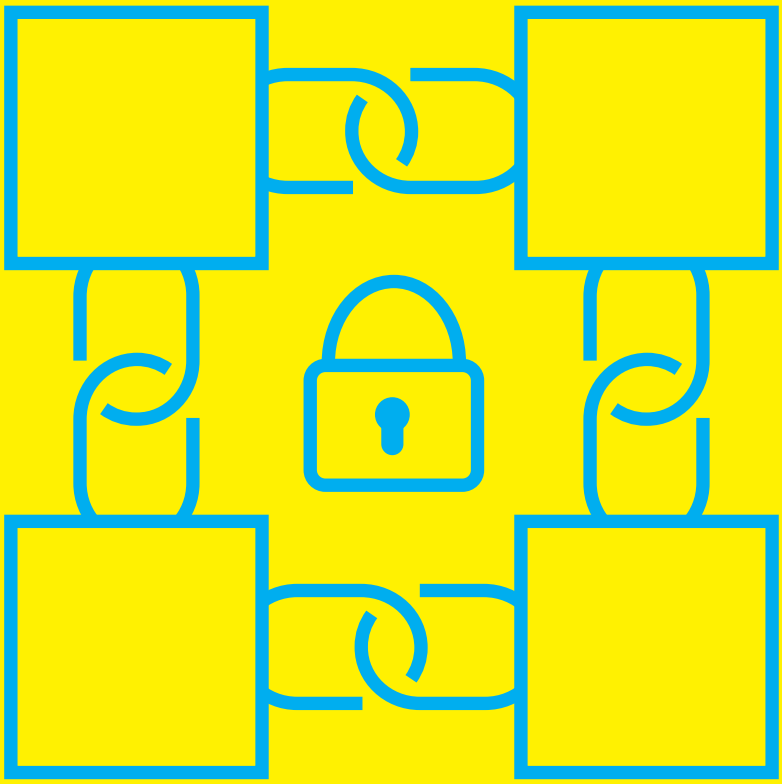
INTERNATIONAL DATA SPACES ASSOCIATION

White Paper | Version 1.0 | April 2020

Specification: IDS Clearing House



- ○ Position Paper of members of the IDS Association
- ○ Position Paper of bodies of the IDS Association
- ○ Position Paper of the IDS Association
- ● White Paper of the IDS Association

Publisher

International Data Spaces Association
Anna-Louisa-Karsch-Str. 2
10178 Berlin Germany

Editor

Sebastian Steinbuss,
International Data Spaces Association

Corresponding Author

Sebastian Bader, Fraunhofer IAIS

Authors & Contributors

Dr. ir. Harrie Bastiaansen, TNO

Georg Bramm, Fraunhofer AISEC

Juan Ceballos, T-Systems

Mark Gall, Fraunhofer AISEC

Maarten Kollenstart, TNO

Cite as

Steinbuss S., Bader S., et al. (2020):
Specification. IDS Clearing House.
International Data Spaces Association.
https://doi.org/10.5281/zenodo.5675765

Contents

1 Introduction

1.1 Goals and Scope of the document

This document describes minimum requested requirements to be met by the IDS Clearing House as one of IDS' core components/roles supporting data exchange transactions. Technically speaking, the IDS Clearing House is a component that is implemented on top of the IDS Connector.

1.2 Purpose of the document

The document contains the technical specification of the IDS Clearing House. It thereby constitutes the basis regarding the certification criteria to be met by the IDS Clearing House.

1.3 Related Documents

The following public documents are related to this document and should be considered as important:

- IDS-Reference Architecture Model 4.0[1]
- IDS Certification Scheme 2.0[2]
- IDS Certification Criteria[3]
- IDS and Blockchain[4]
- IDS-G[5]

The following internal documents are related to this document:

- IDS Communication Guide
- IDS Handshake

[1] https://www.internationaldataspaces.org/ressource-hub/publications-ids/
[2] https://www.internationaldataspaces.org/ressource-hub/publications-ids/
[3] https://www.internationaldataspaces.org/ressource-hub/publications-ids/
[4] https://www.internationaldataspaces.org/ressource-hub/publications-ids/
[5] https://github.com/International-Data-Spaces-Association/IDS-G

2 Motivation

The IDS Clearing House acts as an Intermediary in the IDS ecosystem. This means that the IDS Clearing House mediates between a Data Provider (DP) and a Data Consumer (DC), making sure both parties meet their contractual obligations, such as

- the DP sharing data with the DC according to Usage Contracts and Data Usage Policies defined; or
- the DC using data according to Usage Contracts and Data Usage Policies defined, and effecting payment to the DP as agreed.

For each data exchange transaction, the DP attaches metadata to the data requested by the DC, specifying e.g. data usage restrictions, pricing information, payment entitlement, time of validity, etc. This way, the DP can specify a Data Usage Policy as deemed appropriate, making sure data sovereignty is guaranteed.

Please note: Although this document speaks of 'the IDS Clearing House', multiple instances of this IDS role can exist and federate. Such federation of several IDS Clearing Houses is not in the scope of this document though.

The IDS Clearing House is a trusted partner of both the DP and the DC. As in many cases the two parties may not have trust in each other (since they don't know each other and/or haven't done data exchange transactions with each other so far), the IDS Clearing House reduces risk and uncertainty on both sides. For example, if the DP agrees to provide data to the DC based on a Usage Contract, and there is no one else to verify and back the transaction, it may be possible that one party does not fulfill the contract (e.g. by not delivering the data as agreed or providing data of poor quality on the DP side, or by misusing the data or failing with payment on the DC side). Such transactional risk can be mitigated by involving the IDS Clearing House.

The IDS Clearing House provides two basic functions for all financial and data exchange transactions taking place in the IDS ecosystem: clearing and settlement on the basis of transaction logging. In IDS, the activities carried out by the IDS Clearing House are separated from other services, since these activities are executed at different stages of the lifecycle of the data-sharing support processes. Moreover, IDS Clearing House activities differ from other support services and Intermediary roles also from a technical perspective:

- The *Identity Provider* provides services to create, maintain, manage and validate identity information. These are fundamental services to avoid unauthorized access to data [see IDS-RAM 4.0].
- *Dynamic Trust Management (DTM)* provides services for continuous monitoring of network security and behavior. It shares information with the Dynamic Attribute Provisioning Service (DAPS) to notify each of the two participants in a data exchange transaction of the current level of trustworthiness of the other participant. Furthermore, it interacts with DAPS and the Identity Provider in cases in which it is necessary to reduce the level of trust assigned to a certain participant (e.g. in case of a security incident) [see IDS-RAM 4.0].
- *Policy Enforcement Points (PEP)* enforce data usage restrictions, since the system's actions need to be monitored and potentially intercepted by control points. These actions must be judged by a decision engine (i.e. a Policy Decision Point, PDP) for requesting permission or denial. The PDP is implemented for transactions executed via the IDS Clearing House [see IDS-RAM 4.0].

