

● iSHARE Trust Framework

Build trusted, secure and interoperable dataspaces with
the iSHARE Trust Ledger and open-source components

i4Trust - Train the Trainers

Rajiv Rajani | CTO iSHARE Foundation |

rajiv@ishare.eu

Monday June 27th, 2022

iSHARE.eu



 i4Trust

iSHARE

What do these remind you of, subconsciously?



● We need trust everyday!



When there is trust, nothing is impossible!

- Can we say the same for data online or with our (business) data since our businesses depend on it

Which leads to bilateral contracts, secrets exchange and heavy data clauses everytime!



What if you could build on a digitally
verifiable Trust Anchor ..



And with that as a foundation authorize organisations to only access that data set with those conditions that you want. Dynamically, Digitally Verifiable, Controllable and Traceable





iSHARE

- ✓ Data agnostic
- ✓ Federated
- ✓ Distributed
- ✓ Non Profit
- ✓ Universal



Bringing:
Data Sovereignty and
Trust
in Data Sharing
in Data Spaces

Live since 2018

Data of over 1,5 Mln
businesses

Trusted by Governments



Growing 100x this year

Reaching + 100.000
participants this year

Compliant with Gaia-X, IDSa

iSHARE was co-created by the market, for the market



Preparation

Co-creation partners were invited and guiding principles were established

Co-creation

Four working groups (Functional, Technical, Operational and Legal) co-created the iSHARE Scheme. Additionally, 5 POCs were realized

Live

Launching customers have started to implement the iSHARE Scheme. Additionally, the iSHARE Foundation is being created

Foundation

The iSHARE Scheme will be fully managed by the Foundation which is independent, transparent and not focused on maximizing profit

2016

2017

2018

2019



● iSHARE's guiding principles



Generic building block to enable data exchange



Limited scope:
identification,
authentication and
authorization



Leverage existing
(international) building
blocks



Agnostic towards nature
and content of data



Benefits outweigh
investment for all types of
Participants



International



Enable federation

● iSHARE is foundation of...

- **Business aspects** - iSHARE framework forms the basis for business data exchange allowing businesses to share data in sovereign manner
- **Legal aspects** - iSHARE framework is a multilateral legal framework which enables you to exchange data with any other participant with trust and confidence
- **Operational aspects** - iSHARE framework covers necessary operational requirements for essential services
- **Functional and Technical aspects** - iSHARE role model and specifications are designed keeping in mind your technical and functional needs and describes what is needed minimally to support any use case



● Businesses and organizational aspects

- Businesses/organisations usually play one or more of the roles who want to share data, namely - service consumer, service provider and/or entitled party
- These organisations have signed legal agreement where they have agreed to abide by the usage rights on the data that they receive
- The data rights are digitally shared and can be managed digitally as well



● Legal aspects

- iSHARE framework is a multilateral agreement that all its participants sign when they onboard iSHARE as participants
- iSHARE terms of use and accession agreements contains common set of agreements that allows participants to trust each other as well as share data with each other
- The technical specifications for each role are designed such that each participant can keep logs of digitally signed information which can be used in courts of law incase of legal disputes



Licenses create trust about who does what with data *after it has been shared*

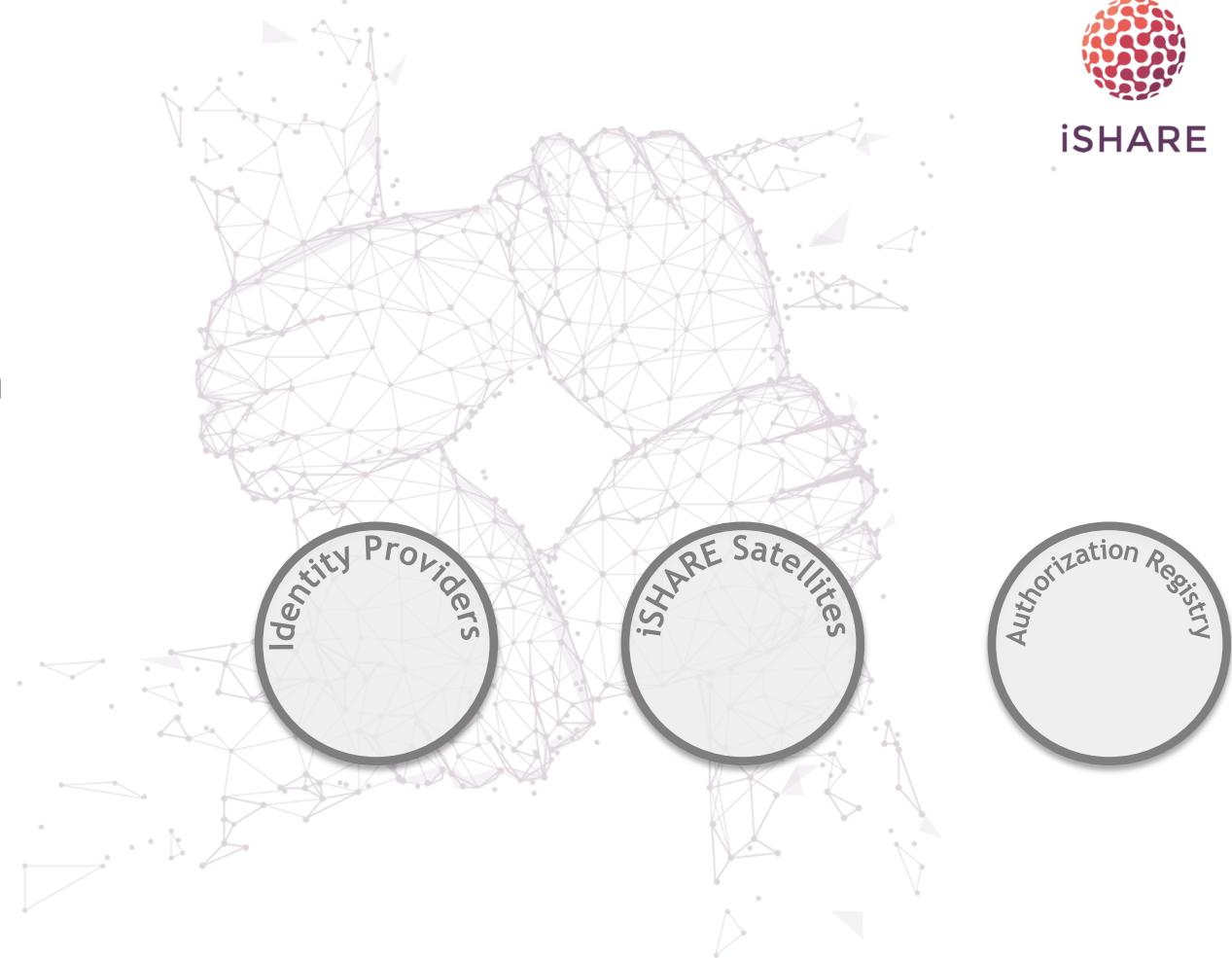


- Under iSHARE, it is possible to provide explicit instructions about the **conditions** under which data can be exchanged
 - *For example: you, as the recipient of my data, may only make use of this data for one month and may NOT share it with others*
- Such instructions are called **licenses** in the iSHARE scheme, and are defined in the authorization language
- iSHARE Participants can hold each other to licenses because they have all signed the same agreement with the Scheme Owner - thus creating a **network of trust**



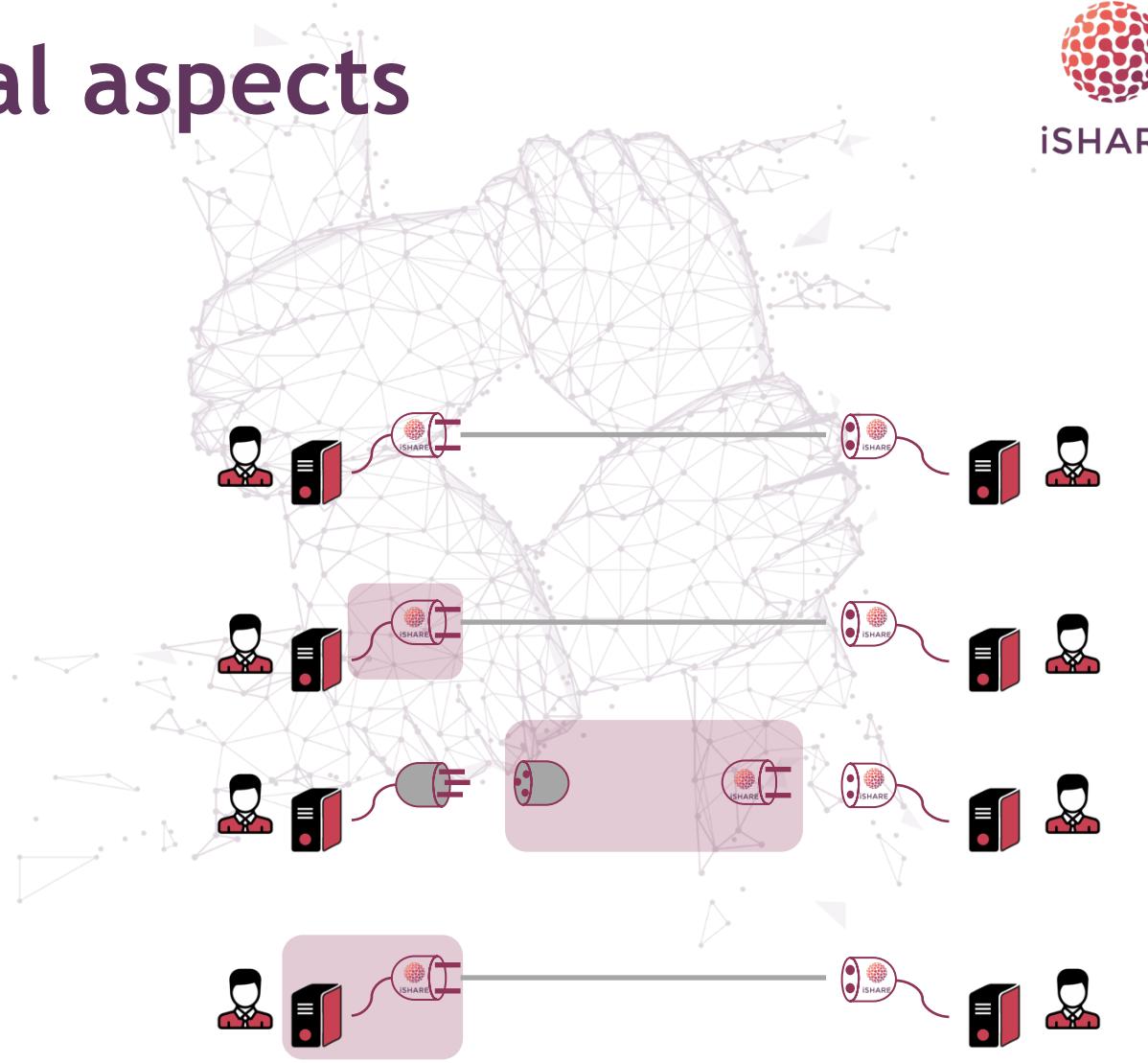
● Operational aspects

- Essential roles in iSHARE framework enable the parties to share data with each other
- Since these roles can be played by other organisations basic SLA and other organisational level requirements are additionally specified for these roles
- Organisations playing these roles also sign additional agreements which covers these aspects



● Technical & Functional aspects

- iSHARE framework includes specifications for Identification, authentication and authorisation for each roles
- It is agnostic to technology as well as data, so using this framework you can share any kind of data
- Build new integrations or re-use existing interfaces to share data
- Importantly it allows decentralised data sharing, meaning data can be shared directly from the source
- It enables federation of essential services which prevents lock-ins on one hand while promotes innovation as competitive space is expended



● iSHARE Role model

Service consumer

Identity Providers

Entitled Party

iSHARE Satellites

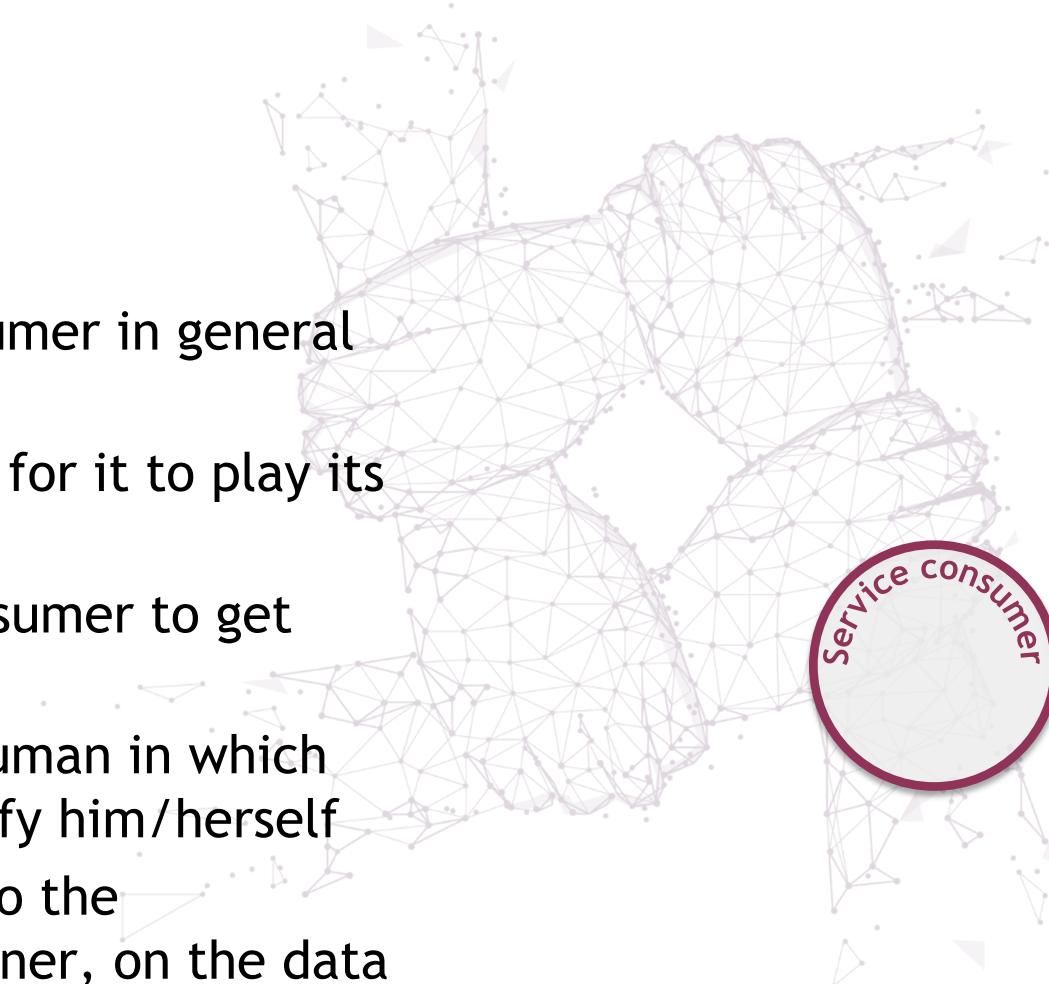
Service provider

Authorization Registry



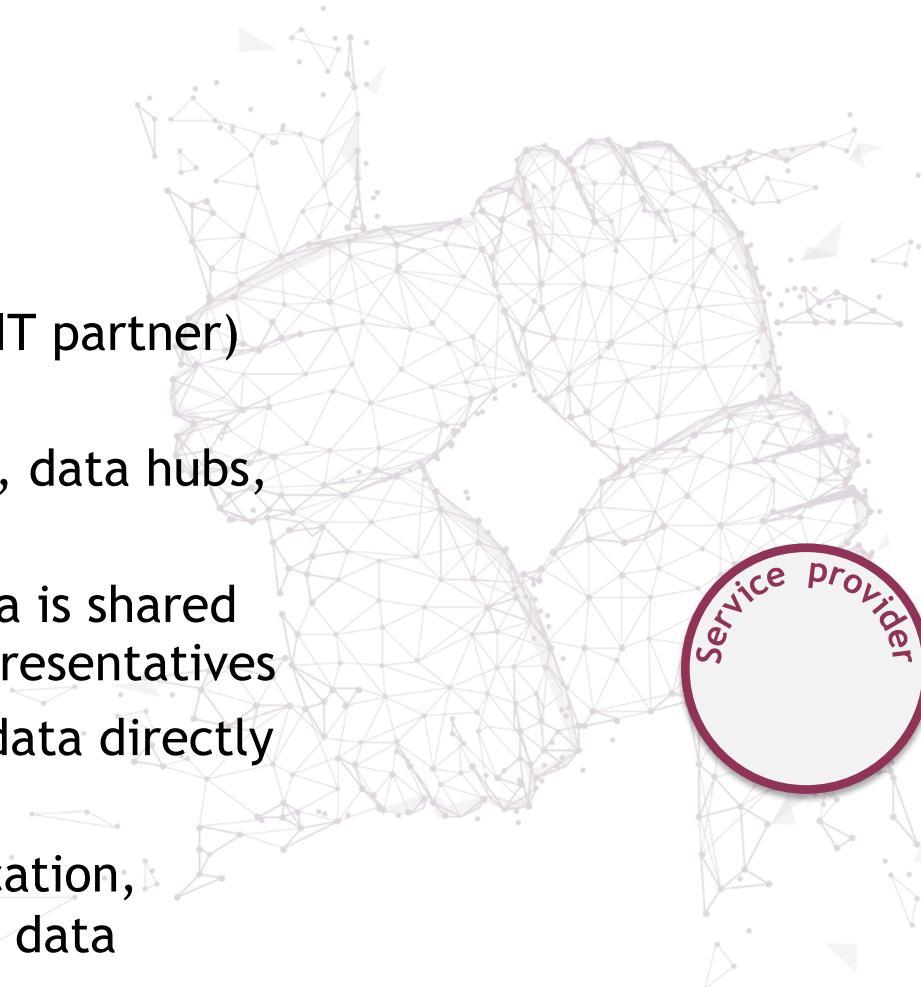
● Service consumer

- Service consumer is usually data consumer in general contexts.
- It needs data or updates data in order for it to play its part in the business process
- Data owner gives rights to service consumer to get data directly at source
- Data consumer can be a machine or human in which case it uses identity provider to identify him/herself
- Abides by the data license, attached to the authorisation it receives from data owner, on the data it receives



