COST EUROPEAN COOPERATION IN SCIENCE & TECHNOLOGY

Protect

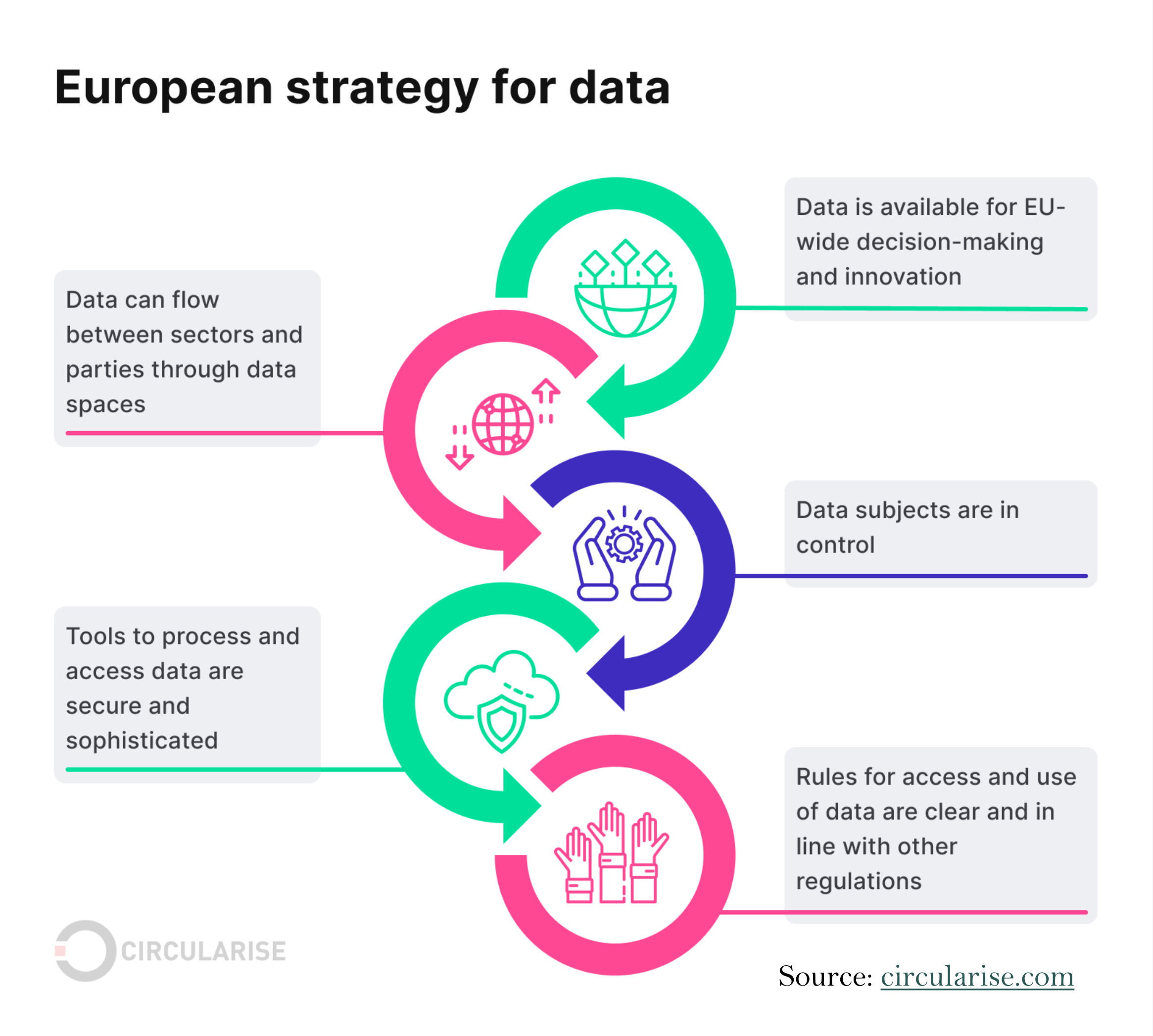
Policies in Solid: The Road Ahead

Beatriz Esteves, Ontology Engineering Group, Universidad Politécnica de Madrid

beatriz.gesteves@upm.es | besteves4@eupolicy.social

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 813497.

Motivation



European strategy for data

Data is available for EU-wide decision-making and innovation

Data can flow between sectors and parties through data spaces

Data subjects are in control

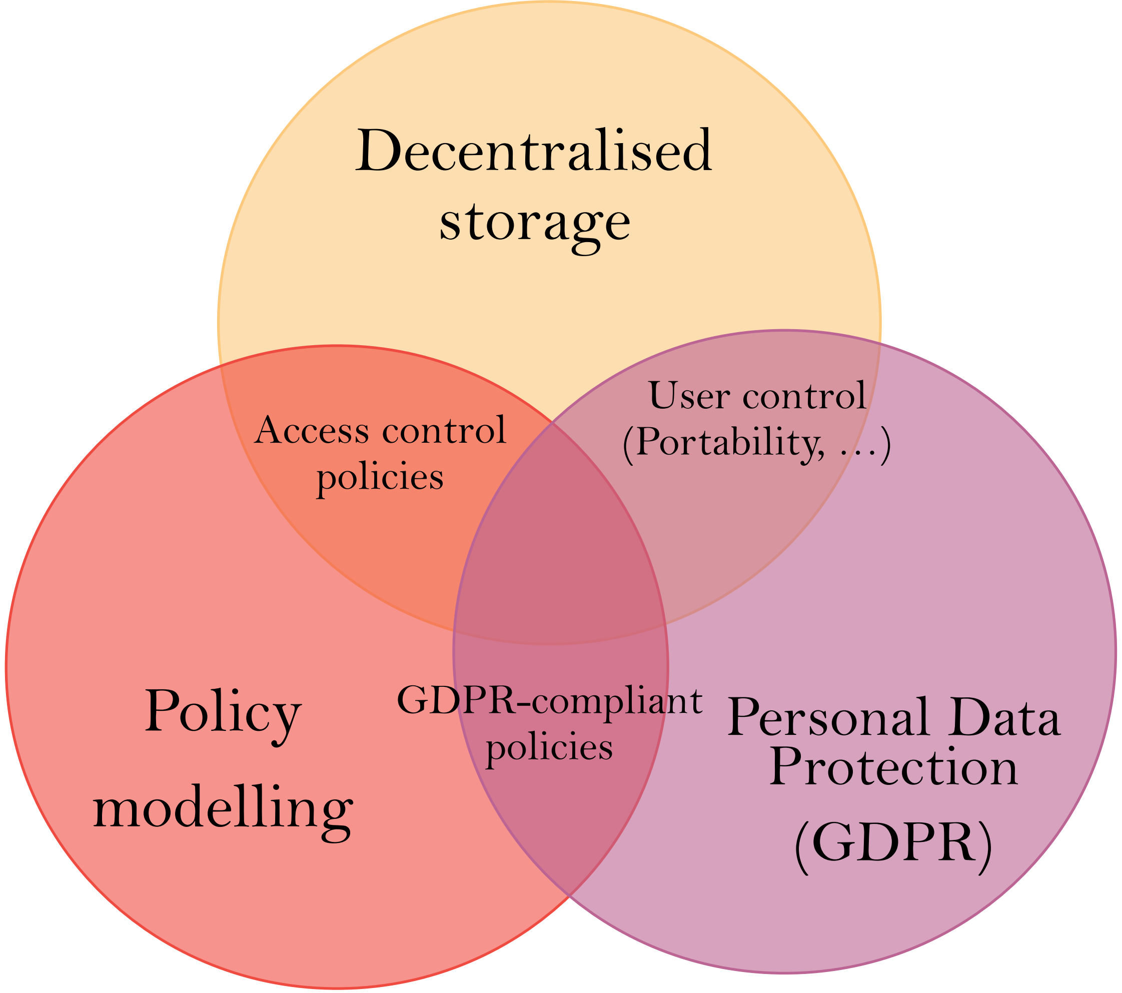
Tools to process and access data are secure and sophisticated

Rules for access and use of data are clear and in line with other regulations

Source: circularise.com

- ePrivacy 2008
- GDPR 2016
- DGA 2020
- DMA 2020
- DSA 2020
- AI Act 2021
- Data Act 2022
- Health Data Space 2022

Motivation


Decentralised storage
Access control policies
User control (Portability, …)
Policy modelling
GDPR-compliant policies
Personal Data Protection (GDPR)

SotA – Solid Authorisation

WAC

Beatriz has read-write access to the resource located at https://victor.pod/docs/file1

