Trust Envelopes as Instruments of Transparency and Accountability

Beatriz Esteves

Solid Community day (June 20th, 2025):
Solid Foundations, Smart Spaces: Transforming Health Through Data

beatriz.esteves@ugent.be | w3id.org/people/besteves

Trust Envelopes as Instruments of Transparency and Accountability

Why does our data need trust?

What is needed in a trust envelope?

How are we building trust envelopes?

Where we are and where we want to go

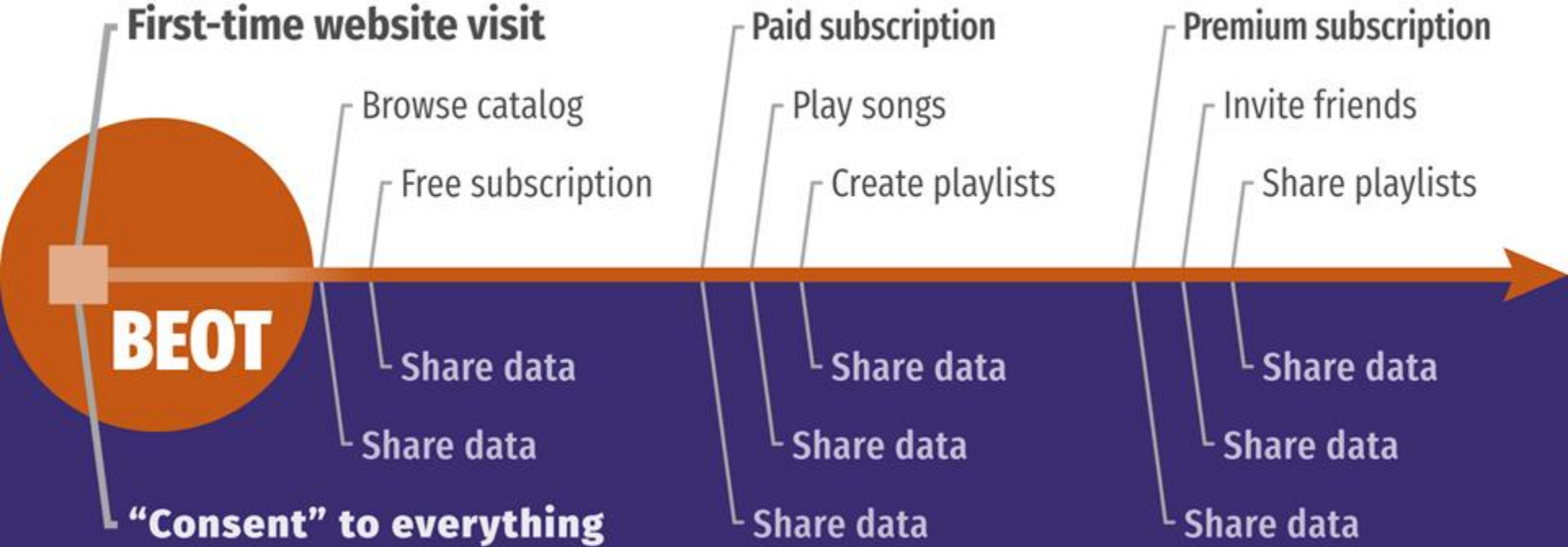# Trust Envelopes as Instruments of Transparency and Accountability

Why does our data need trust?

What is needed in a trust envelope?

How are we building trust envelopes?

Where we are and where we want to go

Trustless consent model

INTERACTION PLANE

First-time website visit

Paid subscription

Premium subscription

Browse catalog

Play songs

Invite friends

Free subscription

Create playlists

Share playlists

BEOT

Share data

Share data

Share data

Share data

Share data

Share data

"Consent" to everything

Share data

Share data

DATA PLANE

Regulations

Regulations

Regulations

Regulations

Case law

Guidelines

Compliance

Automation

Insights

Personalisation

Evolving trust relationships

INTERACTION PLANE

First-time website visit

Browse catalog

Free subscription

Paid subscription

Play songs

Create playlists

Premium subscription

Invite friends

Share playlists

Trust evolves over time

Data & **Trust**

Data & **Trust**

Data & **Trust**

Data & **Trust**

Data & **Trust**

Data & **Trust**

Data & **Trust**

Data & **Trust**

Data & **Trust**

TRUST PLANE

Trust Envelopes as Instruments of Transparency and Accountability

Why does our data need trust?

