Fraunhofer

FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG

Deliverable 1.1

Business Architecture for the Industrial Data Space

Revision History

Version	Date	Name, Institute	Description
1.0	14.06.2016	Christoph Quix, FIT	Initial version
1.1	15.08.2016	Christoph Quix, FIT	Added statements about certification, clearing house

Inhalt

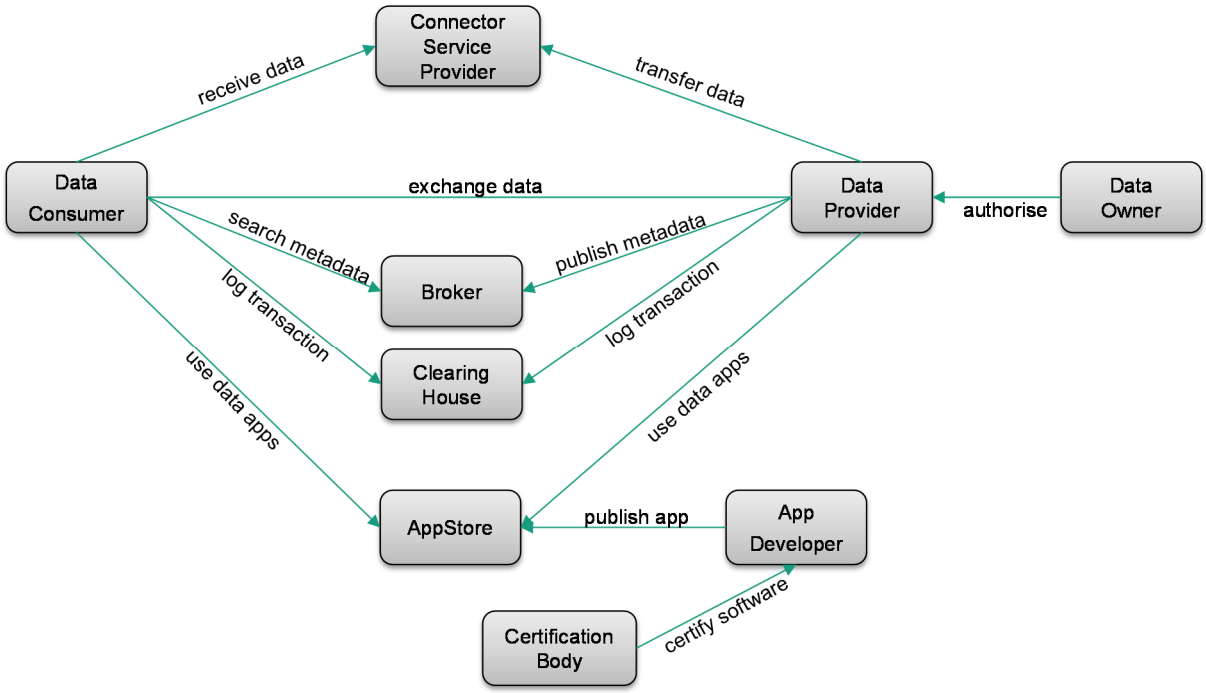
1 Purpose of this document

The Industrial Data Space (IDS) enables a reliable exchange of data with common rules for participating organisations. The IDS will be based on an open architecture in which different partners can collaborate with each other in a peer-to-peer like architecture without a central control. Participation in the IDS does not require the use of a specific software provided by certain vendors, only the interfaces and protocols for data exchange need to be implemented or provided by participating parties. This implies that a service in the IDS can be provided by different organisations; this includes also general services in the IDS infrastructure such as a metadata broker or a digital distribution platform (often known as "AppStore").

The goal of this document is the identification of the different roles in the IDS from a business perspective and the modelling of the processes in which these roles are involved. This should contribute, on the one hand, to the business models which might be applied by the participators in the IDS. On the other hand, the process models can be used the verify the technical architecture of the IDS, e.g., whether all required interfaces between the IDS components have been specified and whether all required information for running the business process is available for the IDS components.

2 Roles of IDS Participants

The following figure gives an overview of the roles in the IDS.



Each of these roles will be described in the following in detail with the related activities. Based on this abstract description of the activities, section 3 will provide detailed business process models for the processes in the IDS.

The certification of the participating organisations which represents the different roles is discussed in detailed in deliverable 5.1 of work package 5 (Certification). For certain roles, it will be necessary that the organisations themselves will be certified in addition to the used software. This applies especially to central roles such as the AppStore or the Clearing House which should act as trusted intermediaries.