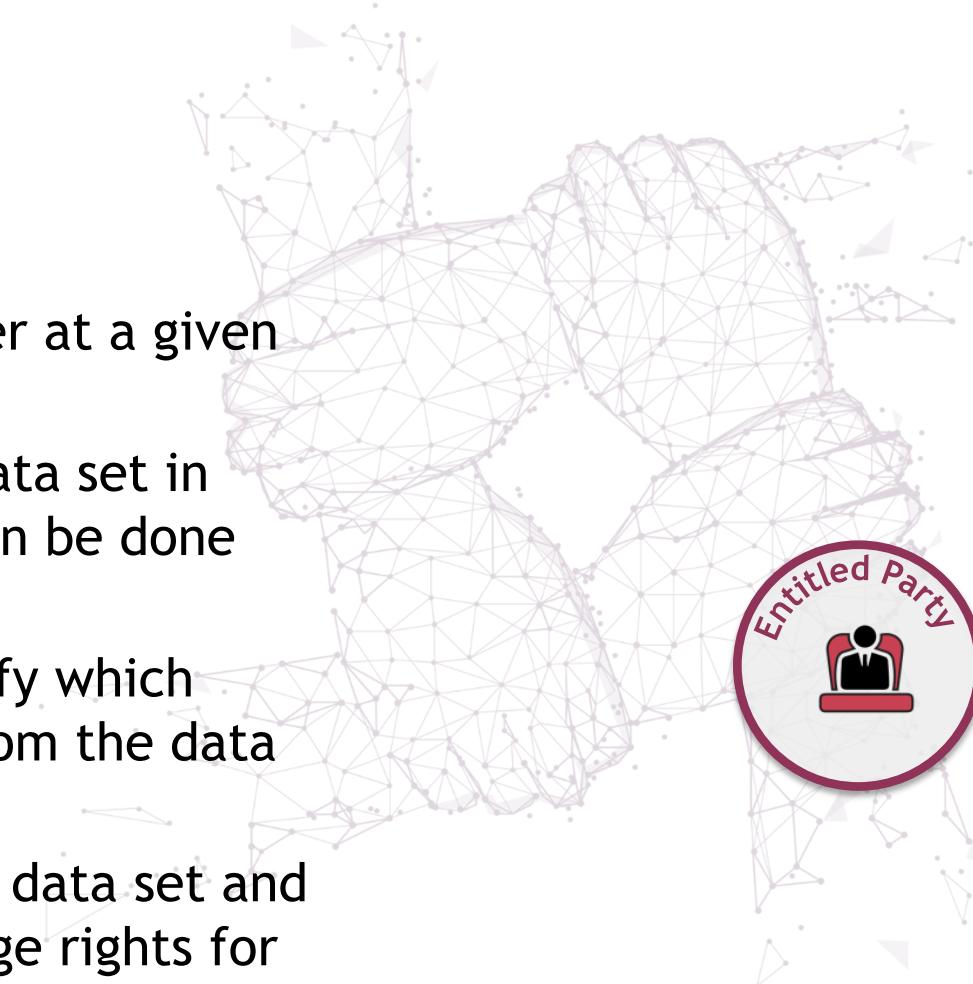
● Service Provider

- Service provider is usually the data provider (IT partner) who has data owner's data
- Examples are cloud SaaS solutions, data lakes, data hubs, hosted software platforms, etc.
- They are responsible for making sure that data is shared with only right organisations' machines or representatives
- Service provider and service consumer share data directly with each other
- iSHARE specifies API specification for Identification, Authentication and Authorisation for exposing data services
- The specifications are modified version of OAuth 2.0 which support verification of credentials inline with verifiable credentials principles



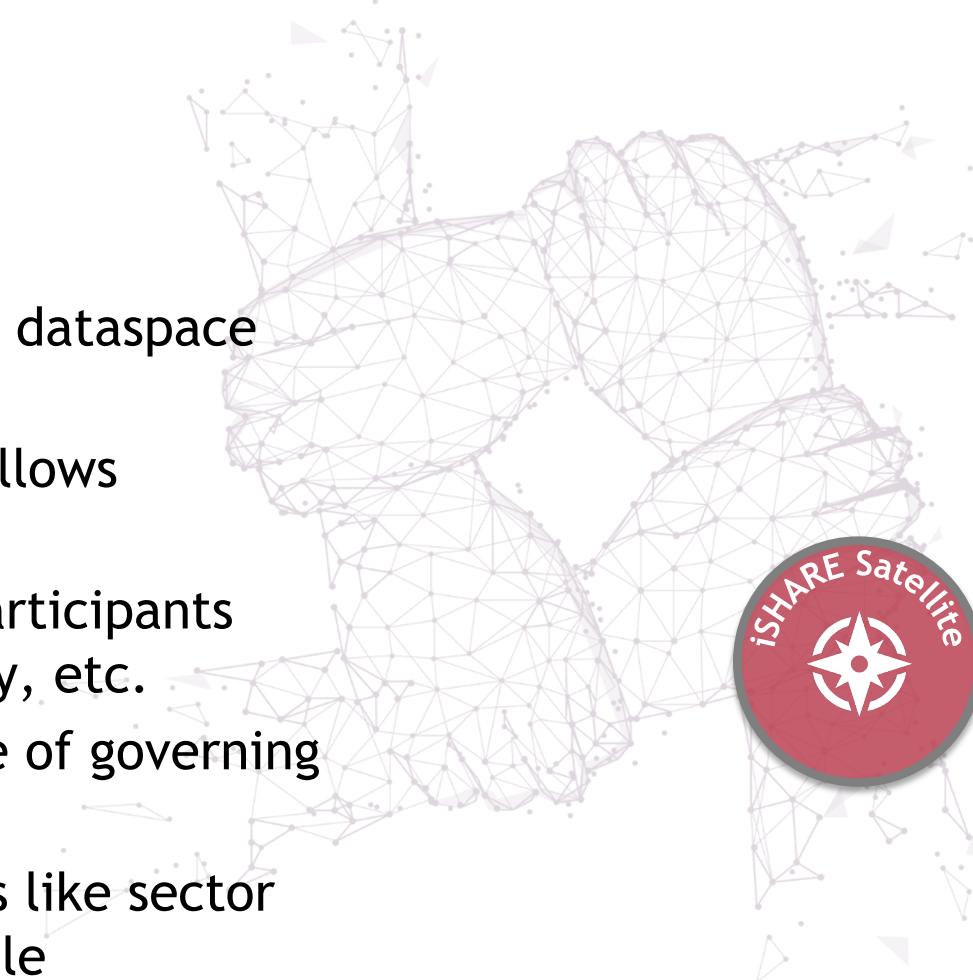
● Entitled Party

- Entitled party is a party who is data owner at a given time and context of that data
- Entitled party has the first right on the data set in question and they can determine what can be done with that data
- They use authorization registries to specify which consumer has access to which data set from the data set they are entitled to
- They also specify the data license for the data set and consumer which determines the data usage rights for consumers



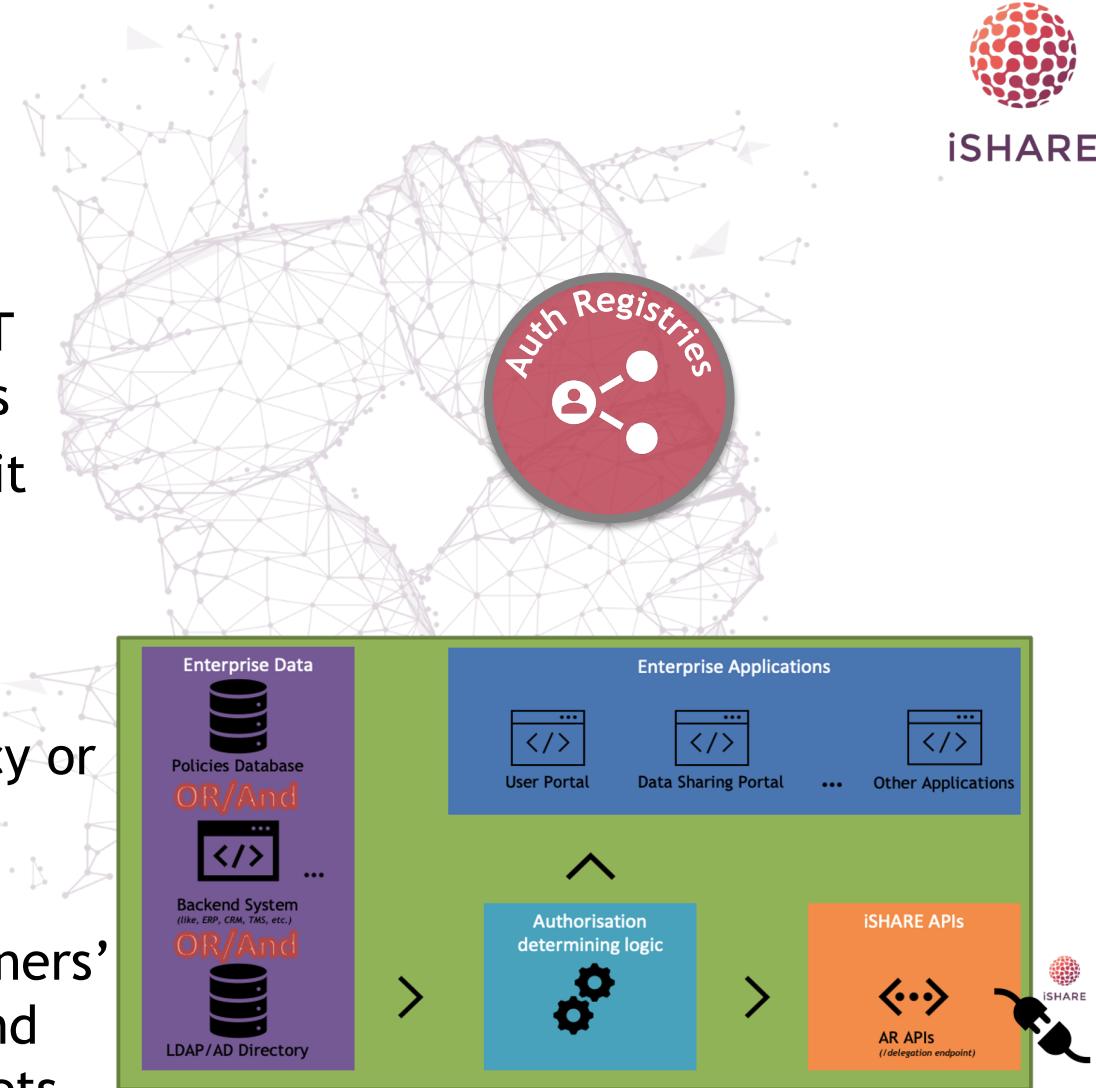
● iSHARE Satellite

- iSHARE satellite is the trust anchor of the dataspace and its participants
- It is a registry of the participants which allows participants to find each other
- It also acts as basic discovery point for participants data services, roles, authorisation registry, etc.
- It is usually also expected to play the role of governing body of the dataspace
- Ideally, not for profit sector organisations like sector associations are highly suitable for this role
- It registers participants in compliance with iSHARE framework as well as dataspace specific requirements
- iSHARE satellite is not involved in data sharing transaction (it is involved only during authentication)



● Authorization registry

- Authorization registry role is usually played by IT vendors who provide it as service to data owners
- A data owner could also implement this role on its own for its own authorisations
- iSHARE only defines the endpoint for this role whereas it is agnostic to its implementation
- It is possible to serve authorisations from a policy or operational data or transactional data or a combination thereof on the fly
- It is responsible for making it easier for data owners' business users to create policy or define rules and source to determine the authorisation on data sets



● Identity Provider

- Identity provider role provides the identity of humans
- It can be identities of employees, partners, contractors, etc. of an organization
- Identity providers can authenticate subjects at the specified level of assurance as determined by the service provider along with the request
- Identity providers level of assurance is determined following eIDAS framework
- iSHARE specifies APIs for identity provider role based on openIDConnect but is modified to suit the requirements for federation and B2B, B2G, G2B, G2G, etc. interactions



iSHARE supports a set of key functionalities



Interaction



Machine-to-Machine (M2M)

Communication between machines, without interference by a human



Human-to-Machine (H2M)

Communication between a human and (a) machine(s). Requires a user interface

Facilitate



Flexible authorizations

- Coarse-grained: broad authorization
- Fine-grained: specific authorization
- Flexibility on where to store authorizations



Portable identities

Identities can be spread out and recognised, i.e. portable, across multiple, independent systems

Enable



Delegations

Functions as evidence that a party is directly or indirectly operating on behalf of a known party



Customer in control

iSHARE allows parties to modify or withdraw access rights to their data or services, whenever they wish

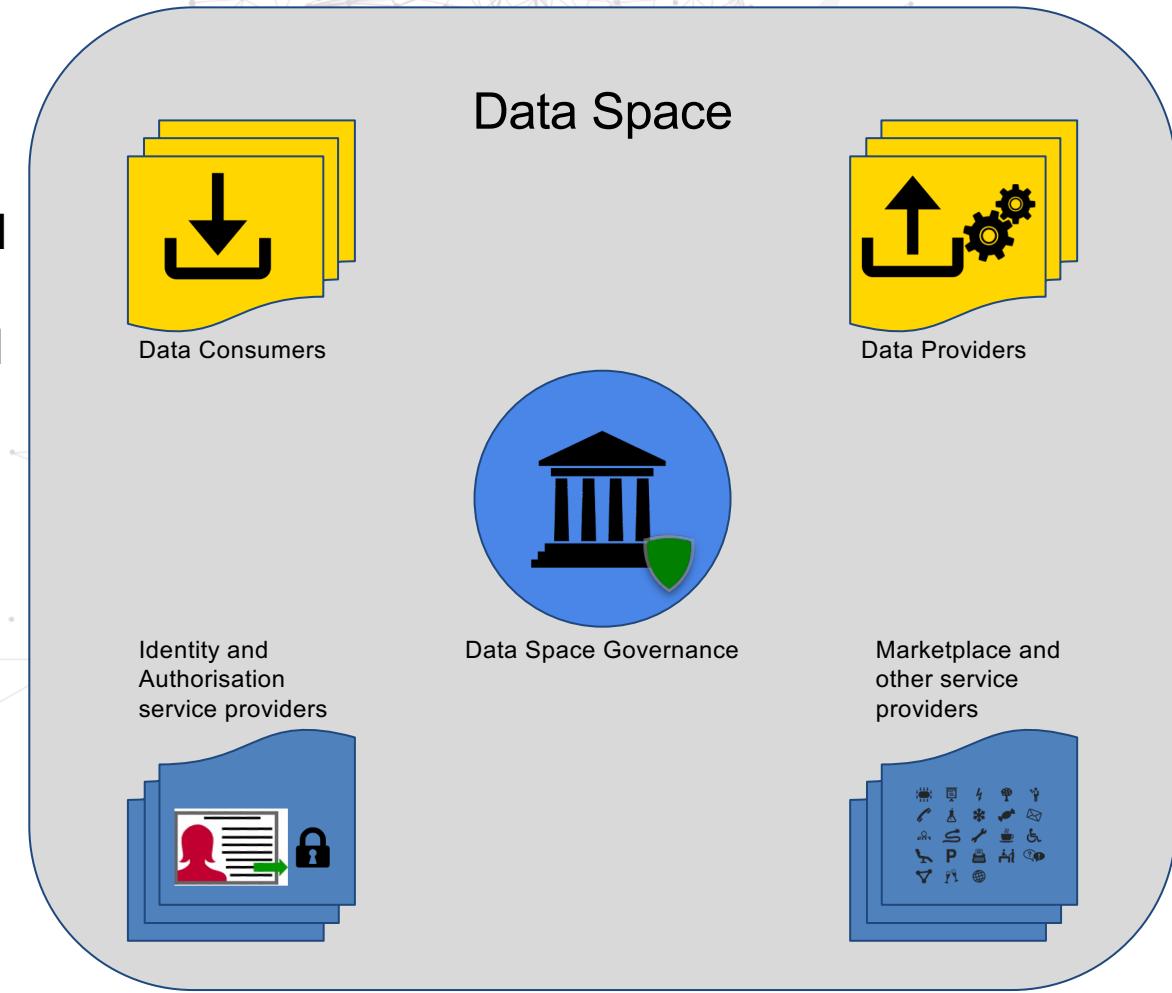
● Introduction to data spaces



iSHARE

A data space is an decentralized data ecosystem built by the parties with common purpose

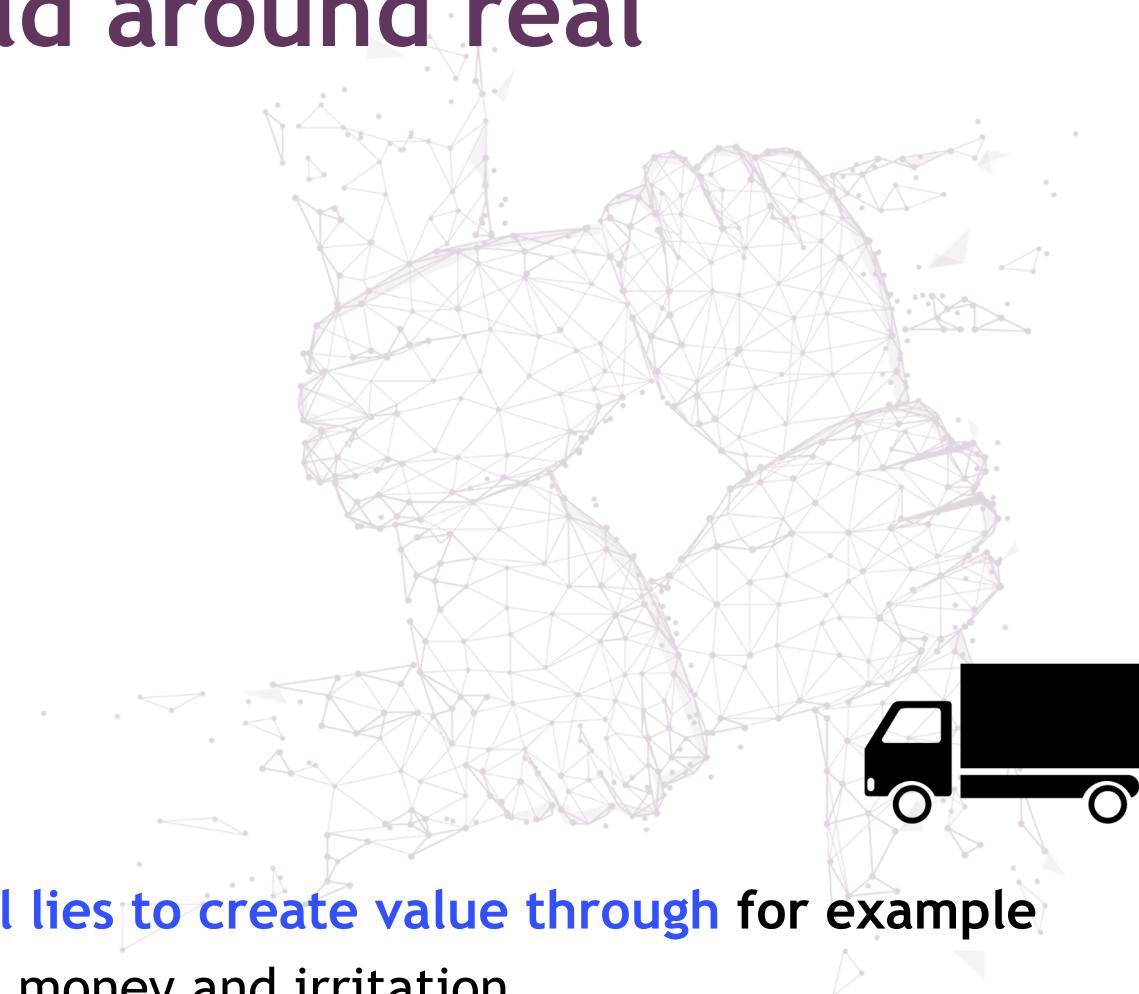
- Further, it can be defined as a decentralized data ecosystem built around commonly agreed building blocks enabling an effective and trusted sharing of data among participants.
- Data consumers, data providers and identity and authorisation service providers form an ecosystem with a governance structure in place to create a basic data space
- Additionally, service providers like Marketplaces, Brokers, Billing and Clearing etc. can be part of data space to support variety of use cases
- In i4Trust iSHARE and FIWARE bring the necessary components along with basic governance structure to create the i4Trust data space



