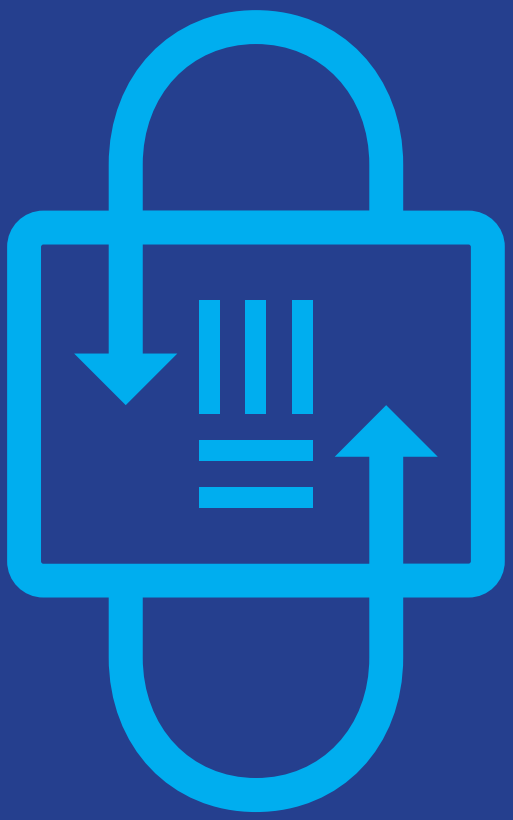
INTERNATIONAL DATA SPACES ASSOCIATION

Report | No 12 | February 2024

Data Connector Report



Publisher

International Data Spaces Association

Head office:
Emil-Figge-Str. 80
44227 Dortmund
Germany

Authors and contributors

Giulia Giussani,
International Data Spaces Association

Sebastian Steinbuss,
International Data Spaces Association

Mario Holesch,
International Data Spaces Association

Nora Gras,
International Data Spaces Association

We thank the maintainers of the data connectors for their contribution to this report.

Cite as

Giussani G., Steinbuss S., Data Connector Report, International Data Spaces Association, (2), February 2024
https://doi.org/10.5281/zenodo.7405406

Table of Content

What's new?

Added

- 2.1.19 Tekniker IDS Connector

Changed

- Figure 3 Overview of connectors with up-to-date information
- 2.1.13 Mitsubishi Electric Dataspace Connector
- 2.1.26 VTT DSIL Connector
- 5 Conclusion
- Figure 5 Data connector development streams
- Figure 6 Number of connector variants

Removed

- None

1 Introduction

1.1 The data connector report

The data connector report is a key monthly publication from IDSA aiming to bring clarification around the topic of data connectors.

In particular, the connector report:

- highlights the importance of data connectors, explaining what they are and why they are a key element in data spaces.
- It describes the main four typologies of connectors (data connector frameworks, open-source generic solutions, proprietary generic solutions and off-the-shelf data connectors or connectors integrated in data-related products).
- It provides a summary of all the necessary requirements to make data connectors interoperable (e.g. relying on standards, having clear specifications, enabling semantic interoperability via the Data Catalog Vocabulary (DCAT) and specific vocabularies, etc) and it highlights the importance of having a protocol agnostic standard, which IDSA is in the process of creating.
- It gives visibility to existing connector implementations, it provides details about them (e.g. license type, maturity, adoption cases,...) and follows their evolution over time.
- It wants to be the reference point for learning and fostering interoperability in data sharing ecosystems. Therefore, it provides and overview of additional existing approaches that enable data sharing in data-driven business ecosystems, with the ambition of fostering interoperability and future alignment with IDS.
- It also lists additional technologies (e.g. Gaia-X trust framework, iShare, SOLID,...) that are contributing in different ways to achieve trustworthy data sharing in data spaces.

To provide feedback on the connector report, to add a connector to the list, to update the information on an already-listed connector or to suggest the inclusion of additional existing technologies or emerging technologies, please reach out to IDSA via this form[1]:.

Please note that the connector report aims to focus on the above-listed topics, therefore details on IDS use cases or deployment scenarios are not in scope. For a deep dive into those topics, please refer to some complementary IDSA resources:

- Regarding the topic of use cases:
    - Please refer to the Data Spaces Radar[2] . This recent version of Data Spaces Radar has been launched in January 2024. It is an interactive tool created by IDSA in the context of the Data Spaces Support Center (DSSC)[3] to offer an overview and quick information on several data spaces initiative and use cases, highlighting their different implementation stages, domains and providing several additional details.

[1] https://forms.office.com/e/kvtbvh2VRu
[2] https://www.dataspaces-radar.org/radar/
[3] https://dssc.eu/

  - More details on the use cases based on IDS are regularly described in the Radar Brochure (released quarterly). You can download the most recent version on the IDSA Website[4]

- To know more about how IDS components have been implemented and combined, please refer to the Deployment Scenarios on the IDSA GitHub[5] (i.e. technical descriptions of how a component or a set of components has been deployed and which steps have been followed). In the Deployment Scenario repository on GitHub, you will be able to find more information on the exact definition of a Deployment Scenario, you will find the list of the existing ones, and you will also be able to submit a request to add a deployment scenario, in case you would like to give visibility to some of your implementation work. For a more user-friendly reading mode, the content on GitHub is also published in the IDS Knowledge Base[6]

1.2 Why do we need data connectors?

We need data connectors to share data - because connectors enable secure and effective communication and exchange in data spaces. They are a tool to connect many data endpoints to increase the pool of available data and to accelerate the data economy. By linking data connectors, data spaces become protected environments where participants can freely share data. Data sovereignty, transparency and fairness are ensured by adherence to a set of rules. data connectors act as nodes in a data space and provide data sovereignty by design. This report focuses on data connectors for data spaces.

Sharing and exchanging data is not a new thing, but the requirements for it are evolving. A data connector essentially realizes two relevant aspects: It provides Data Exchange Services that are (1) the Application Programming Interface (API) to other participants in a data space to achieve interoperability and (2) the trustworthy component to handle data by implementing policy enforcement mechanisms and a common baseline for cybersecurity. However, as data can be different and the requirements for data sharing can be different as well, variants of connectors are needed (see the IDS RAM section 2.2[7] and section 2.4[8] for more information). This report provides an overview of these data connectors, their purpose, use and distinctions.

The figure below shows the diversity of requirements in industrial ecosystems. A data connector for (I)IoT devices may have substantially different requirements (in terms of resource consumption, efficiency, and cyber security), then a connector of a data marketplace or an industrial cloud platform. At the same time, such services must seamlessly integrate open data. A data connector will enable interoperability and will put data to use, to link it with other data and to support modern concepts such as (shared and distributed) digital twins, AI, or federated learning. To do so, the connectors realize archetypical patterns for management service, orchestrate cloud-based service, lightweight API gateways, or IoT gateways. They may use concepts like distributed ledgers, but they will rely on state-of-the-art data management capabilities.

[4] https://internationaldataspaces.org/publications/most-important-documents/
[5] https://github.com/International-Data-Spaces-Association/IDS-Deployment-Scenarios
[6] https://docs.internationaldataspaces.org/ids-knowledgebase/v/ids-deployment-scenarios
[7] https://docs.internationaldataspaces.org/ids-ram-4/context-of-the-international-data-spaces/2_1_data-driven-business_ecosystems/2_2_data_sovereignty_as_a_key_capability
[8] https://docs.internationaldataspaces.org/ids-ram-4/context-of-the-international-data-spaces/2_1_data-driven-business_ecosystems/2_4_data_exchange_and_data_sharing

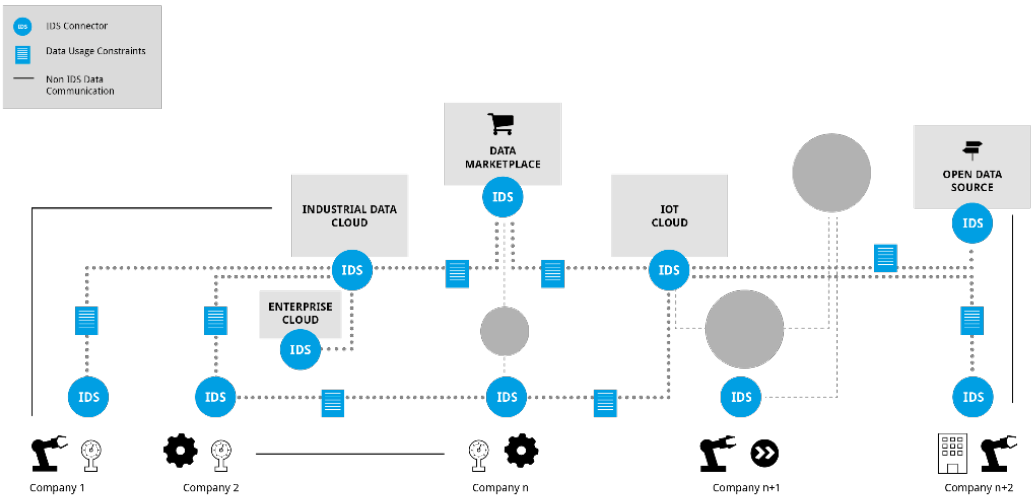


Figure 1 International data spaces connecting different clouds, on-premises applications, devices, marketplaces, and open data in an industrial scenario.

While the requirements for data sovereignty, i.e., the ability to express and enforce the rights and obligations the usage policies, are different in such scenarios, a need for basic interoperability is fundamental for data connectors to build interoperable data spaces.

1.3 What is a data connector?

Data connectors are essential for enabling trust and interoperability in data sharing and exchange within data spaces, which are designed to provide data sovereignty. Data spaces, and with that, data sovereignty will be the level playing field on a global scale. This represents a significant advantage and revolutionizes the data economy of the future – with the goal of benefiting society, businesses, and individuals.

New data spaces may have different implementations and standards, which can lead to the creation of new data silos. Therefore, a strong push for convergence is needed to enable interoperability, data continuity, and common governance models that support data sovereignty for all data spaces. The IDSA Rulebook[9] provides an overview on the functional requirements of a data space, the fundamental structure and introduces the mandatory and optional functionalities of a data space.

The International Data Spaces Association's (IDSA) core role is developing and maintaining a reference architecture for data sharing and exchange that prioritizes data sovereignty in data-driven business ecosystems. The IDSA has created a global standard and a reference architecture model (RAM)[10] that facilitates secure and self-determined data sharing between trusted parties across various ecosystems.

Certified users gain access to the data ecosystem and attach usage restriction policies to their data before making it available to other users. The IDS Connector is a central component of

[9] https://docs.internationaldataspaces.org/idsa-rulebook
[10] https://docs.internationaldataspaces.org/ids-ram-4/introduction/1_1_goals_of_the_international_data_spaces

the IDS standard and enables data exchange services as described in the IDS-RAM section 3.5.2[11] (see also figure below). It uses container technology to ensure "trusted execution", which means that the data within the container is always protected from unauthorized access and manipulation. As interoperability is crucial for data connectors in data spaces, the implementation of the Dataspace Protocol[12] is mandatory for data connectors and will be subject to IDS Certification, once the Version 1.0 of the Dataspace Protocol is available.

The IDS standard addresses technical, operational, and legal agreements in data spaces[13], which combine technical, organizational, and legal complexities. It provides guidelines for data sharing and adds features such as identity management, communication security, and usage control. The IDS Connector is defined in DIN SPEC 27070 as part of the German standardization work and subject to international standardization in ISO/IEC, CEN/CENELEC, IEEE, and W3C.

To prove compliance with these requirements the IDS Certification[14] was launched in 2022, offering different trust and assurance levels for both connectors and operational environments. Some connectors are labelled as 'IDS-Ready' indicating they successfully underwent a pre-certification, a third-party assessment to prepare for certification.

Implementations of data connectors based on the IDS Standard can be found as closed-source software and as open-source software. Regarding the latter, The IDSA has developed the IDS Graduation Scheme[15], which provides a set of rules, processes, and criteria to manage these open-source implementations on the IDSA GitHub [16].

[11] https://docs.internationaldataspaces.org/ids-ram-4/layers-of-the-reference-architecture-model/3-layers-of-the-reference-architecture-model/3_5_0_system_layer/3_5_2_ids_connector#ids-connector-functionalities
[12] https://docs.internationaldataspaces.org/dataspace-protocol
[13] https://internationaldataspaces.org/rule-book-on-structures-and-processes-for-implementing-ids-in-the-real-world/
[14] https://internationaldataspaces.org/use/certification/
[15] https://github.com/International-Data-Spaces-Association/idsa/tree/main/graduation_scheme
[16] International-Data-Spaces-Association/idsa: This is the main repository of International Data Spaces Association on GitHub, where you can find general overview and useful information on IDS Landscape.

