Representing and enforcing policies with ODRL in decentralised systems

Wout Slabbinck
PhD Researcher at KNoWS
W3C ODRL CG Contributor
wout.slabbinck@ugent.be | https://woutslabbinck.com

Representing and enforcing policies with ODRL and DPV in decentralised systems

A Solid background

Representing policies with ODRL

Deterministic enforcement of policies

ODRL Enforcement in practice

Representing and enforcing policies with ODRL and DPV in decentralised systems

A Solid background

Representing policies with ODRL

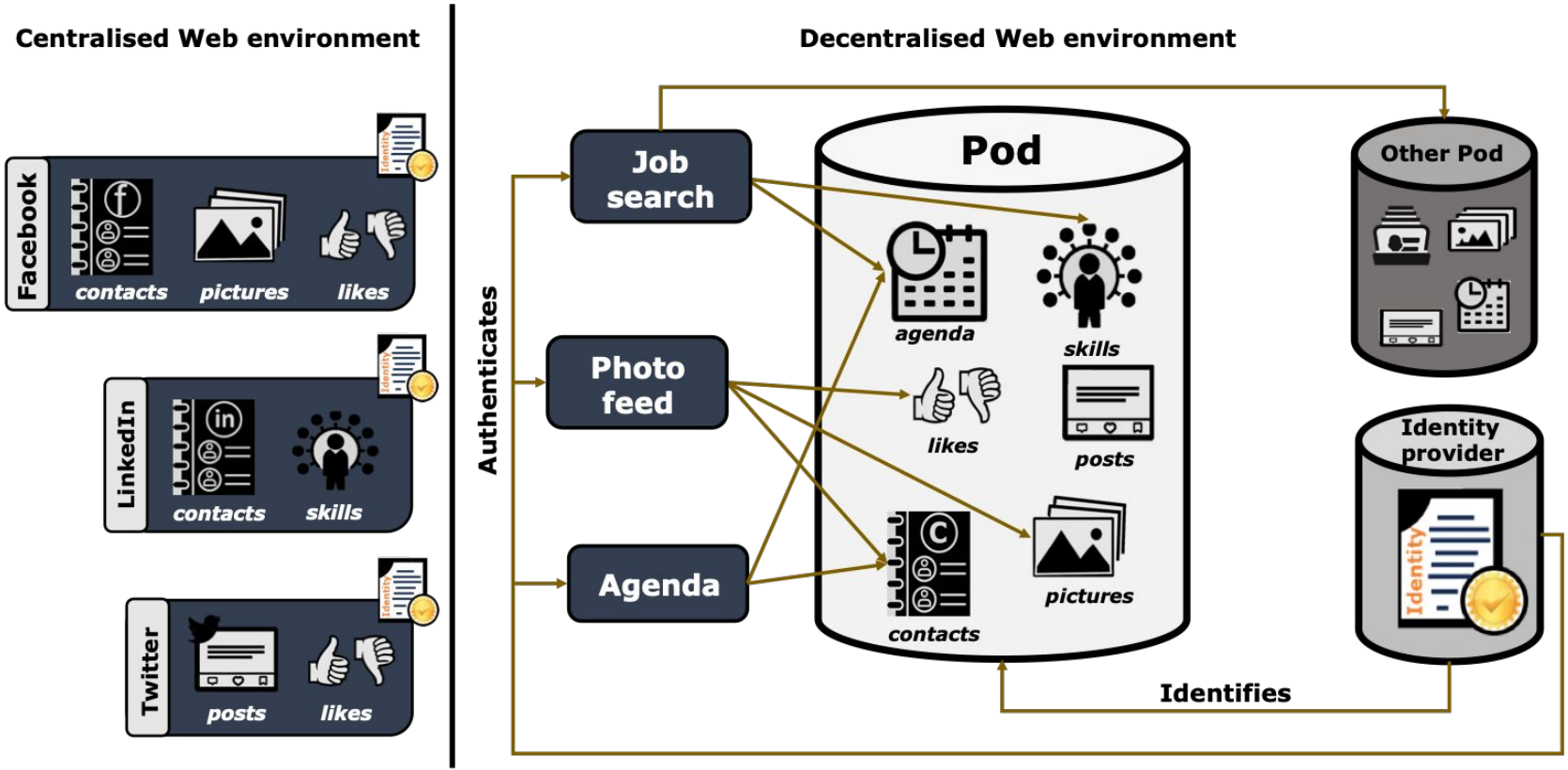
Deterministic enforcement of policies

ODRL Enforcement in practice

Walled Gardens

THE BATTLE OF THE INTERNET: OPEN VS CLOSED – FURTHER EXPLORATION, Christopher Langley

Centralisation vs Decentralisation



Personal Information Management Systems

"PIMS provide features for individuals to be able to access their personal data, as well as to rectify or erase them, as provided for by the GDPR, either because the data are in repositories under their direct control or because all shared data are linked to a source, which is again in the control of the individual."

EDPS TechDispatch #3/2020 – PIMS [1]

[1] https://www.edps.europa.eu/sites/default/files/publication/21-01-06_techdispatch-pims_en_0.pdf

Solid

Separating storage from apps

Build on existing specifications

https://solidproject.org/

Identity	*(webID)*
Authentication	*(Solid-OIDC)*
Authorization	*(WAC or ACP)*
Storage	*(LDP)*

https://podpro.dev/

Solid's Access Control

WAC – Web Access Control

```
@prefix acl: <http://www.w3.org/ns/auth/acl#>.

<#authz>
    a acl:Authorization;
    acl:agent <https://solidweb.me/besteves4/profile/card#me>;
    acl:accessTo <https://providerX.org/userY/contacts>;
    acl:mode acl:Read .
```

https://solidproject.org/TR/wac

ACP – Access Control Policy

```
@prefix acl: <http://www.w3.org/ns/auth/acl#>.
@prefix acp: <http://www.w3.org/ns/solid/acp#>.

<#acp> a acp:AccessGrant ;
  acp:grant acl:Read ;
  acp:context [
    acp:agent <https://solidweb.me/besteves4/profile/card#me> ;
    acp:target <https://providerX.org/userY/contacts> ;
    acp:client <https://appZ.org>
  ] .
```

