TRUSTWORTHINESS AND DATA SOVEREIGNTY
THE INTERNATIONAL DATA SPACES AS AN EXAMPLE

MATTHIAS BÖCKMANN
FRAUNHOFER IAIS
ENTERPRISE INFORMATION SYSTEMS

Fraunhofer

The Presenter

Matthias Böckmann
Research Engineer – Fraunhofer IAIS
matthias.boeckmann@iais.fraunhofer.de

Fraunhofer

Agenda

Part I

- Introduction Trustworthiness and Data Sovereignty
- The International Data Spaces Reference Architecture
- Institutional Trustworthiness in the International Data Space Association

BREAK (5 Minutes)

Part II

- Break out Session (10 Minutes)
- Discussion Break out Sessions (10-15 Minutes)
- Takeaway Technology: Modelling Digital Contracts

Fraunhofer

Introduction Trustworthiness and Data Sovereignty

Fraunhofer

What does Data Sovereignty mean ?

Fraunhofer

What does Data Sovereignty mean ?

Wikipedia:

Data sovereignty is the idea that data are subject to the laws and governance structures within the nation it is collected.

Fraunhofer

What does Data Sovereignty mean ?

Wikipedia:

Data sovereignty is the idea that data are subject to the laws and governance structures within the nation it is collected.

GDPR (ART5, PAR1):

Personal Data:

>> processed lawfully, fairly and in a transparent manner <<

>> collected for specified, explicit and legitimate purpose<<

>> adequate, relevant and limited to what is necessary in relation to purposes for which they are processed<<

Fraunhofer

What does Data Sovereignty mean ?

Wikipedia:

Data sovereignty is the idea that data are subject to the laws and governance structures within the nation it is collected.

Google Cloud:

Data sovereignty provides customers with a mechanism to prevent the provider from accessing their data, approving access only for specific provider behaviors that customers think are necessary.

GDPR (ART5, PAR1):

Personal Data:

>> processed lawfully, fairly and in a transparent manner <<

>> collected for specified, explicit and legitimate purpose<<

>> adequate, relevant and limited to what is necessary in relation to purposes for which they are processed<<

Fraunhofer

What does Data Sovereignty mean ?

Wikipedia:

Data sovereignty is the idea that data are subject to the laws and governance structures within the nation it is collected.

Google Cloud:

Data sovereignty provides customers with a mechanism to prevent the provider from accessing their data, approving access only for specific provider behaviors that customers think are necessary.

GDPR (ART5, PAR1):

Personal Data:

>> processed lawfully, fairly and in a transparent manner <<

>> collected for specified, explicit and legitimate purpose<<

>> adequate, relevant and limited to what is necessary in relation to purposes for which they are processed<<

Database Directive

The database owner is vested with the right to prevent the unauthorized extraction or re-utlization of the whole or substantial parts, evaluated qualitatively or quantitatively, of the contents of the database.

Fraunhofer

What does Data Sovereignty mean ?

Wikipedia:

Data sovereignty is the idea that data are subject to the laws and governance structures within the nation it is collected.

Google Cloud:

Data sovereignty provides customers with a mechanism to prevent the provider from accessing their data, approving access only for specific provider behaviors that customers think are necessary.

Gaia-X

Each user decides for herself where her data is stored, as well as who may process it and for what purpose, based on the user's own data classification.

GDPR (ART5, PAR1):

Personal Data:

>> processed lawfully, fairly and in a transparent manner <<

>> collected for specified, explicit and legitimate purpose<<

>> adequate, relevant and limited to what is necessary in relation to purposes for which they are processed<<

Database Directive

The database owner is vested with the right to prevent the unauthorized extraction or re-utlization of the whole or substantial parts, evaluated qualitatively or quantitatively, of the contents of the database.

Fraunhofer

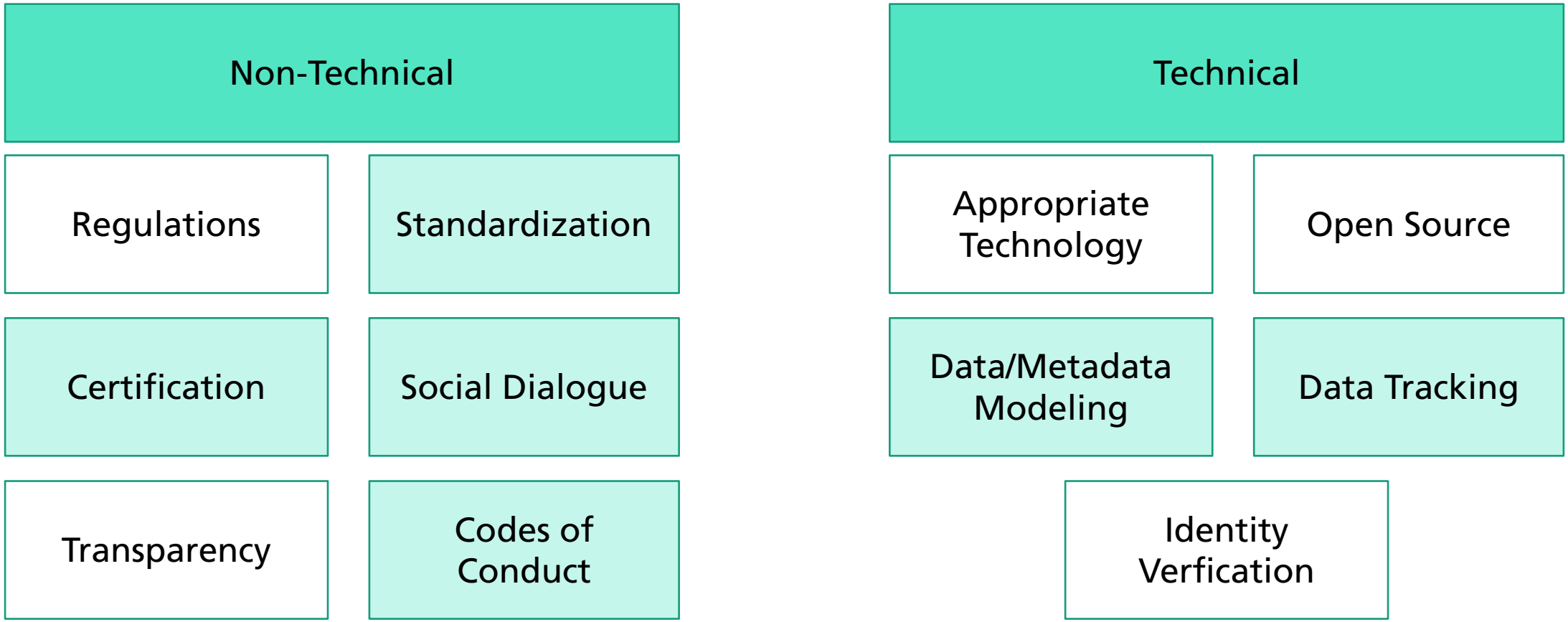
Questions for Data Sovereignty in the context of Data sharing

- Before the Sharing:
  - Under which conditions should my data be used ?
  - For what purposes do I want to share my data ?
  - How can I formulate these conditions ?

- During the Sharing
  - **Who** has access to the data ?
  - **Where** will the data be stored ?

- After the Sharing
  - How will the data be processed ?
  - How can I ensure, that there are no violations of my conditions ?

