Protect

Automating the response to GDPR's Right of Access

Beatriz Esteves, Víctor Rodríguez-Doncel, Ricardo Longares
Ontology Engineering Group, Universidad Politécnica de Madrid, Spain

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.

Overview

Motivation

GDPR's Right of Access

Related Work

Methodology

API Development

Exercising the Right of Access in Solid

Conclusions and Future Work

Automating the response to GDPR's Right of Access

Beatriz ESTEVES [a,1], Víctor RODRÍGUEZ-DONCEL [a], Ricardo LONGARES [a]

[a] *Ontology Engineering Group, Universidad Politécnica de Madrid, Spain*

Abstract.
With the enforcement of the European Union's General Data Protection Regulation, users of Web services – the 'data subjects' –, which are powered by the intensive usage of personal data, have seen their rights be incremented, and the same can be said about the obligations imposed on the 'data controllers' responsible for these services. In particular, the 'Right of Access', which gives users the option to obtain a copy of their personal data as well as relevant details such as the categories of personal data being processed or the purposes and duration of said processing, is putting increasing pressure on controllers as their execution often requires a manual response effort, and the wait time is negatively affecting the data subjects. In this context, the main goal of this work is the development of an API, which builds on the previously mentioned structured information, to assist controllers in the automation of replies to right of access requests. The implemented API method is then used in the implementation of a Solid application whose main goal is to assist users in exercising their right of access to data stored in Solid Pods.

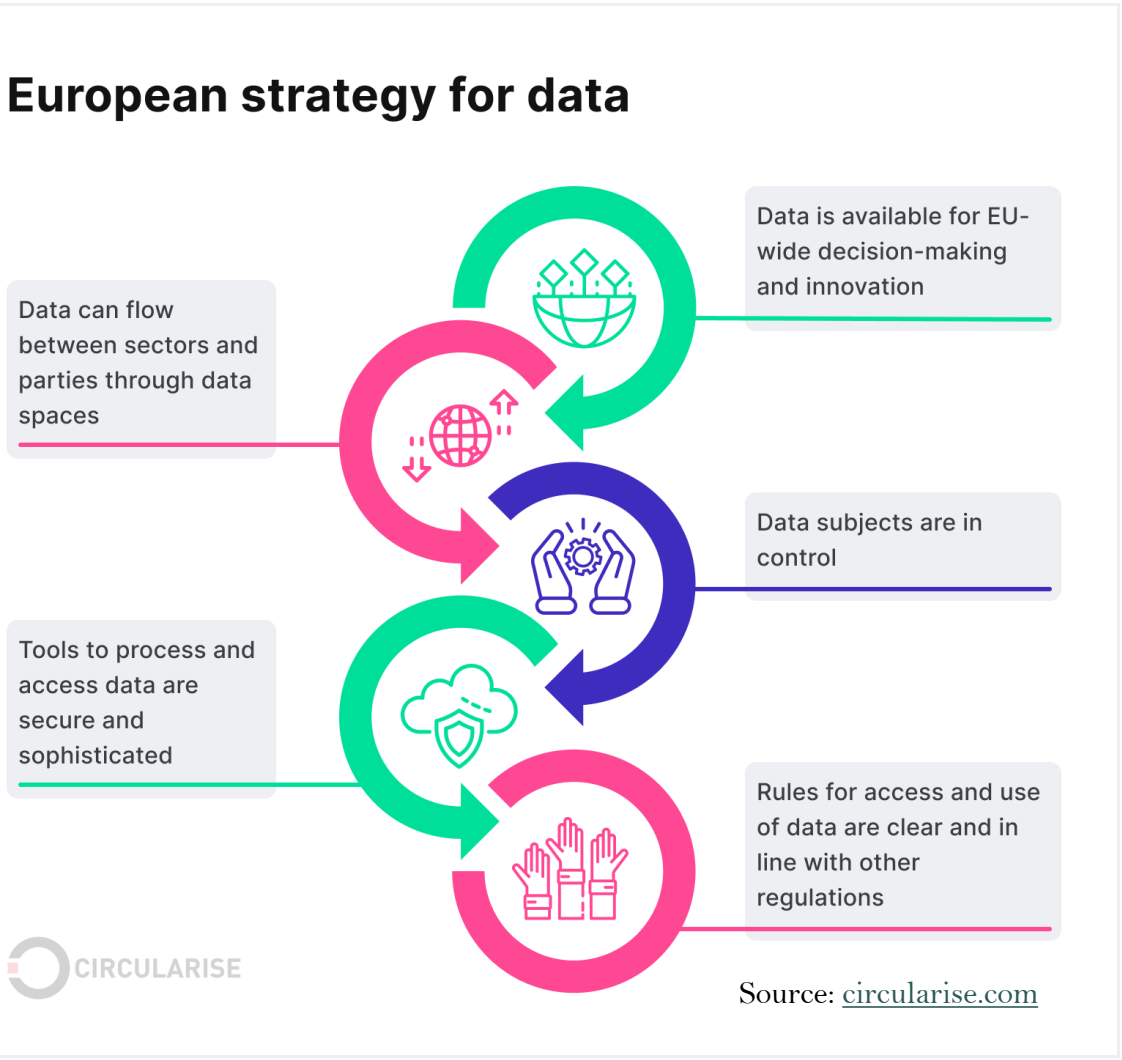
Keywords. digital rights management, GDPR, right of access, Solid

