Protect

Using Patterns to Manage Governance of Solid Apps

Beatriz Esteves, Harshvardhan J. Pandit
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.

Outline

M Motivation & Challenges to the Solid Vision

B Background & Related Work

- Machine-readable Policies and Auditing Metadata in Solid
- Alignment of Solid with Data Protection Requirements

P PLASMA: A Metadata Language for Solid

- Entities
- Infrastructure
- Pod-related Data
- Policies

I Integrating PLASMA in the Solid Ecosystem through the Usage of Ontology Design Patterns

L Conformance and Legal Compliance

C Conclusions and Future Work

Using Patterns to Manage Governance of Solid Apps

Beatriz Esteves[1,*], Harshvardhan J. Pandit[2]

[1]Ontology Engineering Group, Universidad Politécnica de Madrid, Spain
[2]ADAPT Centre, Dublin City University, Ireland

Abstract
Currently, the Solid Protocol and its specifications lack the necessary vocabulary and processes for ensuring transparency and accountability in the use of data. In particular, to deal with the obligations and requirements required by regulations related to (personal) data protection and privacy. In addition, the lack of a guiding vocabulary leads to no common mechanism through which apps can request data and how Solid maintains information about its use. To address these, we propose PLASMA – a policy language to describe the entities, infrastructure, legal roles, policies, notices, and records to understand and establish responsibilities and accountability within the Solid ecosystem. We present how ontology design patterns using PLASMA can provide a common interface to create structured policies, records, and logs within the diverse Solid use cases, and thereby solve challenges regarding the management and governance of apps and their privacy considerations.

Keywords
Solid, access control, policies, GDPR, regulatory compliance, ontology design patterns

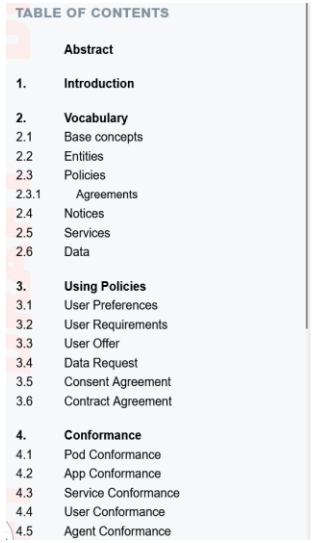
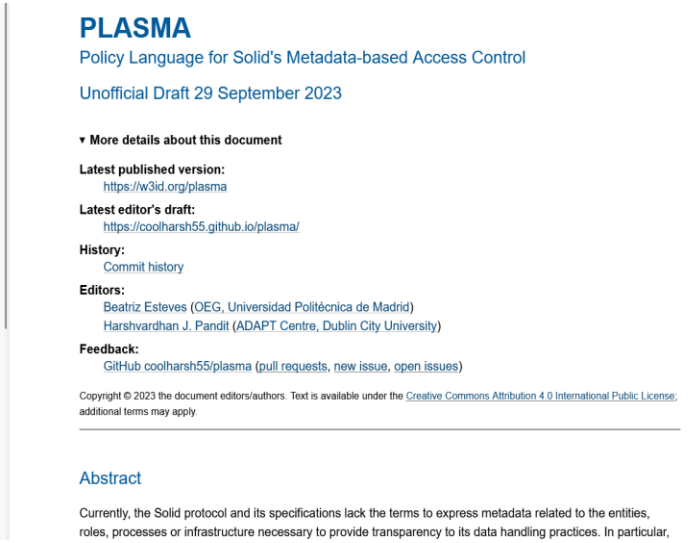


TABLE OF CONTENTS


PLASMA
Policy Language for Solid's Metadata-based Access Control
Unofficial Draft 29 September 2023

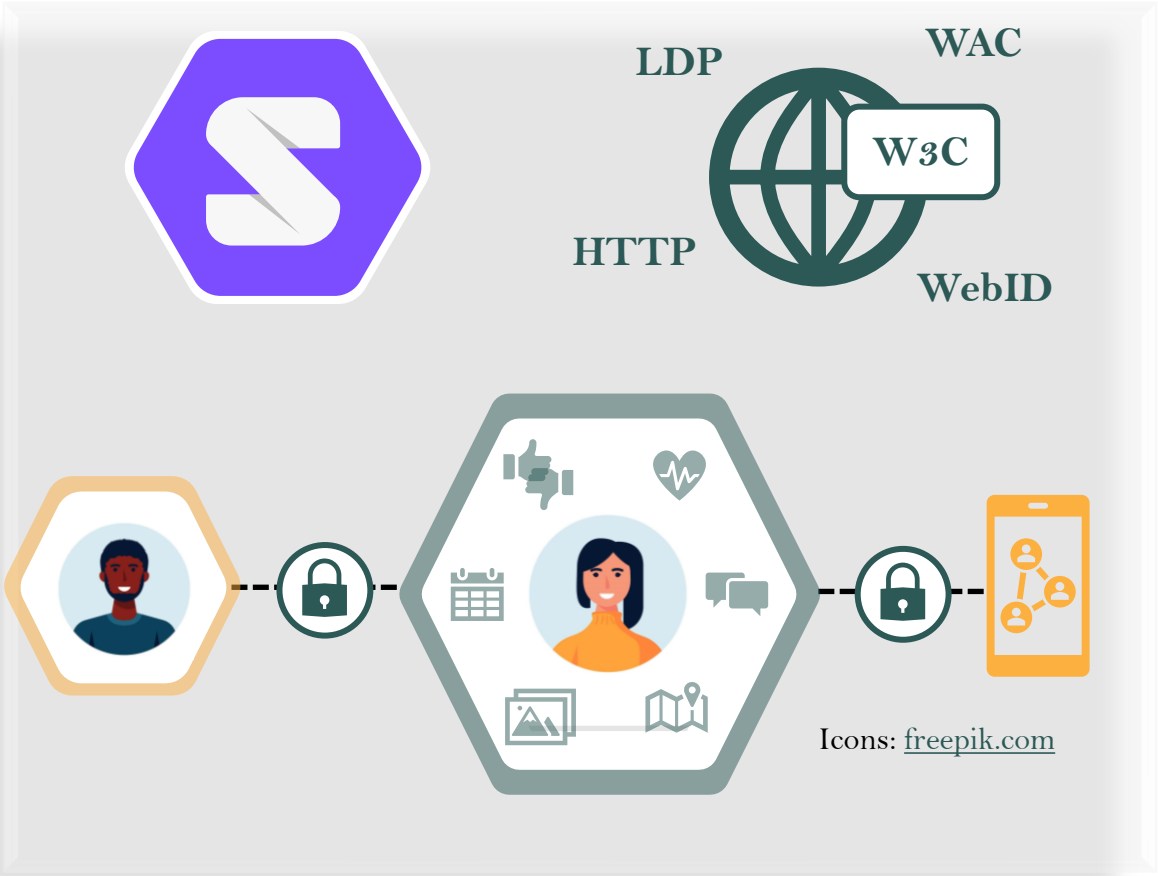
▾ More details about this document

Latest published version:
https://w3id.org/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, Dublin City University)
Feedback:
GitHub coolharsh55/plasma (pull requests, new issue, open issues)

