Ref. Ares(2026)6576416 - 30/06/2026

D3.3 Data Spaces Connectors

ExPEDite

Horizon Europe

101139527

Deliverable information

Deliverable Number	**D3.3**
Date of Issue	30/06/2026
Nature of Deliverable	OTHER
Dissemination Level	PU - Public
Main Editor(s)	Sergio Palacios (Bull)

This project has received funding from the European Union's Horizon Europe Research and Innovation Program, under Grant Agreement No. 101139527.

Document History

Date	Version	Remarks
01/03/2026	0.1	ToC
14/05/2026	0.2	Main content for Executive Summary, Sections 1,3,4,5,6 and 7
29/05/2026	1.0	Contributions finished. References added. Figures indexed.

List of Contributors

Beneficiary	Contributor(s)
Bull	Sergio Palacios Prieto
Bull	Jesús Martínez Gadea
OASC	Vincent Demortier

Document Reviewers

Beneficiary	Peer Reviewer(s)
VSB-TUO	Zdenek Slanina
RTU	Jānis Kampars

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency (CINEA). Neither the European Union nor the granting authority can be held responsible for them.

Contents

List of Acronyms 5
Executive Summary 8
1 Introduction 9
1.1 Purpose of the document and relation to the project 9
1.2 Relation to GA Objectives 9
1.3 Structure of the document 9
2 Energy Data Model 11
3 Overview of Data Spaces from European Union perspective 13
3.1 The EU Concept of Data Spaces 13
3.2 Policy Objectives and Strategic Rationale 13
3.2.1 Economic and Innovation Goals 13
3.2.2 Societal and Public Interest Objectives 13
3.3 Sectoral Scope of Common European Data Spaces 14
3.4 A Layered Regulatory Approach 14
3.5 Governance, Architecture and Interoperability 15
3.5.1 Governance Models and Roles 15
3.5.2 Technical Architecture and Interoperability 15
4 IDSA standards for connectors interoperability 17
4.1 IDSA Information Model 17
4.2 IDSA Dataspace Protocol 17
4.3 IDSA Reference Architecture model 18
4.4 Certification 19
5 ExPEDite Data Space Integration Suite 21
5.1 Description 21
5.2 Components 21
5.2.1 Keycloak & DAPS 21
5.2.2 Authority Portal 22
5.2.3 Data space connector 22
5.3 Implementation 23
5.4 Deployment and validation 24
6 Conclusions 32
7 References 33

Figures

Figure 1: The EU Local Digital Twin Toolbox framework [1] 11
Figure 2: The ExPEDite technical components mapping based on the EU Local Digital Twin framework 11
Figure 3: The central role of the ExPEDite Core Data Platform as to make it Data Space ready 12
Figure 4: Data Space Connectors communication scheme 18
Figure 5: Reference Architecture Model, layers and perspectives 19
Figure 6: IDSA certification process. 20
Figure 7: Authority Portal connectors client's section. 22
Figure 8: Data Space Connector infrastructure. 23
Figure 9: DS connectors infrastructure main data flows. 24
Figure 10: Authority Portal client creation. 25
Figure 11: Data offer creation in ExPEDite's connector. 26
Figure 12: Available assets. 27
Figure 13: Search for assets from other connectors in the Data Space. 28
Figure 14: Assets retrieved from ExPEDite's connector. 29
Figure 15: Contract negotiation. 29
Figure 16: Infrastructure main fluxes. 30
Figure 17: Initiate data transfer. 30
Figure 18: Data received in webhook website. 31

List of Acronyms

Acronym	Meaning
ABAC	Attribute-based access control, an authorisation model where permissions are granted based on attributes of users, resources or environment
AHU	Air Handling Unit, a central component of an HVAC (Heating, Ventilation, and Air Conditioning) system
AI	Artificial Intelligence
API	Application Programming Interface, an interface used for multiple systems to communicate with each other
ASGI	Asynchronous Server Gateway Interface, a specification for Python web servers and applications that allows for asynchronous (non-blocking) communication in addition to traditional synchronous handling
BMS	Building Management System, a centralized software and hardware platform used to monitor, control, and optimize a building's essential systems
BMSIC	Building Management System integration component, a component developed as part of WP3 for integrating BMS
CDS	Core Data Services, a set of components developed as part of WP3 serving as data and knowledge exchange backbone
CEDS	Common European Data Space
CoAP	Constrained Application Protocol, a lightweight, web-like protocol designed specifically for resource-constrained devices
CO_2	Carbon Dioxide
CPU	Central Processing Unit
CSV	Comma-separated Values, a file format used for data exchange
D	Deliverable
DA	Data Act
DAPS	Dynamic Attribute Provisioning Service, a system that issues and manages digital identities
DDFE	District Data Fusion Engine, a component developed in WP3 used for data aggregation and anomaly detection
DGA	Data Governance Act
DITF	BMS code used to denote building Zunda krastmala 10
DS	Data Space
DSC	Data Space Connectors
DSIS	Data Spaces integration suite, a component developed in WP3 used for integrating with external dataspaces
DT	Digital Twin
EU	European Union
EDC	Eclipse Data Space Connector
FAIR	Findable, Accessible, Interoperable, and Reusable
GA	Grant Agreement
GDPR	General Data Protection Regulation
HTML5	HyperText Markup Language version 5, a language used to create and structure content on the web

Acronym	Meaning
HTTP	Hyper Text Transfer Protocol
HVAC	Heating, ventilation, and air conditioning, a system used to control the indoor environment, controlled by BMS
IAM	Identity and Access Management, a framework of technologies, policies, and processes that ensures that users or systems are provided with the correct level of access
IdP	Identity provider, a service or system that authenticates users and manages their identities
IDSA	International Data Spaces Association, a non-profit alliance of companies, organisations, and researchers that promotes secure, sovereign, and standardized data exchange across industries
IoT	Internet of Things, a network of physical devices (e.g sensors, machines) that are connected to the internet and are used for data acquisition or control
JSON	JavaScript Object Notation, a file format used for data exchange
M	Month
MCU	Microcontroller Unit, a small computer on a single chip designed to control electronic devices
MIMs	Minimum Interoperability Mechanisms, technical and organisational building blocks that ensure independent digital systems can collaborate
ML	Machine learning, an approach that allows computers to learn from data and make decisions or predictions without being explicitly programmed.
MQTT	Message Queuing Telemetry Transport, a protocol widely used in IoT systems
NGSI-LD	Next Generation Service Interface-Linked Data, API and data model for managing context information that is widely used in smart cities, IoT, and data spaces scenarios
OAuth	Open Authorisation, open standard for access delegation that allows applications to access resources (like your data) on your behalf, without sharing your password.
OGC	Open Geospatial Consortium, an international organisation that develops and promotes open standards for geospatial data and services
PA	BMS code used to denote building at Zunda krastmala 8
PED	Positive Energy District, an urban area that produces more renewable energy than it consumes annually within its geographical and/or virtual boundaries
PR	Pattern Repository, a component developed within WP3 that is used for knowledge dissemination
RAM	Reference Architecture Model
RBAC	Role-based access control, an authorisation model where permissions are granted based on the role of the user or system
REST	Representational State Transfer, architectural style for designing networked applications
RES	Renewable Energy Sources, energy that come from natural processes that are constantly replenished (e.g. solar, wind energy)

Acronym	Meaning
RH	Relative Humidity, the percentage of water vapor in the air compared to the maximum amount of water vapor the air can hold at a specific temperature
RMS	Root Mean Square, a statistical measure
RPT	Requesting Party Token, a specialised token used in access management
RTU	Riga Technical University
SDK	Software Development Kit, a collection of tools and resources that are used to build software
SEO	Search Engine Optimisation, a process of improving a website's ranking in search engines
SME	Small and Medium-sized Enterprises
SSL	Secure Sockets Layer, security protocol used to encrypt data
SSO	Single sign-on, authentication system that allows a user to log in once and gain access to multiple applications or services without needing to log in repeatedly
T	Task
TLS	Transport Layer Security, a cryptography protocol used in data exchange over the network
UART	Universal Asynchronous Receiver/Transmitter, a hardware communication module used to send and receive data asynchronously between digital devices
UI	User interface
UMA	User-Managed Access, an authorisation protocol built on OAuth 2.0 that gives users fine-grained control over who can access their personal data and services
UPS	Uninterruptible Power Supply, a device that provides emergency backup power
URI	Uniform Resource Identifier, a string of characters used to identify a resource on the internet
URL	Uniform Resource Locator
UUID	Universally Unique Identifier, a number used to uniquely identify information
WP	Work Package

Executive Summary

This deliverable, D3.3 “Data Spaces Connectors”, documents the research about the different connectors available under the IDSA standards and details the developments made for the Data Space Integration Suite (DSIS) component.

Additionally, the study around the Energy Data Model to be adopted in ExPEDite that was roughly initiated and sketched in D3.1 “Data and Knowledge Management Framework (v1)” has been finalised and detailed in this deliverable.

The DSIS is a containerized suite that will allow the project partners or any other interested participant to deploy their own data spaces connectors and join to the ExPEDite data space under the policies established by the IDSA.

The main components delivered under the DSIS and covered under this deliverable are:

- Keycloak & DAPS duo.
- Authority Portal.
- Data Space Connector.

Each component is described in the deliverable to give a detailed view of each of them and have been developed ensuring compliance with the standards required and under FAIR principles.