1. Introduction

With the enforcement of the European Union's General Data Protection Regulation (GDPR), users of Web services have seen their rights as GDPR 'data subjects' being expanded when it comes to the processing of their personal data. On the other hand, on top of other GDPR-related obligations, 'data controllers', the entities that effectively process the data, have seen an increase in workload related to the response to data subject's right-related requests. GDPR's Chapter III[2] details a set of 10 data subject rights, starting with the 'Right to be Informed' described in Articles 13 and 14 and ending with the 'Right to object to automated decision making' in Article 22. Considering this, data controllers would benefit from having the information they need to provide to data subjects in a structured format to automate the response to such requests [1]. In particular, the 'Right of

https://ebooks.iospress.nl/volumearticle/62049

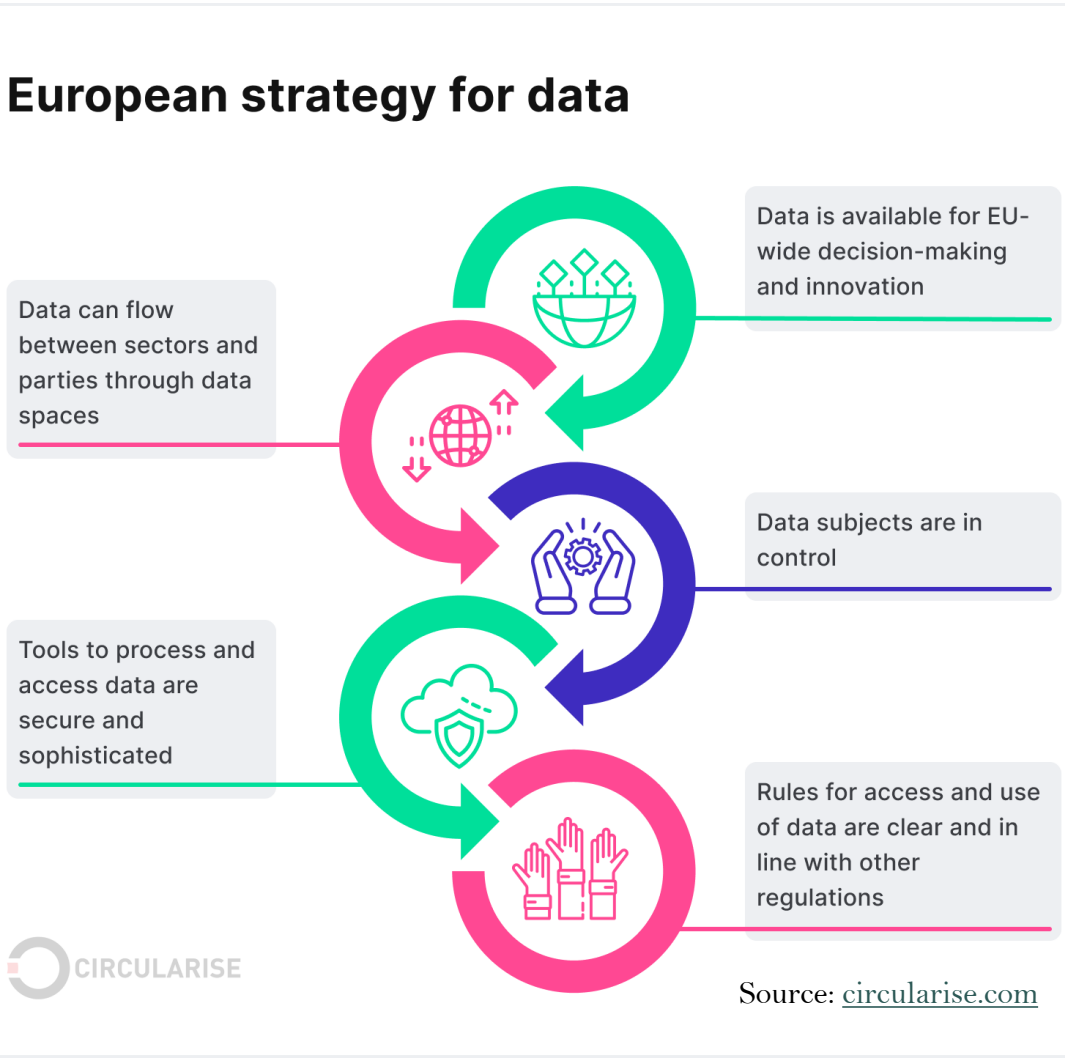
Motivation



Source: circularise.com

https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

Motivation

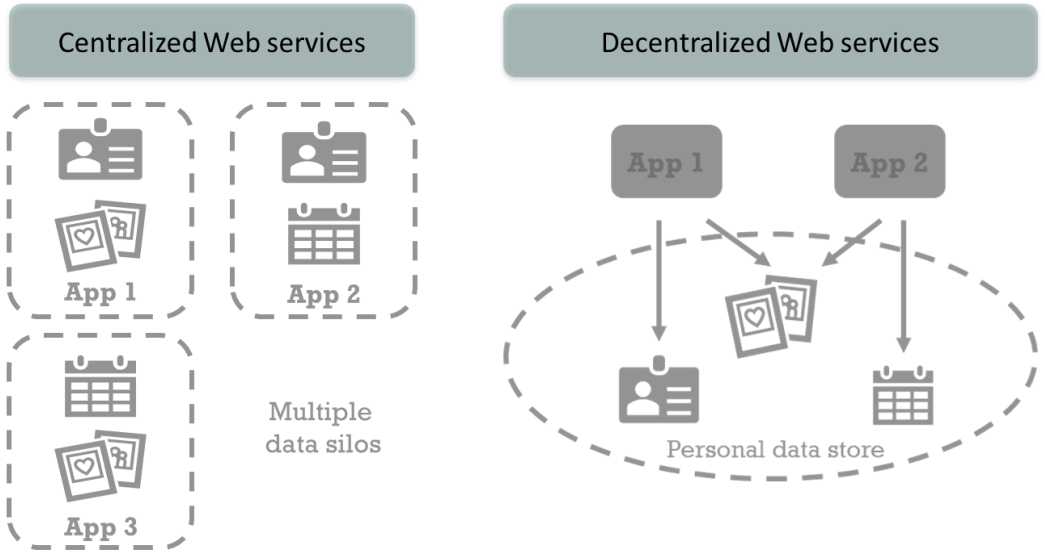


Source: circularise.com

https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

Personal Information Management Systems

https://edps.europa.eu/data-protection/our-work/subjects/personal-information-management-system_en