Claiming is not enough – Ensuring Trustwortyness

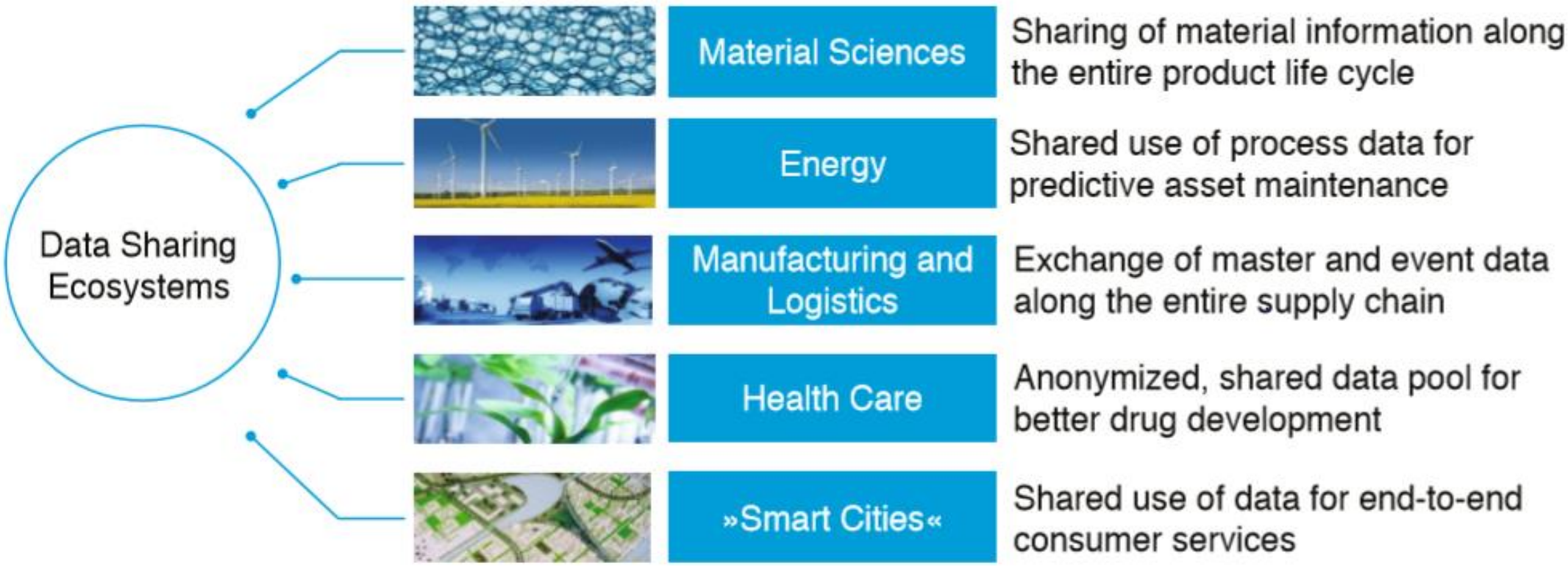


Fraunhofer

The International Data Spaces Reference Architecture

Fraunhofer

Motivation



Fraunhofer

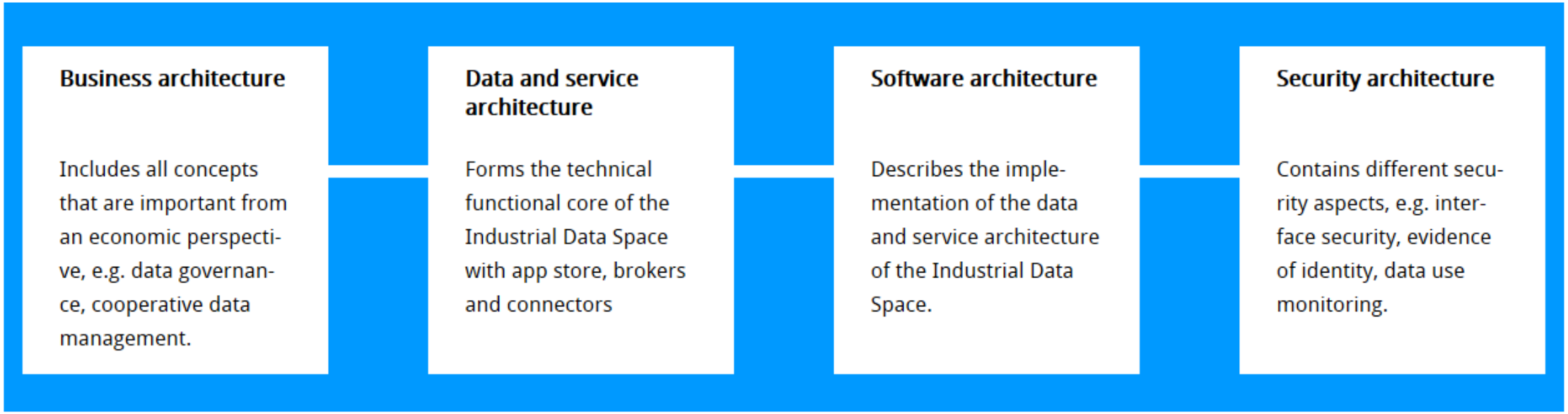
What is the IDS(A) ?

- International Data Spaces Association
  - Organisation with 100 Members consisting of Companies and Research Institutes
  - National Hubs in Germany, France, Netherlands, Spain, Finland, Italy and Czech Republic
  - The objective of the International Data Spaces Association (IDSA) is to establish a standard for data sovereignty – for the trustworthy, self-determined exchange of data.

Fraunhofer

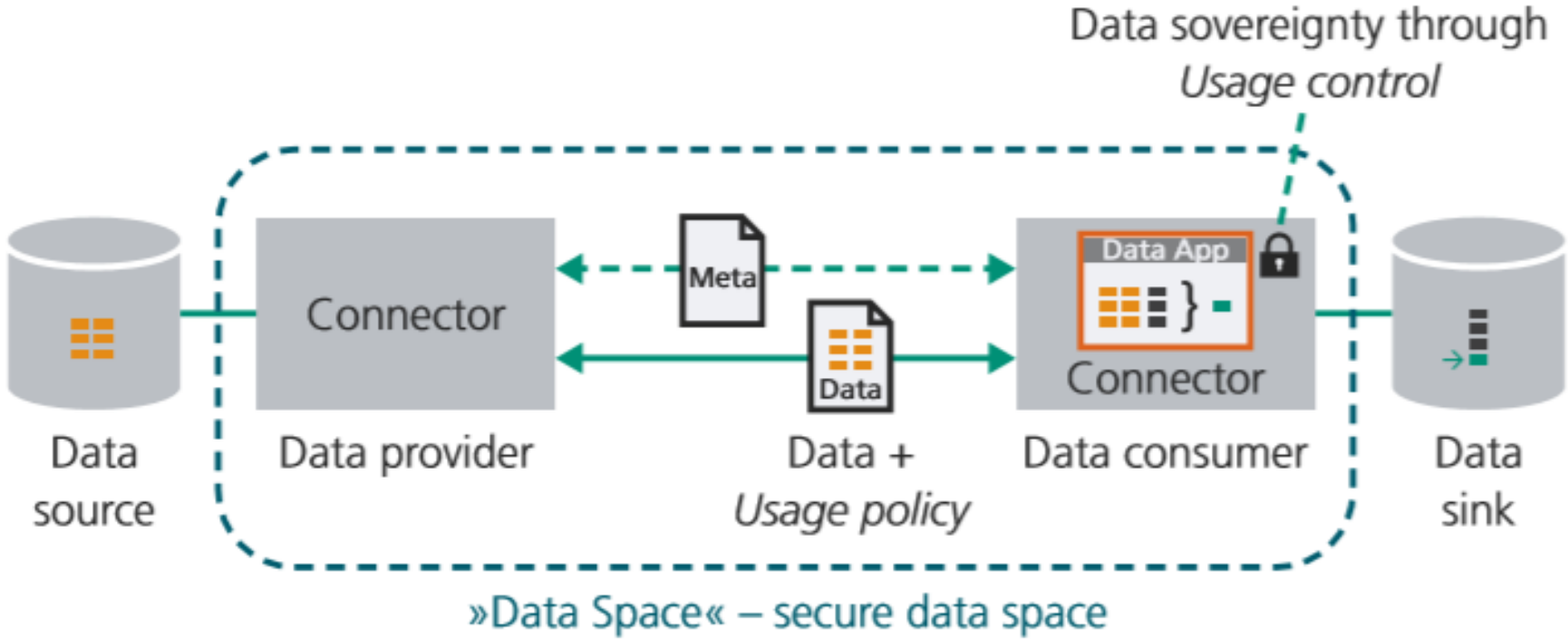
What is the IDS(A) ?

