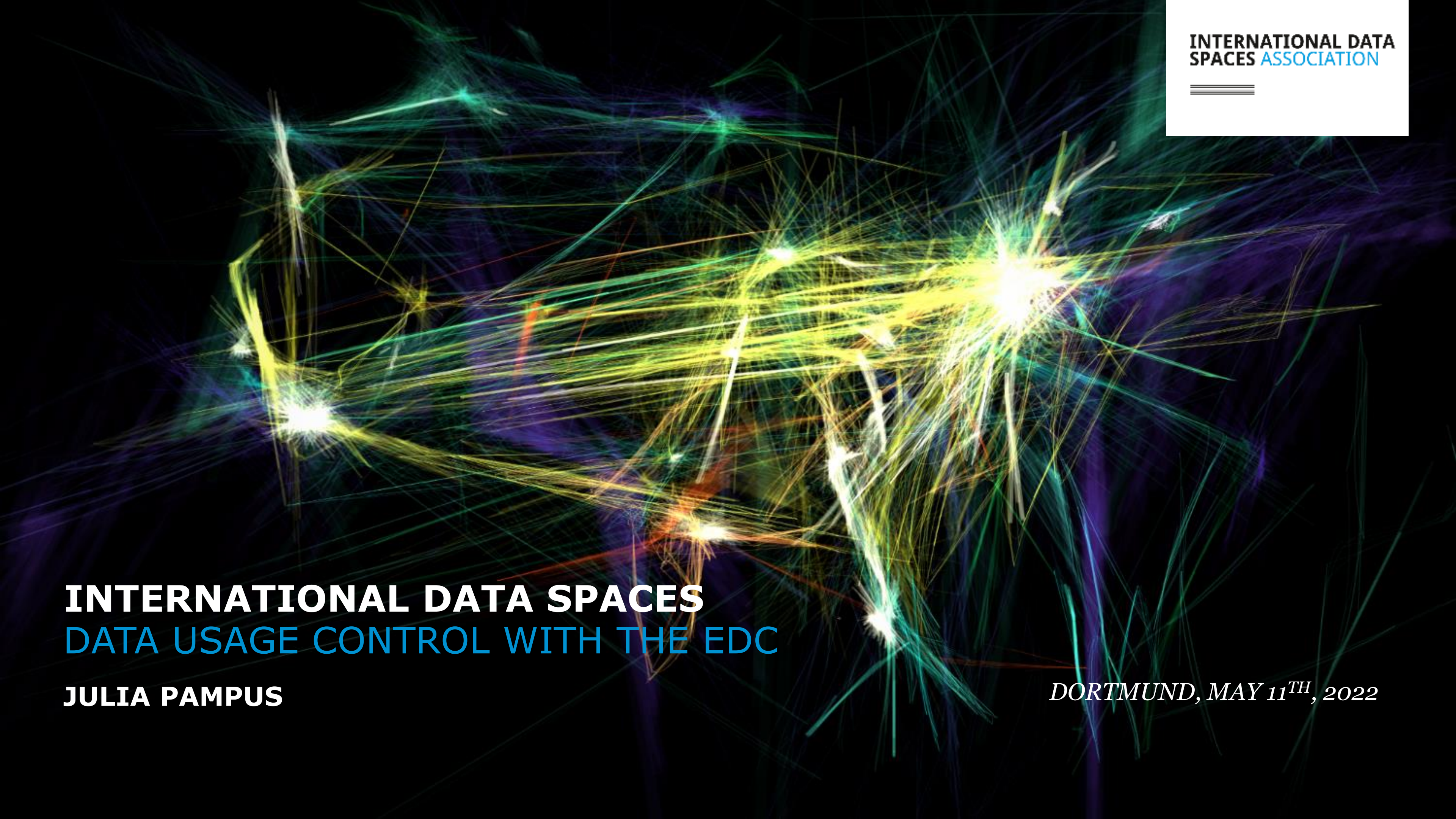
INTERNATIONAL DATA SPACES ASSOCIATION



INTERNATIONAL DATA SPACES
DATA USAGE CONTROL WITH THE EDC

JULIA PAMPUS