- The *IDS Meta Data Broker* is a service for publishing and searching metadata of connectors and resources between International Data Spaces Participants. It provides a collection of additional functionalities for indexing services in order to effectively and efficiently respond to queries and present known Connectors and other resources and interfaces for Users or IDS-Messages to ensure access to the stored information [see IDS-RAM 4.0].

The IDS Clearing House interfaces with, and relies upon, the support services described above, in order to provide the functions for managing data-sharing and payment processes after a mutual agreement has been made by the DP and the DC (i.e. managing actual data-sharing transactions in accordance with data-sharing agreements including logging and reporting thereof). It plays an important role in providing legal, financial and technical support functions; i.e. functions for clearing (prior to a data exchange transaction) and for settlement (after a data exchange transaction).

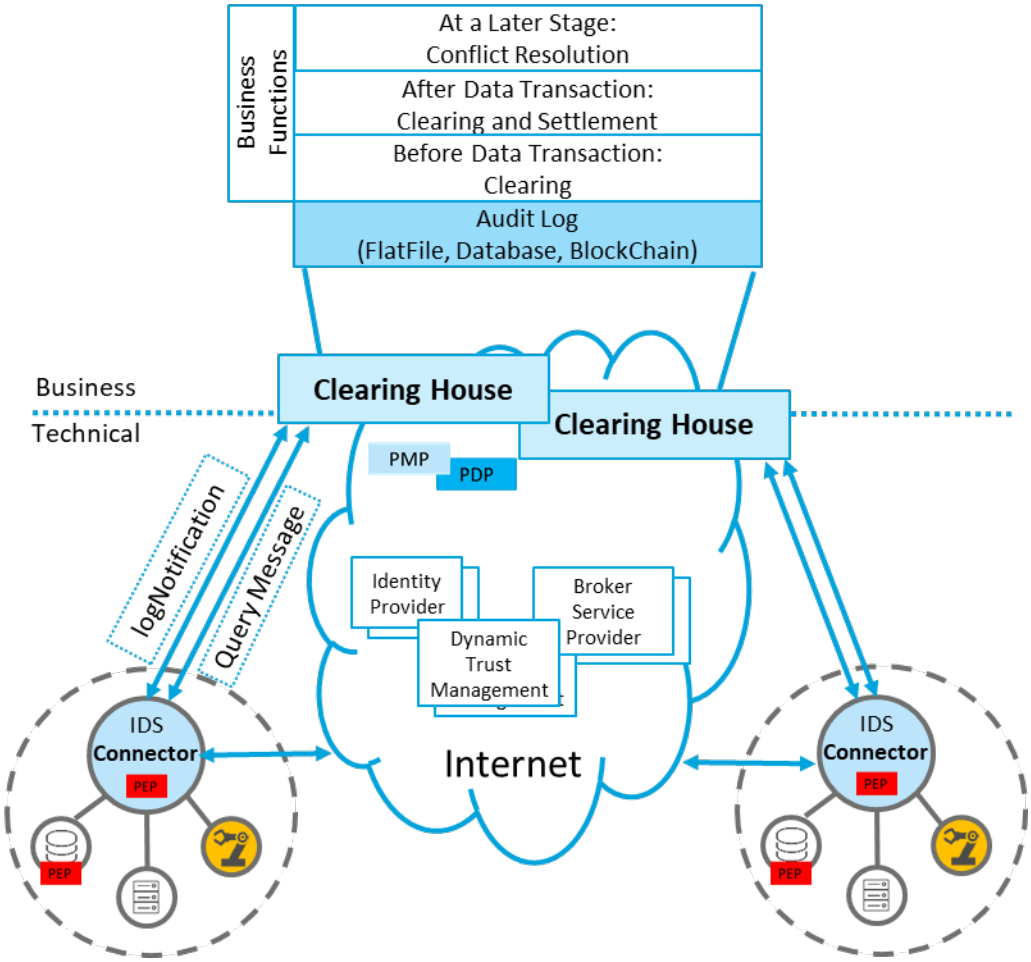


Figure 1: Logic and functions of the IDS Clearing House

Note: Even though from a technical perspective the functional range of the Broker Service Provider and of the IDS Clearing House could be implemented together, it is recommended to separate the two roles from each other, as this allows support of transactions that do not require a broker (i.e. DP and DC negotiate usage terms and conditions directly, but need a neutral party for clearance and settlement) and creates transparency (i.e. by separating negotiation and execution of transaction).

2.1 Purpose of the IDS Clearing House

As stated in the IDS Reference Architecture Model: '**Data sovereignty is about ˝nding a balance between the need for protecting one's data and the need for sharing one's data with others.**

It can be considered a key capability for companies to develop in order to be successful in the data economy'.

Within the IDS ecosystem and in alignment with the IDS service architecture, the IDS Clearing House provides a set of clearing and settlement functions, which are described in the following.

2.2 Clearing house functions

To protect the data provider's data, several activities should be supported that typically belong to the function set as provided by a clearing house:

Prior to sharing data: clearing functions.

An important function prior to data being exchanged is usage control. It provides the functions to enforce Data Usage Policies by means of a Usage Contract. In addition, a function for data control and release may be required, in order to ensure that also legal and financial conditions are met before data is exchanged (this can be compared to the function offered by a financial clearing house to support financial/stock brokering transactions, or to the notary function in real estate trading).

In addition to legal and financial functions, there may also be specific technical support functions that should be offered by the IDS Clearing House. One such function may be non-repudiation, meaning that the DC cannot deny having received the data, nor can the DP deny having sent the data.

Clearing functions (prior to sharing data):

- Clearing of data-sharing transaction:
  - Legal: Verifying Usage Contract and Data Usage Policy
  - Financial: Verifying payment conditions
  - Technical: Enabling execution of transaction and binding transaction to an instance of a data-sharing agreement and Usage Contract

During the data-sharing process: monitoring and logging functions

During a data-sharing transaction, the IDS Clearing House can be invoked for logging of metadata (audit proven, if necessary) and to query previously stored items, e.g. for data provenance tracking or data monitoring, as well as for discharging the data-sharing transaction.