- International Data Spaces
  - Data Space for Decentralized Data Sharing
  - Reference Architecture



Fraunhofer

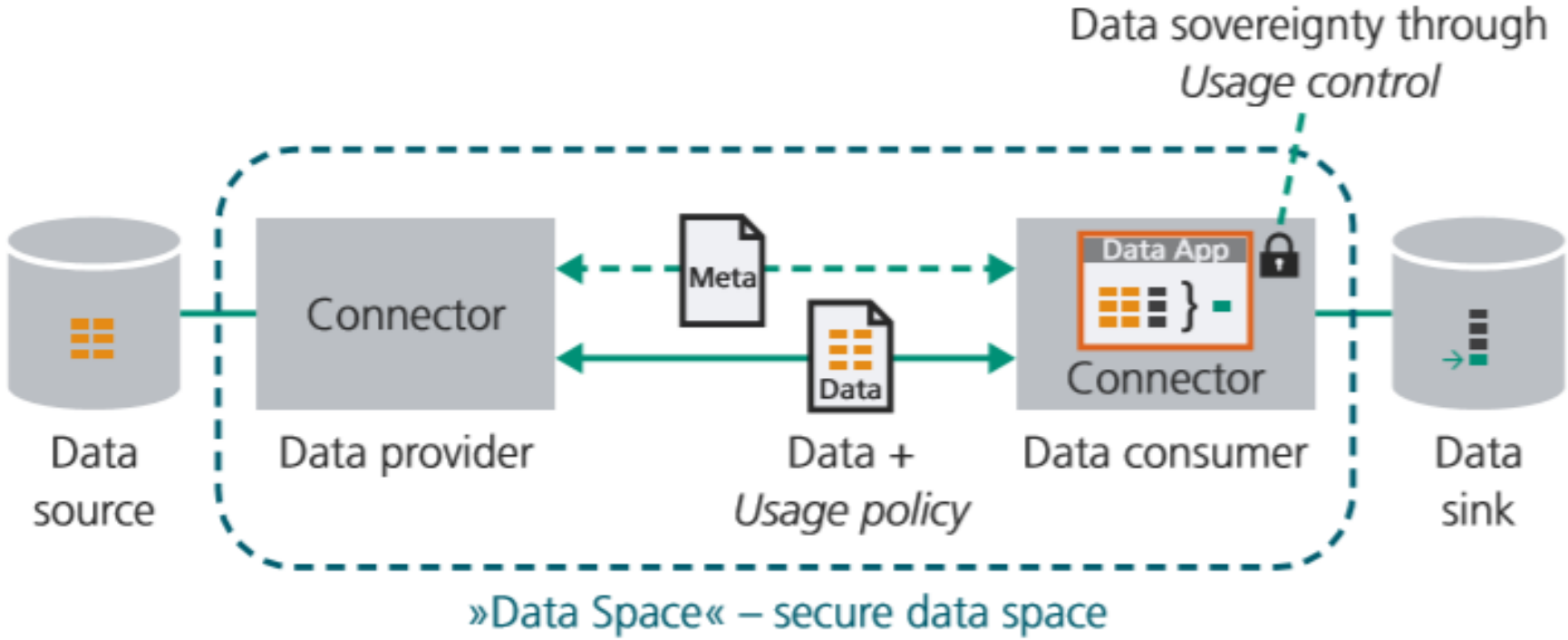
The Basic Data Sharing Infrastructure



- Idea
  - Connectors encapuslate Data Apps and communicate with other
  - Data Apps are regualated and monitored to comply with the Usage Policies inside of a Connector

Fraunhofer

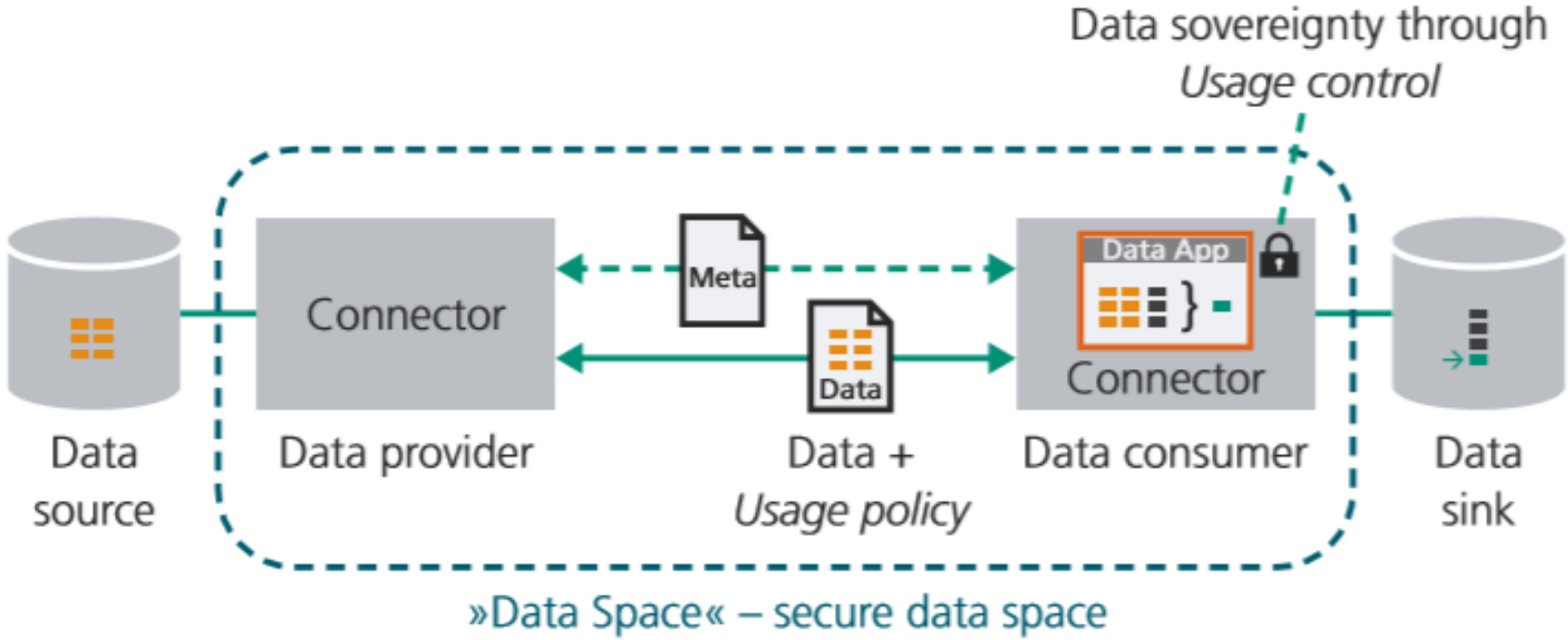
The Basic Data Sharing Infrastructure



- Problems in this Setting
  - How to model Usage Policies ?
  - How to ensure them ?