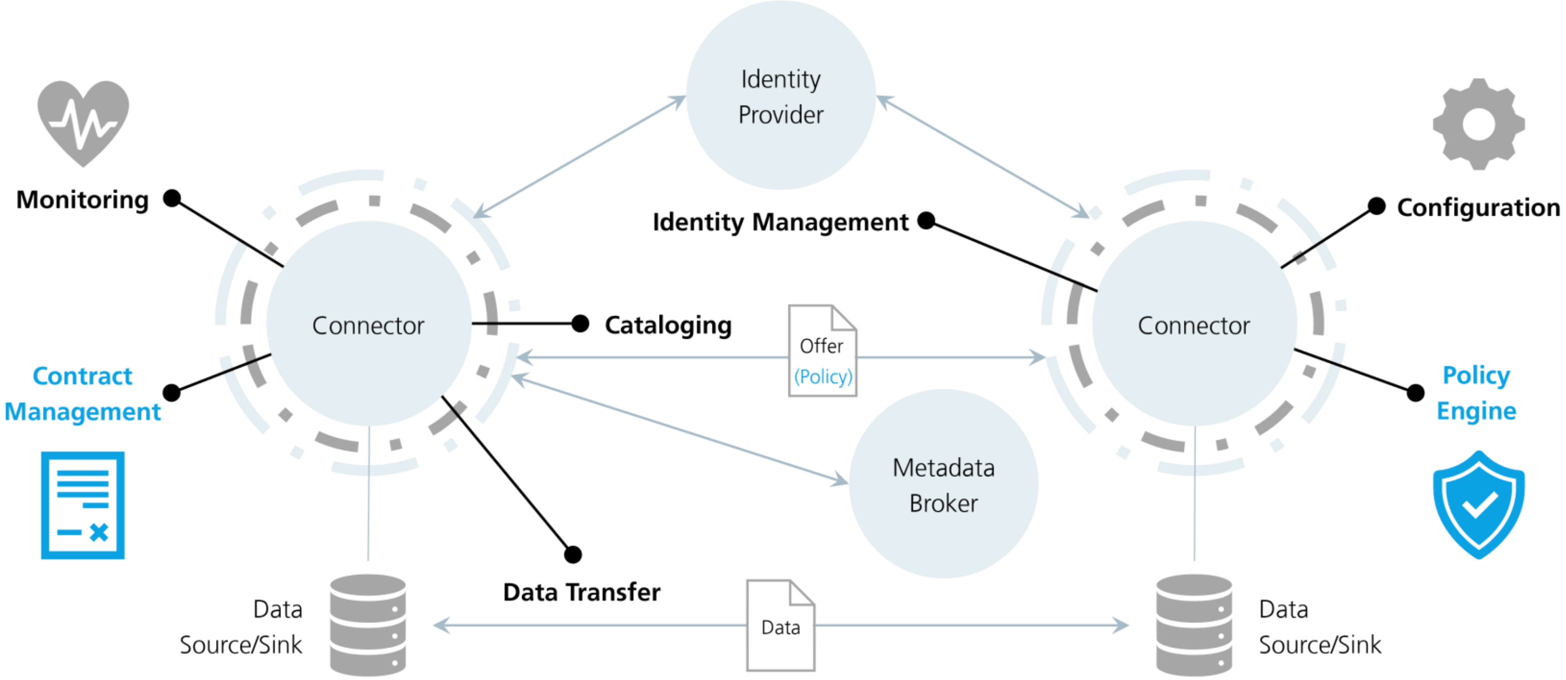
DORTMUND, MAY 11TH, 2022

AGENDA

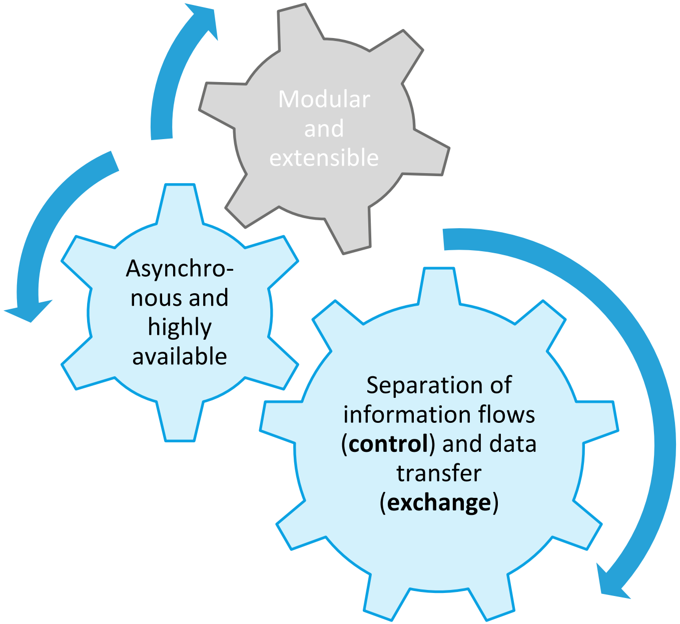
- Overview
- Contract Management
- Policy Enforcement
- Outlook