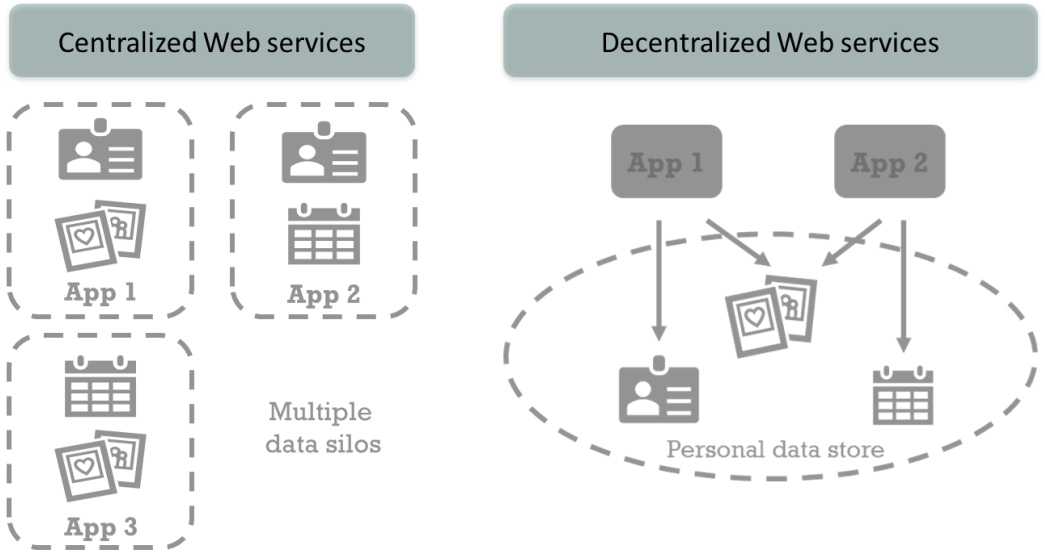
Motivation

Source: circularise.com

https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

Personal Information Management Systems

https://edps.europa.eu/data-protection/our-work/subjects/personal-information-management-system_en



Source: iconscout.com

GDPR's Right of Access

"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

GDPR's Right of Access

"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

Copy of the personal data

Purposes of the processing
Categories of personal data
Recipients
Storage duration
Data source
Other rights

GDPR's Right of Access

"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

RO1. Implementing an API method that automates the reply to an access right request, making use of RDF information.
RO2. Developing a Solid application which uses the implemented method to assist users in exercising their right of access in a decentralised storage environment, such as data stored in Solid Pods.

Copy of the personal data

Purposes of the processing
Categories of personal data
Recipients
Storage duration
Data source
Other rights

Related Work

Microsoft Graph compliance and privacy API

https://bit.ly/3DhPnCp

Oracle's Data Privacy API

https://bit.ly/3MPJFLn

AppsFlyer

https://bit.ly/3eSFphG

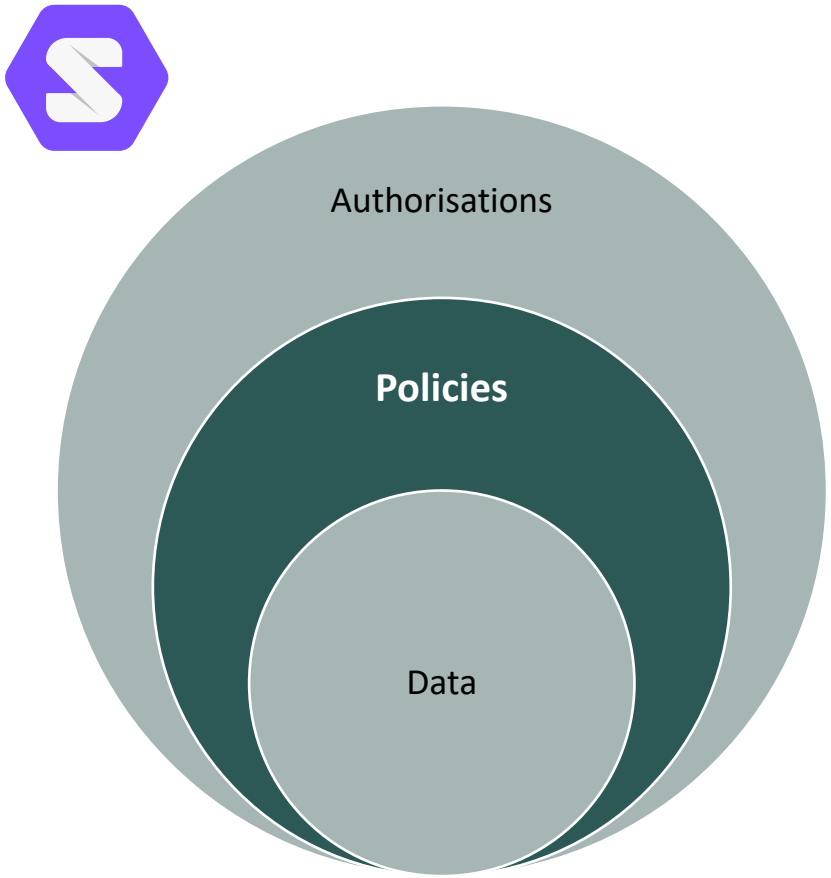
Gaps

- Solutions focus on providing a copy of the data and don't provide detailed information regarding purposes for processing, duration of the processing and so on.
- Some components require manual intervention
- "Fine-grained" access