Fraunhofer

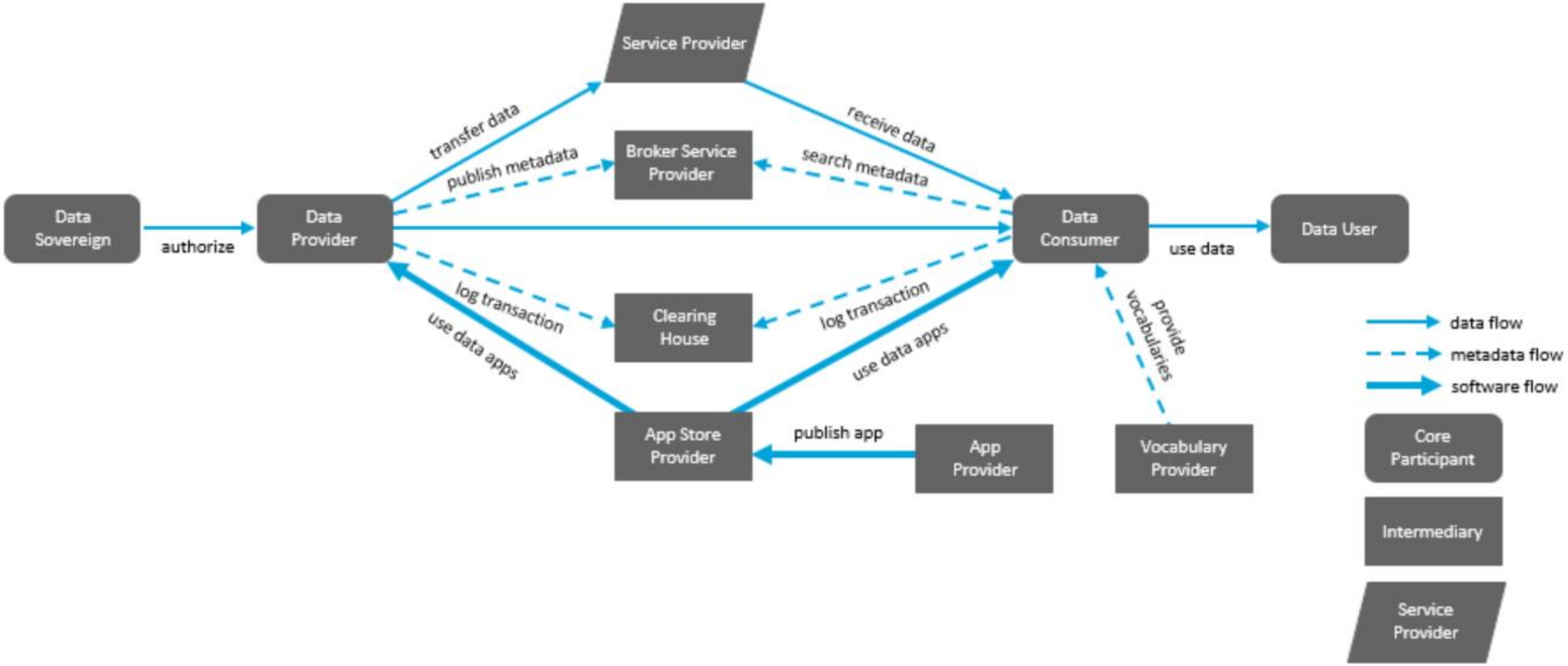
The Basic Data Sharing Infrastructure



- Problems with the Setting
  - Only two Connectors are Participating
  - How to cope with new Connectors / new Data
  - How verify the „Correctness“ ?

Fraunhofer

The Full Data Sharing Infrastructure



Fraunhofer

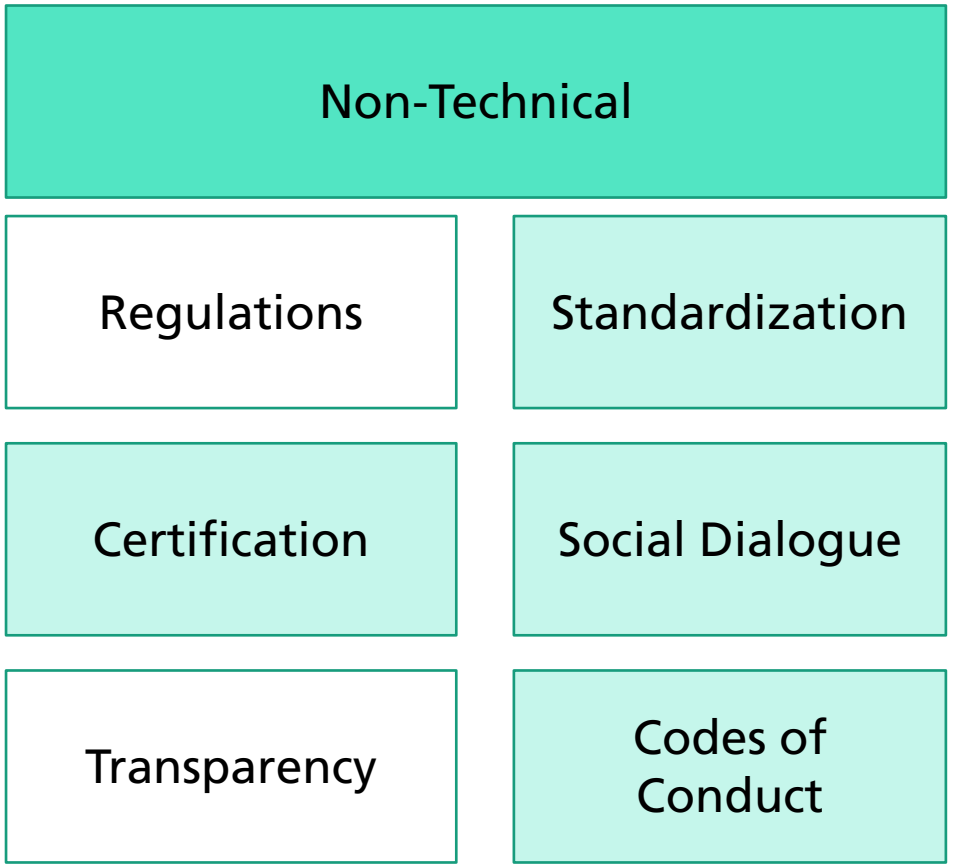
Participant Management and Certificates

- Two mechanisms are in place for Identity Mangement
  - ParIS : A catalogue of registered and authenticated users of the data ecosystem
    - Roles and authorities are published
    - Information managed by the connector providers
    - Only organisations with valid certificates are allowed to publish their internal structures
  - Certificates:
    - Organisational certificates -> Information about legal entities
    - Component certificates -> Information about used software

Institutional Trustworthiness in the International Data Space Association

Fraunhofer

Aspects of Institutional Trustworthyness



Fraunhofer

Standardisation

- External standards
  - Modeling and provisioning of all information according to W3C standards
  - Communication only over standardized interfaces (REST / HTTP Multipart / IDSCP)

Fraunhofer

Standardisation

- External standards
  - Modeling and provisioning of all information according to W3C standards
  - Communication only over standardized interfaces (REST / HTTP Multipart / IDSCP)
  - All organizations are complient with ISO 27001:2013
  - All software is complient with ISO 9001 / IEC 62443

Standardisation

- Internal Standards
  - Publicly available specification for all requirements for components
  - Specifications defined as an open community effort