https://solid.github.io/authorization-panel/acp-specification/

Representing and enforcing policies with ODRL and DPV in decentralised systems

A Solid background

Representing policies with ODRL

Deterministic enforcement of policies

ODRL Enforcement in practice

Representing and enforcing policies with ODRL and DPV in decentralised systems

A Solid background

Representing policies with ODRL

Deterministic enforcement of policies

ODRL Enforcement in practice

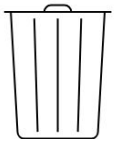
Access Control Rule

WHO can perform what **ACTION** on which **RESOURCE**

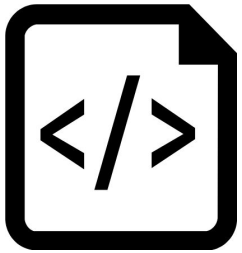
Create

Read

Update



Delete



ACCESS CONTROL RULE

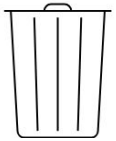
Usage Control Rule

WHO can perform what **ACTION** on which **RESOURCE** under which **CONDITIONS**

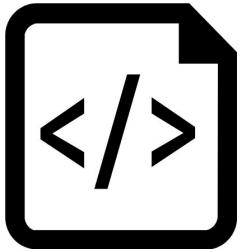
Create

Read

Update



Delete



Time
Location
Purpose
Payment

Usage Control Policies

Definition: a set of Usage Control Rules
Usage Control Rule

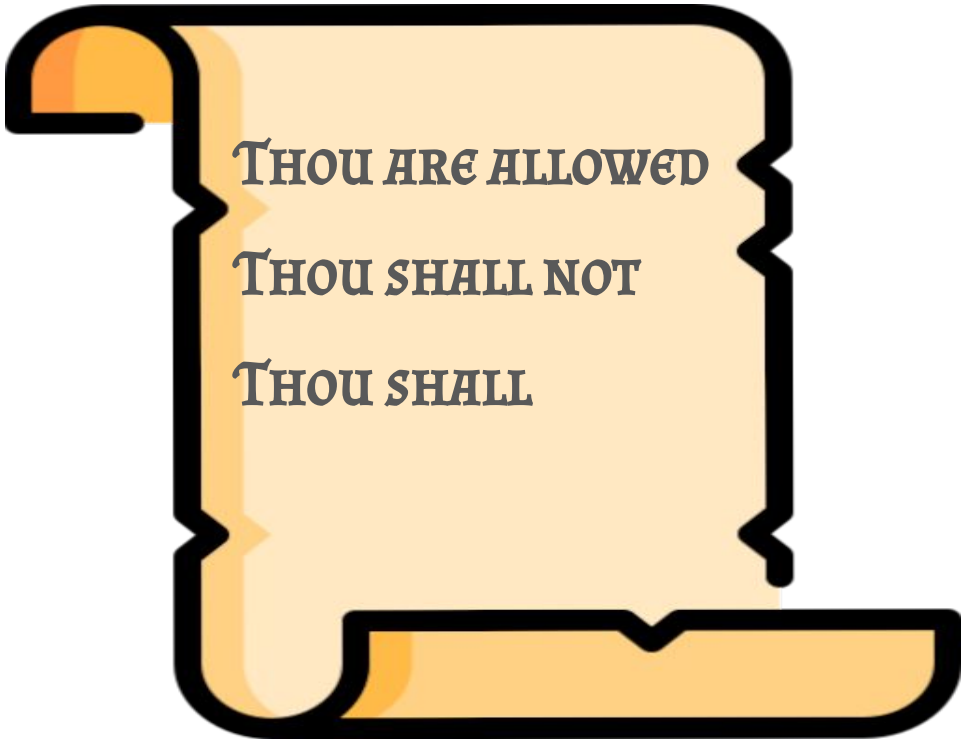
- Access Control + conditions

Usage Control Policies

Definition: a set of Usage Control Rules

Usage Control Rule

- Access Control + conditions
- **Deontic concepts**
  - Permission rules
  - Prohibition rules
  - Obligation rules



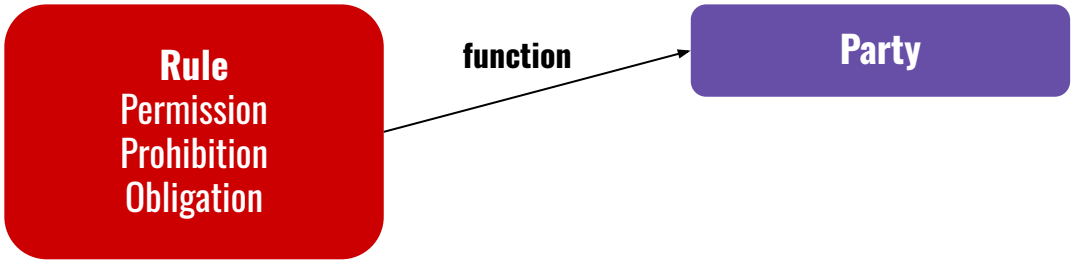
Open Digital Rights Language (ODRL)

- Standard for the expression of policies
  - ODRL Information Model – W3C Recommendation
  - ODRL Core Vocabulary – W3C Recommendation
- Maintained by the W3C ODRL Community Group
- Composed by several other specifications
  - ODRL Implementation Best Practices
  - ODRL Profile Best Practices
  - ODRL Formal Semantics [Under development]
  - ODRL Community Vocabulary [Under development]
- Easily extendable through the use of ODRL profiles

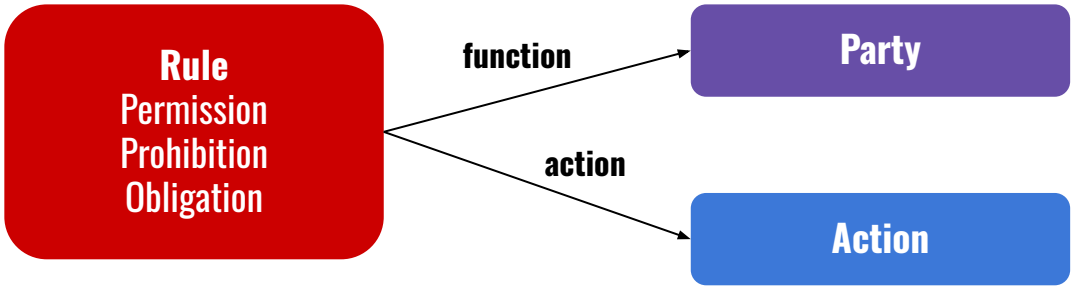
Who [can|cannot|must] act what in which resource how

Rule
Permission
Prohibition
Obligation

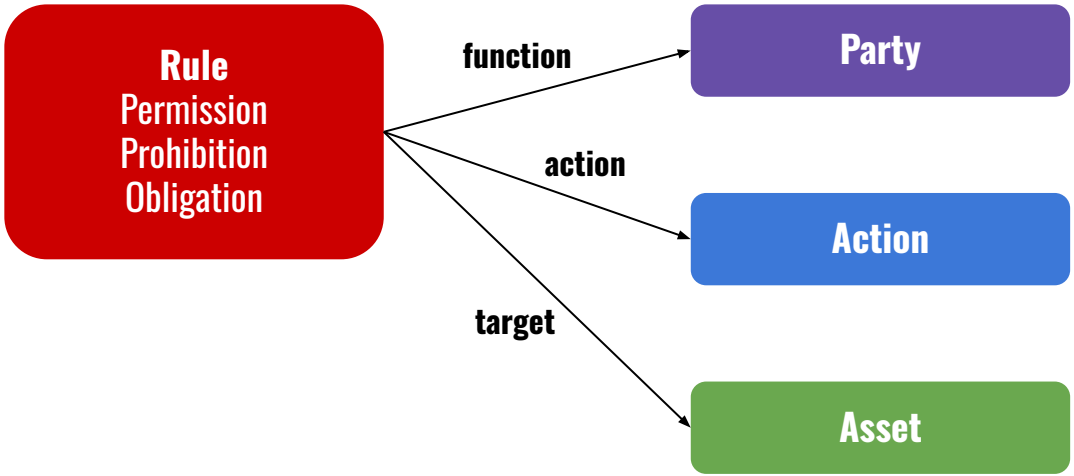
Who [can|cannot|must] act what in which resource how



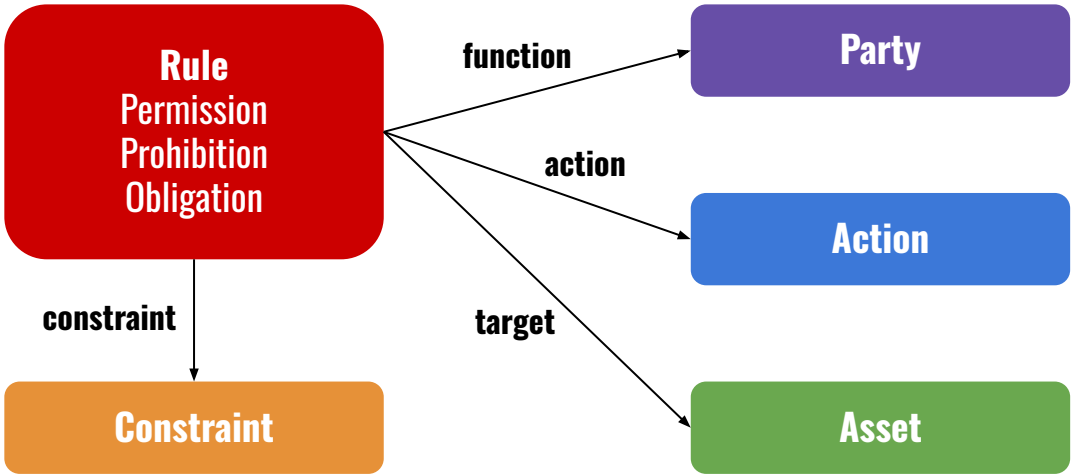
Who [can|cannot|must] act what in which resource how



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



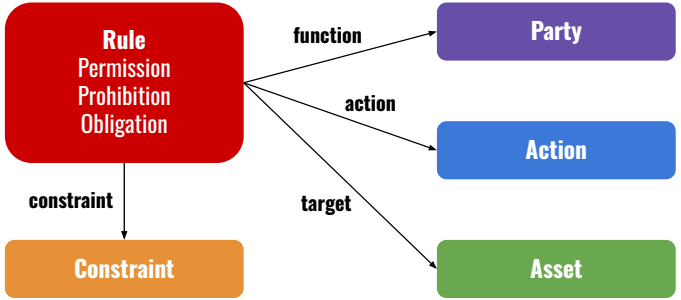
Who [can|cannot|must] act what in which resource how