What is needed in a trust envelope?

How are we building trust envelopes?

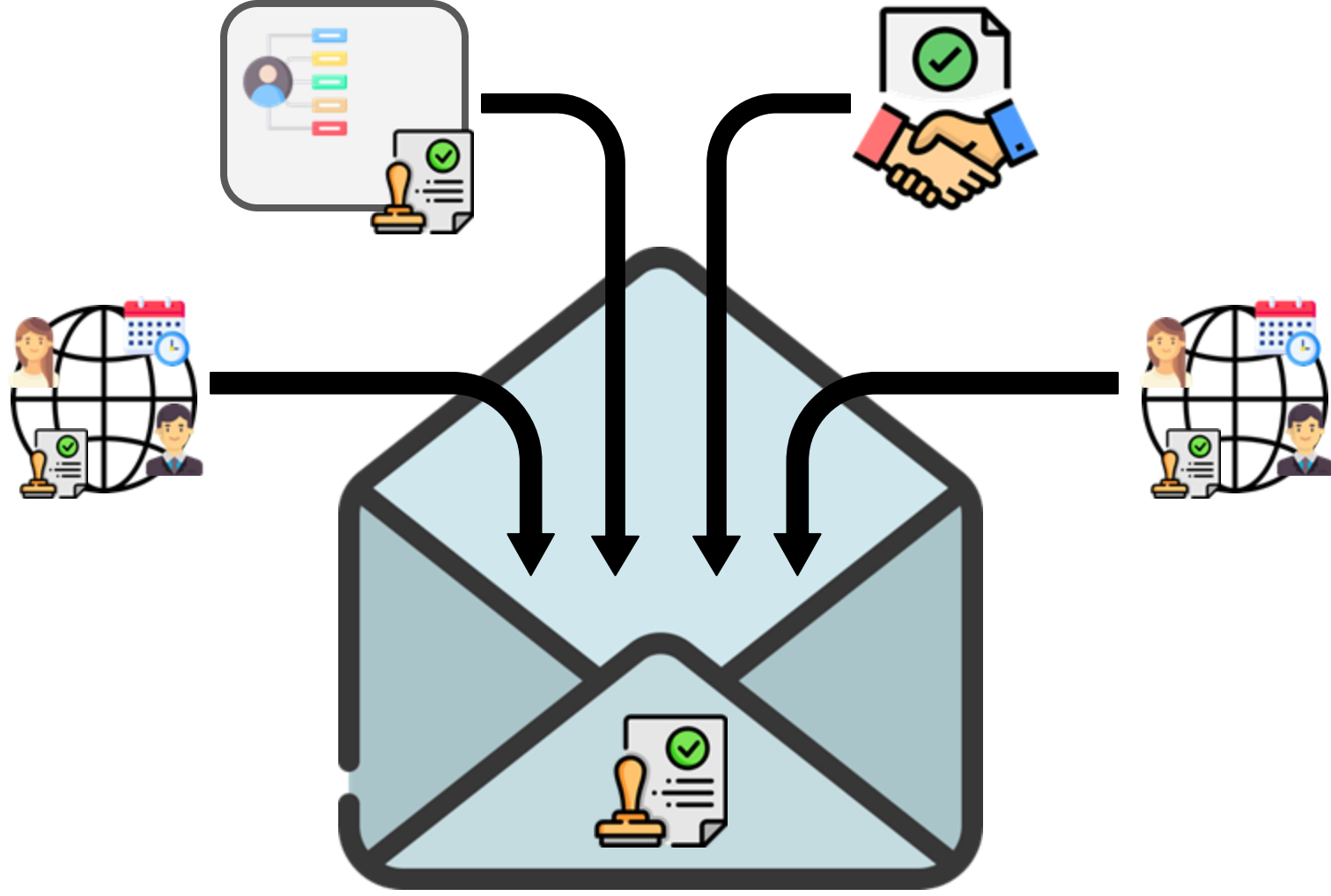Where we are and where we want to go

Verifiable data

Instantiated policy

Data Provenance

Policy Provenance

Trust Envelopes as Instruments of Transparency and Accountability

Why does our data need trust?

