WORKSHOP :
USAGE POLICIES IN THE IDS

V1 20.01.2021

Dennis Oliver Kubitza

Fraunhofer
IAIS

The Presenter

Dennis Kubitza
Research Engineer – Fraunhofer IAIS
dennis.oliver.kubitza@iais.fraunhofer.de

IDS(A) Involements:

- Responsible Developer of the Enterprise Integration Connector
- AP Lead in the Moblity Data Space Project
- Co-Auther of the SPECIFICATION: IDS META DATA BROKER and CRITERIA CATALOGUE: COMPONENTS – BROKER

Scope of this Presentation

- **Topic:** Overview of Concepts in the IDS related to Usage Control & Usage Policies
- **Target Audience:** IDSA Members who seek knowledge about the conceptualization and implementaion of Usage Control in the IDS
- **Goal:** Form the Basis for further Joined Task Forces to solve legel Problems with Usage Control

Scope of this Presentation

- **Topic:** Overview of Concepts in the IDS related to Usage Control & Usage Policies
- **Target Audience:** IDSA Members who seek knowledge about the conceptualisation and implementaion of Usage Control in the IDS
- **Goal:** Form the Basis for further Joined Task Forces to solve legel Problems with Usage Control

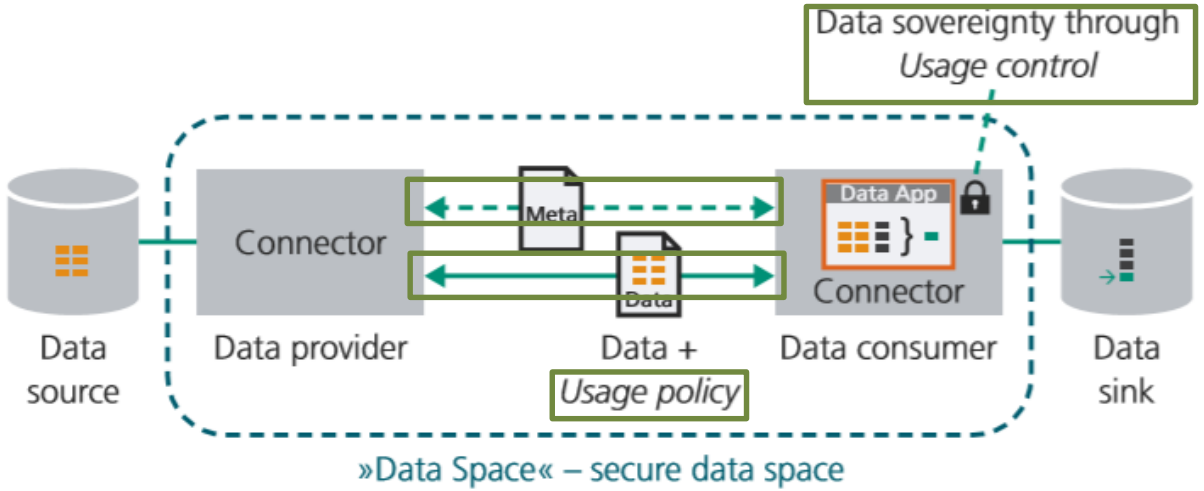


Figure: Data Exchange in the IDS between Connectors, with Focus Areas of the Discussion

Table of Contents

1. Modellation of Contractas – The IDS Policy Language

The IDS Policy Language

- Is a Machine readible representation of Contracts and Usage Policies
- Part of the Information Modell
- Modelling Capabilities: Actions, Geographic Positions, Time Constraints, Logical Expressions, Endpoints

Goal: Digital Contracts should be defined/translatable to be binding to regulations.

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.