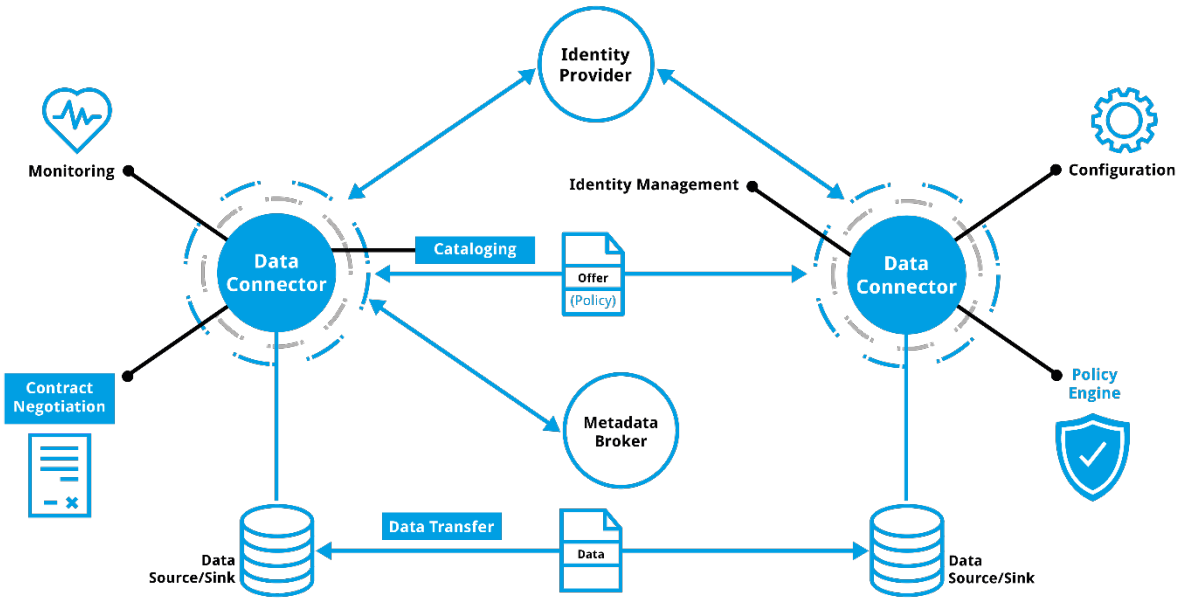


Figure 2 Data Exchange Services realized by a data connector as described in the IDS-RAM section 3.5.2

1.4 Interoperability of data connectors

Technical Interoperability is a major requirement in data spaces. It should be realized by data connectors, based on specifications and standards rather than relying on singular implementations or reference implementations. To do that, multiple levels of interoperability must be addressed: first, the general interaction between the connectors for the description of data assets and the related endpoints must be addressed including the definition of policies for access control and usage control, followed by the negotiation of those policies and contracts. The initiation and management of the data exchange process needs a clear specification, which can be mapped then to tangible protocols, like https, MQTT, web sockets or others. This is the handover to use case specific, domain-specific or ecosystem-specific definitions and standards. General interactions require a robust standard that can be implemented by the different connectors, while the subsequent data exchange makes use of domain or use case-specific standards. The same applies to semantic interoperability, which can be achieved on the foundation of the Data Catalog Vocabulary (DCAT)[17]. The further definition of the data exchanged is handled by semantic models, taxonomies, schemas or other similar mechanisms, the so-called “vocabularies”.

To achieve robustness and reliability in a data space, the interoperability of connectors requires verification. Based on standards and specifications, compliance to those can and must be continuously evaluated to maintain this foundation in addition to the continuous management and verification of security aspects related to the data connectors.

Today we already have a set of usable standards to achieve the goals described above, but additional standards are required. The interaction of the connectors on the general level as depicted in Figure 2 requires a protocol agnostic standard as foundation for interoperable data spaces. For this reason, IDSA is working on a specific Dataspace Protocol, a set of

[17] https://www.w3.org/TR/vocab-dcat-3/

specifications designed to facilitate interoperable data sharing between entities governed by usage control and based on Web technologies. These specifications define the schemas and protocols required for entities to publish data, negotiate usage agreements, and access data as part of a federation of technical systems termed a data space. The Dataspace Protocol, therefore, represents the foundation for technical interoperability in data spaces. Every data connector to be used in a Data Space must implement the Dataspace Protocol. More information on the Dataspace Protocol is provided on GitHub[18].

1.5 The relation of data connector solutions and frameworks

Data connectors differ based on various dimensions. They can nonetheless be grouped into four main categories: data connector frameworks, open-source generic solutions, proprietary generic solutions and off-the-shelf data connectors or connectors integrated in data-related products. More details on each of them are provided below.

Data connector frameworks are modular data space components to be used as a basis to implement a data connector. Most of the data connector frameworks are available as Free and Open-Source Software (FOSS). Based on this common foundation, extensions are available and being developed to create solutions. The Eclipse Data Space components, the FIWARE ecosystem including the TRUE Connector and the IDS Messaging Library are good examples of such frameworks. The frameworks are for developers that use it to implement their solutions. They are not intended for direct use of end-users to share and consume data.

Generic open-source solutions offer data connectors that can be integrated directly into an IT-Landscape and connected to services. Often, these act as proxies or gateways to companies' IT-Services. Configuring the components and adding custom extensions is typically required to share and consume data. The Data Space Connector and the TNO Secure Gateway are good examples of such connectors. Some connectors mentioned later in this report build on and extend generic open-source solutions to provide additional generic open-source solutions or proprietary software.

Generic solutions are provided by companies and organizations as proprietary software for generic usage. Like the open-source solutions described above, they cannot be used directly for sharing and consuming data, but need additional configuration and extension, such as the nicos GAIAboX.

Data connectors are off-the-shelf solutions that are provided as a service or as a directly usable connector solution without requiring any development activities to consume and share data. Nevertheless, configuration and adaption to the companies IT-Services is still needed, but with minimal effort, such as the connector as a service offering by sovity. In extension to such data connector offerings, this report also includes data connectors that are already integrated in data-related products, like the Data Intelligence Hub and the Tech2B Connector.

[18] Github: https://docs.internationaldataspaces.org/dataspace-protocol/overview/readme.

2 Implementations of data connectors

This section brings clarity on implementations of IDS data connectors. First of all, it provides a clear structure on how connectors can be described; secondly, it offers an overview of some of the existing data connectors; and lastly, it dives deeper into a detailed description for each connector in the overview.

Please note that the overview is not exhaustive, and it will be regularly updated by IDSA to document progress and new developments.

To provide a clear mapping of existing connectors, an effective structure of the information is necessary. For this reason, some existing scientific work and, specifically, the following paper: Gieß, A., Hupperz, M., Schoormann, T., Möller, F. (2024): What Does it Take to Connect? Unveiling Characteristics of Data Space Connectors. In Proceedings of the 57th Hawaii International Conference on System Sciences (HICSS), Honolulu, Hawaii, USA[19]. The paper has been leveraged to create a new ad-hoc structure to collect and report detailed information on each connector. This maps both general information on the connector and its adoption (e.g. name, maintainer, short description, example of applications of the connector...) going deeper into technical features (e.g. deployment options, protocol supported, integration with other components...). Please note that to facilitate the description of some features, some options are provided, but do not aim to be exhaustive and additional options may be added in the future.

The structure based on which each connector can be described, is explained here below.

- *Connector Overview*
  - Name of the connector
  - Maintainer (company name)
  - Peculiarity of the connector, i.e. short description, describing Unique Selling Point and/or main field of application of the connector (for example: cloud, IoT,..)
  - More information (e.g. links for further deep-dive)
- *Connector Details*
  - Type of connector, based on the description on paragraph 1.5 , i.e.:
    - A data connector framework (i.e. modular data space components to be used as a basis to implement a data connector)
    - A generic open-source solutions (i.e. data connectors that can be integrated directly into an IT-Landscape and connected to services, often acting as proxies or gateways to companies' IT-Services)
    - A generic solutions software (proprietary generic solutions)
    - An off-the-shelf solution, provided as a service
    - An off-the-shelf solution, directly usable integrated in data-related products

[19] https://www.researchgate.net/publication/374169204_What_Does_it_Take_to_Connect_Unveiling_Characteristics_of_Data_Space_Connectors

  - Maturity of the connector. The maturity level can be described with different indicators based of your preference. Examples of indicators are the levels of the IDS Graduation Scheme20, IDS Certification[21], TRL;
  - Portability, i.e. existing dependencies to the environment:
    - Agnostic (e.g. platform agnostic: the connector can be hosted on various cloud environments)
    - Specific (e.g. operating-system specific, e.g. only Linux)
  - License type, i.e. availability of the code:
    - Open source (i.e. without restrictions, e.g., Apache 2.0)
    - Open source - copyleft (i.e., free, but requiring that all modified and extended versions of the program also be free)
    - Closed source - extendable (i.e., extensions permitted)
    - Closed source (i.e., source text is not publicly viewable)
  - IDS Certification
  - Adoption examples i.e. existing cases of applications of the connector, to give visibility to the projects where the connector is implemented.
- Deployment options, i.e. for example:
  - Edge (e.g., manufacturing units, smartphones)
  - On-premises (e.g., local server)
  - Cloud (e.g., Microsoft Azure, AWS)
  - IoT/CPS/OT devices
- Service level, i.e. effort required to deploy a connector
  - Connector as a service (i.e., SAAS, plug-and-play solution)
  - Platform as a service (i.e., configuration)
  - Self-service (i.e. all self-made, e.g. by using an established framework like EDC)
- *Access and usage control*
  - Access control, i.e. how the interception of data processing and prohibition of data access is managed
    - OAuth (Open authorization, standard/framework for REST/APIs)
    - Basic auth (Basic access authorization, providing username and password)
    - API key (Manage access through a unique code for programming interface)
  - Usage control, i.e. technical enforcement of usage restrictions. More info on data usage control is provided in the IDSA Position Paper “Data Usage Control in IDS”[22].
  - Types of policies supported (If usage control is ensured). This information must be based on the IDS policy classes. More information on the IDSA GitHub[23].
- *Communication*

[20] https://github.com/International-Data-Spaces-Association/idsa/tree/main/graduation_scheme
[21] https://internationaldataspaces.org/offers/certification/; TRL: https://www.nasa.gov/directorates/heo/scan/engineering/technology/technology_readiness_level
[22] https://internationaldataspaces.org/data-sovereignty-updated-position-paper-on-data-usage-control-in-the-ids/
[23] https://github.com/International-Data-Spaces-Association/IDS-G/tree/main/UsageControl/Contract#policy-classes

  - Communication protocol, i.e. how is the connection between two electronic devices for data exchange enabled?
    - IDS Multipart
    - IDS protocol (IDSCP)
    - IDS-REST
    - Dataspace protocol (HTTPS)
    - Dataspace Protocol (other binding)
  - Transfer protocol, i.e. how the data from different databases is indexed and retrieved. More information in the IDS-RAM section 3.4.4[24]
    - In-band with determined protocol bindings
    - In-band with not determined protocol bindings
    - Out-of-band utilizing data planes without determined protocol bindings (data planes to be added)
    - Out-of-band utilizing data planes with protocol bindings (data planes are part of the connector offering)
- *Graphical user interface*, i.e. any GUI of computer systems facilitating operation
  - No (i.e. the connector can only be used via command line or operator needs to develop their own GUI)
  - Graphical user interface for users
  - Graphical user interface for management
  - Graphical user interface for administration
- *Identity management*, i.e. Participant information based on organizational assessment
  - Centralized (X.509)
  - Decentralized (did:web)
  - Decentralized (SSI)
  - None
- *IDS Information Model* and, in case, version supported. More information on the IDSA GitHub[25]
- *Vocabulary supported*, e.g. a domain specific vocabulary
- *Integration with additional components* and, in case, version supported:
  - Catalogue / Broker
  - Clearing House

IDSA is constantly collecting and updating information on various connector implementations. This version of the Connector Report offers a detailed updated description of 26 connectors, based on the above-mentioned structure, which was provided by the maintainers after August 2023. In addition, five other connectors are also listed in 2.2 Connectors with latest updates in May 2023, based on information provided in May 2023 or before. In total, 31 connectors are described in this Report.

[24] https://docs.internationaldataspaces.org/ids-knowledgebase/v/ids-ram-4/layers-of-the-reference-architecture-model/3-layers-of-the-reference-architecture-model/3_4_process_layer/3_4_4_exchanging_data
[25] https://github.com/International-Data-Spaces-Association/InformationModel

2.1 Connectors with up-to-date information

This paragraph provides detailed information on 26 connectors which have been described based on the structure defined in 2 Implementations of data connectors. The information was provided after August 2023.

An overview of the connectors is provided in Figure 3 Overview of connectors with up-to-date information. All details are described in the course of this chapter.