Settlement functions (prior to and during data-sharing process):

- Discharging of data-sharing transaction
- Logging of transaction's metadata
- Tracing data provenance
- Monitoring and reporting of data transaction
- Auditing and tracking of data transactions for determining accountability and resolving possible conflict
- Billing and invoicing of data transactions

After sharing data: settlement functions

After the data has been exchanged, the administrative part of the transaction must be addressed, including aspects such as logging, billing, and invoicing. The Clearing House charges a fee for conducting these functions and for absorbing the risk of not fulfilling the contract between both parties.

Settlement functions (after sharing data, or in case of not sharing any data) for conflict resolution:

- Investigating claim on violation of Usage Contract and/or Data Usage Policy
- Enforcing action upon violation of Usage Contract and/or Data Usage Policy
  - Legal: Escalate to a court
  - Technical: Block a participant via Identity Provider or downgrade its degree of trust using DTM
  - Financial: Request financial compensation

The clearing house functions for clearing and settlement as listed above require metadata artefacts from other services . Table 1 lists and describes these metadata artefacts needed to execute the clearing house functions.

Data Transaction	Represents a specific instance of sharing primary data, including data request, data response, and associated processes for management and administration thereof; applied both to controlled sharing of datasets (e.g. inventory levels) and to sharing of data resulting from business transactions (e.g. data of a purchasing transaction)
Data-Sharing Agreement	Specifies conditions under which certain data will be shared; consists of Contractual Conditions and Usage Contract
Contractual Conditions	Combine Service Levels, Usage Contract, Legal Contract, and Commercial Contract
Usage Contract	Combines Access Control Policies and Usage Control Policies; expresses DP's internal (business) data-sharing policies and external (regulatory) policies
Access Control Policy	States which individuals, roles, and/or systems are granted access to data provided
Usage Control Policy	States how data may be used or distributed after access has been granted to individuals, roles, and/or systems
Service Levels	State quality parameters of data provided, such as completeness, accuracy, or timeliness
Commercial Contract	States commercial conditions under which certain data will be provided, including price of data and invoicing and payment conditions
Legal Contract	States legal aspects required for (or to avoid) conflict resolution (e.g. IPR conditions, applicable law, etc.)

Table 1: Metadata artifacts required for IDS Clearing House functions

2.3 Requirements regarding Business Service Architecture

For the implementation of an IDS Clearing House in the context of the IDS role and interaction model, the following requirements have to be taken into account:

Distributed implementation When sharing data, the Data Provider and the Data Consumer will be subscribed with the IDS Clearing House. The IDS Clearing House may be proposed, or requested, by one of the parties. The selection happens upon mutual agreement and implies that the IDS Clearing House is trusted by both parties. Under this model, the service architecture (API and functional architecture) should be standardized in order to ensure provider flexibility.

Business Service Orientation

Not only the data to be shared, but also the metadata artefacts required for the IDS Clearing House to execute its data-sharing support processes (see table 1), contain potentially sensitive information. Therefore, the Data Provider needs a well-defined business policy and appropriate technical means to protect this metadata. To allow the Data Provider to focus on its core business and minimize costs, and to maintain data sovereignty, outsourcing the enforcement of its Data Usage Policy to an external (trusted) clearing house might be an adequate approach. However, such an approach would require adequate service offerings regarding trust and data sovereignty on the part of this clearing house. Consequently, this should be done by means of a service-oriented business architecture. Such an approach would give Data Providers flexibility and agility in balancing manageability and cost efficiency of such outsourcing to external organizations against the increased risks of misuse of data and metadata.

Interoperability between various clearing houses and with other intermediary roles In a distributed and service-oriented approach, interoperability regarding the information exchange and interaction patterns between various clearing houses should be possible by design. An essential aspect is the extent to which connectivity of different clearing houses, and interoperability between clearing houses and other Intermediary roles (e.g. Identity Provider, Service Broker Provider, PEP, DTM), is needed, including the need for an interconnection architecture, protocol and/or API. In a distributed architecture, a hierarchical clearing house interconnection architecture, protocol, and/or API should be avoided by default.

3 IDS Clearing House in Relation to IDS-RAM Layers

3.1 Process layer

The process of interacting with the IDS Clearing House can follow two patterns: 1) clearing without direct confirmation of the remote party's Clearing House, and 2) clearing with confirmation of the remote party's Clearing House.

3.1.1 Clearing without con˝rmation

The process of interacting with the IDS Clearing House follows simple request-reply flow schemes, as shown in figure 2 and figure 3. TThe more difficult question is: When do these interactions take place, and what information do these requests and replies entail?

For the logging of messages, two points in the interaction with another IDS Connector can be identified:

1) the point where an IDS Connector receives a request from another IDS Connector, which ensures all incoming messages are logged before they are processed;
2) the point where an IDS Connector sends a request to another IDS Connector, which ensures all outgoing messages are logged.

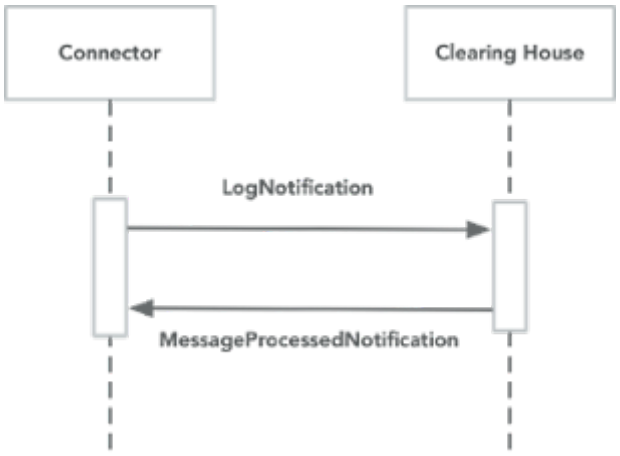


Figure 2: IDS Clearing House message logging process

The information that is shared with the IDS Clearing House can be split into three categories, which represent different levels of data sovereignty:

1) both message header and message payload;
2) only message header and a hash of message payload;
3) only a hash of message header and message payload combined.

The first category (i.e. sharing the complete message with the IDS Clearing House) may be undesirable in most cases, as oftentimes messages contain sensitive data that is not intended to be shared with a clearing house, but only between the Data Provider and the Data Consumer.

In contrast, both category 2 and category 3 use a model where parts of the original message are hashed. This creates a system where the IDS Clearing House is not able to decrypt the message, thus ensuring data sovereignty for both the Data Provider and the Data Consumer. However, this model requires the IDS Connector to safely store the message, so that it is available in case of a possible dispute between the parties. Furthermore, the original message belonging to the hash that is stored at the IDS Clearing House must be available to recreate the hash.