Abstract

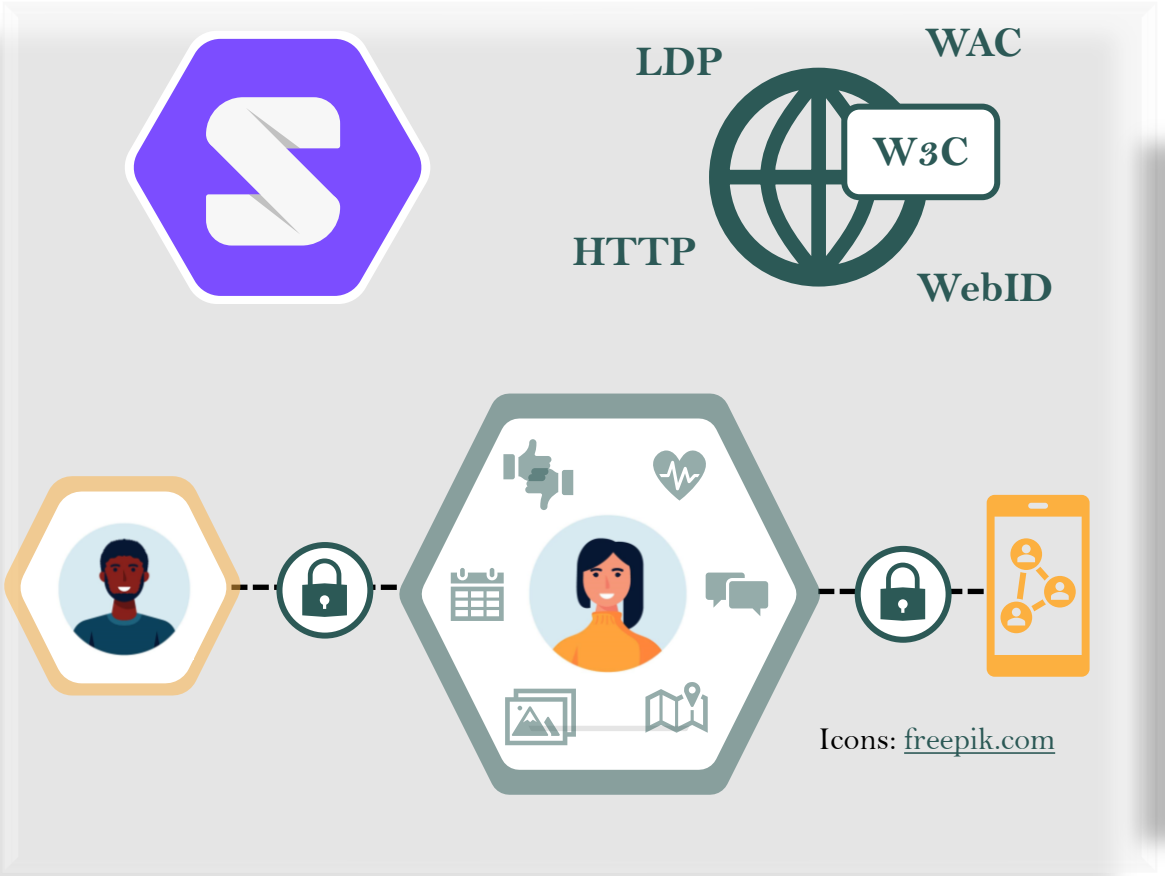
Currently, the Solid protocol and its specifications lack the terms to express metadata related to the entities, roles, processes or infrastructure necessary to provide transparency to its data handling practices. In particular,

Motivation

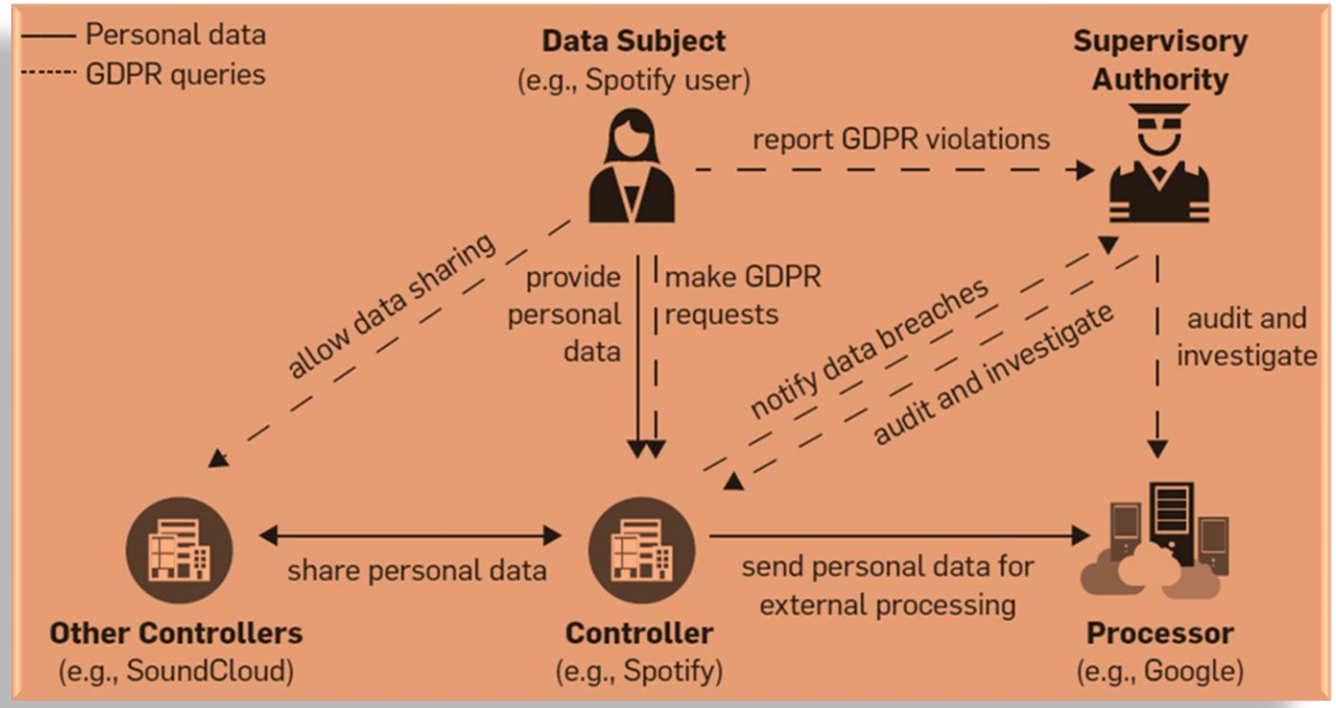


Solid is a specification for decentralised data stores based on interoperable data formats and protocols

Motivation



Solid is a specification for decentralised data stores based on interoperable data formats and protocols

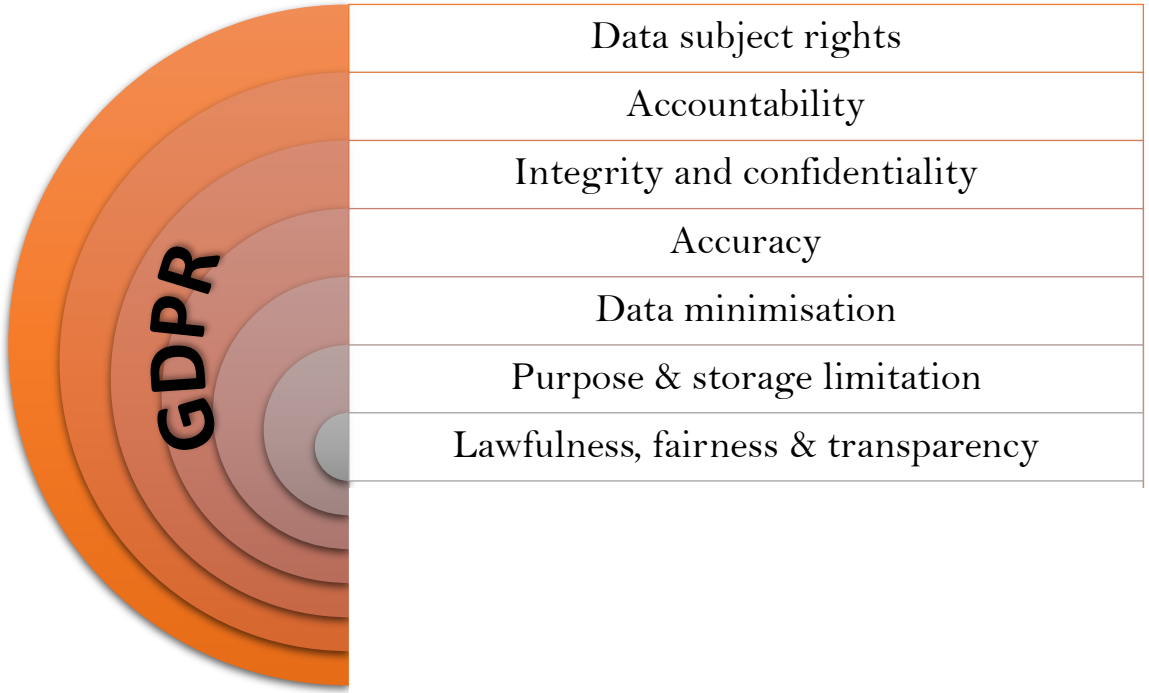


Shastri, S., Wasserman, M., Chidambaram, V. (2021). *GDPR Anti-Patterns.* Communications of the ACM Vol. 64 No. 2 (pp. 59-65). https://doi.org/10.1145/3378061

Challenges to the Solid Vision

"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."