Connectors with up-to-date information

Section	Name of connector	Maintainer	Open source	IDS certified	Identity management	Deployment options	Service level
2.1.1	AI.SOV Connector	Cefriel				• Edge • On-premises • Cloud	Platform-aaS
2.1.2	Boot-X Connector	HUAWEI					Connector-aaS
2.1.3	ECI IDS Connector powered by TNO	eci Gatewise			X.509	Cloud	• Connector-aaS • Self-service
2.1.4	Eclipse Dataspace Components (EDC)		✓			Not specified	Service level is best effort of the open-source-community
2.1.5	EdgeDS Connector	INTRACOM TELECOM	✓			• Edge • On-premises • Cloud • IoT/CPS/OT	Connector-aaS
2.1.6	EGI Datahub Connector	egi	✓		X.509	• On-premises • Cloud	Platform-aaS
2.1.7	FIWARE Data Space Connector	FIWARE FOUNDATION	✓		X.509	• On-premises • Cloud	• Connector-aaS • Self-service
2.1.8	GATE Dataspace Connector	GATE	✓		X.509	On-premises	Platform-aaS
2.1.9	GDSO Connector - Tyre Information Service	GDSO	Partially		AWS Cognito	• Edge • On-premises • Cloud • IoT/CPS/OT	Platform-aaS
2.1.10	HEALTH-X dataLOFT EDC	Fraunhofer ISST			SSI	• On-premises • Cloud	Self-service
2.1.11	IIOC (Intel IONOS Orbiter Connector)	truzzt	✓		SSI	• Cloud • IoT/CPS/OT	
2.1.12	Kharon IDS Connector	HOLONIX			Kharon	• Edge • Cloud	• Connector-aaS • Platform-aaS
2.1.13	Mitsubishi Dataspace Connector	MITSUBISHI ELECTRIC	Partially			IoT/CPS/OT	Serf-service
2.1.14	OneNet Connector	ENGINEERING	✓		X.509	On-premises	Connector aaS
2.1.15	Silicon Economy EDC	Fraunhofer ISST	✓			• Edge • On-premises • Cloud • IoT/CPS/OT	Self- service
2.1.16	sovity CaaS (Connector-as-a-Service)	SOVITY			• X.509 • did:web • SSI	• On-premises • Cloud • Others	Connector aaS
2.1.17	sovity Open-Source EDC Connector	SOVITY	✓		• X.509 • Mock IAM	• On-premises • Cloud • Others	Self-Hosted
2.1.18	Tech2B SCSN Connector	TECH2B			did:web	Cloud	
2.1.19	Tekniker IDS Connector	Tekniker			SSI (planned)	• On-premises • Cloud	Connector-aaS
2.1.20	Telekom DIH Connector	T Systems		✓	• X.509 • did:web	• On-premises • Cloud	Connector-aaS
2.1.21	TNO Security Gateway (TSG)	TNO	✓		X.509	Cloud	Self-service
2.1.22	Tritom Enteprise Connector	Tritom				• On-premises • Cloud	Platform aaS
2.1.23	TRUE Connector	ENGINEERING	✓		X.509	• Edge • On-premises • Cloud • IoT/CPS/OT	• Connector-aaS • Platform-aaS • Self- service
2.1.24	Trusted Connector	Fraunhofer AISEC	✓		X.509	• Edge • On-premises • Cloud	Platform aaS
2.1.25	Trusted Supplier Connector (TSC)					• Edge • On-premises • Cloud	• Connector-aaS • Platform-aaS • Self- service
2.1.26	VTT DSIL Connector	VTT		✓	X.509	• On-premises • Cloud	• Connector-aaS • Platform-aaS

Figure 3 Overview of connectors with up-to-date information

2.1.1 AI.SOV Connector

Connector Overview	
Name	AI.SOV Connector
Logo of the connector or company logo	Cefriel POLITECNICO DI MILANO
Maintainer	Cefriel
Peculiarity of the connector	The AI.SOV connector is built upon the Fraunhofer open connector plus a resources catalogue created by Cefriel levaraging the KCong asset. The asset obtained is a user-friendly data exchange platform for the supply chain domain compliant to the IDS data sovereignty concept.
More Information	AI.SOV GitLab[26]
Connector Details	
Type	A generic solutions software (proprietary generic solutions)
Maturity	TRL7, used in data exchange domains
Portability	Agnostic
License	Closed source – extendable (i.e., extensions permitted)
IDS Certification	No
Adoption examples	The connector is used by both Whirpool and Sonae Arauco to share data with their supply chain. It has been used by another important automotive company to gather data from ologer trackers installed in their plants.
Deployment options	» Edge » On-premises » Cloud
Service level	Platform as a service

[26] https://gitlab.cefriel.it/groups/ai-sov

Access & Usage Control	
Access control	yes
Type of access control	» OAuth (Open authorization, standard/framework for REST/APIs) » Basic Auth (Basic access authorization, providing username and password)
Support of usage control	Yes
Usage control policies	» Data Consumer » IDS Connector
Communication	
Communication protocol	IDS protocol (IDSCP)
Transfer protocol	In-band with determined protocol bindings
User Interface	
Graphical user interface	Yes
Type	» for users » for management » for administration
Identity Management	
Identity management supported	No
Type	-
Information Model	
IDS Information Model	Yes
Supported version of IDS Information Model	Version 4.1
Vocabulary	
Supported	No
Type of vocabulary provided	-
Integration	
Integration with Catalogue/Meta Data Broker	Yes
Catalogue/Meta Data Broker type	a customized catalogue developed by Cefriel
Integration with Clearing House	No
Clearing House type	-

2.1.2 Boot-X Connector

Connector Overview	
Name	Boot-X Connector
Maintainer	Huawei, Munich Research Center
Logo of the connector or company logo	
Peculiarity of the connector	The Boot-X is Gaia-X / IDSA compliance ready, cloud-based Data Space implementation. The main focus is on cross-border data exchange, e.g. following international standards for data exchange between Chinese and European industries. Boot-X Connector is compatible to Eclipse Data Space connector, with enhanced features like local data policy, Self-Sovereign identity federation and compliance monitoring.
More Information	Boot-X website[27]
Connector Details	
Type	» A data connector framework » A generic solutions software » An off-the-shelf solution, provided as a service
Maturity	TRL 7, “live” in IDSA Radar
Portability	Agnostic
License	Open-source license not finally determined yet.
IDS Certification	No
Adoption examples	Boot-X[28] is a Data Space platform for cross-border Data Exchange. The first use case is in supply chain management, but Boot-X itself is domain agnostic. Boot-X has been developed in Europe according to Gaia-X / IDSA standards. It is also interoperable with a Data Space service offered by Huawei Cloud in China, called EDS (“Exchange Data Service”[29]), to enable cross-border Data exchange between China and Europe.
Deployment options	» On-premises » Cloud » Huawei Cloud

[27] www.boot-x.eu
[28] www.boot-x.eu
[29] https://www.huaweicloud.com/product/eds.html

Service level	» Connector as a service » Platform as a service
Access & Usage Control	
Access control	Yes
Type of access control	» via OAuth (Open authorization, standard/framework for REST/APIs) » Basic auth (Basic access authorization, providing username and password) » API key (manage access through a unique code for programming interface) » SSI OIDC credential bridge is integrated in Boot-X
Support of Usage Control	Yes
Usage Control Policies	» Data Consumer » IDS Connector » Application inside a Connector » User Role » Time Interval » Duration » Location » Number of usage » Inform a participant about the Data Usage » Delete Data
Communication	
Communication protocol	Dataspace protocol (HTTPS)
Transfer protocol	» In-band with determined protocol bindings » Out-of-band utilizing data planes with protocol bindings (data planes are part of the connector offering)
User Interface	
Graphical User Interface	Yes
Type	» For users » For management » For administration
Identity Management	
Identity management supported	Yes

Type	» Centralized (X.509) » Decentralized (did:web) » Decentralized (SSI) » Boot-X includes credential bridge for SSI and OIDC.
Information Model	
IDS Information Model	No
Supported version of IDS Information Model	-
Vocabulary	
Supported	No
Type of vocabulary provided	-
Integration	
Integration with Catalogue/Meta Data Broker:	Yes
Catalogue/Meta Data Broker type	EDC Catalouge
Integration with Clearing House:	-
Clearing House type	-

2.1.3 ECI Gatewise IDS Connector powered by TNO

Connector Overview	
Name	ECI Gatewise IDS Connector powered by TNO
Maintainer	ECI Software Solutions and TNO
Logo of the connector or company logo	eci Gatewise™
Peculiarity of the connector	By using the cloud-based IDS connector, companies affiliated with a SCSN Service Provider can digitally exchange supply chain related messages with companies affiliated with another SCSN Service Provider.
More Information	TNO website on IDS technology[30]
Connector Details	
Type	» A data connector framework » A generic open-source solution » An off-the-shelf solution, provided as a service
Maturity	TRL 9 (live)
Portability	Specific
License	Open-source. The IDS connector developed by TNO is open-source. The developments carried out by ECI Software Solutions are not open-source.
IDS Certification	No
Adoption examples	The IDS Connector is used for the exchange of order-related data between manufacturing companies and with wholesalers.
Deployment options	Cloud
Service level	» Connector as a service » Self-service
Access & Usage Control	
Access control	Yes
Type of access control	» via OAuth (Open authorization, standard/framework for REST/APIs) » API key (manage access through a unique code for programming interface)
Support of Usage Control	Yes

[30] https://www.tno.nl/en/technology-science/technologies/international-data-spaces/

Usage Control Policies	IDS Connector
Communication	
Communication protocol	IDS-REST
Transfer protocol	Information not available
User Interface	
Graphical User Interface	No
Type	-
Identity Management	
Identity management supported	No
Type	-
Information Model	
IDS Information Model	No
Supported version of IDS Information Model	-
Vocabulary	
Supported	No
Type of vocabulary provided	-
Integration	
Integration with Catalogue/Meta Data Broker:	No
Catalogue/Meta Data Broker type	-
Integration with Clearing House:	No
Clearing House type	-

2.1.4 Eclipse Dataspace Components (EDC) – Framework

Connector Overview

Name	Eclipse Dataspace Components – Framework
Maintainer	Committer Group in Eclipse Foundation
Logo of the connector or company logo	
Peculiarity of the connector	Whatever the individual setup is – on-premises bare-metal, different cloud vendors, hybrid, even single end-user machines – the EDC can be customized to work within any environment at scale. The to be build connector's added value is achieved through the separation of control and data plane, enabling a modular and thereby customizable way to build data spaces. Due to common interfaces and mapping of existing standards, the connector adds capabilities of contract negotiating and policy handling in an interoperable manner. As an open-source project hosted by the Eclipse Foundation, it provides a growing list of modules for many widely deployed cloud environments out-of-the-box and can easily be extended for more customized environments, while avoiding any IP right headaches. The EDC are a framework to build connectors but cannot be used as standalone connector implementation.
More Information	» Source code repository of the EDC connector[31] » EDC homepage[32]

Connector Details

Type	Data connector framework
Maturity	TRL 8-9
Portability	Java-based environment required[33]
License	Open source (Apache 2.0)
IDS Certification	No
Adoption examples	Several data space projects (e.g. Catena-X, Eona-X, mobility Data Space-MDS, Omega-X...) and connector

[31] https://github.com/eclipse-edc/Connector
[32] https://projects.eclipse.org/projects/technology.edc
[33] https://github.com/eclipse-edc/Samples/blob/main/basic/basic-01-basic-connector/README.md

	implementations (e.g. Health-X DataLOFT connector, sovity's EDC, Cofinity-X connector)
Deployment options	Not specified
Service level	Framework to build services. Service level is best effort of the open-source-community
Access & Usage Control	
Access control	No
Type of access control	Subject of Data Planes
Support of Usage Control	No, subject to data planes
Usage Control Policies	
Communication	
Communication Protocol	» Dataspace protocol (HTTPS)
Transfer Protocol	Out-of-band utilizing data planes without determined protocol bindings (data planes to be added and not part of EDC)
User Interface	
Graphical User Interface	No
Type	
Identity Management	
Identity management provided	No
Type	None
Information Model	
IDS Information Model	No
Supported version of IDS Information Model	
Vocabulary	
Supported	No
Type of Vocabulary provided	
Integration	
Integration with Catalogue/Meta Data Broker	No

Catalogue/Meta Data Broker type	-
Integration with Clearing House	No
Clearing House type	-

2.1.5 EdgeDS Connector

Connector Overview	
Name	EdgeDS Connector
Maintainer	Intracom Telecom
Logo of the connector or company logo	
Peculiarity of the connector	The connector is based on the open-source Dataspace Connector by Fraunhofer ISST. It has been adapted to be incorporated within a MEC Platform for Edge Computing applications, therefore combining the IDS capabilities and the ETSI Multi-access Edge Computing (MEC) Architectural Framework.
More Information	» EdgeDS Github[34] » Paper "EdgeDS: Data Spaces enabled Multi-access Edge Computing"[35]
Connector Details	
Type	off-the-shelf solution, provided as a service
Maturity	TRL 4
License	Open-source, Apache 2.0
IDS Certification	No
Adoption examples	The connector is employed in the Edge Data Space featured on IDSA's Data Space Radar. It demonstrates the advantages of data-driven collaboration among systems and stakeholders through an illustrative use case from the Autonomous Driving field. This scenario envisions various situations for autonomous, connected vehicles on a highway, leveraging advanced safety, traffic routing, and other capabilities via data service ecosystems. E.g., consider a 'see-through' case where a vehicle aims to overtake a truck and temporarily gains access to a video stream from the leading car equipped with a camera. These scenarios extend to 'platooning,' where vehicles can drive in a synchronized manner, sharing sensor data, or the exchange of safety and traffic alerts between highway vehicles.
Deployment options	» Edge » On-premises » Cloud » IoT/CPS/OT devices
Service level	Connector as a service

[34] https://github.com/jkalogero/EdgeDS
[35] https://arxiv.org/abs/2304.05966

Access & Usage Control	
Access control	Yes
Type of access control	API key (Manage access through a unique code for programming interface)
Support of Usage Control	Yes
Usage Control Policies	IDS Connector
Communication	
Communication Protocol	Dataspace protocol (HTTPS)
Transfer Protocol	Out-of-band utilizing data planes with protocol bindings (data planes are part of the connector offering)
User Interface	
Graphical user interface	No
Type	-
Identity Management	
Identity management supported	No
Type	-
Information Model	
IDS Information Model	Yes
Supported version of IDS Information Model	As the DSC 8.0.2, the EdgeDS connector uses the IDS Messaging library[36] which implements Info Model 4.2.7
Vocabulary	
Supported	Yes
Type of Vocabulary Provided	IDS Information Model
Integration	
Integration with Catalogue/Meta Data Broker	Yes
Catalogue/Meta Data Broker type	MEC Service Registry
Integration with Clearing House	No
Clearing House type	-

