

INTERNATIONAL DATA SPACES (IDS)

Harrie Bastiaansen

TNO innovation
for life

January 29th 2019
Commit2Data - Landelijk overleg data innovation





INTERNATIONAL DATA SPACES (IDS)

Contents

- › The DL4LD project
- › The Reference Architecture Approach
- › The International Data Spaces (IDS) Initiative
- › The Status
- › The Way Forward / Next Steps
- › Relation with DL4LD Forward Looking Research
 - › Ideas/proposals on alignment



SHORT HISTORY: THE DL4LD PROJECT

Data Logistics for Logistics Data (DL4LD) project

Data Logistics for Logistics Data (DL4LD) is an innovation project that aligns with the ambitions of the 'Topsector Logistiek' and 'Commit2Data'.

The logistics companies will strive for an internationally leading position, amongst others as chain orchestrator, and will therefore have to share logistics data on a large scale.

To support this, a data sharing infrastructure is required as basis for essential logistics information services. The data sharing infrastructure must be secure and trusted.



- › 'Ter leering ende vermaeck': IDS als onderdeel genoemd bij de ondertekening van de [Fraunhofer en TNO samenwerking](#).



IDS - SECURITY VERSUS TRUST

Security

Non-functional design aspect:

The implementation of an IT-system must comply to its security level requirements as defined at system design and protect against malicious or unintentional security breaches.

- › Confidentiality, Integrity, Availability (CIA), ...
- › All ICT-systems must be secure



Trust Enablers

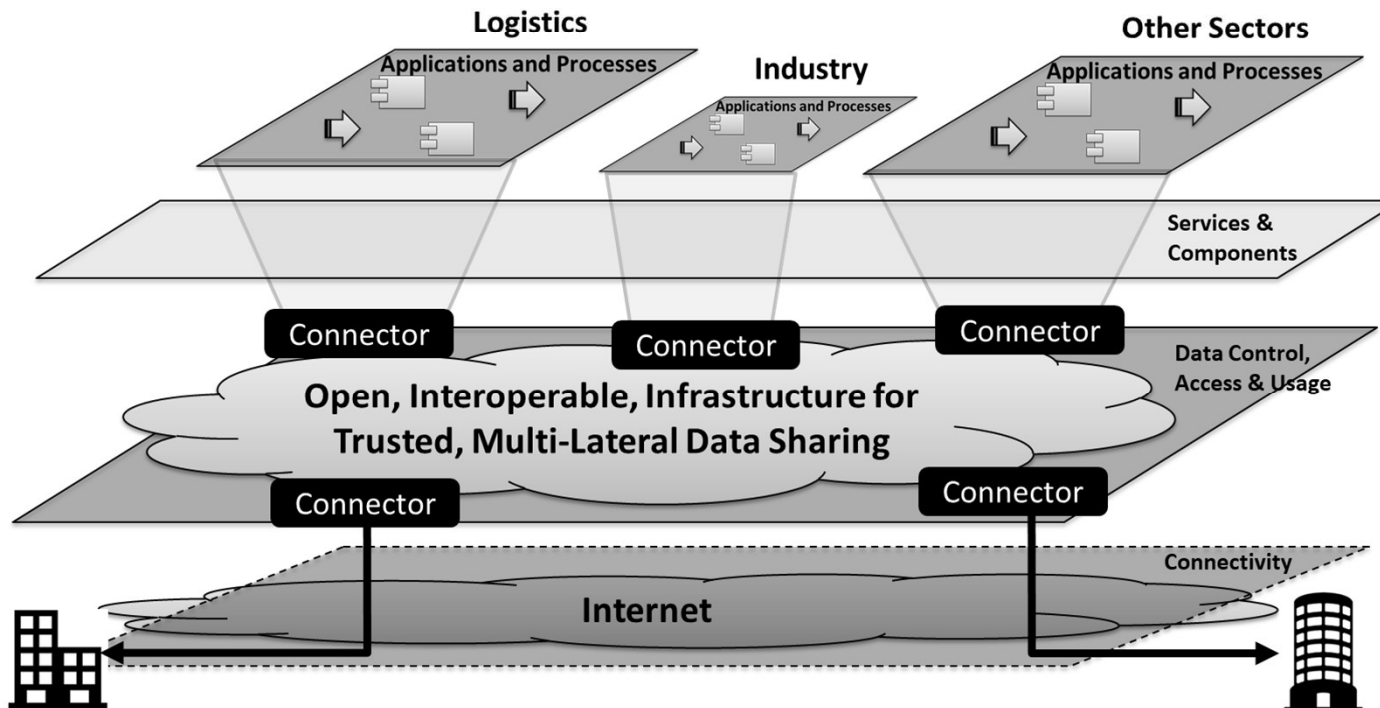
Functional design aspects:

- › **Data sovereignty**
- › Data sharing agreements
- › Enforcement of data sharing agreements
 - › *legal enforceability,*
 - › *implementation enforceability*
- › Data provenance, logging, reporting
- › System integrity monitoring



IDS – THE VISION

Infrastructure connecting organizations across sectors for multi-lateral, trusted, data sharing.





