WEBINAR AGENDA

1. OUR APPROACH
2. CONTEXT OF IDS
3. THE PRINCIPLES
4. THE CONCEPTS
5. OUR OFFERING
6. THE WAY FORWARD
OUR APPROACH
CLEANROOMS FOR A PROSPERING DATA ECONOMY
The key focus for a data-driven economy and new business models is in linking data.
Trading with data creates huge revenues for some focal companies in an ecosystem, which tend to assume monopolistic attitudes.

Rarely, the creators of data are benefitting from this value in an adequate way.

Companies do not take advantage of the value.

Making data economy really a success, there is a need for a ...

- vendor independent data market place
- connecting vendor-specific platforms
- open to all
- at low (transaction-) cost and
- easy to adopt and easy to use.
WE ADDRESS THIS NEED.

IDSA reference architecture forms the base of

- an open, **distributed** data market place,
- ensuring **data sovereignty** for the creator of the data,
- and **proven data-provenance** for the user of data,
- all above **audit-proof**, if requested
- based on **European values**.
THE IDSA DEFINES...

1 Reference Architecture
2 Interfaces
3 Contractual Framework
4 Sample Code

...FOR AN OPEN DATA-ECOSYSTEM.

www.internationaldataspaces.org
Companies want to link data without regret.

Interoperability
Data Exchange
»Sharing Economy«
Data Centric Services

Data Ownership
Data Security
Data Value

Digital Sovereignty

is the ability of a natural or legal person to exclusively and sovereignly decide concerning the usage of data as an economic asset.
300 people contributing
18 countries
THE INTERNATIONAL DATA SPACES APPROACH CONNECTS ALL KINDS OF DATA ENDPOINTS

When broadening the perspective from an individual use case scenario to a platform landscape view, the INTERNATIONAL DATA SPACES positions itself as an architecture to link different cloud platforms through secure exchange and trusted sharing of data, short: through data sovereignty.

By proposing a specific software component, the INTERNATIONAL DATA SPACES Connector, industrial data clouds can be connected, as well as individual enterprise clouds and onpremise applications and individual connected devices.
CONTEXT OF IDS
MANY PLAYERS
TO BRING OUR APPROACH TO LIFE

- Commercial Software • Data Markets • Technology Development • Central Service Offerings (e.g. Certification) • Roll-out and Scale-up Activities • Professional Services • Domain-specific (vertical) Implementations • ...

- Reference Architecture Model Maintenance • Requirements Management • Standardization Activities • Specification and RfQ with regard to Central Services • Knowledge Transfer • Internationalization • Platform for Domain-Specific Activities ...

- Reference Architecture Model (initial version) • Prototype Implementation in Use-Cases • Basic Versions IDS Components • Knowledge Transfer (Research Delivery and Support Center) • Technology Innovation (Usage Control, Trusted Connector etc.) • Support of Standardization Activities • ...

www.internationaldataspaces.org
@ssteinbuss // 14
Interweaving our architecture with other leading global initiatives
**IDSA Communities**

A community that gathers relevant stakeholders to develop Use Cases that blueprints the community specific perspective.

**OUR COMMUNITIES**

- Medical Data Space
- Logistics Data Space
- Industrial Data Space

**THEIR TARGETS**

- Gather relevant **stakeholders**
- Set up & describe **Use Cases**.
- Show the **added value** by the IDS concepts.
- Verify and promote the **concepts** of the IDS RAM
- Comment and **define items** in the Functional Overview.
IDSA Hubs

IDSA goes Europe - first six hubs set up across Europe ...

... with the central support centre operating out of Germany.
THE PRINCIPLES
OK.

What’s new?
“HOW TO” DATA ECONOMY
UNLEASH THE VALUE OF YOUR DATA

1. Make data available – dynamic, on demand (describe, expose)

2. Link with ecosystem partners (connect, match, interprete)

3. Control the access to your data (usage control)

4. Create value (Apps, remote software execution, aggregation)
INTERNATIONAL DATA SPACES APPROACH:
SELF DETERMINED CONTROL OF DATA FLOWS

Unlimited Interoperability
Enabled by semantic data descriptions

Trust between different security domains
Certified, comprehensive security functions providing a maximum level of trust

Governance for the data economy
Usage control and enforcement for data flows
**IDS-ready**

Compliance to IDS reference architecture for components & organizations

**THE 2 PHASES**

**IDS-ready Review** (available)

The review is carried out by members of the WG certification; the IDSA Head Office is responsible for issuing the IDS-ready statements.