What is needed in a trust envelope?

How are we building trust envelopes?

Where we are and where we want to go

Regulations

Case law

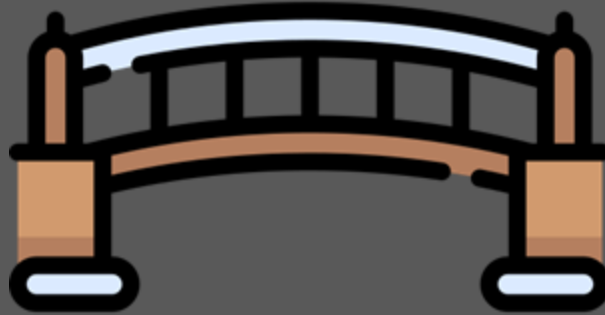Guidelines

Compliance

Automation

Insights

Personalisation

Verifiable data

https://www.w3.org/TR/vc-data-model-2.0/

W3C Recommendation

Verifiable Credentials Data Model v2.0

W3C Recommendation 15 May 2025

▼ More details about this document

This version:
    https://www.w3.org/TR/2025/REC-vc-data-model-2.0-20250515/
Latest published version:
    https://www.w3.org/TR/vc-data-model-2.0/
Latest editor's draft:
    https://w3c.github.io/vc-data-model/
History:
    https://www.w3.org/standards/history/vc-data-model-2.0/
    Commit history
Implementation report:
    https://w3c.github.io/vc-data-model-2.0-test-suite/
Editors:
    Manu Sporny (Digital Bazaar) (v1.0, v1.1, v2.0)
    Ted Thibodeau Jr (OpenLink Software) (v2.0)
    Ivan Herman ⊙ (W3C) (v2.0)
    Gabe Cohen (Block) (v2.0)
    Michael B. Jones (Invited Expert) (v2.0)
Former editors:
    Grant Noble (ConsenSys) (v1.0)
    Dave Longley (Digital Bazaar) (v1.0)
    Daniel C. Burnett (ConsenSys) (v1.0)
    Brent Zundel (Evernym) (v1.0)
    Kyle Den Hartog (MATTR) (v1.1)

Verifiable Credential
Credential Metadata
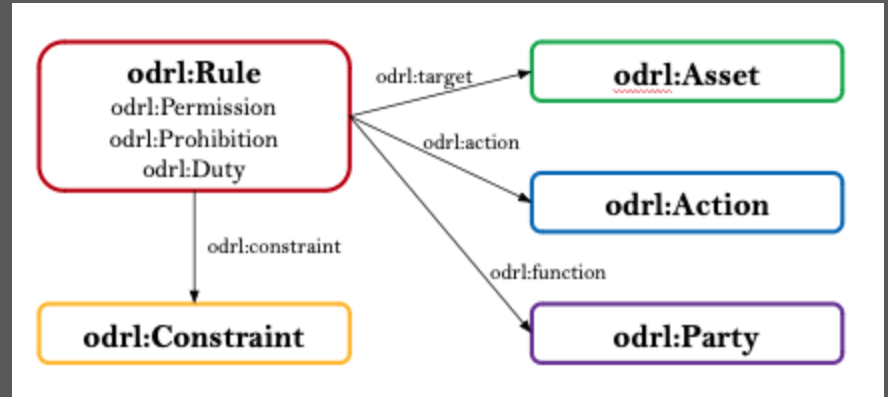Claim(s)
Proof(s)

Verifiable Presentation
Presentation Metadata
Verifiable Credential(s)
Proof(s)

