INTERNATIONAL DATA SPACES (IDS)

Harrie Bastiaanssen

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

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

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

---

**International Data Spaces Association**

**Fraunhofer**
IDS ASSOCIATION: MEMBERS

85+ Companies and Organizations
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: 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.

Data Sovereignty
Self determined control of data flows

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
IDS REFERENCE ARCHITECTURE: THE TECHNOLOGY

- Connectors
  - Standard
  - Trusted
  - Trusted+

- Attribute-based Access Control (XACML)
- Message Queues
- MQTT
- X.509
- IDS Communication Protocol (IDSCP)
  - DIN 27070 norm

- Usage Control Enforcement (INDUCE)
- Message Oriented Middleware
- REST
- Label-based Usage Control (LUCON)
- PX/P/EP/P/PEP/P/LP/PAP/PMP
- Core Containers
- Custom Containers
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

Usage Control Overview
Usage Control Technologies in the Industrial Data Space

- Integrated Distributed Data Usage Control Enforcement (INDUCE)
  Fraunhofer IESE, Kaiserslautern

- Label-based Usage Control (LUCON)
  Fraunhofer AISEC, Munich

- Information Flow Tracking (IFT)/Provenance Tracking
  Fraunhofer IOSB, Karlsruhe
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 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
Individual (technical) aspects have been shown before

So, why should it work (this time):
  ‣ Governance, standardisation, interoperability ….

**SO WHAT IS NEW?**

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
Ecosystem, open for stakeholders to participate
Multitude of trusted, interoperable, intermediary roles
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,....
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

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

Tel: +31 6 51295527
Harrie.Bastiaansen@TNO.NL