**IDS Certification** (starting mid 2019)

The evaluation is carried out by evaluation facilities approved by the IDS Certification Body; the IDS Certification Body is responsible for issuing the IDS certificates.

**Evaluators for IDS-Component**

- Fraunhofer AISEC
- Fraunhofer FOKUS
- Fraunhofer IOSB

**Evaluators for IDS-Organization**

- PwC
- TÜV SÜD
THE CONCEPTS
DISTRIBUTED GOVERNANCE IN INTERNATIONAL DATA SPACES ECOSYSTEMS
INFORMATION MODEL
DESCRIBING DATA ASSETS

• The essential agreement shared by the participants and components of data ecosystems, facilitating compatibility and interoperability

• Three formal levels of digital representation of the information model
  – Conceptual (generic description in UML)
  – Declarative (formal, machine-interpretable specification of IDS concept, semantic description)
  – Programmatic (IDS information model library in java)
**IDS REFERENCE ARCHITECTURE**

**INTERACTION OF COMPONENTS**

[Diagram showing the interaction of components in an IDS reference architecture.]

- **App Store**
- **Broker**
- **Data Source**
- **Connector**
- **Data Provider**
- **Data Consumer**
- **Data Sink**
- **Dataset(s) transferred from Provider to Consumer**
- **Metadata Description of Datasets/Provider/Consumer**
- **Application for specific data manipulation**

- **Data exchange (active)**
- **Data exchange (inactive)**
- **Metadata exchange**
- **App download**
IDS REFERENCE ARCHITECTURE
ARCHITECTURE OF A CONNECTOR

Execution
- Custom Container
  - API
  - Data App
  - Runtime
- App Store Container
  - API
  - Data App
  - Runtime
- Execution Core Container
  - Data Router
  - Data Bus
  - Execution Core
  - Runtime

Configuration
- Configuration Manager
  - Configuration model
  - Validator
- Network Execution Configurator
- Workflow Execution Configurator
- ...
### 4 SECURITY PROFILES
YOU DECIDE DEPENDING ON THE USE SCENARIO

<table>
<thead>
<tr>
<th>Reference Development</th>
<th>Base Free</th>
<th>Base</th>
<th>Trust</th>
<th>(Managed)Trust+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference Development</td>
<td>Open Source</td>
<td>IDS Community</td>
<td>IDS Community</td>
<td>Bound to strong SLAs</td>
</tr>
<tr>
<td>Roles</td>
<td>Own infrastructure</td>
<td>All IDS Roles supported, Billing and Clearing optional</td>
<td>All IDS Roles supported</td>
<td>All IDS Roles supported</td>
</tr>
<tr>
<td>Communication Abilities</td>
<td>Only private IDS with self signed certificates</td>
<td>Full interoperable, reduced trust</td>
<td>Full interoperable, Free decision of communication</td>
<td>Full interoperable, Free decision of communication, Hardware anchor</td>
</tr>
</tbody>
</table>

www.internationaldataspaces.org

@ids_association

@ssteinbuss
DATA SOVEREIGNTY IS A KEY PREREQUISITE FOR INNOVATIVE DATA-CENTRIC SCENARIOS IN VARIOUS INDUSTRIES

### Healthcare
- **Domain:** Healthcare
- **Data:** Patient Data
- **Usage Conditions:**
  - Usage purpose
  - Anonymization
  - System constraints
- **Business Benefits:**
  - Personalized medicine
  - Better healthcare

### Industrial Manufacturing
- **Domain:** Industrial Manufacturing
- **Data:** Product Data
- **Usage Conditions:**
  - Usage frequency
  - Number of usage purposes
  - Expiration dates
- **Business Benefits:**
  - Innovative production networks
  - Production as a service