● Data spaces are build around real businesses

Agreeing on

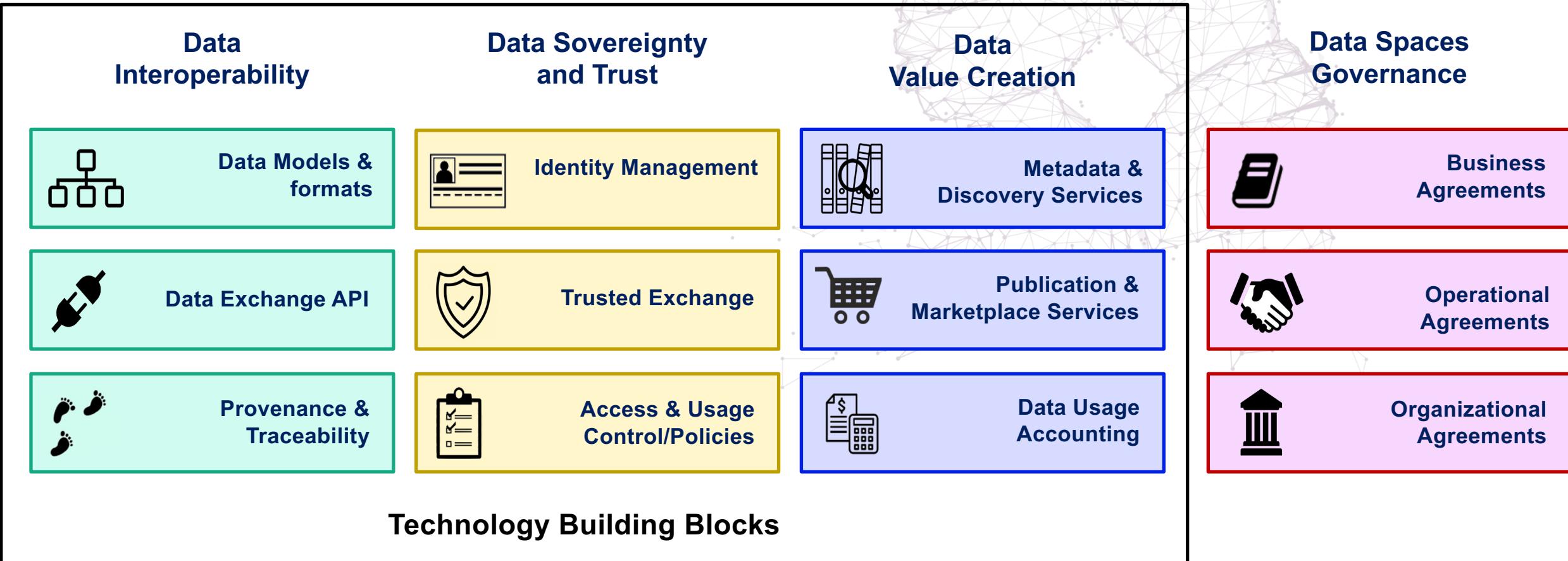
1. Data interoperability
2. Data sovereignty
3. Data value creation
4. Governance



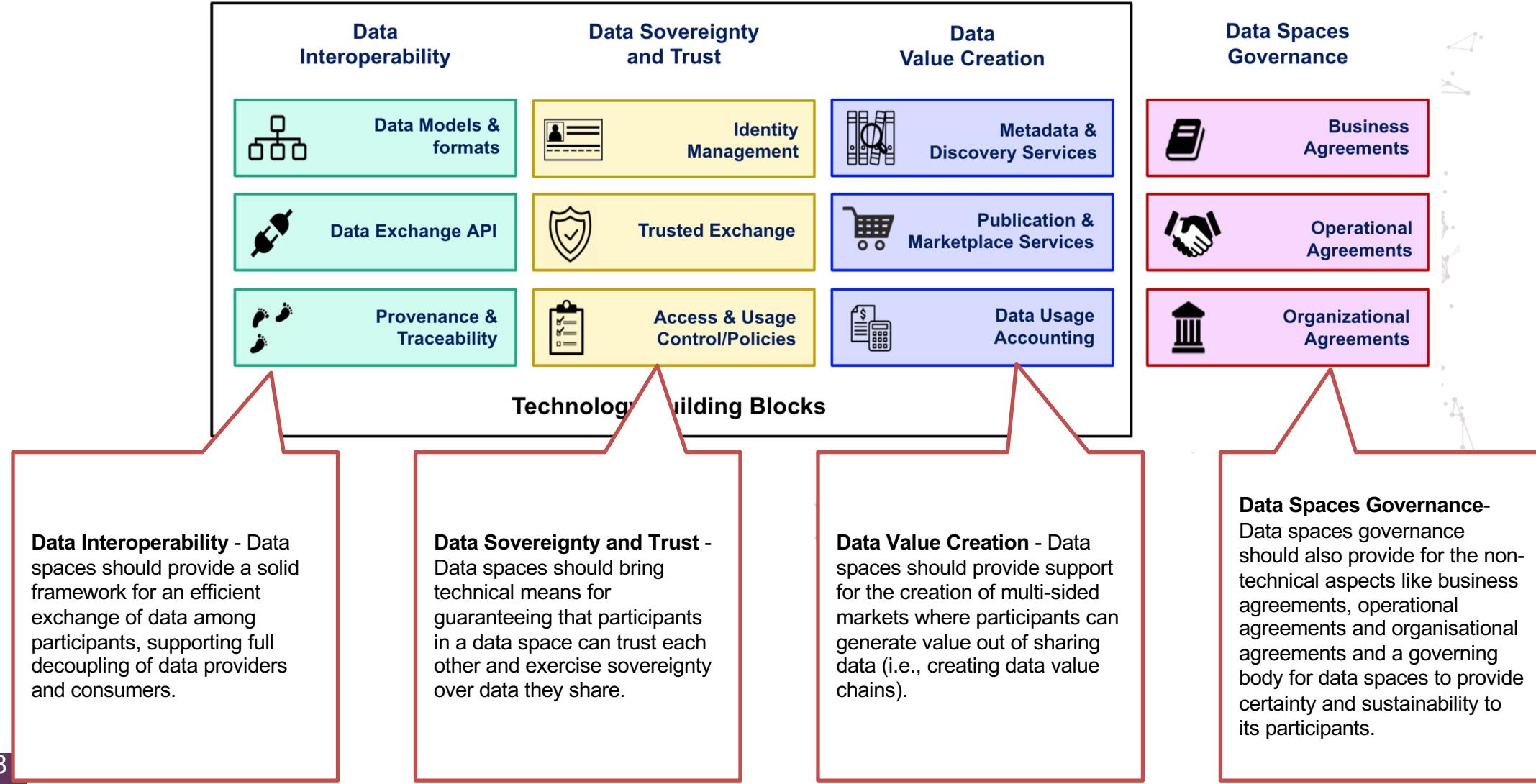
Within sectors, verticals the real potential lies to create value through for example

- Exchange of hidden data to save time, money and irritation
- Allowing AI to run on long value chains to provide new insights
- Save emissions

● Data Spaces Building Blocks



Data space building blocks



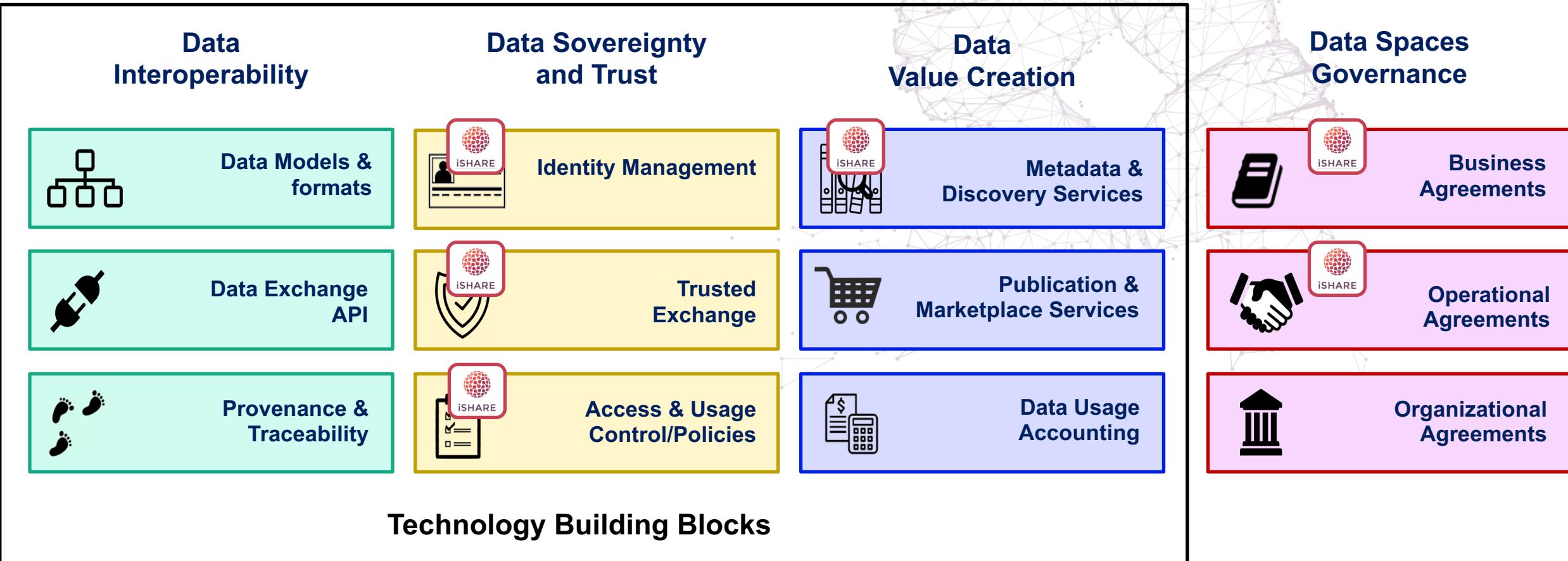
Covers key building blocks for creating Data

Spaces

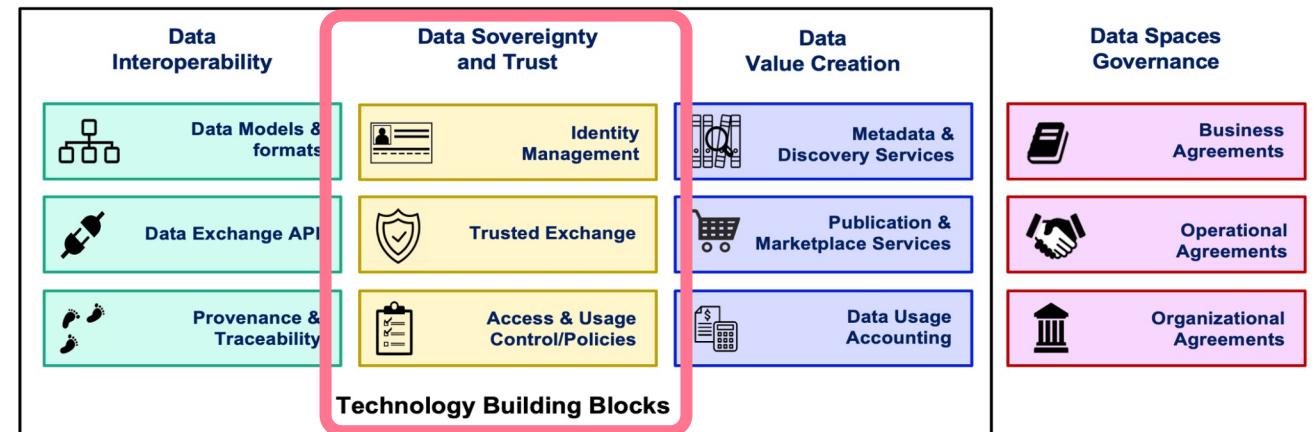
opendei.eu



iSHARE

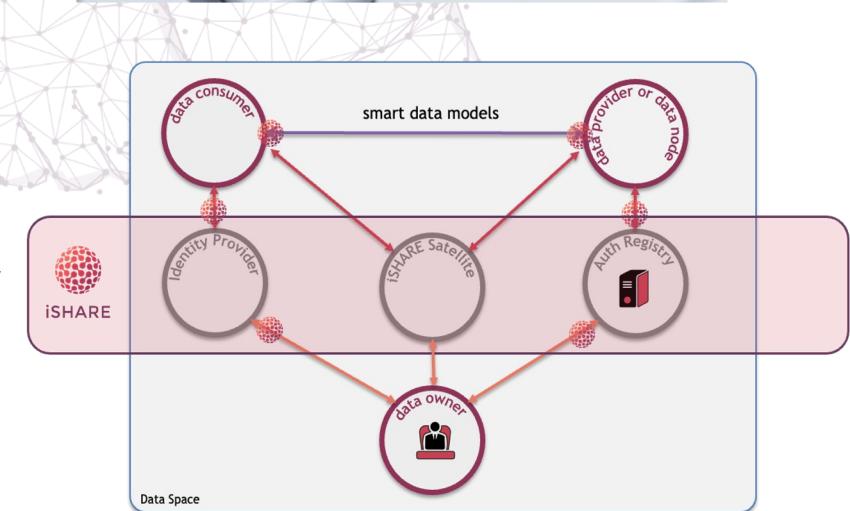


● Data Sovereignty and Trust

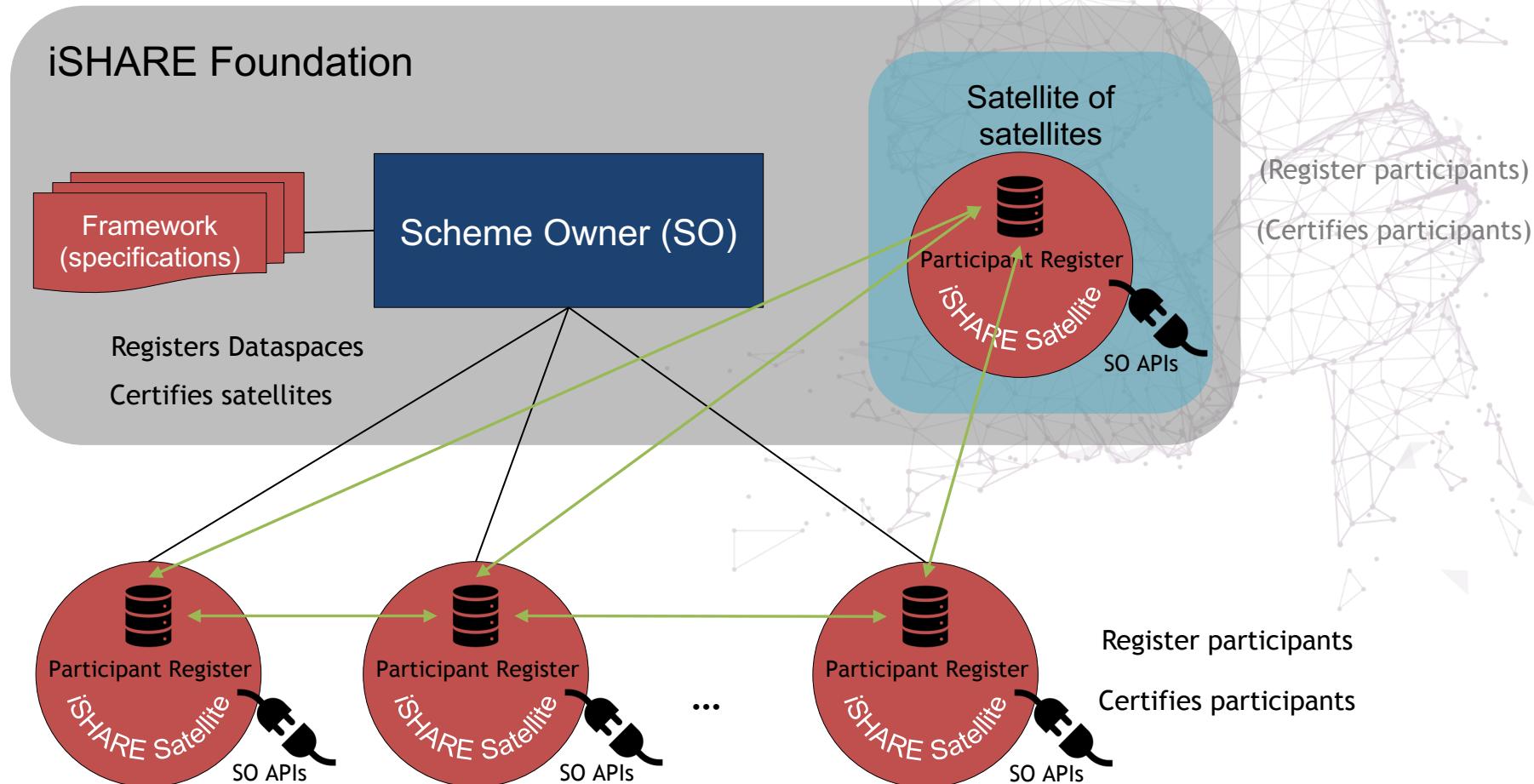


● Data sovereignty and trust: principles

- Identity and access/control policies should be handled:
 - At organization level (participants)
 - At the level of users of applications within each organization
- Identity, Authentication and Authorization based on standards:
 - OpenId Connect
 - OAuth2
 - XACML
- There will be a trust authority that certifies what organizations are considered trusted parties in a data space
- Model should work assuming there is no single global Identity Provider and Authorization Registry, each organization may have:
 - A certified Identity Provider of its own choice for managing identity of end users
 - Its own Authorization Registry (PMP/PAP server)
 - Its own PEP proxy and PDP server