[36] https://github.com/International-Data-Spaces-Association/IDS-Messaging-Services

2.1.6 EGI DataHub Connector

Connector Overview	
Name	EGI DataHub Connector
Maintainer	EGI Foundation
Logo of the connector or company logo	
Peculiarity of the connector	The EGI DataHub Connector is based on the Dataspace Connector available open source. Policy based access via IDS to multiple storage backends supported by EGI DataHub (e.g. S3, Swift, NFS, GlusterFS, etc). The EGI DataHub is a high-performance data management solution that offers unified data access across globally distributed environments and multiple types of underlying storage, allowing users to share, collaborate and perform computations on the stored data easily.
More Information	» EGI DataHub Website[37] » DataHub documentation[38]
Connector Details	
Type	A generic open-source solutions
Maturity	TRL 4-5
Portability	Agnostic
License	Open-source
IDS Certification	No
Adoption examples	EUHubs4Data
Deployment options	» On-premises » Cloud
Service level	Platform as a service
Access & Usage Control	
Access control	Yes
Type of access control	Basic auth (Basic access authorization, providing username and password)
Support of Usage Control	Yes
Usage Control Policies	» Data Consumer » IDS Connector

[37] https://www.egi.eu/service/datahub/
[38] https://docs.egi.eu/users/data/management/datahub/

	» Security Level » Application inside a Connector
Usage Control Policies (cont.)	» User Role » Time Interval » Duration » Location » Purpose
Communication	
Communication Protocol	IDS Multipart
Transfer Protocol	In-band with determined protocol bindings
User Interface	
Graphical user interface	Yes
Type	For management
Identity Management	
Identity management supported	Yes
Type	Centralized (X.509)
Information Model	
IDS Information Model	Yes
Supported version of IDS Information Model	4.2.7
Vocabulary	
Supported	No
Type of Vocabulary provided	-
Integration	
Integration with Catalogue/Meta Data Broker	Yes
Catalogue/Meta Data Broker type	IDS Metadata Broker
Integration with Clearing House	No
Clearing House type	-

2.1.7 FIWARE Data Space Connector

Connector Overview	
Name	FIWARE Data Space Connector
Maintainer	FIWARE Foundation
Logo of the connector or company logo	
Peculiarity of the connector	Highly modular and scalable Data Space Connector following DSBA Technical Convergence recommendation[39]
More Information	» Documentation[40] » Source code[41]
Connector Details	
Type	Generic and modular open-source solution
Maturity	TRL 6-7
Portability	Agnostic
License	Open source (MIT)
IDS Certification	No
Adoption examples	» Used to connect participants in the DOME Marketplace[42] project » Experiments from i4Trust acceleration program[43]
Deployment options	» On-premises » Cloud
Service level	» Connector as a service » Self-service
Access & Usage Control	
Access control	Yes
Type of access control	» Attribute-based access control (ABAC) following an XACML P*P architecture[44] where attributes of users map to claims in their VCs
Support of Usage Control	Yes

[39] https://data-spaces-business-alliance.eu/wp-content/uploads/dlm_uploads/Data-Spaces-Business-Alliance-Technical-Convergence-V2.pdf
[40] https://github.com/FIWARE/data-space-connector
[41] https://github.com/FIWARE-Ops/data-space-connector
[42] https://dome-marketplace.eu/
[43] https://i4trust.org/experiments/
[44] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

Usage Control Policies	Data inside the connector can be safeguarded within a Context Broker deployed inside to which only applications, deployed within the connector and owning VCs as specified in usage policies can access data for processing.
Communication	
Communication protocol	HTTPS
Transfer protocol	HTTPS (NGSI-LD)
User Interface	
Graphical User Interface	Yes
Type	» No central control plane » UI for parts of the system: ○ Credentials Management ○ On-Boarding ○ Acquisition of rights to use products (BAE Marketplace[45])
Identity Management	
Identity management supported	Yes
Type	Decentralized (based on Decentralized Identifiers[46] and Verifiable Credentials[47]). Supporting SIOPv2[48] and OIDC4VP[49] for authentication.
Information Model	
IDS Information Model	No
Supported version of IDS Information Model	-
Vocabulary	
Supported	Planned
Type of vocabulary provided	Supports multiple dataspace specific vocabularies compatible based on Smart Data Models[50] and others. Description of resources accessible through the connector following DCAT-AP/DCAT
Integration	

[45] https://github.com/FIWARE-TMForum/Business-API-Ecosystem
[46] https://www.w3.org/TR/did-core/
[47] https://www.w3.org/TR/vc-data-model/
[48] https://openid.net/specs/openid-connect-self-issued-v2-1_0.html#name-cross-device-self-issued-op
[49] https://openid.net/specs/openid-4-verifiable-presentations-1_0.html#request_scope
[50] https://smartdatamodels.org/

Integration with Catalogue/Meta Data Broker:	Yes
Catalogue/Meta Data Broker type	» Catalogs based on TMForum-APIs » Data Publication platforms (e.g., CKAN) using DCAT/DCAT-AP
Integration with Clearing House:	Yes
Clearing House type	Gaia-X Digital Clearing Houses (GXDCH)

2.1.8 GATE Dataspace Connector

Connector Overview	
Name	GATE Dataspace Connector
Maintainer	GATE Institute
Logo of the connector or company logo	
Peculiarity of the connector	GATE Dataspace connector is based on IDS reference implementation and is fully integrated with other components of IDS RAM, namely the Identity provider, the Metadata Broker, the Clearing House, the Vocabulary Hub and the App Store. Digital identities of interacting components are used to ensure trustful message exchange. The connector supports provision of resources via static values, files, APIs and databases. It implements various policies for data usage and follows the negotiation process required for establishing data sharing between two participants. The accompanying UI provides a better user experience with comprehensive functionality for data exchange, metadata search and data application usage.
More Information	GATE Institute GitHub repository[51]
Connector Details	
Type	» A generic open-source solutions (i.e. data connectors that can be integrated directly into an IT-Landscape and connected to services, often acting as proxies or gateways to companies' IT-Services) » An off-the-shelf solution, directly usable integrated in data-related products
Maturity	TRL 5
Portability	Specific
License	Open source (i.e. without restrictions, e.g., Apache 2.0)
IDS Certification	No

[51] https://github.com/gate-institute/DataspaceConnector/blob/main/LICENSE

Adoption examples	
Deployment options	On-premises
Service level	Platform as a service
Access & Usage Control	
Access control	Yes
Type of access control	» OAuth » Basic auth
Support of Usage Control	Yes
Usage Control Policies	» IDS Connector » Security Level » Time Interval » Duration » Number of usage » Log Data Usage Information
Communication	
Communication Protocol	» IDS Multipart » IDS protocol (IDSCP)
Transfer Protocol	In-band with determined protocol bindings
User Interface	
Graphical User Interface	Yes
Type	For users
Identity Management	
Identity management provided	Yes
Type	Centralized (X.509)
Information Model	
IDS Information Model	Yes
Supported version of IDS Information Model	Supported Info Model versions: Inbound: "4.0.0", "4.1.0", "4.1.2", "4.2.0", "4.2.1", "4.2.2", "4.2.3", "4.2.4", "4.2.5", "4.2.6", "4.2.7". Outbound: "4.2.7";
Vocabulary	
Supported	Yes
Type of Vocabulary provided	vocabularies can be added using the vocabulary hub
Integration	

Integration with Catalogue/Meta Data Broker	Yes
Catalogue/Meta Data Broker type	IDS Metadata Broker
Integration with Clearing House	Yes
Clearing House type	IDS Clearing House

2.1.9 GDSO Connector - Tyre Information Service

Connector Overview	
Name	GDSO Connector - Tyre Information Service
Maintainer	GDSO - Global Data Service Organisation for tyres and automotive components
Logo of the connector or company logo	GDSO STANDARDIZE. SHARE. SIMPLIFY.
Peculiarity of the connector	Communication protocol based on a rest API with a vocabulary made of standardized data set for all GDSO Members, the meta data broker is a resolver that provides information about the endpoints offered by GDSO Members. Data usage policies allow also to initiate the B2B contract negotiation between GDSO Members and Data users by connecting the parties, but to be managed and finalized outside GDSO.
More Information	GDSO website[52]
Connector Details	
Type	A generic solutions software, partially open source
Maturity	Live - TRL 9
Portability	Agnostic
License	Partially open source. Proprietary source code that through the REST API can be integrated directly into an IT-Landscape and connected to services. The API is made freely available, but the terms of use do not allow to change it. For GDSO members, one implementation code is also available.
IDS Certification	No
Adoption examples	The connector is adopted by different stakeholders along the tyre value chain: tyre manufacturers, vehicle manufacturers, distributors and others.
Deployment options	» Edge » On-premises » Cloud » IoT/CPS/OT devices

[52] https://gdso.org/Members-description/Technical-documentation

Service level	Platform as a service (i.e., configuration)
Access & Usage Control	
Access control	Yes
Type of access control	OAuth (Open authorization, standard/framework for REST/APIs)
Support of Usage Control	Yes
Usage Control Policies	Data Consumer
Communication	
Communication Protocol	REST API
Transfer Protocol	In-band with determined protocol bindings
User Interface	
Graphical User Interface	No
Type	-
Identity Management	
Identity management provided	Yes
Type	Centralized based on AWS Cognito
Information Model	
IDS Information Model	No
Supported version of IDS Information Model	-
Vocabulary	
Supported	Yes
Type of Vocabulary provided	Self-developed, called data referential
Integration	
Integration with Catalogue/Meta Data Broker	Yes
Catalogue/Meta Data Broker type	resolver, storing information about the data endpoints offered by GDSO Members
Integration with Clearing House	No
Clearing House type	-

2.1.10 HEALTH-X dataLOFT EDC

Connector Overview	
Name:	HEALTH-X dataLOFT EDC
Maintainer	Fraunhofer ISST
Logo of the connector or company logo	Fraunhofer ISST
Peculiarity of the connector	The HEALTH-X dataLOFT EDC is an extended and configured version of the EDC Connector. It has been extended in order to realize specific Use Cases from the Healthcare domain.
More Information	Not available
Connector Details	
Type	A data connector framework
Maturity	Use-case specific approach (work in progress)
Portability	Agnostic
License	Has not been finally determined yet, probably open-source (Apache 2.0) in the future.
IDS Certification	No
Adoption examples	Within HEALTH-X dataLOFT project
Deployment options	» On-premises » Cloud
Service level	Self-service
Access & Usage Control	
Access control	Yes
Type of access control	Using that of the EDC Core (currently API key)
Support of Usage Control	Using that of the EDC Core
Usage Control Policies	Information not available
Communication	
Communication Protocol	Dataspace protocol (HTTPS)
Transfer Protocol	Out-of-band utilizing data planes with protocol bindings (data planes are part of the connector offering)

User Interface	
Graphical User Interface	No specific GUI has been implemented yet, but the EDC DataDashboard could be used for management/administration
Type	-
Identity Management	
Identity management provided	Yes
Type	Decentralized (SSI)
Information Model	
IDS Information Model	No
Supported version of IDS Information Model	-
Vocabulary	
Supported	No
Type of Vocabulary provided	-
Integration	
Integration with Catalogue/Meta Data Broker	Yes
Catalogue/Meta Data Broker type	Currently integration with project-specific Federated Catalog implementation that offers Participant Self-Descriptions via REST interface; planned integration with GXFS Federated Catalog.
Integration with Clearing House	No
Clearing House type	-

2.1.11 IIOC IoT Connector

Connector Overview	
Name	IIOC IoT Connector (Intel IONOS Orbiter Connector)
Maintainer	truzzt
Logo of the connector or company logo	truzzt
Peculiarity of the connector	IoT Version of IDS Connector – compatible to EDC, Extra resource-saving executable for sensors and small devices, Rust & C based
More Information	Not available
Connector Details	
Type	» A generic open-source solutions » An off-the-shelf solution, provided as a service
Maturity	The connector is already live and usable. Connector is a part of IDSA Base Camp.
Portability	Agnostic
License	Open-source, Apache 2.0
IDS Certification	No
Adoption examples	truzzt Box
Deployment options	» Cloud » IoT/CPS/OT devices
Service level	» Connector as a service » Platform as a service » Self-service
Access & Usage Control	
Access control	Yes
Type of access control	API key
Support of Usage Control	No
Usage Control Policies	-
Communication	
Communication Protocol	» IDS Multipart » Dataspace protocol (HTTPS)
Transfer Protocol	Out-of-band utilizing data planes with protocol bindings
User Interface	

Graphical user interface	Yes
Type	» for users » for management » for administration
Identity Management	
Identity management supported	Yes
Type	Decentralized (SSI)
Information Model	
IDS Information Model	Yes
Supported version of IDS Information Model	4.x
Vocabulary	
Supported	No
Type of Vocabulary provided	-
Integration	
Integration with Catalogue/Meta Data Broker	Yes
Catalogue/Meta Data Broker type	Base Camp Federated Catalogue
Integration with Clearing House	Yes
Clearing House type	Base Camp Clearing House