### Automotive Logistics
- **Domain:** Automotive Logistics
- **Data:** Supply Chain Risk Data
- **Usage Conditions:**
  - Usage purpose
  - Expiration data
  - System constraints
- **Business Benefits:**
  - Improved risk management
  - Less supply chain disruptions

Image sources: perm4.com (2017); hccs.edu (2017); dvz.de (2017).
BUSINESS INNOVATION IN HEALTHCARE
MEDICAL DATA SPACE

Usage context
Clinical research

Anonymization
Data record must consists of at least 150 individual anonymized data sets

- Health data
- Medication plan
- Electronic case records

University Hospital

Patient Management

Pharma Company

Smart Drug Development
FLEXIBLE AND DYNAMIC PRODUCTION NETWORKS
INDUSTRIAL DATA SPACE

- OEM
  - Production Planning and Control
  - Maintenance

- "Production as a Service" Provider
  - Machine type
    - Maintenance, no forwarding
      - Operator anonymous
  - Usage context
    - Usage time
      - Temperature data
      - Certificates
  - Usage volume
  - CAD data
  - Configuration parameters
  - Production volume
  - Usage time
  - Temperature data
  - Certificates
BUSINESS INNOVATION IN AUTOMOTIVE

Tier 1 Supplier

- Contact person
- Risk type
- Risk location
- Numbers of affected parts
- DUNS numbers of affected sub-suppliers
- Inventory of affected parts

Usage Context
Supplier Management

Condition
Deletion after 14 days

OEM

- Contact person
- Parts demand
- Inventory of affected parts

Usage Context
Risk Management

Condition
Deletion after 3 days

Supplier Management
ADDITIVE MANUFACTURING ECOSYSTEM
Data Control in the Context of Digital Transformation

Data Analyst
If no user consent is given, data must be anonymized before sharing.

Supplier
Data must only be used by supplier for at most 3 days.

Energy Provider
Building consumption analysis must comply with GDPR and citizen must give consent for added value services.

Law Enforcement Agency
Case files must be filtered at attribute level when used for investigations.
Access Control

- Classical security controls are well established, but not flexible enough
  - Unable to express complex conditions
  - Only binary yes / no decisions

Application Context: "Risk Management"

Role: "Risk Manager"?

Grant access?

yes

no
Modern security controls are more expressive, but still allow only binary decisions!

- Location: “Office”
- Security Policies: “Up to date”
- Device: “Tablet”
- Application Context: “Risk Management”
- Role: “Risk Manager”?

Grant access?

- yes
- no
Attribute-based Usage Control

- Today’s systems need full flexibility, regarding both decisions and enforcement

- Location: “Office”
- Security Policies: “Up to date”
- Device: “Tablet”
- Application Context: “Risk Management”
- Role: “Risk Manager”?

Grant usage?
- Yes, but only for 3 days
- Yes, but inform owner
- Yes, but only in anonymized form
- No
- No, and report incident
Solution: Moving from Access Control to Usage Control

- **Grant and control data** usage based on
  - **Context**: e.g., current location and role of the user, previous events
  - **Obligations**: e.g., time-based, amount-based usage conditions
  - **Modification and Filtering**: e.g., use of anonymized data

---

![Diagram](image-url)
Data Usage Control in the IDS
Overview of DUC activities in the IDS

- Conception and development ...

1. ... a language for the specification of data sovereignty requirements (technology-independent)

2. ... of technologies for the technical implementation of data sovereignty requirements

⇒ Formalization of data sovereignty requirements and their technical enforcement
14 USAGE POLICY CLASSES (SO FAR)

- Allow the usage of the data
- Inhibit the usage of the data
- Restrict the data usage for a group of users or systems
- Restrict the data usage for specific purposes
- Restrict the data usage when a specific event has occurred
- Use or do not use the data in a specific time interval
- Use the data not more than N times
- Use data and delete it after
- Modify data (in transit)
- Modify data (in rest)
- Log the data usage information
- Notify a party or a specific group of users when the data is used
- Share the data under specific circumstances
- Restrictions on the fine-grained use actions
USAGE CONTROL ONION
DATA USAGE CONTROL CAN AFFECT MULTIPLE LAYERS