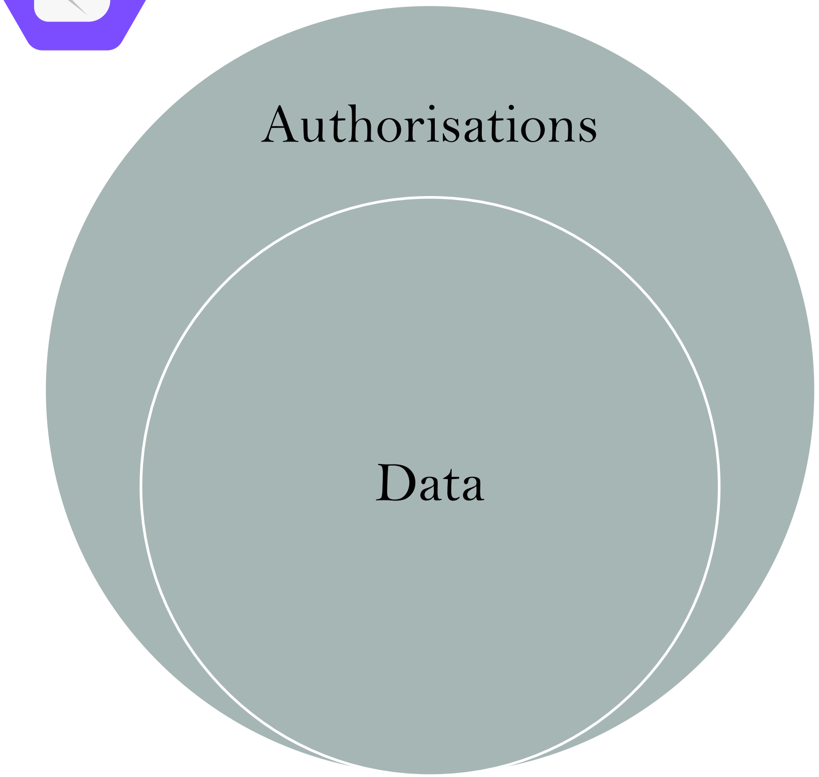
```
<#authorization1>
     a acl:Authorization;
     acl:agent  <https://beatriz.pod/profile/card#me>;
     acl:accessTo  <https://victor.pod/docs/file1.ttl>;
     acl:mode acl:Read, acl:Write.
```

ACP

Beatriz has read-write access to the resource located at https://victor.pod/docs/file1

```
<#grant1> a acp:AccessGrant ;
 acp:grant acl:Read, acl:Write ;
 acp:context [
  acp:agent <https://beatriz.pod/profile/card#me>;
  acp:target <https://victor.pod/docs/file1.ttl>
] .
```

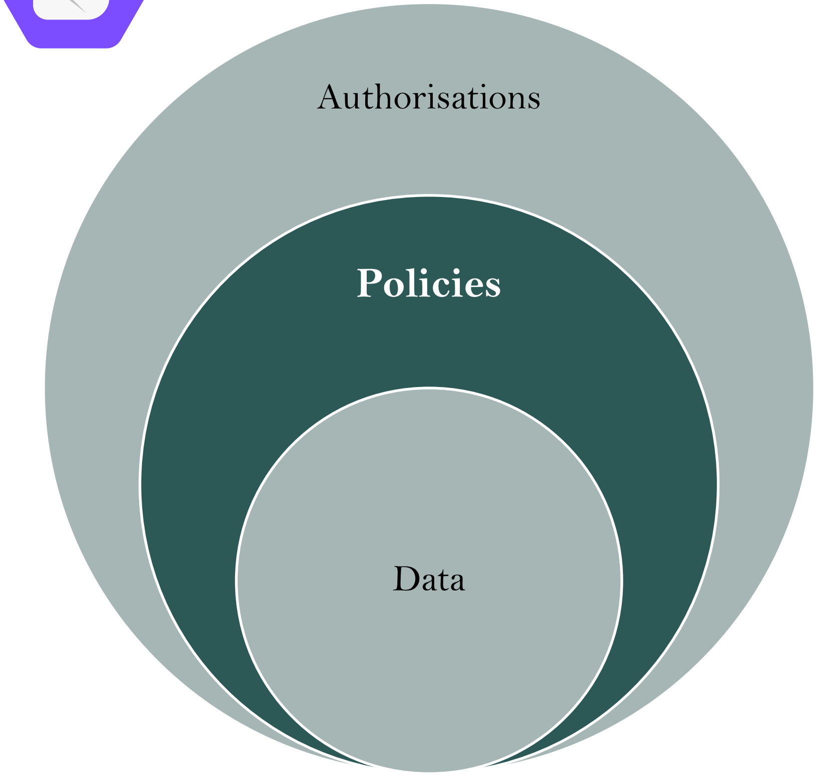
Problems



Authorisations

Data

Problems

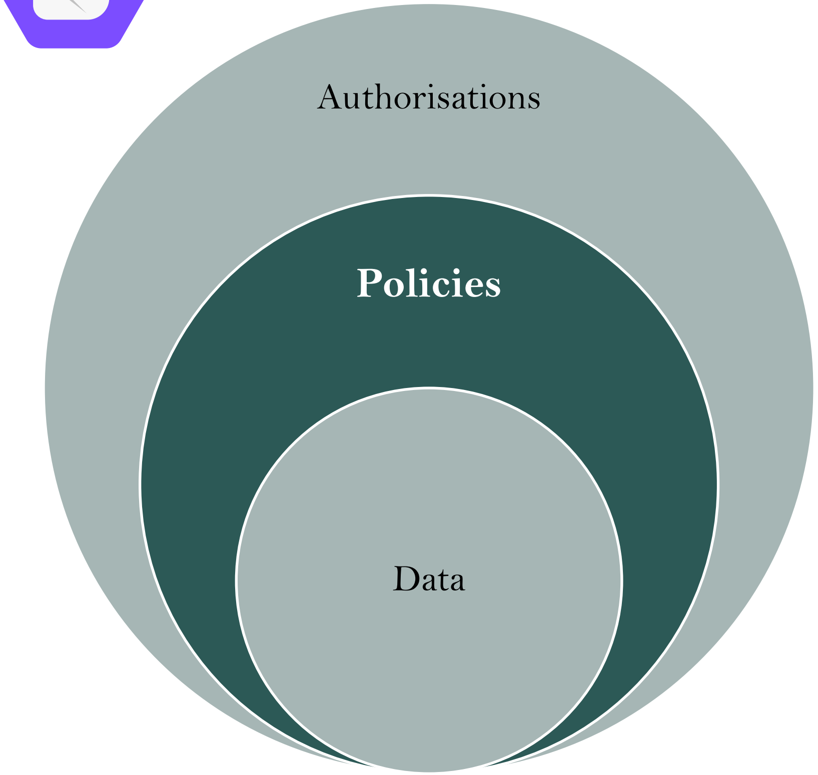


Esteves, B., Pandit, H. J., & Rodríguez-Doncel, V. (2021). ODRL Profile for Expressing Consent through Granular Access Control Policies in Solid. In 2021 IEEE European Symposium on Security and Privacy Workshops (pp. 298-306). https://ieeexplore.ieee.org/abstract/document/9583717

Requisites for a GDPR-aligned Solid

R1. Support specifying user preferences as policies.
R2. Incorporate vocabulary specifying or aligned to legal concepts.
R3. Support specifying permissions and prohibitions at arbitrary granularity.
R4. Record (store) policies used to authorize access.
R5. Keep logs (what? who? why? where? when? how?) to establish responsibilities and accountability within the Solid ecosystem

Problems



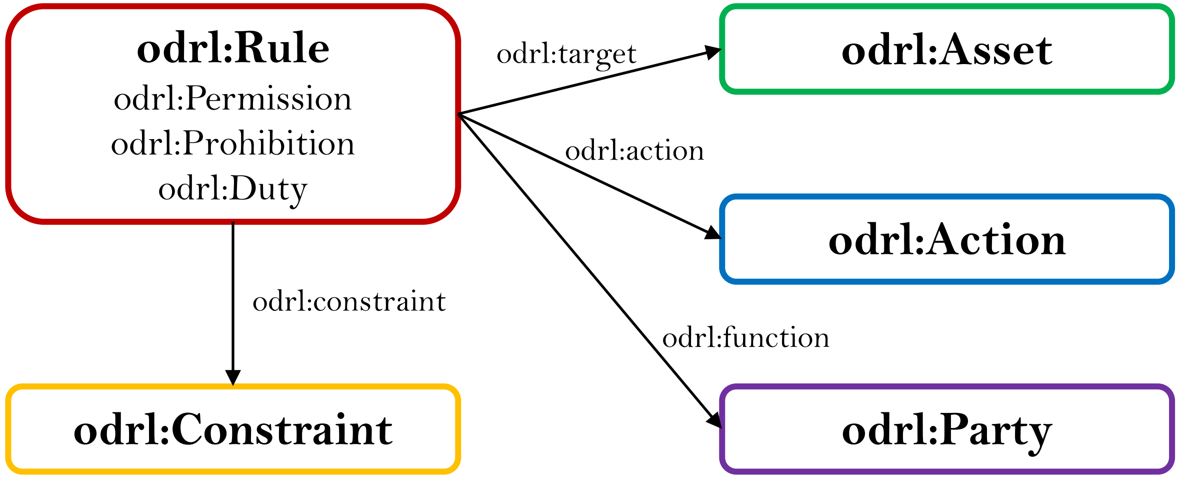
Esteves, B., Pandit, H. J., & Rodríguez-Doncel, V. (2021). ODRL Profile for Expressing Consent through Granular Access Control Policies in Solid. In 2021 IEEE European Symposium on Security and Privacy Workshops (pp. 298-306). https://ieeexplore.ieee.org/abstract/document/9583717

Requisites for a GDPR-aligned Solid

R1. Support specifying user preferences as policies.
R2. Incorporate vocabulary specifying or aligned to legal concepts.
R3. Support specifying permissions and prohibitions at arbitrary granularity.
R4. Record (store) policies used to authorize access.
R5. Keep logs (what? who? why? where? when? how?) to establish responsibilities and accountability within the Solid ecosystem