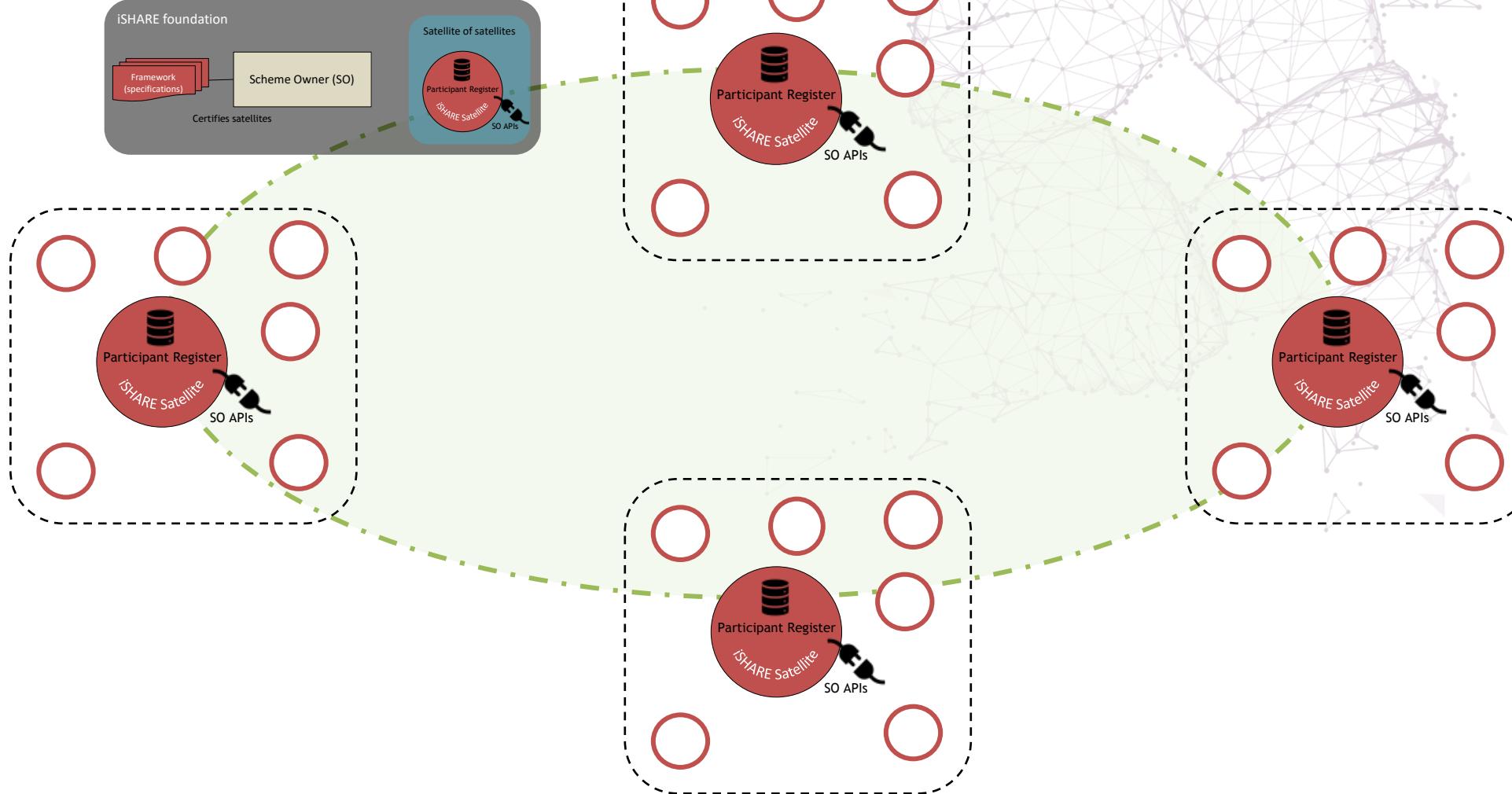
Federation of iSHARE scheme owner creates interoperable dataspaces



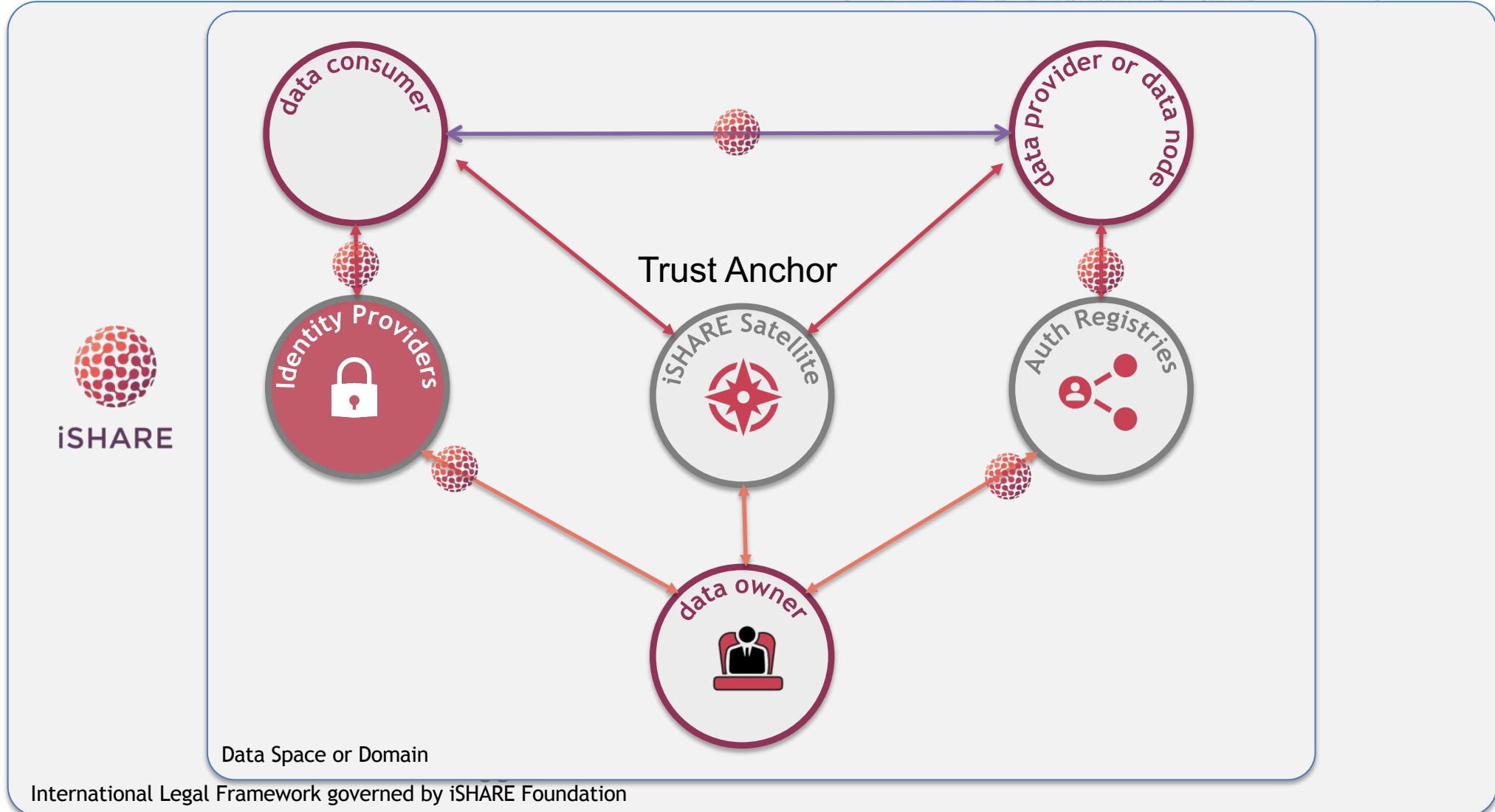
Interoperable Trust between various data spaces



iSHARE

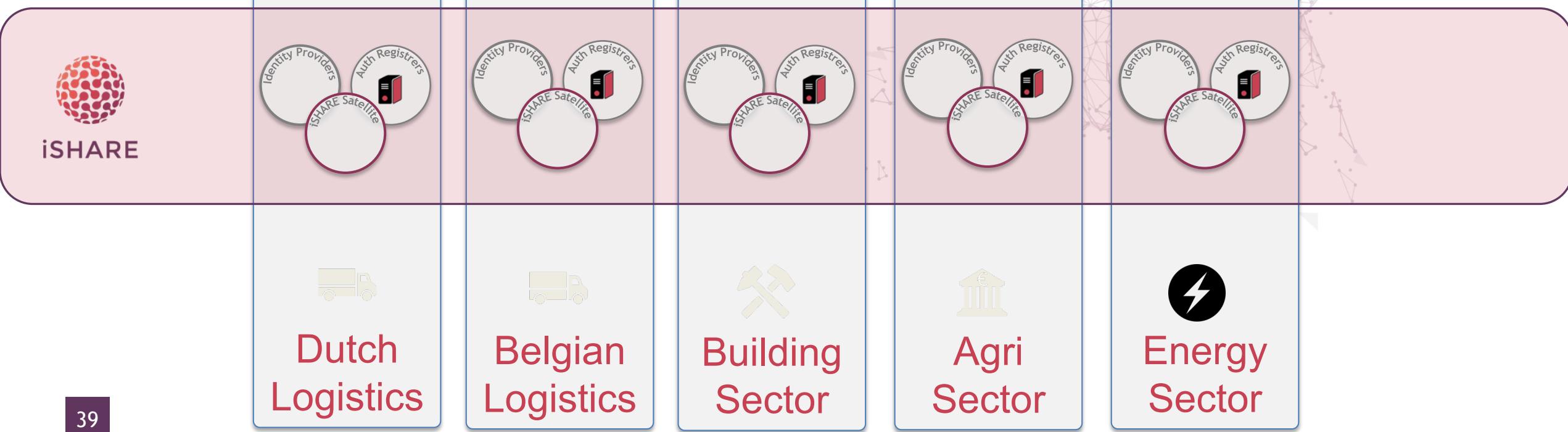


iSHARE role model forms the data space core roles

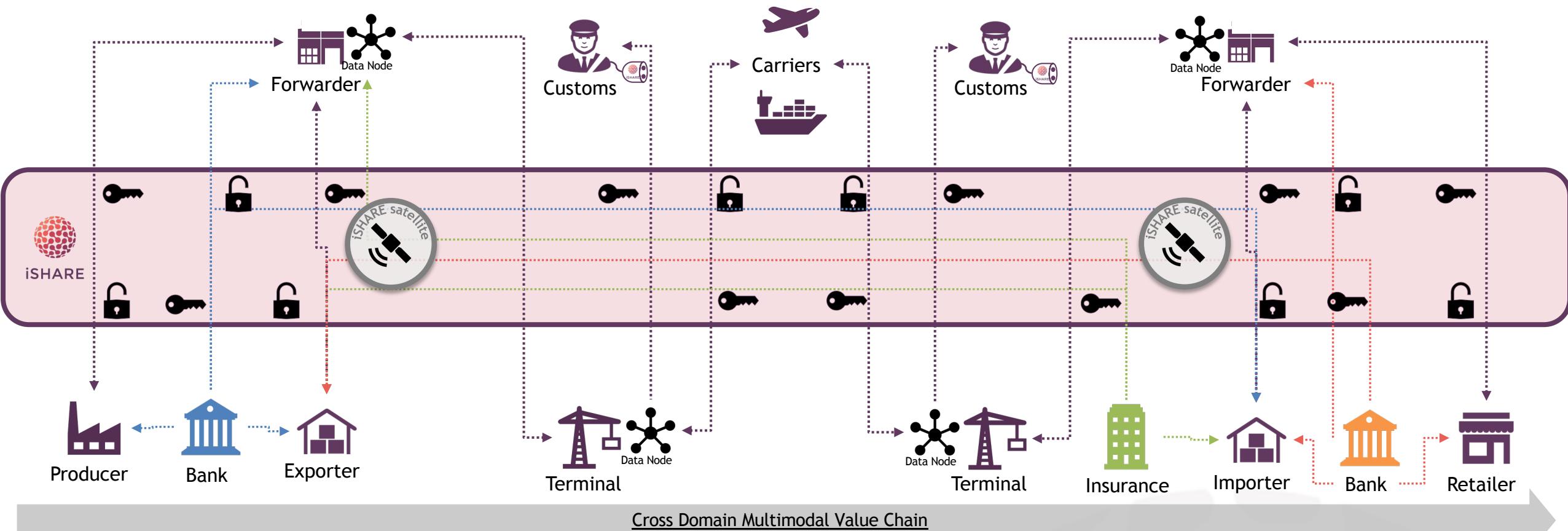


and thus enabling data spaces across sectors and geographies...

Data sharing between dataspaces is enabled by the distributed iSHARE Register of participants



Bringing value with cross domain trusted data sharing



Cross Domain Multimodal Value Chain

.....► Data flows enabled by iSHARE Authorisation Registries and iSHARE Identities

● Trust validation of Participants



Signed Contracts

- iSHARE Legal Framework
- Data Spaces Specific additional legal

Validated by

Registering satellite

Validated and registered

Chamber of Commerce
Documentation
EORI Number

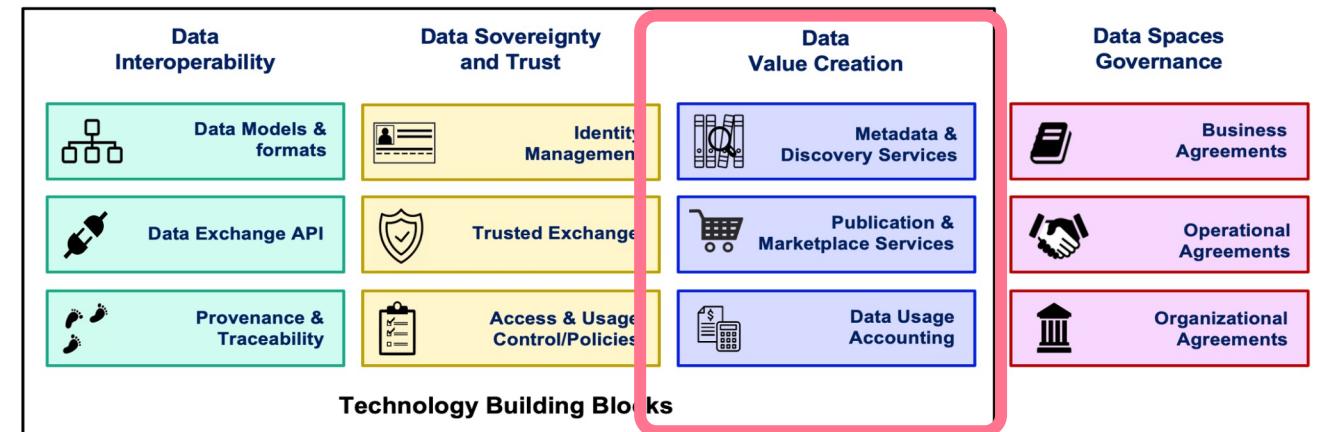
Level of Assurance

Validated and registered

EIDAS Certificate
Public Key available

Role in the network

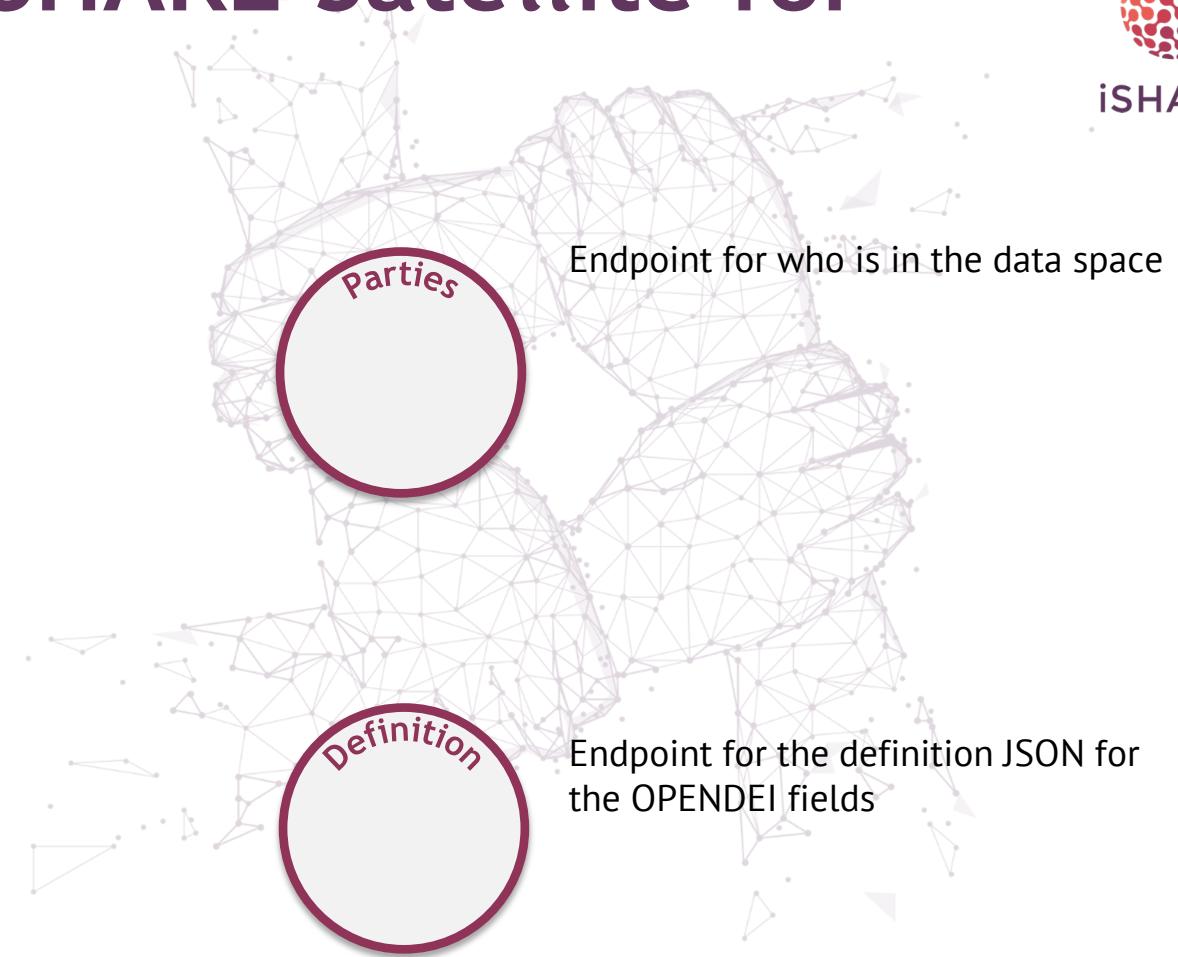
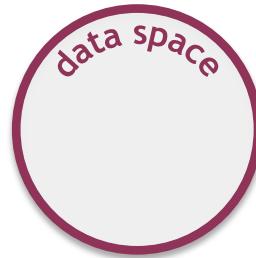
● Data value creation



Data Pointers in the iSHARE Satellite for data spaces



iSHARE



Data Pointers in the iSHARE Satellite for participants



iSHARE



Details on Participants

- Contact details
- Logo URL
- Specifications
- Location
- Tags



Endpoint for the data sources;

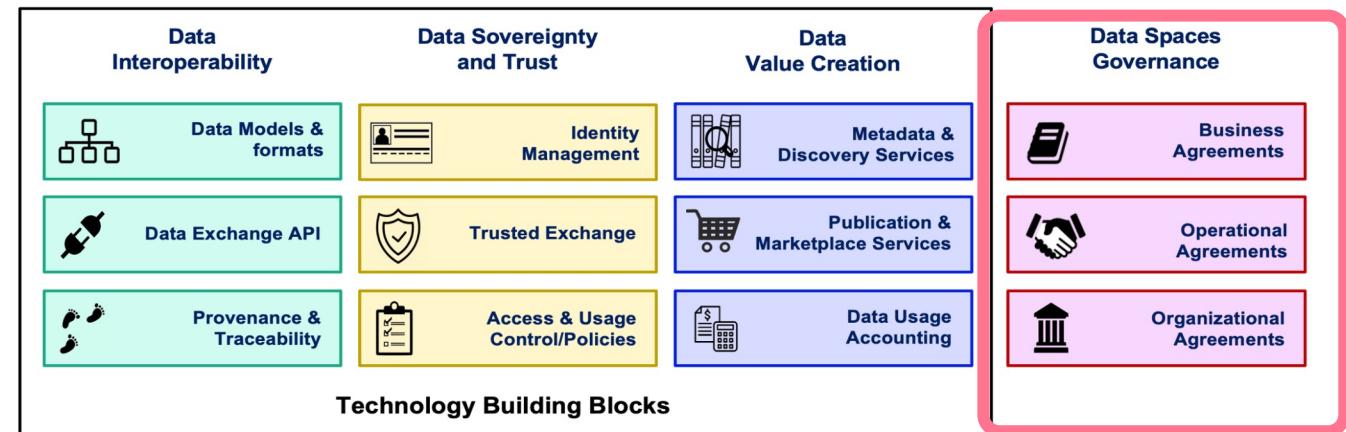
- Single endpoint + standard
- Array [JSON] of endpoints + standard
- Marketplace pointer