1 Introduction

1.1 Purpose of the document and relation to the project

The present document, D3.3 “Data Spaces Connectors”, documents the final release of the work achieved inside the T3.3 “Data Spaces Integration Suite” between M10 and M30. Some insights of the work done were included in D3.1 “Data and Knowledge Management Framework (v1)” that was submitted on M18.

Data Spaces Integration Suite is a component that will provide the project with the required functionalities to interoperate with other projects or any external participants that could be interested in providing data for the models developed in the WP4 “ExPEDite Modeling and Simulation Suite”.

In the same way, give the opportunity to these participants to consume data sets that potentially could be published by any project partner in the project Data Space. It is worth to say that any data exchange between the project partners could be done maintaining the data sovereignty and without creating any internal data repository.

This directly contributes to the Expected Outcome 2: “Enhanced data gathering approaches with identification relevant (standardized) multidimensional data set (e.g. meteorological, load profile, social, geo-spatial, etc.) high-resolution real-time data streams (e.g. renewable energy production, energy consumption), and relevant forecasting data, drawing also on the work of common European data spaces, including the smart communities data space and Destination Earth” giving the to the project the tools to establish links with the EU’s Data Spaces initiative, and to benefit from and contribute to the high-quality data gathered.

1.2 Relation to GA Objectives

The results of the developments covered under this deliverable contributes directly to the achievement of O1: “Deliver a standardized data framework enabling a consolidated view of all district-level energy related data streams, including energy consumption and generation, mobility and transport and smaller scale (building) management systems, through a district Digital Twin”.

The component developed allow the project to potentially provide valuable data to other energy projects and/or retrieve data that could enrich the quality of the modelling tools developed under WP4. These exchanges could be done granting the data security and sovereignty that are provided by the International Data Space Association (IDSA) regulation framework under what has been developed the DSIS.

1.3 Structure of the document

In the present deliverable is documented the component developed under the task T3.3 covering all the subtasks identified for the development of the Data Spaces Integration Suite.

Section 2 give details about the research done to decide if any of the standards Energy Data Models present in the market could fit the project requirements or if a tailored one was required. In that way, the final decision taken in explained.

Section 3 gives an idea about what is the perspective of the Data Spaces for the European Union. The section covers what is the aim of the European Commission to put focus on Data

Spaces, the objectives that is pursuing and an overview of the main regulatory framework that is being designed to guarantee the standardization, the interoperability and the trust.

Section 4 discusses the details about the different standards that are evolving if we talk about connectors interoperability, those standards are certificated by the International Data Spaces Association (IDSA). In that line, an overview about the certification's processes set by IDSA is given.

Section 5 describes what is the Data Space Integration Suite and give details about the different components that are part of it. The section includes critical information about the implementation of the solution and details the validation process followed to assure all the features expected are covered and are operational.

Lastly, section 6 joins the conclusions of the present deliverable, outlining the decisions taken and the importance of the described component for the overall project. In that line, the section remarks the alignment of the ExPEDite project with the EU objectives through the European Strategy for Data.

2 Energy Data Model

As a wide variety of data must be consumed and produced to support the ExPEDite Digital Twins services offered by heterogeneous technical components (delivered by WP3, WP4 and WP5), it is first important to map and to characterize these datasets shared among the ExPEDite technical components in order to leverage the Data Space paradigm. In this perspective, the [1] EU LDT Toolbox framework (see Figure 1) has been used as a starting point to support the general mapping of the ExPEDite technical components.

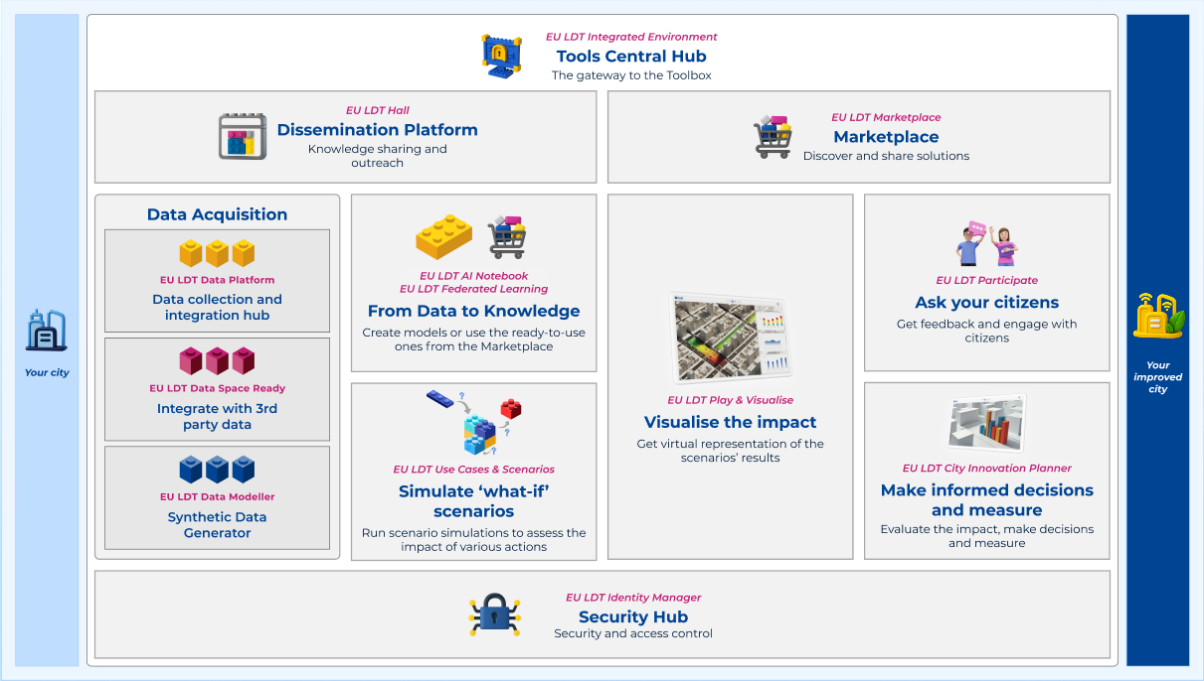

Figure 1: The EU Local Digital Twin Toolbox framework [1]

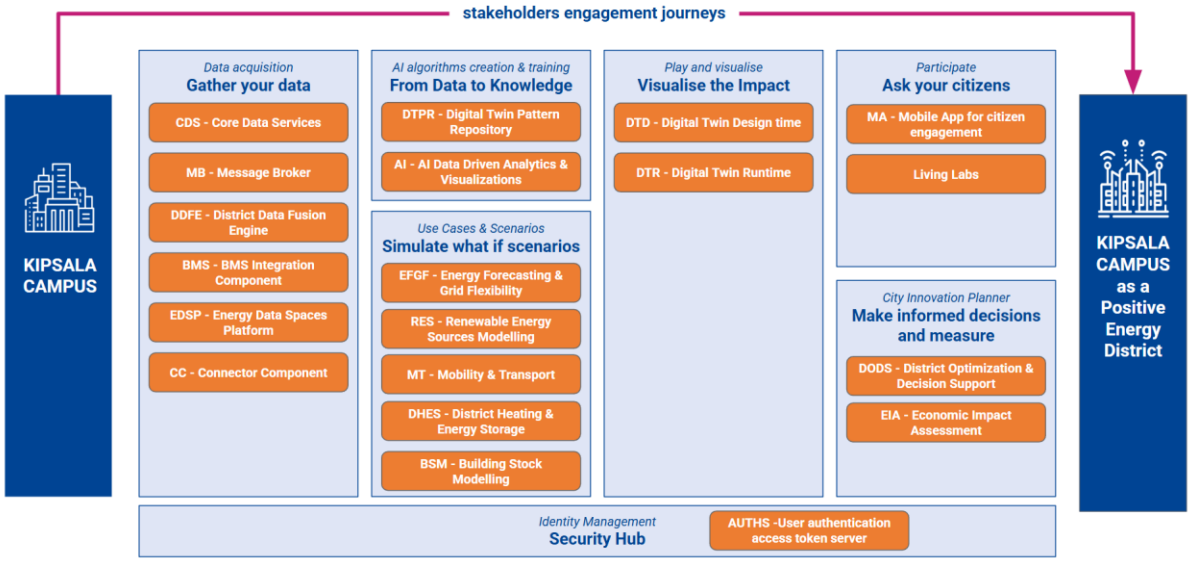

Figure 2: The ExPEDite technical components mapping based on the EU Local Digital Twin framework

In this ExPEDite technical mapping (see Figure 2) the Core Data Services (CDS) component designed and implemented in T3.1 plays a central role for harmonizing the data models and to control the distribution and usage of the Digital Twin data among the other components, including external ones through data space connectors.

Then, the [2] Living-in.eu Minimal Interoperable Mechanisms (MIMs Plus Version 7.0) have been incrementally implemented, evaluated and improved through the CDS for facilitating the characterization of the Digital Twins assets and the data they produced and consumed (see the article on the ExPEDite website: [3] EU LDT Toolbox and MIMs reinforcing ExPEDite DT platform).