ODRL + DPV

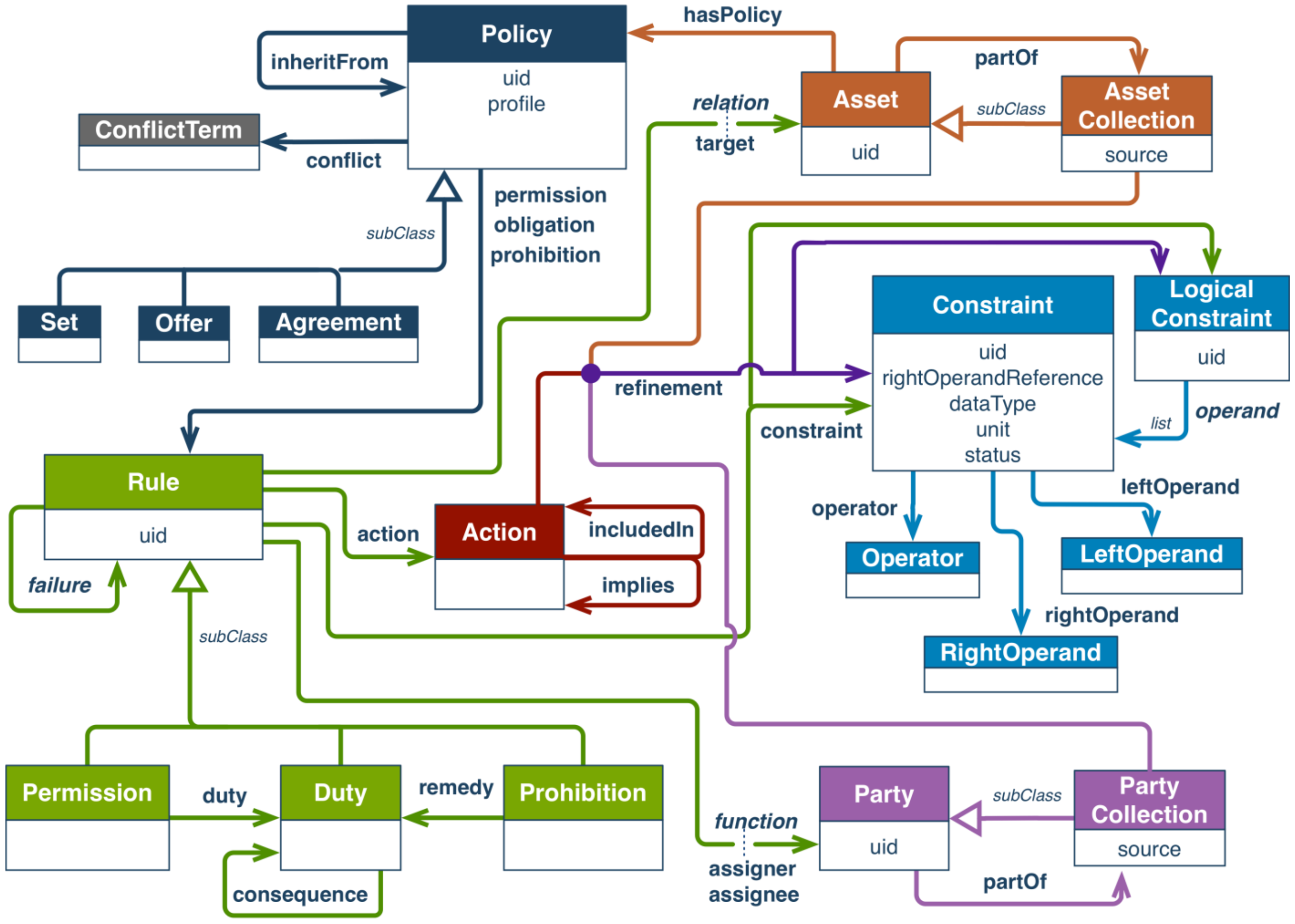
Open Digital Rights Language (ODRL)



W3C Recommendation to represent "Policies that express Permissions, Prohibitions and Duties related to the usage of Asset resources"
https://www.w3.org/TR/odrl-model/

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

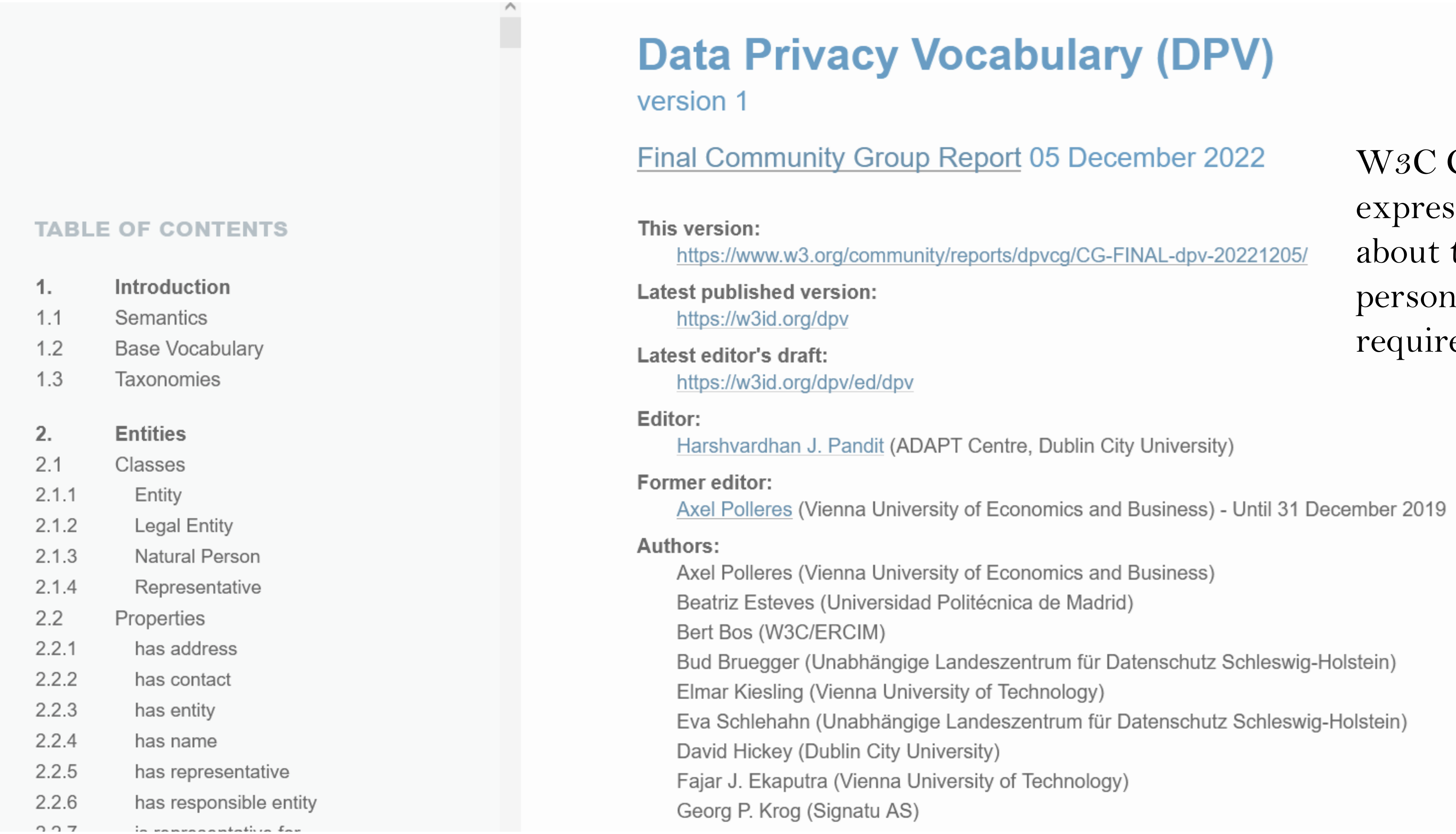
Open Digital Rights Language (ODRL)



Target asset may be distributed until 2024-01-01

```
<#policy1> a odrl:Offer ;
 odrl:permission [
  odrl:assigner <http://example.com/org:43>;
  odrl:target <http://example.com/document:44>;
  odrl:action odrl:distribute;
  odrl:constraint [
   odrl:leftOperand odrl:dateTime;
   odrl:operator odrl:lt;
   odrl:rightOperand “2024-01-01”^^xsd:date
  ]
 ].
```

Data Privacy Vocabulary (DPV)



Data Privacy Vocabulary (DPV)

version 1

Final Community Group Report 05 December 2022

This version:
https://www.w3.org/community/reports/dpvcg/CG-FINAL-dpv-20221205/

Latest published version:
https://w3id.org/dpv

Latest editor's draft:
https://w3id.org/dpv/ed/dpv

Editor:
Harshvardhan J. Pandit (ADAPT Centre, Dublin City University)