IDS-Extensions: Contracts, Participants

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

Fraunhofer IAIS

A Digital Contract in Place

```
@prefix ns0: <https://w3id.org/idsa/core/> .
@prefix xsd: <http://www.w3.org/2001/XMLSchema#> .

<https://w3id.org/idsa/autogen/contractAgreement/11544585-8707-4758-94cb-ad8634f4ac88>
                a <https://w3id.org/idsa/core/ContractAgreement> ;
                ns0:contractStart "2020-10-02T14:25:47.355+02:00"^^xsd:dateTimeStamp ;
                ns0:permission <https://w3id.org/idsa/autogen/permission/60c24c3c-9a84-4528-8d78-834fb1543a1f> .

<https://w3id.org/idsa/autogen/permission/60c24c3c-9a84-4528-8d78-834fb1543a1f>
                a ns0:Permission ;
                ns0:action <https://w3id.org/idsa/code/USE> ;
                ns0:assignee <http://njh.me/www.example.org/YourURI> ;
                ns0:assigner <http://ExampleSoftwareInstitute.mobids.de> ;
                ns0:targetArtifact <https://w3id.org/idsa/autogen/artifact/ce760269-cde8-4d73-a473-307e3f6fdffd> .

<http://njh.me/www.example.org/YourURI>
                 a ns0:Participant ;
                ns0:corporateEmailAddress "mail@example.org"^^xsd:string ;
                ns0:corporateHomepage <http://njh.me/www.example.org/ExampleConsumer> .

<http://ExampleSoftwareInstitute.mobids.de>
                a ns0:Participant ;
                ns0:corporateEmailAddress "example.Person@example.company"^^xsd:string ;
                ns0:corporateHomepage <https://www.example.company/us/> .

<https://w3id.org/idsa/autogen/artifact/ce760269-cde8-4d73-a473-307e3f6fdffd>
                a ns0:Artifact ;
                ns0:byteSize 0 ;
                ns0:fileName "EM_FCD_UI_City.csv "^^xsd:string .
```

Current Problems

Actions, Participants need a proper legal / human readable definition, that is well defined. How can we ensure this ?

Are we allowed to interprete these Policy Language to legal Contracts ?

What measures can we deploy to interpret them as legal Contracts (f.e deterministic Conversion to Human Language)

Ids:Grant_USE: "To grant use of a resource to another party. Does *not* imply any other usage rights."@en ;

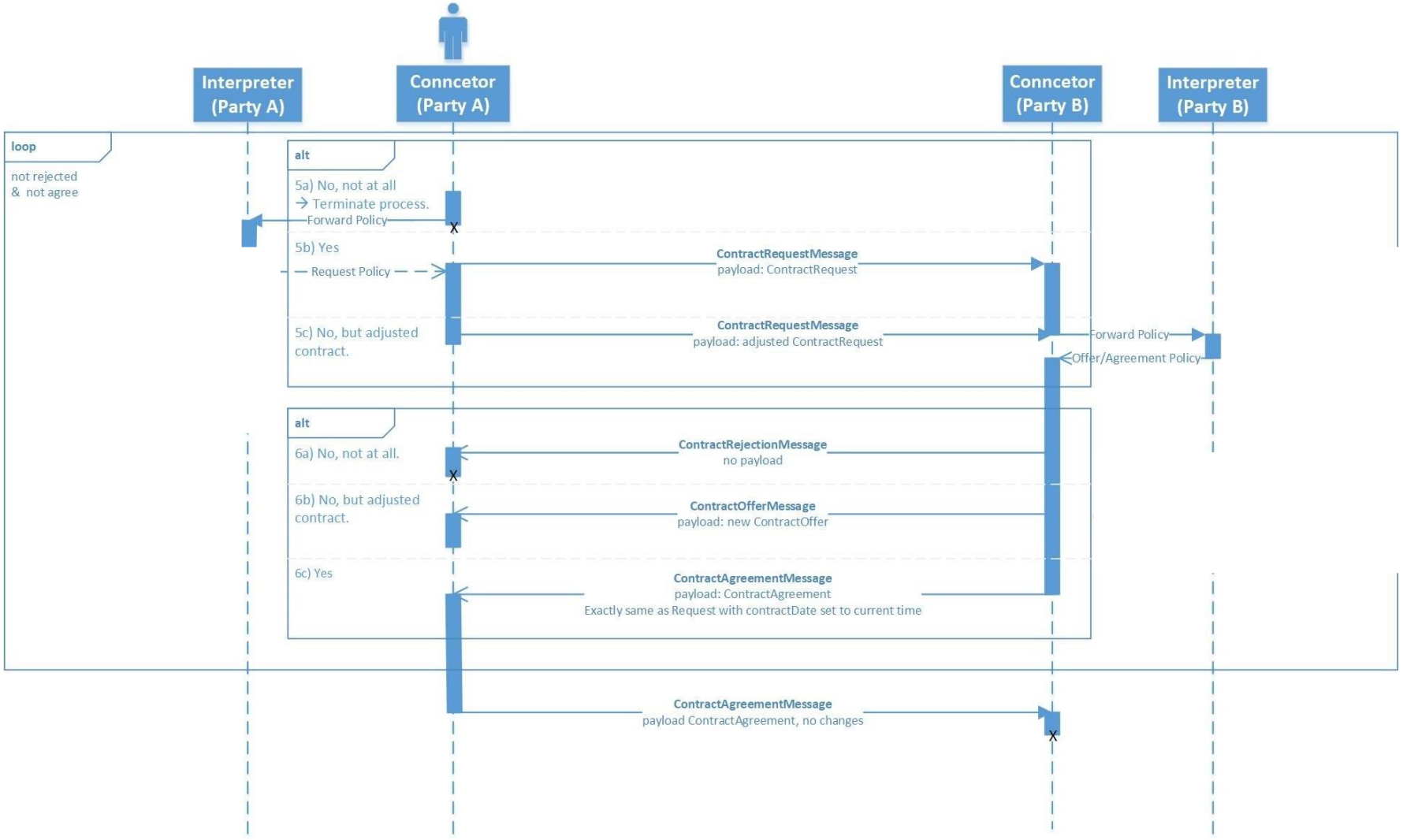
2. Modellation of Contractas – Contract Handshake