SPECIFICATION: IDS META DATA BROKER

WHITE PAPER 2020

SPECIFICATION: IDS CLEARING HOUSE

WHITE PAPER 2020

CRITERIA CATALOGUE: COMPONENTS – CONNECTOR

WHITE PAPER 2020

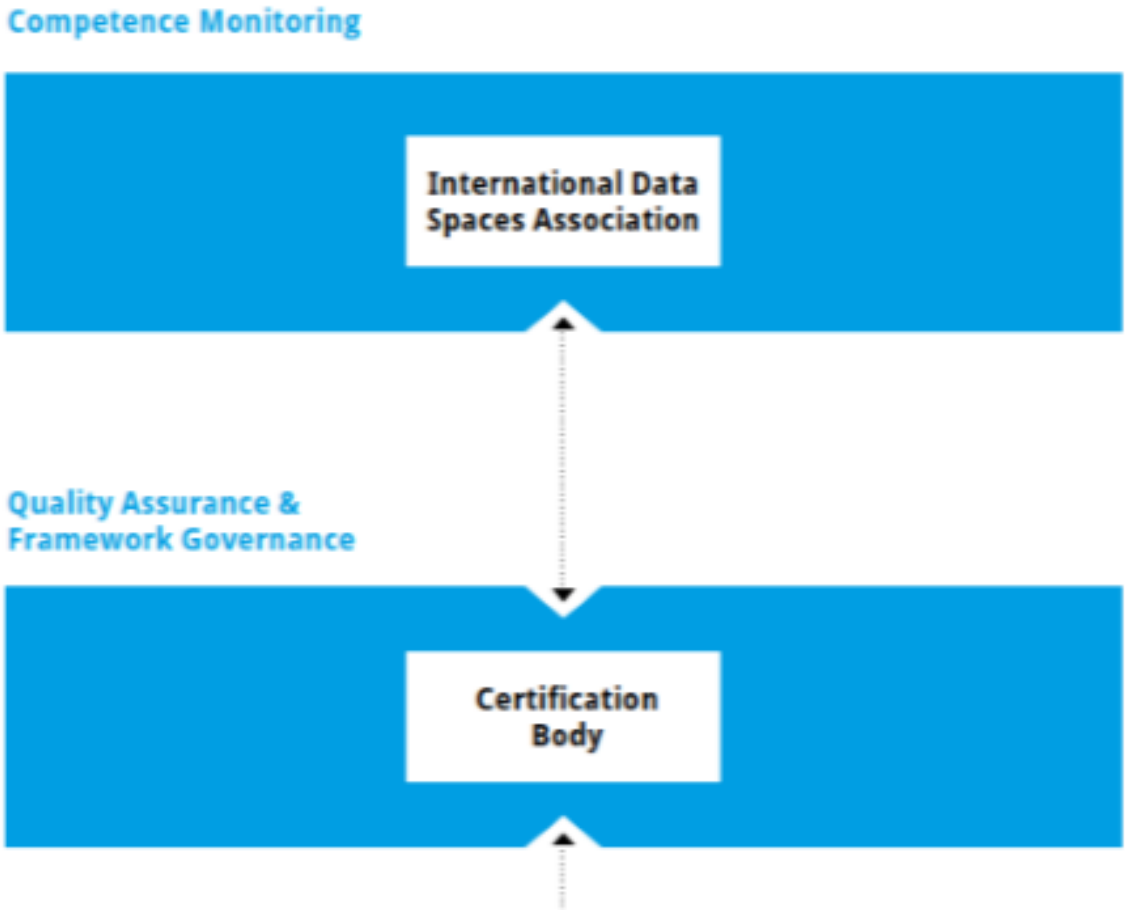
Fraunhofer

IDS Certification

- Seperation between component and organization
  - Only certified components by certified organizations are allowed to participate
  - Software developer is not necessarly also the provider
  - Certified organziations can purchase different components from different providers