2.1.12 Kharon IDS Connector powered by the Dataspace Connector

Connector Overview	
Name	Kharon IDS Connector powered by the Dataspace Connector
Maintainer	HOLONIX SRL
Logo of the connector or company logo	
Peculiarity of the connector	The connector is embedded with a complete IoT asset management solution backed called Kharon. IoT data and augmented intelligence results are now manageable through IDS thanks to the integration of the Kharon solution with the Dataspace Connector; this enables companies to enlarge their IoT network interacting with other device providers and users in a secure way keeping sovereignty and industrial confidentiality.
More Information	» Holonix website[53] » Dat4Zero project website[54]
Connector Details	
Type	» generic solution (proprietary software) » off-the-shelf solution, provided as a service
Maturity	TRL 7
Portability	Specific
License	Closed source
IDS Certification	No
Adoption examples	» Kharon platform » Dat4Zero project European project (G.A.958363)
Deployment options	» Edge » Cloud
Service level	» Connector as a service » Platform as a service

[53] https://www.holonix.it/en/
[54] https://dat4zero.eu/work-packages/

Access & Usage Control	
Access control	Yes
Type of access control	OAuth (Open authorization, standard/framework for REST/APIs)
Support of Usage Control	Yes, in Kharon, not implemented in the connector as today
Usage Control Policies	-
Communication	
Communication Protocol	IDS-REST
Transfer Protocol	In-band with not determined protocol bindings
User Interface	
Graphical user interface	Yes
Type	For management
Identity Management	
Identity management supported	It's centralized for Kharon, under development for the connector.
Type	-
Information Model	
IDS Information Model	No
Supported version of IDS Information Model	-
Vocabulary	
Supported	No
Type of Vocabulary provided	-
Integration	
Integration with Catalogue/Meta Data Broker	No
Catalogue/Meta Data Broker type	-
Integration with Clearing House	No
Clearing House type	-

2.1.13 Mitsubishi Electric Dataspace Connector

Connector Overview	
Name	Mitsubishi Electric Dataspace Connector
Maintainer	Mitsubishi Electric Europe B.V. - German Branch
Logo of the connector or company logo	
Peculiarity of the connector	Connect an iQ-R PLC system via the Mitsubishi Electric Dataspace Connector running on an RD55UP-12-V module.
More Information	-
Connector Details	
Type	An off-the-shelf solution, directly usable integrated in data-related products
Maturity	Early stage / Sandbox Stage
Portability	Specific
License	» Open source (Apache License 2.0)[55] » Closed source (modifications, extensions and PLC specific adaptations are not publicly available)
IDS Certification	-
Adoption examples	Proof of concept executed together with the company NTT. It was finished September 2023.
Deployment options	IoT devices. The main purpose was to execute it at the Mitsubishi Electric C Intelligent Function Module RD55UP12-V (module installed in a PLC system).
Service level	Self-service. The connector can be installed at the Mitsubishi Electric C Intelligent Function Module RD55UP12-V.
Access & Usage Control	
Access control	Yes
Type of access control	» Basic auth (Basic access authorization, providing username and password) » The communication is secured with a password

[55] The connector is based on the open-source EDC. The EDC repository (https://github.com/eclipse-edc/Connector) has been forked to https://github.com/huebl/DataSpaceConnector.

Support of Usage Control	The communication can be restricted to certain IP addresses, which is enforced by our IT department independent from the connector.
Usage Control Policies	» IDS Connector » Duration
Communication	
Communication Protocol	» Dataspace Protocol (other binding) » HTTP
Transfer Protocol	HTTP
User Interface	
Graphical user interface	No (i.e. the connector can only be used via command line or operator needs to develop their own GUI)
Type	-
Identity Management	
Identity management supported	No
Type	-
Information Model	
IDS Information Model	No
Supported version of IDS Information Model	-
Vocabulary	
Supported	No
Type of Vocabulary provided	-
Integration	
Integration with Catalogue/Meta Data Broker	No
Catalogue/Meta Data Broker type	-
Integration with Clearing House	No
Clearing House type	-

2.1.14 OneNet Connector

Connector Overview	
Name	OneNet Connector

Maintainer	Engineering Ingegneria Informatica S.p.a. and EUROPEAN DYNAMICS Luxembourg S.A.
Logo of the connector or company logo	ONENET one network for Europe
Peculiarity of the connector	» The OneNet Connector, based on TRUE Connector, aims to enable a European Energy Data Space, combining the IDS principles with the advantages of the FIWARE ecosystem ensuring a seamless and secure data exchange in a completely end-to-end decentralized approach. The main features of the OneNet Connector are: » Ready-to-go, ready to be installed in any environment and integrated with existing platforms via APIs » Fully integrated with the FIWARE Context Broker (in the NGSI-LD version) » Offers a rich graphical user Interface for connector's configuration and for a series of additional services (KPI's, data exchange timeline, cross-platform services catalogue, vocabularies, etc.) » Facilitates through the GUI or via API the data exchange process, and extends the interaction between data producer/consumer by providing an "offered service" handshake and publish/subscribe mechanisms, accordingly » Integrates data harmonization tool for supporting and mapping CIM standards into NGSI/LD » Can be integrated with third-party Identity Management Services » Supports more than 60 different harmonized services and data profiles in the smart grid and energy field, but can be easily extended with additional services also in other domains » Is completely integrated with the OneNet » Orchestration Workbench and OneNet Monitoring and Analytics Dashboard, two additional tools that allows participants to deploy and evaluate their own services on data coming from the OneNet system and integrate it with analytics and data visualization.
More Information	OneNet project website[56]
Connector Details	
Type	A generic open-source solution
Maturity	TRL 7 (status Aug. 2023). The OneNet Connector was deployed and tested in 12 different European countries'

[56] https://onenet-project.eu/

	environments, within the OneNet Demonstration phase. The target TRL at the end of the project is 8.
Portability	Agnostic
License	» Open-source » Open-source – copyleft » Upon project conclusion, it will be open-source under a GPLv3 or similar license.
IDS Certification	No
Adoption examples	Information not available
Deployment options	On-premises
Service level	Connector as a service
Access & Usage Control	
Access control	Yes
Type of access control	» Basic auth (Basic access authorization, providing username and password) » API key (Manage access through a unique code for programming interface)
Support of Usage Control	Yes
Usage Control Policies	» Data Consumer » IDS Connector » Time Interval » Duration » Log Data Usage Information » Inform a participant about the Data Usage
Communication	
Communication Protocol	Dataspace protocol (HTTPS)
Transfer Protocol	In-band with determined protocol bindings
User Interface	
Graphical user interface	Yes
Type	» for users » for management » for administration
Identity Management	
Identity management supported	Yes

Type	Centralized (X.509)
Information Model	
IDS Information Model	No
Supported version of IDS Information Model	-
Vocabulary	
Supported	Yes
Type of Vocabulary provided	Information not available
Integration	
Integration with Catalogue/Meta Data Broker	No
Catalogue/Meta Data Broker type	-
Integration with Clearing House	Yes
Clearing House type	Fraunhofer Clearing House

2.1.15 Silicon Economy EDC

Connector Overview	
Name	Silicon Economy EDC
Maintainer	Fraunhofer ISST
Logo of the connector or company logo	
Peculiarity of the connector	The connector is developed for the needs of the Silicon Economy. The connector is based on the EDC framework.
More Information	» GitLab repository[57] » Silicon Economy project website[58]
Connector Details	
Type	A generic open-source solution
Maturity	TRL 3
Portability	Agnostic
License	Open-source, Open Logistics License
IDS Certification	No
Adoption examples	There is no usage of the connector. Use cases in the logistics domain are being discussed within the silicon economy for the use of the connector.
Deployment options	» Edge » On-premises » Cloud » IoT/CPS/OT devices
Service level	» Self-service
Access & Usage Control	
Access control	No
Type of access control	-
Support of Usage Control	No
Usage Control Policies	-
Communication	
Communication Protocol	DSP HTTPS
Transfer Protocol	HTTP

[57] https://git.openlogisticsfoundation.org/silicon-economy/base/ids/silicon-economy-edc
[58] https://www.silicon-economy.com/

User Interface	
Graphical user interface	No
Type	-
Identity Management	
Identity management supported	Information not available
Type	-
Information Model	
IDS Information Model	No
Supported version of IDS Information Model	-
Vocabulary	
Supported	No
Type of Vocabulary provided	-
Integration	
Integration with Catalogue/Meta Data Broker	No
Catalogue/Meta Data Broker type	-
Integration with Clearing House	No
Clearing House type	-

2.1.16 sovity CaaS (Connector-as-a-Service)

Connector Overview	
Name	sovity CaaS (Connector-as-a-Service)
Maintainer	sovity GmbH
Logo of the connector or company logo	
Peculiarity of the connector	Fully managed ready-to-use connector based on EDC for easy data sharing between data space participants with usage control and other enhanced usability features. Compatible with data spaces like MDS, Catena-X and more.
More Information	» sovity website[59] » sovity LinkedIn[60] » sovity YouTube[61]
Connector Details	
Type	Off-the-shelf solution, provided as a service
Maturity	TRL 9, used in production
Portability	Agnostic
License	Closed-source
IDS Certification	No
Adoption examples	Catena-X, Mobility Data Space, other user groups and customers of sovity
Deployment options	» On-premise » Cloud » Others
Service level	» Connector as a service
Access & Usage Control	
Access control	Yes
Type of access control	» OAuth 2.0 » Basic Auth (Basic access authorization, providing username and password) » API Key (Manage access through a unique code for programming interface)
Support of Usage Control	Yes
Usage Control Policies	» Connector Restriction » Time Interval

[59] https://sovity.de/en/connect-to-data-space-en/
[60] https://www.linkedin.com/company/sovity
[61] https://www.youtube.com/@sovitygmbh6305

Communication	
Communication Protocol	Dataspace Protocol (HTTPS)
Transfer Protocol	Out-of-band
User Interface	
Graphical user interface	Yes, protected with user accounts (OAuth2)
Type	» for users » for management » for administration
Identity Management	
Identity management supported	Yes
Type	» Centralized DAPS (X.509) » Decentralized (did:web) » Decentralized (SSI)
Information Model	
IDS Information Model	No
Supported version of IDS Information Model	-
Vocabulary	
Supported	Yes
Type of Vocabulary provided	DCAT, ODRL, DSpace
Integration	
Integration with Catalogue/Meta Data Broker	Yes
Catalogue/Meta Data Broker type	EDC's built-in catalogue (all versions), IDS Broker supported (< v5.0.0), EDC-based Broker with auto-crawling (currently developed for MDS; soon to be open-sourced) (all versions), Catena-X Digital Twin Registry[62]
Integration with Clearing House:	Yes
Clearing House type	IDS Clearing House supported (< v5.0.0), EDC-based Clearing House (in development; soon to be open-sourced)

[62] https://github.com/eclipse-tractusx/sldt-digital-twin-registry/tree/main/docs

2.1.17 sovity Open-Source EDC Connector

Connector Overview	
Name	sovity Open-Source EDC Connector
Maintainer	sovity GmbH
Logo of the connector or company logo	
Peculiarity of the connector	Ready to use open-source connector for easy sharing of data between data space participants with usage control and other enhanced usability features.
More Information	» Documentation[63] » GitHub (extensions)[64] » GitHub (UI)[65]
Connector Details	
Type	» A generic open-source solution » An off-the-shelf solution » A generic solutions software (proprietary generic solutions)
Maturity	TRL 9, used in production.
Portability	Agnostic
License	Open source, Apache 2.0
IDS Certification	No
Adoption examples	Mobility Data Space and broad range of other user groups and research projects
Deployment options	» On-premise » Cloud » Others
Service level	» Self-Hosted
Access & Usage Control	
Access control	Yes
Type of access control	» Basic auth (Basic access authorization, providing username and password) » API key (Manage access through a unique code for programming interface) » Others

[63] https://edc.docs.sovity.de
[64] https://github.com/sovity/edc-extensions
[65] https://github.com/sovity/edc-ui

Support of usage control	Yes
Usage control policies	» Connector Restriction » Time Interval
Communication	
Communication protocol	Dataspace Protocol (HTTPS)
Transfer protocol	Out-of-band
User Interface	
Graphical user interface	Yes
Type	» for users » for management » for administration
Identity Management	
Identity management supported	Yes
Type	» Centralized DAPS (X.509) » Mock IAM
Information Model	
IDS Information Model	No
Supported version of IDS Information Model	-
Vocabulary	
Supported	Yes
Type of vocabulary provided	DCAT, ODRL, DSpace
Integration	
Integration with Catalogue/Meta Data Broker	Yes
Catalogue/Meta Data Broker type	» EDC's built-in catalogue (all versions) » IDS Broker supported (< v5.0.0) » EDC-based Broker with auto-crawling, soon to be open-sourced (all versions)
Integration with Clearing House	Yes
Clearing House type	» IDS Clearing house supported (< v5.0.0) » EDC-based Clearing House (in development; soon to be open-sourced)

2.1.18 Tech2B SCSN Connector

Connector Overview	
Name	Tech2B SCSN Connector
Maintainer	Tech2B
Logo of the connector or company logo	
Peculiarity of the connector	Enabling data spaces for SMEs
More Information	Via the Tech2B AppStore for industry-specific applications, allowing one-click expansion of the Tech2B's core features and enabling data spaces for SMEs
Connector Details	
Type	» An off-the-shelf solution, provided as a service » An off-the-shelf solution, directly usable integrated in data-related products
Maturity	TRL: 7-8
Portability	Agnostic
License	Closed source
IDS Certification	No
Adoption examples	» Smart Connected Supplier Network » Market 4.0 » Example use cases: 1on1 transactions: Share daily order transactions with suppliers that have none or an outdated software system. Standardized, secure and easy to use for companies without digitization knowledge, to build a future-proof and connected supply chain. Supply & Demand: Enable the opportunity for buyers to use the reach of our network in the quotation phase. Our service provider acts as proxy to place incoming RFQ on Tech2B Supply & Demand and return quotations directly to the buyer.
Deployment options	Cloud
Service level	» Connector as a service » Platform as a service » Self-service