Open Digital Rights Language (ODRL)

```
@prefix dcterms:       <http://purl.org/dc/terms/> .
@prefix dpv:           <https://w3id.org/dpv#> .
@prefix dpv-odrl:      <https://w3id.org/dpv/mappings/odrl#> .
@prefix ex:            <https://example.org/> .
@prefix odrl:          <http://www.w3.org/ns/odrl/2/> .

ex:read-multiple-purposes a odrl:Set ;
    odrl:uid ex:read-multiple-purposes ;
    odrl:profile dpv-odrl: ;
    dcterms:description "User A allows Company B to read to its contact details."@en ;
    odrl:permission [
        odrl:action odrl:read ;
        odrl:target <https://example.org/userA/contacts> ;
        odrl:assigner ex:userA ;
        odrl:assignee faqir:companyB ;
        odrl:constraint [
            odrl:leftOperand dpv-odrl:Purpose ;
            odrl:operator odrl:isAnyOf ;
            odrl:rightOperand dpv:ServiceProvision, dpv:NonCommercialResearch ] ] .
```



Representing and enforcing policies with ODRL and DPV in decentralised systems

A Solid background

Representing policies with ODRL

Deterministic enforcement of policies

ODRL Enforcement in practice

Representing and enforcing policies with ODRL and DPV in decentralised systems

A Solid background

Representing policies with ODRL

Deterministic enforcement of policies

ODRL Enforcement in practice

How to interoperably enforce ODRL policies?

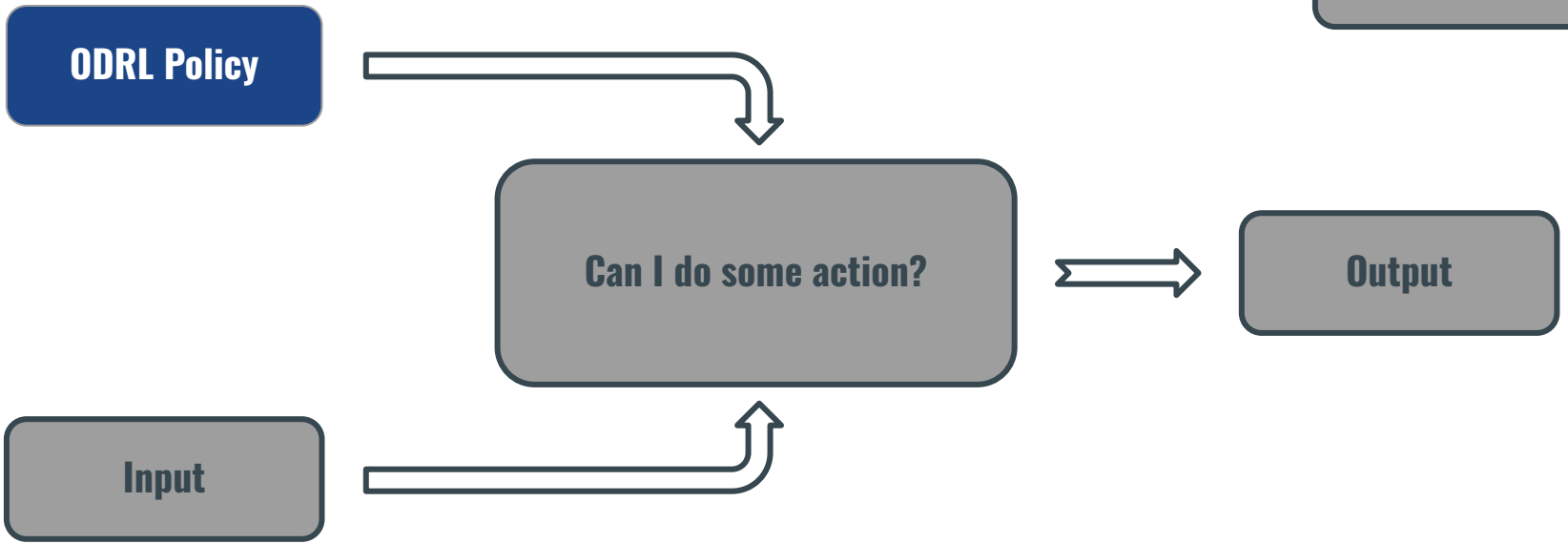
Standardised

ODRL Policy

How to interoperably enforce ODRL policies?