THE DL4LD PROJECT

Data Sovereignty is Key

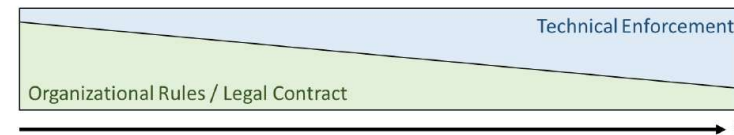
Being in control over your own data

- › Who is allowed access to your data, for which purpose and under which conditions



Realisation of data sovereignty requires a variety of enablers, i.e.:

- › Technical enablers, e.g.:
 - › Mechanisms for access control and for usage control
 - › Enforcement of external (law, regulations) and internal (business) policies.
 - › Security mechanisms: peer-to-peer data sharing, encryption, PKI / Key Management, ...
- › Procedural enablers, e.g.:
 - › Making a data sharing agreement
 - › Doing data sharing transactions: clearing, settlement, ..
 - › Logging, data provenance and reporting



IDS REFERENCE ARCHITECTURE INFOGRAPHIC (SEPTEMBER 2018)

INTERNATIONAL DATA SPACES ASSOCIATION

A TRUSTWORTHY ARCHITECTURE FOR THE DATA ECONOMY

The IDS provides self-determined control between all imaginable data endpoints

INTERNATIONAL DATA SPACES APPROACH

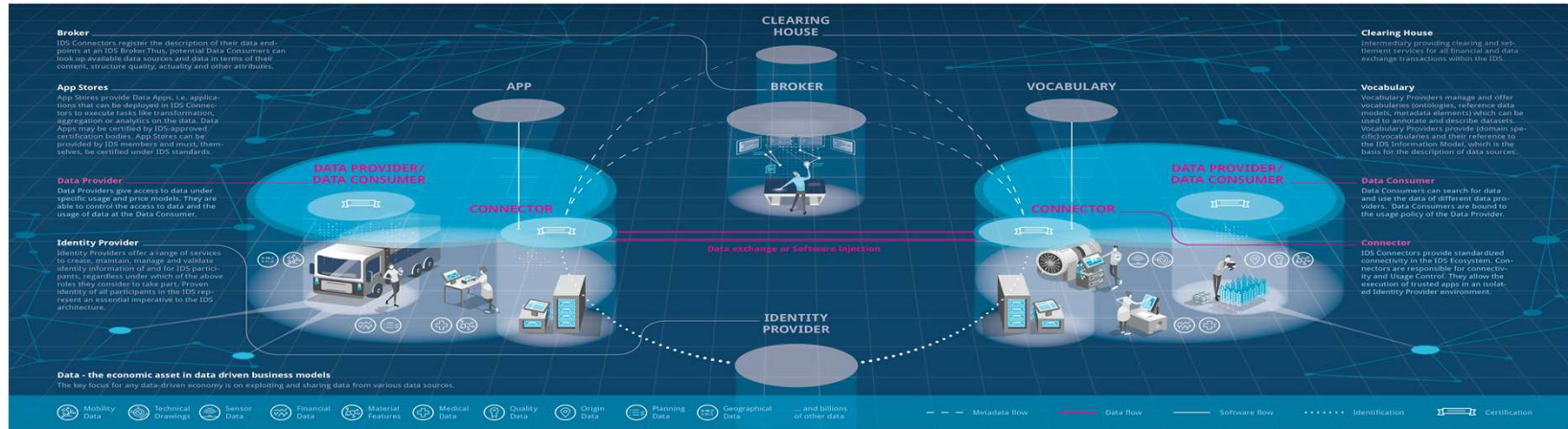
- Endless Connectivity**
Standard for data flows between all kinds of data endpoints
- Trust between different security domains**
Comprehensive and audit-proven security functions providing a maximum level of trust
- Governance for the data economy**
Usage control and enforcement for data flows and assignments of data

MISSION STATEMENT

- Secure Data Exchange**
It forms the basis for a variety of certifiable software solutions, smart services ...
- Business Models**
Data Owners remain sovereign owners of their data at any time
- International Standards**
IDSA defines the basic conditions and governance for a reference architecture and interfaces
- Use Cases**
This standard is actively developed and updated on the basis of use cases

DIGITAL IDENTITIES

A network of trusted entities in the data economy requires a mechanism for digital entities, that can reliably identify a participant and can provide more information on transaction partners. Additional information must be updated regularly and be provided in a trusted manner.