Methodology

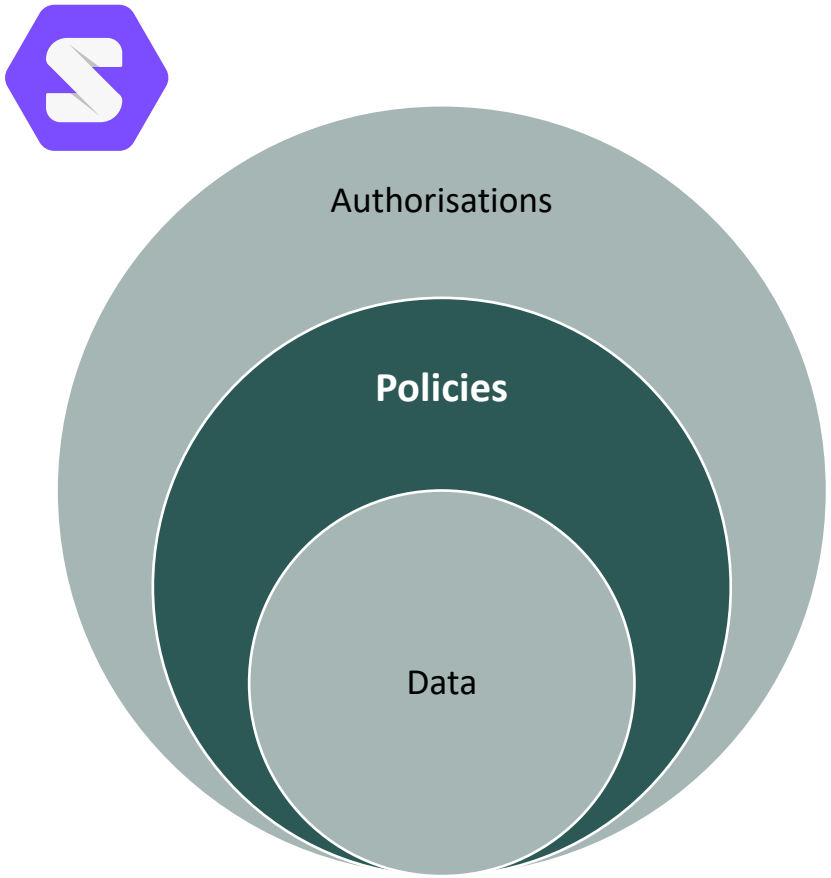
1. An evaluation of current gaps on the right of access APIs was performed.
2. Similar regulation from other jurisdictions was reviewed in order to understand if new requirements needed to be added into consideration.
3. Semantic Web vocabularies were used to tag the data in terms of the personal data they contain, to specify the policies that determine the access to said data and to store the consent record of an authorized access request.
4. The API method and documentation were developed.
5. Solid's personal data storage ecosystem was then chosen to verify the applicability of the API method as it is based on Web standards.