Access & Usage Control	
Access control	Yes
Type of access control	OAuth (Open authorization, standard/framework for REST/APIs)
Support of Usage Control	Yes
Usage Control Policies	Number of usages
Communication	
Communication Protocol	Dataspace protocol (HTTPS)
Transfer Protocol	Information not available
User Interface	
Graphical user interface	Yes
Type	» for users » for management » for administration
Identity Management	
Identity management supported	Yes
Type	Decentralized (did:web)
Information Model	
IDS Information Model	No
Supported version of IDS Information Model	-
Vocabulary	
Supported	No
Type of Vocabulary provided	-
Integration	
Integration with Catalogue/Meta Data Broker	No
Catalogue/Meta Data Broker type	-
Integration with Clearing House	No
Clearing House type	-

2.1.19 Tekniker IDS Connector

Connector Overview	
Name	Tekniker IDS Connector
Maintainer	Tekniker
Logo of the connector or company logo	
Peculiarity of the connector	IDS Connector which, following the Dataspace protocol, serves as a single and interoperable point of entry for multiple data sources while preserving the data sovereignty. The Tekniker IDS Connector is being developed to manage building permits in a data space for the construction industry. In this regard, it also implements the required data planes to transfer files as well as BIM data.
More Information	
Connector Details	
Type	A generic open-source solutions
Maturity	TRL 3
Portability	Agnostic
License	Currently closed source. Probably open source (Apache 2.0) in the future.
IDS Certification	No
Adoption examples	Construction Data Space for Building Permit Management (DigiChecks project[66])
Deployment options	» On-premises » Cloud
Service level	» Connector as a service
Access & Usage Control	
Access control	Yes (planned)
Type of access control	SSI
Support of Usage Control	No
Usage Control Policies	-
Communication	

[66] https://digichecks.eu/

Communication Protocol	Dataspace protocol (HTTPS)
Transfer Protocol	Out-of-band utilizing data planes with protocol bindings
User Interface	
Graphical user interface	No
Type	-
Identity Management	
Identity management supported	Yes (planned)
Type	Decentralized (SSI)
Information Model	
IDS Information Model	Yes
Supported version of IDS Information Model	Dataspace Information Model from Dataspace protocol v0.8
Vocabulary	
Supported	Yes (planned)
Type of Vocabulary provided	ifcOWL
Integration	
Integration with Catalogue/Meta Data Broker	No
Catalogue/Meta Data Broker type	-
Integration with Clearing House	No
Clearing House type	-

2.1.20 Telekom DIH Connector

Connector Overview	
Name	Telekom DIH Connector
Maintainer	T-Systems International GmbH
Logo of the connector or company logo	T Systems
Peculiarity of the connector	Connect to any dataspace in less than 5 minutes and start sharing data through one of the first soon-IDS certified, Gaia-X compliant, cloud agnostic, plug-and-play connectors. We remove technical configuration complexities and provide an easier and user-friendly way for trusted data exchange, with sovereignty protection.
More Information	Data Intelligence Hub website[67]
Connector Details	
Type	An off-the-shelf solution, provided as a service, directly usable integrated in data-related products
Maturity	TRL 8
Portability	Agnostic
License	Closed source
IDS Certification	Yes (Connector Certification - Concept Review[68])
Adoption examples	» Data chains in Catena-X » Traceability applications in Catena-X » Research use-cases in Gaia-X 4 Future Mobility
Deployment options	» On-premises » Cloud
Service level	Connector as a service
Access & Usage Control	
Access control	Yes
Type of access control	» OAuth (Open authorization, standard/framework for REST/APIs) » API key (Manage access through a unique code for programming interface)
Support of Usage Control	Yes
Usage Control Policies	» Data Consumer

[67] https://dih.telekom.com/
[68] https://internationaldataspaces.org/t-systems-and-idsa-achieve-milestone-for-data-spaces-first-certification-of-a-connector-promotes-standardization-and-interoperability/

	» User Role » Time Interval » Duration » Location » Purpose
Communication	
Communication Protocol	Dataspace protocol (HTTPS)
Transfer Protocol	» Out-of-band utilizing data planes without determined protocol bindings (data planes to be added) » Out-of-band utilizing data planes with protocol bindings (data planes are part of the connector offering)
User Interface	
Graphical user interface	Yes
Type	» for users » for management » for administration
Identity Management	
Identity management supported	Yes
Type	» Centralized (X.509) » Decentralized (did:web)
Information Model	
IDS Information Model	Yes
Supported version of IDS Information Model	4.2.0
Vocabulary	
Supported	Yes
Type of Vocabulary provided	Supports multiple dataspace specific vocabularies
Integration	
Integration with Catalogue/Meta Data Broker	Yes
Catalogue/Meta Data Broker Type	» Federated Catalogue » IDS based Meta Data Broker
Integration with Clearing House	Yes

Clearing House type	Supports integration with Gaia-X Digital Clearing House

2.1.21 TNO Security Gateway (TSG)

Connector Overview	
Name	TNO Security Gateway (TSG)
Maintainer	TNO
Logo of the connector or company logo	TNO
Peculiarity of the connector	Multi-purpose connector
More Information	GitLab repository[69]
Connector Details	
Type	A generic open-source solution
Maturity	TRL 8
Portability	Agnostic
License	Open-source
IDS Certification	No
Adoption examples	SCSN[70] - actively used in production. Different European and Dutch projects.
Deployment options	Cloud
Service level	» Self-service
Access & Usage Control	
Access control	Yes
Type of access control	» OAuth (Open authorization, standard/framework for REST/APIs) » API key (Manage access through a unique code for programming interface)
Support of Usage Control	Yes
Usage Control Policies	» Data Consumer » Security Level » Time Interval » Location » Number of usages
Communication	

[69] https://tno-tsg.gitlab.io/
[70] https://smart-connected-supplier-network.gitbook.io/processmanual/

Communication Protocol	IDS Multipart
Transfer Protocol	IDS Multipart
User Interface	
Graphical user interface	Yes
Type	» for users » for management » for administration
Identity Management	
Identity management supported	Yes
Type	Centralized (X.509)
Information Model	
IDS Information Model	Yes
Supported version of IDS Information Model	4.1.0
Vocabulary	
Supported	No
Type of Vocabulary provided	-
Integration	
Integration with Catalogue/Meta Data Broker	Yes
Catalogue/Meta Data Broker type	MetaData Broker Open Core[71]
Integration with Clearing House	Not yet
Clearing House type	-

[71] https://github.com/International-Data-Spaces-Association/metadata-broker-open-core

2.1.22 Tritom Enterprise Connector

Connector Overview	
Name	Tritom Enterprise Connector
Maintainer	DataSpace Europe Oy
Logo of the connector or company logo	Tritom
Peculiarity of the connector	Enables data source and target systems technical connectivity to the Tritom service to produce services based on data sovereignty principles. Tritom also brings together ecosystem parties and provides the capabilities to create data and service catalogues.
More Information	Tritom website[72]
Connector Details	
Type	An off-the-shelf solution, provided as a service
Maturity	Used in the Tritom service current version, TRL8
Portability	Agnostic
License	Closed source, Tritom Enterprise license
IDS Certification	No
Adoption examples	In the Tritom service licensed by DataSpace Europe Oy
Deployment options	» On-premises » Cloud
Service level	Platform as a service
Access & Usage Control	
Access control	Yes
Type of access control	» OAuth (Open authorization, standard/framework for REST/APIs) » API key (Manage access through a unique code for programming interface)
Support of Usage Control	No
Usage Control Policies	-

[72] https://www.dataspace.fi/en/data-intermediation-service

Communication	
Communication Protocol	REST
Transfer Protocol	Information not available
User Interface	
Graphical user interface	No
Type	-
Identity Management	
Identity management supported	No
Type	-
Information Model	
IDS Information Model	No
Supported version of IDS Information Model	-
Vocabulary	
Supported	No, the connector is agnostic to content
Type of Vocabulary provided	-
Integration	
Integration with Catalogue/Meta Data Broker	No
Catalogue/Meta Data Broker type	-
Integration with Clearing House	No
Clearing House type	-
Additional Comments	Our Tritom service is in version 1.0 and is being still developed.

2.1.23 TRUE Connector

Connector Overview	
Name	TRUE Connector
Maintainer	Engineering Ingegneria Informatica SpA
Logo of the connector or company logo	
Peculiarity of the connector	The TRUE Connector enables the trusted data exchange in order to be an active part of an IDS Ecosystem, a virtual data space leveraging existing standards and technologies, as well as governance models well accepted in the data economy, to facilitate secure and standardized data exchange and data linkage in a trusted business ecosystem. The TRUE connector is also part of the Fiware Catalogue: the integration of existing Fiware ecosystems is guaranteed by the dedicated Data APP, enabling the IDS-based interaction in a plug-and-play way.
More Information	GitHub repository[73]
Connector Details	
Type	A generic open-source solution
Maturity	TRL 6; Part of the IDSA Graduation Scheme (Sandbox)
Portability	Agnostic
License	Open source (AGPL version 3)[74]
IDS Certification	No
Adoption examples	Several research projects (Market4.0, AI Regio, Platoon, Circular TwAIn, Eur3ka, CLARUS, SCREAM, CiTrace)
Deployment options	» Edge » On-premises » Cloud » IoT/CPS/OT devices
Service level	» Connector as a service » Platform as a service » Self-service
Access & Usage Control	
Access control	Yes
Type of access control	Basic auth (Basic access authorization, providing username and password)

[73] https://github.com/Engineering-Research-and-Development/true-connector
[74] https://github.com/Engineering-Research-and-Development/true-connector-execution_core_container/blob/master/LICENSE

Support of Usage Control	Yes
Usage Control Policies	» IDS Connector » Security Level » User Role » Time Interval » Duration » Purpose » Number of usages
Communication	
Communication Protocol	» IDS Multipart » IDS protocol (IDSCP)
Transfer Protocol	In-band with determined protocol bindings
User Interface	
Graphical user interface	No
Type	-
Identity Management	
Identity management supported	Yes
Type	Centralized (X.509)
Information Model	
IDS Information Model	Yes
Supported Version of IDS Information Model	4.2.7
Vocabulary	
Supported	No, responsibility to manage data is up to the data app
Type of Vocabulary Provided	-
Integration	
Integration with Catalogue/Meta Data Broker	Yes
Catalogue/Meta Data Broker Type	Fraunhofer Meta Data Broker (5.0.0)
Integration with Clearing House	Yes
Clearing House Type	Fraunhofer Clearing House from IDSA GitHub repository

2.1.24 Trusted Connector

Connector Overview	
Name	Trusted Connector
Maintainer	Fraunhofer AISEC
Logo of the connector or company logo	Fraunhofer AISEC
Peculiarity of the connector	» Enforceable Usage Control using Trusted Execution Environment integration and Remote Attestation
More Information	GitHub respository[75]
Connector Details	
Type	A generic solutions software (i.e., data connectors that can be integrated directly into an IT-Landscape and connected to services, often acting as proxies or gateways to companies' IT-Services)
Maturity	IDS_ready Component, ~ TRL 7
Portability	Agnostic
License	Open-source, Apache 2.0
IDS Certification	No
Adoption examples	None
Deployment options	» Edge » On-premises » Cloud
Service level	Platform as a service
Access & Usage Control	
Access control	Yes
Type of access control	» OAuth (Open authorization, standard/framework for REST/APIs) » Basic auth (Basic access authorization, providing username and password)
Support of Usage Control	Yes
Usage Control Policies	» Application inside a Connector » Time Interval
Communication	

[75] https://github.com/Fraunhofer-AISEC/trusted-connector

Communication Protocol	» IDS Multipart » IDS protocol (IDSCP)
Transfer Protocol	No
User Interface	
Graphical user interface	Yes
Type	For administration
Identity Management	
Identity management supported	Yes
Type	Centralized (X.509)
Information Model	
IDS Information Model	Yes
Supported version of IDS Information Model	Version 4.1.0
Vocabulary	
Supported	No
Type of Vocabulary provided	-
Integration	
Integration with Catalogue/Meta Data Broker	No
Catalogue/Meta Data Broker type	-
Integration with Clearing House	Yes
Clearing House type	AISEC-provided Clearing House

2.1.25 Trusted Supplier Connector

Connector Overview	
Name	Trusted Supplier Connector
Maintainer	German Edge Cloud GmbH & Co. KG
Logo of the connector or company logo	
Peculiarity of the connector	» Usability through Configuration and Monitoring UI, tailored for Cloud, Edge and hybrid scenarios
More Information	» German Edge Cloud website[76] » IDSA blog article[77]
Connector Details	
Type	An off-the-shelf solution, provided as a service
Maturity	IDS_ready, TRL 8
Portability	Agnostic
License	Closed source, proprietary / individual
IDS Certification	No
Adoption examples	Fraunhofer HHI, Fraunhofer HHI Digitale Signalverarbeitung, ICNAP IPT-HHI
Deployment options	» Edge » On-premises » Cloud
Service level	» Connector as a service » Platform as a service » Self-service
Access & Usage Control	
Access control	Yes
Type of access control	API key
Support of Usage Control	No
Usage Control Policies	-
Communication	

[76] https://gec.io/solutions/gaia-x-dienste/
[77] https://internationaldataspaces.org/secure-and-trusted-data-exchange-german-edge-clouds-oncite-is-ids-ready/

Communication Protocol	» IDS Multipart » HTTP, Cloud Events, IDS Header
Transfer Protocol	Database access is handled by provider
User Interfce	
Graphical user interface	Yes
Type	» for users » for administration
Identity Management	
Identity management supported	No
Type	-
Information Model	
IDS Information Model	No
Supported version of IDS Information Model	-
Vocabulary	
Supported	No
Type of Vocabulary provided	-
Integration	
Integration with Catalogue/Meta Data Broker	No
Catalogue/Meta Data Broker type	-
Integration with Clearing House	No
Clearing House Type	-
Additional Comments	We have validated the connector in external research projects and are looking for business customers.