USE CASES

Services and functionalities of the IDS are specified and validated in use cases. Additional requirements are fed into the architecture development. The IDS approach is applied and tested in pilots. Smart Services are developed facilitating the Data Owner and Data Consumers to exploit the IDS.

COMMUNITIES

Interest and user groups of same or similar domains with common challenges validate and proliferate the IDS approach, technology and ecosystem. Based on their practical experience the IDS reference architecture and the ecosystem around it are continuously developed. Thus, specific application scenarios for verticals are set up, implemented and systematically pushed forward, allowing participants to enhance existing or to launch new services.

- Medical Health
- Energy
- Materials
- Banking/ Insurances
- Industrial
- Smart Cities
- Farm & Food
- Legislation

10 THINGS TO KNOW ABOUT

- Containerization, e.g. Docker
- WebServices, e.g. https, MQTT, REST, Multi Part Messages
- Message Oriented Middleware
- Digital Identities and Digital Certificates, e.g. X509
- Semantic Data Descriptions, e.g. Business Description Framework
- Requirements Engineering, Processes and tools, e.g. UML and RUPIN
- Enterprise Integration Patterns
- Software Engineering, e.g. tools like Maven, git
- Data Ecosystems
- Certification, e.g. IEC 62443, ISO 27001

CERTIFICATION APPROACH

The IDS Certification Body is appointed by the IDSA and regularly aligns with the IDSA to manage the certification process, defines the standardized evaluation procedures and supervises the actions of the evaluation facilities. An Evaluation Facility is contracted by an Applicant and is responsible for carrying out the detailed technical and organizational evaluation work during a certification.



CALL TO ACTION

Become a member in the International Data Spaces Association:



Concept and Design: INFOGRAFIK PRO GmbH - www.infografik.pro

IDS ASSOCIATION AND THE IDS RESEARCH PROJECT

IDS Association (IDSA)

Objectives:

- › To foster the general conditions and governance of a reference architecture for the International Data Space and interfaces with the aim of achieving an international standard
- › To develop and continue to work on the standards for the International Data Space based on use cases
- › To support certifiable software solutions and business models

INTERNATIONAL DATA SPACES ASSOCIATION

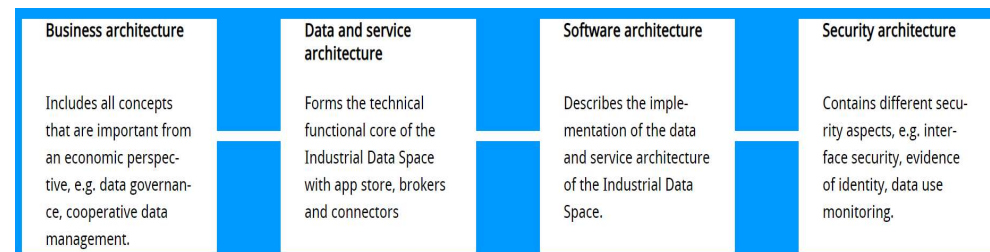


IDS Research Project

Objectives:

- › Create a blueprint for the data space
 - › Consisting of four partial architectures
 - › Safe data exchange and the efficient combination of data
 - › Configurable for individual use cases / scenarios

Done by Fraunhofer



IDS ASSOCIATION: MEMBERS

TNO innovation
for life

INTERNATIONAL DATA
SPACES ASSOCIATION

85+
Companies and
Organisations

15+
Countries

25+
Use
Cases

1
Ecosystem



IDS REFERENCE ARCHITECTURE: FUNCTIONAL

1. TRUST

- Roles
- Identity management
- User certification
- Governance

2. SECURITY AND DATA SOVEREIGNTY

- Authentication & authorization
- Usage policies & usage enforcement
- Trustworthy communication & security by design
- Technical certification

3. ECOSYSTEM OF DATA

- Data source description
- Brokering
- Vocabularies

4. STANDARDIZED INTEROPERABILITY

- Integration of existing vocabularies
- Handling of different data formats
- Connection of clouds and platforms