The Contract Handshake

- Is a sequence of Interactions between connectors
- Based on a three way Handshake
- Does not have to Supervised by a User (from a technical point of view)
- Process might be oversighted by a clearing house

Goal: Contracts agreed on by machines (Supervised or even Unsupervised) should be legally binding.

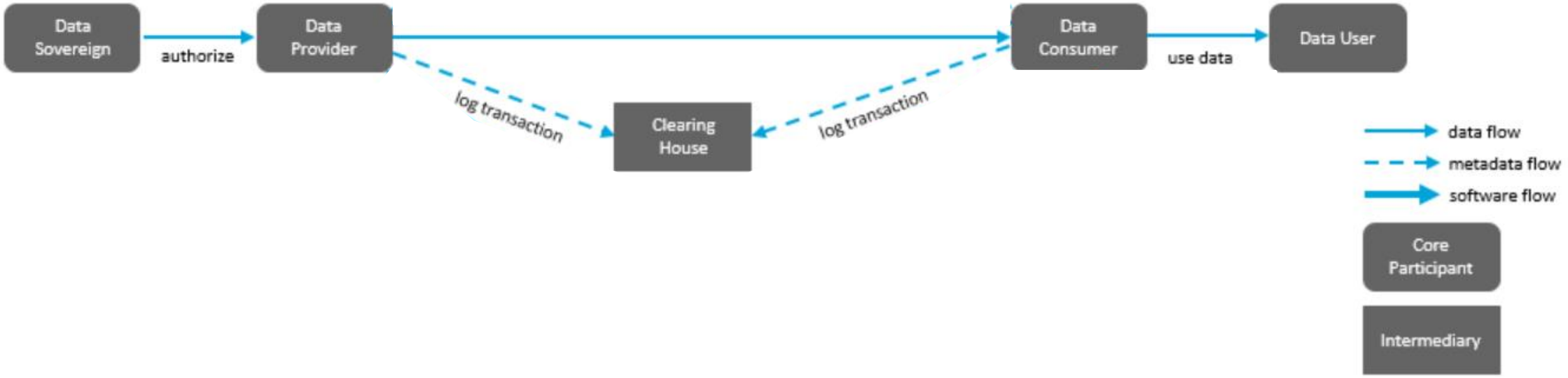
The IDS Contract Handshake



Fraunhofer IAIS

The IDS Clearing House

- Decentralized and trustworthy logging service
- Messages are persistently stored
- Authenticity of Logging Parties is technically ensured