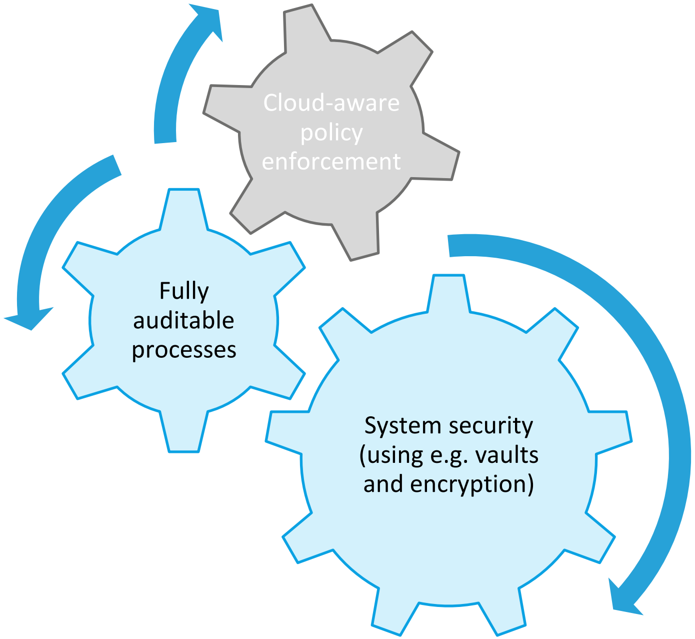
ECLIPSE DATASPACE CONNECTOR
OVERVIEW

TECHNICAL CAPABILITIES



DESIGN PRINCIPLES

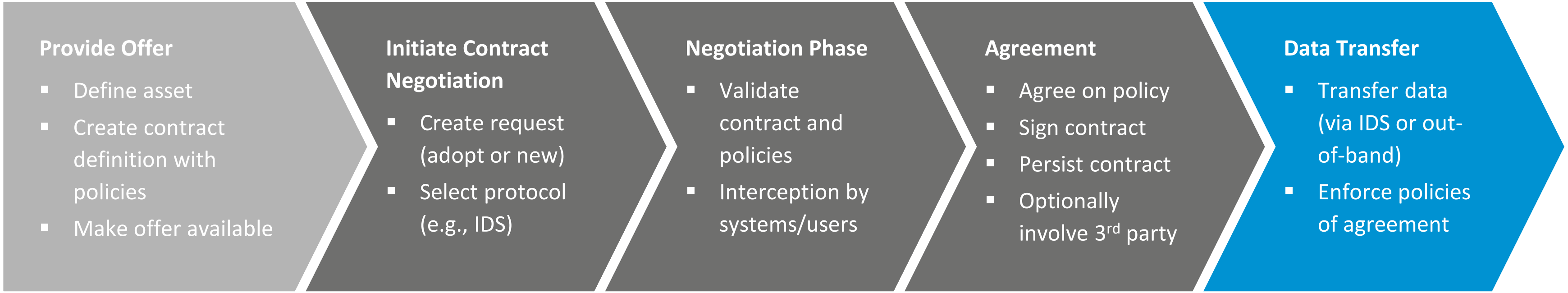

Modular and extensible
Asynchro-nous and highly available
Separation of information flows (**control**) and data transfer (**exchange**)


Cloud-aware policy enforcement
Fully auditable processes
System security (using e.g. vaults and encryption)

INTERNATIONAL DATA
SPACES ASSOCIATION

ECLIPSE DATASPACE CONNECTOR
CONTRACT MANAGEMENT

COMMUNICATION PROCESS



Provide Offer

- Define asset
- Create contract definition with policies
- Make offer available

Initiate Contract Negotiation

- Create request (adopt or new)
- Select protocol (e.g., IDS)

Negotiation Phase

- Validate contract and policies
- Interception by systems/users

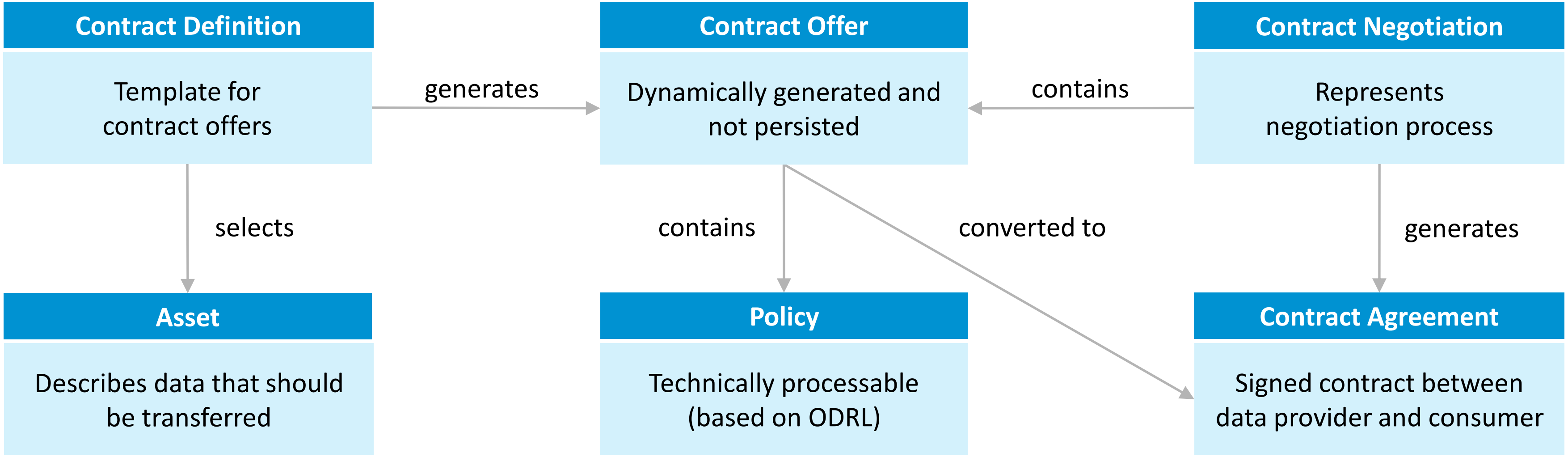
Agreement

- Agree on policy
- Sign contract
- Persist contract
- Optionally involve 3rd party