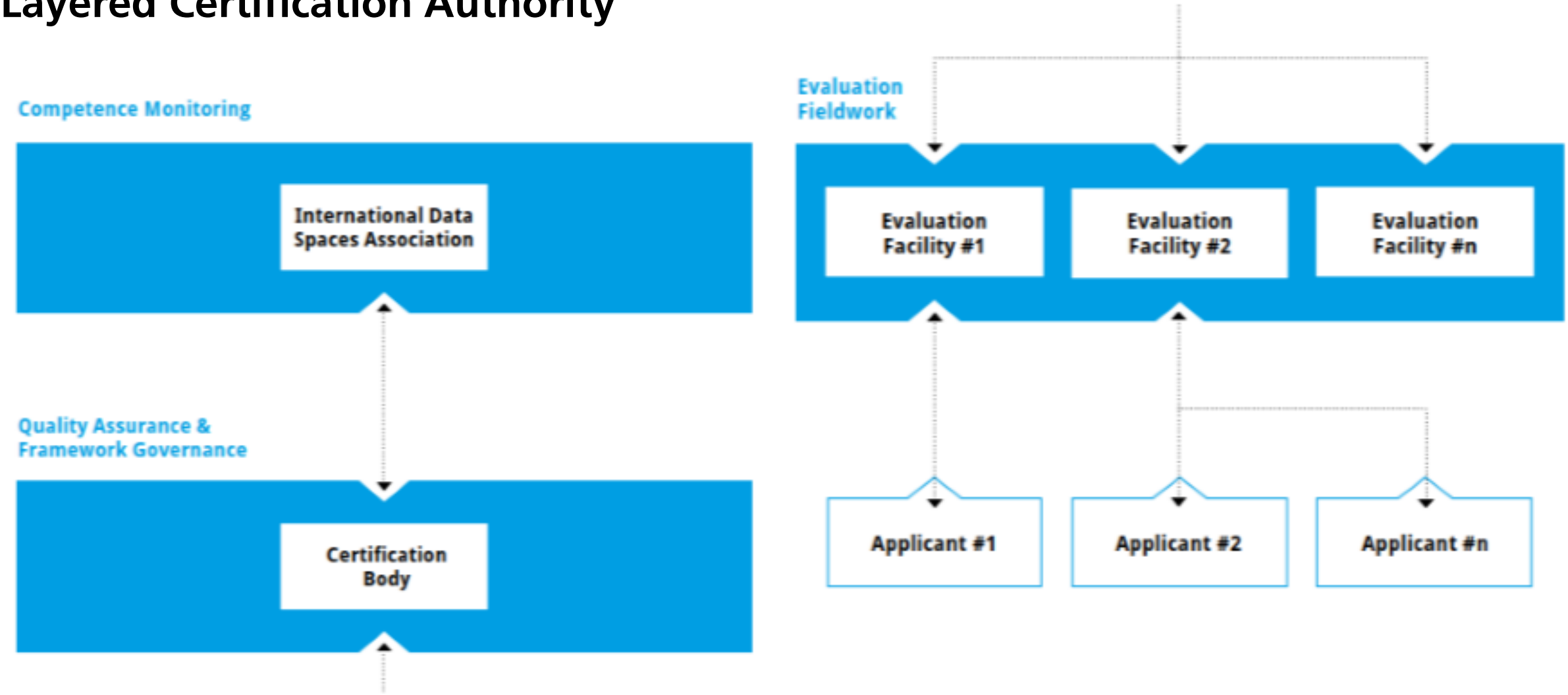
Fraunhofer

Layered Certification Authority



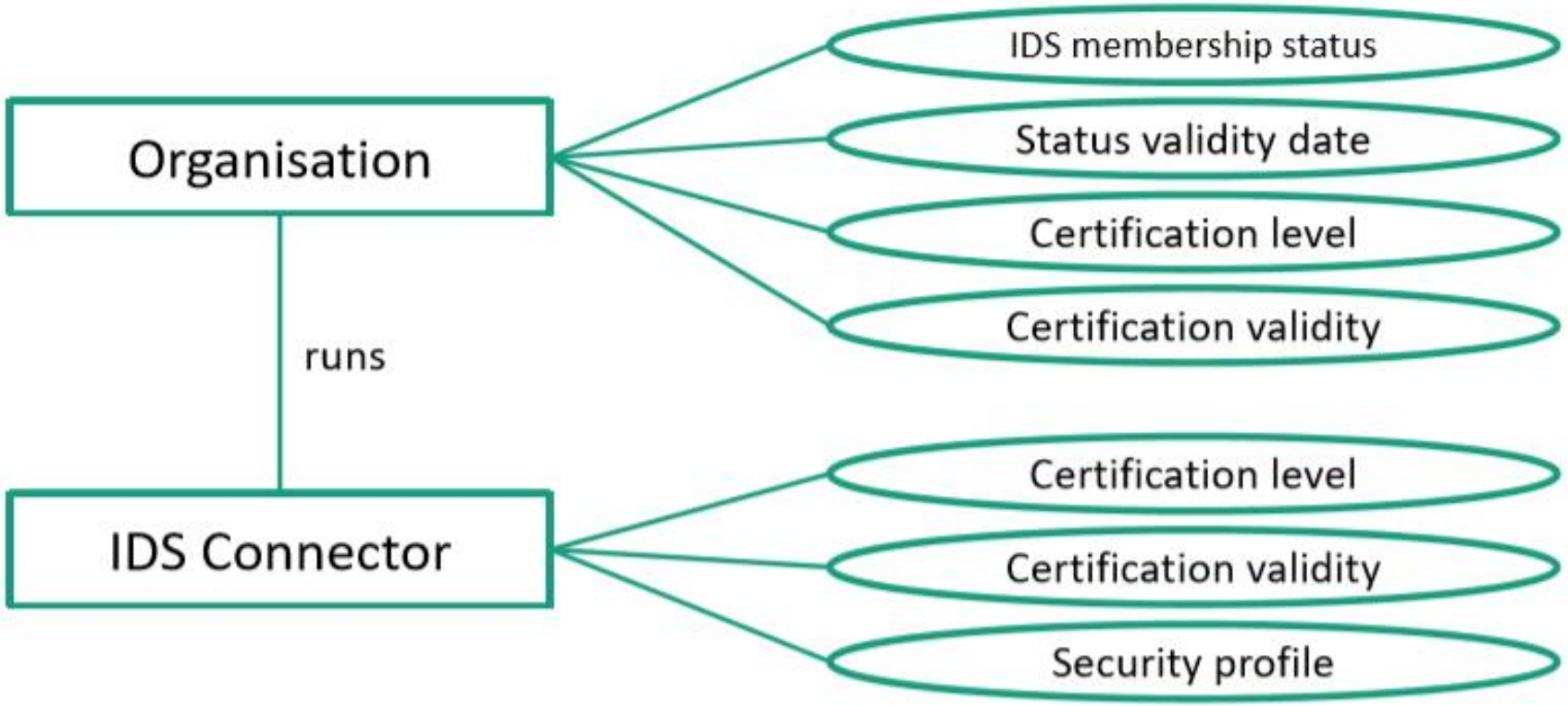
Fraunhofer

Layered Certification Authority



Fraunhofer

Certification in the Technical Environment



Fraunhofer

Social Dialogue – Diversity is the key

- Members of the IDSA are:
  - Research institutes
  - Component developers
  - Auditing companies
  - Federal institutions
  - Use case partners / industry partners

- The creation of all official documents
  - Is an open process
  - Approved by an elected steering comitee

Fraunhofer

Social Dialogue – Open Community Efforts

- Documents (onboarding / presentations / specificaitons) are publicly available
- Knowledge sharing events are publicly announced and conducted
  - Workshop series are available on youtube
  - Presentation slides are published online
- Reference architecture components almost fully published open-source

Code of Conduct

- The Development of a Code of Conduct is in process
  - Incoorporates all Agreements, that are not ensured by Laws, Specifications or Certifications
  - Covers Ethical Principles of Data Sharing
  - Based on Existing Code of Conduct initiavies
    - Sitras Rulebook for Fair Data Sharing
    - iShare Agreement

BREAK

Fraunhofer

Breakout Sessions

Individual Part (5-10 Minutes)

- Create a 1-Slide Presentation:
  - Describe your particular UseCase / Service / Idea (2-3 Sentence)
  - What aspects of data – sovereignty, trustworthyness did you not thought about yet ?
  - What are your initial ideas to solve them ?

Community Part (10 Minutes)

- Voluntarily present your use case (2-3 minutes, max 2 use cases)
  - Receive a short public community feedback

Fraunhofer

Breakout Sessions (Discussion)

Individual Part

- Create a 1-Slide Presentation:
  - Describe your particular UseCase / Service / Idea (2-3 Sentence)
  - What aspects of data – sovereignty, trustworthyness did you not thought about yet ?
  - What are your initial Ideas to solve them ?
- Enjoy the Break

Community Part

- Voluntarily present your Use Case (2-3 minutes, max 2 Use Cases)
  - Receive a short public Community feedback

Modelling Digital Contracts

Fraunhofer

Requirements

- Usage rights should be readable by
  - Machines
  - Humans
- Not only cover standard licences
  - Customizable
  - Negotiatable

Requirements

- Usage rights should be readable by
  - Machines
  - Humans

- Not only cover standard licences
  - Customizable
  - Negotiatable

Solution: Define a formal Language based on RDF!

Usage Rights

Usage rights in the IDS are always bound to a particular resource. The stakeholder of the resource specifies the terms and conditions.

The Usage rights may specify for example ...

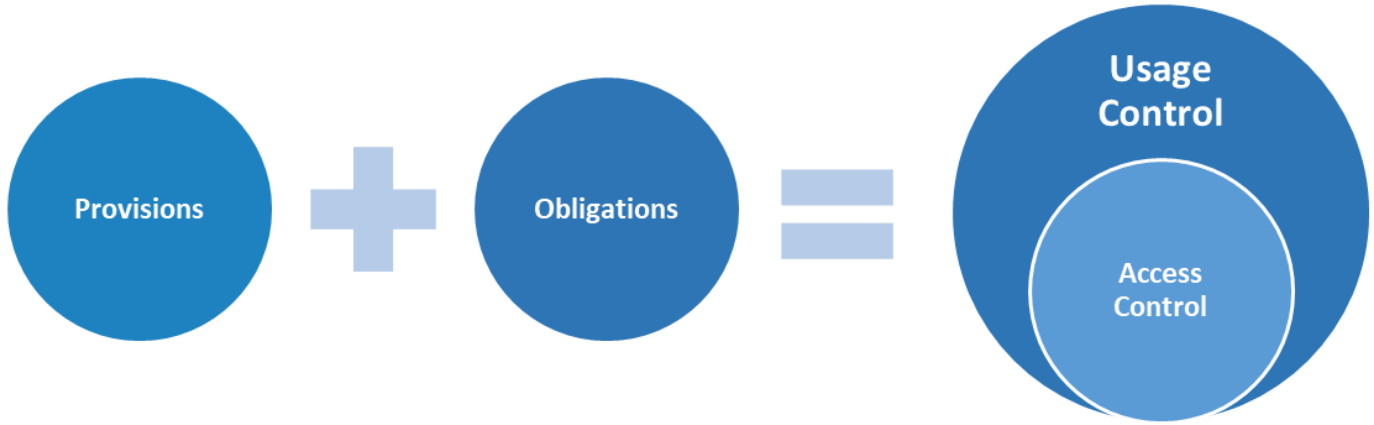
- … that only particular organisations are allowed to use the data
- … that technological standards are required for using the data
- … only specific conditions, where the data can be used (geographical bounding, time constraints)

Usage Rights

Usage rights in the IDS are always bound to a particular resource. The stakeholder of the resource specifies the terms and conditions.