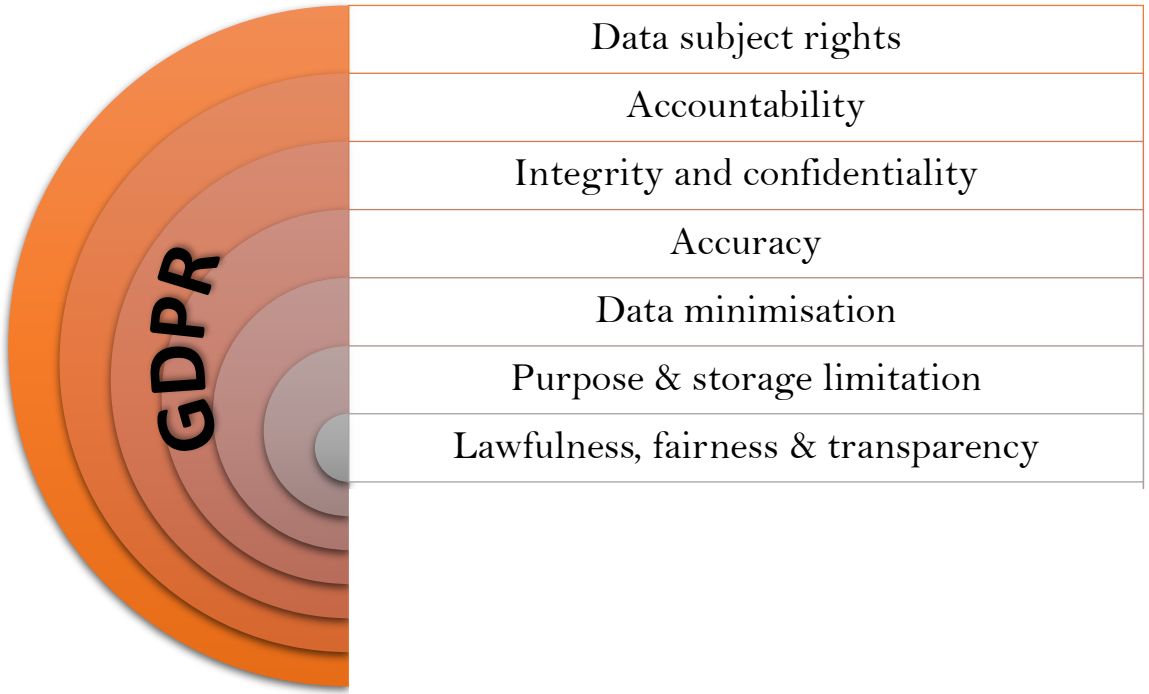
EDPS TechDispatch #3/2020 – PIMS [Source]



Challenges to the Solid Vision

"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 [Source]



What is missing from Solid?

No records of agreements for the provision of services

Lack of tools to give / withdraw consent

No metadata about Solid infrastructure

No information on the identity and contacts of Solid providers

Lack of tools to get available categories of data

Record keeping and log maintenance are nonexistent

Lack of tools to rectify data inaccuracies

Difficulty for users to set (granular) access to resources

Access grants valid in perpetuity

Data requests miss a purpose

Compatibility of purposes cannot be checked

Consent dialogue not enough for informed decision

Access grants not sufficient to be a valid record of consent

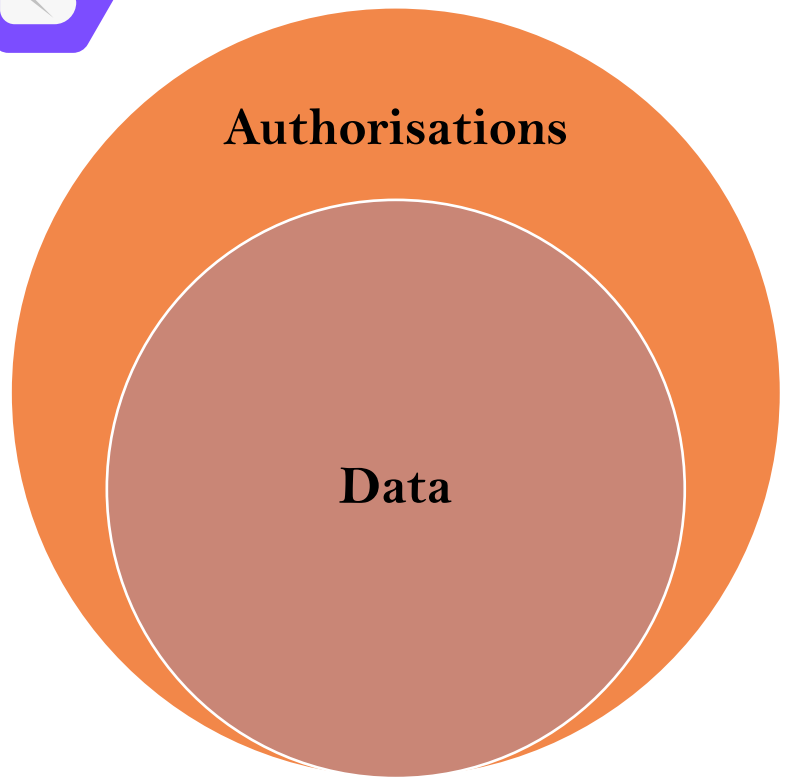
Research Objectives

RO1. Creating a taxonomy of Solid's entities and infrastructure to describe the actors and processes involved in the Solid ecosystem;

RO2. Providing a metadata policy language (PLASMA), using the terms identified in RO1, to express information regarding legal roles and other compliance requirements in a jurisdiction-agnostic manner (while satisfying requirements from GDPR);

RO3. Using PLASMA for defining a set of Solid-related ODPs regarding users and apps policies, data use logs, and registries to provide easy access to data in Pods.

B Background – Giving Access to Data in Solid



Solid's authorisation mechanism currently relies on two access control languages – WAC and ACP

WAC – Web Access Control

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

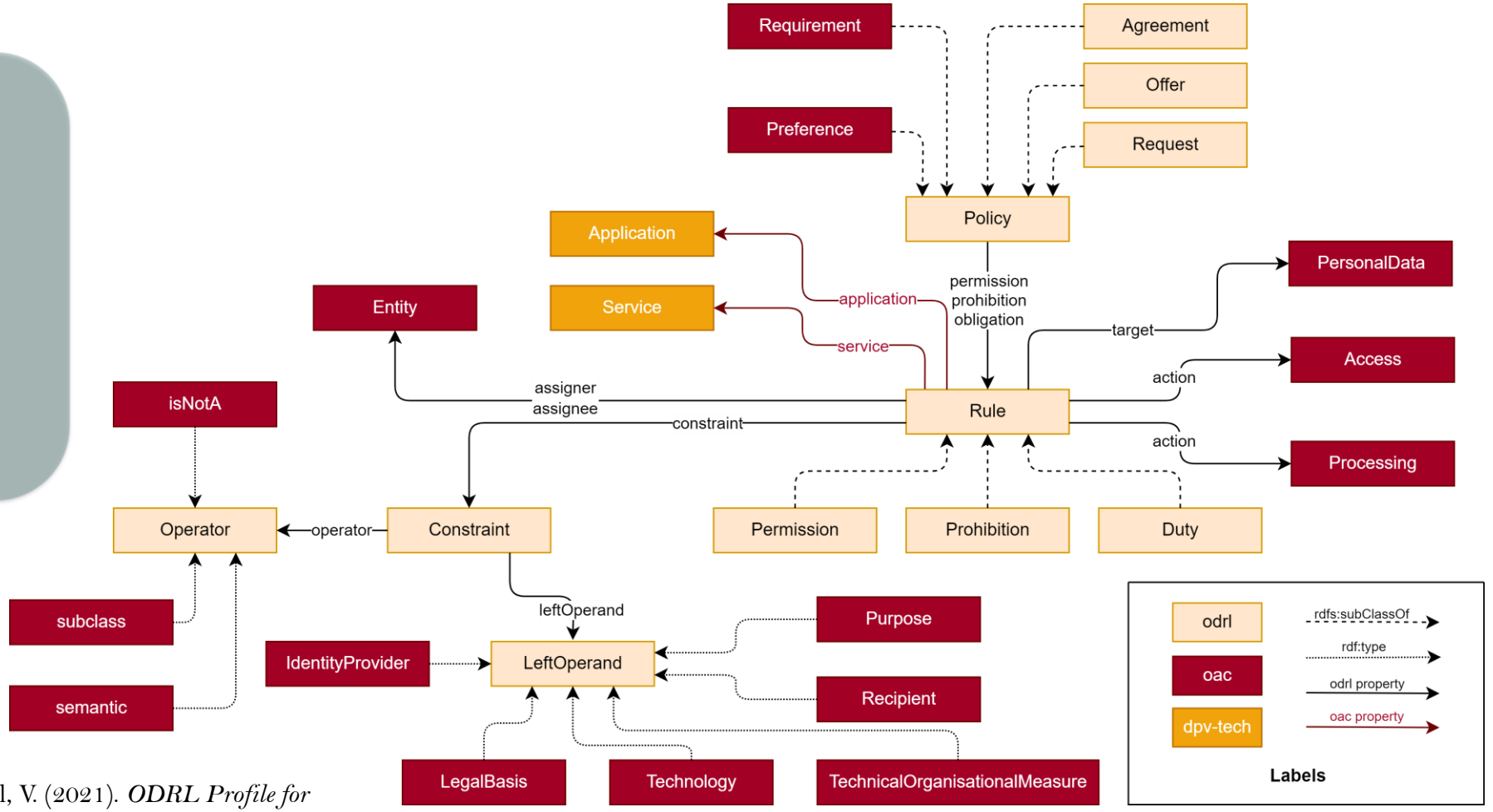
ACP – Access Control Policy

```
<#grant1> a acp:AccessGrant ;
 acp:grant acl:Read, acl:Write ;
 acp:context [
  acp:agent <https://beatriz.providerZ.com/profile/card#me> ;
  acp:issuer <https://identityProviderZ.com> ;
  acp:target <https://victor.providerY.com/docs/file1.ttl> ;
  acp:client <https://clientApplicationA.com>
 ] .
```