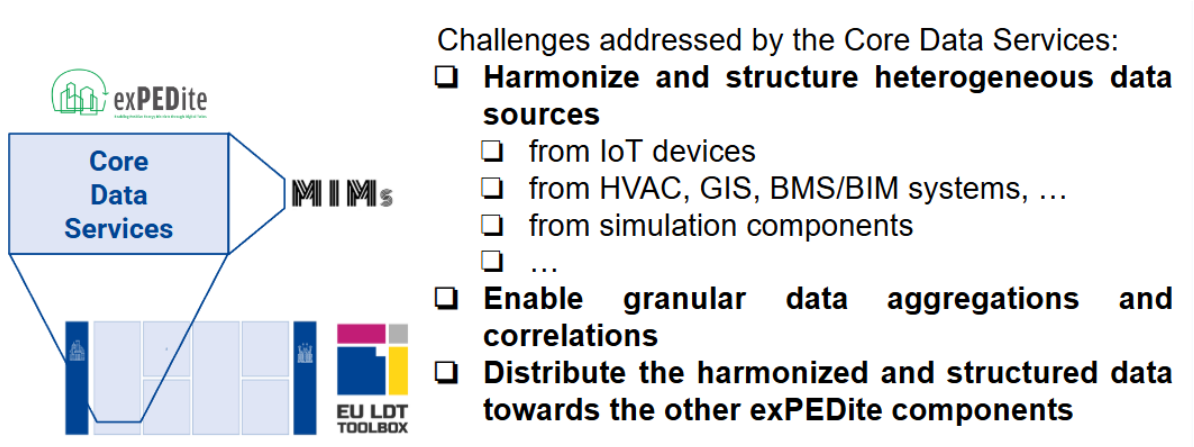

Figure 3: The central role of the ExPEDite Core Data Platform as to make it Data Space ready

Mainly based on MIM1 and MIM2 specifications, the CDS (see Figure 3) evolved from tailor made API and data models towards NGSI-LD (standard from [4] ETSI TC DATA) API and data models leveraging the [5] Smart Data Models repository.

The data products exposed or consumed through the ExPEDite DSIS component should rely on NGSI-LD data model. This will also facilitate the possible integration of ExPEDite platform in emerging data spaces that could be relevant for Positive Energy Districts management.

This approach has also been validated based on discussions with sister projects BiPED and Tips4PED and with the DS4SSC pilot project [6] Data Spaces for Positive Energy Districts DS4PED.

3 Overview of Data Spaces from European Union perspective

3.1 The EU Concept of Data Spaces

In the European Union, data spaces are becoming a core instrument for building a single market for data, it has been defined in the European Strategy for Data that was published by the European Commission in February 2020. Instead of centralized data repositories, the data spaces are federated ecosystems that enable trusted data sharing among multiple participants (public authorities, private companies, researchers, and individuals) while maintaining the data sovereignty in the data providers, allowing them to keep the control of their data.

The European Commission defines a Common European Data Space (CEDS) as an environment that brings together:

- Interoperable data infrastructures.
- Common governance frameworks.
- Shared standards, tools, and services.

That is to facilitate secure, voluntary, and sovereign data sharing across borders and sectors.

As mentioned, a defining feature is data sovereignty, participants decide who can access their data, under which conditions, and for which purposes, aligning with European values such as privacy, fairness, and competition.

3.2 Policy Objectives and Strategic Rationale

3.2.1 Economic and Innovation Goals

Data is being recognised as a strategic resource for economic growth, artificial intelligence (AI) and industrial competitiveness. The EU estimates that a large share of industrial and public-sector data is not being used and exploited due to fragmentation, legal uncertainty and lack of trust.

Data spaces could help use this data by:

- Unlocking cross-sectoral data reuse.
- Supporting SMEs' access to high-quality datasets.
- Fostering EU-based data ecosystems as an alternative to platform-dominated models.
- Strengthen Europe's global competitiveness in AI and advanced analytics.

3.2.2 Societal and Public Interest Objectives

Beyond economic value, EU data spaces seek other societal objectives, for example:

- Help to improve public policy and evidence-based decision-making.
- Improved healthcare outcomes.
- Climate action and Green Deal implementation.

- Mobility efficiency, energy transition and precision agriculture.

For the public sector, data spaces provide mechanisms to reuse data that cannot be released as open data (sensitive health or administrative datasets) under controlled and lawful conditions.

3.3 Sectoral Scope of Common European Data Spaces

The European Data Strategy has identified a set of strategic sectors for the development of common data spaces. The key domains include:

- Health (European Health Data Space).
- Mobility and transport.
- Energy.
- Agriculture.
- Manufacturing and industry.
- Finance.
- Public administration.
- Skills and employment.
- Green Deal and environment.
- Open Science (European Open Science Cloud).

Additional domains have been added to the previous list (p.e. tourism, media, language, cultural heritage, defence and research & innovation).

Each data space is specific for each sector, including different data types, stakeholders, and regulatory constraints, but they share common architectural and governance principles to enable future interconnection.

3.4 A Layered Regulatory Approach

Data spaces are not governed by a single law. Different regulations affect directly to them:

- General Data Protection Regulation (GDPR): for personal data protection.
- Open Data Directive: focusing on the reuse of public sector information.
- Data Governance Act (DGA): focusing on increasing trust in data sharing regulating trust mechanisms between data intermediaries.
- Data Act (DA): establishing rights and obligations for accessing and sharing data generated by connected products and services (mainly for industrial and IoT data).
- AI Act: lawful and trustworthy AI development.

Together, these instruments establish legal preconditions for scalable and trustworthy data spaces.

3.5 Governance, Architecture and Interoperability

3.5.1 Governance Models and Roles

Governance is a key point of European data spaces and a differentiator from data sharing models managed by market and based on a centralized platform. EU data spaces are built over a federated governance approach, meaning that there is not a single actor that owns or controls the entire ecosystem. Instead, governance is distributed among multiple stakeholders according to different roles and defined rules (European Commission, 2020; 2024).

Typical governance roles include:

- Data holders: participants that generate and/or control data and decide whether, how, and under which conditions it is shared.
- Data users: participants that access and reuse data for specific purposes, such as service provision, research, or policy-making.
- Intermediaries and service providers: technical or organisational participants offering services such as data exchange, identity management, metadata catalogues, or usage monitoring.
- Governing bodies: sector-specific or domain-level organisations responsible for defining common rules, access policies, certification schemes, and compliance mechanisms.

This approach based on the governance by design helps to foster trust. That trust is what European Commission identifies as the main bottleneck for large-scale data sharing in Europe.

3.5.2 Technical Architecture and Interoperability

From a technical perspective, Data Spaces follow a federated and interoperable architecture, rather than a centralised one. As previously said, data sovereignty is one of the key principles of Data Spaces, so data remains with the data holder and is made accessible through standardised interfaces and secured connections.

Core architectural building blocks commonly include:

- Identity and access management (IAM): that enable authentication, authorisation, and role-based access.
- Metadata and cataloguing services: that allow participants to discover datasets, understand usage conditions, and assess data quality before accessing to the data itself.
- Interoperability layers: common data models, semantic standards, APIs, and ontologies that ensure data from different sources can be combined.

- Usage control and monitoring mechanisms: that enforce contractual and legal constraints on how data can be used after the data transfer.

The Data Act collect the rules that reinforces these architectural principles by imposing explicit obligations on data holders to provide data in a machine-readable, structured, and interoperable format, and by making interoperability within common European data spaces a legal requirement.

4 IDSA standards for connectors interoperability

Data Space Connectors (DSC) are the key elements in information exchange in Data Spaces (DS), they can be considered as the plug that makes possible for a participant to connect and share data with others in a secure and transparent way while maintaining the sovereignty over their own information. In order to make them capable of connecting Data Spaces with different standards, they need to be highly interoperable and, to achieve such interoperability, IDSA (International Data Spaces Association) has developed the [7] IDS Information Model (IDS IM), the [8] IDS Dataspace Protocol (IDS DP) and the [9] Reference Architecture Model (IDS RAM), which allows sharing the information between DS with different standards and/or architectures through the use of several communication protocols, policies and models. Finally, IDSA allows anyone wishing to develop a connector to perform a [10] certification process which ensures that a specific piece of software accomplishes all the requirements defined above.

4.1 IDSA Information Model

The IDSA Information Model defines an ontology containing a set of theoretical objects, declarative representations and software libraries that are used to define the infrastructure, the participants and the regulations of the data assets used within data spaces, as well as the Data Applications. Additionally, each data asset is defined by the following set of layers called Facets that describe the data in further detail:

- **Resource facet**: a high-level definition of the data.
- **Data facet**: the data itself.
- **Application facet**: specific applications that performs operations with the data.
- **Infrastructure facet**: a list of all the components of the infrastructure.
- **Participant facet**: data referencing a real person.
- **Regulations facet**: definition of the contracts.
- **Interactions facet**: list of each action performed.
- **Maintenance facet**: performs maintenance tasks.

Facets are key in data management within a data space because, among other things, they make possible to perform advanced searches, having complete traceability over the information exchanged between participants, performing special operations through apps and identifying the ownership of specific data.

In a nutshell, the information model is the foundation upon which a data space is built; it gives a coherent structure to the data used within and allows a seamless communication between all participants without losing control over sovereignty.

4.2 IDSA Dataspace Protocol

If the information model is the structure, the data space protocol defined by IDSA is the method by which that structured information is transmitted between participants in the same data space or between participants in different data spaces, as shown in Figure 4. It can be compared with

the communication protocol used in internet to perform data exchange, since both establish the rules for basic communication and are used for the same purpose.