API Development



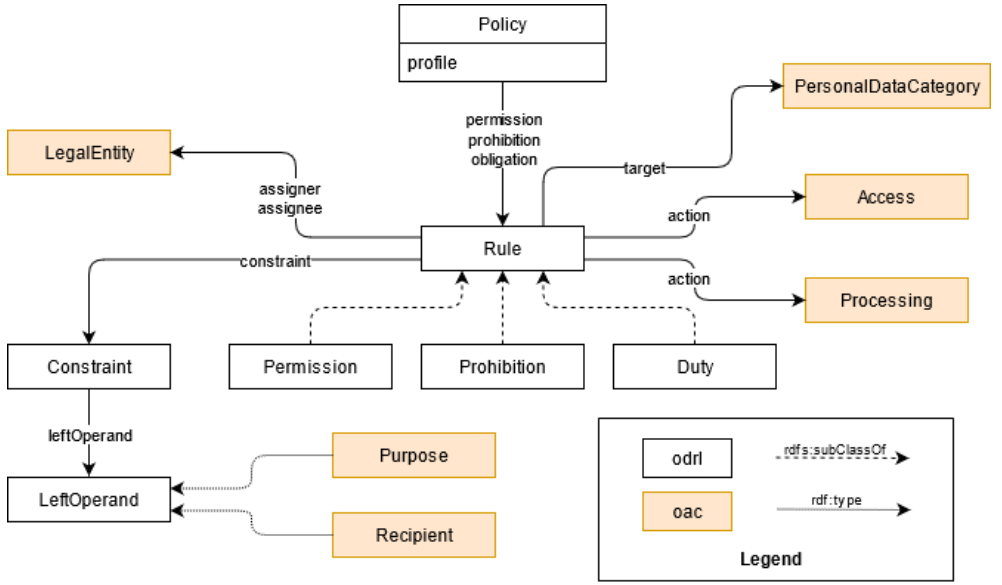
Esteves, B., Pandit, H. J., & Rodríguez-Doncel, V. (2021, September). ODRL Profile for Expressing Consent through Granular Access Control Policies in Solid. In 2021 IEEE European Symposium on Security and Privacy Workshops (pp. 298-306). https://ieeexplore.ieee.org/abstract/document/9583717

API Development



Esteves, B., Pandit, H. J., & Rodríguez-Doncel, V. (2021, September). 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