Data Transfer

- Transfer data (via IDS or out-of-band)
- Enforce policies of agreement

DOMAIN MODEL



Contract Definition

Template for contract offers

Contract Offer

Dynamically generated and not persisted

Contract Negotiation

Represents negotiation process

Asset

Describes data that should be transferred

Policy

Technically processable (based on ODRL)

Contract Agreement

Signed contract between data provider and consumer

https://github.com/eclipse-dataspaceconnector/DataSpaceConnector/blob/main/docs/domain-model.md (accessed: 20.04.2022)

CONTRACT DEFINITION

Unique Identifier

Access Policy

Non-public requirements for accessing a set of assets

- Not part of the data/contract offer
- Used for implementing access control on metadata level
- Represents the same structure as a contract policy
- E.g., this may require another connector to be in a business partner tier

Contract Policy

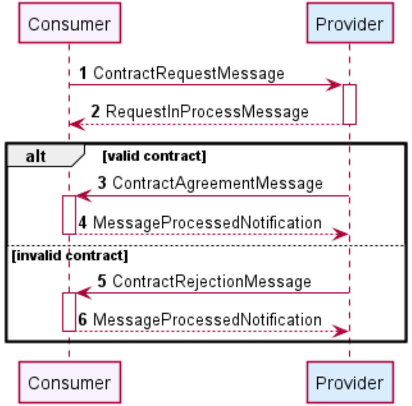
Data usage and access policies

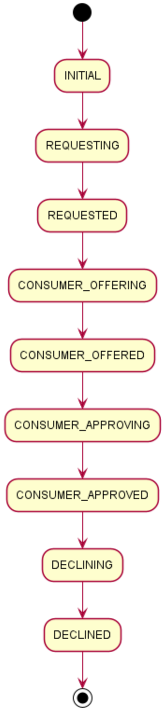
- Defines the requirements a data consumer must follow when using (e.g., processing) the data
- Advertised to other connectors as part of a contract
- The final contract is agreed upon during a negotiation process
- Follows the structure of ODRL: target, assigner, assignee, rules, constraints, etc.

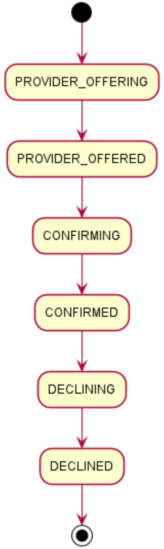
Asset Selector

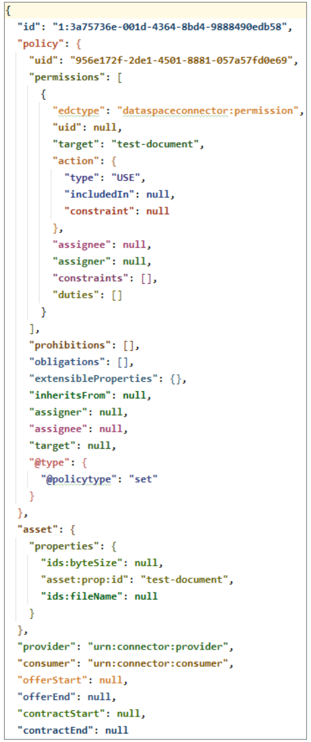
CONTRACT NEGOTIATION

- State machine architecture (asynchronous processing)
- Protocol: IDS multipart
- Following the sequences defined in RAM v4.0


Consumer
Provider
1 ContractRequestMessage
2 RequestInProcessMessage
alt
[valid contract]
3 ContractAgreementMessage
4 MessageProcessedNotification
[invalid contract]
5 ContractRejectionMessage
6 MessageProcessedNotification
Consumer
Provider