Endpoint for the Authorization Registry

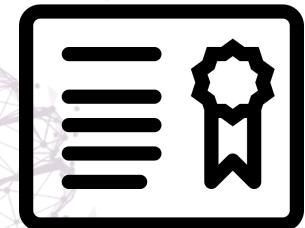
- Single AR
- Multiple AR { same order as array }

● Data spaces governance

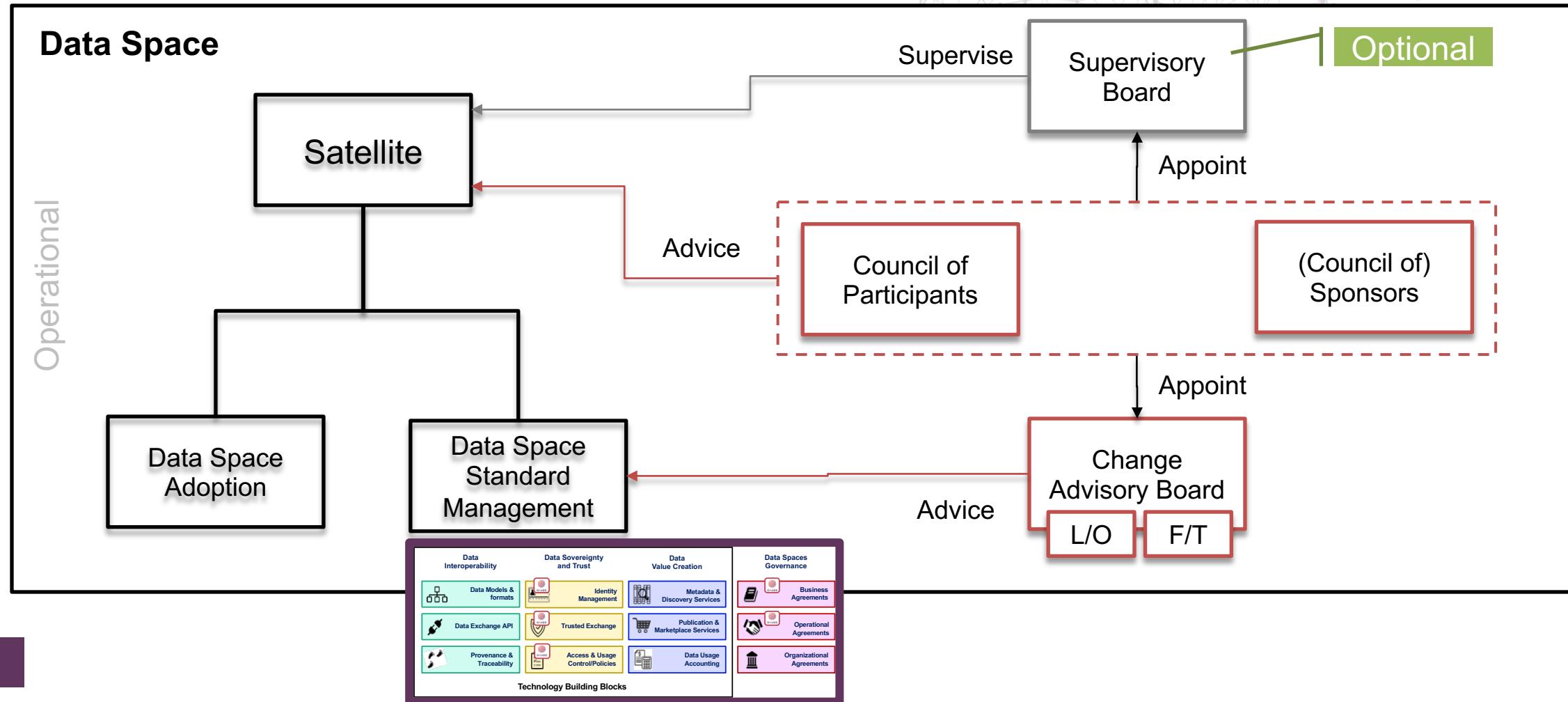


● Data spaces governance

- iSHARE framework provides with basic legal and [governance framework](#) which forms the basis for governance building blocks of dataspaces
 - **Data Sovereignty** is achieved by participants with use of iSHARE [data licenses](#) with which participants are able to legally oblige each other to data usage policies with or without technical enforcement
- While a smaller group of organisations are involved in creating Data Spaces it still requires basic governance elements covering
 - **Business Agreements** - agreements that have business impact like, what can the data be used for or for what period of time, etc.
 - **Operational Agreements** - agreements that have operational impact like, availability of certain services which are critical to the business to remain operational, etc.
- **Organisational Agreements** - agreements that defines the data space agreed amongst the organisations involved in creation of data space as well as for future participants of that data space



Ready governance template of taxonomy, interoperability and value creation per data space.



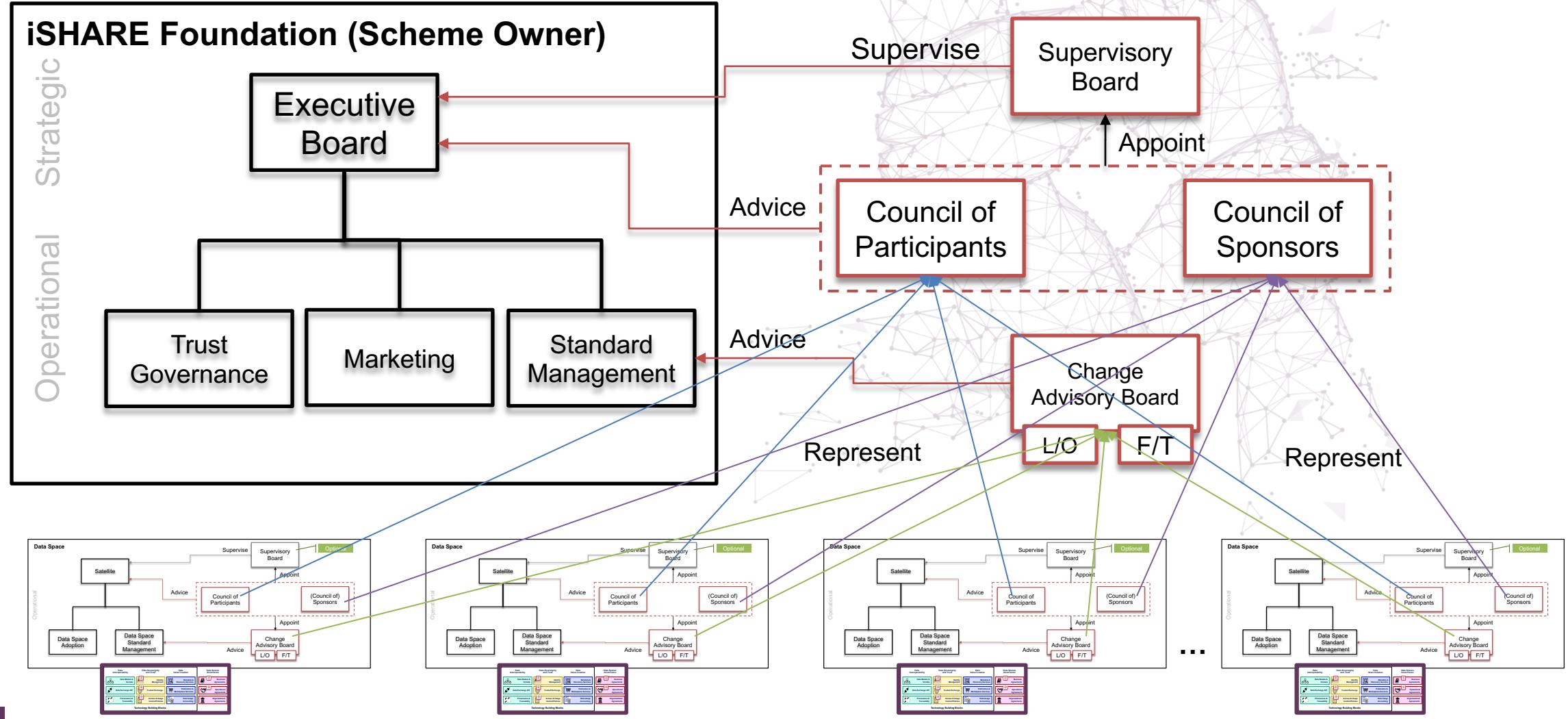
● Dataspace definition and governance

- iSHARE provides basics for key building blocks to create your dataspace
- Dataspace is responsible for selecting/defining the standards and models to use for the 12 building blocks of dataspaces
- Each participant joining the dataspace agrees to use those standards and models so that they can interoperate with each other
- Dataspace also selects who plays the role of satellite (trust anchor). Ideally, a not-for-profit sector organisation like sector association is highly suitable for this role
- Satellite could also be responsible as a governing body of that dataspace which is responsible for maintaining compliance to dataspace definition

Dataspaces

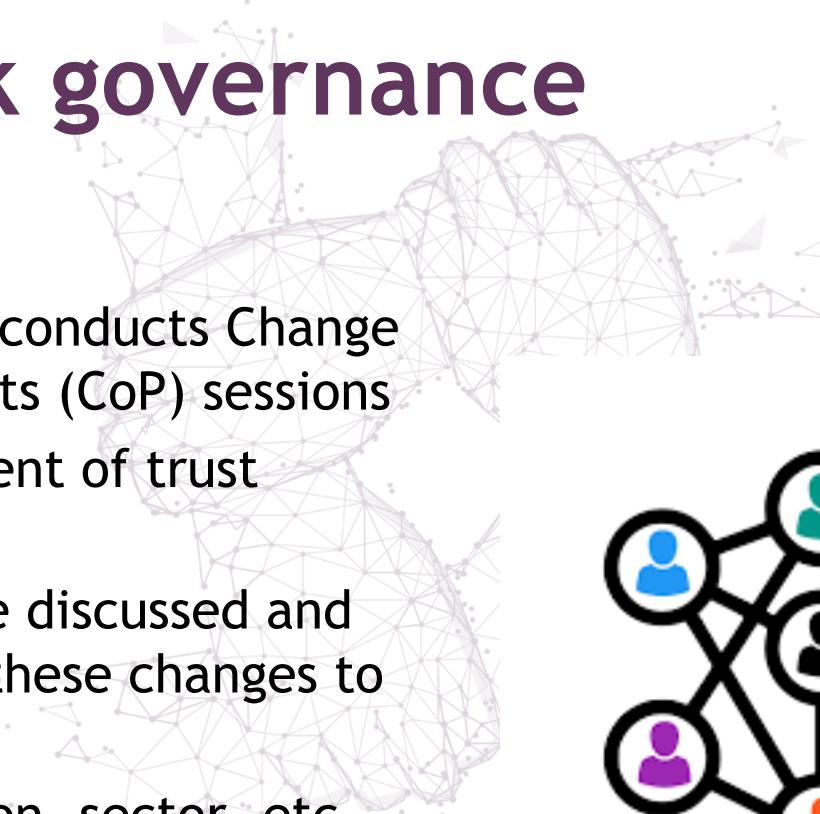
TITLE*	DATASPACE ID*	DATASPACE DEFINITION URL
Logistics NL	DSPEU.NLLOGISTICS	https://logisticsnl.nl/dspdef
DATASPACE WEBSITE	TAGS	STATUS*
https://logisticsnl.nl	Logistics Maritime Road Rail AirCargo	<input checked="" type="checkbox"/> Active
COUNTRY OF REGISTRATION	COUNTRIES OF OPERATION	SECTOR/INDUSTRY
<input checked="" type="radio"/> Netherlands	Netherlands x	Utilities x
SPECIFIC AGREEMENTS	SPECIFIC AGREEMENTS	
• TermsOfUse-LogisticsNL	+	

With federated trust governance accross multiple data spaces



● iSHARE Trust framework governance

- iSHARE foundation as Scheme Owner regularly conducts Change Advisory Board (CAB) and Council of Participants (CoP) sessions
- All participants contribute to future development of trust framework
- Participant can also propose changes which are discussed and solutioned in these boards before committing these changes to framework
- Each participant irrespective of its size, location, sector, etc., get equal rights at the table as other participants, thereby making sure that framework remains relevant for all
- Similar processes can be set by dataspace governing body to maintain the dataspace definition



● Example...