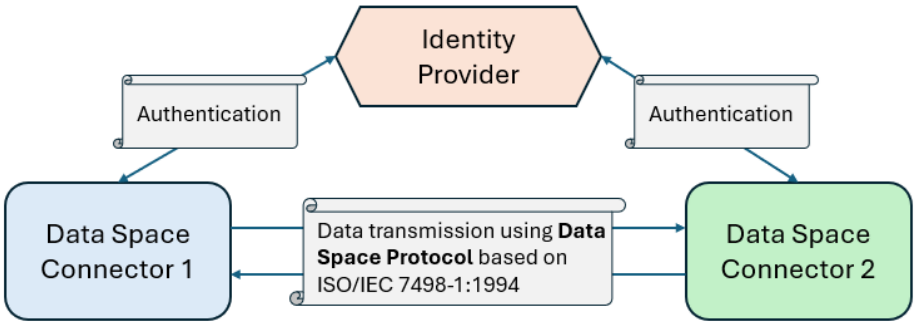

Figure 4: Data Space Connectors communication scheme

In the case of the data space protocol, it is based on [11] ISO OSI model (ISO/IEC 7498-1:1994) and is used by the connectors to establish communication between them in order to exchange data. In addition to connectors, there are some other relevant actors such as the identity provider, which oversees performing the security checks needed to ensure the identity of the participants in a data transaction.

4.3 IDSA Reference Architecture model

The Reference Architecture Model (RAM) is a set of rules that establish the way how data is managed. Such ruleset has the objective of preserving sovereignty over the data shared within/between dataspaces, ensuring that the owner never loses control. It is composed by several layers as shown in Figure 5 and described next:

- **Business Layer**: in charge of defining the roles of the participants.
- **Information Layer**: in charge of specifying the information model used.
- **Process Layer**: in charge of defining all the interactions within a DS.
- **Functional Layer**: in charge of defining functional requirements.
- **System Layer**: in charge of defining real architecture.

In addition to such layers, there are three transversal perspectives:

- **Security**: in charge of the security.
- **Governance**: in charge of defining the processes and roles of a DS.
- **Certification**: defining the need for a certification of participants.

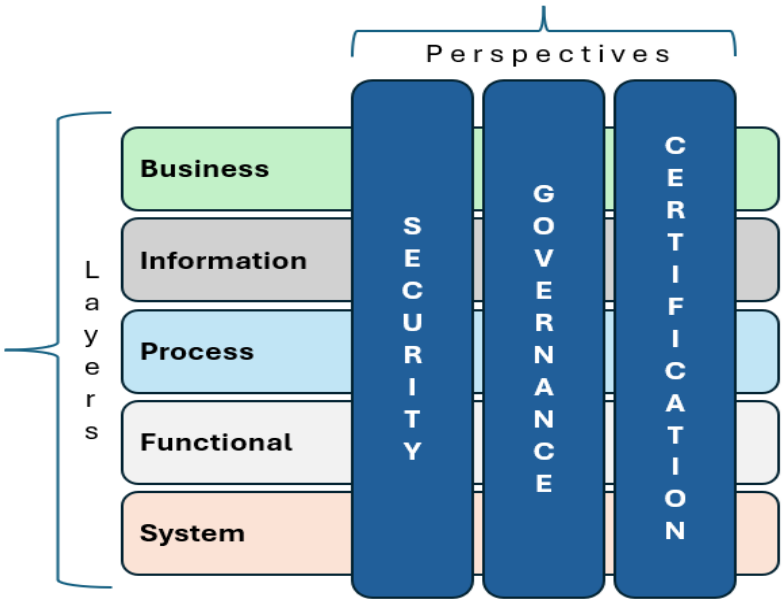

Figure 5: Reference Architecture Model, layers and perspectives

The current version of the architecture is RAM 4, but version 5 is being developed right now and, as soon as it becomes finished, it will improve policies, models, scalability, interoperability and protocols as requested by the community and based on IDSA' experience during developments.

4.4 Certification

Last but not least, IDSA implements a certification process based on rigorous standards such as **ISO 27001** and **IEC 62443**. Any company wishing to create its own connector or core component must go through this process in order to get the official certification that ensures that such components have the highest quality and adhere to all data space specifications (e.g. security, communication protocols, data model).

The process offers to applicants three levels of trust depending on their needs:

- **Trust level 1**: a trust level intended for low security cases with basic security.
- **Trust level 2 and 3**: each of these two levels offers increasingly more security through the use of containers, encryption, users monitoring. They can be considered the best option for high-end professionals and companies.

The certification is composed of the following roles:

- **Applicant**: the entity wishing to perform the certification process. It must cover all the costs of the process itself, including the evaluation facility and the certification body.
- **Evaluation facility**: the entity in charge of performing the evaluation of the applicant.
- **Certification body**: the entity in charge of supervising the evaluation process.

Once the applicant opts for one of the above-mentioned trust levels, they must go through the proper process consisting of the next steps:

- **Application phase**: this phase starts the evaluation and the certification.
- **Evaluation phase**: this phase evaluates the component or the applicant.
- **Certification phase**: in this phase, the evaluation is examined by the certification body and, in case of passing the evaluation, creates the certificate.

This process may vary slightly depending on the requested trust level, but remains mostly the same as shown in Figure 6:

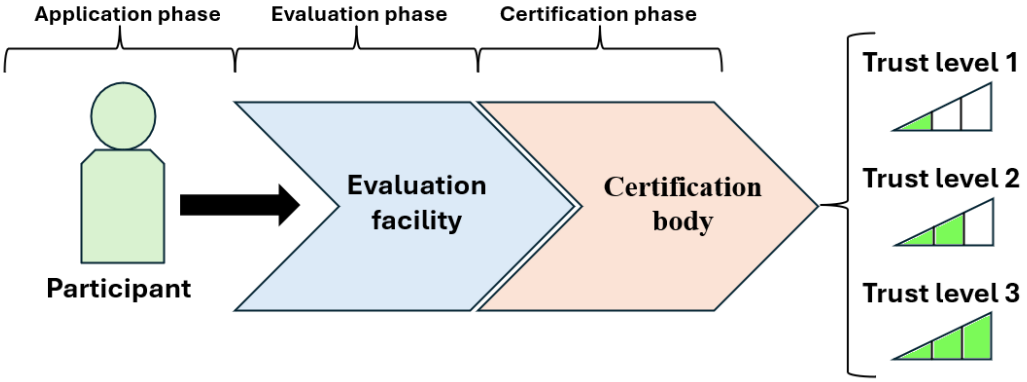

Figure 6: IDSA certification process.

5 ExPEDite Data Space Integration Suite

5.1 Description

IDSA, together with GAIA-X, are two of the main associations driving towards the creation, promotion and implementation in the European Union of data spaces, which as described in [12] IDSA's official website, can be defined as:

> *"a trusted and sovereign environment where organizations can share data securely and interoperably"*

Such description means the birth of a new paradigm in data managing and exchange in which companies can perform data trading without losing their sovereignty over them while accomplishing all security standards in industry. ExPEDite wishes to use such cutting-edge technology to be prepared for future data exchanges, which would mean a huge added value for the project and, in order to do so, has decided to integrate within its architecture a data space connector based on Sovity's components that will allow such connectivity.

The next sections of this deliverable describe all components forming part of such architecture and the working methodology to use and configure it.

5.2 Components

The ExPEDite infrastructure regarding data spaces is composed of the Keycloak & DAPS duo, the Authority Portal and the Data Space Connector itself, each of which is described in deep over the next sections.

5.2.1 Keycloak & DAPS

The first of the components that are part of ExPEDite's data space infrastructure is the tandem composed by Keycloak and the DAPS, which is in charge of the security of the data space by allowing two connectors to communicate with each other in a secure way.

In one hand, [13] Keycloak is one of the most important applications for managing the access to platforms. It has been developed by Red Hat under Apache License 2.0 and uses authentication protocols such as OAUTH, SAML and OpenID in order to manage users and roles. In this specific configuration, Keycloak acts as a base for the security management, allowing the use of clients and tokens.

In the other hand, the [14] DAPS (Dynamic Attribute Provisioning Service) is a Keycloak plugin created by Sovity under Apache License 2.0 that is in charge of managing identity in data spaces through the creation of clients and tokens to allow secure communication between connectors. The component comes usually in a bundle among with Keycloak in order to ease the access configuration. In case of two connectors willing to communicate with each other, one of them must act as a host, creating/storing all the clients and certificates which will be used for logging in.

Both components are key in Data space communication because, apart of the security itself, they allow trust in data spaces, which is a basic feature in that kind of environments.

5.2.2 Authority Portal

The authority portal (or DS Portal in most recent versions) is a component developed by Sovity which is in charge of managing, in a centralised way, the users who can access to a connector/data space. Its main objective is helping to create all the clients/certificates of the other connectors which may access to a specific data space, as shown in Figure 7.

It provides a user-friendly user interface (UI) that facilitates the creation of such users and their corresponding clients and certificates through a step-by-step wizard. It is an optional component, but using it is highly recommended, because it facilitates some difficult or long steps such as for example the certificate creation which, other way, would consume huge amounts of time.

The project has been developed by Sovity using Java technology for the backend part and TypeScript for the frontend and is released under AGPL v3.0 license.