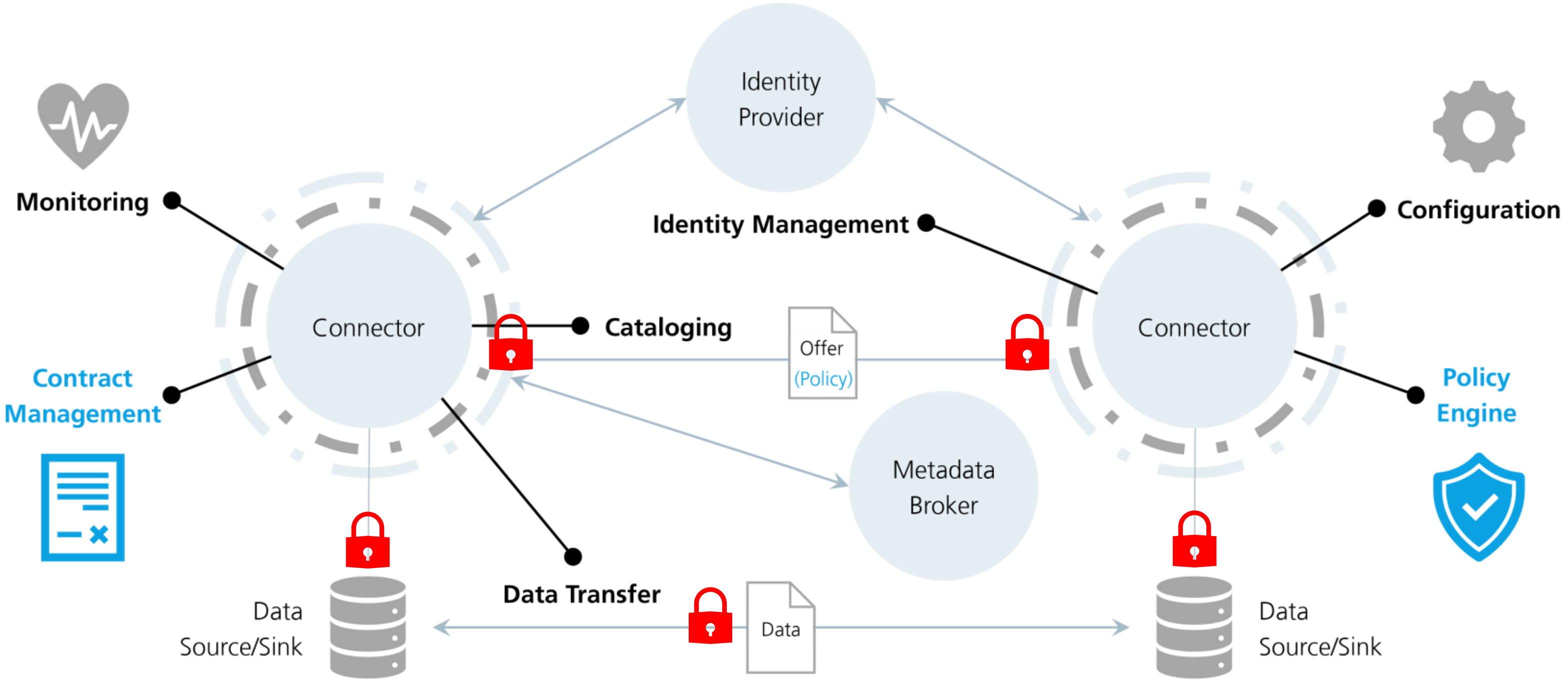


```
{
  "id": "1:3a75736e-001d-4364-8bd4-9888490edb58",
  "policy": {
    "uid": "956e172f-2de1-4501-8881-057a57fd0e69",
    "permissions": [
      {
        "edctype": "dataspaceconnector:permission",
        "uid": null,
        "target": "test-document",
        "action": {
          "type": "USE",
          "includedIn": null,
          "constraint": null
        },
        "assignee": null,
        "assigner": null,
        "constraints": [],
        "duties": []
      }
    ],
    "prohibitions": [],
    "obligations": [],
    "extensibleProperties": {},
    "inheritsFrom": null,
    "assigner": null,
    "assignee": null,
    "target": null,
    "@type": {
      "@policytype": "set"
    }
  },
  "asset": {
    "properties": {
      "ids:byteSize": null,
      "asset:prop:id": "test-document",
      "ids:fileName": null
    }
  },
  "provider": "urn:connector:provider",
  "consumer": "urn:connector:consumer",
  "offerStart": null,
  "offerEnd": null,
  "contractStart": null,
  "contractEnd": null
```

ECLIPSE DATASPACE CONNECTOR

POLICY ENFORCEMENT

INTERFACES


Identity Provider
Monitoring
Identity Management
Configuration
Connector
Cataloging
Offer
(Policy)
Connector
Contract Management
Metadata Broker
Policy Engine
Data Source/Sink
Data Transfer
Data
Data Source/Sink

DSC VS. EDC

Dataspace Connector

- Fixed implementation (and interpretation) of selected IDS usage control classes
- Restriction: data cannot leave the connector

Eclipse Dataspace Connector

- Modular implementation
- Policy engine with fixed interfaces
- Supported policies depend on the deployment/setup/extensions
- Easily replaceable and expandable

https://international-data-spaces-association.github.io/DataspaceConnector/Documentation/v6/UsageControl (accessed: 09.05.2022)

POLICY SCOPES
DEFINITION

- Assumption 1: Policy rules may only be applicable in certain runtime contexts.
    - Example: "Data must be anonymized."
    - May be applicable to policy evaluation when a resource is provisioned
    - May not be applicable during data transfer
- Assumption 2: Policy rules may have different implementation semantics in certain runtime contexts.
    - Example: "Data must remain in EU-based compute environments."
    - When this rule is evaluated during authorization, a verifiable credential may be checked.
    - When data transfer occurs, this rule may require data to be stored in a particular cloud region.