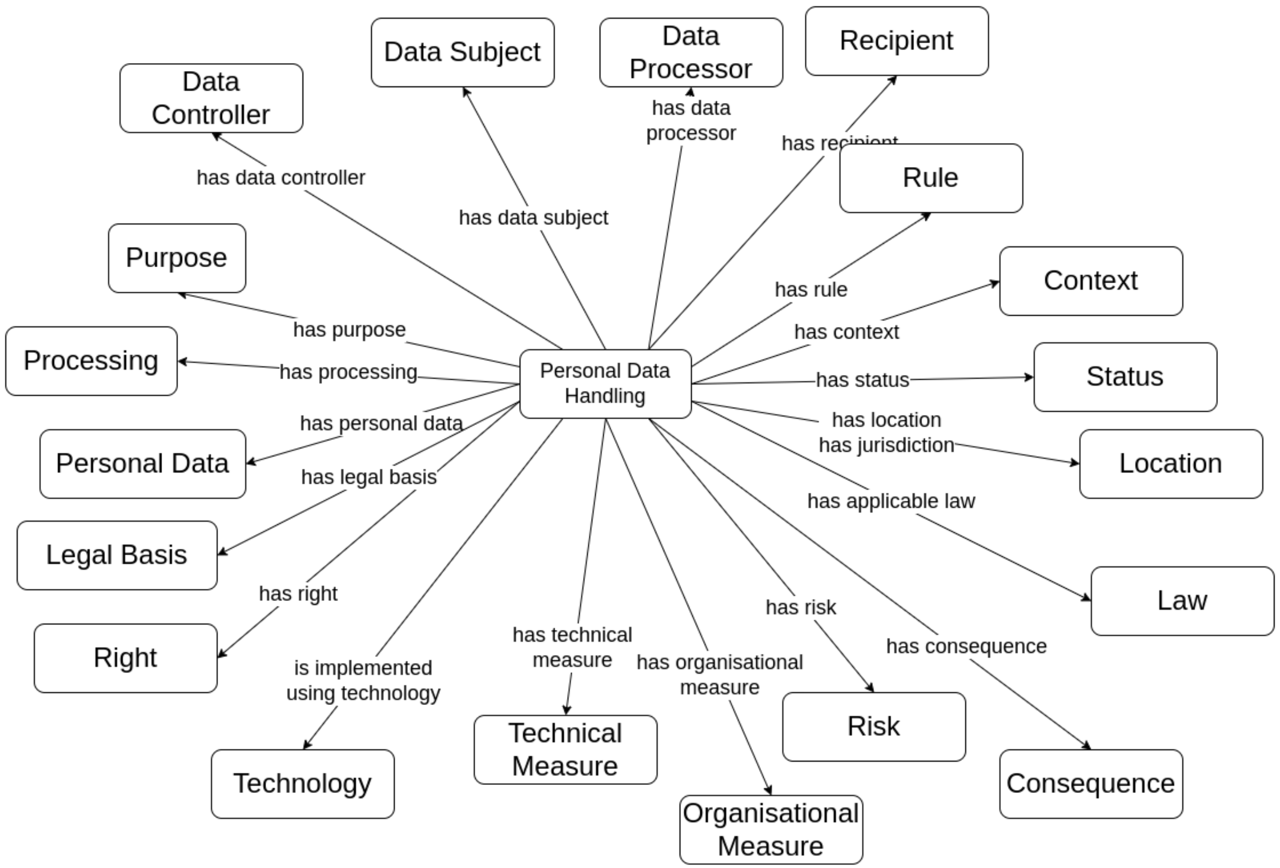
Former editor:
Axel Polleres (Vienna University of Economics and Business) - Until 31 December 2019

Authors:
Axel Polleres (Vienna University of Economics and Business)
Beatriz Esteves (Universidad Politécnica de Madrid)
Bert Bos (W3C/ERCIM)
Bud Bruegger (Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein)
Elmar Kiesling (Vienna University of Technology)
Eva Schlehahn (Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein)
David Hickey (Dublin City University)
Fajar J. Ekaputra (Vienna University of Technology)
Georg P. Krog (Signatu AS)

W3C Community Group Report to express "machine-readable metadata about the use and processing of personal data based on legislative requirements such as the GDPR"

https://w3id.org/dpv

Data Privacy Vocabulary (DPV)