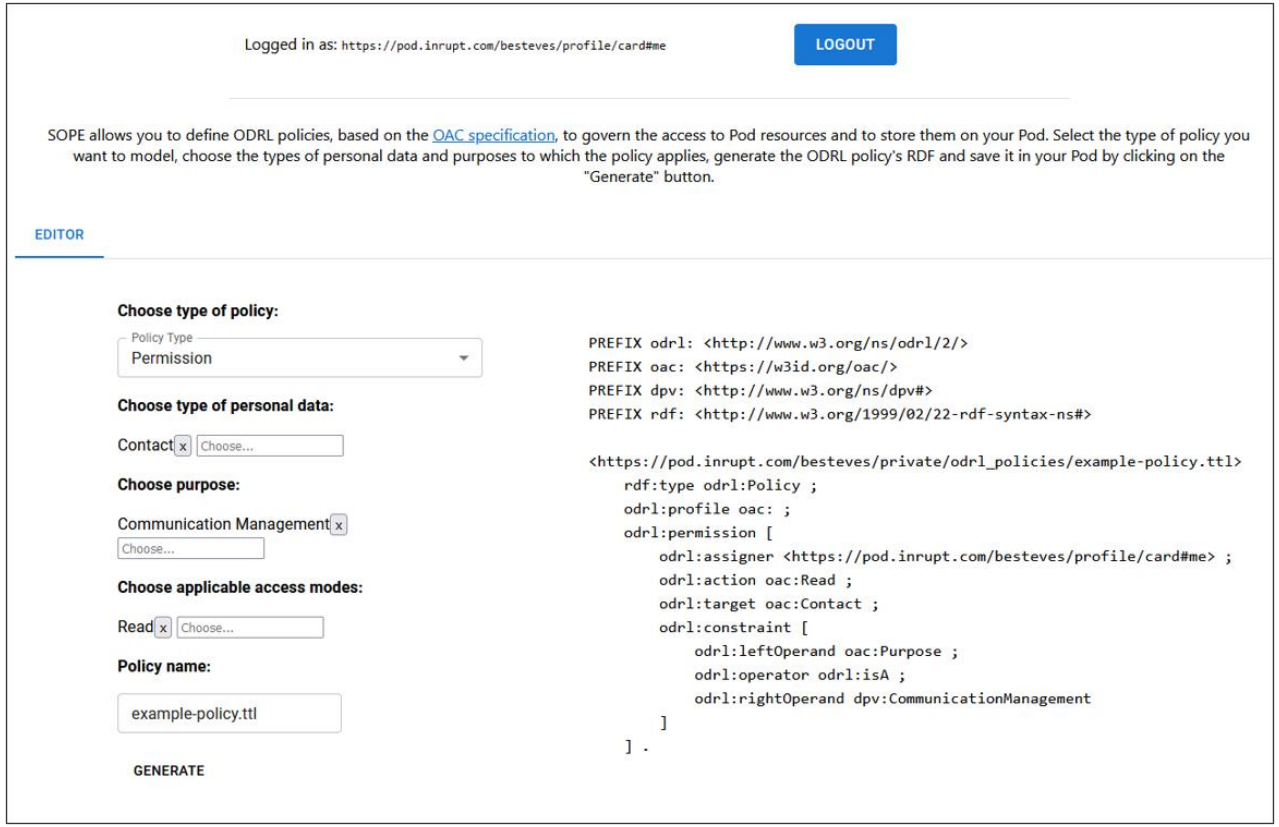
ODRL Profile for Access Control



Extension of Solid's access control mechanism using the **ODRL specification** to define policies that express permissions and/or