Distributed Usage Control

Access Control
DATA PROVENANCE TRACKING
# IDS REFERENCE ARCHITECTURE MODEL
## Roles & Responsibilities in IDSA Certification

<table>
<thead>
<tr>
<th>Role</th>
<th>Entry Level</th>
<th>Member Level</th>
<th>Central Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Owner</td>
<td>Required</td>
<td>Recommended</td>
<td>Optional</td>
</tr>
<tr>
<td>Data Provider</td>
<td>Required</td>
<td>Recommended</td>
<td>Optional</td>
</tr>
<tr>
<td>Data Consumer</td>
<td>Required</td>
<td>Recommended</td>
<td>Optional</td>
</tr>
<tr>
<td>Broker Service Provider</td>
<td>Required</td>
<td>Required</td>
<td>Optional</td>
</tr>
<tr>
<td>App Store Provider</td>
<td>Required</td>
<td>Required</td>
<td>Optional</td>
</tr>
<tr>
<td>Vocabulary Provider</td>
<td>Required</td>
<td>Required</td>
<td>Optional</td>
</tr>
<tr>
<td>Service Provider</td>
<td>Required</td>
<td>Recommended</td>
<td>Optional</td>
</tr>
<tr>
<td>Clearing House</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>Identity Provider</td>
<td></td>
<td>Required</td>
<td>Required</td>
</tr>
</tbody>
</table>
IDS REFERENCE ARCHITECTURE MODEL
Roles & Responsibilities in IDSA Certification

<table>
<thead>
<tr>
<th>Participants</th>
<th>Self-Assessment</th>
<th>Management System</th>
<th>Control Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry Level</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Member Level</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Central Level</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Components</th>
<th>Checklist Approach</th>
<th>Concept Review</th>
<th>High Assurance Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Security Profile</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Trust Security Profile</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Trust+ Security Profile</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
DIN SPEC 27070 - INFRASTRUKTUR

ANFORDERUNGEN UND REFERENZARCHITEKTUR EINES SECURITY GATEWAYS ZUM AUSTAUSCH VON INDUSTRIEDATEN UND DIENSTE
## DIN SPEC 27070 – SECURITY GATEWAY PROFILE

ANFORDERUNGEN UND REFERENZARCHITEKTUR EINES SECURITY GATEWAYS ZUM AUSTAUSCH VON INDUSTRIEDATEN UND DIENSTE

<table>
<thead>
<tr>
<th>Security Gatewayprofil</th>
<th>Erläuterung</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trust</strong></td>
<td>Das Trust-Profil dient für Anwendungsszenarien, in denen der Schutz der verarbeiteten und übertragenen Daten wesentlich ist. Es wird generell auf SL-3 abgebildet und bietet Schutz gegen versehentliche Fehlbedienung durch Administratoren, beispielsweise durch eine strikte Containerisolation, integritätsgeschütztes Logging, Verschlüsselung aller persistierten Daten, siehe auch Tabelle in 6.1.</td>
</tr>
</tbody>
</table>
## DIN SPEC 27070 - SICHERHEITSLEVEL

ANFORDERUNGEN UND REFERENZARCHITEKTUR EINES SECURITY GATEWAYS ZUM AUSTAUSCH VON INDUSTRIEDATEN UND DIENSTE

<table>
<thead>
<tr>
<th>Fähigkeiten des Angreifers</th>
<th>Mittel</th>
<th>Ressourcen</th>
<th>Fähigkeiten</th>
<th>Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SL-1</td>
<td></td>
<td></td>
<td>Zufällige/beiläufige Beeinträchtigung/Manipulation</td>
<td></td>
</tr>
<tr>
<td>SL-2</td>
<td>einfach</td>
<td>begrenzt</td>
<td>allgemein</td>
<td>niedrig</td>
</tr>
<tr>
<td>SL-3</td>
<td>ausgefeilt</td>
<td>mittel</td>
<td>domänenspezifisch</td>
<td>mittel</td>
</tr>
<tr>
<td>SL-4</td>
<td>ausgefeilt</td>
<td>umfangreich</td>
<td>domänenspezifisch</td>
<td>hoch</td>
</tr>
</tbody>
</table>
OUR OFFERING
IDS CONNECTOR IMPLEMENTATIONS
RUNNING ON DIFFERENT DEVICES