An alternative to hashing is encryption, where the message payload and/or the message header are/is encrypted by keys that the IDS Clearing House cannot decrypt without intervention of the Data Provider and/or the Data Consumer. This makes it needless for an IDS Connector to store the message locally; however, it increases traffic between the IDS Connector and the IDS Clearing House.

IDS Connectors must be able to specify what type of logging is allowed by the other party, which is specified by the Usage Contract.

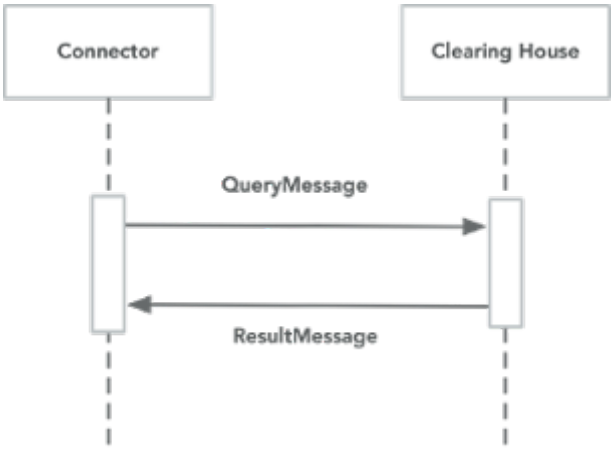


Figure 3: Clearing House query process

Querying the IDS Clearing House is done via ordinary query messages, this is where the IDS Clearing House may offer additional services.

Different IDS Clearing Houses must be able to communicate with each other (e.g. in case of a dispute between two parties). They may do this also by ways of offline interaction.

3.1.2 Clearing with con˝rmation

If the Data Consumer and the Data Provider use different entities to act as their respective Clearing House, the process becomes more difficult (especially when trying to prevent interactions between the two IDS Clearing Houses, as they might not have a direct relationship with each other).

Figure 4 shows the process of using evidences of the interaction between the Data Consumer and/or the Data Provider and their respective IDS Clearing House.

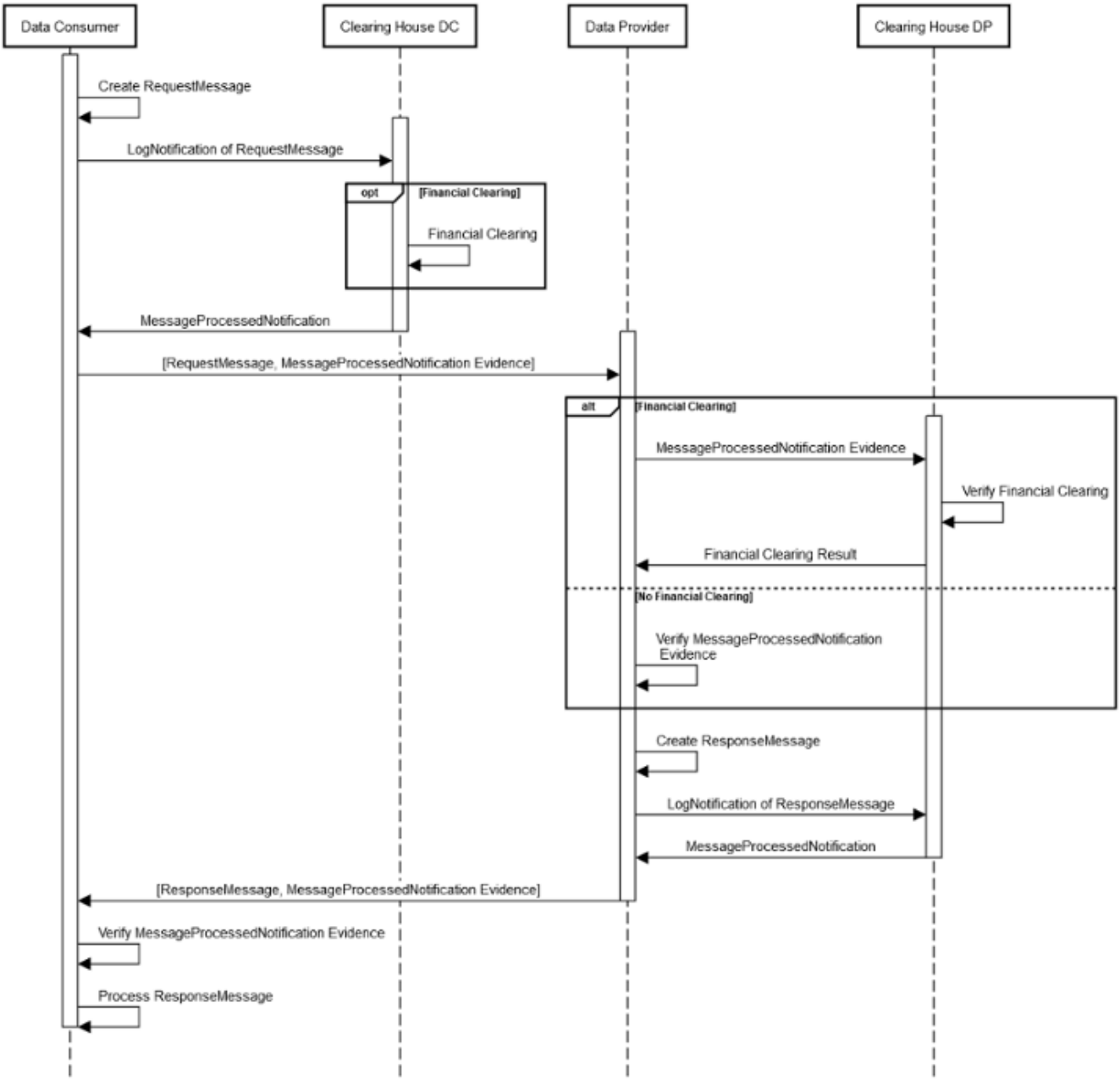


Figure 4: Clearing process with evidence structure for clearing, without error handling

In this case, the `MessageProcessedNotification` coming from an IDS Clearing House must contain a body with verifiable evidence of the `LogNotification`. This could be done via a Signed JSON Web Token (JWS) containing claims on the header and body it received (e.g. by attaching signatures of those parts). The evidence should also contain a DAPS token in order for the receiver to be able to verify the current status of the IDS Clearing House. This evidence should be sent either together with the original message or in separate requests. The receiver of the IDS Clearing House evidence can verify the JWS by checking the validity of the JWS itself and by checking the validity of the DAPS token inside the JWS, in order to verify whether the Clearing House is still a valid IDS Clearing House.