5. VALUE ADDING APPS

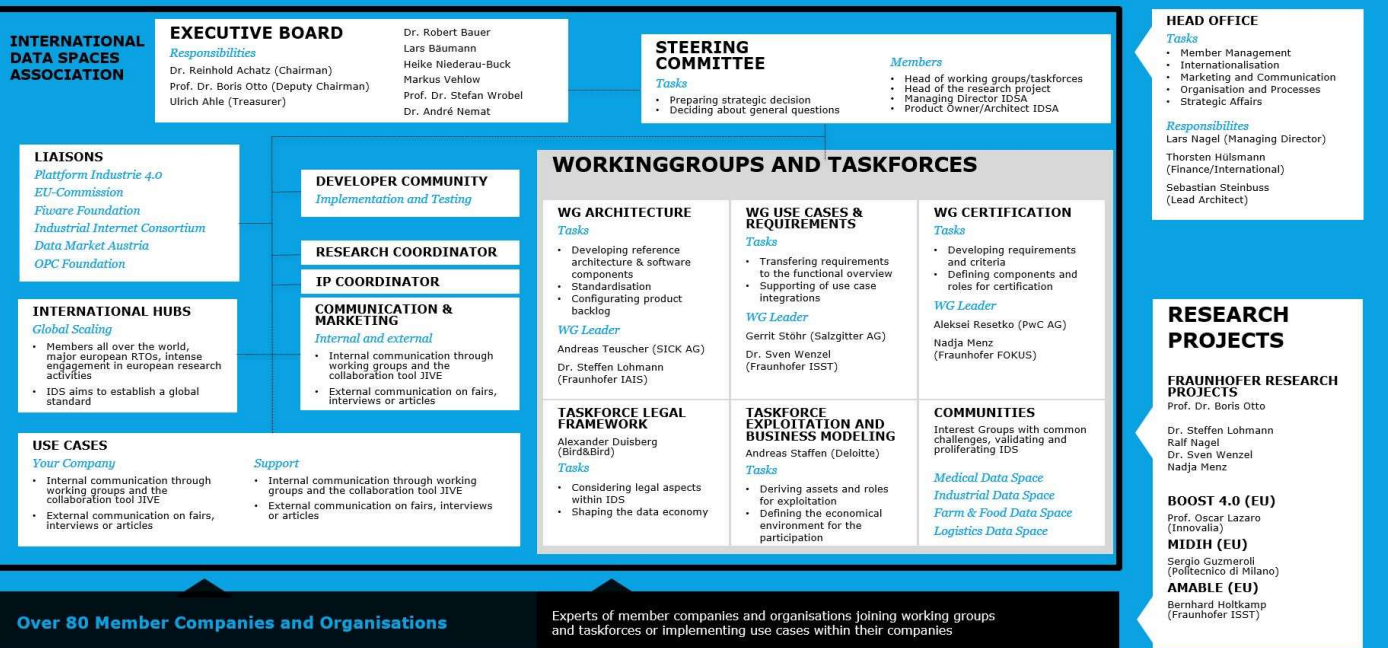
- Processing of data
- Remote execution

6. DATA MARKETS

- Clearing & billing
- Domain-specific broker and marketplaces
- Use restrictions and legal aspects (contract templates, etc.)

IDS ASSOCIATION: ORGANIZATIONAL STRUCTURE

ORGANISATION



IDS: VISION, MISSION AND APPROACH



IDS Vision

IDS is a global de facto market standard for the sovereign use of data'

IDS blueprint for data spaces

Business architecture

Includes all concepts that are important from an economic perspective, e.g. data governance, cooperative data management.

Data and service architecture

Forms the technical functional core of the Industrial Data Space with app store, brokers and connectors

Software architecture

Describes the implementation of the data and service architecture of the Industrial Data Space.

Security architecture

Contains different security aspects, e.g. interface security, evidence of identity, data use monitoring.