Personal Data Handling

has data controller → Data Controller

has data subject → Data Subject

has data processor → Data Processor

has recipient → Recipient

has rule → Rule

has context → Context

has status → Status

has location
has jurisdiction → Location

has applicable law → Law

has consequence → Consequence

has risk → Risk

has organisational measure → Organisational Measure

has technical measure → Technical Measure

is implemented using technology → Technology

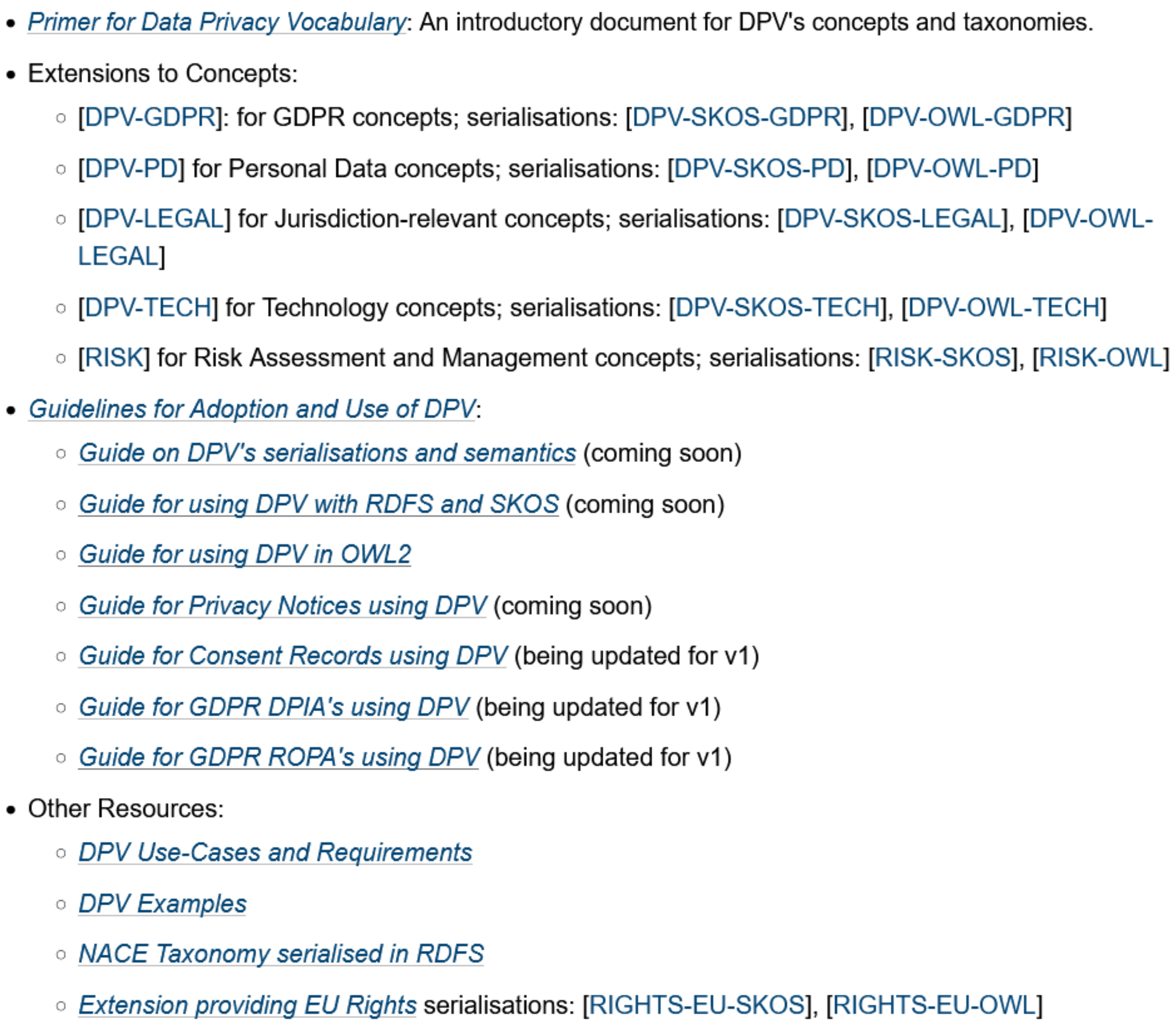
has right → Right

has legal basis → Legal Basis

has personal data → Personal Data

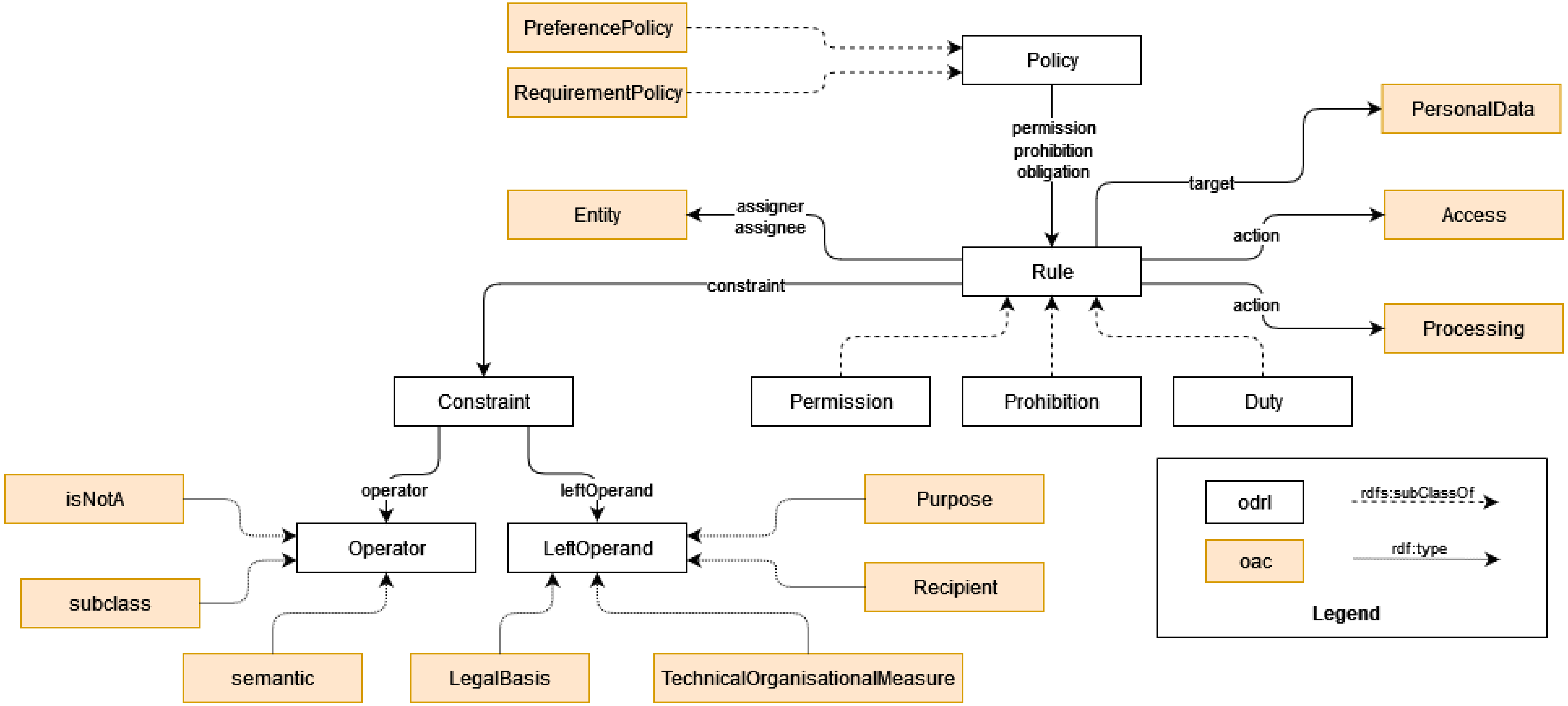
has processing → Processing

has purpose → Purpose



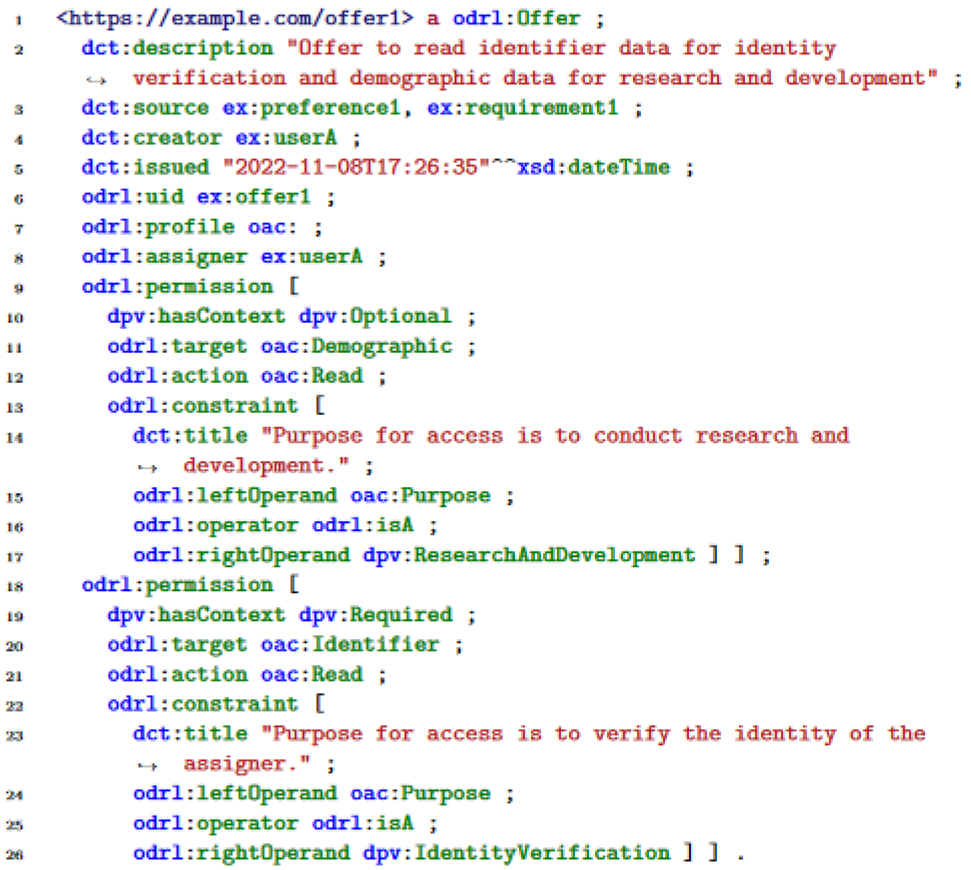
- *Primer for Data Privacy Vocabulary*: An introductory document for DPV's concepts and taxonomies.
- Extensions to Concepts:
  - [DPV-GDPR]: for GDPR concepts; serialisations: [DPV-SKOS-GDPR], [DPV-OWL-GDPR]
  - [DPV-PD] for Personal Data concepts; serialisations: [DPV-SKOS-PD], [DPV-OWL-PD]
  - [DPV-LEGAL] for Jurisdiction-relevant concepts; serialisations: [DPV-SKOS-LEGAL], [DPV-OWL-LEGAL]
  - [DPV-TECH] for Technology concepts; serialisations: [DPV-SKOS-TECH], [DPV-OWL-TECH]
  - [RISK] for Risk Assessment and Management concepts; serialisations: [RISK-SKOS], [RISK-OWL]
- *Guidelines for Adoption and Use of DPV*:
  - *Guide on DPV's serialisations and semantics* (coming soon)
  - *Guide for using DPV with RDFS and SKOS* (coming soon)
  - *Guide for using DPV in OWL2*
  - *Guide for Privacy Notices using DPV* (coming soon)
  - *Guide for Consent Records using DPV* (being updated for v1)
  - *Guide for GDPR DPIA's using DPV* (being updated for v1)
  - *Guide for GDPR ROPA's using DPV* (being updated for v1)
- Other Resources:
  - *DPV Use-Cases and Requirements*
  - *DPV Examples*
  - *NACE Taxonomy serialised in RDFS*
  - *Extension providing EU Rights* serialisations: [RIGHTS-EU-SKOS], [RIGHTS-EU-OWL]

ODRL profile for Access Control (OAC)