B Related Work – ODRL profile for Access Control (OAC)

Collection of ODRL policies

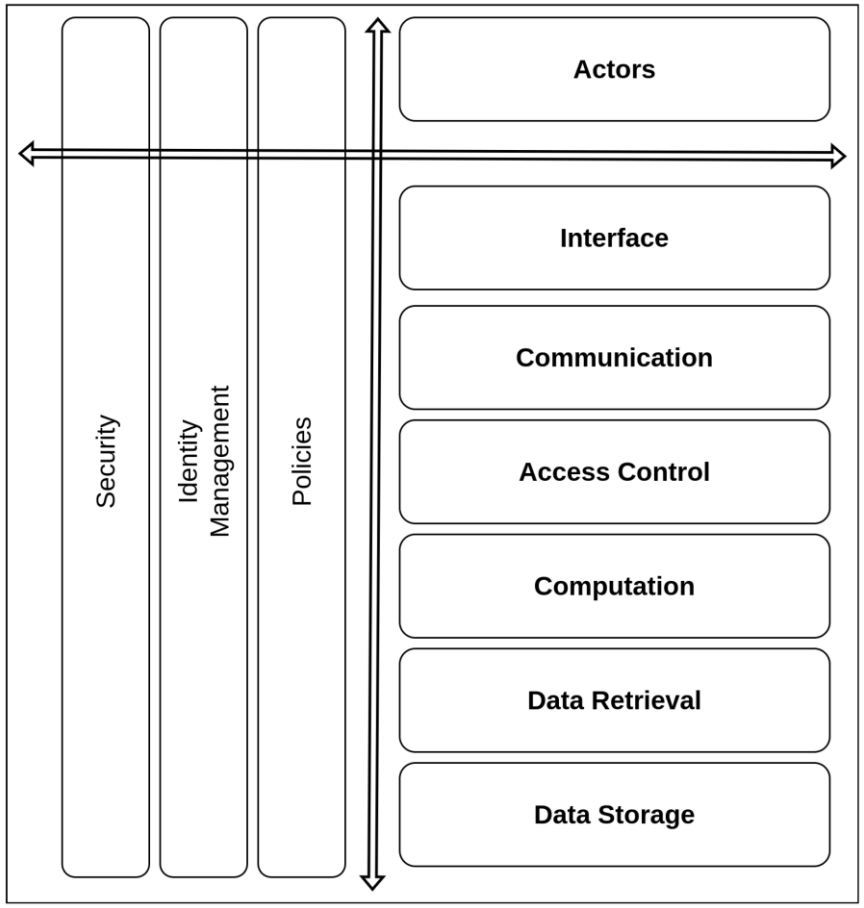
https://github.com/besteves4/oac-policies



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 S&P Workshops (pp. 298-306). https://ieeexplore.ieee.org/abstract/document/9583717

https://w3id.org/oac

B Related Work – Alignment of Solid with Data Protection Requirements

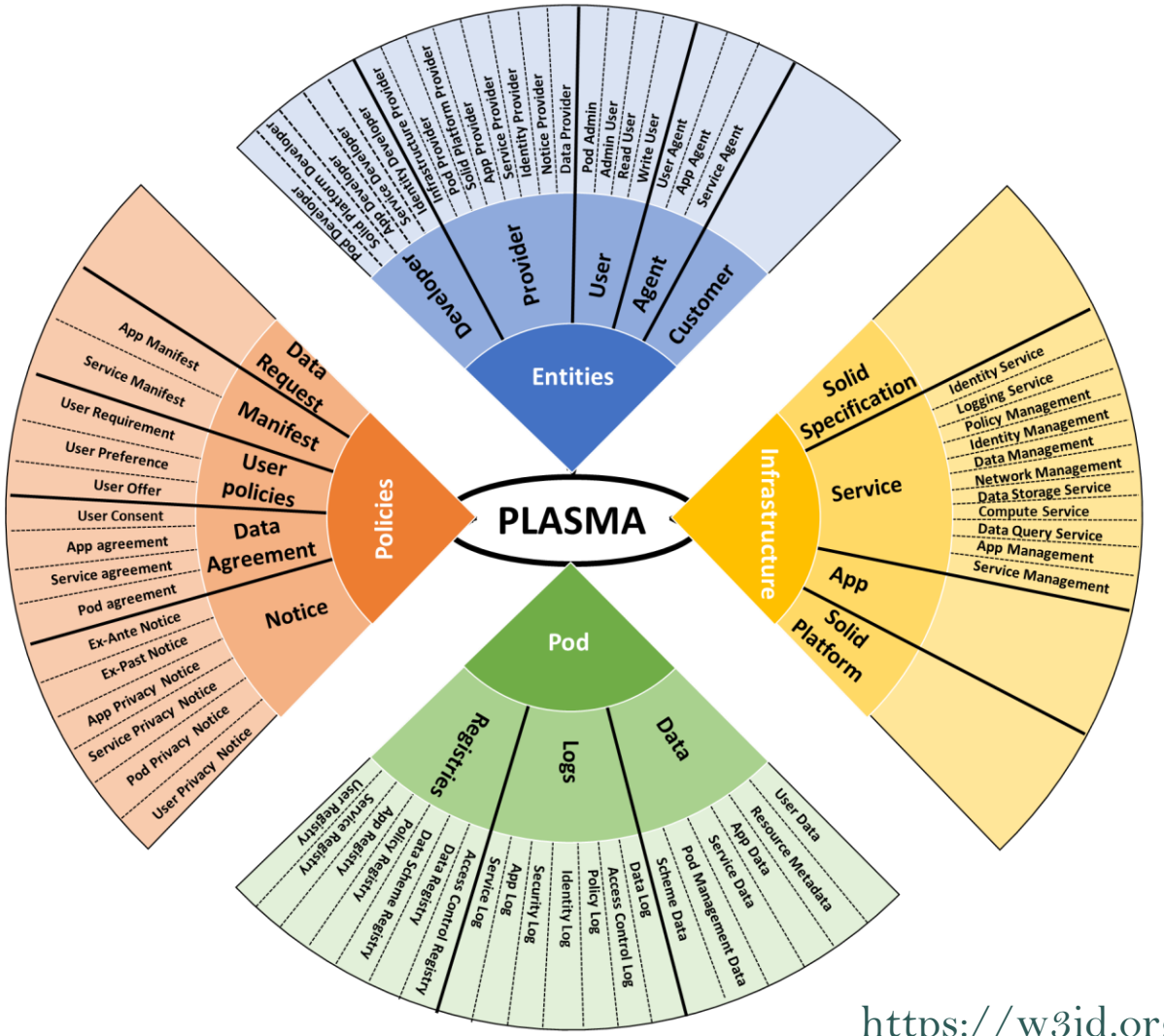


Pandit, H. J. (2023). *Making Sense of Solid for Data Governance and GDPR*. Information 14(2), 114. https://doi.org/10.3390/info14020114