2.1 Data Owner

The data owner is legally the owner of the data. The owner might be different from the data provider in the case that the data is technically managed by a different entity than the data owner. An example is a company which uses an IT service company for data management. Usually, the roles of the data owner and the data provider will be played by the same organisation.

2.1.1 Activities

2.1.1.1 Authorise Data Provider

The only activity of the data owner is the authorisation of a data provider to publish the data owned by the data owner. The authorisation should be documented in a contract that includes a policy describing the permissions granted to the data. The contract is not necessarily a legal paper document, it can be also established by electronic means.

2.2 Data Provider

The data provider is an organisation that manages data to be published in the IDS. The data provider usually owns the data, but it might be also authorised by the data owner.

2.2.1 Activities

2.2.1.1 Publish Metadata at Broker

The data provider needs to use the broker to publish the metadata. To be able to do this, the provider first needs to describe the data according to an IDS metadata model.

2.2.1.2 Exchange Data with Data Consumer

The data exchange is the core activity of the IDS.

2.2.1.3 Log Transaction Details at Clearing House

After a data exchange has been performed (completely or partially), the successful completion of the transaction from the viewpoint of the data provider should be logged at a clearing house (for billing, conflict resolution, etc.).

2.2.1.4 Use Data Apps

Data providers can use Data Apps to enrich, to transform, or to improve their data in some way. Data Apps are specific applications that can be integrated into the data workflow of an IDS connector.

2.2.1.5 Transfer Data to a Connector Service Provider

If the data provider does not deploy an IDS connector by itself, the data provider can transfer the data to a service provider which hosts IDS Connectors for other organisations. The service provider plays then the role of a data provider and can perform the aforementioned activities.

2.3 Data Consumer

The data consumer is an organisation that receives data from a data provider in the IDS. From a functional or business process modelling point of view, it is the mirror entity to a data provider. Therefore, the activities are similar to the activities of the data provider.

2.3.1 Activities

2.3.1.1 Search Metadata at Broker

Before a connection to a provider can be established, the data consumer needs to retrieve the metadata of the peer from the broker. It might be also the case that the connection information of the data provider is already known; then, the metadata can be retrieved directly from the data provider.

2.3.1.2 Exchange Data with Data Provider

The data exchange is the core activity of the IDS.

2.3.1.3 Log Transaction Details at Clearing House

After a data exchange has been performed (completely or partially), the successful completion of the transaction from the viewpoint of the data consumer should be logged at a clearing house (for billing, conflict resolution, etc.).

2.3.1.4 Use Data Apps

Data consumers can use Data Apps to enrich, to transform, or to improve the data received from the data provider (or also their own data) in some way. Data Apps are specific applications that can be integrated into the data workflow of an IDS connector.

2.3.1.5 Transfer Data to a Connector Service Provider

If the data consumer does not deploy an IDS connector by itself, the data consumer can transfer the data to a service provider which hosts IDS Connectors for other organisations. The service provider plays then the role of a data consumer and can perform the aforementioned activities.

2.4 Broker

The broker is a metadata repository that provides information about the data sources available in an IDS network. There can be multiple brokers (e.g., for different domains) as the role of the broker is central but non-exclusive. The IDS Whitepaper also assigned clearing activities to the broker; however, as clearing is a very different activity from maintaining a metadata repository, we decided to separate the roles of broker and clearing house in this document. In practice, the roles of broker and clearing house could be still performed by the same organisation.

2.4.1 Activities

2.4.1.1 Receive Metadata from Data Provider

The broker needs to provide an interface to receive metadata from data providers. The metadata should be stored in some internal repository so that it can be later queried in a structured way. The core of the metadata model needs to be specified by the IDS, but a broker can extend the metadata model to manage additional metadata elements.

2.4.1.2 Provide Search Interface for Metadata

It should be possible to query the stored metadata in a structured way. The query interface should be standardised by the IDS, but a broker can provide specific extensions. After the broker has provided the metadata about a data provider to a data consumer, the broker is not anymore involved in the data exchange.

2.5 Clearing House

The clearing activities have been separated from the broker as these activities are technically different from maintaining a metadata repository. As stated above, it might be still possible that the roles clearing house and broker are played by the same organisation, as they need to act as a trusted, intermediate entity between data provider and data consumer.

2.5.1 Activities

2.5.1.1 Log Transaction Details from Data Provider and Data Consumer

After a (part of a) data exchange has been completed, both data provider and data consumer need to confirm the transmission and the reception of the data by logging the transaction at the clearing house. Based on the logged data, a billing of the transactions can be performed. The log information can also be used to resolve conflicts (e.g., whether a data package has been received or not).