2.1.26 VTT DSIL Connector

Connector Overview

Name	VTT DSIL Connector
Maintainer	VTT Technical Research Centre of Finland
Logo of the connector or company logo	VTT
Peculiarity of the connector	The VTT DSIL Connector (DSILC) significantly elevates the capabilities of the Dataspace connector reference implementation by introducing a suite of advanced features. These include support for the OPC UA communication protocol, a robust user and role-based access management system, and a heightened level of security, which includes protection against XSS (Cross-Site Scripting), clickjacking, and DOS (Denial of Service) attacks. Furthermore, we've enforced rigorous validation checks for the connector to ensure its integrity and reliability. In addition, our implementation incorporates enhanced security measures for the Postgres database. The VTT DSIL Connector finds its primary domain of application within the manufacturing sector, where it plays an indispensable role in facilitating seamless data communication while ensuring the utmost security and data resource access integrity.
More Information	Article on VTT Hub Facilitator website[78]

Connector Details

Type	» An off-the-shelf solution, provided as a service » An off-the-shelf solution, directly usable integrated in data-related products
Maturity	Information not available
Portability	Agnostic
License	Closed source (i.e., source text is not publicly viewable). No final decisions for the license have been made.
IDS Certification	Yes (Connector Certification - Concept Review)
Adoption examples	The DSIL connector is being used in several research and development projects. These include TRUSTEE (Trust and Privacy Preserving Computing Platform For Cross-Border Federation Of Data), OSME[79] (Open Smart Manufacturing Ecosystem) and RESONANCE[80] (Replicable and Efficient

[78] https://www.idsa-finland.fi/vtt-has-officially-kicked-off-the-certification-process-for-their-ids-connector/
[79] https://www.mexfinland.org/osme/
[80] https://www.resonance-project.eu/

	Solutions for Optimal Management of Cross-sector Energy).
Deployment options	» On-premises » Cloud
Service level	» Connector as a service » Platform as a service
Access & Usage Control	
Access control	Yes
Type of access control	» OAuth (Open authorization, standard/framework for REST/APIs) » Basic auth (Basic access authorization, providing username and password)
Support of Usage Control	Yes
Usage Control Policies	» Data Consumer » IDS Connector » Security Level » User Role » Time Interval » Duration » Number of usages » Log Data Usage Information » Inform a participant about the Data Usage » Delete Data
Communication	
Communication Protocol	» IDS Multipart » IDS protocol (IDSCP) » Dataspace protocol (HTTPS)
Transfer Protocol	In-band with determined protocol bindings
User Interface	
Graphical user interface	No
Type	-
Identity Management	
Identity management supported	Yes
Type	Centralized (X.509)

Information Model	
IDS Information Model	Yes
Supported version of IDS Information Model	Supported Info Model versions: Outbound: "4.2.7"; Inbound: "4.0.0", "4.1.0", "4.1.2", "4.2.0", "4.2.1", "4.2.2", "4.2.3", "4.2.4", "4.2.5", "4.2.6", "4.2.7".
Vocabulary	
Supported	No
Type of Vocabulary provided	-
Integration	
Integration with Catalogue/Meta Data Broker	Yes
Catalogue/Meta Data Broker type	The IDS metadata broker reference implementation[81]
Integration with Clearing House	No
Clearing House type	-

[81] https://github.com/International-Data-Spaces-Association/metadata-broker-open-core

2.2 Connectors with latest updates in May 2023

This section describes five connectors whose information was provided before May 2023. No updates have been provided since then.

An overview of these six connectors is reported in Figure 4 Overview of connectors with latest updates in May 2023.

Connectors with latest updates in May 2023			
Section	*Name of connector*	*Maintainer*	*Open source*
2.2.1	Dataspace Connector (DSC)	SOVITY	
2.2.2	GAIAboX®.IDS. BasicConnector	NICOS	
2.2.3	MPAD-C	MONDRAGON UNIBERTSITATEA	✓
2.2.4	TeraLab Connector	Institut Mines-Télécom / TERALAB Data Science for Europe	
2.2.5	WeTech Smart Data Connector	WeTech IDS-China	

Figure 4 Overview of connectors with latest updates in May 2023

2.2.1 Dataspace Connector

Name of the connector	Dataspace Connector
Logo of the connector or company logo	
Maintainer (company name)	sovity
Type of connector	Generic open-source solution
Short description	The Dataspace Connector is an IDS connector that is currently being maintained by sovity. The connector was originally developed at the Fraunhofer ISST. With the help of the Dataspace Connector, existing software can easily be extended by IDS connector functionalities in order to integrate them into an IDS data ecosystem. Furthermore, it is possible to use the Dataspace Connector as a basis for the development of own software that is to be connected to an IDS data ecosystem.
Maturity Level	IDS-Ready and part of the IDS Graduation Scheme
License type	Open-source software
Features	The Dataspace Connector integrates the IDS Information Model and uses the IDS Messaging Services for IDS functionalities and message handling. The core component in this repository provides a REST API for loading, updating, and deleting resources with local or remote data enriched by its metadata. It supports IDS conform message handling with other IDS connectors and components and implements usage control for selected IDS usage policy patterns.
Adoption	The Dataspace Connector has been used in different projects and it is also part of the IDSA Reference Testbed[82]
External resources	» Project website[83] » GitHub repository AI.SOV on the Data Spaces Radar[84]

[82] https://github.com/International-Data-Spaces-Association/IDS-testbed
[83] https://international-data-spaces-association.github.io/DataspaceConnector/
[84] https://www.dataspaces-radar.org/radar/

2.2.2 GAIAboX

Name of the connector	GAIAboX®.IDS. BasicConnector
Logo of the connector or company logo	
Maintainer (company name)	nicos AG
Type of connector	Generic solution (proprietary software)
Short description	IDS BasicConnector, based on IDS-G specifications and ready to be equipped with additional protocols and/or application-functionalities.
Maturity Level	Up and running for and in nicos.testbed.IDS, following given IDS Certification criteria for components. Starting with Certification Trust Level 1 – Assurance Level 1 (Checklist Approach) and preparing for next level of certification.
License type	Closed-source Software
Features	» Uses IDS DAPS as identity provider » Ready for VC/VP » Usage Control (subset of IDS Usage Control, plus superset of well-known access control features) » Aligned to current IDS Information Model (IDS-IM) » Works as a Linked Data Platform (LDP, so aligned to W3C “solid”) » Aims to work with gRPC as an additional (but IDS-aligned) application protocol.
Adoption	Used by nicos.testbed.IDS as “Alice and Bob” Base for “Delegated Access Control Service” (expressed by DACL, the “Dynamic Access Control Language”) Base for Clearing House / Logging Service, too (Linked Data Notification, IDS Multipart Message, etc.).
External resources	Homepage will be provided in the next version of the Report.

2.2.3 MPAD-C

Name of the connector	MPAD-C (Manufacturing Process Anomaly Detection Connector)
Logo of the connector or company logo	
Maintainer (company name)	
Type of connector	Generic open-source solution
Short description	The technologies and tools for anomaly detection analysis are not always available within the company and 3rd party experts and algorithms are required to analyze this data. The IDS Connector can assure that this data is used only by the desired company agreeing to the terms established in the contract.
Maturity Level	TRL 4-5 – the solution presented is a prototype using the connector available in Github where we have implemented/tested different control capabilities and connection modes (direct, subscription ...).
License type	Open-source software
Features	Different control capabilities (temporarily, certificates ...) have been implemented, as well as connection modes (direct, subscription ...) creating different resources in the IDS Connector.
Adoption	QU4LITY project homepage[85]
External resources	The repository is currently closed for the Qu4lity consortium. Updates will be provided in the next versions of this Report.

[85] https://qu4lity-project.eu/

2.2.4 Teralab Connector

Name of the connector	TeraLab Connector
Logo of the connector or company logo	
Maintainer (company name)	TeraLab
Type of connector	Generic open-source solution
Short description	Test connector used to get familiar with IDS and interact with EUHubs4Data partners. It is based on the Dataspace Connector[86] (v8.0.2).
Maturity Level	TRL 3 – experimental proof of concept
License type	Proprietary
Features	» RAM Version: 3.0 » Info Model version: 4.2.7 » Protocol: HTTPS / multipart » Usage Control Capabilities: in line with the Dataspace Connector v8.0.2
Adoption	TeraLab Marketplace: Enabling data to move between the Marketplace and the connector using a back-end server.
External resources	» TeraLab Marketplace[87] » Code repository: internal (protected in a private network) » TeraLab Connector URL[88]

[86] Dataspace Connector repository: https://github.com/International-Data-Spaces-Association/DataspaceConnector/blob/main/LICENSE
[87] https://marketplace.teralab-datascience.fr/home
[88] https://ws37.tl.teralab-datascience.fr:30089

2.2.5 WeTech Connector

Name of the connector	WeTech Smart Data Connector
Logo of the connector or company logo	
Maintainer (company name)	WeTech Holding Co., Limited
Type of connector	N.A.
Short description	With the standard data usage strategy and asymmetric encryption technology defined in IDS, this connector achieves safe and reliable data transmission between the data sharing parties, and the implementation of the data provider's policies in the control of data usage time interval, usage times, usage methods and other policies. It can be applied to the sharing, use and control of important official documents, finance data, and market or business opportunities etc. between internal departments of large enterprises. A big tech firm in China has been using the connector, and its reliability has been proven.
Maturity Level	Preparing for IDS Certification (Trust Level 1 Assurance Level 2)
License type	Closed-source software
Features	Technological stack: Java, IDSCP, Personal Host
Adoption	Cross-border data sharing for a major Chinese telecom operator
External resources	

3 Additional initiatives and promising emerging solutions

In addition to the existing IDS-based data connectors described above, other approaches also support data sharing in data-driven business ecosystems and data spaces. The diversity of data sharing requirements, all based on confidentiality, regulatory aspects, technology limitations and more, leaves room for additional initiatives and promising (new) technologies. To realize the full potential of the available data, all data sharing approaches need to be interoperable – therefore IDSA is building a global standard for data connectors, gradually including other technologies and concepts. As this is the project of many years, we will conduct an ongoing assessment, and continuously update this section with further information and items on the list:

- OKP4 Protocol: OKP4 is a domain-specific layer-1 dedicated to trust-minimized data sharing. The blockchain orchestrates assets shared by participants in the Data verse: data, algorithms, software, storage and computation to enable a new generation of applications. Any contributor earns rewards thanks to these new value chains. For more information visit their website[89]
- Ocean Protocol: The Ocean Protocol is a comprehensive framework for data services in crypto ecosystems. Based on crypto tokens it provides mechanisms for smart contracts, marketplaces, and compute 2 data. It is available as open source. For more information visit their website[90].
- Ocean Provider: More detailed information is provided here below:

[89] https://okp4.network/
[90] https://docs.pontus-x.eu/

Ocean Provider: solution overview

Name	Ocean Provider
Maintainer	BigchainDB GmbH, Ocean Protocol, deltaDAO AG
Peculiarity	The Ocean Provider acts as an access controller and proxy controlling access to data services and can be compared to other connectors as the component responsible for access management. It leverages audit trials and identity management components to decide if a consumer or process shall receive access to a connected resource for further processsing or download. The fine-grained access controls provide explicit access control options with the use of access tokens and SSI verifier solutions by means of i.e., a keycloak integration. Only users with valid access tokens and credentials can access certain resources or trigger the orchestration of Compute-to-Data processes. The access controller allows a wide variety of data sources, besides infrastructure and software services for computation. It allows the provisioning of data from static data sources (files), decentralized data sources (IPFS, Arweave), databases and APIs. The Ocean Provider performs encryption/ decryption of the asset metadata, permission checking for consumption flows, data streaming, initiation of Compute-to-Data flows and offers multichain support for any public or private EVM-compatible blockchain network.
More Information	Pontus-X documentation[91] Software documentation[92]

Solution Details

Type	A generic open-source solution
Maturity	TRL Level 8-9 (used in production)
Portability	Agnostic
License	Open-source[93]
IDS Certification	No
Adoption Examples	Gaia-X Lighthouses (EuProGigant, Gaia-X 4 Future Mobility), Pontus-X ecosystem for Gaia-X, Future Mobility Marketplace, COOPERANTS, Airbus Defense and Space, CrossAsia Catalogue State Library of Berlin, Acentrik,
Adoption Examples (cont.)	Clinical Insights Exchange, Unversity de Lleida Agriculture Dataspace, deltaDAO marketplace, Energy Share Marketplace, OVAL Open Validation Platform, FELT Labs, GX4M Federated Analytics, EuProGigant Federated Analytics