Standardised

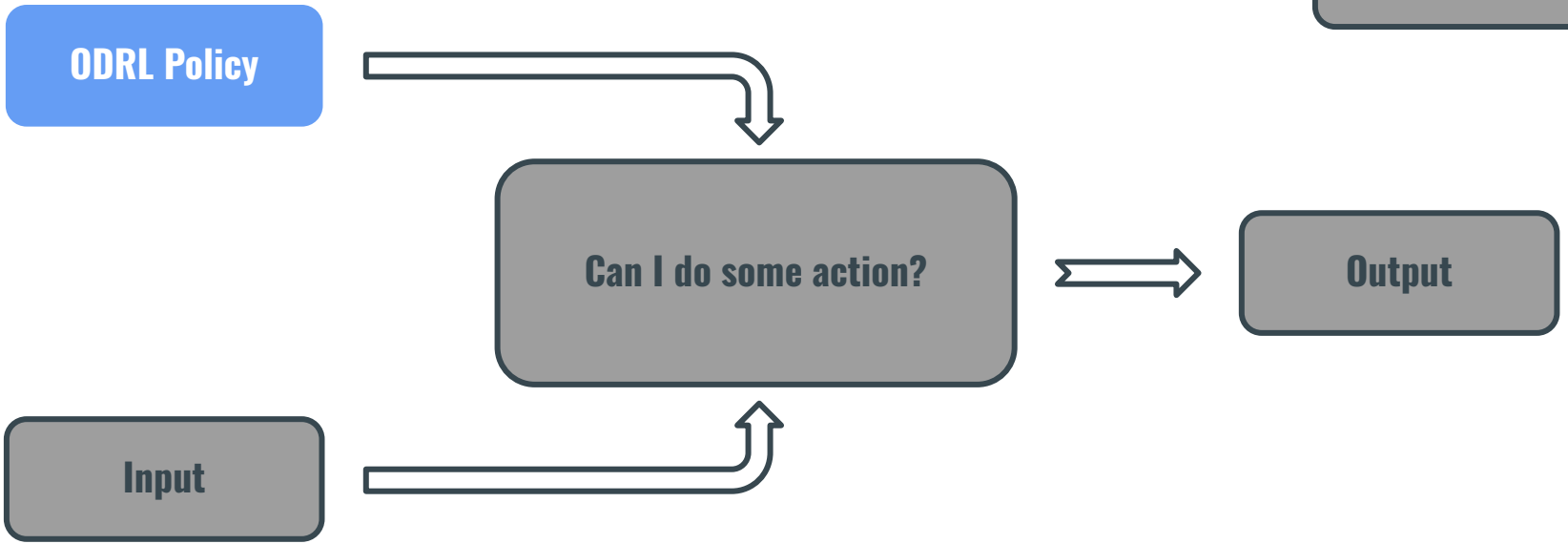
Not standardised



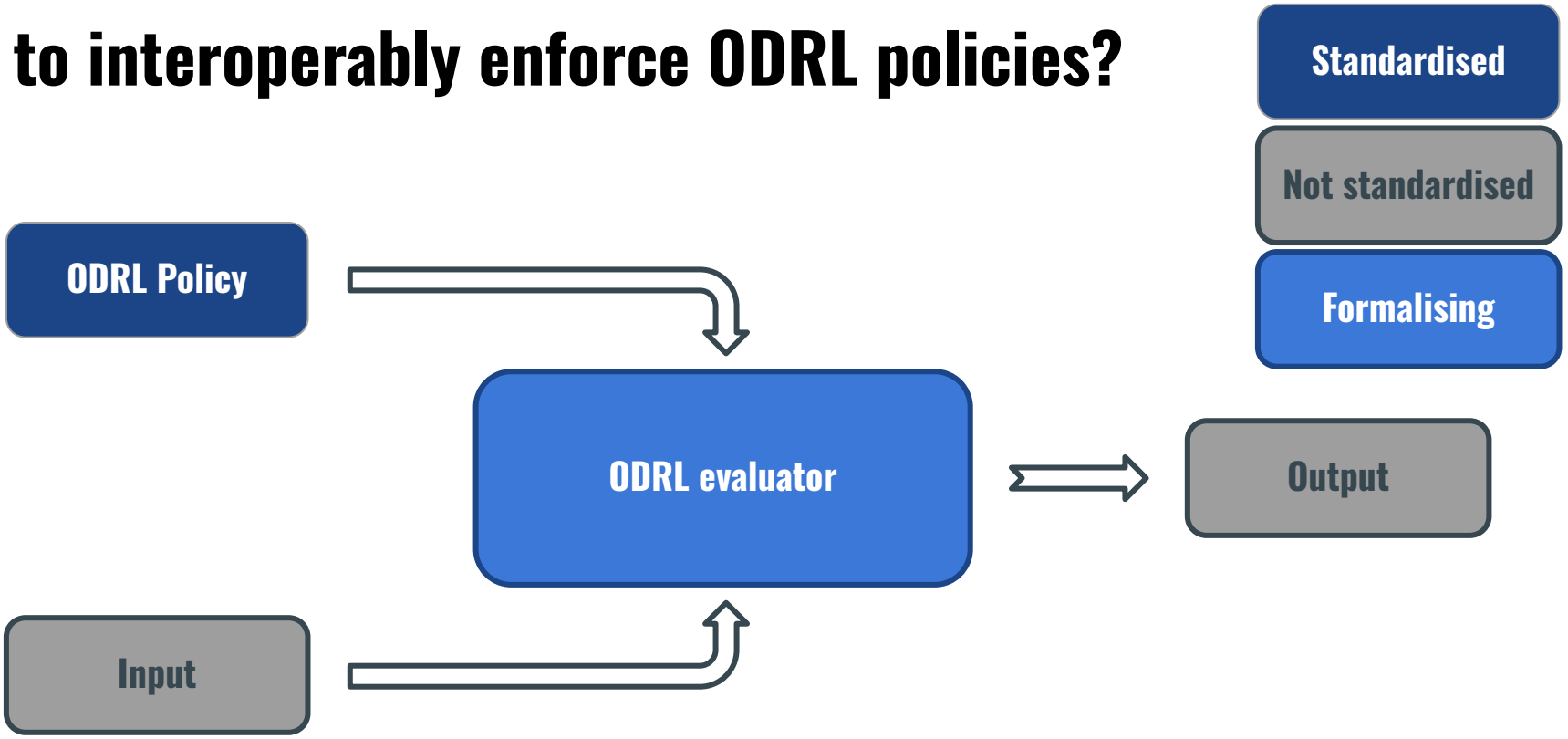
How to interoperably enforce ODRL policies?

Standardised

Not standardised

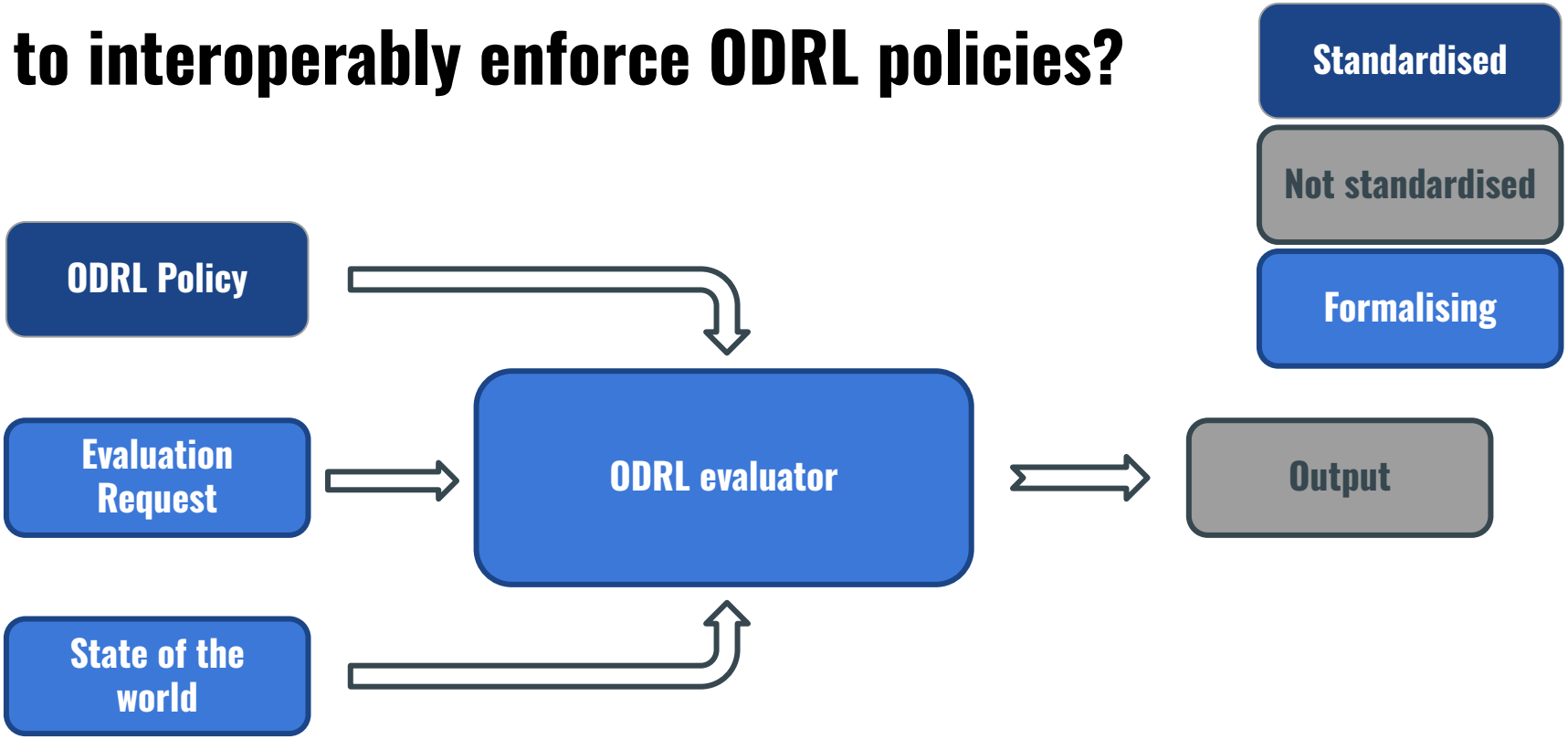


How to interoperably enforce ODRL policies?



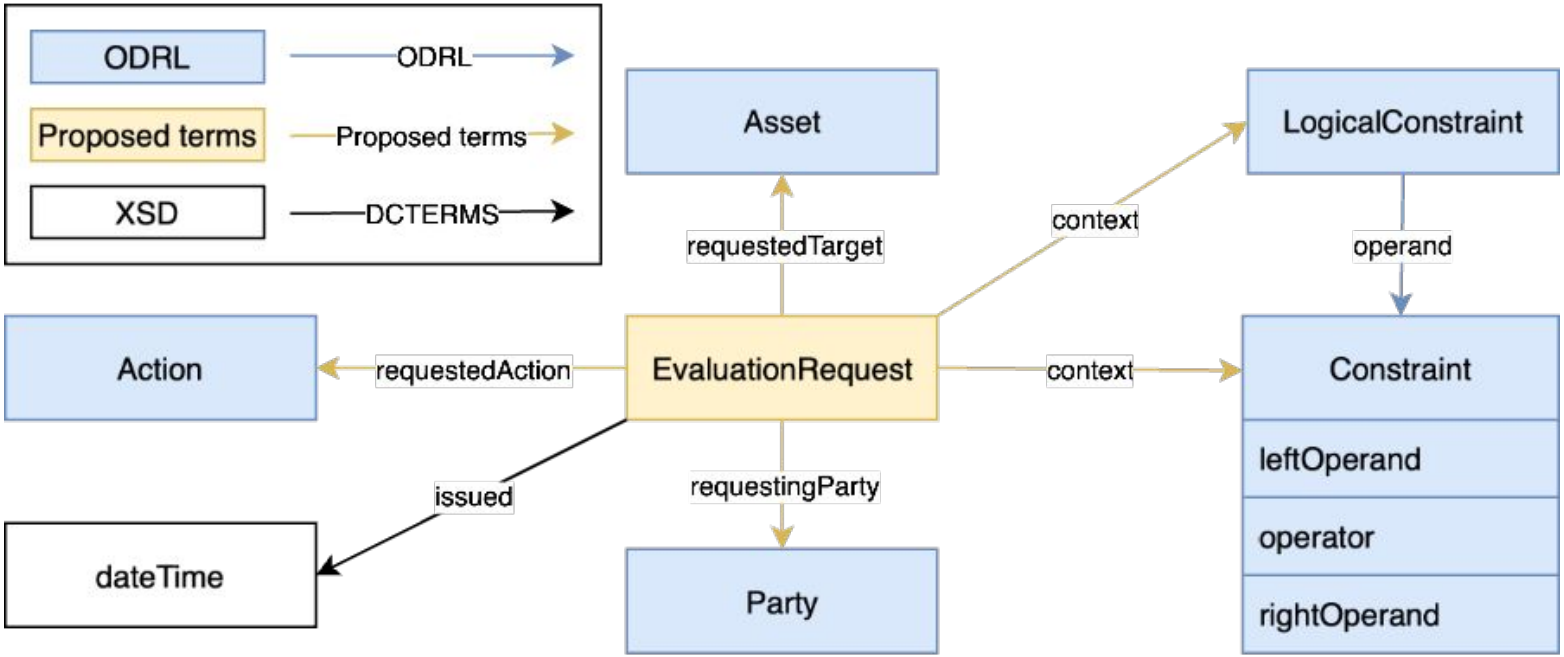
https://w3c.github.io/odrl/formal-semantics/

How to interoperably enforce ODRL policies?