We need to consider two subtypes

- Access Control
- Usage Control



Defintion of the Rights

The IDS usage policy language is a deriviation of the ODRL (Open Digital Rights Language)

```
{
 "@context": "http://www.w3.org/ns/odrl.jsonld",
 "@type": "Set",
 "uid": "http://example.com/policy:1010",
 "permission": [{
        "target": "http://example.com/asset:9898.movie",
        "action": "display",
        "constraint": [{
           "leftOperand": "dateTime",
           "operator": "gt",
           "rightOperand":  { "@value": "2019-01-01", "@type": "xsd:date" }
       }]
 }]
}
```

Source: https://w3c.github.io/odrl/bp/

Concepts of ODRL

Policy
A group of one or more Rules

Rule
An abstract concept that represents the common characteristics of Permissions, Prohibitions, and Duties.

Action
An operation on an Asset

Permission
The ability to exercise an Action over an Asset

Prohibition
The inability to exercise an Action over an Asset

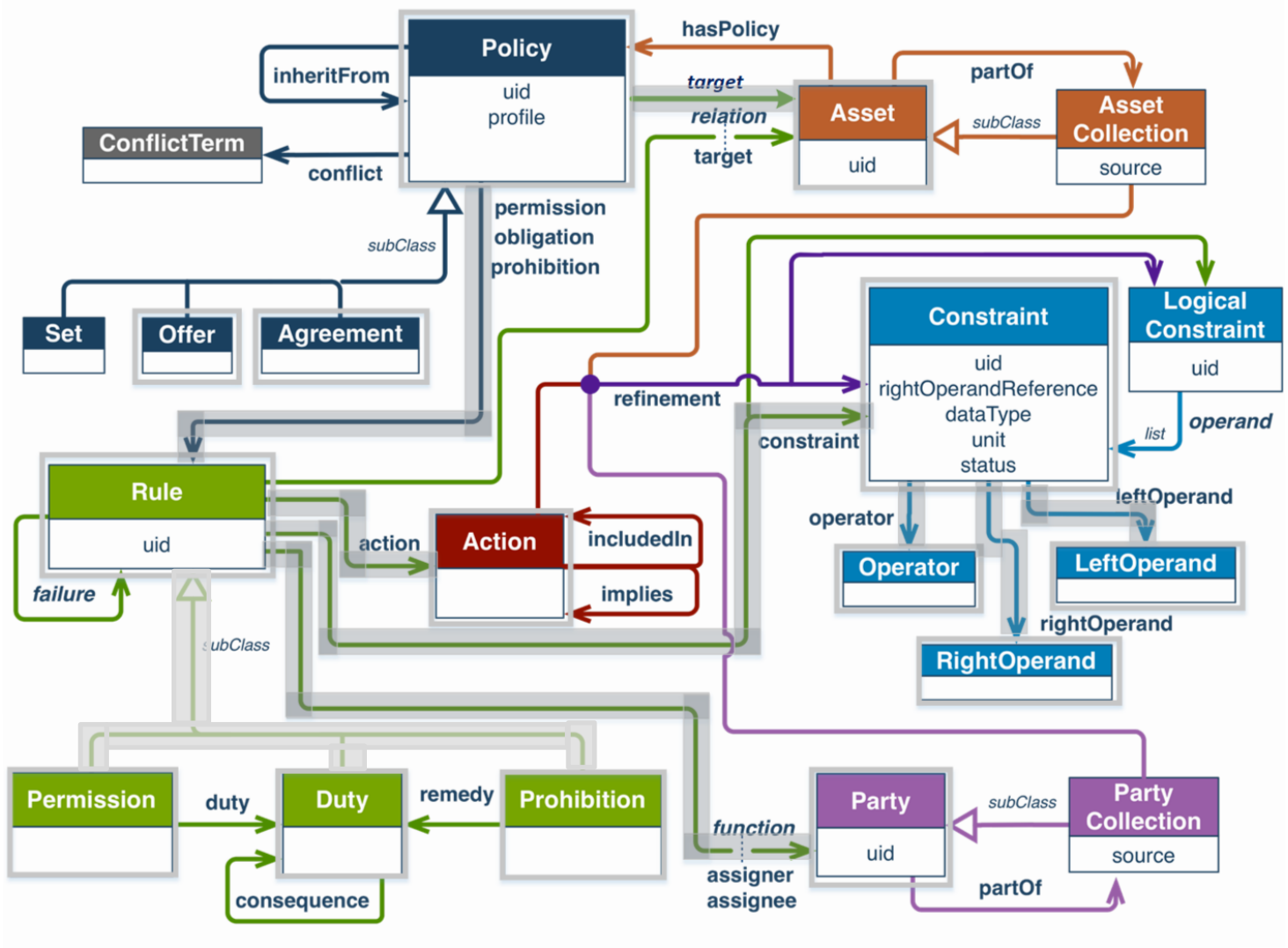
Duty
The obligation to exercise an agreed Action.

Asset
A resource or a collection of resources that are the subject of a Rule

Party
An entity or a collection of entities that undertake Roles in a Rule

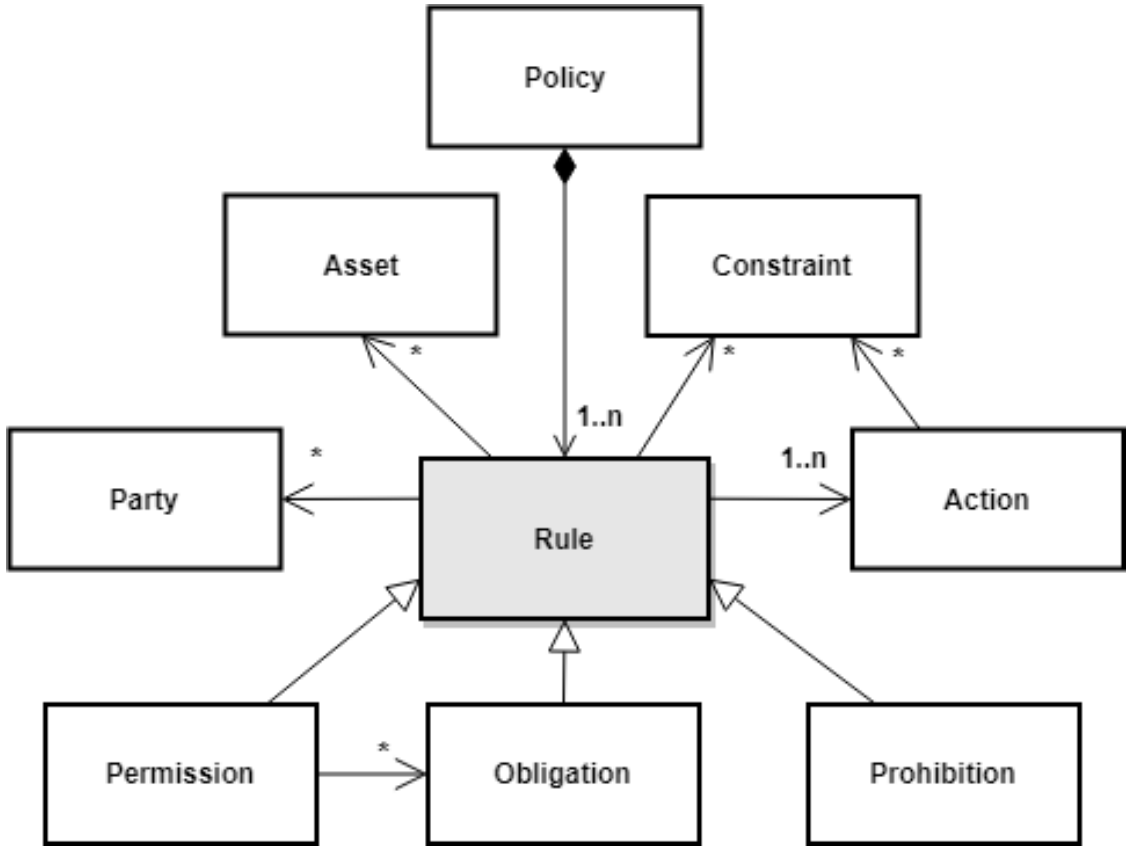
Constraint
A boolean/logical expression that refines an Action and Party/Asset collection or the conditions applicable to a Rule.