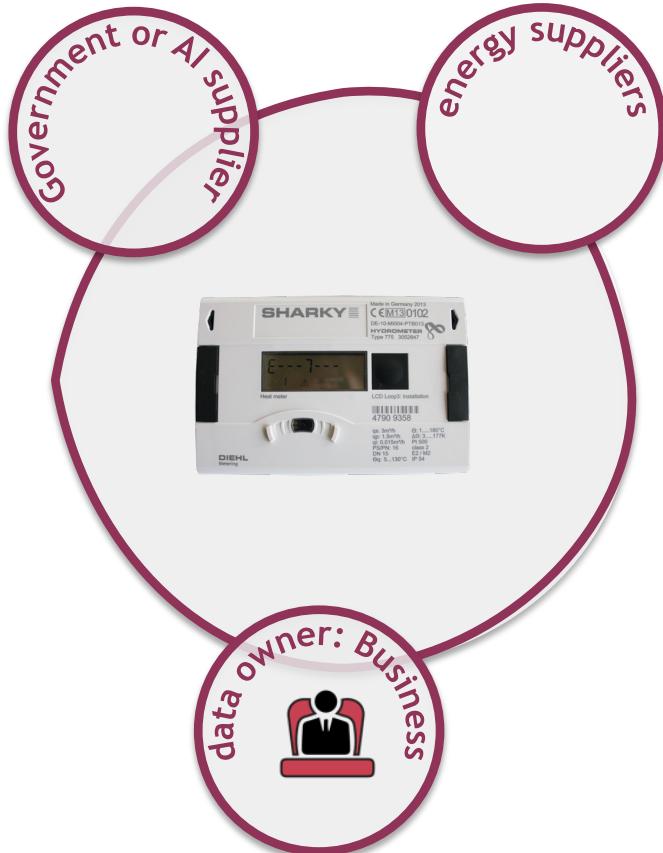


iSHARE

Use case examples of pragmatic data spaces



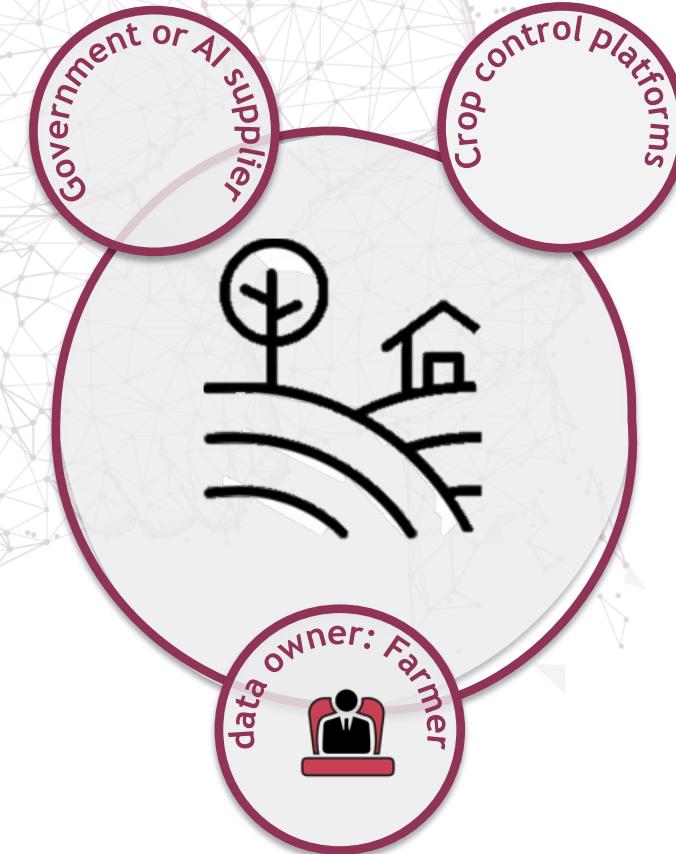
iSHARE



Climate agreement reporting



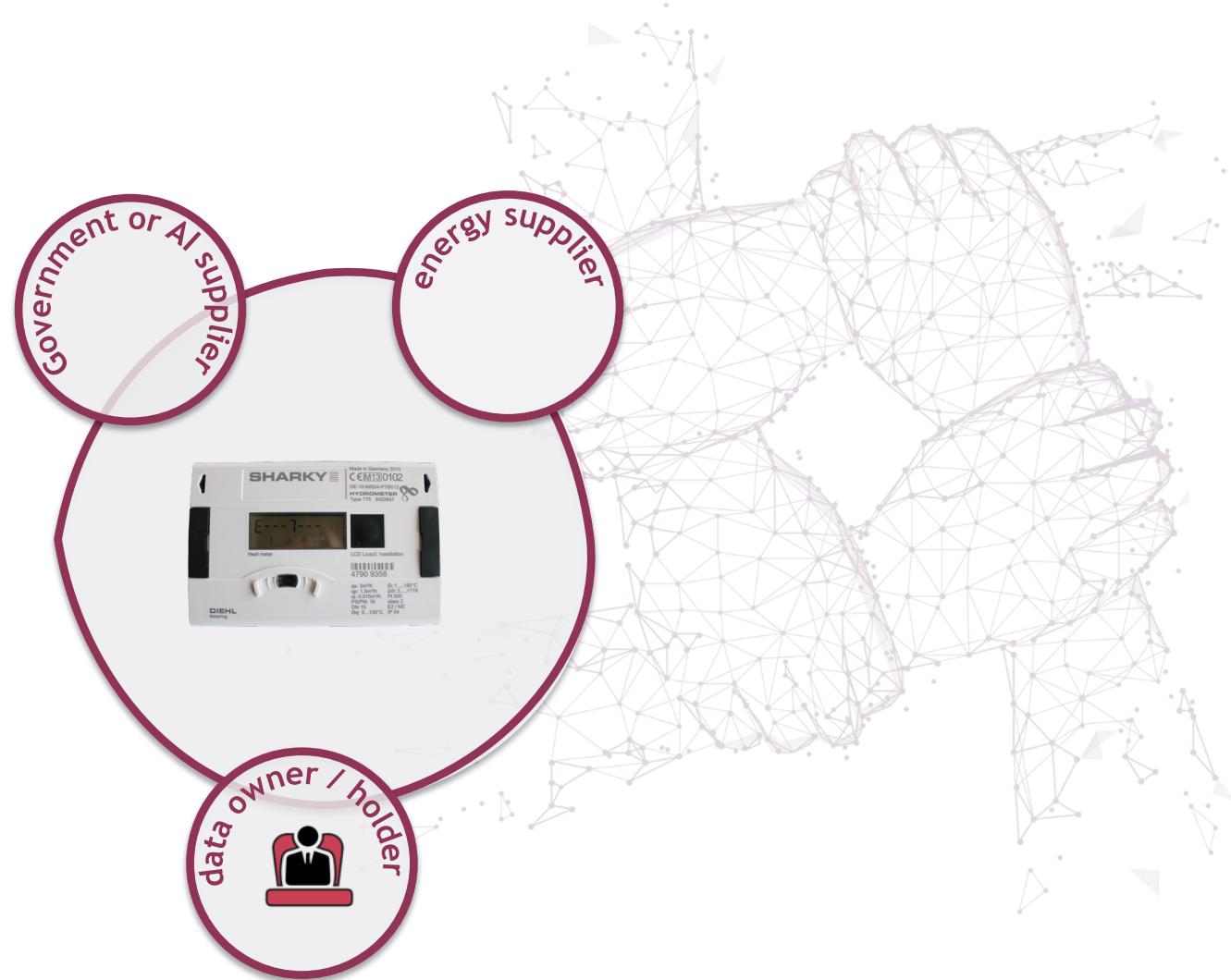
Prediction of arrival of goods



Food value chain reporting

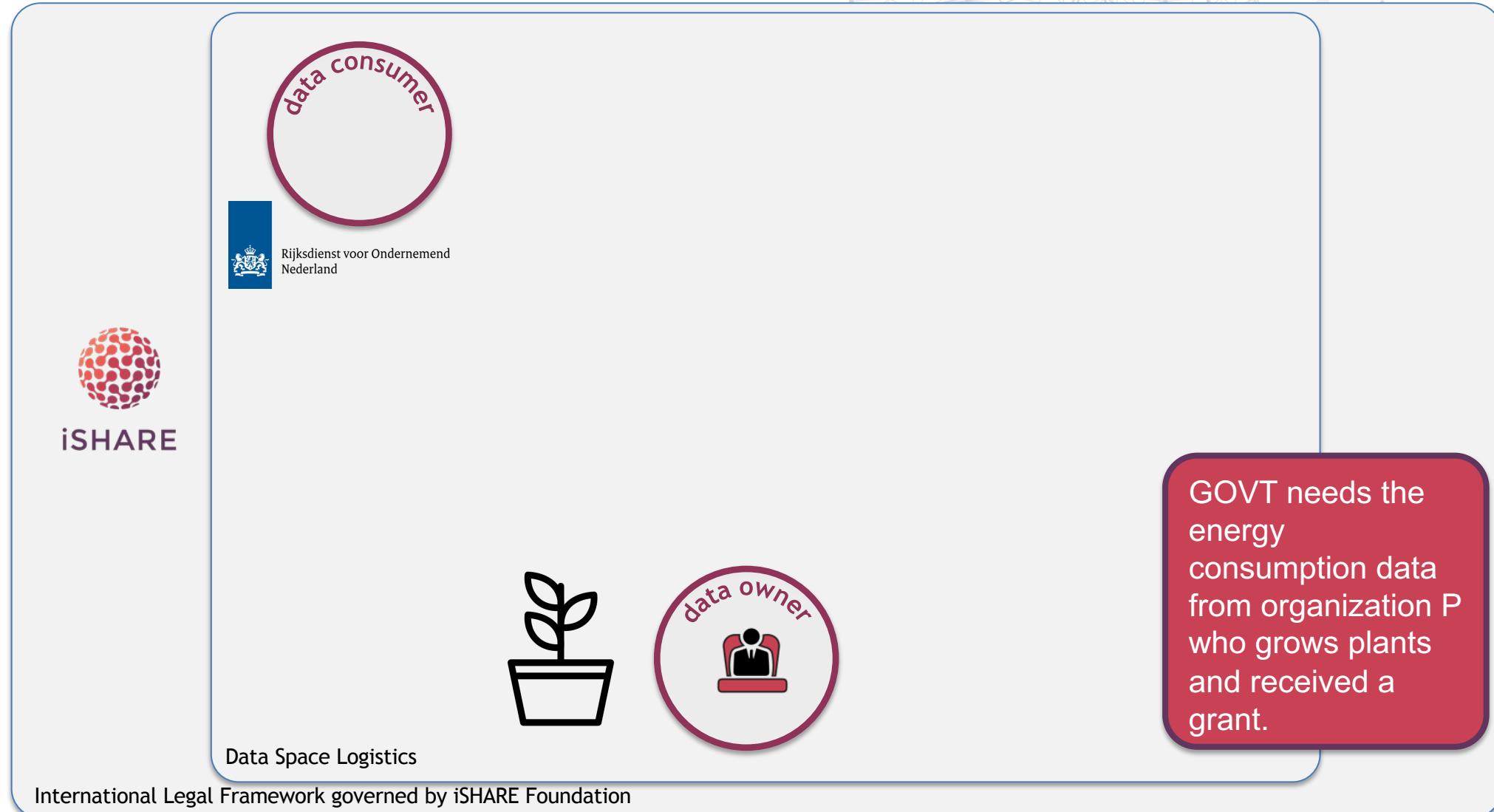


iSHARE

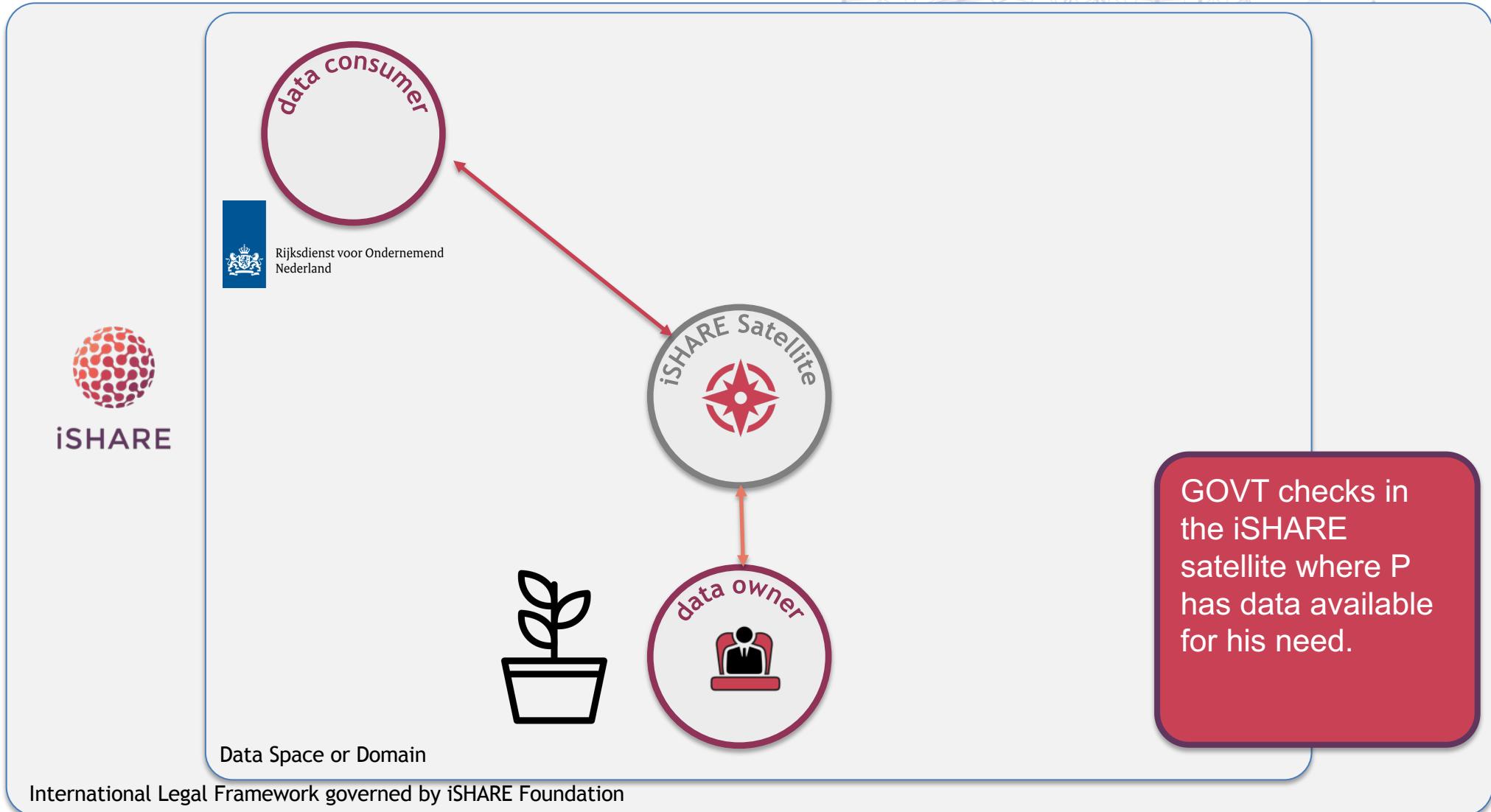


Climate agreement reporting

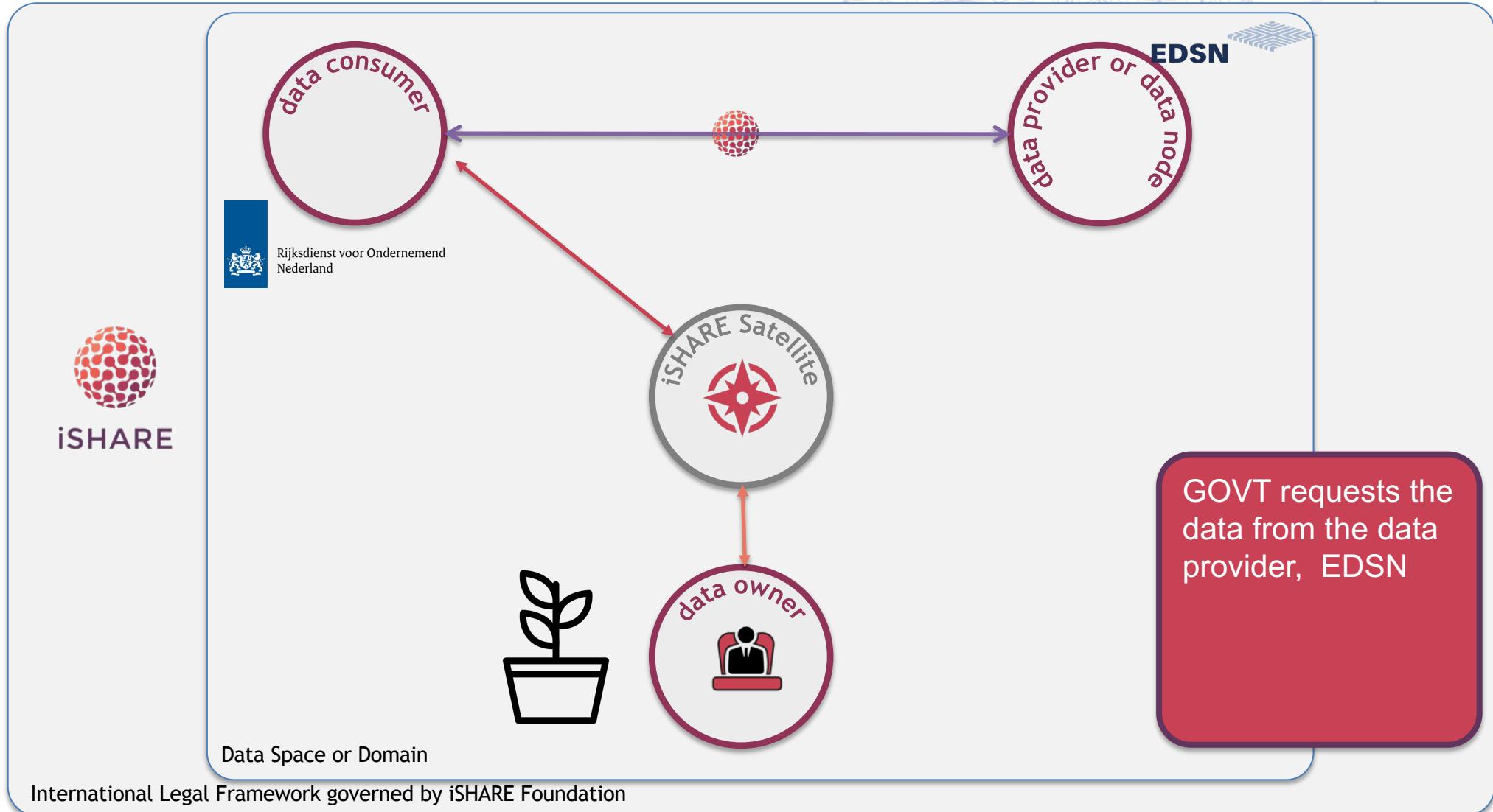
Reality example : Climate Agreement Reporting



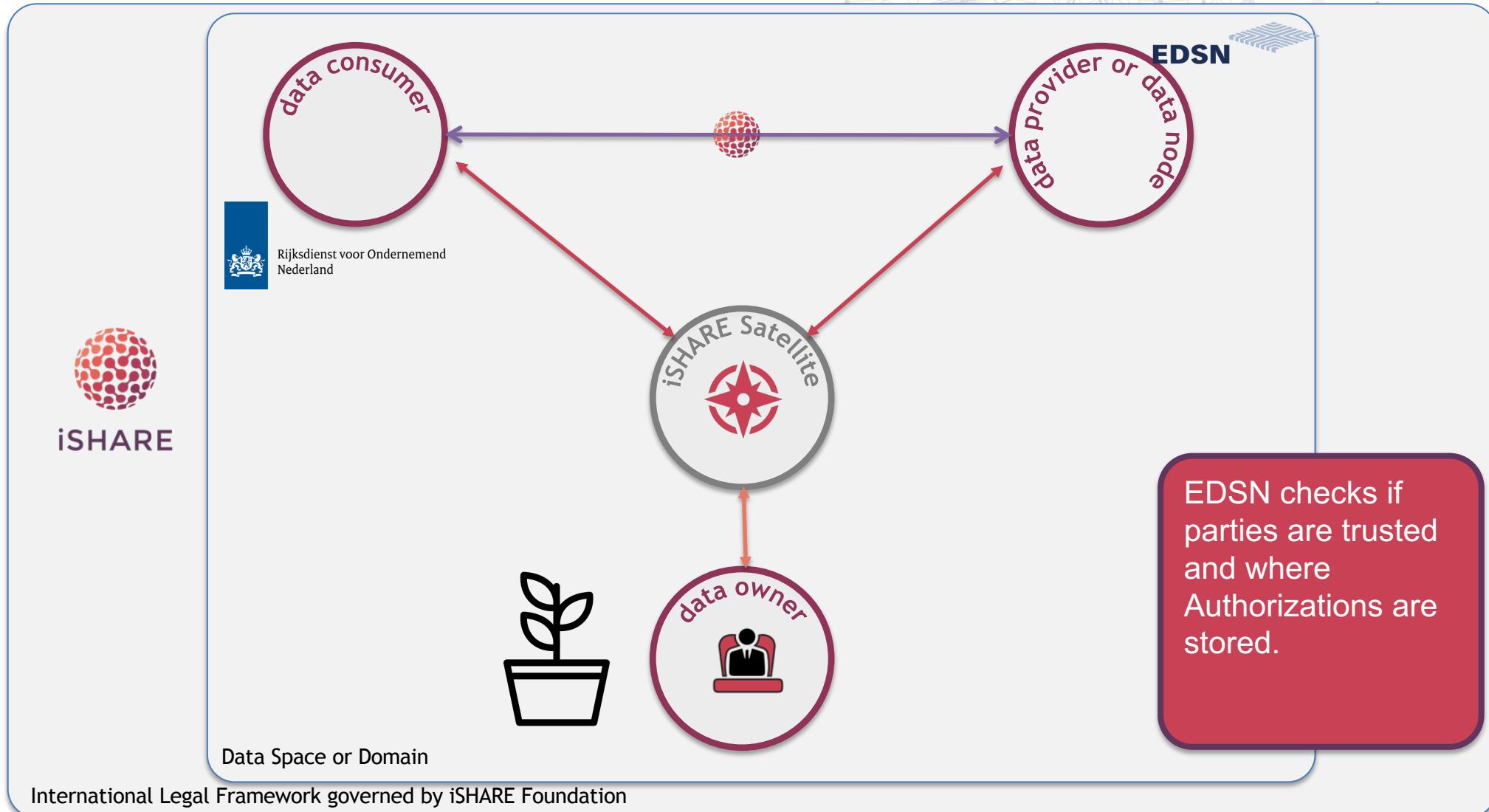
Reality example : Climate Agreement Reporting



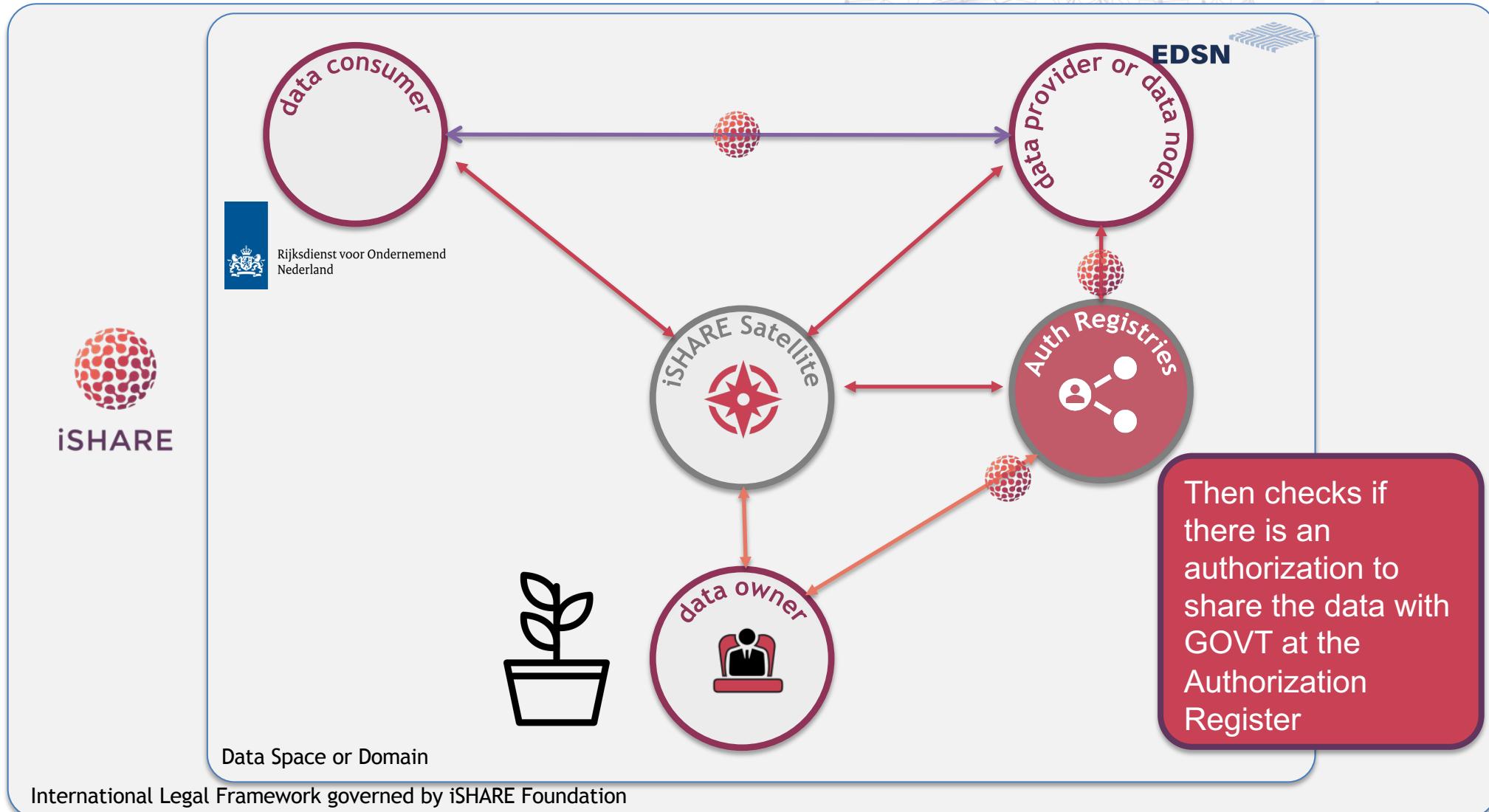
Reality example : Climate Agreement Reporting