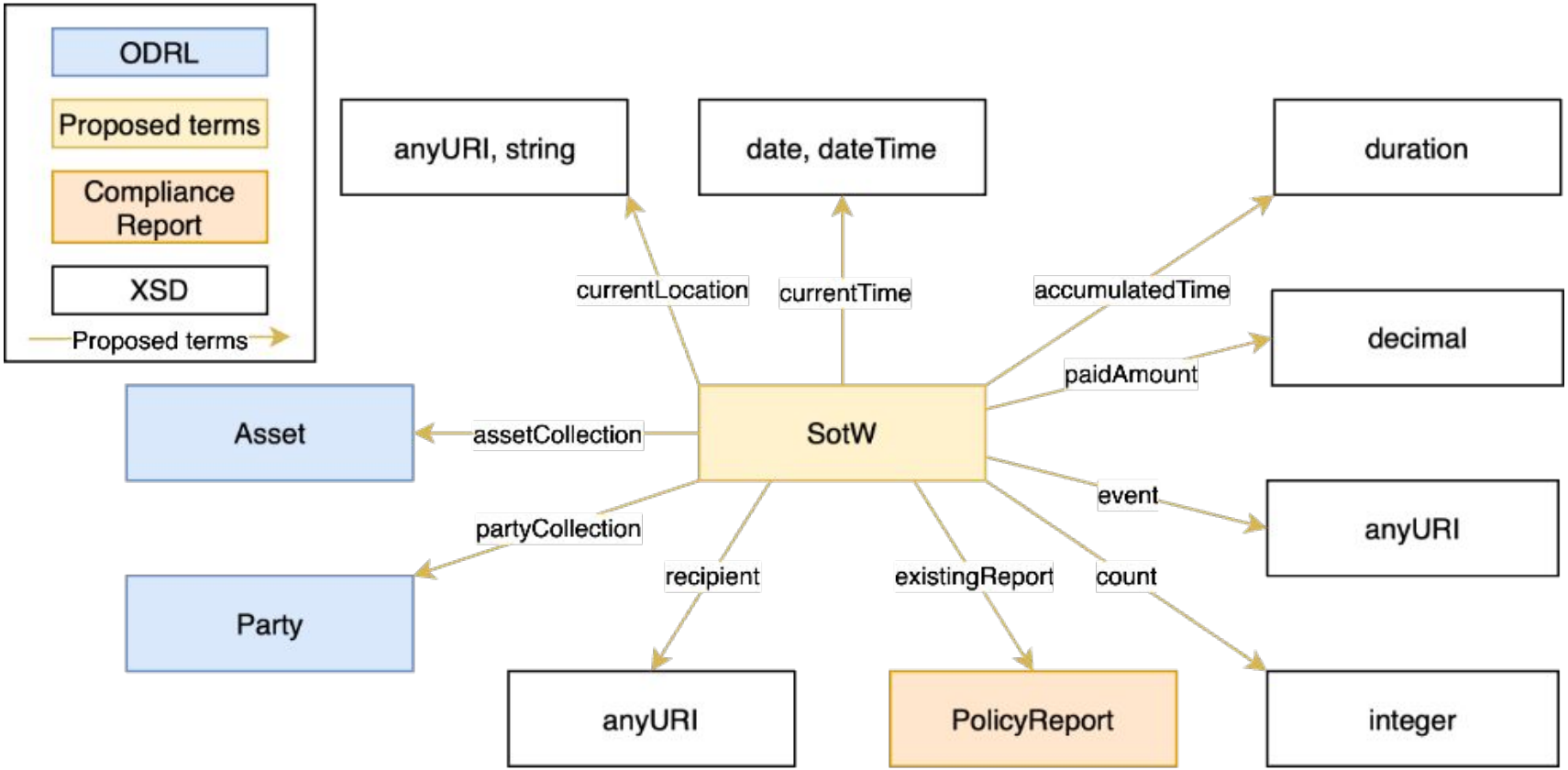


Esteves, Beatriz, Wout Slabbinck, Yassir Sellami, Andrea Cimmino, Víctor Rodríguez-Doncel, and Ruben Verborgh. **'Capturing Requests and Context for ODRL-Based Access and Usage Control'**. *Joint Proceedings of the 16th Workshop on Ontology Design and Patterns and the 1st Workshop on Bridging Hybrid Intelligence and the Semantic Web (WOP-HAIBRIDGE 2025) Co-Located with the 24th International Semantic Web Conference (ISWC 2025)*, 2025. https://ceur-ws.org/Vol-4093/paper5.pdf.

Evaluation Request



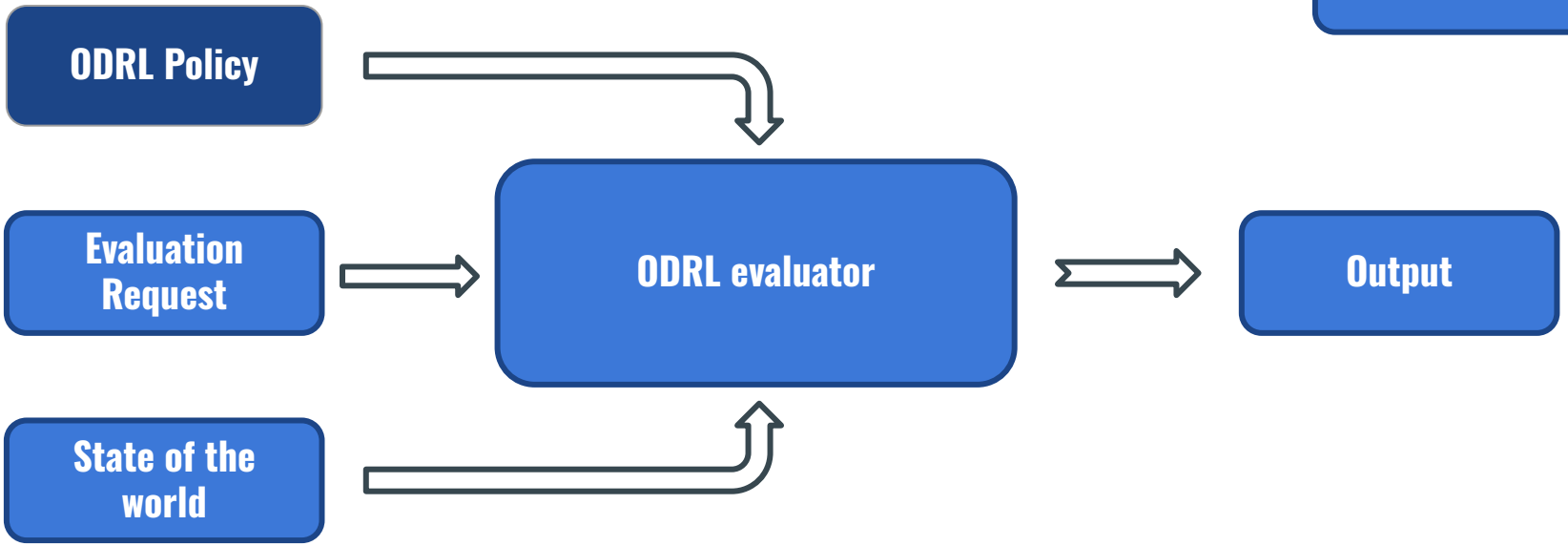
State of the world



How to interoperably enforce ODRL policies?