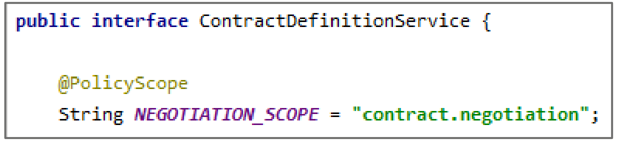
Policy Scopes = runtime visibility and semantic boundaries for policy rules

- Hierarchical and expressed using dot notation (e.g., "provision.verify")
- If a rule is visible in a given scope, it will be included in policy evaluations for that scope; otherwise, it will be omitted.

Rule Binding = makes a rule type visible in a policy scope

POLICY SCOPES
APPLICATION

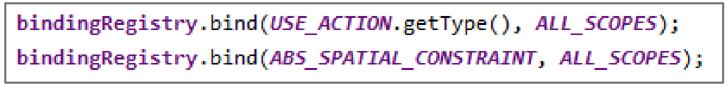
1. Define policy scope in service extension



```
public interface ContractDefinitionService {

    @PolicyScope
    String NEGOTIATION_SCOPE = "contract.negotiation";
```

2. Add RuleBindingRegistry to ServiceExtensionContext
3. Bind policy with scope



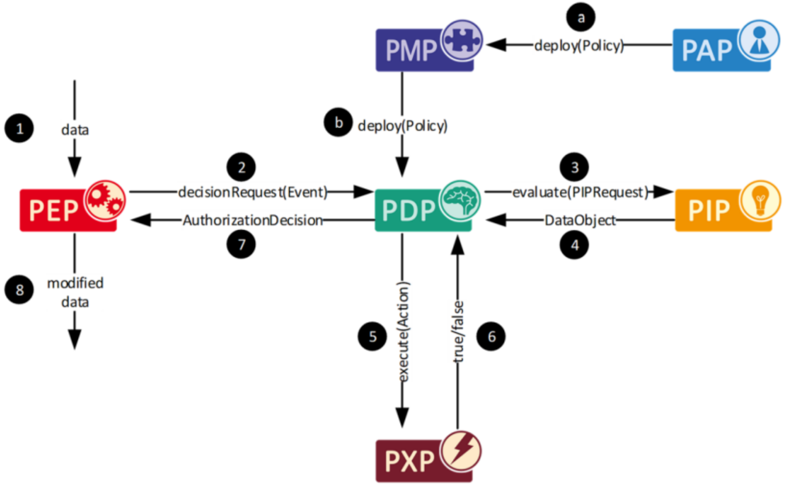
```
bindingRegistry.bind(USE_ACTION.getType(), ALL_SCOPES);
bindingRegistry.bind(ABS_SPATIAL_CONSTRAINT, ALL_SCOPES);
```

4. During execution: ScopeFilter filters a policy for a scope. This involves recursively removing rules and constraints not bound to the scope and returning a modified copy of the unfiltered policy. (applicable to policy, permission, duty, prohibition, condition)

ECLIPSE DATASPACE CONNECTOR
OUTLOOK

NEXT STEPS

- Design policy engine, perhaps oriented towards
  - eXtensible Access Control Markup Language (XACML)
  - and its interpretation and extension by IDS
- Implement policy enforcement for selected attributes



Discussion points

- What kinds of policy need to be supported?
- How to connect standardized interfaces and use external tools (e.g., OPA)?
- How to provide standardized interfaces for extensions?
- How to ensure policy enforcement for data that leaves the connector?

EVENTS

2nd Gaia-X Hackathon (12/2021)