Current Problems

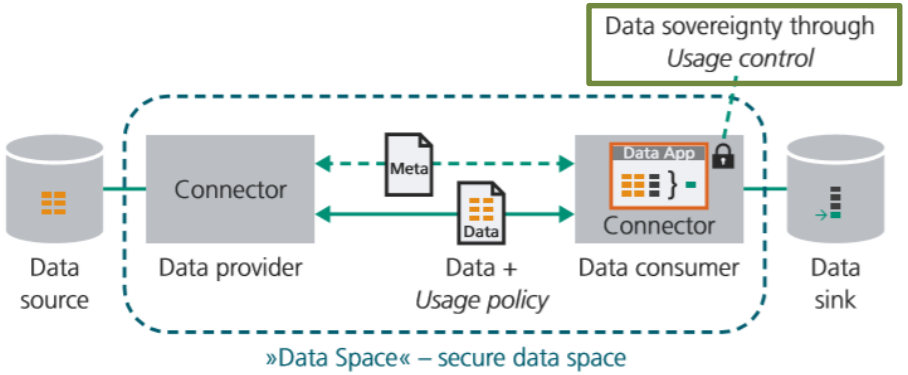
To what extend is automation allowed ?

Do we always need a superviser sending Agreements ?

What do we need to make the exchanged Contracts binding to all involved parties ?

What do we need to make the Clearing House a source for evidence ?

3. Usage Policy Enforcement – General Ideas



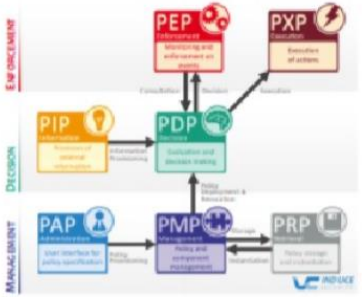
Usage Control should:

- Enforce that the exchanged Policies are ensured on a technical level
- Example: Log the Data Processing at a certain Endpoint
- Example: Permit Data leaving the Connector

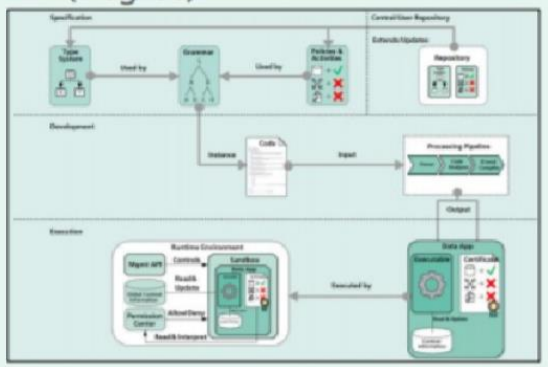
Usage Control Engines

- Several approaches to ensure Usage Control Exist
- Each of them has different capabilities

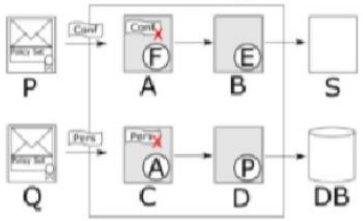
■ MYDATA Control Technologies (MYDATA)



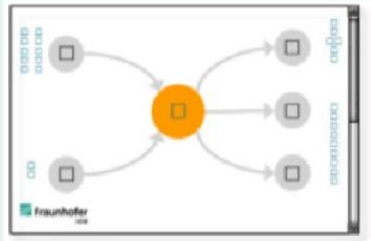
■ D° (Degree)



■ Label-based Usage Control (LUCON)