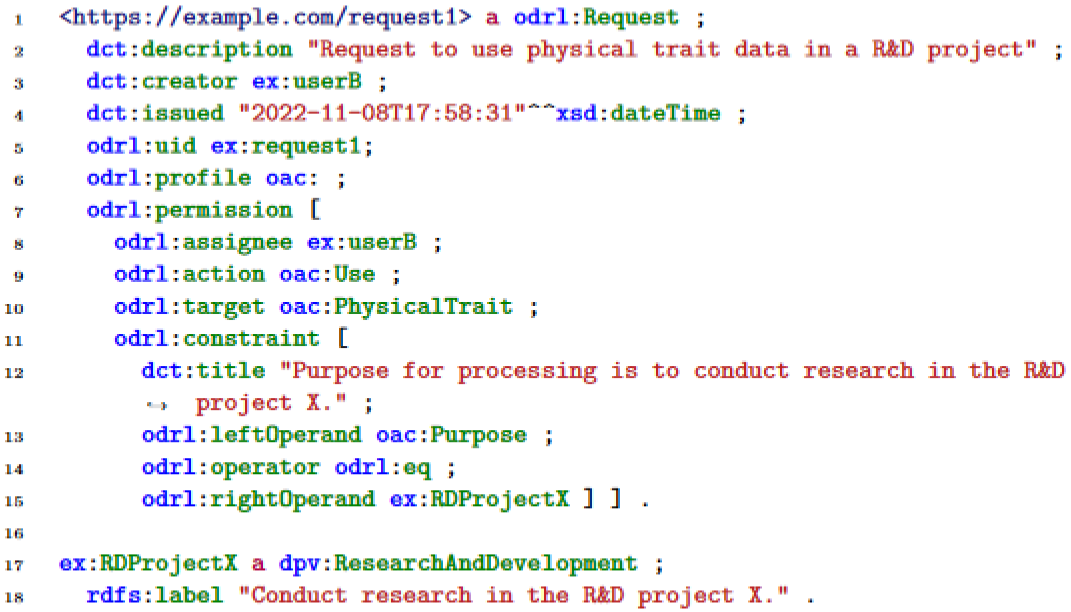


https://w3id.org/oac

ODRL profile for Access Control (OAC)



```
<https://example.com/offer1> a odrl:Offer ;
  dct:description "Offer to read identifier data for identity
  ↪  verification and demographic data for research and development" ;
  dct:source ex:preference1, ex:requirement1 ;
  dct:creator ex:userA ;
  dct:issued "2022-11-08T17:26:35"^^xsd:dateTime ;
  odrl:uid ex:offer1 ;
  odrl:profile oac: ;
  odrl:assigner ex:userA ;
  odrl:permission [
    dpv:hasContext dpv:Optional ;
    odrl:target oac:Demographic ;
    odrl:action oac:Read ;
    odrl:constraint [
      dct:title "Purpose for access is to conduct research and
      ↪  development." ;
      odrl:leftOperand oac:Purpose ;
      odrl:operator odrl:isA ;
      odrl:rightOperand dpv:ResearchAndDevelopment ] ] ;
  odrl:permission [
    dpv:hasContext dpv:Required ;
    odrl:target oac:Identifier ;
    odrl:action oac:Read ;
    odrl:constraint [
      dct:title "Purpose for access is to verify the identity of the
      ↪  assigner." ;
      odrl:leftOperand oac:Purpose ;
      odrl:operator odrl:isA ;
      odrl:rightOperand dpv:IdentityVerification ] ] .
```



```
<https://example.com/request1> a odrl:Request ;
  dct:description "Request to use physical trait data in a R&D project" ;
  dct:creator ex:userB ;
  dct:issued "2022-11-08T17:58:31"^^xsd:dateTime ;
  odrl:uid ex:request1;
  odrl:profile oac: ;
  odrl:permission [
    odrl:assignee ex:userB ;
    odrl:action oac:Use ;
    odrl:target oac:PhysicalTrait ;
    odrl:constraint [
      dct:title "Purpose for processing is to conduct research in the R&D
      ↪  project X." ;
      odrl:leftOperand oac:Purpose ;
      odrl:operator odrl:eq ;
      odrl:rightOperand ex:RDProjectX ] ] .

ex:RDProjectX a dpv:ResearchAndDevelopment ;
  rdfs:label "Conduct research in the R&D project X." .
```

Different Use Cases, Different Requirements

Data Spaces

Focused on usage control

Temporal constraints (duration, interval, …)
Payments
Constraints on systems
Number of usages
Deletion after usage

Solid Agents

Make decisions for you in terms of what data can be automatically shared

For what data types?
For what purpose?
For which recipients?
For what type of automation?

Different Use Cases, Different Requirements

IoT data

Aggregated data
If containing personal data, anonymisation needs to be considered

Temporal constraints
Spatial constraints

Logistics

Disclose location of transports, routes, …
Type of vehicles
Types of material being transported, ...
Information about people

Different Use Cases, Different Requirements

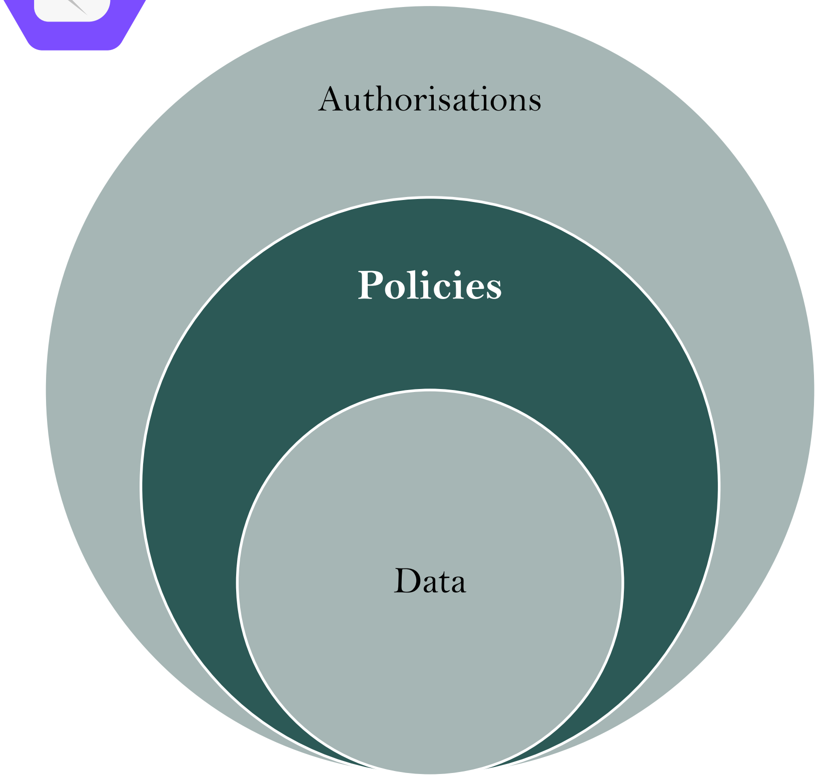
Collection of ODRL policies

https://github.com/besteves4/oac-policies

Different use cases will require different concepts to be modeled – should we aim to have an ODRL profile for Solid that caters to all of these requirements?

Difficult as new requirements might appear at any point…

Policies in Solid



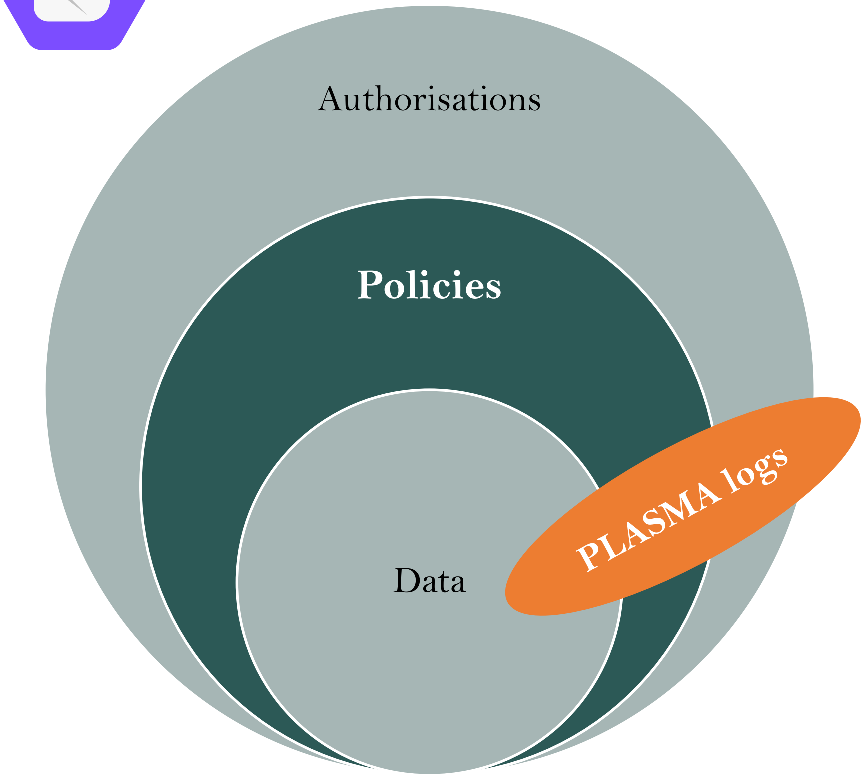
Esteves, B., Pandit, H. J., & Rodríguez-Doncel, V. (2021). ODRL Profile for Expressing Consent through Granular Access Control Policies in Solid. In 2021 IEEE European Symposium on Security and Privacy Workshops (pp. 298-306). https://ieeexplore.ieee.org/abstract/document/9583717

Requisites for a GDPR-aligned Solid

R1. Support specifying user preferences as policies.
R2. Incorporate vocabulary specifying or aligned to legal concepts.
R3. Support specifying permissions and prohibitions at arbitrary granularity.
R4. Record (store) policies used to authorize access.
R5. Keep logs (what? who? why? where? when? how?) to establish responsibilities and accountability within the Solid ecosystem

ODRL + DPV (OAC)

Policies in Solid + Logging



Requisites for a GDPR-aligned Solid

R1. Support specifying user preferences as policies.
R2. Incorporate vocabulary specifying or aligned to legal concepts.
R3. Support specifying permissions and prohibitions at arbitrary granularity.
R4. Record (store) policies used to authorize access.
R5. Keep logs (what? who? why? where? when? how?) to establish responsibilities and accountability within the Solid ecosystem