GDPR Articles	Obligations	Controller	Processor
Art 5	Comply with fundamental data protection principles	+	+ (according to controller instructions)
Art 13 &14 Art 15 – 22	Comply with information obligations and data subjects' requests to exercise their rights	+	
Art 25	Implement data protection by design and by default	+	
Art 30	Keep records of processing activities	+	+
Art 32	Implement appropriate technical and organisational measures	+	+
Art 33, 34	Comply with the personal data breach notification obligations	+	+ (Art 33 only)

Janssen, H., Cobbe, J., Norval, C., Sing, J. (2020). *Decentralized data processing: personal datastores and the GDPR*. International Data Privacy Law 10(4) (pp. 356-384). https://doi.org/10.1093/idpl/ipaa016

PLASMA: a 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:

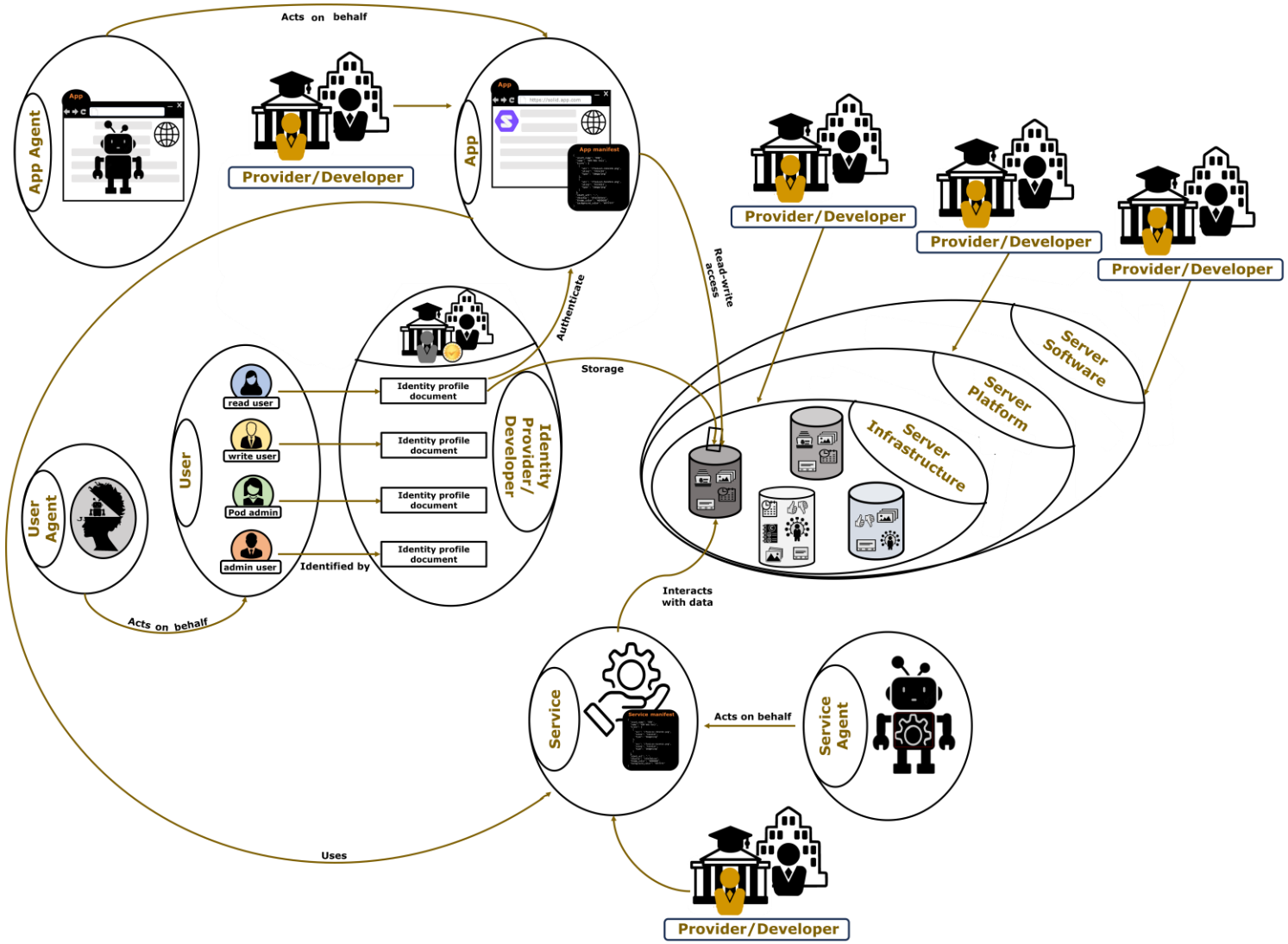
- *What?* i.e. the data in question
- *Who?* i.e. who's data and who is requesting/using/providing it
- *Where?* i.e. where the data is coming from, where it will be stored and where is it going
- *Why?* i.e. for what purpose is the data being requested/used/shared?
- *When?* i.e. over what temporal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

https://w3id.org/plasma

```
<https://example.com/DataRequest> a plasma:DataRequest, odrl:Request ;
    odrl:profile oac: ;
    odrl:uid <https://example.com/DataRequest> ;
    dcterms:description "Request to erase temporary data from the Pod." ;
    dcterms:creator <https://example.com/ServiceDeveloper_EntityA> ;
    dcterms:issued "2023-10-24T22:13:14"^^xsd:dateTime ;
    odrl:permission [
        odrl:assignee <https://example.com/ServiceDeveloper_EntityA> ;
        odrl:action oac:Erase ;
        odrl:target plasma:AppPersistentData, plasma:ServiceTemporaryData ;
        odrl:constraint [
            dcterms:title "Purpose for access is to clean temporary data that
             ↪ is no longer needed." ;
            odrl:leftOperand oac:Purpose ;
            odrl:operator odrl:eq ;
            odrl:rightOperand <https://example.com/CleanTemporaryData> ] ] .

<https://example.com/ServiceDeveloper_EntityA> a plasma:ServiceDeveloper .
```