2.5.1.2 Report on Performed Transactions

The clearing house should also provide reports on the performed (logged) transactions for billing, conflict resolution, etc.

2.6 Connector Service Provider

Data providers and data consumers can delegate the technical interface to the IDS to an external organisation that hosts IDS connectors and provides them as a service.

2.6.1 Activities

2.6.1.1 Send and Receive Data from Data Providers and Data Consumers

The data to be send to or the data which has been received from the IDS has to be transferred to the data provider or data consumer, respectively. This data transfer is done outside of the IDS network and therefore not under the control of the IDS. The service provider could use specific system connectors to establish a connection to a data management system of data provider or data consumer.

2.6.1.2 Activities as Data Provider or Data Consumer

If the Connector Service Provider acts as data provider or as a data consumer, it can perform the same activities as defined for these roles.

2.7 App Store

The App Store in the IDS provides applications and specific (meta)datasets (e.g., vocabularies, ontologies, reference data models, etc.) that can be deployed in IDS connectors to enrich the data processing workflows. Content in an AppStore should be certified by a certification body, according to the certification procedures specified by the IDS. Details about the certification process can be found in a separate document for the certification in the IDS.

2.7.1 Activities

2.7.1.1 Manage Data Apps

The AppStore is responsible for managing Data Apps that have been provided by app developers. App developers should describe their apps with metadata according to a metadata model to be specified by the IDS. The AppStore should provide interfaces for publishing and retrieving apps and their metadata.

2.8 App Developers

App developers provide certified apps to be used in IDS connectors. They need to request a certification from the certification body.

2.8.1 Activities

2.8.1.1 Publish Apps

Apps need to be published at an AppStore so that they can be deployed by data consumers or data providers in an IDS connector. Apps have to be certified before publication. Metadata should describe the app (e.g., its functionality and the interfaces).

2.8.1.2 Request Software Certification

App developers need to request the certification for their apps from a certification body.

2.9 Certification Body

The certification process is specified in a separate document on the IDS certification process (see deliverable 5.1 of work package 5).

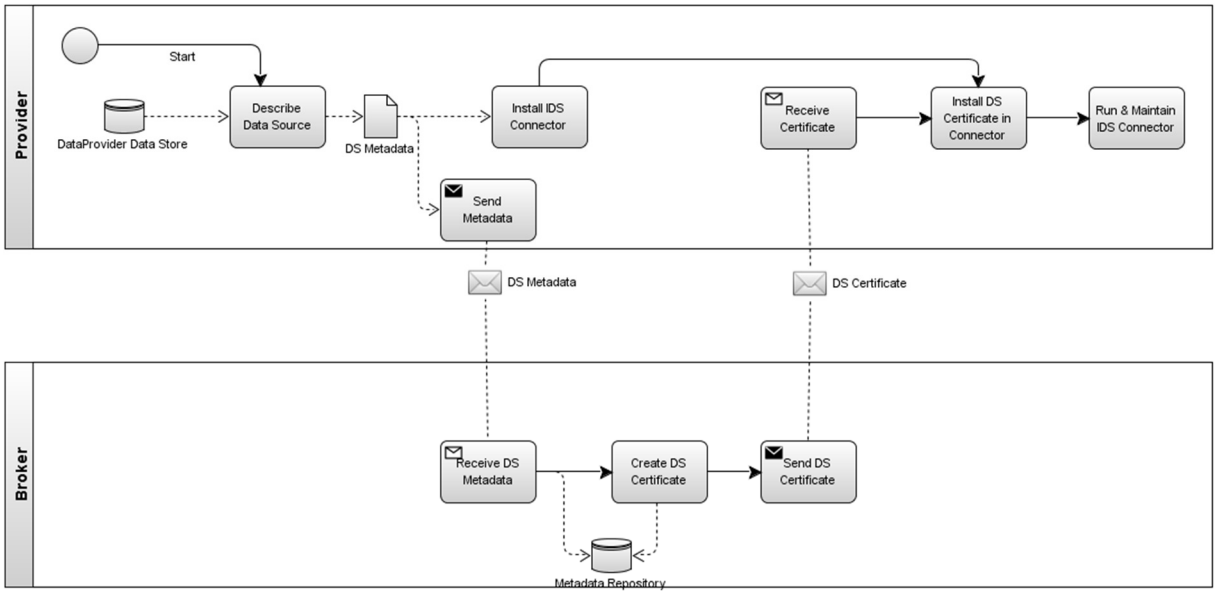
3 Basic Business Processes

The business processes have been modelled in BPMN (Business Process Model and Notation) using the Yaoqiang BPMN Editor (http://bpmn.sourceforge.net/).