Unlimited Interoperability

standard for data flows between all kinds of data endpoints



Trust between different security domains

comprehensive security functions providing a maximum level of trust



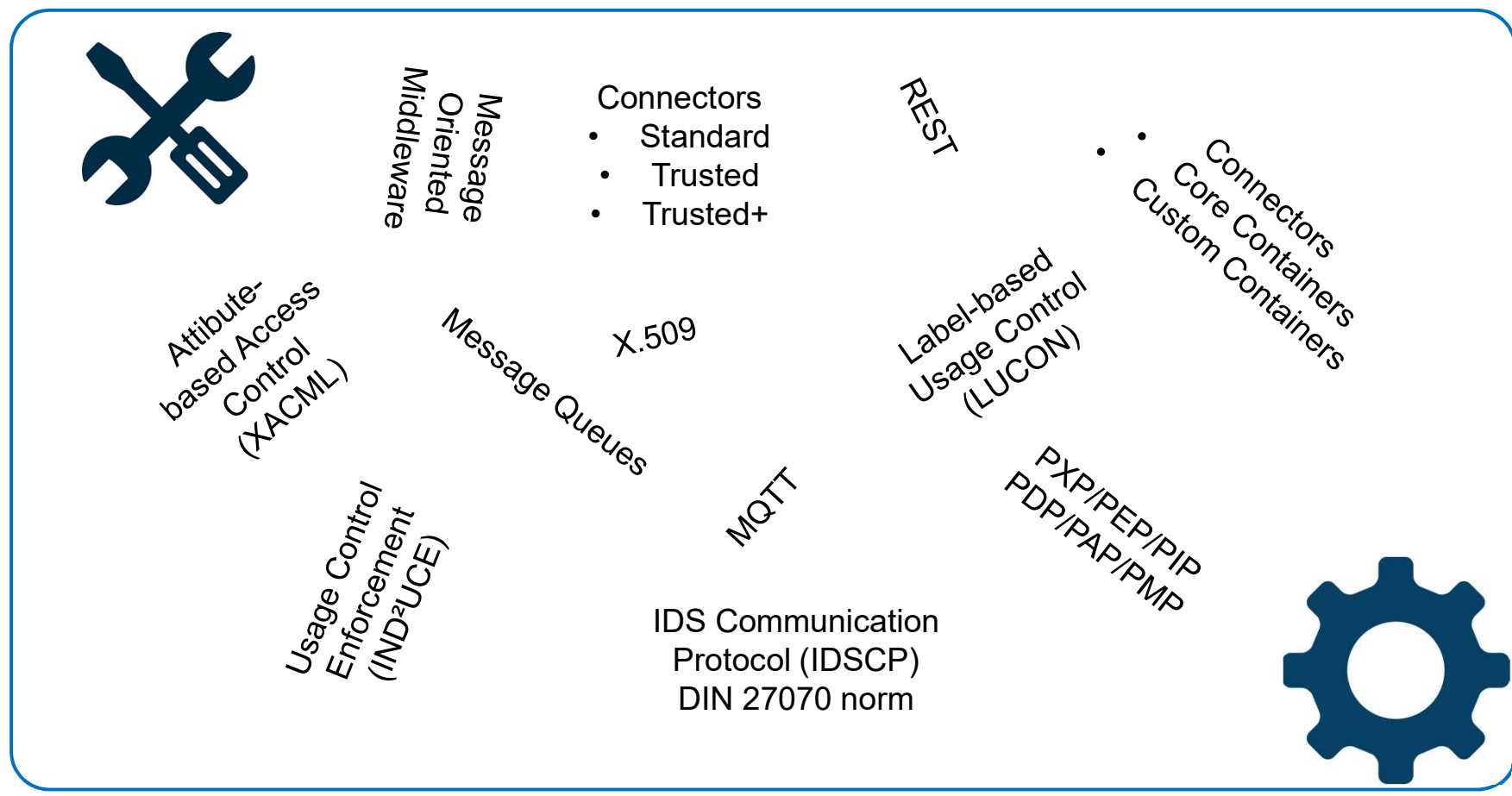
Governance for the data economy

usage control and enforcement for data flows

Data Sovereignty

Self determined control of data flows

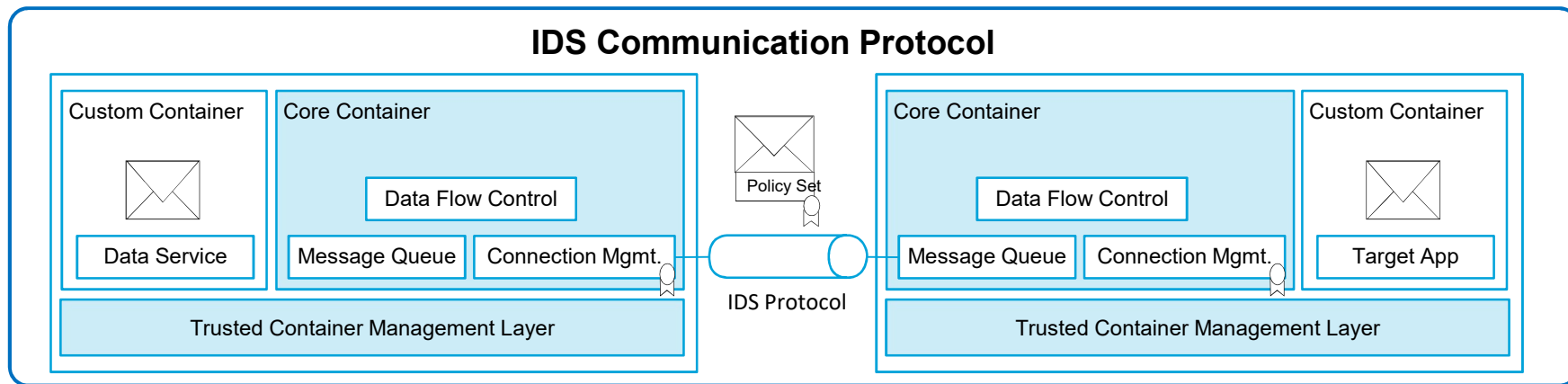
IDS REFERENCE ARCHITECTURE: THE TECHNOLOGY



IDS REFERENCE ARCHITECTURE: IDSCP

Approach:

- › Peer-to-peer data communication: no central data lakes
- › Enabled by interacting IDS connectors
 - › Standardised by IDS Communication Protocol (IDSCP): DIN 27070 norm



Scope:

- › IDS Handshake -> *Continuous usage*
- › IDS On-boarding process -> *Initial usage*

Usage Control for Data Sovereignty in IDS

Usage Control Motivation Technical vs. Organisational/Legal Enforcement

- Usage Control extends, replaces and supplements existing contractual and organizational enforcement
 - Long-term Goal:
Technical Enforcement compensates Organisational/Legal Enforcement

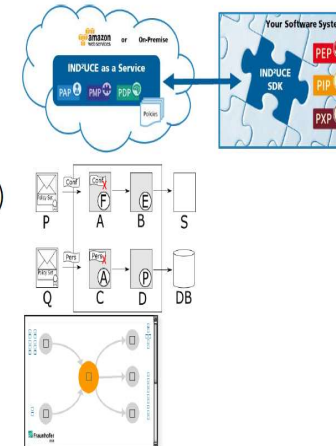


Quellen
© Fraunhofer 8



Usage Control Overview Usage Control Technologies in the Industrial Data Space

- Integrated Distributed Data Usage Control Enforcement (IND²UCE)
Fraunhofer IESE, Kaiserslautern
- Label-based Usage Control (LUCON)
Fraunhofer AISEC, Munich
- Information Flow Tracking (IFT)/
Provenance Tracking
Fraunhofer IOSB, Karlsruhe

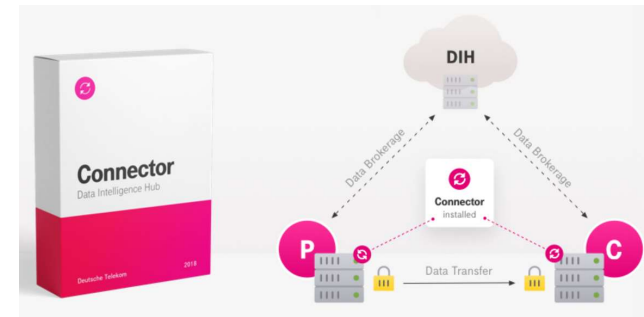


Quellen
© Fraunhofer 5



IDS: FOR ILLUSTRATION

- › Deutsche Telekom has announced IDS-based commercial services / products
 - › Based on IDS versions in development
 - › Connector, Data Broker, Identity Provider
 - › Data Intelligence Hub



DATA SOVEREIGNTY

The Data Intelligence Hub is the first data marketplace to meet the stringent security requirements of the International Data Spaces Association (IDSA). Taking into account the data protection standards, data trust architecture, decentralized data management and subscriber certification your data is safe – and ensures your full control.

- › Data Sovereignty based on IDS
 - › For policy definition and signalling
 - › Extend and enforce into the DT domain, i.e.
 - › The DT data lakes for AI
 - › The DT AI workbench/tools

SO WHAT IS NEW?

- › Individual (technical) aspects have been shown before
- › So, why should it work (this time):
 - › Governance, standardisation, interoperability