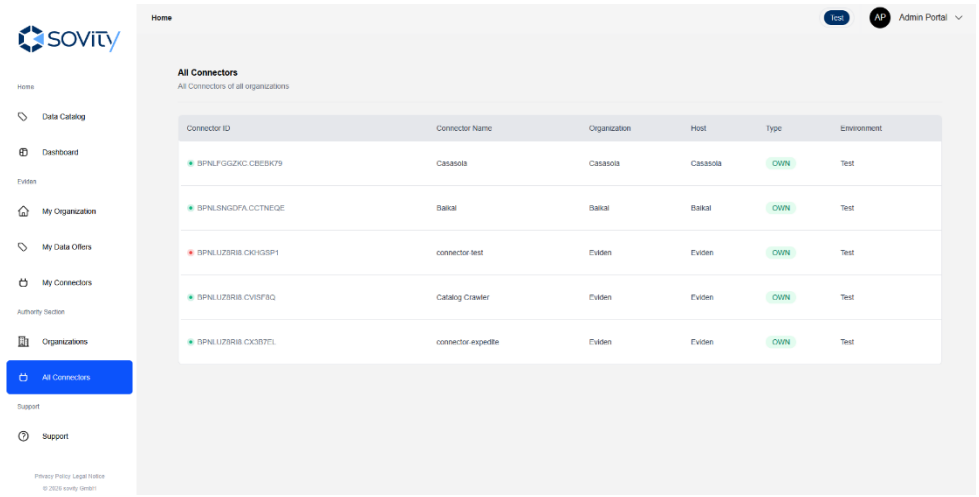

Figure 7: Authority Portal connectors client's section.

5.2.3 Data space connector

The Sovity connector is a software component developed by Sovity under Apache License v2.0 and based in the Eclipse Data Space Connector (EDC). It is the key piece in the data space infrastructure, as it allows the data exchange itself between all the participants in a data space in an interoperable way. The configuration used in ExPEDite makes it work in conjunction with the Authority portal and the Keycloak/DAPS in a smooth way, making it very easy-to-install. As described previously, the connector not only works as a plug making data exchange possible but ensures that the data offers are reachable by all data space participants and owners never lose sovereignty over it.

The connector also offers a user-friendly interface where users can search for data offers from other participants in the dataspace in order to acquire them and also allows them to create their own offers in order to sell data under their own premises.

5.3 Implementation

This section describes the ideal implementation of a data space connector deployment, focusing on an infrastructure perspective. Figure 8 shows the deployment of the three components described previously:

- Keycloak/DAPS.
- Authority portal.
- DS connector.

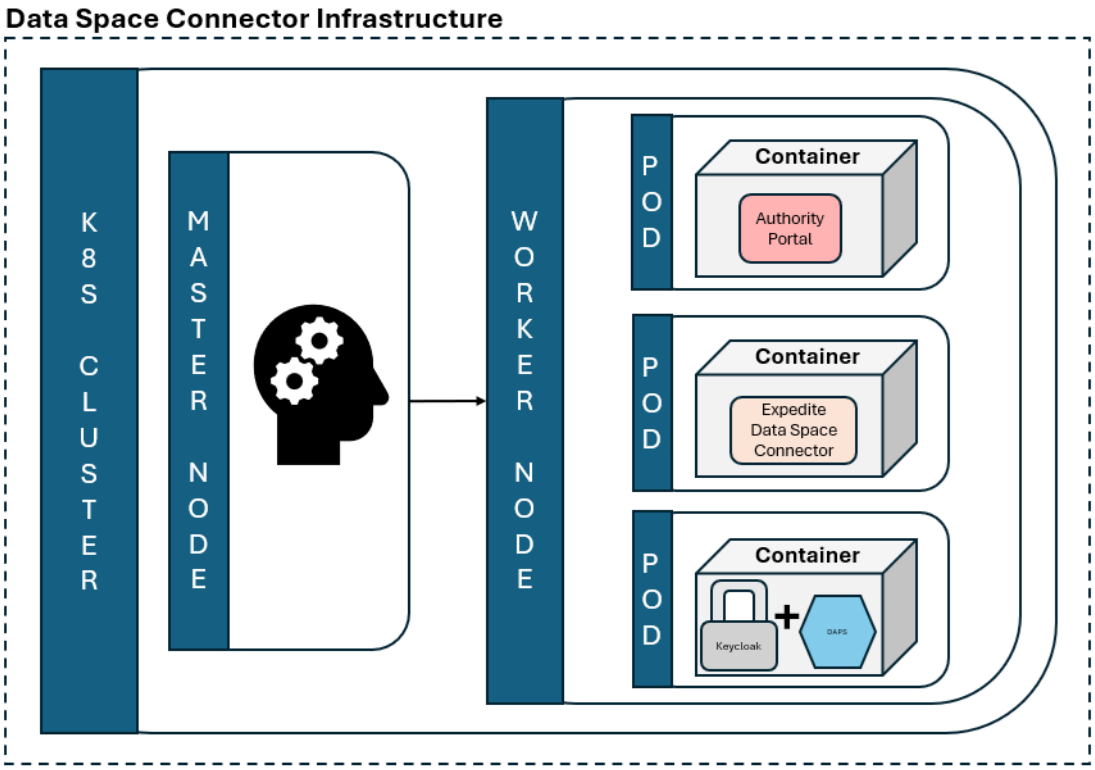

Figure 8: Data Space Connector infrastructure.

Such infrastructure should be deployed on a cluster using containerization technology based on Docker and Kubernetes (k8s), which would make it resilient to failure and totally secure against any security threats. Each of the components forming part of it is deployed inside of its own container which, at the same time, resides inside a Pod. Kubernetes watches such Pods actively and keeps them in a healthy state, performing all the corrections needed in case a failure happens and re-escalating the number of pods accordingly when the situation requires it, so the service never gets interrupted.

In the case of ExPEDite, the cluster physical machines used by Bull for such deployment are composed of a 16 cores CPU with AMD 64 architecture, 16 Gb of RAM memory and Kubernetes version 1.31.9.

5.4 Deployment and validation

This section defines the main data flows existing when using a data space connector through the description step-by-step of a use case in which one connector requires data from ExPEDite's connector. The overall data flows are shown in detail in Figure 9.

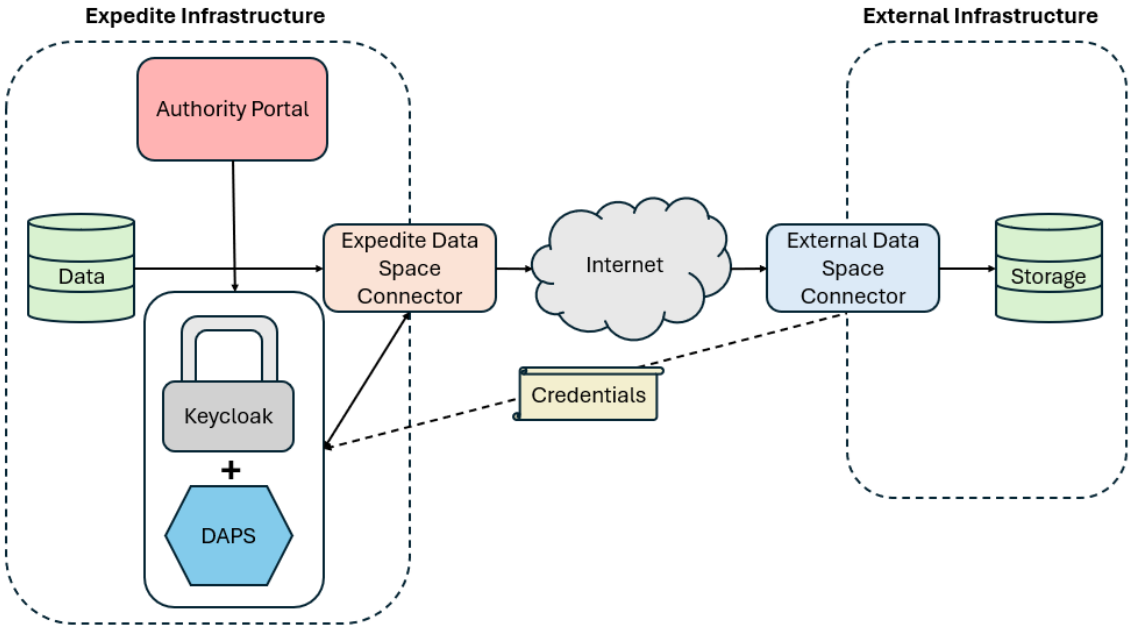

Figure 9: DS connectors infrastructure main data flows.

As indicated in Section 5.2.2, there is a previous step that needs to be performed in order to be able to exchange data between connectors, which consists in creating the client of the connector requiring the data among with its corresponding certificate in ExPEDite's Keycloak/DAPS through the use of the Authority Portal as shown in Figure 10, otherwise the connectors will not be able to see each other. The client creation using the Authority Portal is an easy and almost automated process consisting of a wizard and, as a result, will not be described in this deliverable. The next picture shows ExPEDite's Authority portal where such action must be performed.