OAC + PLASMA

PLASMA - Policy LAnguage for Solid's Metadata-based Access control

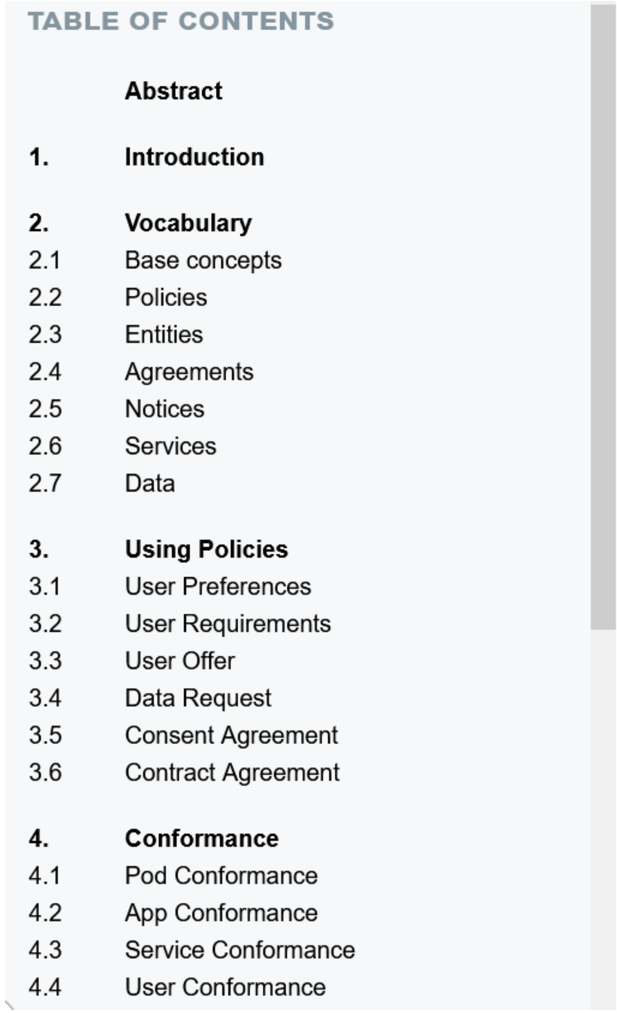
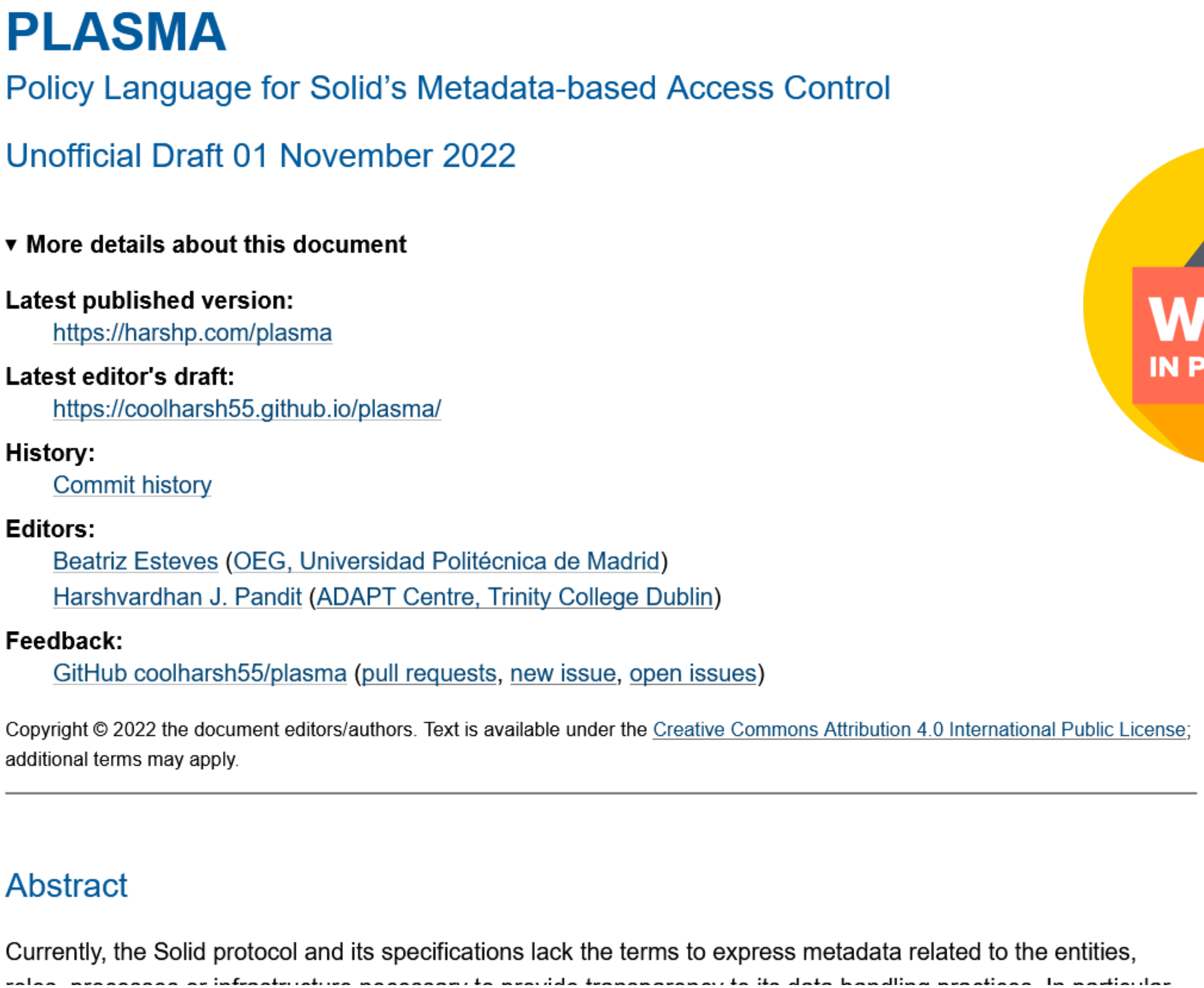


TABLE OF CONTENTS



PLASMA

Policy Language for Solid's Metadata-based Access Control

Unofficial Draft 01 November 2022

▾ **More details about this document**

Latest published version:
https://harshp.com/plasma

Latest editor's draft:
https://coolharsh55.github.io/plasma/

History:
Commit history

Editors:
Beatriz Esteves (OEG, Universidad Politécnica de Madrid)
Harshvardhan J. Pandit (ADAPT Centre, Trinity College Dublin)

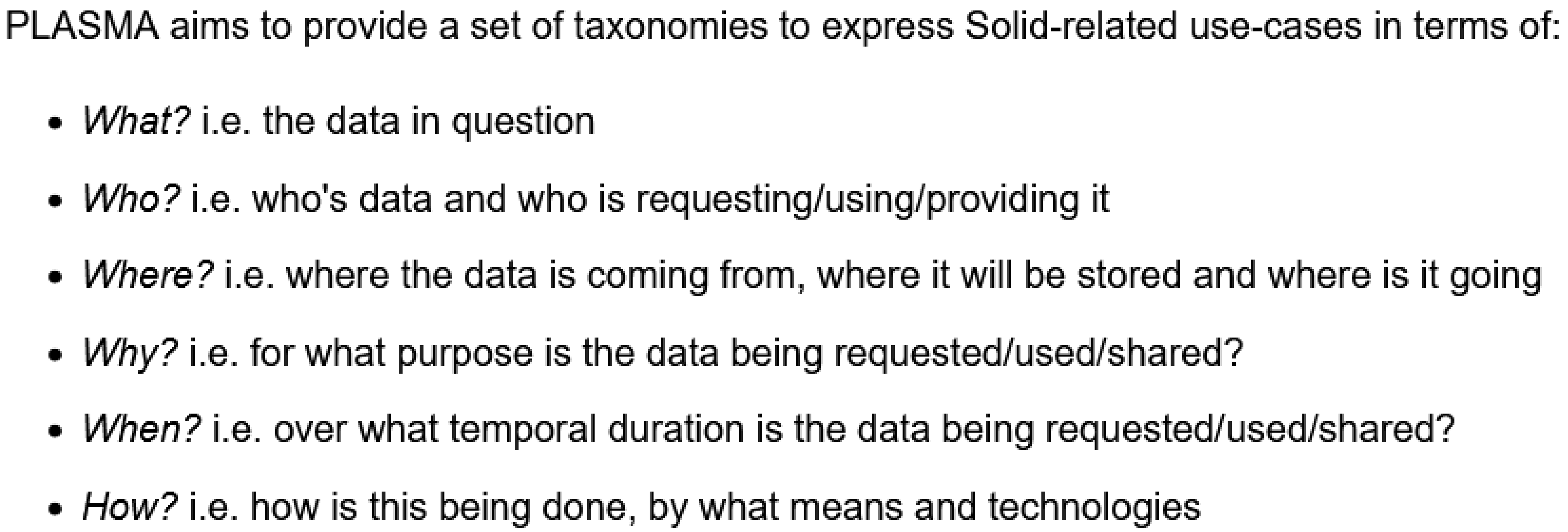
Feedback:
GitHub coolharsh55/plasma (pull requests, new issue, open issues)

Abstract

Currently, the Solid protocol and its specifications lack the terms to express metadata related to the entities, roles, processes or infrastructure necessary to provide transparency to its data handling practices. In particular

Source: Flaticon

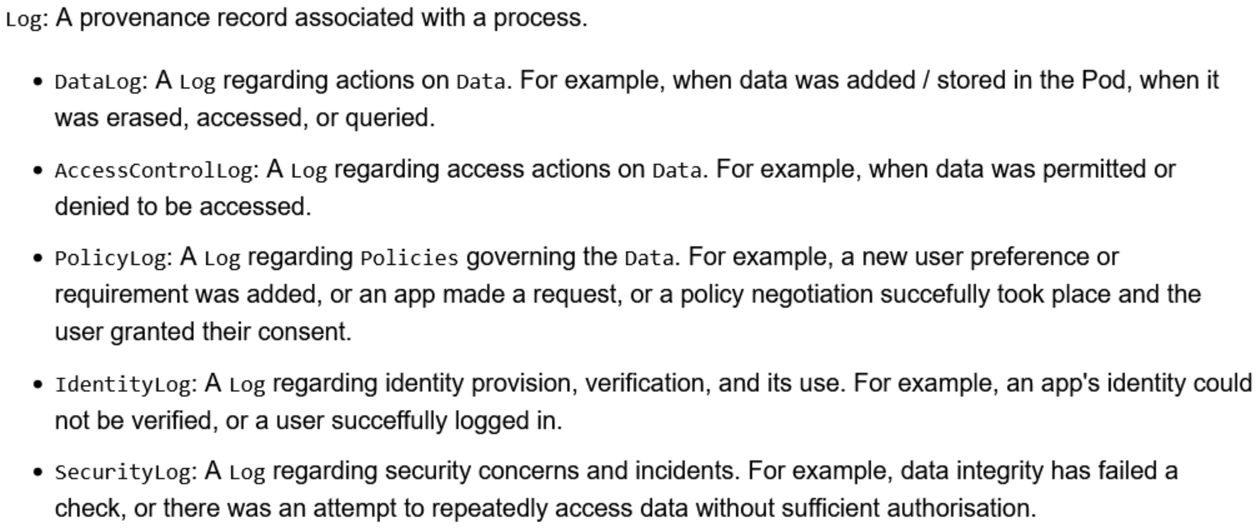
PLASMA - Policy LAnguage for Solid’s Metadata-based Access control