[91] https://docs.pontus-x.eu/
[92] https://docs.oceanprotocol.com/developers/provider
[93] https://github.com/oceanprotocol/provider/blob/main/LICENSE

Access & Usage Control

Access control	Yes
Type	» Other (We support data sources protected by Basic Auth and API Keys behind the Ocean provider, but what we use to enable access controls is best summarized as “Web3 Authentication) » Layer 1: Identity o Web3 authentication leverages a user’s private key to generate a cryptographic signature as proof of ownership of a specific public key (address). Applications or services then verify this signature to authenticate the user, eliminating the need for traditional username/password systems and relying on the inherent security of blockchain private/public key pairs. In addition to that address white- and blacklists are used to manage access on the individual service level. Optionally we can replace the layer of cryptographic signature with Auth Tokens. » Layer 2: Contracting o Service providers and consumers can engage through ERC20 access tokens. ERC20 access tokens can be used to access a data service and leave an audit trail / immutable event log. This logged spending event will be used as a contractual basis for access through the Ocean provider (access controller), enabling access for the identified consumer, within the boundaries set by the associated license terms and conditions.
Support of Usage Control	Yes
Usage Control Policies	» Data Consumer » Application inside a Connector » Time Interval » Duration » Purpose » Data Sale Contract » Data Rental Contract » Log Data Usage Information » Inform a participant about the Data Usage

Communication

Communication Protocol	HTTPS, Negotiations based on OCEAN Protocol

Transfer Protocol	Out-of-band utilizing data planes without determined protocol bindings (data planes to be added)
User Interface	
Graphical user interface	Yes
Type	» for users » for management » for administration
Identity Management	
Identity management supported	Yes
Type	Decentralized (SSI)
Information Model	
IDS Information Model	No
Supported version of IDS Information Model	-
Vocabulary	
Supported	No
Type of Vocabulary provided	-
Integration	
Integration with Catalogue/Meta Data Broker	Yes
Catalogue/Meta Data Broker type	Ocean Aquarius (meta data) / Ocean Subgraph (transaction data)
Integration with Clearing House	No
Clearing House type	-

4 Other technologies contributing to trustworthily share data

Data sharing in data spaces is built on more than the use of data connectors in distributed networks. A soft data infrastructure based on centralized or decentralized essential services is the foundation for data sharing. This is not just technology put into practice, but it provides a frame for solutions based on the BLOFT thinking (business, legal, operational, functional, technological) that span data spaces. Additionally, it makes a difference if the data to be shared is personal data or not, and whether the data is shared by an organization, a service or an individual. Various initiatives and approaches work on these aspects. We will list some of them below and continue to assess and expand on them.

- Gaia-X trust framework[94]
- The Eclipse XFSC[95] (Cross Federation Services Components) formerly known as GXFS
- iShare trust framework[96]
- MyData Operators[97]
- SOLID[98]

Data connectors and the soft data infrastructure do not aim to reinvent the wheel, but to use common standards and frameworks and combine them into a comprehensive solution. Important standards to consider are for the realization of identity and access management, claim management, data and data contract policies. Some of the relevant standards are listed below:

- The W3C Tech Stack:
  - RDF[99]
  - ODRL[100]
  - DCAT[101]

[94] https://gaia-x.eu/gaia-x-framework/
[95] https://projects.eclipse.org/projects/technology.xfsc
[96] https://ishare.eu/
[97] https://oldwww.mydata.org/mydata-operators/
[98] https://solidproject.org/
[99] https://www.w3.org/RDF/
[100] https://www.w3.org/TR/odrl-model/
[101] https://www.w3.org/TR/vocab-dcat-3/

5 Conclusion

The data connector report is a comprehensive guide that explains what data connectors are, why they are essential for data spaces, and which aspects to consider making them interoperable. It also provides a clear and comprehensive overview of the different types of data connectors, their features and adoption scenarios. Since the September version, more information on the connectors has been added to provide additional details on their technical features, such as type of identity management, access control, usage control, protocols supported. This allows not only for a more accurate and comprehensive insight of the different connectors, but it also paves the way for future comparisons, taxonomies, and analysis on how the different connectors evolved. The Report also showcases other emerging solutions and technologies for data spaces, highlighting the role of IDSA and other relevant initiatives in this context and fostering a shared vision for future alignment and interoperability.

Some exclusive insights can be derived from a first analysis of the information provided in this Data Connector Report. First of all, among the 31 connectors described in 2 Implementations of data connectors, 13 connectors are reported to be open source, two partially open source and 16 closed source. Four major development streams for data connectors can be identified. The first one is the Eclipse Dataspace Components, which serves as a foundation for seven different connector variants. The second one is the Dataspace Connector, which is used as a foundation in seven connector variants. The third one is the TNO Security Gateway (TSG), which is used as a basis by two different connectors. The fourth one is the TRUE Connector, which serves as a foundation for one additional connector. Beyond this, the Report contains nine unique variants of data connector implementations.

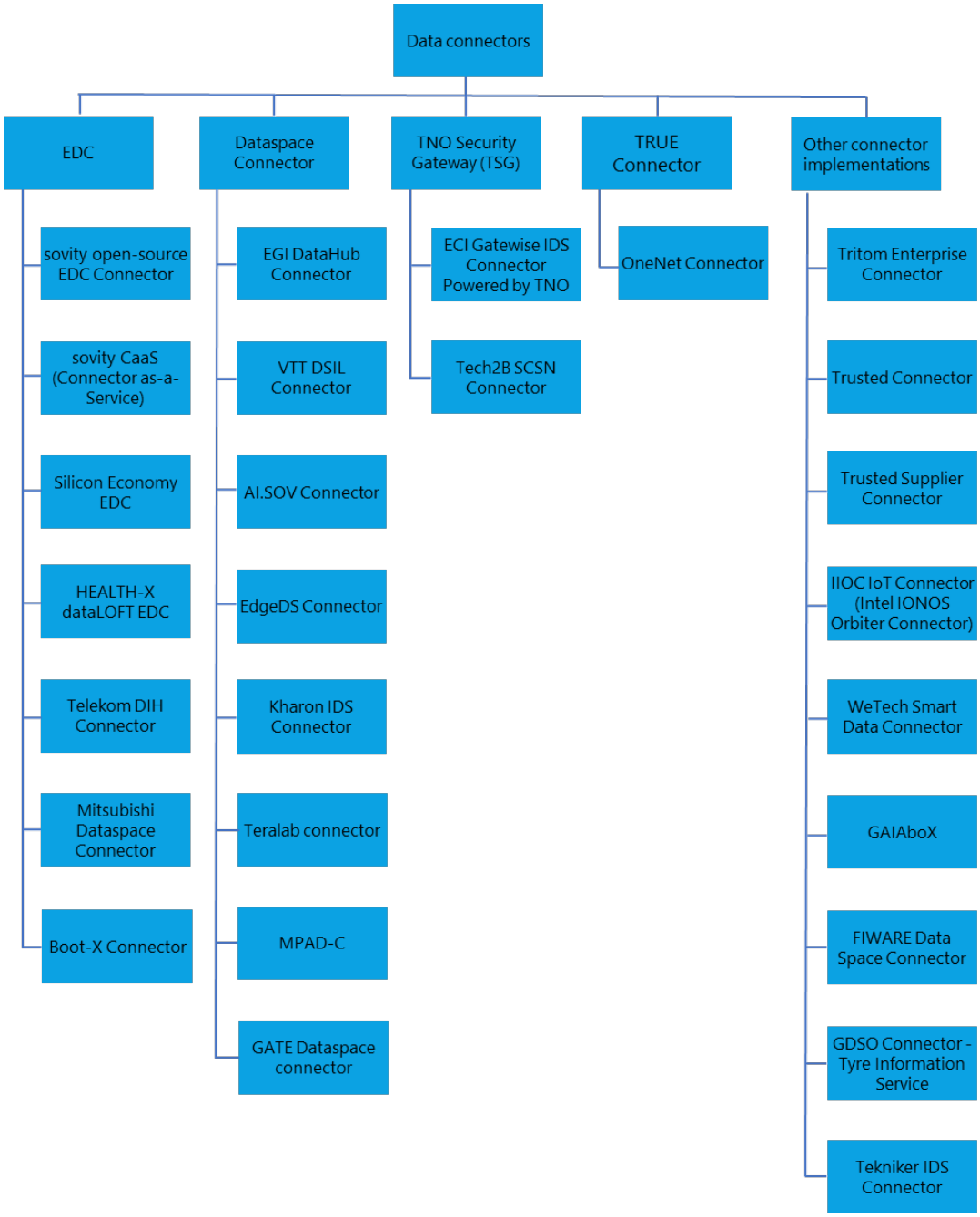


Figure 5 Data connector development streams

In addition to the listed data connectors, three emerging technologies have been identified, which are not qualified yet as data connectors.

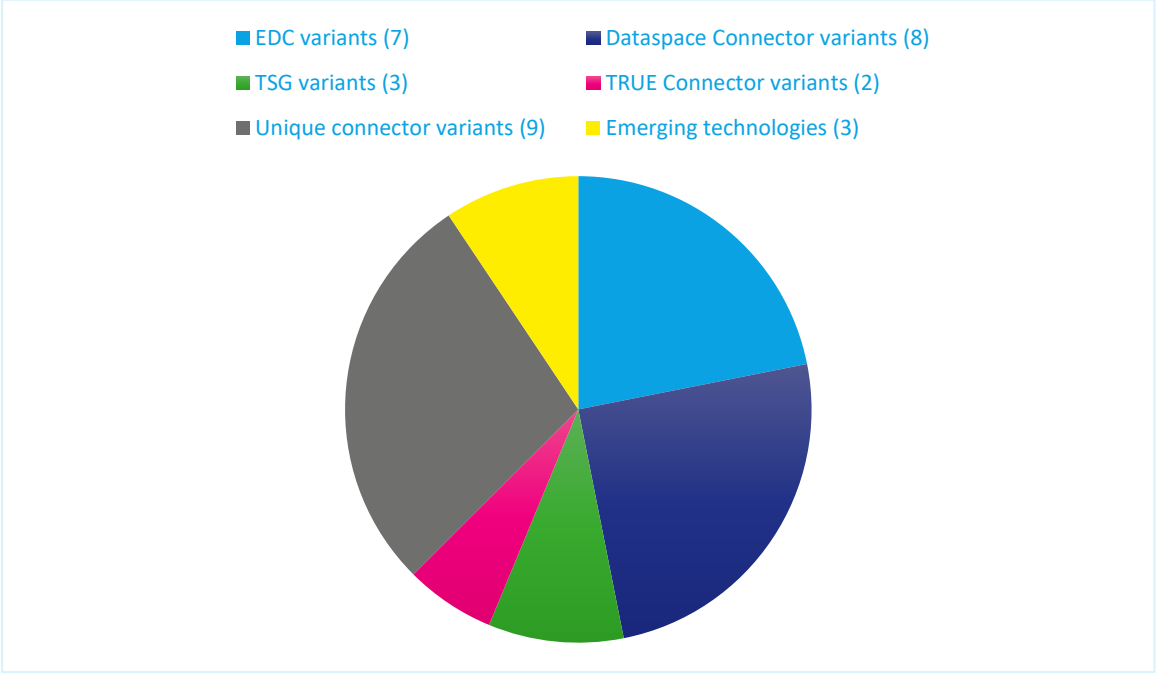


Figure 6 Number of connector variants

The above listed connectors support different identity management mechanisms: based on the information available[102], 12 connectors support X.509, three support did:web, four SSI, three support other identity management mechanisms and eight do not support any.

Regarding IDS Certification[103], two data connectors have completed the IDS Certification process. They are the Telekom DIH connector by t-systems and the VTT DSIL Connector. They have both been certified with the Concept Review certification, respectively in December 2023 and February 2024. The IDS Certification ensures that the connector meets the security and functionality requirements defined by the IDSA Working Group Certification. This milestone marks, therefore, a significant step towards market-ready data spaces, paving the way towards interoperability and making the life of end users easier.

"Witnessing T-Systems and VTT obtaining the world's first IDS Certification for their IDS connectors is a momentous occasion. This achievement not only signifies a crucial step in standardizing data spaces but also highlights our dedication to fostering secure, interoperable solutions that contribute to the sustainable development of the data economy."
Sonia Jimenez, Director Data Space Technology | IDSA

Some other companies are currently undergoing the process to certify their connectors and updates will be included in the next issues of the IDSA Data Connector Report.

[102] The connectors listed in 2.2 Connectors with latest updates in May 2023 do not provide information on identity management
[103] https://internationaldataspaces.org/offers/certification/

The Data Connector Report is a living document that aims to provide a comprehensive picture of the state-of-the-art and the future trends of data connectors in data spaces. It is not meant to be only informative, but also interactive since feedback and suggestions from the readers is key to its evolution and refinement. To contribute, feel free to contact the IDSA via this new form[104], via which you can provide feedback, add a connector, or update information on a connector that is already listed in the document.

[104] https://forms.office.com/pages/responsepage.aspx?id=NNZGs_usx0K9RPFVfuibG-lZOvXJhFhPq3BHErEl221UMzFWUEhEU1JLM1U2S0ozVkxZR1gxVFFQWC4u

CONTACT

Head Office

INTERNATIONAL DATA SPACES ASSOCIATION

Emil-Figge-Str. 80
44227 Dortmund | Germany

phone: +49 231 70096 501
mail: info@internationaldataspaces.org

WWW.INTERNATIONALDATASPACES.ORG


international-data-spaces-association