Workshop on Usage Control Policies in Dataspaces

Andreas Krimbacher
nexyo, Vienna, Austria

Sebastian Neumaier
St. Pölten University of Applied Sciences

Sebastian Neumaier received funding through the project 891103 “DiDaMe” from the Austrian Research Promotion Agency FFG.
Agenda

- **Intro**: What are Dataspaces
- **Dataspaces Connectors**: A review of existing Implementations
- **Use Case**: “Data-driven Tourism for Sustainability”
- **Demo**: nexyo data Hub and Ecosystem
- **Usage Control Policies**: A Review of Policy Classes
European Dataspaces – Gaia-X

- European project working on the federation of data infrastructure and service providers
- Defines set of *technical and organisational standards* for storage and exchange
- „Dataspaces“ as relationship between trusted partners
- Existing reference architecture model for participation by the *International Data Spaces Association (IDSA)*
Data Spaces

- Data spaces allow organizations to securely share data with other participants
- Data are not stored centrally, only transferred (through semantic interoperability) as necessary
- Data spaces are built on
  - **Identity**: Each participant remains in control of their identity
  - **Trust**: Each participant decides who to trust
  - **Sovereignty**: Each participant decides under what policies their data is shared
  - **Interoperability**: Each participant remains in control of their deployment

https://gaia-x.eu/what-is-gaia-x/deliverables/data-spaces/
Architecture

[Diagram showing a network architecture with nodes labeled as Connector, Identity Provider, Identity Management, Metadata Broker, and a flow of Data Transfer, Cataloging, and Monitoring.]
Data Model

- IDS Information Model published by IDSA
  - RDFS/OWL ontology:
    - International Data Spaces Information Model

Release 2022-09-16

This version: [https://w3id.org/idsa/core-420](https://w3id.org/idsa/core-420)

Latest version: [https://w3id.org/idsa/core](https://w3id.org/idsa/core)

Previous version: [https://w3id.org/idsa/core-410](https://w3id.org/idsa/core-410)

Revision: 4.2.0
A Survey of Dataspace Connector Implementations
IDS Dataspace Connector
sovity, initially Fraunhofer ISST

- IDS Usage Control Language based on ODRL
- Defines 21 policy classes for Usage Control enforcement – 9 are implemented

TRUsted Engineering Connector
Engineering Ingegneria Informatica S.p.A

- Platoon/MyData app (using the IDS language)
- Modification of the IDS Connector

Eclipse Dataspace Connector (EDC)
Consortium: Microsoft, BMW, Fraunhofer, SAP, etc.

- ODRL-based policy definition, however, currently in Java code

Trusted Connector
Fraunhofer AISEC

- LUCON policy language
- Consist of flow rules and a service descriptions
## Development Process / Maturity

<table>
<thead>
<tr>
<th>Connector</th>
<th>Created</th>
<th>Stars</th>
<th>Commits</th>
<th>Language</th>
<th>License</th>
<th>Usage control</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSC</td>
<td>2020-10-07</td>
<td>16</td>
<td>2600</td>
<td>Java</td>
<td>Apache License 2.0</td>
<td>IDS Usage Control Language (based on ODRL)</td>
</tr>
<tr>
<td>EDC</td>
<td>2021-07-26</td>
<td>134</td>
<td>1311</td>
<td>Java</td>
<td>Apache License 2.0</td>
<td>Policies defined in connector code.</td>
</tr>
<tr>
<td>TRUE</td>
<td>2020-10-30</td>
<td>13</td>
<td>77</td>
<td>Java</td>
<td>AGPLv3</td>
<td>Platoon/MyData app (using the IDS language)</td>
</tr>
<tr>
<td>Trusted</td>
<td>2017-09-05</td>
<td>3</td>
<td>2083</td>
<td>Kotlin</td>
<td>Apache License 2.0</td>
<td>LUCON policy language</td>
</tr>
</tbody>
</table>
## Development Process / Maturity