For financial clearing, IDS Clearing Houses should be able to financially clear a message and check the validity of the financial clearing via processes that are outside the scope of the IDS Reference Architecture Model.

3.2 Information Model

There are two types of interaction with the IDS Clearing House: logging messages and querying messages. Regarding the logging process, the following three figures show the header and body information during the transfer of the `LogNotification` for the different categories of data sovereignty (see above) established on the Process Layer: In Figure 5, only a hash of the message header and the message payload combined is logged (category 3); in Figure 6, the message header and a hash of the message payload is logged (category 2); and in Figure 7, the complete message (i.e. message header and message payload) is logged (category 1).

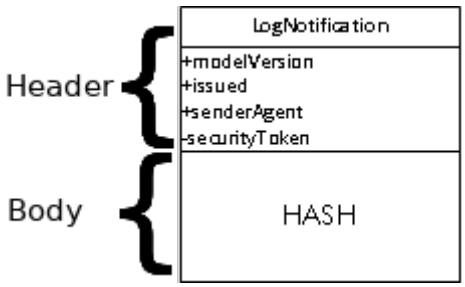


Figure 5: `LogNotification` with Hash value

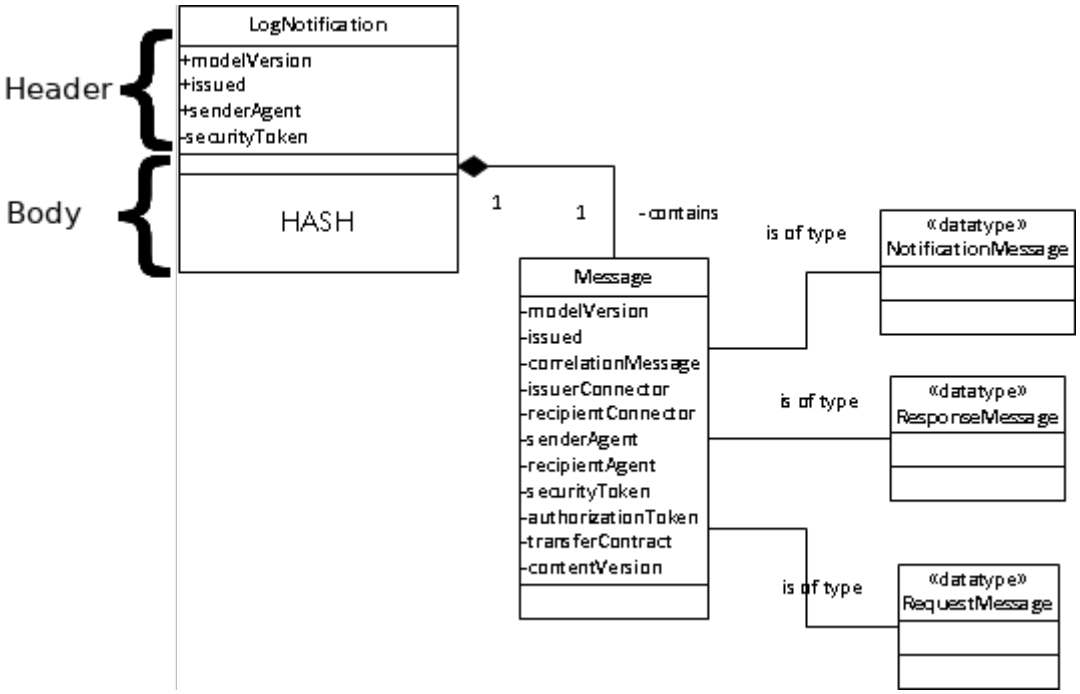


Figure 6: `LogNotification` Header and with Hash value

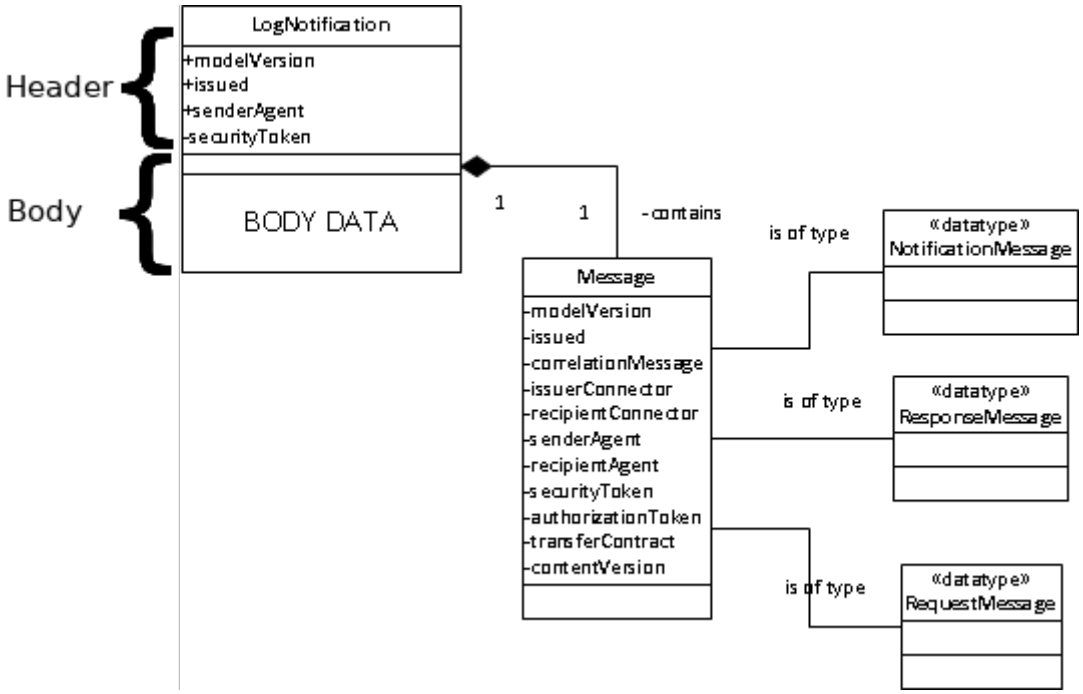


Figure 7: `LogNotification` with Body and Header

With regard to querying the IDS Clearing House, Figure 8 shows the components of the IDS Information Model, while Figure 9 depicts the response of the IDS Clearing House (which may be either a `ResultMessage` containing the result data or a `RejectionMessage` containing information why the query is rejected). All three (`QueryMessage`, `ResultMessage` and `RejectionMessage`) inherit from `Message`.