3.1 Provide Data

This includes the following activities described above:

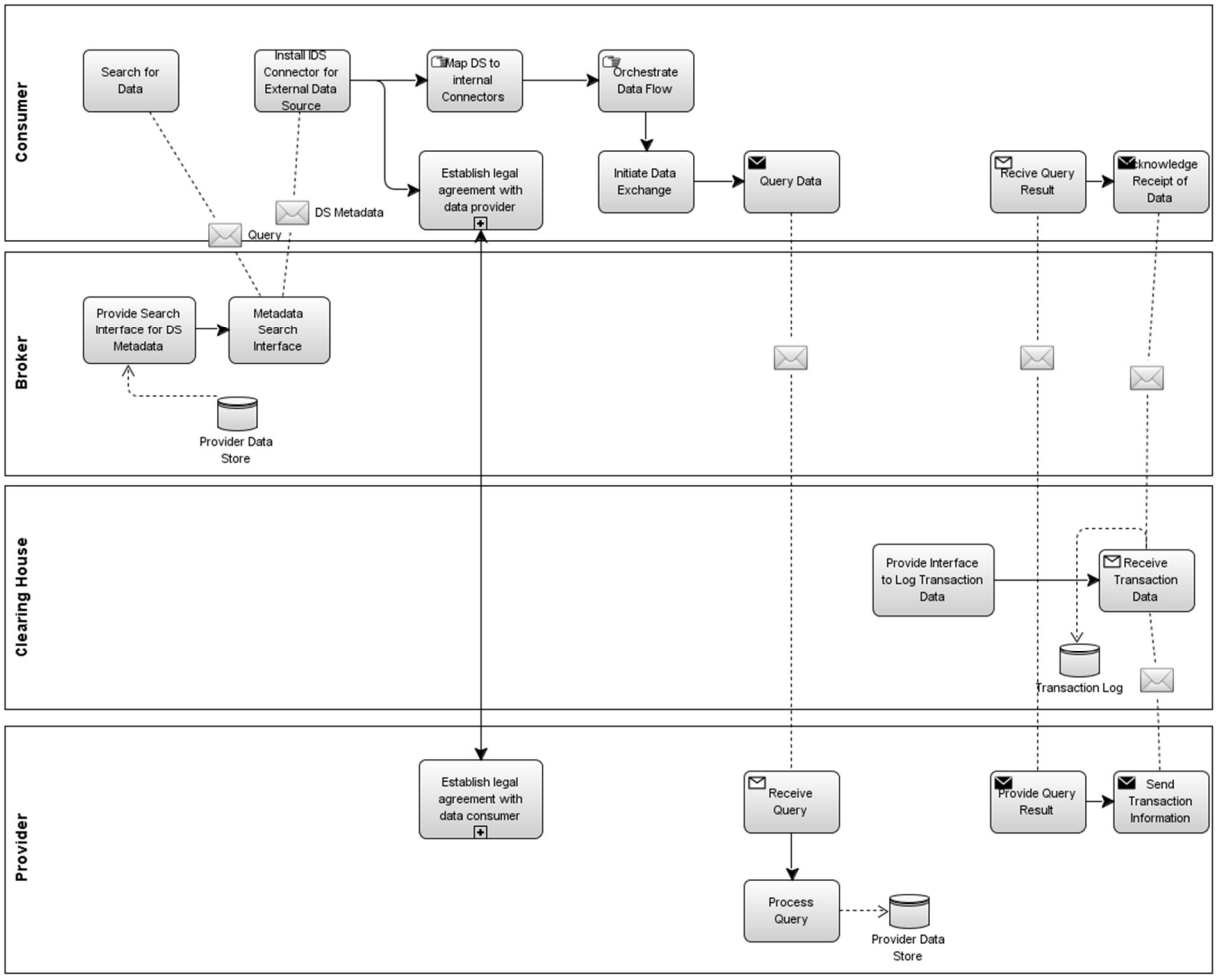
- Data Provider
  - Publish Metadata
- Broker
  - Receive Metadata from Data Provider



3.2 Data Exchange

This process includes the following activities described above:

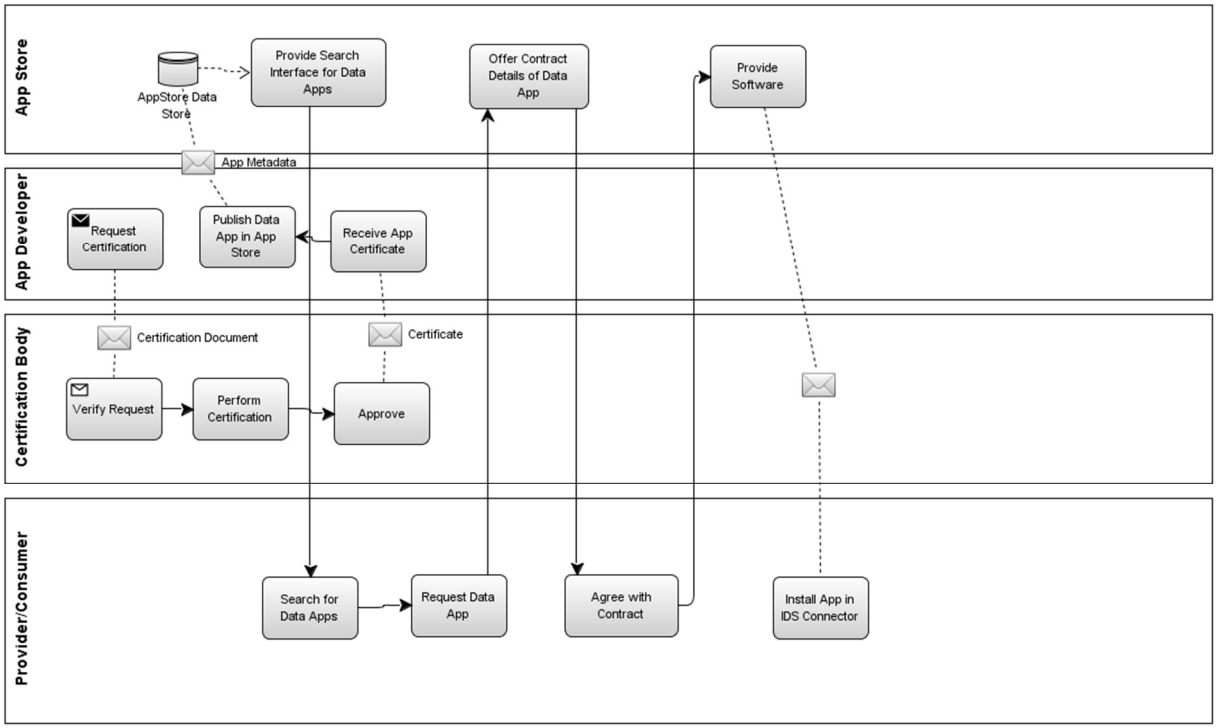
- Data Provider
  - Exchange Data with Data Consumer
  - Log Transaction Details at Clearing House
- Data Consumer
  - Search Metadata at Broker
  - Exchange Data with Data Provider
  - Log Transaction Details at Clearing House
- Broker
  - Provide Search Interface for Metadata
- Clearing House
  - Log Transaction Details from Data Provider and Data Consumer



3.3 Publishing and using Data Apps

This process includes the following activities described above:

- App Developers
  - Publish Apps
  - Request Software Certification
- App Store
  - Manage Apps
- Certification Body
  - Certify software
- Data Provider/Consumer
  - Use Apps


App Store
AppStore Data Store
Provide Search Interface for Data Apps
Offer Contract Details of Data App
Provide Software
App Metadata
App Developer
Request Certification
Publish Data App in App Store
Receive App Certificate
Certification Body
Certification Document
Certificate
Verify Request
Perform Certification
Approve
Provider/Consumer
Search for Data Apps
Request Data App
Agree with Contract
Install App in IDS Connector

4 Additional Roles in the IDS

Some roles which are relevant for the IDS have not been covered in this document because they are not directly involved in the processes related to the IDS. These roles include

- *Developers of IDS software* (e.g., connectors, broker software, clearing software, etc.). These developers will interact with organisations playing the corresponding roles in the IDS, but the contract for using the software are not under the control of the IDS.
- *Data Service Providers* offer additional services to improve data in the IDS. Examples for such services are data analysis, data integration, data cleaning, or semantic enrichment. These service providers could act as data provider and data consumer at the same time, e.g., they receive data as a data consumer from some data provider in the IDS, apply their value-added service, and then offer the data in the IDS as a data provider.
- The role of the *IDS e.V.* needs to be clarified. It could act as the organisation that formally approves the specifications and standardisation documents. If not, than some other organisation should be assigned for that role.