Instantiated policy

odrl:Rule
odrl:Permission
odrl:Prohibition
odrl:Duty

odrl:target → odrl:Asset

odrl:action → odrl:Action

odrl:function → odrl:Party

odrl:constraint → odrl:Constraint

Who [can|cannot|must] act what in which resource how

Instantiated policy

Who [can|cannot|must] act what in which resource how
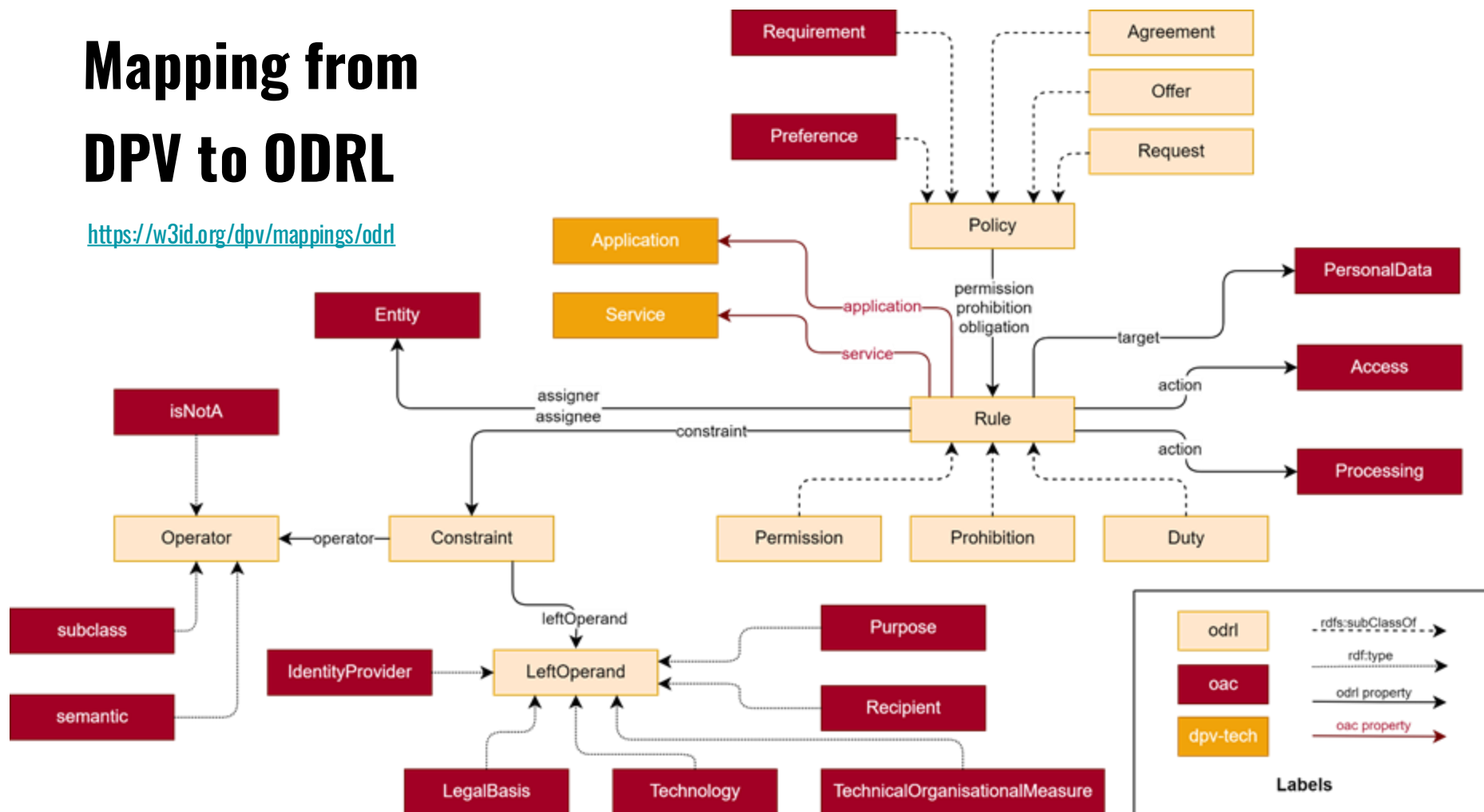
- W3C Recommendation