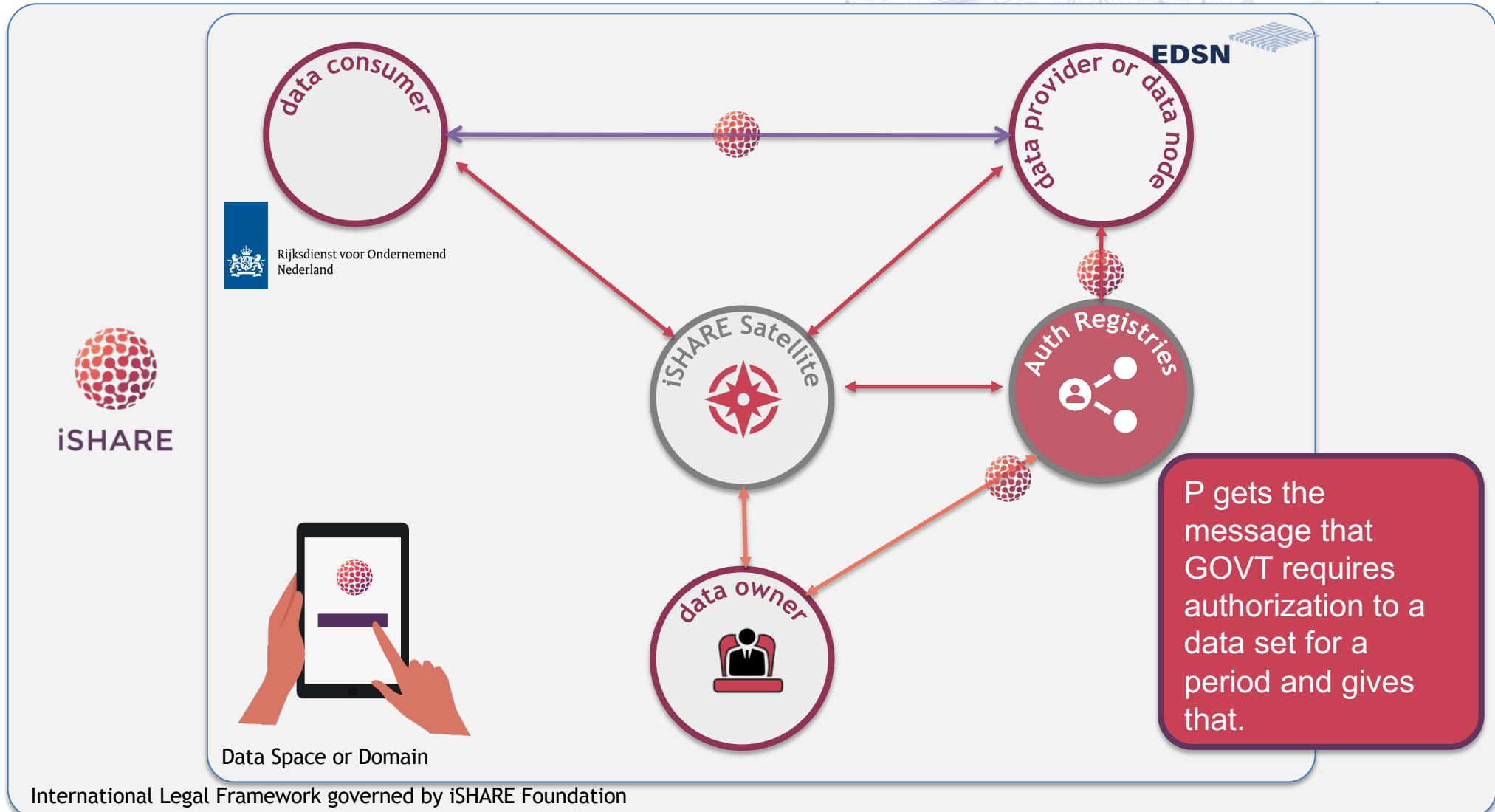
Reality example : Climate Agreement Reporting



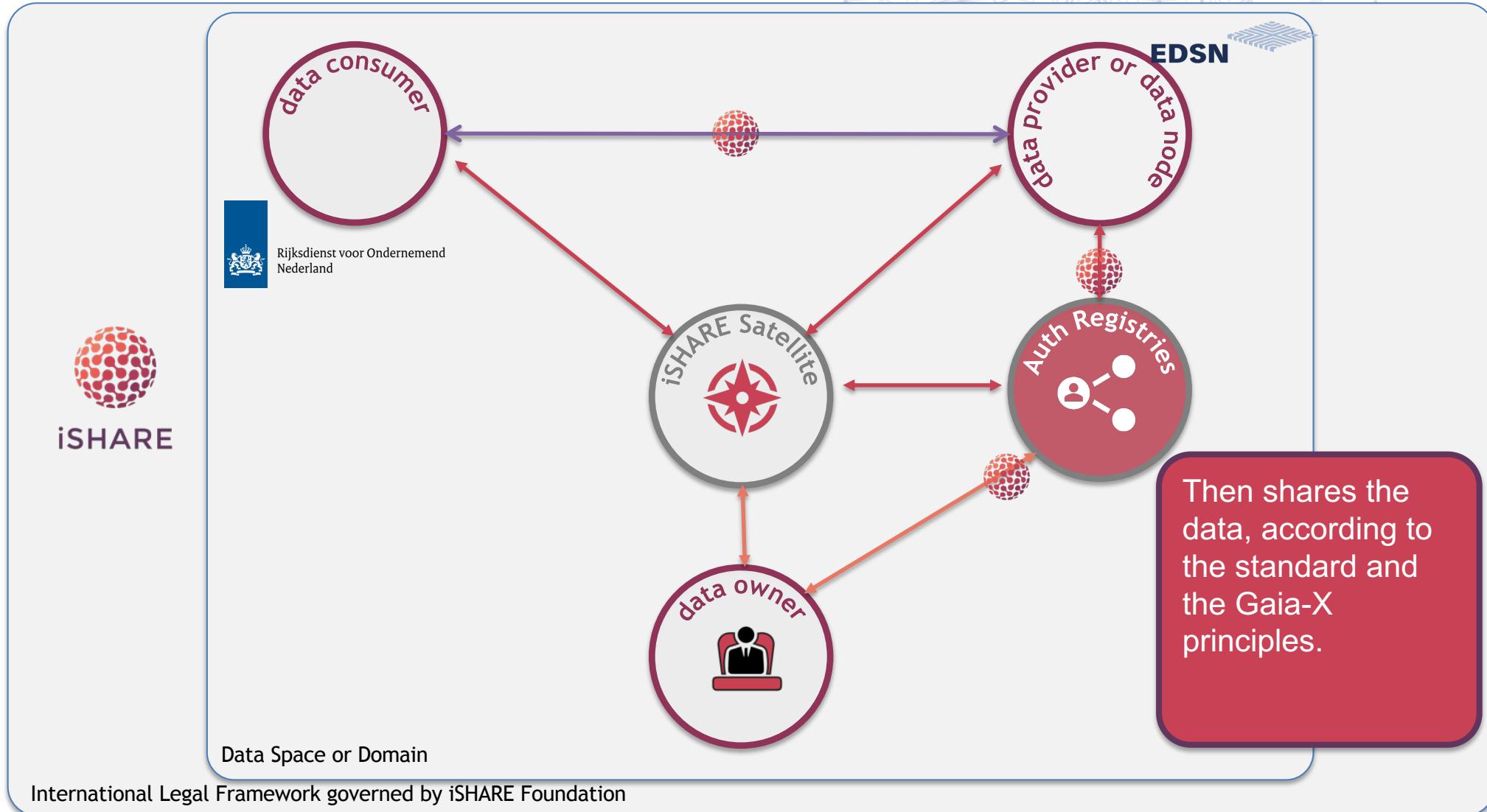
Reality example : Climate Agreement Reporting



Reality example : Climate Agreement Reporting



Reality example : Climate Agreement Reporting



Use case success factors to start your dataspace



Start with **existing** confidential business data of **many organizations** with a launching data consumer

Start with **simple data services** (like max 10 fields in a single service) with a **clear definition**, with **impactful use**.

Build on the **iSHARE trust framework from the start**, instead of waiting till the end.

Don't reinvent the wheel, but **utilize open-source components and open standards**

Follow our 3 step guide to get started with iSHARE today!



Step 1

Identify role and data space you wish to join
(or create)

[TELL ME MORE »](#)



Step 2

Development relevant to your role and testing

[TELL ME MORE »](#)



Step 3

Move to production and complete formalities

[TELL ME MORE »](#)



● Get in touch for more details

iSHARE.eu

And via this to get to the portals for your key interest

- Developers (postman collections etc)
<https://dev.ishare.eu>
<https://github.com/iSHAREScheme>
- Legal and scheme details
<https://ishareworks.atlassian.net>
- Community forum
<https://forum.ishare.eu>



Or by reaching out to our team:

- Gerard van der Hoeven
Director
gerard@ishare.eu
+31651523935
- Rajiv Rajani
CTO
rajiv@ishare.eu
+31617962003





iSHARE

.eu

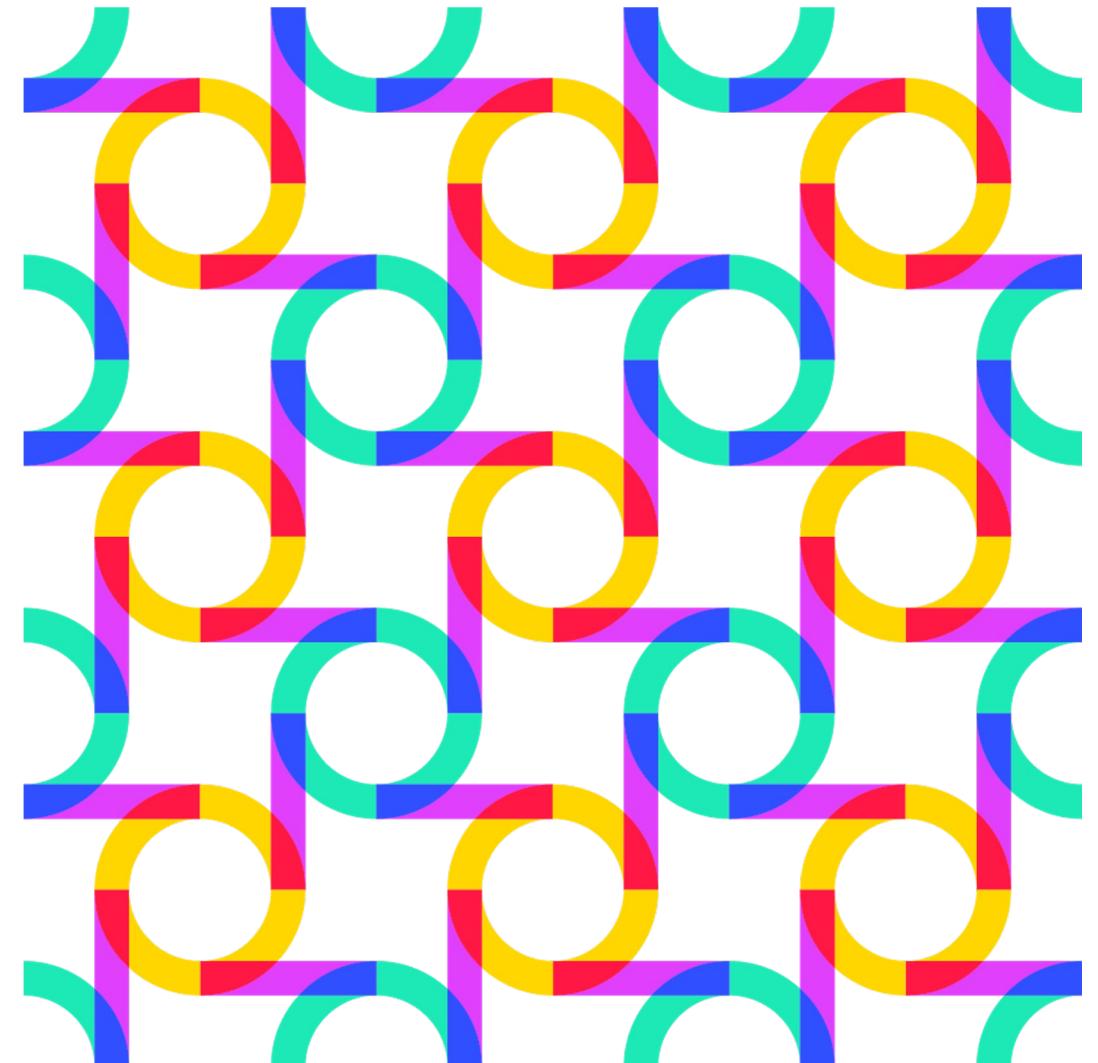


iSHARE has received funding from the Dutch Topsector Logistics,
as part of the Ministry of Infrastructure and Water.



i4Trust has received funding from the European Union's Horizon 2020
research and innovation programme under the Grant Agreement no 951975.

iSHARE and FIWARE bring the necessary components along with basic governance structure to create **i4Trust data spaces**

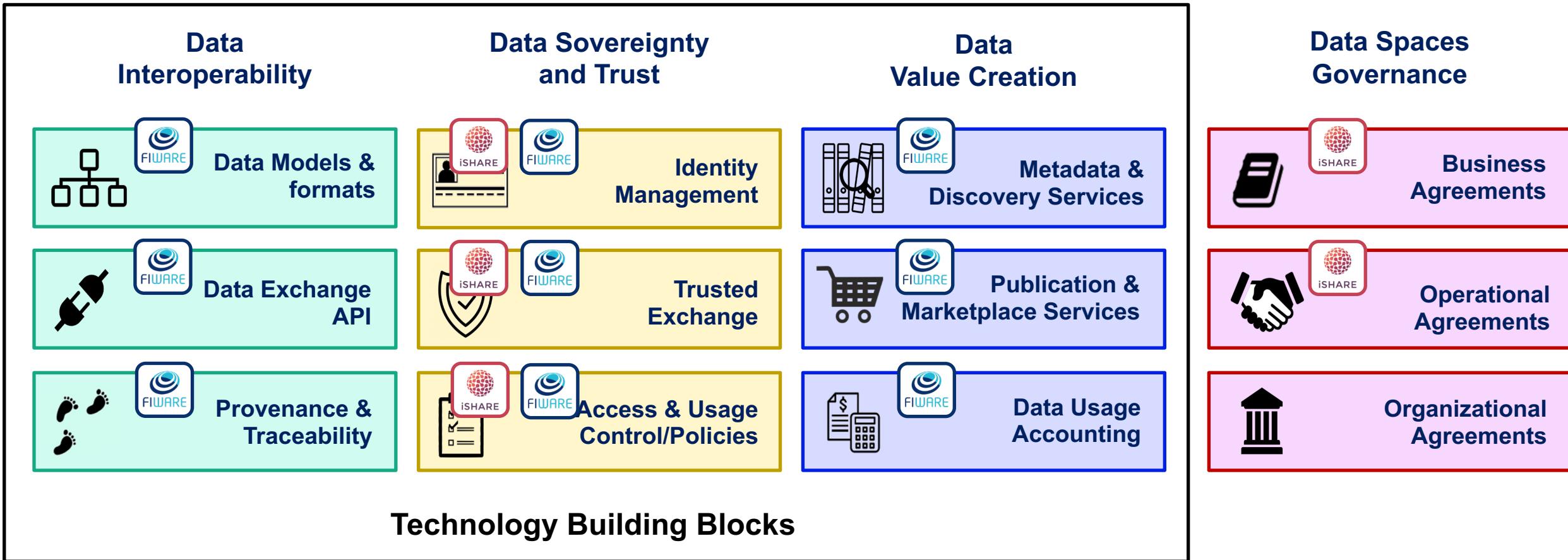


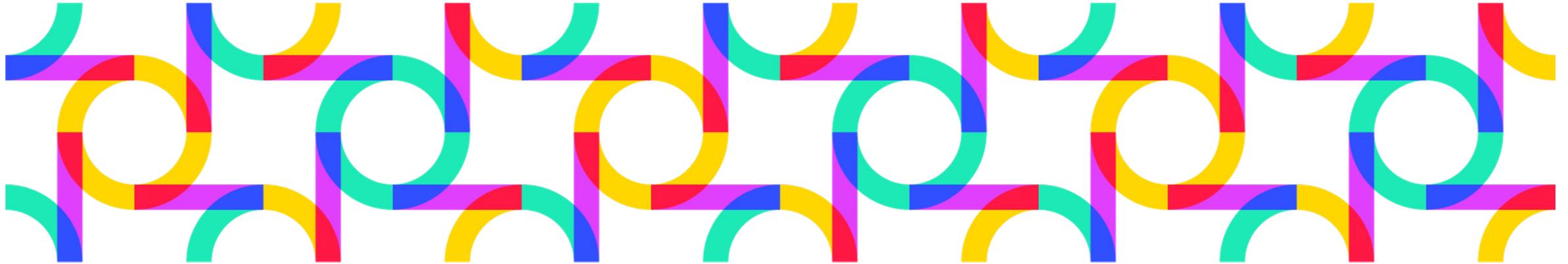
[i4Trust Website](#)

[i4Trust Community](#)