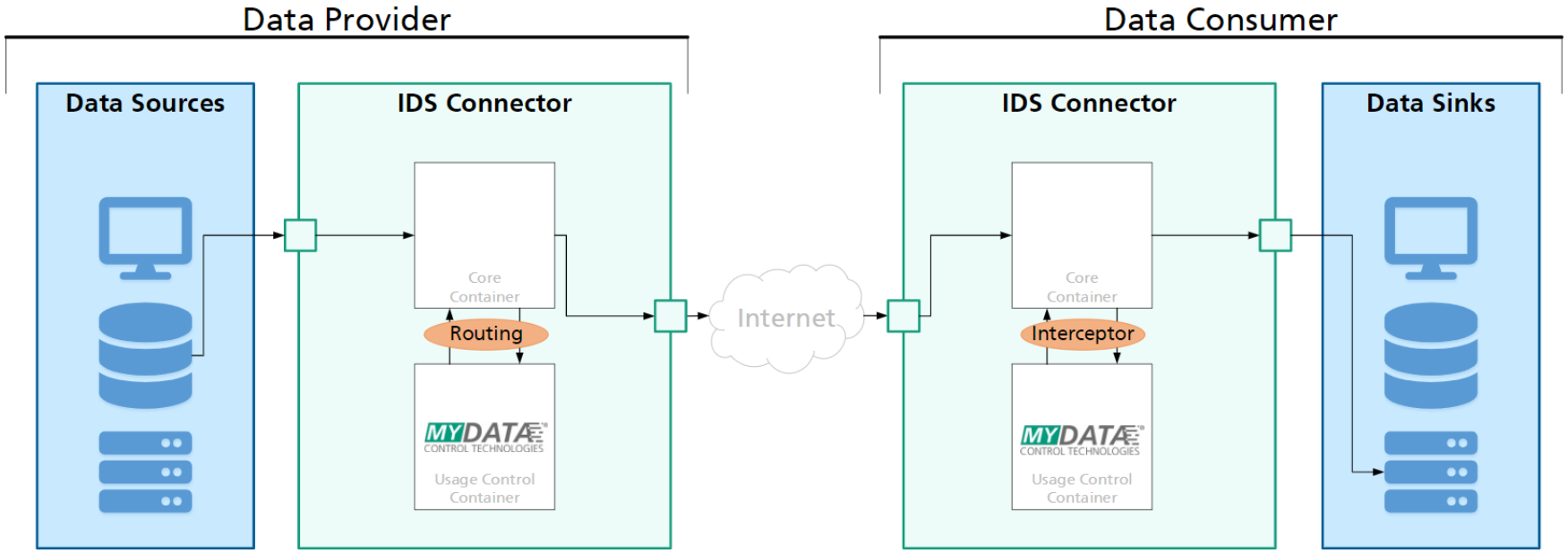
■ Information Flow Tracking (IFT)/Data Provenance



Fraunhofer IAIS

Usage Control Example: How MYDATA works

- MYDATA implements an Routing Adapter and an Interceptor Adapter
  - The Routing Adapter controlls, to which external adresses data might be forwarded
  - The Interceptor controlls every Data Flow inside of the Connector



Fraunhofer IAIS

Current Problems

To what extend is the Usage Control Engine allowed to access the data and under which conditions ?

Do we need to specify in advance from the provider side how usage Control is implemented in the recipient connector ?

4. Usage Policy Enforcement – Usage Control Patterns

Problem: The IDS Usage Policy language is to extensive for an initial implemenation and evaluation

Current Approach: The Development community focuses on example patterns, so called policy classes.

- 20 Classes exist
- All patterns contain parameterized Variables
- Usage Control Engines are implemented and Evaluated against them.

Usage Control Patterns - Example

6. Location Restricted Policy

Location areas

```
"ids:permission": {
        "ids:action": "?action" ,
        "ids:constraint": [{
                "ids:leftOperand":{"@id":"idsc:ABSOLUTE_SPATIAL_POSITION"},
                "ids:operator":{"@id":"idsc:SAME_AS" },
                "ids:rightOperandReference":{"@id":"?areaURI"},
                "ids:pipEndpoint":{"@id":"?locationPipURI"}
        }]
}
```

```
"ids:constraint" : [{
        "ids:leftOperand":{"@id":"idsc:ABSOLUTE_SPATIAL_POSITION"},
        "ids:operator":"@id":"idsc:IN",
        "ids:rightOperandReference":{"@id":["?areaURI"]},
        "ids:pipEndpoint":{"@id":"?locationPipURI"}
}]
```