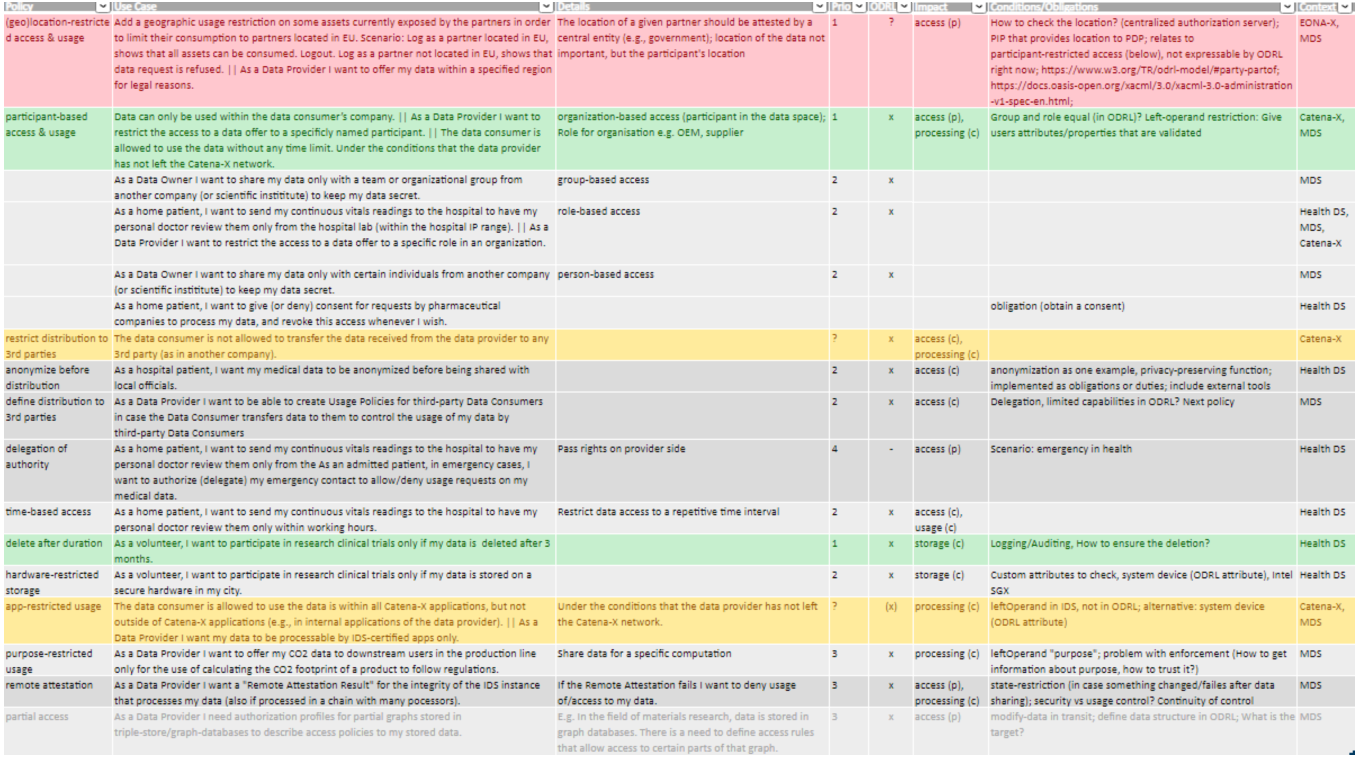
- Bringing Usage Control (UCON+) into the EDC
- Provide extension (EDC-UCS) that extends the default policy behavior of the EDC
- Add custom PEPs and obligations for two samples (file transfer, streaming): anonymize e-mail address with a regex
- More information here

3rd Gaia-X Hackathon (03/2022)

- Understand the mapping between the ODRL and XACML models
- Implement a PoC that outputs ALFA policies based on ODRL policies
- Demonstrate this with the EDC-UCON integration results from the previous hackathon
- More information here

Contributions from German Research Center, Huawei Technologies (Munich) and Security Forge (Pisa)