<table>
<thead>
<tr>
<th>Connector</th>
<th>Created</th>
<th>Stars</th>
<th>Commits</th>
<th>Language</th>
<th>License</th>
<th>Usage control</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSC</td>
<td>2020-10-07</td>
<td>16</td>
<td>2600</td>
<td>Java</td>
<td>Apache License 2.0</td>
<td>IDS Usage Control Language (based on ODRL)</td>
</tr>
<tr>
<td>EDC</td>
<td>2021-07-26</td>
<td>134</td>
<td>1311</td>
<td>Java</td>
<td>Apache License 2.0</td>
<td>Policies defined in connector code.</td>
</tr>
<tr>
<td>TRUE</td>
<td>2020-10-30</td>
<td>13</td>
<td>77</td>
<td>Java</td>
<td>AGPLv3</td>
<td>Platoon/MyData app (using the IDS language)</td>
</tr>
<tr>
<td>Trusted</td>
<td>2017-09-05</td>
<td>3</td>
<td>2083</td>
<td>Kotlin</td>
<td>Apache License 2.0</td>
<td>LUCON policy language</td>
</tr>
</tbody>
</table>
Eclipse Data Space Connector

- Eclipse Dataspase Connector (EDC) provides a framework for dataspace connectors
- Contains modules for data discovery, data exchange, policy enforcement, monitoring and auditing
- Implements decentralized identifiers (DIDs) and uses the DID:Web method
DIDs for Identity Management

- Decentralized identifier (DID)
  - W3C Proposed Recommendation (w3.org/TR/did-core/)
  - E.g., `did:example:123456789abcdefghi`

- Resolves to a DID document
  - simple JSON file that contains information

```json
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ],
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    "// used to authenticate as did:...fgi"
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase": "zH3C2AVvLMv6gwr9N3UuA3VfJ2pfkcJYwOw2nZ6z3W7XmpqPMV"
  }]
}
```
DIDs in a Data Space Architecture
DIDs in a Data Space Architecture (cont’d)
Usage Control Policies in Dataspaces
Methodology

- Survey existing projects/literature on concrete examples and implementations of usage control policies

Criteria:
- Filter policies for Dataspace use cases
- Potentially enforcable
- Defined between the interacting parties:
  - Provider, consumer, third-party / observer
<table>
<thead>
<tr>
<th>General Policies</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow access (e.g. for specific user or connector)</td>
<td>[1,2]</td>
</tr>
<tr>
<td>Location / Regional restriction</td>
<td>[1,2,3]</td>
</tr>
<tr>
<td>Time restriction (e.g. start, end, duration)</td>
<td>[1]</td>
</tr>
<tr>
<td>Access count</td>
<td>[1,2]</td>
</tr>
<tr>
<td>Rate limit (e.g., downloads within hour)</td>
<td>[4]</td>
</tr>
<tr>
<td>Number of concurrent active connections</td>
<td>[4]</td>
</tr>
<tr>
<td>Fixed amount of data (e.g. in streaming)</td>
<td>[2]</td>
</tr>
<tr>
<td>Processing power</td>
<td>[2,9]</td>
</tr>
<tr>
<td>Usage of bandwidth</td>
<td>[2,9]</td>
</tr>
<tr>
<td>Billing / Credit points (perpetual vs. rental)</td>
<td>[1,2]</td>
</tr>
</tbody>
</table>
### Data Usage

| Deletion                                             | [1,5]   |
| Purpose / Application                               | [1]     |

### Attribute based / Obligation fulfilled

<p>| Proofable attributes, e.g. membership credentials, position in company, security clearance/certification | [1,6]   |
| Non-proofable, e.g. legal jurisdiction               | [4,6]   |</p>
<table>
<thead>
<tr>
<th>Privacy Policies</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption: at rest / at transfer</td>
<td>[1,3]</td>
</tr>
<tr>
<td>Aggregation</td>
<td>[7]</td>
</tr>
<tr>
<td>Anonymization</td>
<td>[7,10]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traceability</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging</td>
<td>[1,5]</td>
</tr>
<tr>
<td>Notification</td>
<td>[1]</td>
</tr>
<tr>
<td>Delegation/distribution of permissions to third-party</td>
<td>[1,2]</td>
</tr>
</tbody>
</table>
References


Sebastian Neumaier
St. Pölten University of Applied Sciences
Austria

sebastian.neumaier@fhstp.ac.at
https://sebneumaier.wordpress.com/
https://twitter.com/sebneum