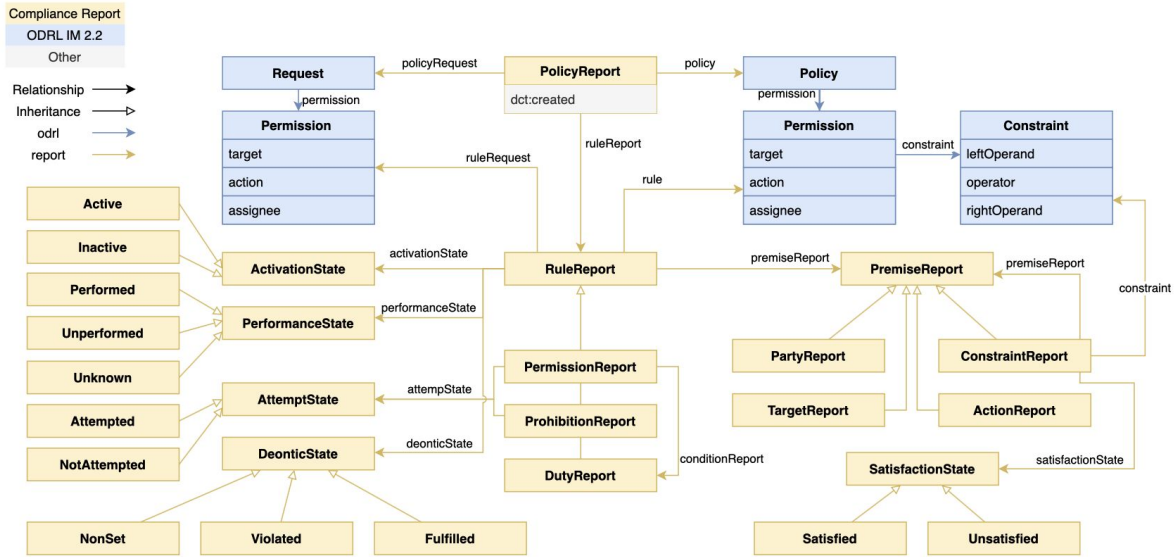
Standardised

Formalising



Slabbinck, Wout, Julián Rojas Meléndez, Beatriz Esteves, Pieter Colpaert, and Ruben Verborgh. '**Interoperable Interpretation and Evaluation of ODRL Policies**'. In *The Semantic Web*, edited by Edward Curry, Maribel Acosta, Maria Poveda-Villalón, et al. Springer Nature Switzerland, 2025. https://doi.org/10.1007/978-3-031-94578-6_11.

Interoperable Interpretation and Evaluation of ODRL Policies



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

ESWC 2025

🌟 Best Resource Nominee

FORC
A Fran valuation

Framework for ODRL Rule Compliance through Evaluation (FORCE)

Living Document, 9 July 2025

This version:
https://w3id.org/force

Previous Versions:
https://spec.knows.idlab.ugent.be/force/all/608977cf506ceb4548c8a8a1b014d1b47817a68e

Issue Tracking:
GitHub

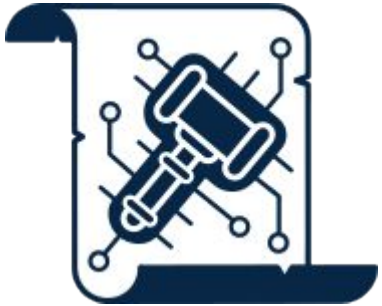
Editors:
Wout Slabbinck (Ghent University - imec)
Beatriz Esteves (Ghent University - imec)

Abstract

The Framework for ODRL Rule Compliance through Evaluation (FORCE) is designed to assist in ODRL policy development and enhance comprehension of ODRL evaluation outputs. Furthermore, it enables experimentation and prototyping of ODRL 3.0 proposals.

A Framework for ODRL Rule Compliance through Evaluation

- A set of specifications
  - Developing and Evaluating ODRL Policies
  - Navigating Related Resources
- A demonstrator
  - https://w3id.org/force/demo



Representing and enforcing policies with ODRL and DPV in decentralised systems

A Solid background

Representing policies with ODRL

Deterministic enforcement of policies

ODRL Enforcement in practice

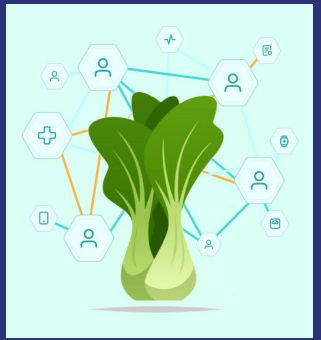
Representing and enforcing policies with ODRL and DPV in decentralised systems