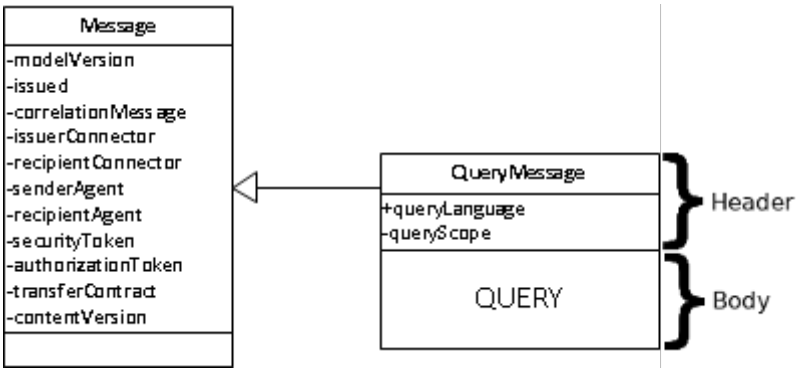


Figure 8: Information model components during a query

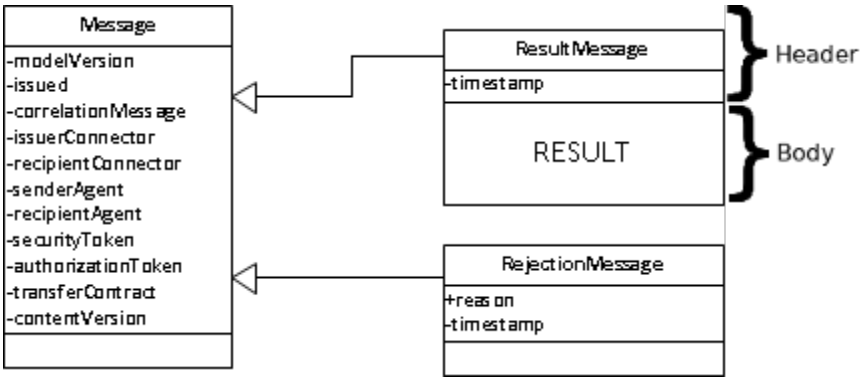


Figure 9: Information model components during a response

3.3 System layer (API)

3.3.1 Clearing House Architecture

The IDS Clearing House is an IDS Connector that runs the Clearing House Container as a service. As such, the Connector part of the Clearing House is responsible for communication with other IDS Connectors. The architecture therefore follows the IDS Connector architecture as presented in RAM 4.0 (see Section 3.5.1).

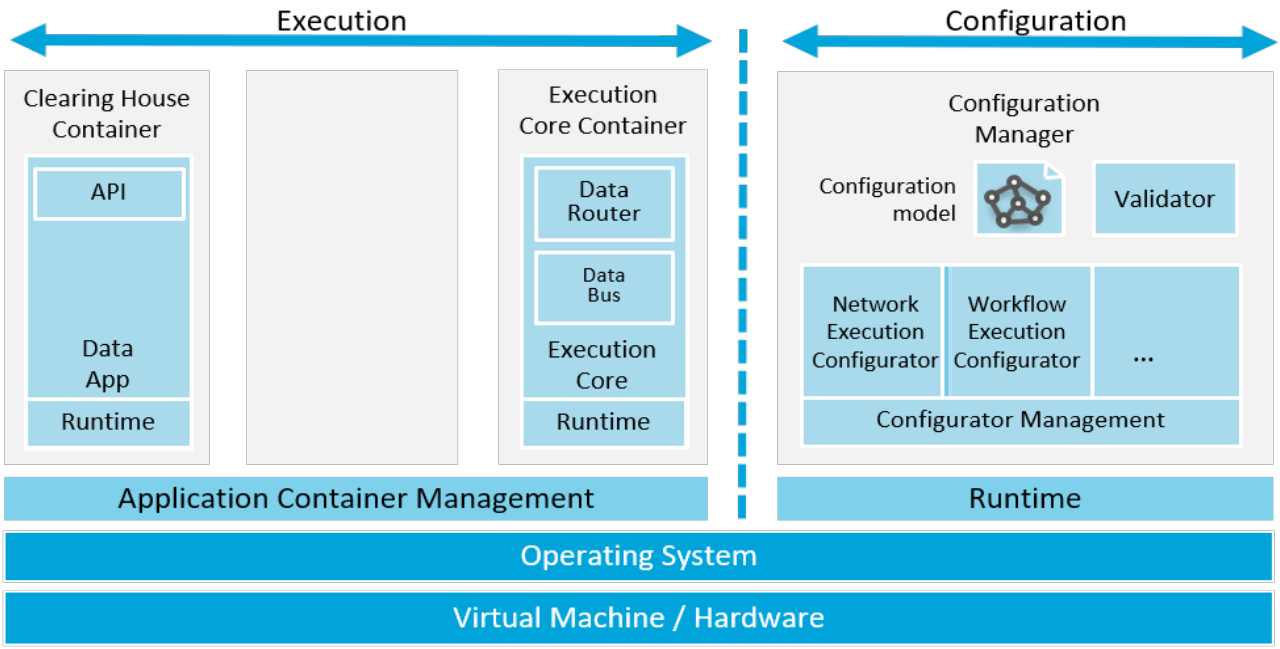


Figure 10: Relationship of IDS Connector and IDS Clearing House Container

3.4 HTTP API

At this moment, the Clearing House Interface consists of at least two HTTP endpoints. One for query operations and the other for logging events.