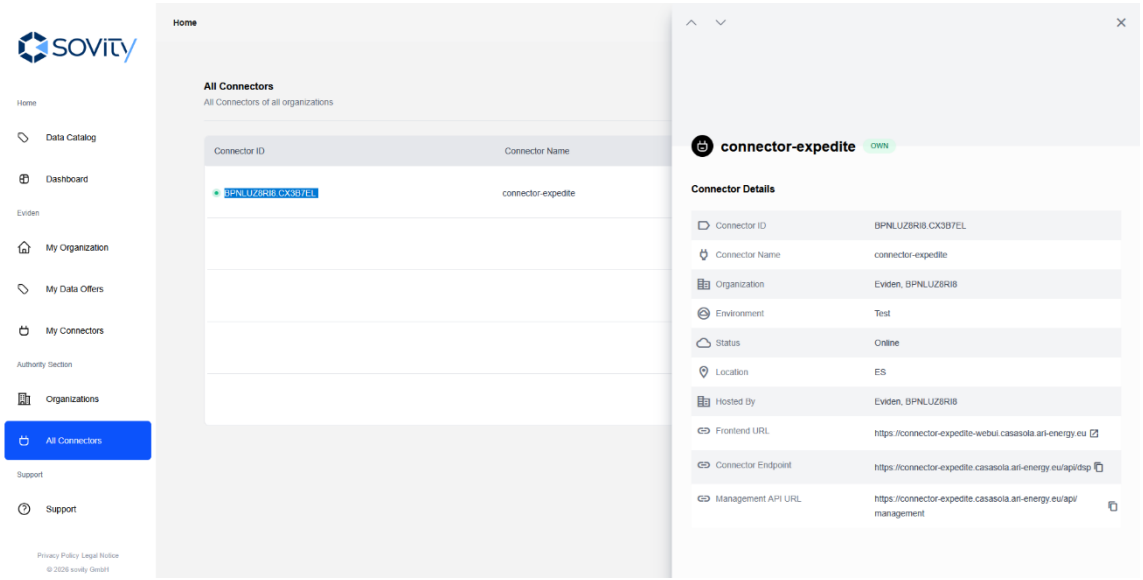

Figure 10: Authority Portal client creation.

Once the client has been created, the first step needed in order to get data from one connector to another consists in creating a data offer in ExPEDite's connector, so the data can be seen by other connectors forming part of the same data space. Figure 11 shows the data offer creation screen.

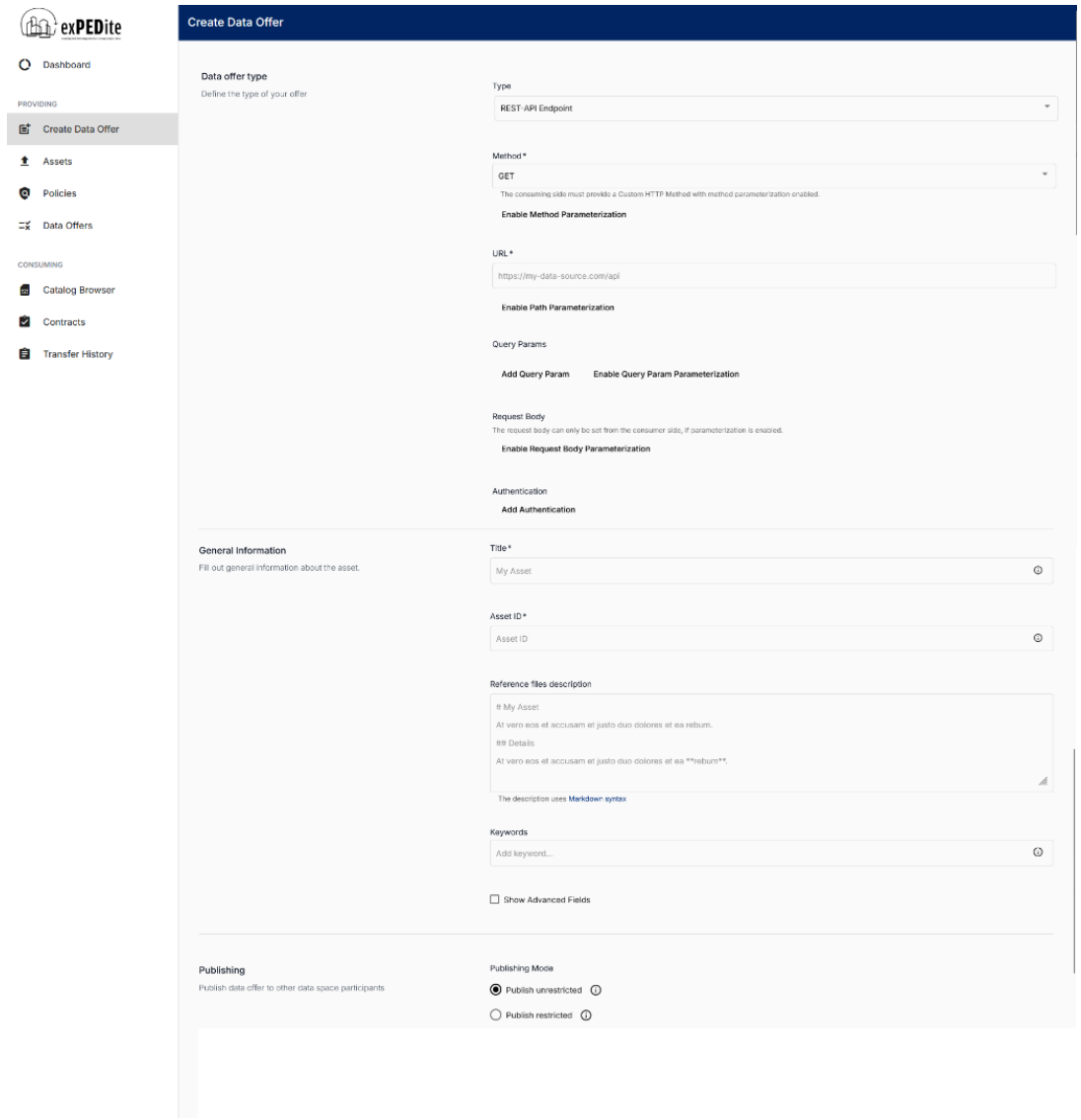

Figure 11: Data offer creation in ExPEDite's connector.

In such data offer, user must indicate a valid HTTPS URL where the data is hosted as well as other parameters, such as:

- **query params**: additional parameters added to retrieve data from the URL.
- **title**: a descriptive name for the data offer which will be used in the main screen.
- **description**: an overall description for the data offer, also used in the main screen.
- **asset ID**: a unique ID used to identify the offer.
- **keywords**: any number of keywords that can be used to perform advanced searches.
- **publication conditions**: indicates whether the data has any restrictive policy such as availability date range, price. Such policies can be created on demand in the corresponding "Policies" section.
- **authentication**: credentials needed to access to the URL which is hosting the data.

In the current example, the URL used as data origin is a public service which provides a string containing the "Lorem Ipsum" text. In a real-world example, a valid data origin such a database or service should be used.

As soon as the offer has been created, a corresponding data asset will appear in the assets section, as shown in Figure 12.

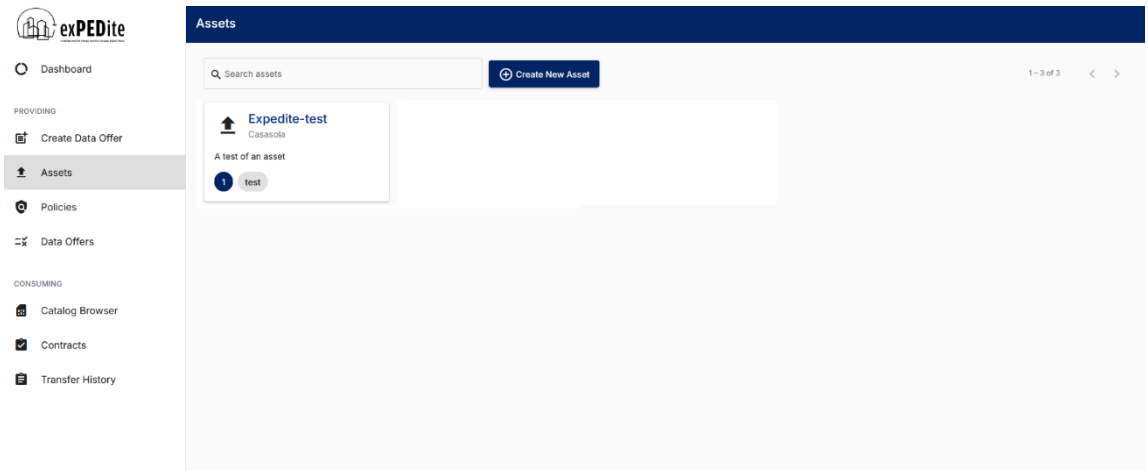

Figure 12: Available assets.

Once the asset is available to the data space under ExPEDite's premises, any connector forming part of such data space can search for it. In order to do so, users must introduce the endpoint URL of ExPEDite's connector in the "Connectors endpoint" section of the catalogue browser from his connector, as shown in Figure 13, so the assets from such connector are shown.