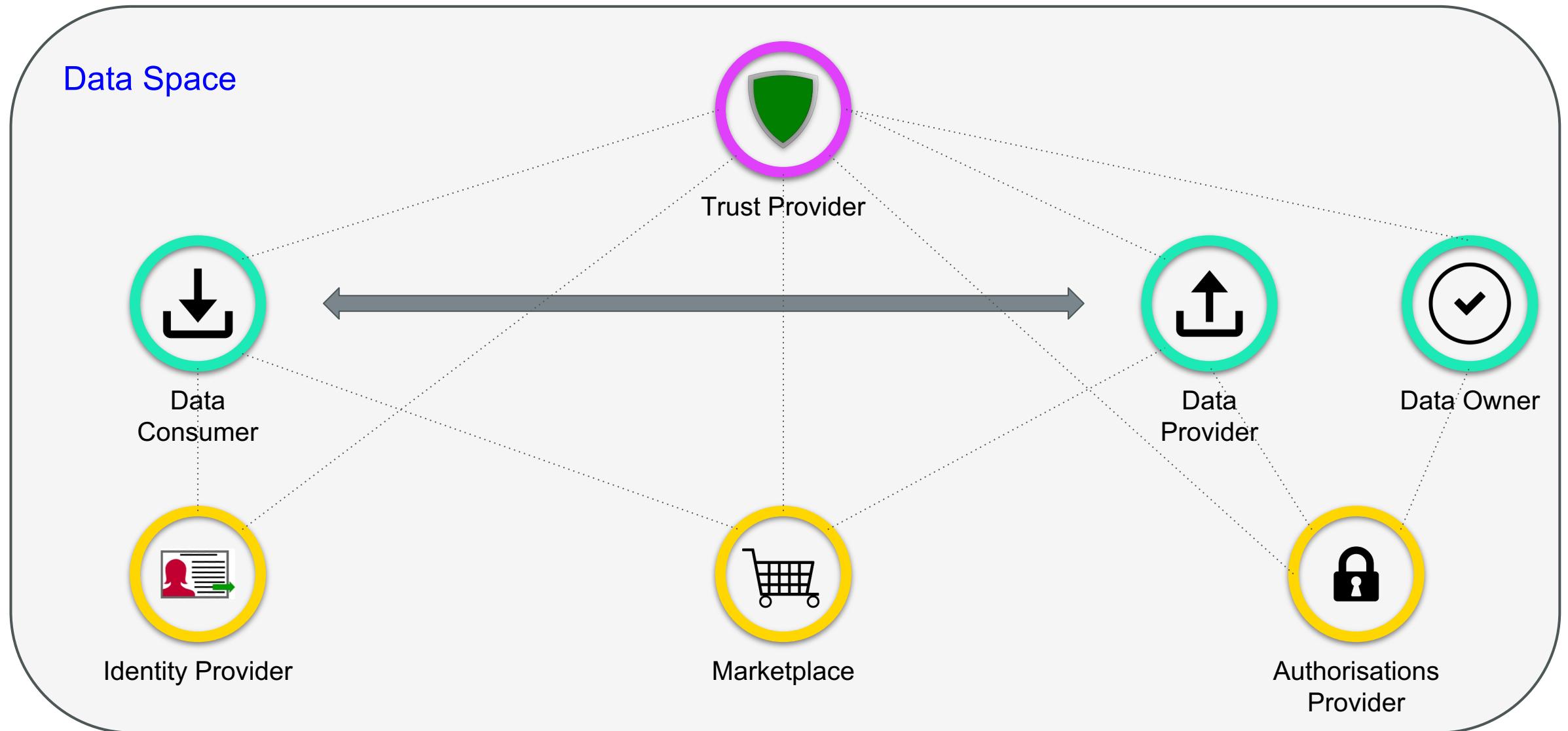
i4Trust: boilerplate for creating dataspaces



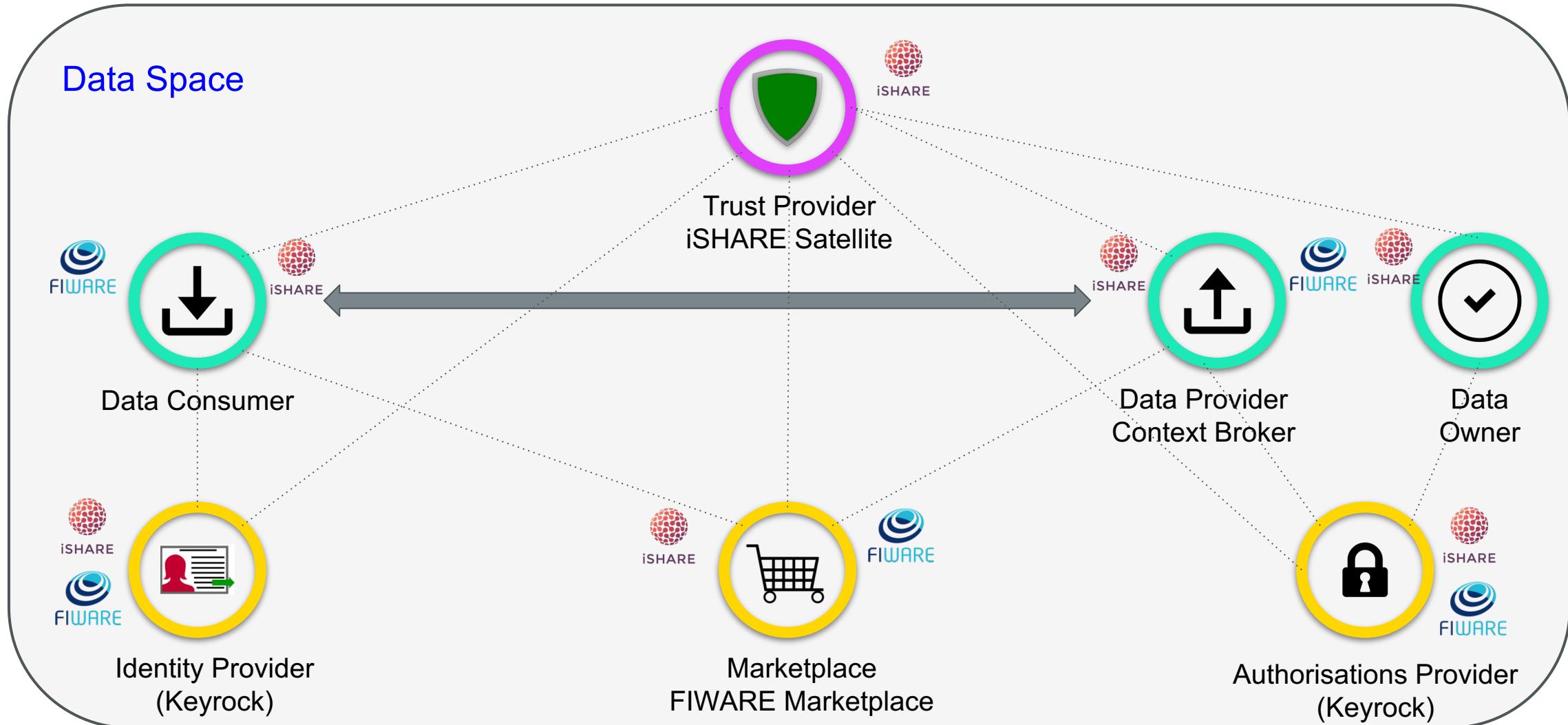


Summary of roles in i4Trust Data Spaces

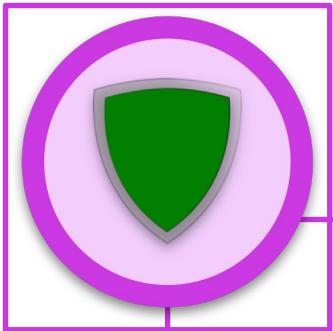
Roles in a Data Space



i4Trust Role model - iSHARE compliant open-source FIWARE components



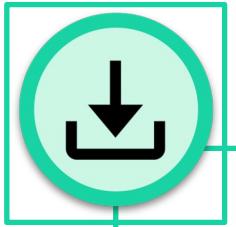
Trust Provider essentially facilitates trust in a data space and acting as a guardian



Trust Provider

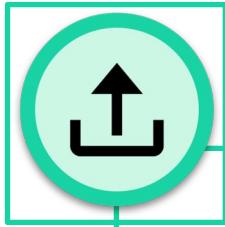
- Every data space needs a trust provider who acts as register of participants of the data space and keeps their status up to date
- They follow predefined and agreed upon procedures to maintain the list of participants
- Since they play important role in a data space it is paramount that trust provider is a neutral party or a party providing this service within the confines of strict agreements on neutrality
- Every data space should have one trust provider at minimum, however, same trust provider organisation can provide service in multiple data spaces
- In a large data space there can be more than one trust provider
- In i4Trust this role will be fulfilled by iSHARE satellite role

i4Trust enables data sharing among parties in an effective, trusted and secure way



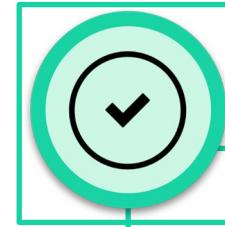
Data Consumer

- Data Consumer is a role played by organisation or a person who is interested in data at other party either for its own use or to provide services to the data owner/data provider
- It needs to handle data it receives in accordance to the conditions set by the data owner



Data Provider

- Data Provider is role played by organisation who provide data via means of service or portal
- Data Provider relies on data owner to provide with authorizations and usage rights for the data it shares with data consumer



Data Owner

- Data Owner is the party who has right over the data in given context and time
- It provides with authorizations, so data consumer can get access to data
- In i4Trust, data owner also can specify the conditions under which data is shared, thereby providing it with data sovereignty

Identity Provider role is designed for users to reuse their existing identity provider at various service/data providers

Identity Provider

- The Identity Provider role deals with the human identities with varying level of assurances, as defined in eIDAS framework, to support various use cases
- Depending on the criticality of the data, appropriate level of assurance for an identity can be requested
- iSHARE specifications are designed such that service/data provider does not necessarily need to pre-register an identity provider as it can verify if it is an iSHARE certified provider from iSHARE satellite
- Keyrock Identity Provider software from FIWARE already complies with iSHARE specifications and is available as open source



Authorisations Provider is a role which can be played by any organization as defined in iSHARE



Authorisations Provider

- The role only defines the interface for asking about authorizations and how the response should look like.
- The authorizations can be determined by using a policy database and/or transactional data from backend systems and/or existing authorizations from LDAP/AD or a combination thereof.
- Keyrock in FIWARE will provide a policy database to define policies for authorizations which can be combined with other sources to determine authorization during runtime.

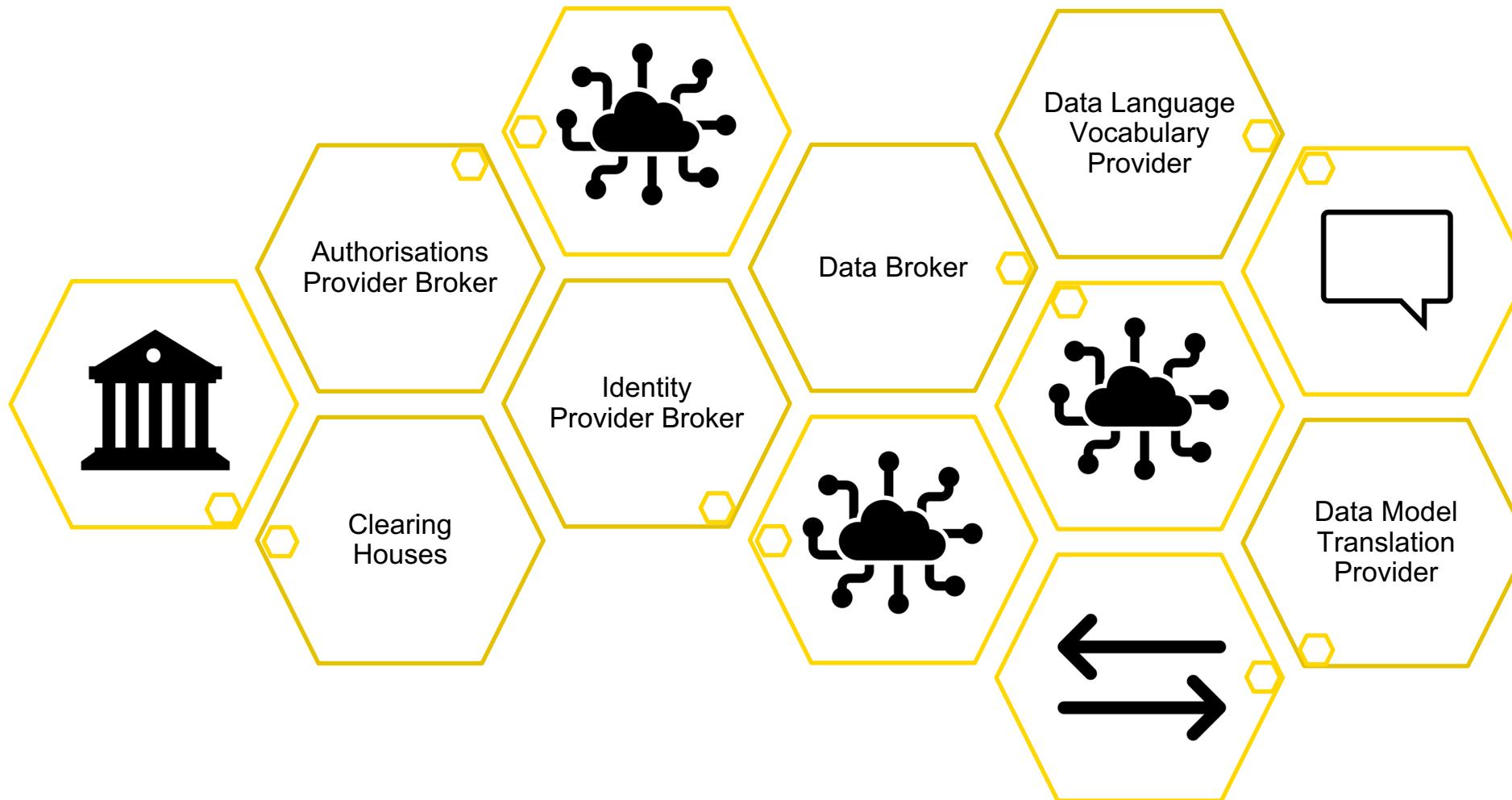
Marketplace allows discovery and monetization of data and services in a data space

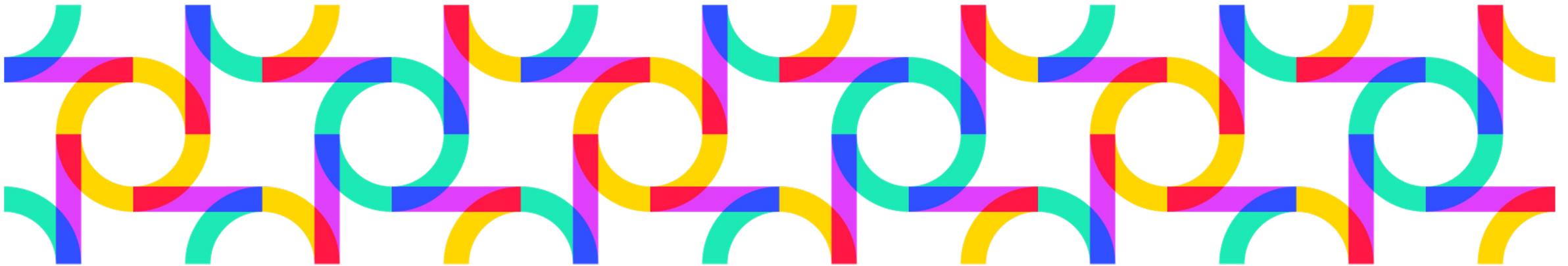


Marketplace

- The Marketplace provided by FIWARE technology allows data providers and data owners to list data and/or services to offer which data consumers can buy/subscribe to.
- On the other hand, data consumers can find offerings of relevant data from multiple data providers/owners.
- Besides, marketplace can act as clearing house and broker when required between the parties exchanging data so that data sharing transactions can be logged at 3rd party for auditing and billing purposes.

Additionally, other service providers can provide specific services within a data space





We take you by the hand in i4Trust.org

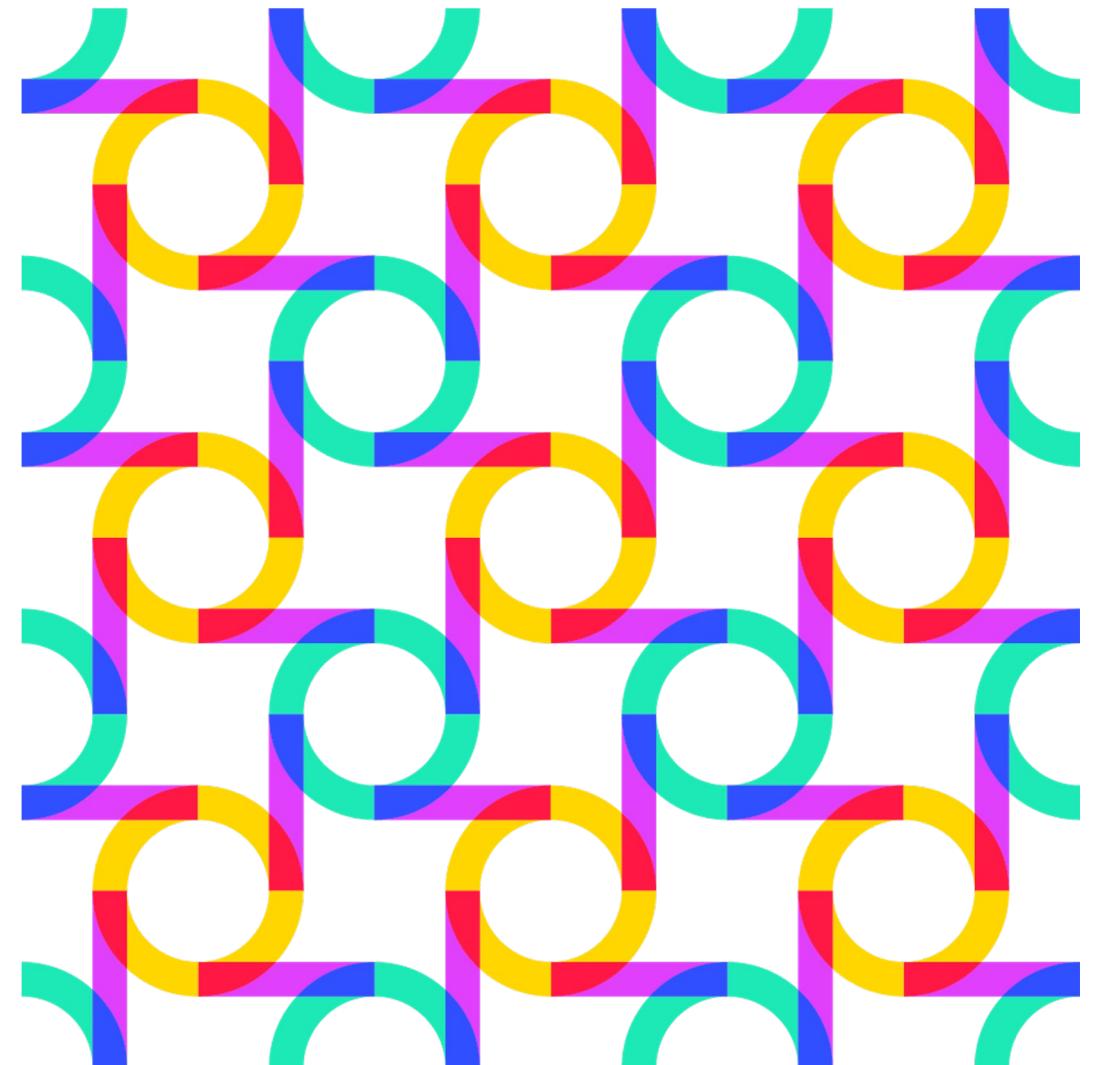
- **9 month customized mentoring programme, which include:**
 - Experiments implementation
 - **Mentoring support** for workforce re/up-skilling
 - Support on **legal, operational, technical and business**
 - Support on **i4Trust technology framework**
 - **Financial support.** Bottom-Up Experiments will be granted with a lump sum that will range in between €72,000.00 to €120,000.00

i4Trust Cross Valuechain Bootcamp

- Join us for i4Trust Cross Valuechain Bootcamp on **28 – 30 June**
- Opportunity to meet with all i4Trust projects
 - Find synergies with them in terms of using their solution and **join the first dataspaces in making**
 - Collaborate with them for making a cross valuechain solution
 - Explore future project possibilities together
 - Explore opportunities to jointly apply for i4Trust 2nd open call
 - ... and many more
- Register now - <https://www.airmeet.com/e/dd513fb0-e742-11ec-b1b2-394b94cc9521>



Thank you!



i4Trust has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement no 951975.