WORKSHOP



Policy	Use Case	Details	Prio	ODRL	Impact	Conditions/Obligations	Context
(geo)location-restricted access & usage	Add a geographic usage restriction on some assets currently exposed by the partners in order to limit their consumption to partners located in EU. Scenario: Log as a partner located in EU, shows that all assets can be consumed. Logout. Log as a partner not located in EU, shows that data request is refused. || As a Data Provider I want to offer my data within a specified region for legal reasons.	The location of a given partner should be attested by a central entity (e.g., government); location of the data not important, but the participant's location	1	?	access (p)	How to check the location? (centralized authorization server); PIP that provides location to PDP; relates to participant-restricted access (below), not expressable by ODRL right now; https://www.w3.org/TR/odrl-model/#party-partof; https://docs.oasis-open.org/xacml/3.0/xacml-3.0-administration-v1-spec-en.html;	EONA-X, MDS
participant-based access & usage	Data can only be used within the data consumer's company. || As a Data Provider I want to restrict the access to a data offer to a specificly named participant. || The data consumer is allowed to use the data without any time limit. Under the conditions that the data provider has not left the Catena-X network.	organization-based access (participant in the data space); Role for organisation e.g. OEM, supplier	1	x	access (p), processing (c)	Group and role equal (in ODRL)? Left-operand restriction: Give users attributes/properties that are validated	Catena-X, MDS
	As a Data Owner I want to share my data only with a team or organizational group from another company (or scientific instititute) to keep my data secret.	group-based access	2	x			MDS
	As a home patient, I want to send my continuous vitals readings to the hospital to have my personal doctor review them only from the hospital lab (within the hospital IP range). || As a Data Provider I want to restrict the access to a data offer to a specific role in an organization.	role-based access	2	x			Health DS, MDS, Catena-X
	As a Data Owner I want to share my data only with certain individuals from another company (or scientific instititute) to keep my data secret.	person-based access	2	x			MDS
	As a home patient, I want to give (or deny) consent for requests by pharmaceutical companies to process my data, and revoke this access whenever I wish.					obligation (obtain a consent)	Health DS
restrict distribution to 3rd parties	The data consumer is not allowed to transfer the data received from the data provider to any 3rd party (as in another company).		?	x	access (c), processing (c)		Catena-X
anonymize before distribution	As a hospital patient, I want my medical data to be anonymized before being shared with local officials.		2	x	access (c)	anonymization as one example, privacy-preserving function; implemented as obligations or duties; include external tools	Health DS
define distribution to 3rd parties	As a Data Provider I want to be able to create Usage Policies for third-party Data Consumers in case the Data Consumer transfers data to them to control the usage of my data by third-party Data Consumers		2	x	access (c)	Delegation, limited capabilities in ODRL? Next policy	MDS
delegation of authority	As a home patient, I want to send my continuous vitals readings to the hospital to have my personal doctor review them only from the As an admitted patient, in emergency cases, I want to authorize (delegate) my emergency contact to allow/deny usage requests on my medical data.	Pass rights on provider side	4	-	access (p)	Scenario: emergency in health	Health DS
time-based access	As a home patient, I want to send my continuous vitals readings to the hospital to have my personal doctor review them only within working hours.	Restrict data access to a repetitive time interval	2	x	access (c), usage (c)		Health DS
delete after duration	As a volunteer, I want to participate in research clinical trials only if my data is deleted after 3 months.		1	x	storage (c)	Logging/Auditing, How to ensure the deletion?	Health DS
hardware-restricted storage	As a volunteer, I want to participate in research clinical trials only if my data is stored on a secure hardware in my city.		2	x	storage (c)	Custom attributes to check, system device (ODRL attribute), Intel SGX	Health DS
app-restricted usage	The data consumer is allowed to use the data is within all Catena-X applications, but not outside of Catena-X applications (e.g., in internal applications of the data provider). || As a Data Provider I want my data to be processable by IDS-certified apps only.	Under the conditions that the data provider has not left the Catena-X network.	?	(x)	processing (c)	leftOperand in IDS, not in ODRL; alternative: system device (ODRL attribute)	Catena-X, MDS
purpose-restricted usage	As a Data Provider I want to offer my CO2 data to downstream users in the production line only for the use of calculating the CO2 footprint of a product to follow regulations.	Share data for a specific computation	3	x	processing (c)	leftOperand "purpose"; problem with enforcement (How to get information about purpose, how to trust it?)	MDS
remote attestation	As a Data Provider I want a "Remote Attestation Result" for the integrity of the IDS instance that processes my data (also if processed in a chain with many pocessors).	If the Remote Attestation fails I want to deny usage of/access to my data.	3	x	access (p), processing (c)	state-restriction (in case something changed/failes after data sharing); security vs usage control? Continuity of control	MDS
partial access	As a Data Provider I need authorization profiles for partial graphs stored in triple-store/graph-databases to describe access policies to my stored data.	E.g. In the field of materials research, data is stored in graph databases. There is a need to define access rules that allow access to certain parts of that graph.	3	x	access (p)	modify-data in transit; define data structure in ODRL; What is the target?	MDS

https://github.com/eclipse-dataspaceconnector/Collateral/tree/main/Work Content/Usage Control (accessed: 06.05.2022)

JOIN THE DISCUSSION ON GITHUB

Issues and discussions

- https://github.com/eclipse-dataspaceconnector/DataSpaceConnector/discussions/878
- https://github.com/eclipse-dataspaceconnector/DataSpaceConnector/discussions/1229
- https://github.com/eclipse-dataspaceconnector/DataSpaceConnector/discussions/792
- https://github.com/eclipse-dataspaceconnector/DataSpaceConnector/discussions/447
- https://github.com/eclipse-dataspaceconnector/DataSpaceConnector/discussions/742
- https://github.com/eclipse-dataspaceconnector/DataSpaceConnector/issues/857

Existing documentation

- https://github.com/eclipse-dataspaceconnector/DataSpaceConnector/blob/main/docs/Policies.md
- https://github.com/eclipse-dataspaceconnector/DataSpaceConnector/blob/main/docs/domain-model.md
- https://github.com/eclipse-dataspaceconnector/DataSpaceConnector/blob/main/docs/architecture/contracts.md
- https://github.com/eclipse-dataspaceconnector/DataSpaceConnector/tree/main/docs/developer/decision-records/2022-03-15-policy-scopes

INTERNATIONAL DATA
SPACES ASSOCIATION

Fraunhofer

JULIA PAMPUS

RESEARCH ASSOCIATE
DEPARTMENT DATA BUSINESS

JULIA.PAMPUS@ISST.FRAUNHOFER.DE
+49 231 97677 429

FRAUNHOFER ISST
EMIL-FIGGE-STR. 91
44227 DORTMUND | GERMANY

JOIN US !

@ids_association
# internationaldataspaces