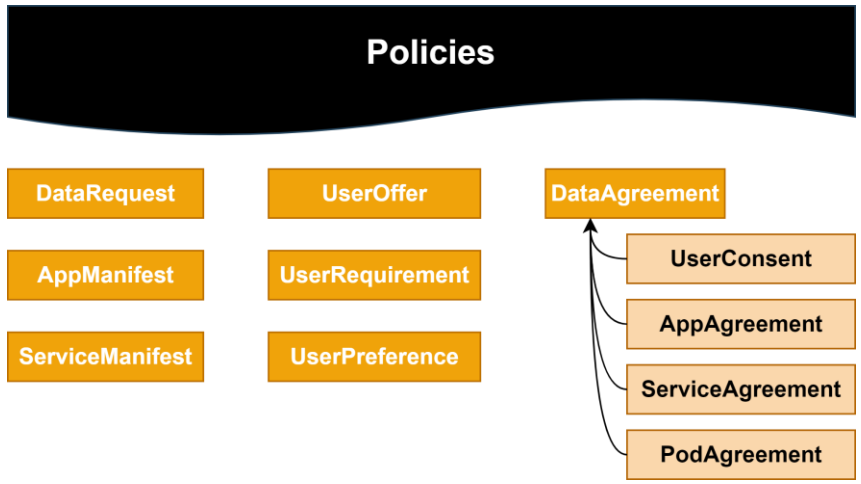
PLASMA – Entities & Infrastructure

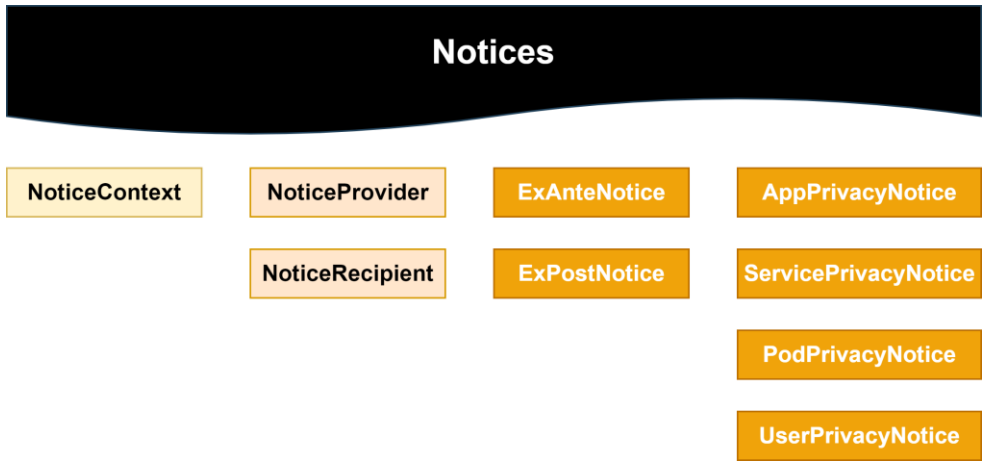


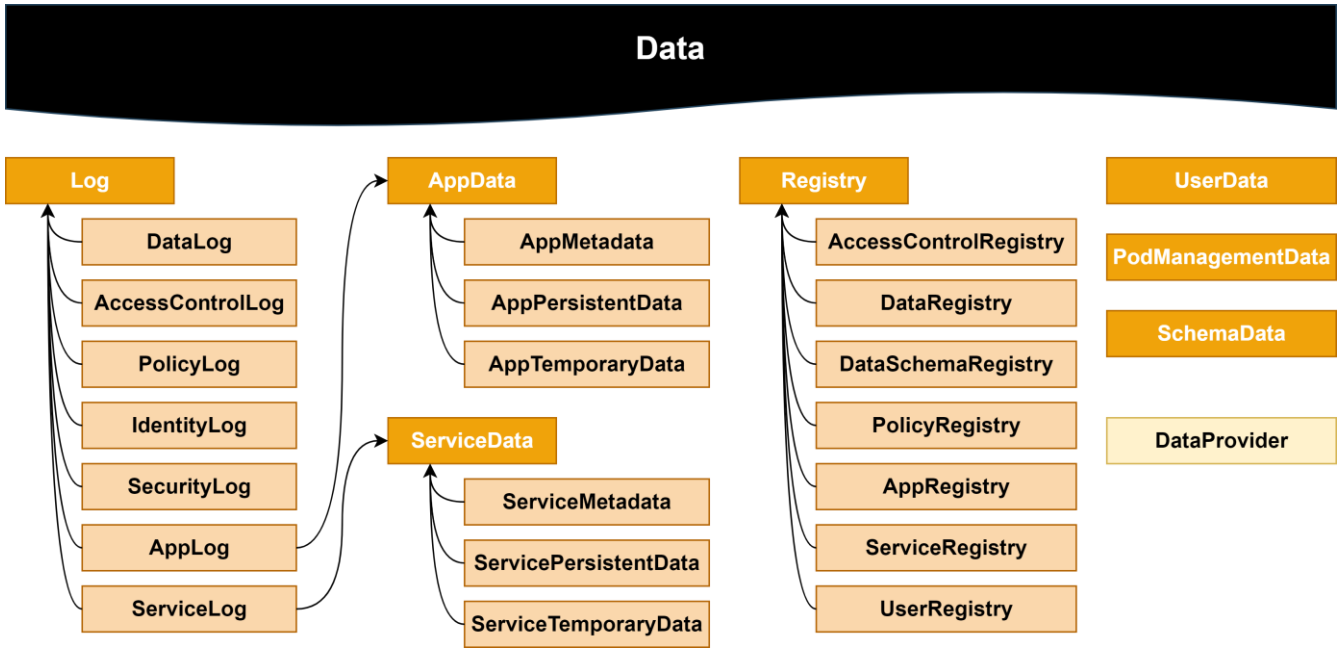
Services

- IdentityService
- PolicyManagementService
- LoggingService
- IdentityManagementService
- ComputeService
- NetworkManagementService
- DataQueryService
- DataManagementService
- ServiceManagement
- AccessControlService
- DataStorageService
- AppManagementService