- Maintained by the W3C ODRL Community Group

- Composed by several specifications
  - ODRL Information Model – W3C Recommendation
  - ODRL Core Vocabulary – W3C Recommendation
  - ODRL Implementation Best Practices
  - ODRL Profile Best Practices
  - ODRL Formal Semantics [Under development]

- Easily extendable through the use of ODRL profiles

Data Privacy Vocabulary (DPV)

- Developed by the **W3C** Data Privacy Vocabularies and Controls Community Group (**DPVCG**)
- Defines a **jurisdiction-agnostic** ontology for expressing metadata about the processing of personal data
- Provides **hierarchical taxonomies**, from abstract to more specific concepts, to instantiate specific concepts in practical use-cases
- Has **law-specific extensions**

  https://w3id.org/dpv

  https://w3id.org/dpv/primer

# Mapping from DPV to ODRL

https://w3id.org/dpv/mappings/odrl

```
ex:physician-request a odrl:Request ;
    odrl:uid ex:physician-request ;
    dcterms:description """Physician requests patient to read health data for primary care
        without time restriction and also for non-direct encounters (e.g. remote monitoring).""" ;
    odrl:permission [
        odrl:action odrl:read ;
        odrl:target ex:health-data ;
        odrl:assignee ex:physician ;
        odrl:constraint [
            odrl:leftOperand dpv-odrl:Purpose ;
            odrl:operator odrl:isAnyOf ;
            odrl:rightOperand sector-health:PrimaryCareManagement, sector-health:PatientMonitoring ],[
            odrl:leftOperand dpv-odrl:LegalBasis ;
            odrl:operator odrl:eq ;
            odrl:rightOperand eu-gdpr:A9-2-a ] ] .
```

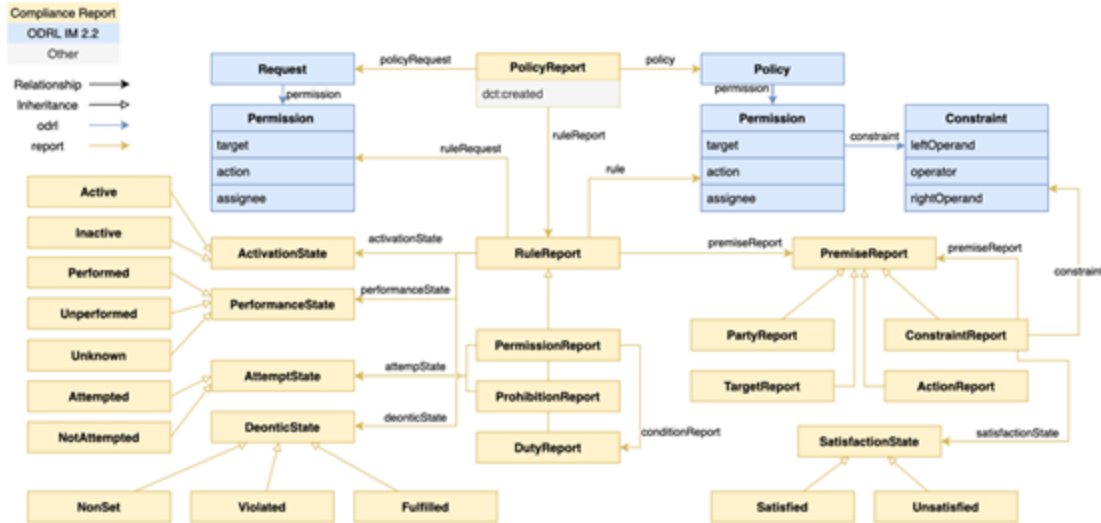# Interoperable Interpretation and Evaluation of ODRL Policies
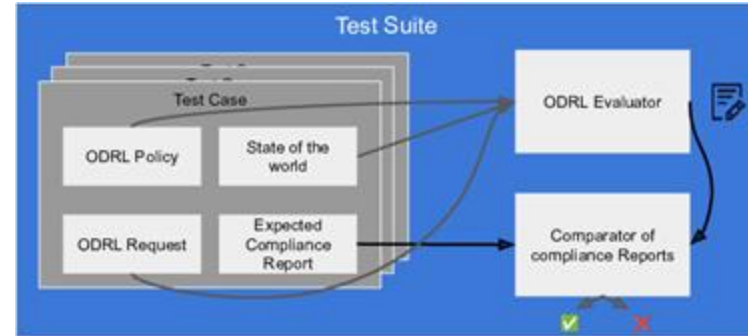