Governance of development

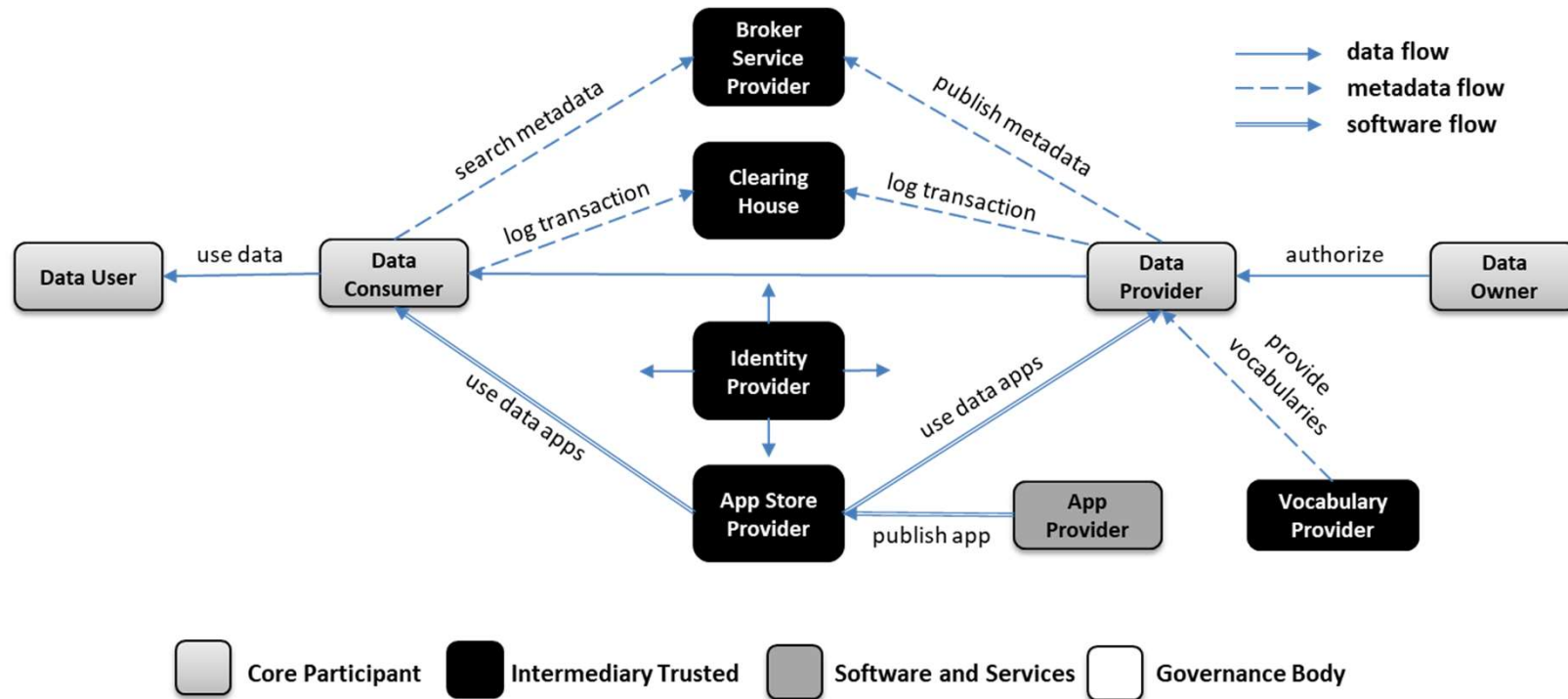
- › *Design for an ecosystem:*
 - › Open to users
 - › Open to service providers and to innovation
 - › Open to solution providers
- › *Interoperability for scale, scope and reach:*
 - › Vertically – inter-organizational
 - › Horizontally – cross organization/sectors
 - › Longitudinally– supply chain
- › *Low barriers to participate*
 - › Open source availability
- › *Open standard design and maintenance process*

Governance of deployment

- › *Provide adequate alternative for closed communities*
- › *Create initial solution with sufficient scale*
- › *Specific roles to be fulfilled by*
 - › Telecommunication operators / service providers
 - › Early adopters: major companies, field labs
 - › Authorities