A Solid background

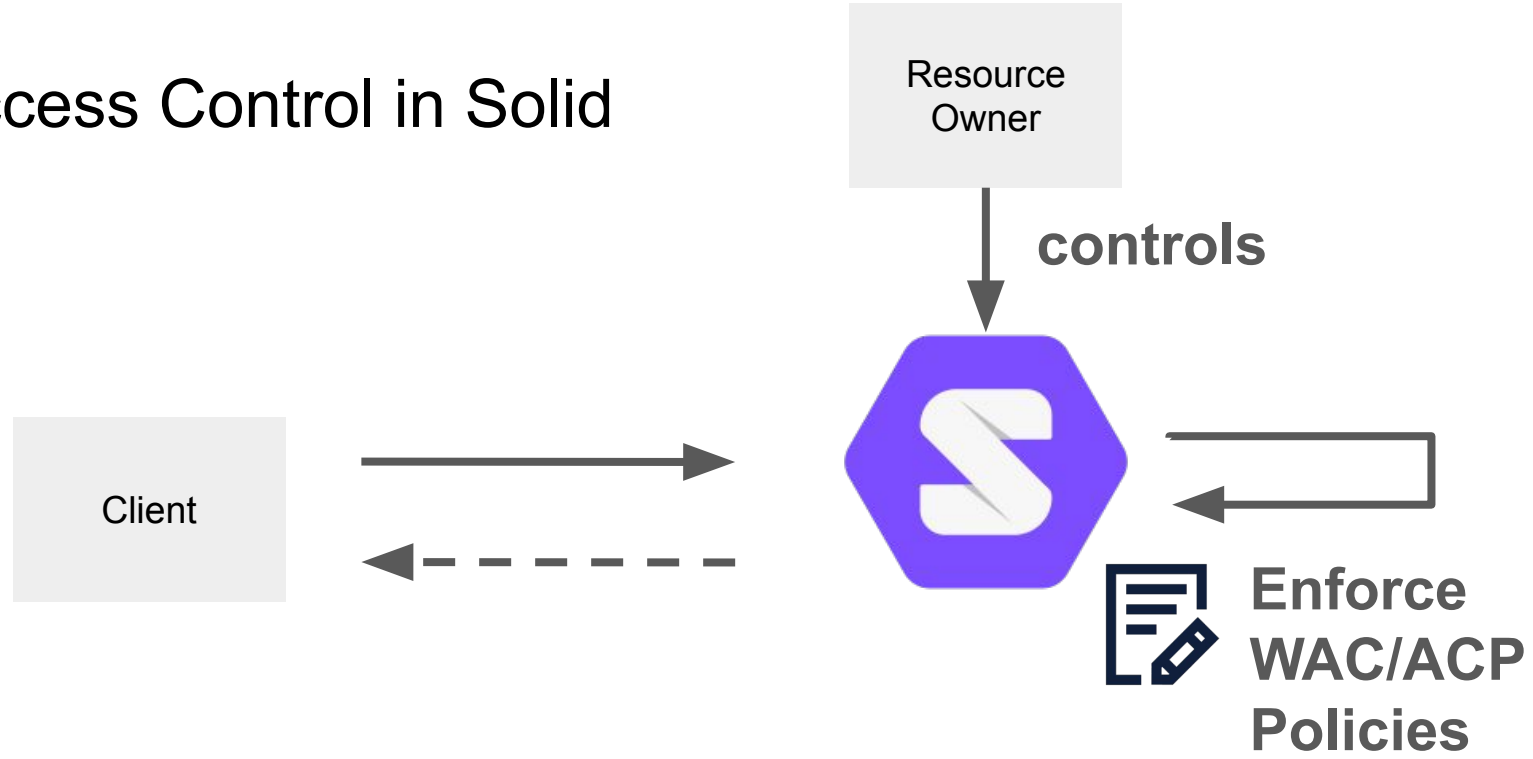
Representing policies with ODRL

Deterministic enforcement of policies

ODRL Enforcement in practice

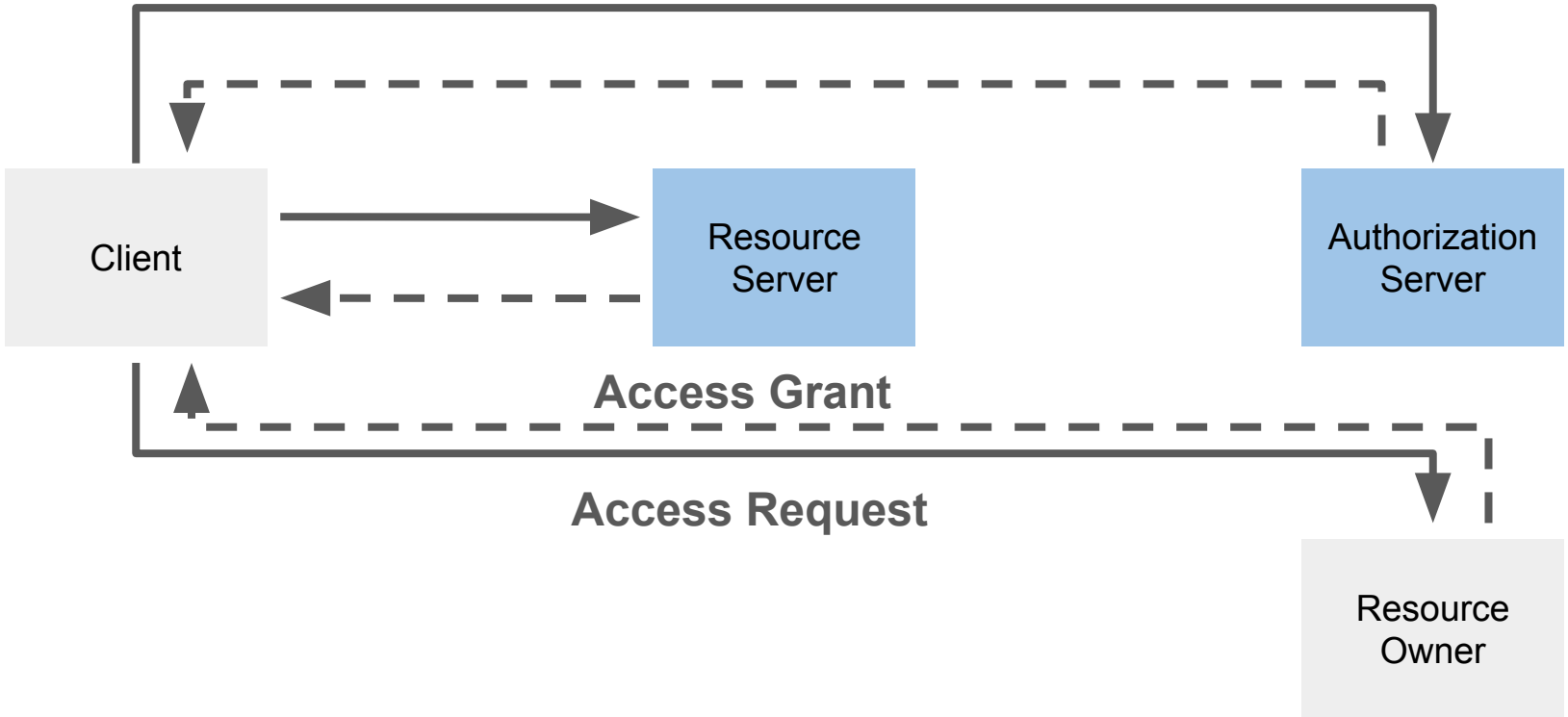


Access Control in Solid



Solid Protocol (§11): https://solidproject.org/TR/protocol#authorization

Oauth 2.0: Delegated Access and Separation of concerns



Oauth 2.0: https://datatracker.ietf.org/doc/html/rfc6749

User-Managed Access (UMA)

Oauth 2.0

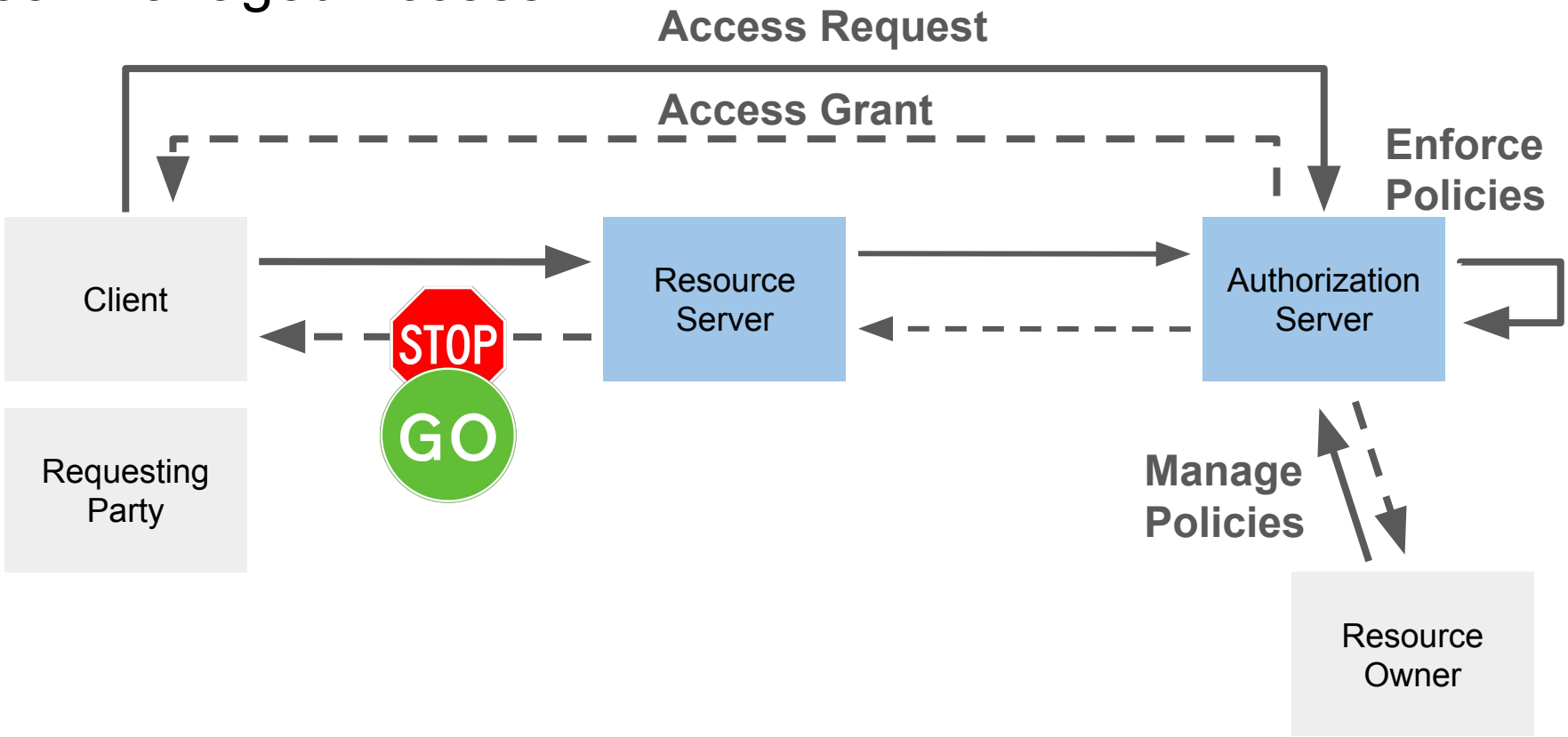
- Delegated Access Control
  - Allow third-party apps access to protected resources (without having to share credentials)
- Separation of concerns
  - Authorization Server and Resource Server
  - Standardizes obtaining an Access Token

UMA is an extension of **Oauth 2.0** and introduces

- Asynchronous access delegation through the distinction of **Requesting Party** and **Resource Owner**