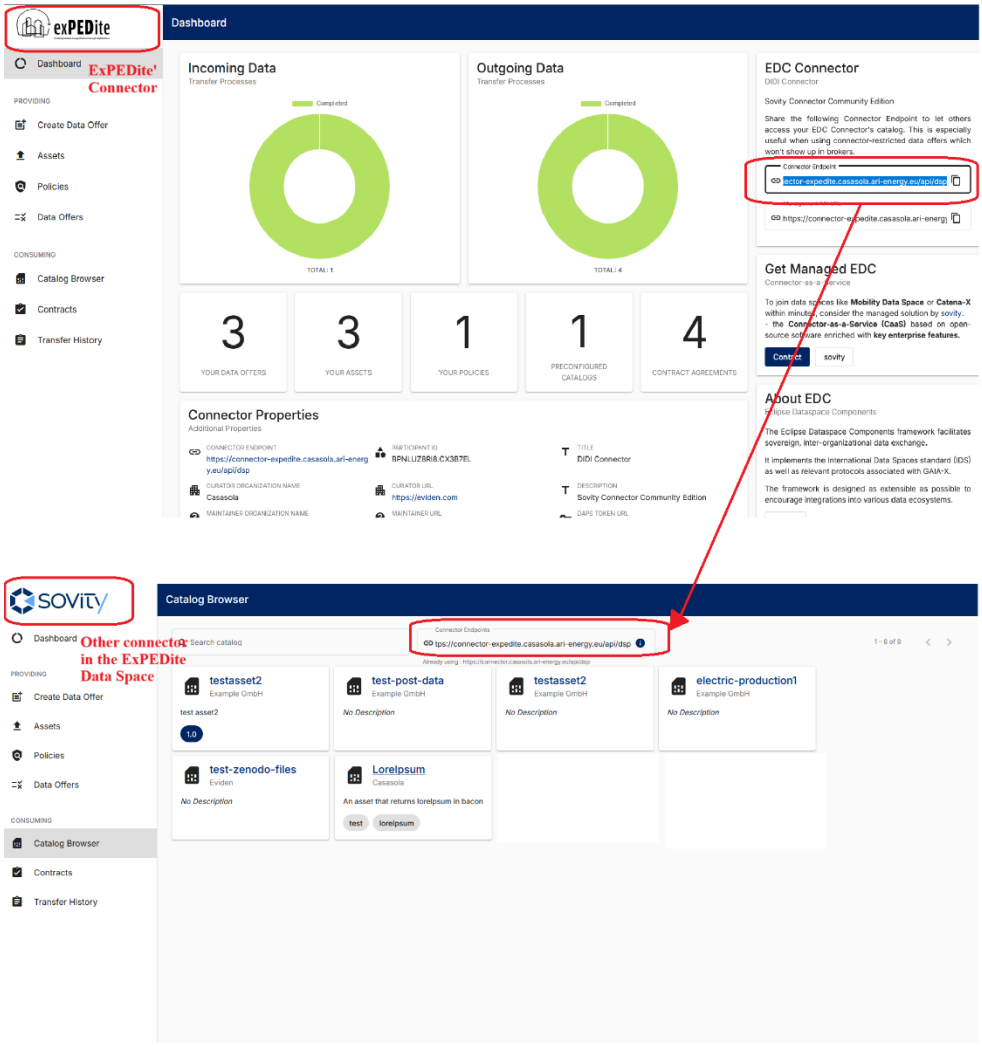

Figure 13: Search for assets from other connectors in the Data Space.

When the URL is introduced, the asset created in ExPEDite's connector should appear in the list of available assets of the catalogue as shown in Figure 14.

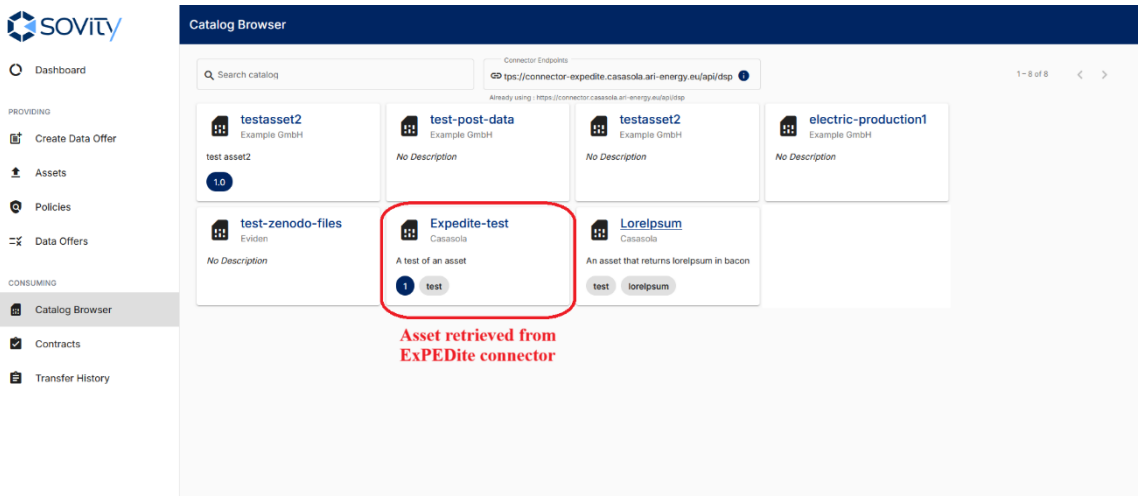

Figure 14: Assets retrieved from ExPEDite's connector.

Next, user should click on such asset to negotiate the conditions to acquire the data, as depicted in Figure 15.

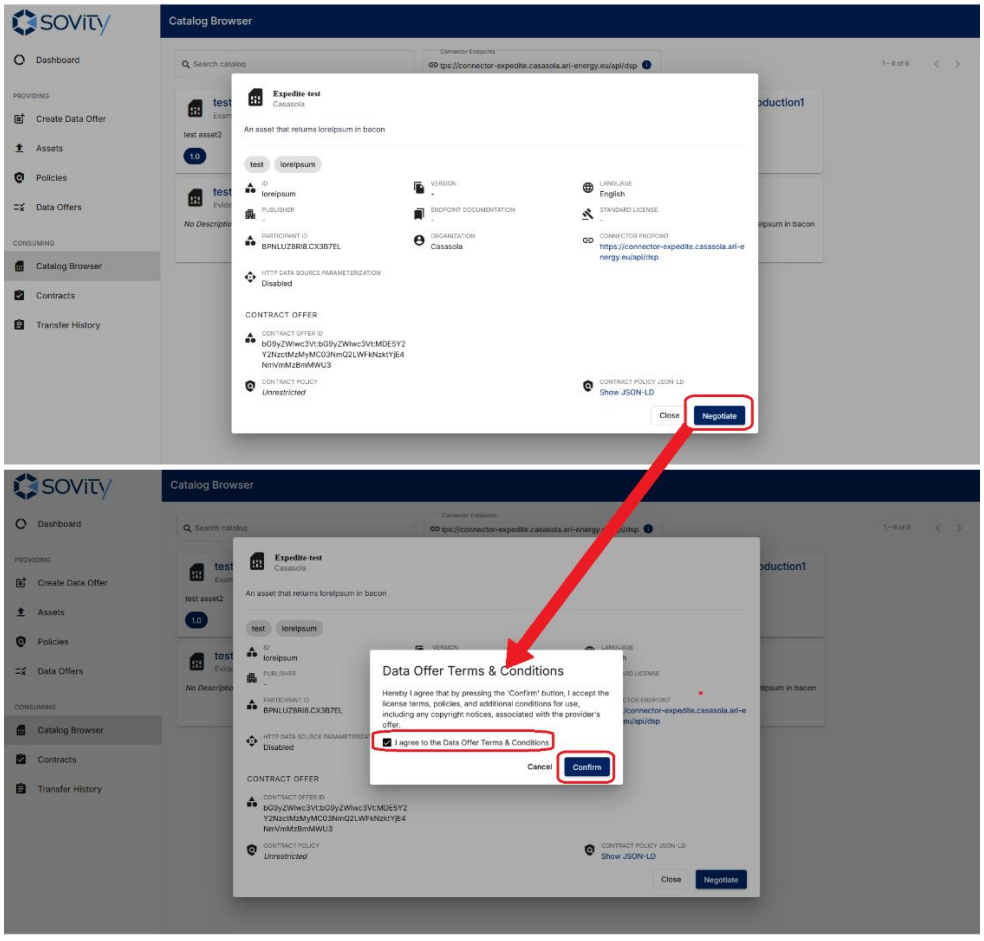

Figure 15: Contract negotiation.

In the current example, no restrictive policies were applied, but in case of existing and agreeing with them, the user should click on the checkbox “I agree with the data offer terms & conditions” and click on the “Confirm” button. As soon as the negotiation is confirmed, a contract is created in the corresponding section as shown in Figure 16.

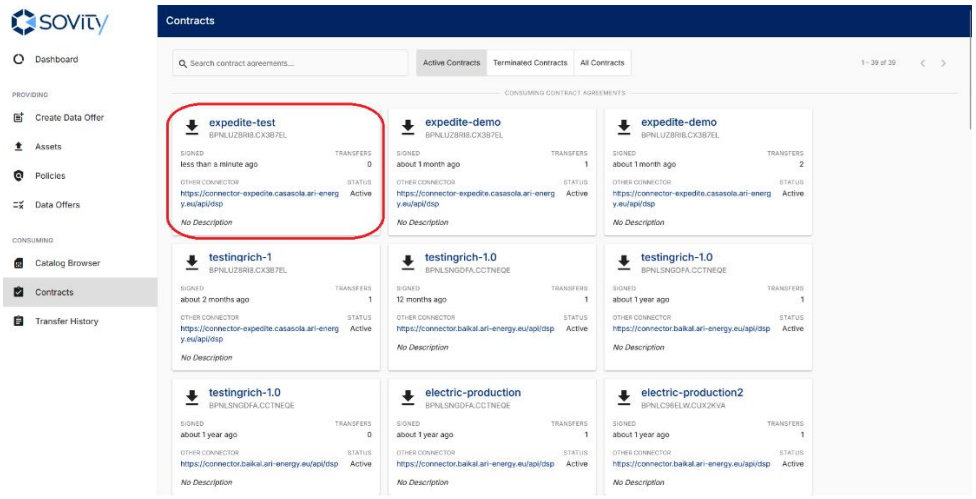

Figure 16: Infrastructure main fluxes.