Definition of Rights (ODRL vs. IDS Information Model)



Fraunhofer

Definition of Rights in the IDS – Concept View



IDS-Vocabular: Provider, Consumer , Contracts

Contract[c]

back to ToC or Class ToC

IRI: https://w3id.org/idsa/core/Contract

Abstract set of rules governing the usage of a Resource.

has super-classes

policy [c]

has sub-classes

Contract agreement [c], Contract offer [c], Contract request [c]

is in domain of

Annex to contract [op], Consumer [op], Contract date [dp], Contract document [op], Contract end [dp], Contract start [dp], Provider [op], obligation [op], permission [op], prohibition [op], refers to policy template [op]

is in range of

transferContract [op]

Participant[c]

back to ToC or Class ToC

IRI: https://w3id.org/idsa/core/Participant

Stakeholder in the Industrial Data Space, assuming one or more of the predefined roles; every participant is given a unique identity by the Identity Provider.

has super-classes

Agent [c], Managed entity [c], organization [c]

is in domain of

corporateEmailAddress [dp], corporateHomepage [dp], industrial classification [op], member participant [op], memberPerson [op], participant certification [op], primarySite [op]

is in range of

Consumer [op], Provider [op], Requested Participant [op], affected Participant [op], assignee [op], assigner [op], curator [op], endedBy [op], maintainer [op], member participant [op], startedBy [op]

Source: https://industrialdataspace.github.io/InformationModel/docs/index.html

IDS-Vocabular: Rules, Permissions, Actions

Rule[c]

back to ToC or Class ToC

IRI: https://w3id.org/idsa/core/Rule

Superclass of Permissions, Prohibitions and Duties.

has super-classes
described [c], rule [c]

has sub-classes
Duty [c], Permission [c], Prohibition [c]

is in domain of
action [op], assignee [op], assigner [op], constraint [op], target [op], target content [op]

Permission[c]

back to ToC or Class ToC

IRI: https://w3id.org/idsa/core/Permission

The class of Permissions as defined in the ODRL ontology.

has super-classes
Rule [c], permission [c]

is in domain of
duty [op]

is in range of
permission [op]

Action[c]

back to ToC or Class ToC

IRI: https://w3id.org/idsa/core/Action

A thing one might be permitted to do or prohibited from doing to something.

has super-classes
action [c]

is in domain of
action refinement [op]

is in range of
action [op]

has members
anonymize [ni], attribute [ni], compensate [ni], delete [ni], distribute [ni], grant use [ni], log [ni], read [ni], track provenance [ni], use [ni]

IDS-Vocabular: Constraints on Rules

Constraint[C]

back to ToC or Class ToC

IRI: https://w3id.org/idsa/core/Constraint

The class of Constraints that restrict a Rule.

has super-classes
constraint [C]

is in domain of
leftOperand [op], operator [op], rightOperand [dp], unit [op]

is in range of
action refinement [op], constraint [op], content refinement [op]

Source: https://industrialdataspace.github.io/InformationModel/docs/index.html

IDS-Vocabular: Constraints on Rules

Constraint[c]

back to ToC or Class ToC

IRI: https://w3id.org/idsa/core/Constraint

The class of Constraints that restrict a Rule.

has super-classes
constraint [c]
is in domain of
leftOperand [op], operator [op], rightOperand [dp], unit [op]
is in range of
action refinement [op], constraint [op], content refinement [op]

rightOperand[dp]

back to ToC or Data Property ToC

IRI: https://w3id.org/idsa/core/rightOperand

has domain
Constraint [c]
has range
literal
is also defined as
annotation property

BinaryOperator[c]

back to ToC or Class ToC

IRI: https://w3id.org/idsa/core/BinaryOperator

The class of binary operators.

has super-classes
operator [c]
is in range of
operator [op]
has members
after [ni], before [ni], equals [ni], greater than [ni], greater than or equals [ni], has Role [ni], in [ni], in time interval [ni], less than [ni], less than or equals [ni], remote [ni]

LeftOperand[c]

back to ToC or Class ToC

IRI: https://w3id.org/idsa/core/LeftOperand

Instances of the LeftOperand class are used as the leftOperand of a Constraint.

has super-classes
left operand [c]
is in range of
leftOperand [op]
has members
Absolute geo-spatial position [ni], count [ni], now [ni], payAmount [ni], purpose [ni], quantity [ni], recurrenceRate [ni], securityLevel [ni], state [ni], user [ni]

Source: https://industrialdataspace.github.io/InformationModel/docs/index.html

A Digital Contract in Place


```
{
  "@context" : {
    "ids" : "https://w3id.org/idsa/core/",
    "idsc" : "https://w3id.org/idsa/code/"
  },
  "@type" : "ids:ContractOffer",
  "@id" : "https://w3id.org/idsa/autogen/contractOffer/f70af0ab-c447-4521-b92b-60fe69dfab94",
  "ids:permission" : [ {
    "@type" : "ids:Permission",
    "@id" : https://w3id.org/idsa/autogen/permission/4d9e77bd-d89f-4c99-ad25-87bd141d878e,
     "ids:action" : [ {
      "@id" : "idsc:USE"
    } ],
    "ids:targetArtifact" : {
      "@type" : "ids:Artifact",
      "@id" : "https://w3id.org/idsa/autogen/artifact/e16d01c8-60da-47d0-b1dc-b10a65e432d8",
      "ids:fileName" : "demoArtifcat2.xml",
      "ids:byteSize" : 455
    }
    "ids:constraint" : [ {
      "@type" : "ids:Constraint",
      "@id" : "https://w3id.org/idsa/autogen/constraint/8349d464-287a-43ae-b6e9-0ca48ef36d1e",
      "ids:leftOperand" : {
        "@id" : "idsc:ABSOLUTE_SPATIAL_POSITION"
```

A Digital Contract in Place


```
},
    "ids:operator" : {
      "@id" : "idsc:INSIDE"
    },
    "ids:rightOperandReference" : {
      "@id" : "https://www.wikidata.org/wiki/Q3308569"
    }
  }, {
    "@type" : "ids:Constraint",
    "@id" : "https://w3id.org/idsa/autogen/constraint/8c1de585-3188-4428-ac45-99dfb6a4ba04",
    "ids:leftOperand" : {
      "@id" : "idsc:POLICY_EVALUATION_TIME"
    },
    "ids:operator" : {
      "@id" : "idsc:BEFORE"
    },
    "ids:rightOperandReference" : {
       "@value" : "2000-07-30T00:00Z",
       "@type" : "http://www.w3.org/2001/XMLSchema#dateTimeStamp"
    }
  } ],
}
```


Fraunhofer

Thank you for your Attention!

Any Questions ?

Fraunhofer

Resources and Further Reading

Slides made by Dennis Oliver Kubitza

IDS in General

A. https://www.internationaldataspaces.org/
B. https://www.internationaldataspaces.org/publications/brochure-IDS-standard-for-data-sovereignty
C. https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf
D. Source: https://industrialdataspace.github.io/InformationModel/docs/index.html

Certification, Trust and Policies

A. https://www.internationaldataspaces.org/wp-content/uploads/2019/07/Trust-in-the-IDS-Nadja-and-Aleksei.pdf
B. https://www.internationaldataspaces.org/wp-content/uploads/2019/07/Trust-and-Security-in-the-IDS.pdf
C. https://www.internationaldataspaces.org/wp-content/uploads/2019/07/IDS-Policy-Language.pdf

Fraunhofer