The API description in OpenAPI 3.0 is publicly available and has the same normative meaning as all other requirements of this document as far as the HTTP binding is concerned. The currently valid

version of the API description can be found at this link:
https://app.swaggerhub.com/apis/idsa/tbd

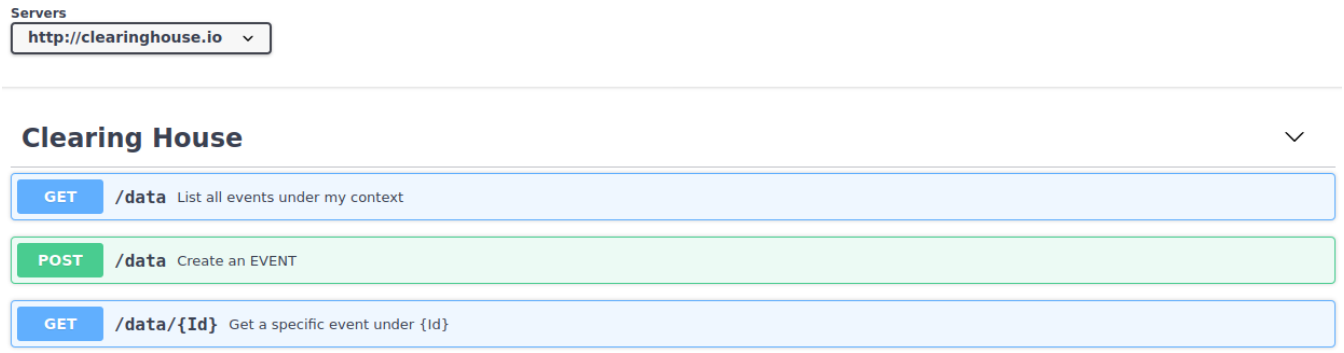


Figure 11: OpenAPI (Swagger) of the IDS Clearing House (link necessary)

4 Governance aspects of an IDS Clearing House

The Governance Perspective of the IDS Reference Architecture Model defines IDS roles, functions, and processes from a governance and compliance point of view. It thereby defines the requirements to be met by the business ecosystem to achieve secure and reliable corporate interoperability. In particular, the Governance Perspective describes how IDS enables participants to define rules and agreements for trustworthy collaboration.

While IDS enables all participants to act in compliance with negotiated rules and processes, it does not make any restrictions or enforce any predefined regulations. Instead, the IDS Architecture can be understood as a functional framework providing mechanisms that can be customized by the participating organizations according to their specific requirements.

IDS supports governance issues by

- providing an infrastructure for data exchange, corporate interoperability, and the use of new, digital business models;
- establishing trustworthy relationships between Data Owners, Data Providers, and Data Consumers;
- acting as a trustee for mediation between participants;
- facilitating negotiation of agreements and contracts;
- aiming at transparency and traceability of data exchange and data user;
- allowing private and public data exchange transactions;
- taking into account specific requirements of participants;
- offering a decentralized architecture (i.e. one that does not require a central authority).

The Governance Perspective in the context of the IDS-RAM relates to concepts from an organizational and technical point of view to establish the development of a healthy and trustful data ecosystem. It supports collaborative governance mechanisms, which facilitate common service and value propositions are achieved, while the interests of all actors are protected.

As innovative business models and digital, data-driven services require enhanced data management capabilities, the role of data governance is receiving increasing attention. Therefore, the management of data-related resources by means of decision rights, accountabilities, roles, and ownership makes data governance a fundamental element in the IDS ecosystem. To manage data under consideration of business needs and the existing digital infrastructure, data governance, being a leadership function of data management, acts as an enabler for successfully engaging in a collaborative ecosystem. It is therefore necessary to establish suitable organizational structures and procedures that determine who makes what kind of decisions concerning data assets, and what responsibilities and accountabilities are associated with these decisions.

In this context, organizations are confronted with new challenges. Innovative, data-driven business solutions often require that data is increasingly used outside the organization. This development transcends organizational boundaries, as internal data is used externally, and vice versa. At the same time, new forms of collaboration in data ecosystems are created and established. Various actors – such as original equipment manufacturers (OEMs), suppliers, or third-party vendors – interact with each other and contribute to delivering a common value proposition.

From an internal perspective of one single organization, the execution and allocation of decision-making rights regarding the management and use of data manifests itself within organizational structures. These structures ensure that relevant guidelines and principles regarding data assets are in place and monitored. However, traditional instruments for assigning data-related decision-making rights and accountabilities usually do not reach beyond an organization's borders. Thus, the influence of authority within a data ecosystem might be limited for the individual actor. The IDS-RAM addresses this challenge by allocating decision-making rights regarding data governance and management activities to different roles in the IDS ecosystem. It thereby supports the requirements to be met by all actors within the ecosystem to achieve secure and reliable interoperability as well as desirable behavior regarding the use of data.

For the IDS Clearing House, the IDS-RAM defines the data governance and data management activities, as follows:

- **Data-related activities**
  - Monitor and log data transactions and data value chains
  - Monitor policy enforcement
  - Provide data-accounting platform
- **Enabling/supporting IDS component**
  - IDS Clearing House
  - Logging data

4.1 Data Provenance

By creating transparency and offering clearing functionality, IDS provides a way to track the provenance and lineage of data. This is strongly linked to the topics of data ownership and data sovereignty. Functions for data provenance tracing can be implemented with the help of local tracking components integrated into the IDS Connectors. Furthermore, such functions can be implemented by means of a central provenance storage component attached to the IDS Clearing House (see Chapter 3.1.1 of IDS-RAM), which receives logging information concerning all activities performed over the course of a data exchange transaction, and which requests confirmation of successful data exchange from both the Data Provider and the Data Consumer. In doing so, data provenance is always recursively traceable. In, addition data provenance information can be integrated into the IDS Vocabulary,

in order to enable participants to maintain data provenance tracing as part of the metadata during the process of data exchange.

IDS thereby provides the possibility to implement and use appropriate concepts and standards. However, it does not force participants to use these concepts and standards. It is therefore up to the individual participant to provide correct information (i.e. metadata) on the provenance of data.

4.2 Data Governance and Data Management Activities of the IDS Clearing House

What data governance and data management activities the IDS Clearing House should carry out has not been defined in detail yet. In the following, three use case examples are laid out to illustrate possible activities and duties of the IDS Clearing House.

4.2.1 Example Use Case #1

Name:
Commercial clearing and settlement
Brief Description:
Successful commercial clearing (before data exchange transaction) and settlement (after data exchange transaction)
Actors:
Data Provider (DP), Data Consumer (DC), IDS Clearing House (CH)
Precondition:
Usage Contract and Commercial Contract exist
Basic Flow:

1) Usage Contract and Commercial Contract have been successfully agreed by DP and DC
2) Clearing process:
    a) Transfer of payment information from DP to DC, and confirmation of receipt by DC
    b) CH receives messages with payment information regarding transaction to be conducted, and verifies contract with three possible outcomes:
        - If payment information is valid, CH clears transaction.
        - If payment information is not valid, CH blocks transaction.
        - If payment information cannot be verified, but appears to be valid, CH may clear transaction (vouch).
3) Settlement process:
    a) Transfer of funds between DC's financial institution and DP's financial institution.
    b) CH receives messages regarding payment of transaction from both financial institutions.
        - If payment has been successfully completed, CH settles transaction.
        - If payment has not been successfully completed,
        - DP can raise a claim against DC (via CH), or
        - CH may assume payment to fulfill the contract, and raise a claim against DC on its part.