PLASMA aims to provide a set of taxonomies to express Solid-related use-cases in terms of:

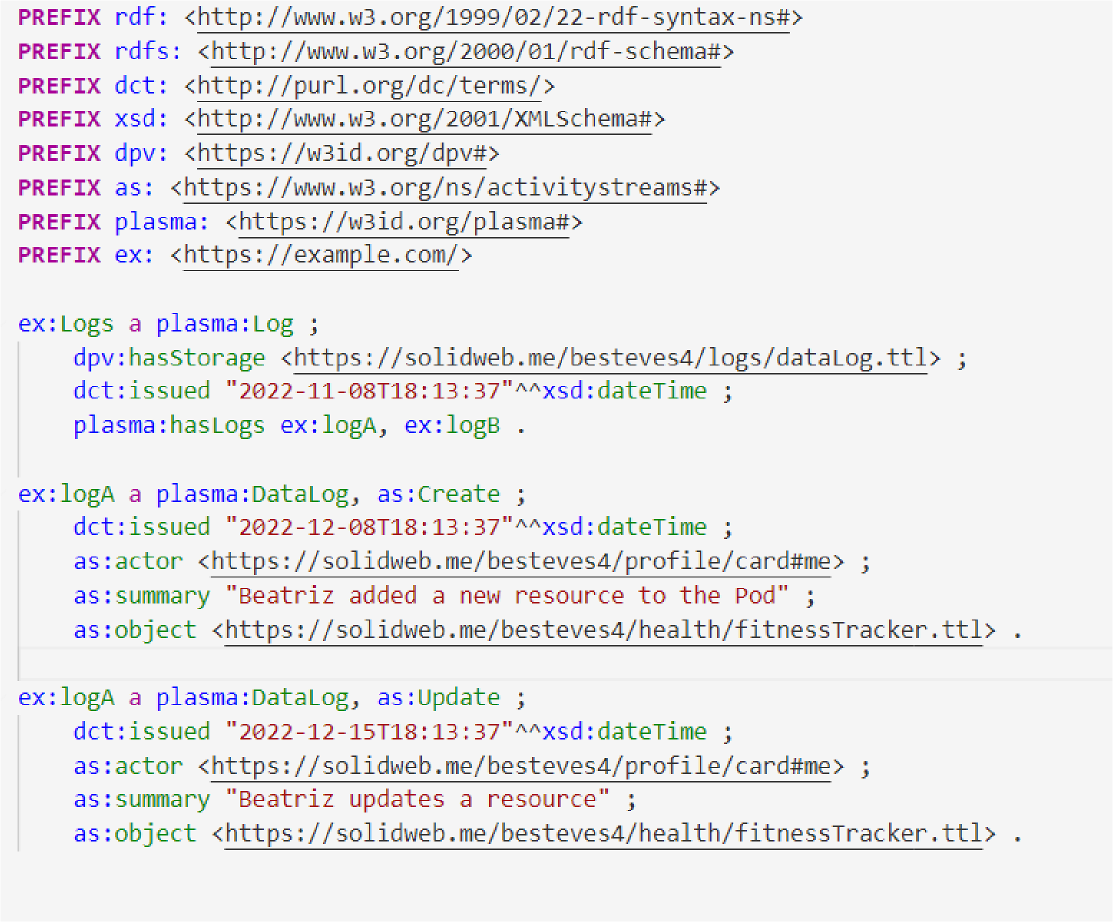
- *What?* i.e. the data in question
- *Who?* i.e. who's data and who is requesting/using/providing it
- *Where?* i.e. where the data is coming from, where it will be stored and where is it going
- *Why?* i.e. for what purpose is the data being requested/used/shared?
- *When?* i.e. over what temporal duration is the data being requested/used/shared?
- *How?* i.e. how is this being done, by what means and technologies

PLASMA - Policy LAnguage for Solid's Metadata-based Access control



`Log`: A provenance record associated with a process.

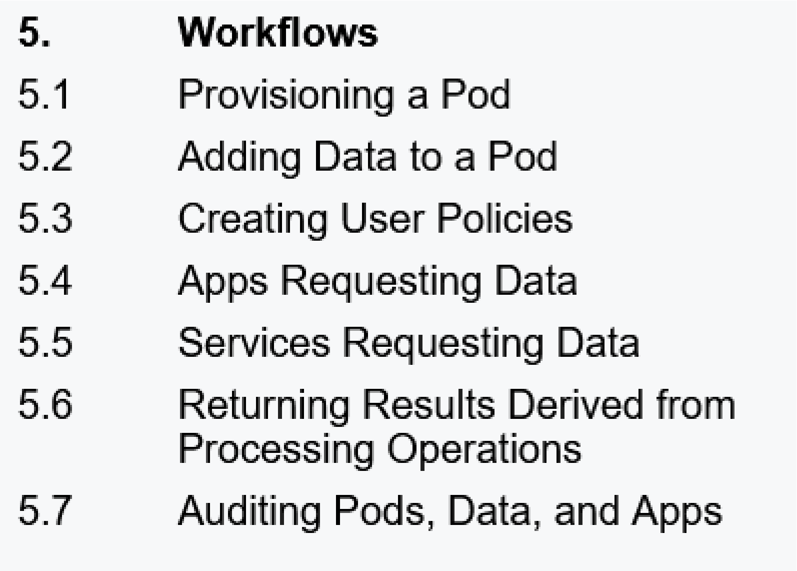
- `DataLog`: A `Log` regarding actions on `Data`. For example, when data was added / stored in the Pod, when it was erased, accessed, or queried.
- `AccessControlLog`: A `Log` regarding access actions on `Data`. For example, when data was permitted or denied to be accessed.
- `PolicyLog`: A `Log` regarding `Policies` governing the `Data`. For example, a new user preference or requirement was added, or an app made a request, or a policy negotiation succefully took place and the user granted their consent.
- `IdentityLog`: A `Log` regarding identity provision, verification, and its use. For example, an app's identity could not be verified, or a user succeffully logged in.
- `SecurityLog`: A `Log` regarding security concerns and incidents. For example, data integrity has failed a check, or there was an attempt to repeatedly access data without sufficient authorisation.



```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX dct: <http://purl.org/dc/terms/>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX dpv: <https://w3id.org/dpv#>
PREFIX as: <https://www.w3.org/ns/activitystreams#>
PREFIX plasma: <https://w3id.org/plasma#>
PREFIX ex: <https://example.com/>

ex:Logs a plasma:Log ;
    dpv:hasStorage <https://solidweb.me/besteves4/logs/dataLog.ttl> ;
    dct:issued "2022-11-08T18:13:37"^^xsd:dateTime ;
    plasma:hasLogs ex:logA, ex:logB .

ex:logA a plasma:DataLog, as:Create ;
    dct:issued "2022-12-08T18:13:37"^^xsd:dateTime ;
    as:actor <https://solidweb.me/besteves4/profile/card#me> ;
    as:summary "Beatriz added a new resource to the Pod" ;
    as:object <https://solidweb.me/besteves4/health/fitnessTracker.ttl> .

ex:logA a plasma:DataLog, as:Update ;
    dct:issued "2022-12-15T18:13:37"^^xsd:dateTime ;
    as:actor <https://solidweb.me/besteves4/profile/card#me> ;
    as:summary "Beatriz updates a resource" ;
    as:object <https://solidweb.me/besteves4/health/fitnessTracker.ttl> .
```

PLASMA logs

PLASMA



5. Workflows

5.1 Provisioning a Pod

5.2 Adding Data to a Pod

5.3 Creating User Policies

5.4 Apps Requesting Data

5.5 Services Requesting Data

5.6 Returning Results Derived from Processing Operations

5.7 Auditing Pods, Data, and Apps

Conclusions & Future Work

- Have different template policies for different use cases
  - The Pod can be created with a predefined set of policies according to the data that is going to be stored
- RDF surfaces as a new component to validate the policies being added to the Pod and to do the matching between user preferences and data requests
- App profile that makes clear the apps needs in relation to the data that is being accessed, the purpose, and so on.
- Logging, logging, logging, …

cost
EUROPEAN COOPERATION
IN SCIENCE & TECHNOLOGY

Protect

Policies in Solid: The Road Ahead

Beatriz Esteves, Ontology Engineering Group, Universidad Politécnica de Madrid
beatriz.gesteves@upm.es | besteves4@eupolicy.social

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 813497.