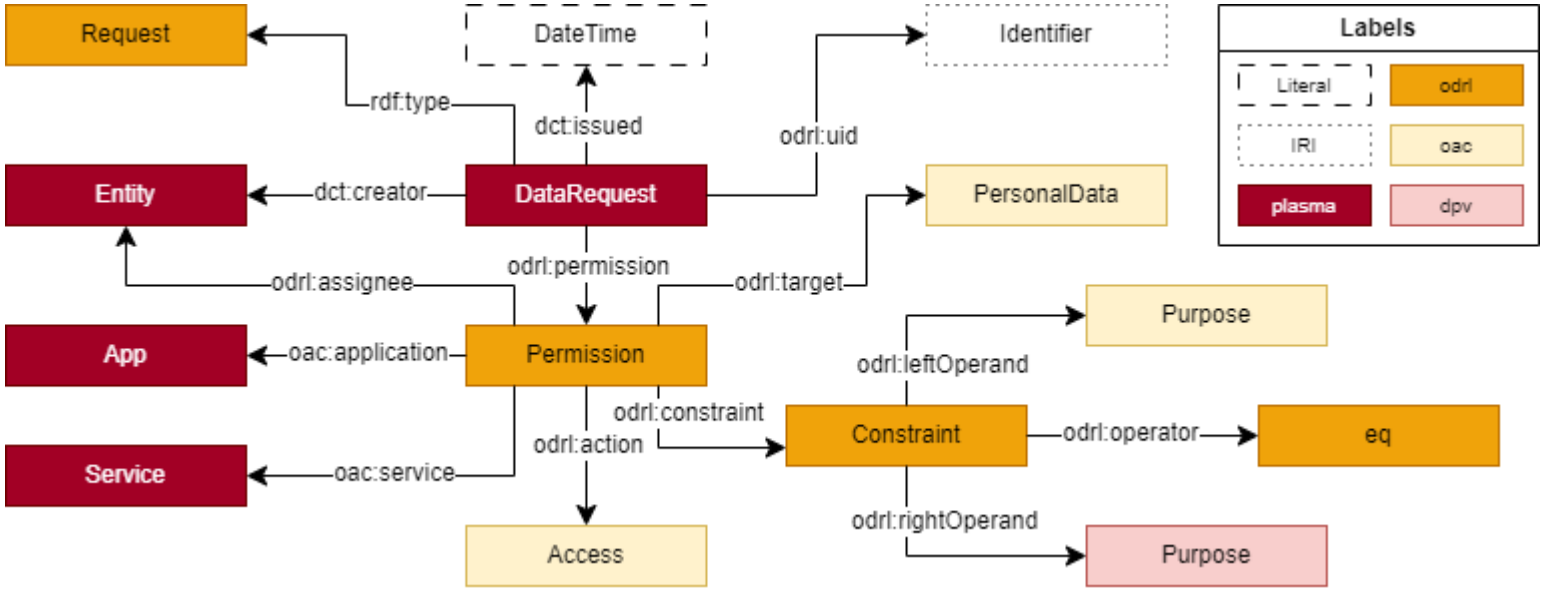
PLASMA – Policies, Notices & Data







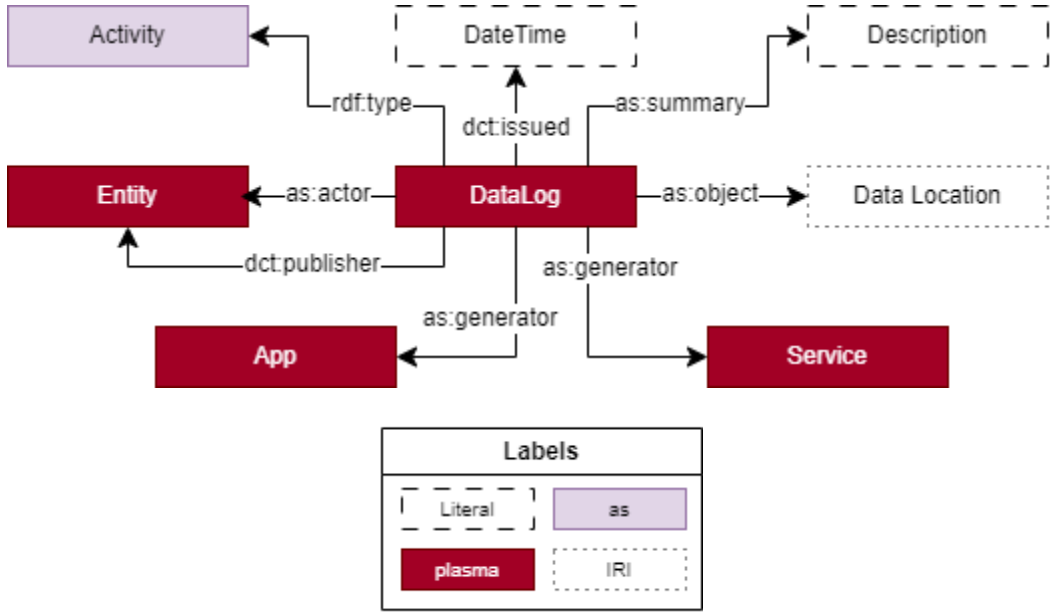
I Integrating PLASMA in the Solid Ecosystem through the Usage of ODPs



(CQP1.) What is the unique identifier of the policy?
(CQP2.) Who is the creator of the policy?
(CQP3.) When was the policy issued?
(CQP4.) Who is the assignee of the policy?
(CQP5.) What application/service is being used to access the data?
(CQP6.) What access mode is being requested?
(CQP7.) What personal data is being accessed?
(CQP8.) What is the purpose for accessing the data?

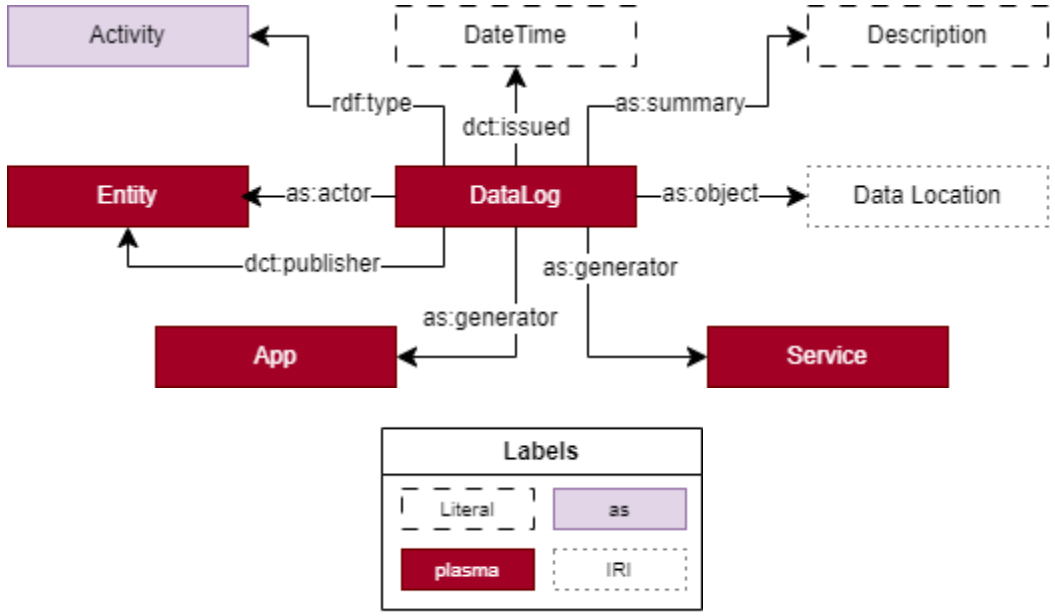
I Integrating PLASMA in the Solid Ecosystem through the Usage of ODPs

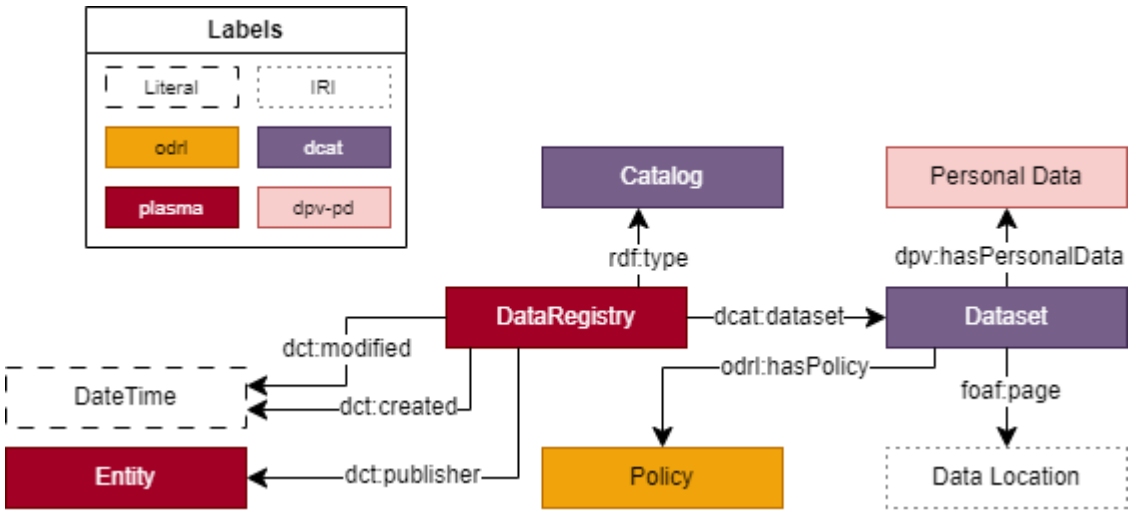
(CQL1.) What type of action, e.g., create, update, erase, is being performed on the data?
(CQL2.) Who is the entity interacting with the data?
(CQL3.) Who is the entity publishing the log?
(CQL4.) When was the log issued?
(CQL5.) Where is the data being stored?
(CQL6.) What application/service is being used to generate the data, if any?



I Integrating PLASMA in the Solid Ecosystem through the Usage of ODPs

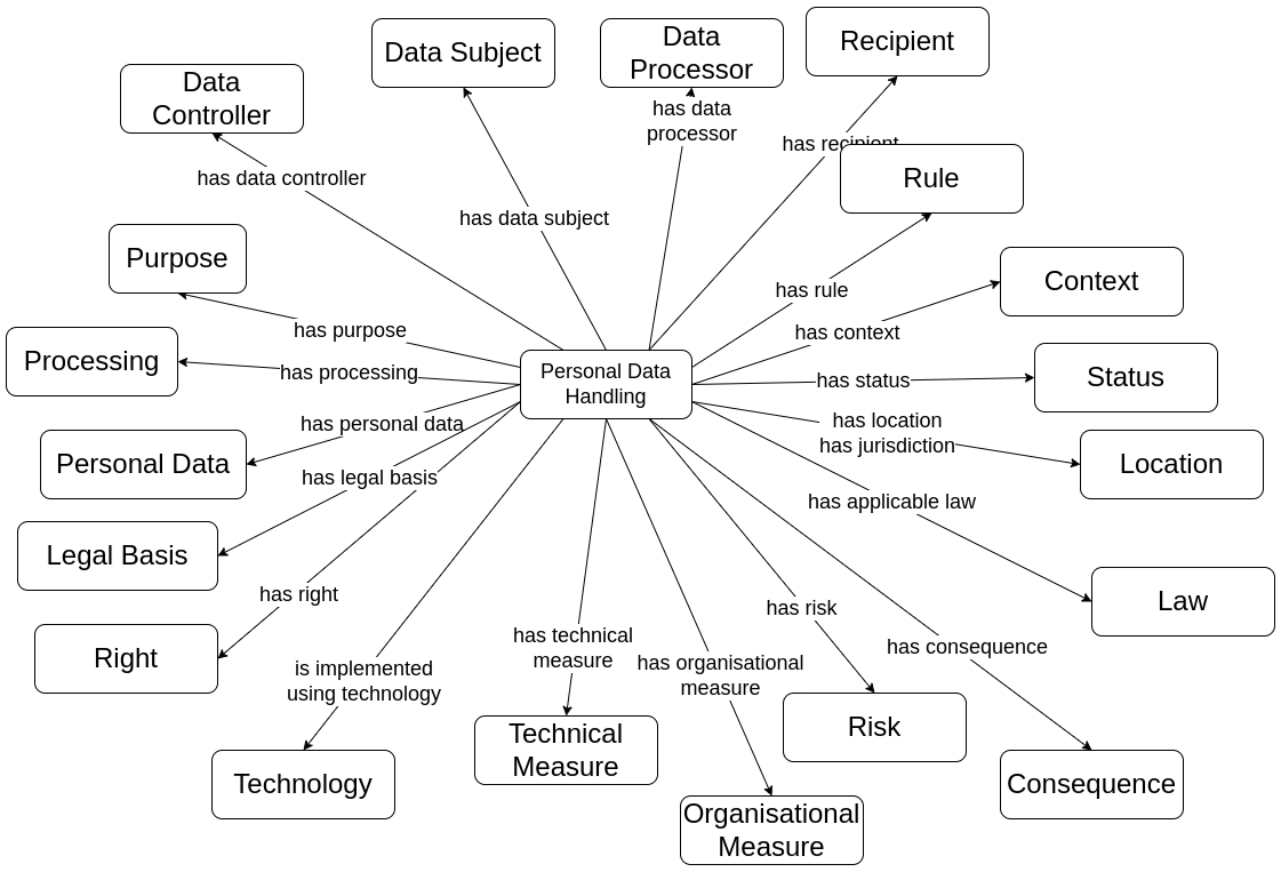
(CQL1.) What type of action, e.g., create, update, erase, is being performed on the data?
(CQL2.) Who is the entity interacting with the data?
(CQL3.) Who is the entity publishing the log?
(CQL4.) When was the log issued?
(CQL5.) Where is the data being stored?
(CQL6.) What application/service is being used to generate the data, if any?