Last but not least, the user should click on the contract, press the “Transfer” button, fill in the URL where data should be sent, the authentication and headers (if required) and finally press the “Initiate transfer” button as shown in Figure 17.

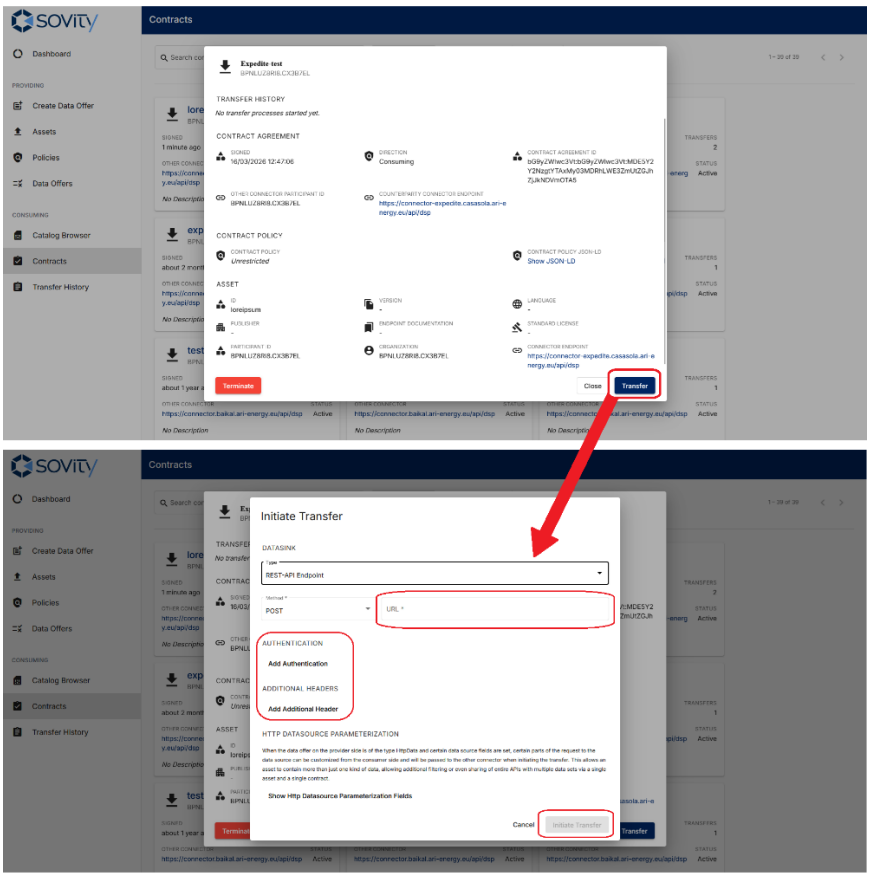

Figure 17: Initiate data transfer.

Finally, the data is sent to the URL specified in previous step. Such URL can be any type of storage, such a data lake or database, but in this example, a service provided by the webhook website, which offers a free service to receive HTTP requests, was used, as shown in Figure 18.

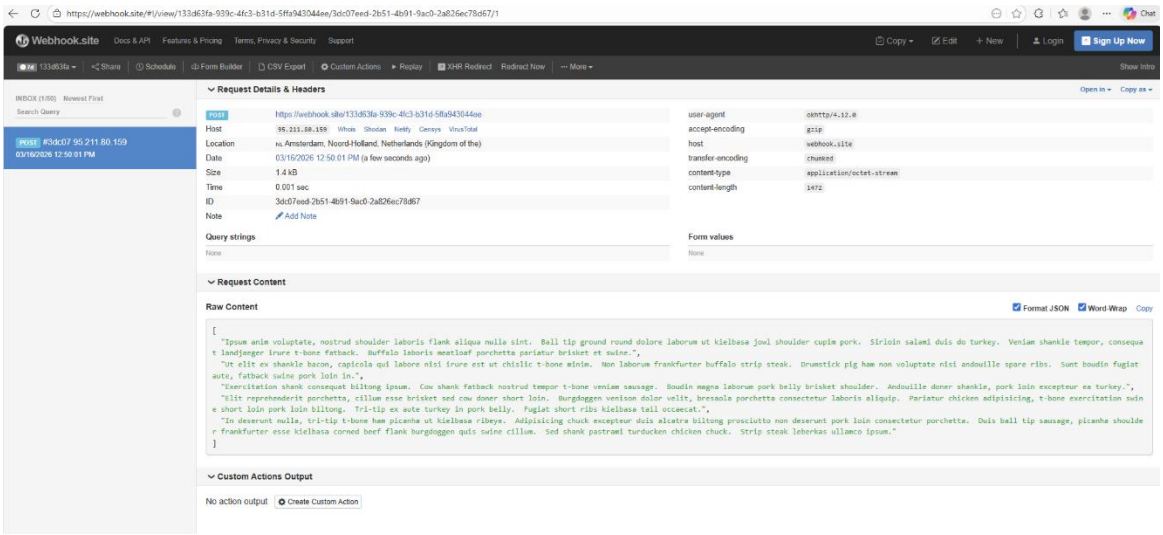

Figure 18: Data received in webhook website.

6 Conclusions

ExPEDite has created a cutting-edge infrastructure consisting of a digital twin with the objective of managing energy efficiency and distribution in the university district of Kipsala, in Riga (Latvia), as well as in adjacent areas. The software used in such infrastructure exploits the data obtained to optimize the efficiency of the system, getting as a result energy usage optimization. In early stages of the project, such data usage was originally limited to such end and, as a result, the project may have run into the risk of becoming an isolated data island where no further profit was obtained from the information gathered.

To avoid such limitation, ExPEDite decided to make a bet on the future and invest in Data Spaces, a revolutionary concept in which data is an asset that can be traded without losing the sovereignty over it while getting further profit. In order to do so, the project has implemented a data space connector; a piece of software in charge of connecting any infrastructure to a data space, acting as a plug and thus making possible to ExPEDite to extend its capabilities towards the future making it compatible with such technology.

Such addition gives the project an added value, aligning it with one of the most strategic objectives of the European Union: Data Sovereignty. As a result, the project infrastructure is prepared for any future interaction with this technology, making it able to exploit its data in further ways than originally expected.

7 References

[1] EU LDT Toolbox consortium, “EU LDT Toolbox,” [Online]. Available: https://interoperable-europe.ec.europa.eu/collection/ldttoolbox/welcomee. [Accessed 2026].

[2] Go Li.EU (Digital Europe, Grant Agreement No. 101083615), “Living-in.eu,” 2024. [Online]. Available: https://living-in.eu/groups/commitments/technical. [Accessed 2026].

[3] ExPEDite project (Horizon Europe, Grant Agreement No. 101139527), “ExPEDite-project,” 27 11 2025. [Online]. Available: https://expedite-project.eu/eu-ldt-toolbox-and-mim8-reinforcing-expedite-dt-platform/. [Accessed 2026].

[4] ETSI’s Technical Committee on Data Solutions (TC DATA) , “ETSI,” 2026. [Online]. Available: https://www.etsi.org/technical-groups/data/. [Accessed 2026].

[5] Smart Data Models (A collaborative program led by FIWARE Foundation, TMForum, IUDX, OASC), “Smart Data Models,” [Online]. Available: https://smartdatamodels.org/. [Accessed 2026].

[6] DS4SSC (Digital Europe Work Programme 2021-2022 under Grant Agreement No. 101123342), “DS4SSC,” [Online]. Available: https://www.ds4sscc.eu/ds4ped. [Accessed 2026].

[7] International Data Spaces Association, “IDS Information Model,” 2026. [Online]. Available: https://international-data-spaces-association.github.io/InformationModel/docs/index.html.

[8] International Data Spaces Association, “IDS Dataspace Protocol,” 2026. [Online]. Available: https://internationaldataspaces.org/offers/dataspace-protocol/.

[9] International Data Spaces Association, “Reference Architecture Model,” 2026. [Online]. Available: https://internationaldataspaces.org/offers/reference-architecture/.

[10] International Data Spaces Association, “IDSA certification process,” 2026. [Online]. Available: https://internationaldataspaces.org/offers/certification/.

[11] International Data Spaces Association, “ISO OSI model (ISO/IEC 7498-1:1994),” 2025. [Online]. Available: https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Position-Paper-Establishing-a-Unified-sovereign-and-open-digital-infrastructure.pdf. [Accessed 2026].

[12] International Data Spaces Association, “IDSA official website,” 2026. [Online]. Available: https://internationaldataspaces.org/why/data-spaces/.

[13] Cloud Native Computing Foundation, “Keycloak,” 2026. [Online]. Available: https://www.keycloak.org/.

[14] Sovity, “Github Sovity Dynamic Attributing Provissionning Service,” 2025. [Online]. Available: https://github.com/sovity/sovity-daps.