18. Remote Notifications

This policy is about notifying a specific party about the data usage.

```
"ids:action": "idsc:USE" ,
"ids:postDuty": [{
        "@type": "ids:Duty",
        "ids:action": [{
                "rdf:value": { "@id": "idsc:NOTIFY" },
                "ids:actionRefinement": [{
                        "@type": "ids:Constraint",
                        "ids:leftOperand": { "@id": "idsc:RECIPIENT" },
                        "ids:operator": { "@id": "idsc:EQUALS" },
                        "ids:rightOperand": {
                                "@value": "?party",
                                "@type": "ids:participant"
                        }
                },{
                        "@type": "ids:Constraint",
                        "ids:leftOperand": { "@id": "idsc:NOTIFICATION_LEVEL" },
                        "ids:operator": { "@id": "idsc:EQUALS" },
                        "ids:rightOperand": {"@value":"idsc:DEBUG_LEVEL_LOGGING"}
                }],
                "ids:frequency": {"@id":"idsc:ANNUAL" }
        }],
        "ids:PXPEndPoint":{"@id":"?notifyPartyPXPUri"}
}]
```

Current Problems

Variables need a proper legal / human readable definition, that is well defined. How can we ensure this ?

How do we reference Entities like areas of a City, to be still binding ?

5. Certification – The Certification Process

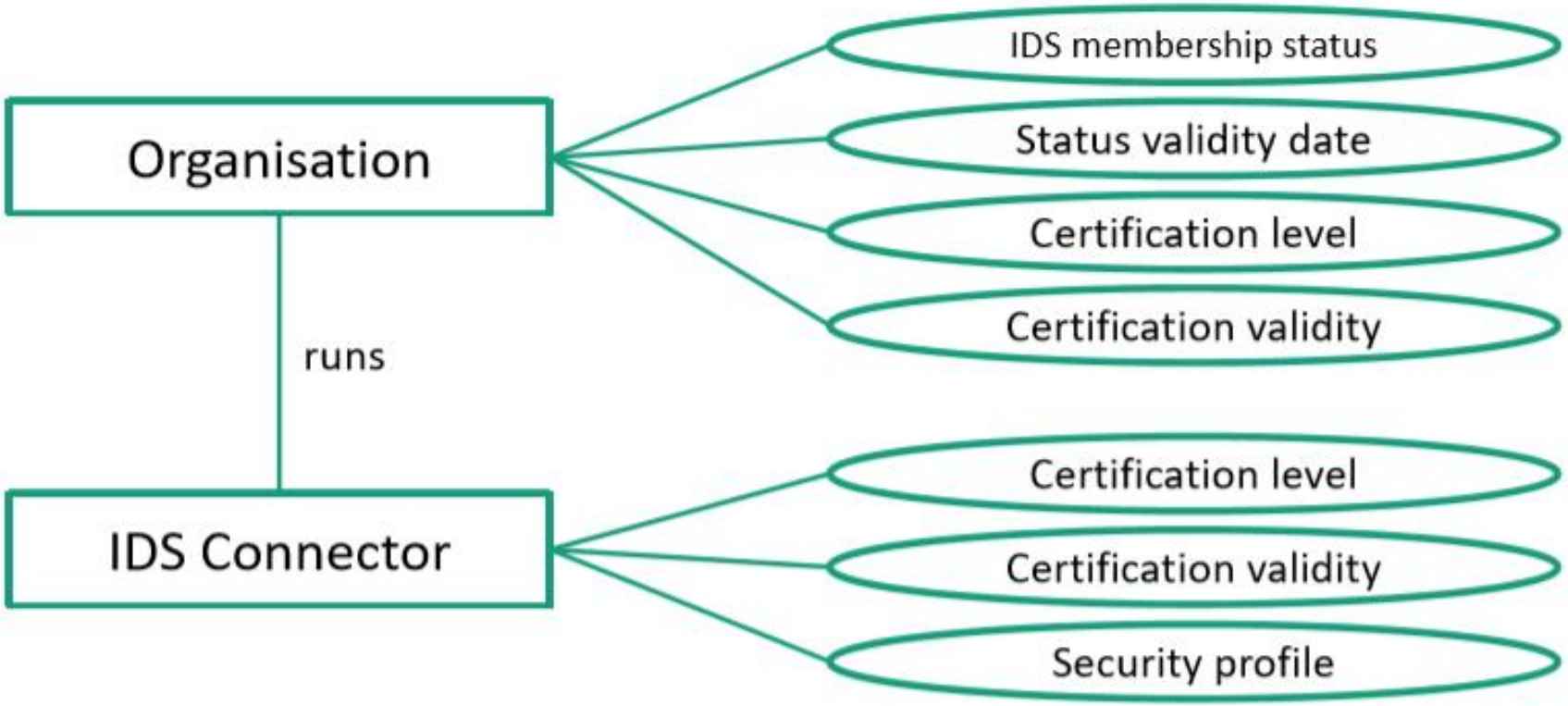
Currently the IDSA is Establishing a Certification Scheme and a Certification Body

