction and messages to and from the Governance Layer.

- Implementation for part the proposed W3C ODRL Profile : usage of the DEPLOYTOUR profile.

Need to be compatible with actual implementations.







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.

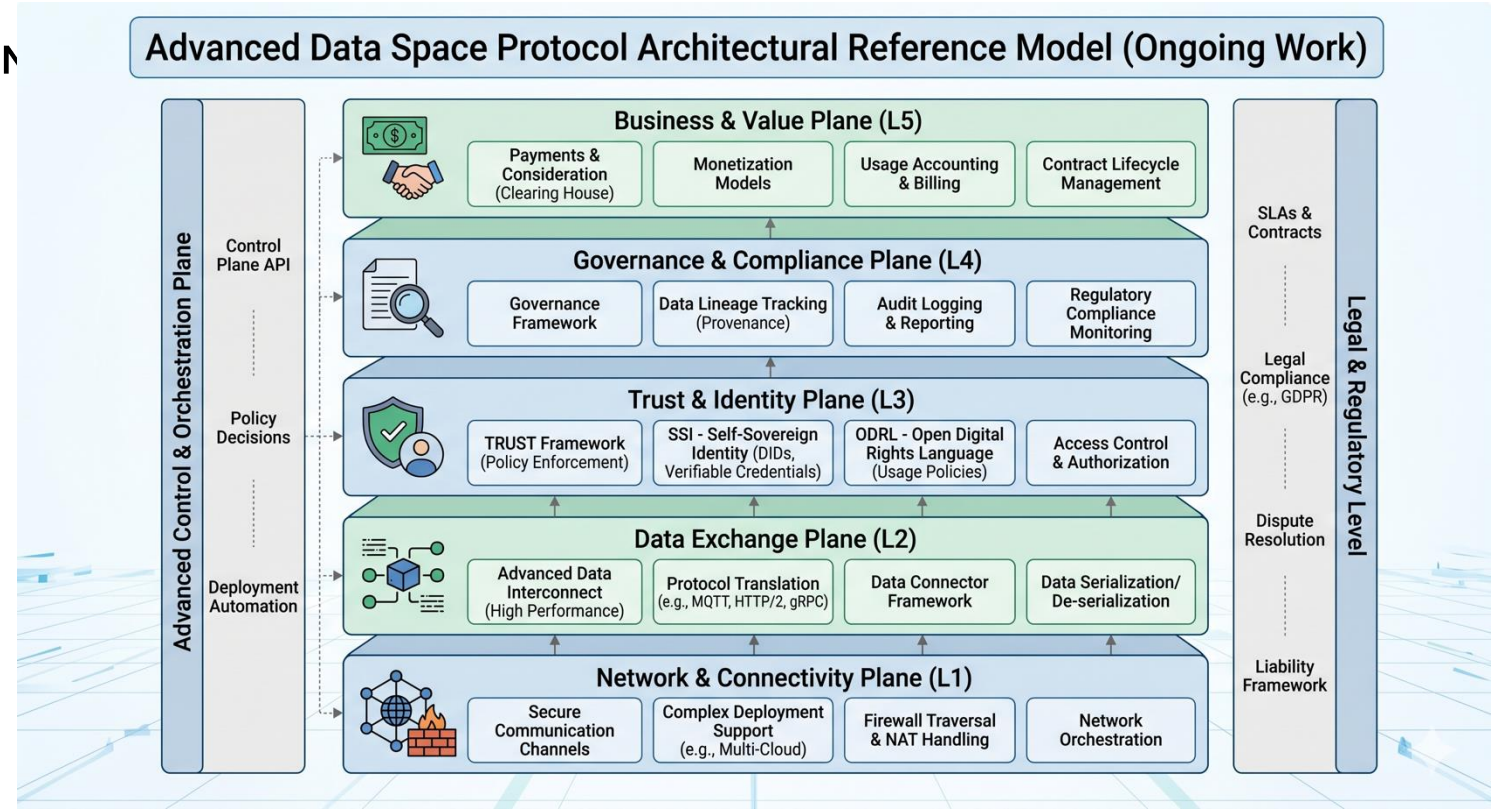
Simplification of complementary operating modes and specification

Advanced deployment

Federated / distributed catalog implementation

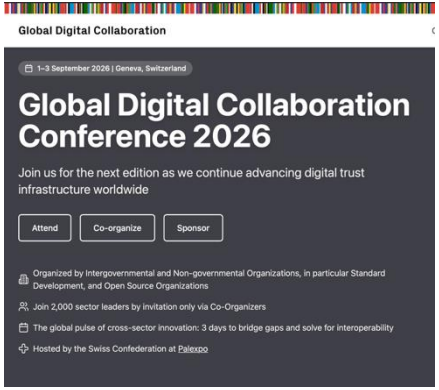
Trust Distributed Model : integration persona project

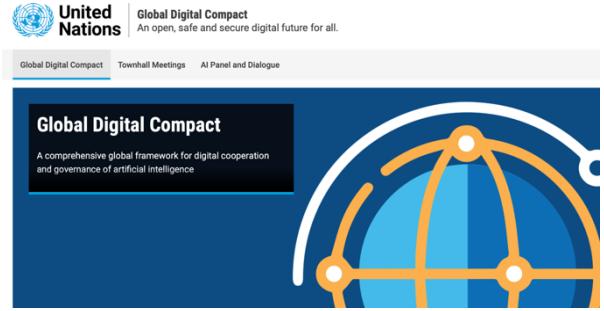
Easy API exposed (declarative mode).


Advanced Data Space Protocol Architectural Reference Model (Ongoing Work)
Advanced Control & Orchestration Plane
Control Plane API
Policy Decisions
Deployment Automation
Business & Value Plane (L5)
Payments & Consideration (Clearing House)
Monetization Models
Usage Accounting & Billing
Contract Lifecycle Management
Governance & Compliance Plane (L4)
Governance Framework
Data Lineage Tracking (Provenance)
Audit Logging & Reporting
Regulatory Compliance Monitoring
Trust & Identity Plane (L3)
TRUST Framework (Policy Enforcement)
SSI - Self-Sovereign Identity (DIDs, Verifiable Credentials)
ODRL - Open Digital Rights Language (Usage Policies)
Access Control & Authorization
Data Exchange Plane (L2)
Advanced Data Interconnect (High Performance)
Protocol Translation (e.g., MQTT, HTTP/2, gRPC)
Data Connector Framework
Data Serialization/ De-serialization
Network & Connectivity Plane (L1)
Secure Communication Channels
Complex Deployment Support (e.g., Multi-Cloud)
Firewall Traversal & NAT Handling
Network Orchestration
SLAs & Contracts
Legal Compliance (e.g., GDPR)
Dispute Resolution
Liability Framework
Legal & Regulatory Level

Global Digital compact

gital-compact/





https://globaldigitalcollaboration.org

Questions ?