4.2.2 Example Use Case #2

Name: Contract violation
Brief Description: Purchased data is not delivered, or delivery violates contract (e.g. quality of data not as specified)
Actors: Data Provider (DP), Data Consumer (DC), Clearing House (CH), Dynamic Trust Management (DTM)
Precondition: Usage Contract and Commercial Contract exist; claim management system must be available to report claims.
Basic Flow:

1) Usage Contract and Commercial Contract have been successfully agreed by DP and DC
2) 2. Transaction has been commercially cleared and settled
3) 3. Data is not delivered as specified in contract / Data is not delivered at all
4) 4. DC raises claim to CH about non-fulfillment of contract
5) 5. CH uses logging information (metadata) to verify validity of claim:
    a) If claim is invalid, CH declares claim unjustified.
    b) If claim is valid, CH starts clarification with DP for correction of delivery or financial compensation.
    c) If claim cannot be resolved, issue may be escalated to DTM for reducing DP's trust level.

4.2.3 Example Use Case #3

Name: Usage Contract violation
Brief Description: Data Usage Control policy is violated
Actors: Data Provider (DP), Data Consumer (DC), Clearing House (CH), Dynamic Trust Management (DTM), Policy Enforcement Point (PEP)
Precondition: Usage Contract and Commercial Contract exist; claim management system is in place
Basic Flow:

1) Usage Contract and Commercial Contract have been successfully agreed by DP and DC
2) Transaction has been commercially cleared and settled
3) DP has delivered data to DC as specified in contract
4) DP, or a PEP, detects violation of Data Usage Policy (e.g. data is distributed to a third party without valid agreement/authorization) and reports it to DTM
5) DP raises claim to CH about usage control violation
6) CH uses logging information (metadata) to verify validity of claim:
    a) If claim is invalid, CH declares claim unjustified.
    b) If claim is valid, CH starts clarification with DC for correction of data usage or financial compensation.
    c) If claim cannot be resolved, issue may be escalated to DTM for reducing DC's trust level.

OUR MEMBERS


Aalto University
ADVANEO
agrarmarkt informatik
Allianz
Atos
Audi
bill-X Collect. Manage. Execute.
Boehringer Ingelheim
Brainport Industries
bdr BUNDESDRUCKEREI
CAICT
SUPERCLUSTER
CDQ SHARING DATA EXCELLENCE
cea
Cefriel POLITECNICO DI MILANO
iti Information Technologies Institute
CHALMERS UNIVERSITY OF TECHNOLOGY
COSMOPlat
Cybus
CTU CZECH TECHNICAL UNIVERSITY IN PRAGUE
DAIMLER
DATAHEAD
DATATRONIQ
DB SCHENKER
Deloitte.
Deutsche Bank
DGZfP
DHBW Duale Hochschule Baden-Württemberg Ravensburg
Digital Green
DIMECC
DR. SCHNEIDER UNTERNEHMENSGRUPPE
eccenca command your data!
EcoDataCenter
ELDORADO
ENGIE
ENGINEERING
8760 Fastems
fir an der RWTH Aachen
FIWARE
Leibniz Universität Hannover
Fraunhofer
GateHouse Logistics
EDGE CLOUD
GESIS
Google
HITACHI Inspire the Next
HUAWEI
i2cat
iav
IBM
ILVO Instituut voor Landbouw-, Visserij- en Voedingsonderzoek
imec
Imperial College London
Institut Mines-Télécom
INDUSTRY 2025 INDUSTRIE INDUSTRIA
INNOPAY
innovalia ASSOCIATION
Insight
Irish Manufacturing Research
ITI INVESTIGATE TO INNOVATE
Klarrio
komsa DIE BESSERE VERBINDUNG
LOSEC LEADERS IN SECURITY
Lobster
Logata Digital Solutions
LOGENIOS
minnosphere
msg
nexedi
nicos AG
olmogo data ownership solutions


orbiter

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΠΑΤΡΩΝ

pi-lar GmbH

POLITECNICO
MILANO 1863

pwc

QuinScape

realworldsystems

RI
SE

REWE
GROUP

RITTAL

SALZGITTERAG
Stahl und Technologie

SAP

SCHAEFFLER

SETLOG
The Smart Connective

SICK
Sensor Intelligence.

SIEMENS
Ingenuity for life

Signal
Solutions

SINTEF

SMEV AG
Smart Mobility Evolution

TARC

tecnalia
Inspiring Business

IK4 TEKNIKER


mtc
Manufacturing Technology Centre

thyssenkrupp

TNO innovation for life

TÜV NORD GROUP

TÜV
SÜD

UNIKLINIK
RWTH AACHEN

UNiSCON
Sealed Cloud Technologies

UNITY
CONSULTING & INNOVATION

universität
Witten/Herdecke

University of Amsterdam

UNIVERSITY
OF TWENTE.

vastuu group

VDMA

VOLKSWAGEN
AKTIENGESELLSCHAFT

VTT

WELOTEC
a byte smarter

WeTech
IDS-China

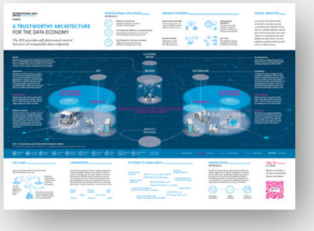
ZVEI:
Die Elektroindustrie

OVERVIEW PUBLICATIONS

Reference Architecture Model

Executive Summary

Image Brochure



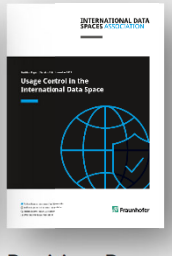
Infographic

Use Case Brochures

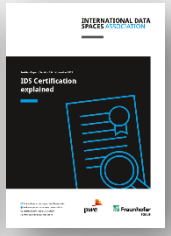
Study on Data Exchange

Position Paper Implementing the European Data Strategy

Position Paper GDPR Requirements and Recommendations



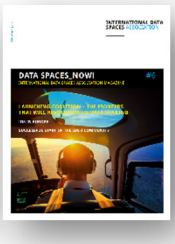
Position Paper Usage Control in the IDS



Position Paper IDS Certification Explained

White Paper Certification

Sharing data while keeping data ownership



Magazine Data Spaces_Now!

For these and further downloads: www.internationaldataspaces.org/info-package

Code available at: https://github.com/industrial-data-space

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

@ids_association

international-data-spaces-association