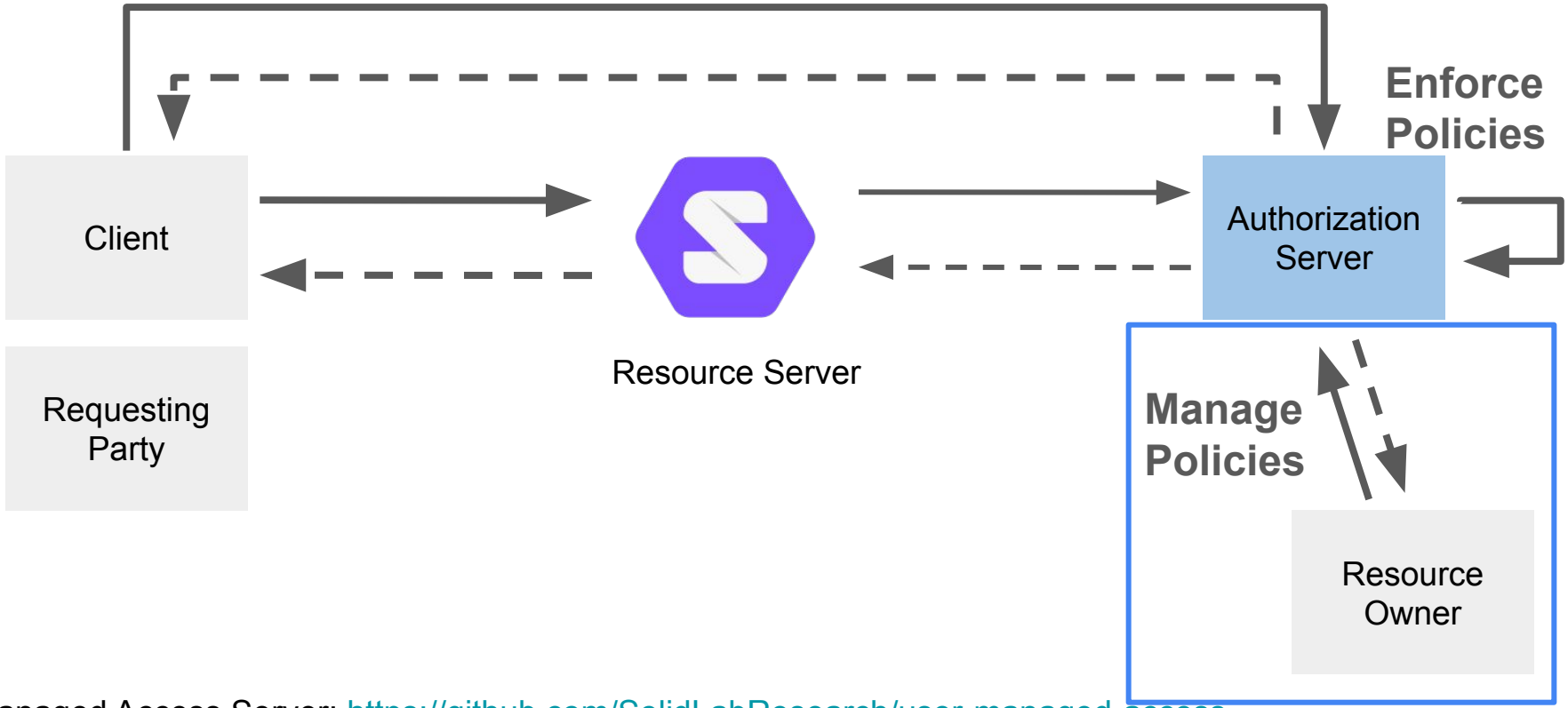
UMA: https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html

User-Managed Access



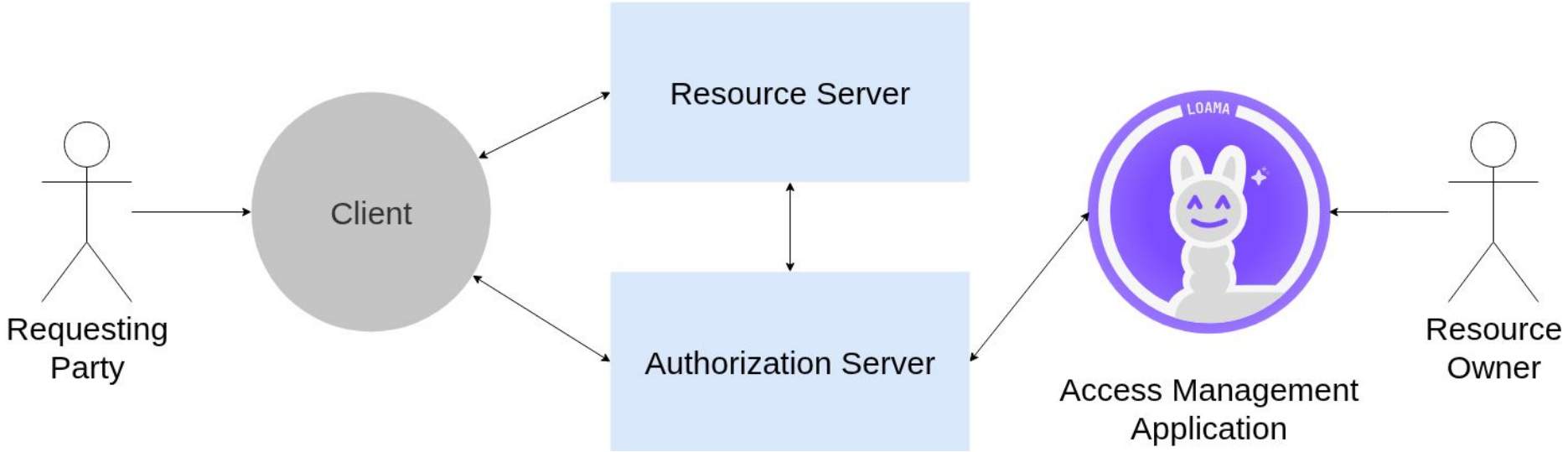
UMA: https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html

User-Managed Access and Solid

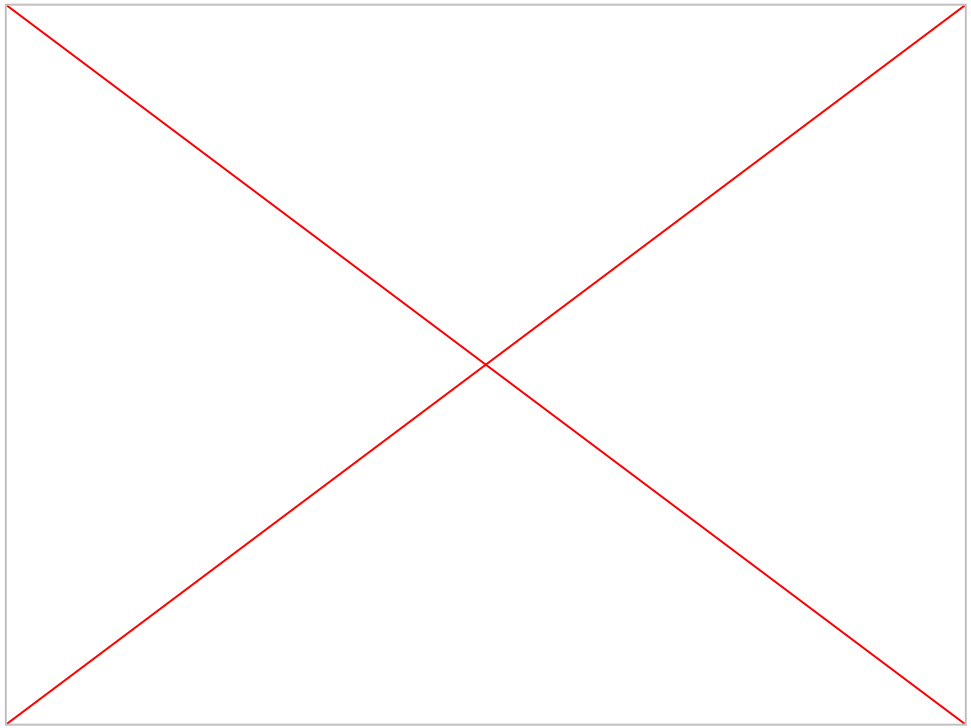


User-Managed Access Server: https://github.com/SolidLabResearch/user-managed-access

LOAMA: Low-code ODRL Access Management Application



LOAMA: Low-code ODRL Access Management Application



Demo: https://zenodo.org/records/16640205
Paper: https://ceur-ws.org/Vol-4085/paper83.pdf

The future for ODRL is bright!

ODRL 3.0 workshop

Policy management UX survey

Trust Triggers
Monday 20 April

ODRL 3.0 workshop: https://w3c.github.io/odrl/W3C-ODRL-Workshop-2026/
Policy management UX survey: https://ugent.qualtrics.com/jfe/form/SV_0x4GXnjlRkDfvAG
Trut Triggers Event: https://trustflows.eu/events/2026/04/trust-triggers-1/