**Trusted Connector**
- Connector running on sensor device
- Implementation by Sick AG

**Lightweight Sensor Connector**
- Connector running on 32 bit microprocessor
- Implementation by Fraunhofer

**Base Connector**
- Connector running on Raspberry Pi
- Implementation by nicos AG

**Mobile Connector**
- Connector running on mobile device
- Implementation by thyssenkrupp AG, Fraunhofer and Logenios GmbH
OUR GALLERY
OF IMPRESSIVE IDS USE CASES

...have a look at our use case brochure and website for more success stories
ENABLING ADOPTION
AS A PARALLEL STREAM TO THE IDS DEVELOPMENT
1. CONTEXT OF THE IDS by Lars Nagel, Managing Director IDSA
2. PROCESS LAYER OF THE IDS by Dr. Christoph Quix, Senior Researcher Fraunhofer FIT
3. DATA GOVERNANCE by Prof. Dr. Boris Otto, Managing Director Fraunhofer ISST
4. THE IDS REFERENCE ARCHITECTURE MODEL FROM A BUSINESS POINT OF VIEW by Dr. Steffen Lohmann, Senior Researcher Fraunhofer IAIS
5. USAGE CONTROL AND ENFORCEMENT IN THE IDS by Christian Jung & Andreas Eitel, Senior Researcher Fraunhofer ISE
6. THE IDS INFORMATIONMODEL by Jaroslav Pullmann, Senior Researcher Fraunhofer FIT
7. THE IDS CONNECTOR ARCHITECTURE, THE IDS CONNECTOR CONFIGURATION MODEL AND CONNECTOR TYPES by Heinrich Pettenpohl, Deputy Head of Department Digitization and Service Industry Fraunhofer ISST
8. TRUST IN THE IDS by Gerd Brost, Senior Researcher Fraunhofer AISEC
9. THE IDS INFORMATIONMODEL POLICY LANGUAGE by Jaroslav Pullmann, Senior Researcher Fraunhofer FIT
10. TRUST IN THE IDS BASED ON CERTIFICATION OF PARTICIPANTS AND CORE COMPONENTS by Nadja Menz, Senior Researcher Fraunhofer Fokus & Aleksei Resetko, Director Cybersecurity & Privacy PwC Germany
JIVE QUESTS
GUIDANCE TO RELEVANT IDSA TOPICS
THE WAY FORWARD
MILESTONES REACHED AND NEXT STEPS

ARCHITECTURE
Release of the reference architecture model 3.0 on Hannover Fair

STANDARD
Foundation of a workinggroup at DIN to create a DIN specification for the IDS connector

INTERNATIONAL
Members all over the world, connecting with important initiatives, major European RTOs, intense engagement in European research activities

GO LIVE
Ecosystem potentially running, first products to come, enhancing global adoption
FURTHER DEVELOPMENT OF THE IDS RESEARCH PROJECTS

Open DEI
Aligning Reference Architectures, Open Platforms and Large-Scale Pilots in Digitising European Industry
JOINTLY PAVING THE WAY FOR A DATA DRIVEN DIGITISATION OF EUROPEAN INDUSTRY
NEW!

https://www.internationaldataspaces.org/info-package/
NEW!
JOIN US!

SEBASTIAN STEINBUß
DIRECTOR ARCHITECTURE
INTERNATIONAL DATA SPACES ASSOCIATION

WWW.LINKEDIN.COM-IN/SEBASTIANSTEINBUSS/
@SSTEINBUSS
JOSEPH-VON-FRAUNHOFER-STR. 2-4
44227 DORTMUND | GERMANY
+49 162 1067878
SEBASTIAN.STEINBUSS@INTERNATIONALDATASPACES.ORG

@ids_association #datasovereignty

www.internationaldataspaces.org
Ressource Hub – Press Area – Blog