- This is an on-going process
- Specifications for the Certification Criteria are already available
- A in detail examination catalogue is currenlty worked on

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

Overview Certificates



State of the Art

The IDSA released 4 White Papers related to Certification

- The framework for the IDS Certification Scheme
- A Criteria Catalogue for the IDS Broker (3 different Levels)
- A Criteria Catalogue for an IDS Connector (3 different Levels)
- A Criteria Catalogue of the Operational Environments. (3 different Levels)

All Levels are dealing with Usage Control and Policies to different extends.

Current Problems

The Certification Criteria are currently derived partially from Law Regulations (IT Security, etc.). Are there any parts of the rule book or laws on contracts, that should also be considered ?

Certification – Current Criteria for Policy Enforcement

The IDS Certification Criterias currently define 5 Requirements for Usace Control

ID	Criteria Title	Base	Trust	Trust+
IDS Specification (Component: Connector)				
Data Usage Control				
USC 01	Definition of usage policies	x	x	x
USC 02	Sending of usage policies	-	x	x
USC 03	Usage policy enforcement	-	x	x
USC 04	Usage policy changes	-	x	x
USC 05	Usage policy changes by administrator	-	-	x

Criteria Details

USC 01 Definition of usage policies

- Connector allows data providers to define usage policies that will be published together with the data offered

USC 02 Sending of usage policies

- Connector offering data sends usage policy to be applied to Connector requesting data every time connection is established.

USC 03 Usage policy enforcement

- Connector facilitates technical enforcement of data usage policy specified.

Certification – Current Criteria for Policy Enforcement

USC 04 Usage policy changes

- Changes to data usage policy can be made only by the data owner or data provider. In case of changes made to policy, connection between two Connectors is re-established.

USC 05 Usage policy changes by administrator

- The administrators of the data provider side cannot change rules regarding data flow without data provider taking notice of the change and approving it.

Current Problems

Are the stated Criteria hard enough, to verify legal or rule book compliance in terms of Usage Control ?

What extensions do we need to achieve this?

Wrap Up

- We talked about 6 areas where Usage Control in the IDS
- We proposed (and will hopefully soon discuss) the following target questions:
  - Actions, Participants need a proper legal / human readable definition, that is well defined. How can we ensure this ?
  - Are we allowed to interprete these Policy Language to legal Contracts ?
  - Do we always need a superviser sending Agreements ?
  - What do we need to make the exchanged Contracts binding to all involved parties ?
  - What do we need to make the Clearing House a source for evidence ?
  - What measures can we deploy to interpret them as legal Contracts (f.e deterministic Conversion to Human Language) To what extend is automation allowed ?
  - To what extend is the Usage Control Engine allowed to access the data and under which conditions ?
  - Do we need to specify in advance from the provider side how usage Control is implemented in the recipient connector ?
  - Variables need a proper legal / human readable definition, that is well defined. How can we ensure this ?
  - How do we reference Entities like areas of a City, to be still binding in the context of Usage Control Patterns?
  - The Certification Criteria are currently derived partially from Law Regulations (IT Security, etc.). Are there any parts of the rule book or laws on contracts, that should also be considered ?
  - Are the stated Criteria hard enough, to verify legal or rule book compliance in terms of Usage Control ?
  - What extensions do we need to achieve this ?

Further Readings (per Topic)

Topic 1: GitHub - International-Data-Spaces-Association/InformationModel, IDS Usage Policy Language (JIVE)

Topic 2: Usage Contract Negotiation (JIVE)

Topic 3: IDS Reference Architecture Model 4.1.3.5 ff

Topic 4: Policy Classes (JIVE)

Topic 5: IDSA - Whitepapers

Topic 6: IDSA - Whitepapers

Thank you for your Attention!

Any Questions ?

Fraunhofer