https://w3id.org/force/compliance-report
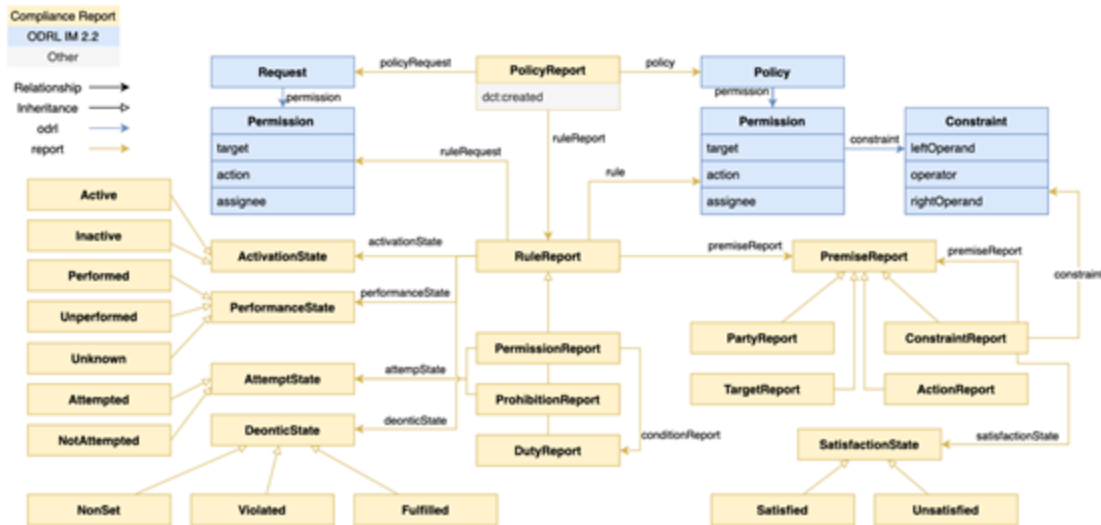
ESWC 2025
🌟 Best Resource Nominee

Interoperable Interpretation and Evaluation of ODRL Policies

https://w3id.org/force/compliance-report

https://w3id.org/force/test-suite

Agreement Instantiation

- Validate the proper modelling of the odrl:Policy, odrl:Request and SoTW information.

- Convert compact policies into their atomic equivalents.

- Evaluate policies to generate compliance reports.

- Reference the ODRL request that triggered the agreement instantiation and the policies from the data subject/holder.

- Instantiate the concrete assigner and assignee of the agreement.

- Include relevant rules with concrete actions, targets and constraints.

https://w3id.org/force/evaluator

https://w3id.org/force/ESWC2025-demo

Trust Envelopes as Instruments of Transparency and Accountability

Why does our data need trust?

What is needed in a trust envelope?

How are we building trust envelopes?

Where we are and where we want to go

Conclusions & future work

Enforcement of interoperable policies
Alignment with legal requirements from GDPR
Validated by legal experts in DPV and SolidLab & PACSOI projects

Finalise Trust Envelopes specification

Extend evaluator to cover all ODRL left operands & operators

Extend evaluator to cover all DPV constraints

Use different legal grounds to share data

Integrate provenance standards (DCAT, PROV, …)

Trust Envelopes as Instruments of Transparency and Accountability

Beatriz Esteves

Solid Community day (June 20th, 2025):
Solid Foundations, Smart Spaces: Transforming Health Through Data

beatriz.esteves@ugent.be | w3id.org/people/besteves