(CQR1.) Who is maintaining the registry?
(CQR2.) When was the registry created/updated?
(CQR3.) What types of data are available?
(CQR4.) Where is a specific type of data being stored?
(CQR5.) What policy is associated with the data?

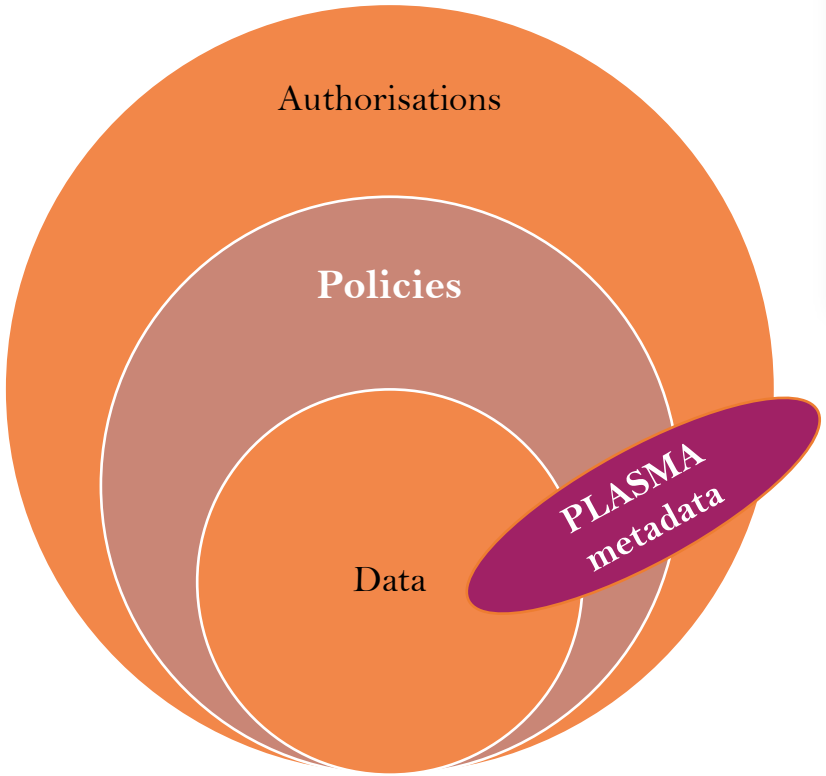
Conformance and Legal Compliance



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

- **DPV-GDPR** to model legal basis, rights and data transfer tools defined in the GDPR
- Extensions for new data-related regulations are being added (**DPV-DGA**)
- Guidance for the implementation of **ISO/IEC 29184 (Privacy Notices)** and **ISO/IEC 27560 (Consent Records)** using DPV concepts to be provided soon by DPVCG
- Contract-related terms from the **smashHit project** to be integrated soon into DPV

Conclusions



The usage of ODPs will ensure that the appropriate information based on legal requirements, e.g., from GDPR's Article 13/14, is present in the Pods to be consulted. As such, the **creation of patterns** for the different types of policies, notices, logs, and registries is of the **utmost importance**.

- Record policies used to authorise access.
- Keep information about the developers and/or providers of Pods, apps, services, data, identity, infrastructure, …
- Keep activity logs regarding important Solid processes, e.g., updating a resource, moving to a different Pod provider, or deleting a given access authorization from the Pod.
- Maintain registries (of policies, users, apps, data, …) for convenient access to data and metadata within a Pod.

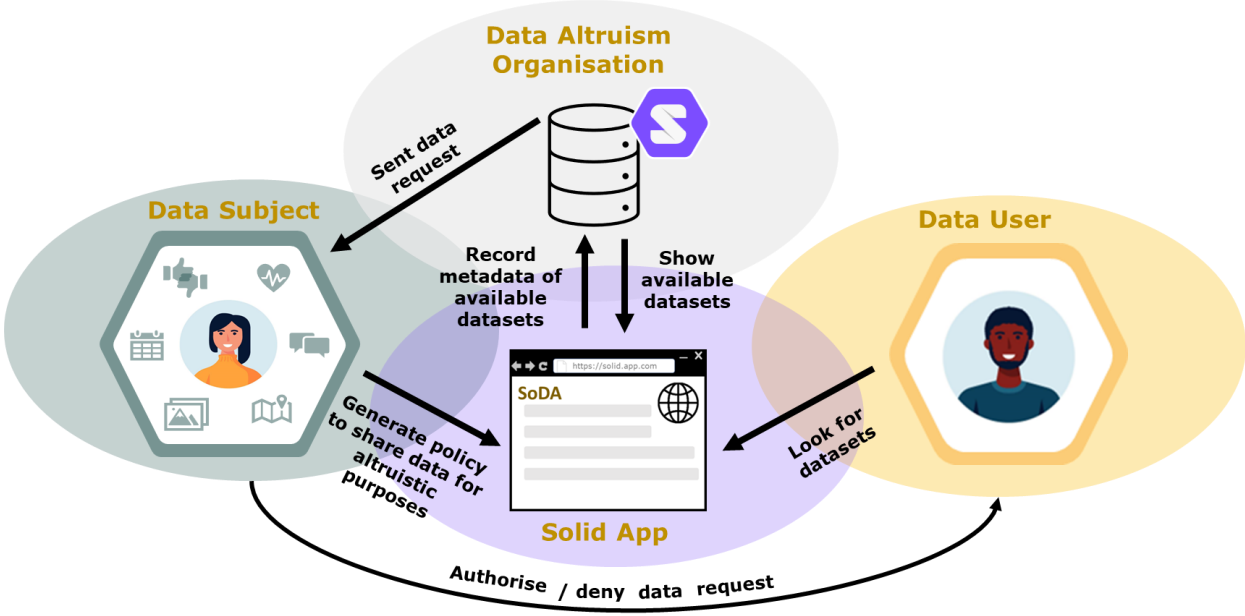
C Future Work

i. Evaluate the coverage of PLASMA to deal with a variety of different workflows.

ii. Integrate the usage of PLASMA, and of ODRL and DPV as well, into the design of Solid servers, applications, and services.

iii. Develop SHACL shapes to check for compliance with the PLASMA specification, including the usage of DPV to comply with legal requirements, e.g., in GDPR.

iv. Support new data-related regulations (Data Governance Act, Data Act, Health Data Spaces, …) requirements.



Towards an Architecture for Data Altruism in Solid

Demo D7

Check out the demo!

Protect

Using Patterns to Manage Governance of Solid Apps

Beatriz Esteves, Harshvardhan J. Pandit
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.