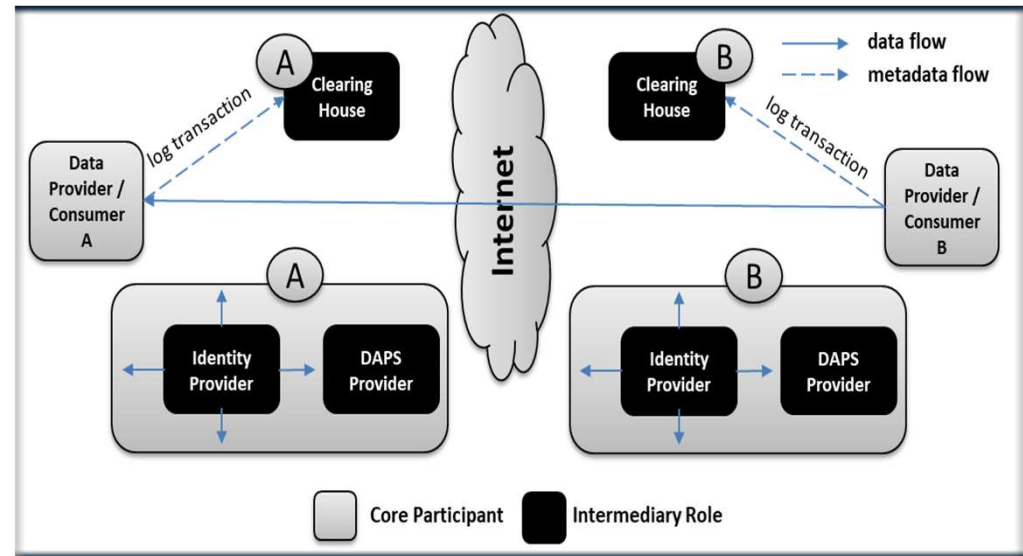
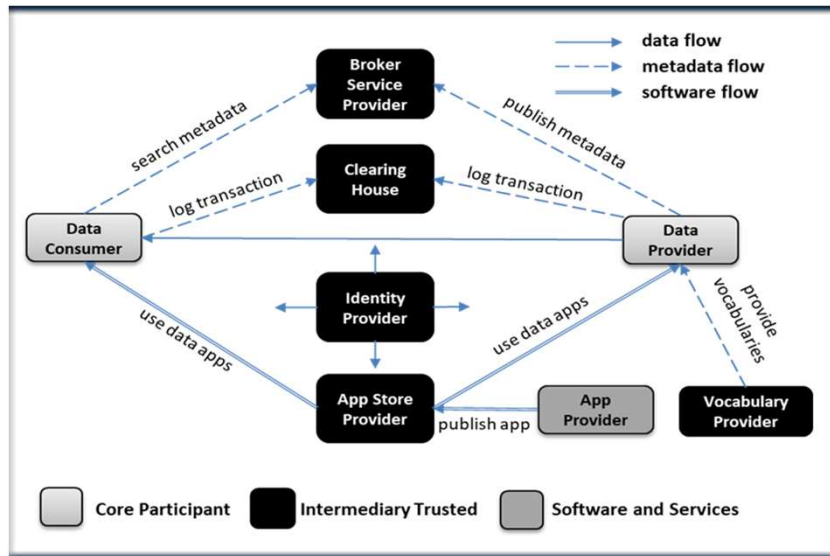
IDS: ROLE MODEL

Ecosystem, open for stakeholders to participate



THE IDS ECOSYSTEM

Multitude of trusted, interoperable, intermediary roles



TODAY'S MESSAGE



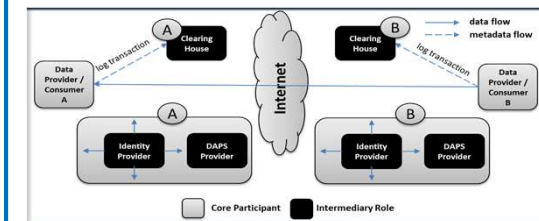
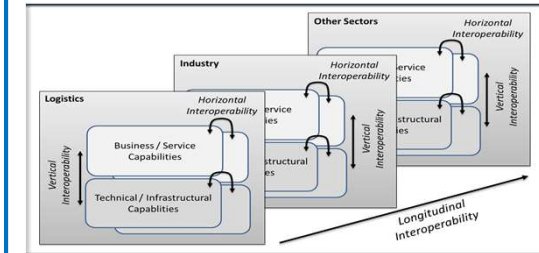
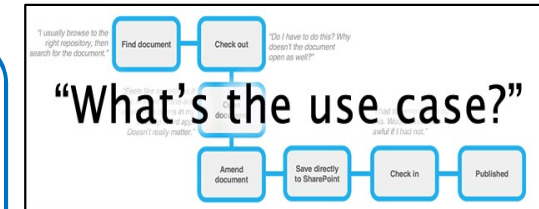
Important
Message

- › Many aspects on sovereignty and trust for data sharing infrastructures are currently being worked on
 - › Try to re-use and extend, not re-invent
 - › Embed it in an international (standardisation) initiatives

- › IDS may provide the basic infrastructure to interconnect and extend upon, for:
 - › Ensuring data sovereignty
 - › Data Market Places, incl. data brokering and clearing house
 - › For enforcing legislation (normative systems), e.g.: software certification, enforced information flows and processing, usage and access control,....

TNO OBJECTIVES

- › Demonstrating viability through representative use case
 - › Initial focus on: connector, identity provider, clearing house
 - › Smart industry, logistics, cross-sector, cross-border,...
- › Interoperability for scale, scope and reach:
 - › Vertically – inter-organizational
 - › Horizontally – cross organization/sectors
 - › Longitudinally– supply chain
- › Elaborating the IDS Service Model
 - › Cross-sectoral
 - › In an open, distributed, infrastructure for multi-lateral data sharing
- › Providing open source IDS components
 - › Connectors: Base, Trusted, Trusted+
 - › Supporting solutions for: identity provider, clearing house, ...





THANK YOU FOR YOUR ATTENTION

Take a look:

- WWW.DL4LD.NET
- TIME.TNO.NL

TNO innovation
for life

H.J.M. (Harrie) Bastiaansen, PhD

Tel: +31 6 51295527

Harrie.Bastiaansen@TNO.NL