prohibitions associated with data stored in a Solid Pod and uses **DPV** as a controlled vocabulary to invoke specific privacy and data protection terms.

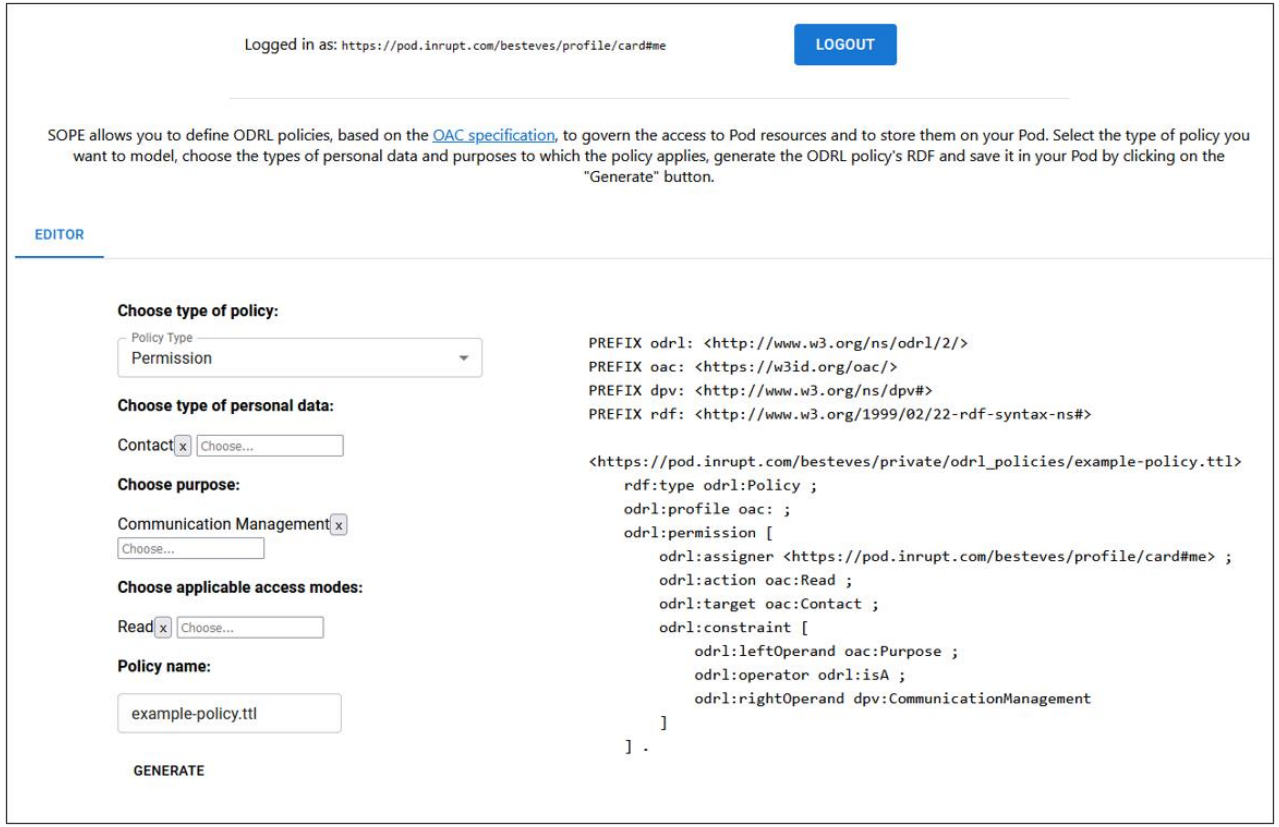
https://w3id.org/oac

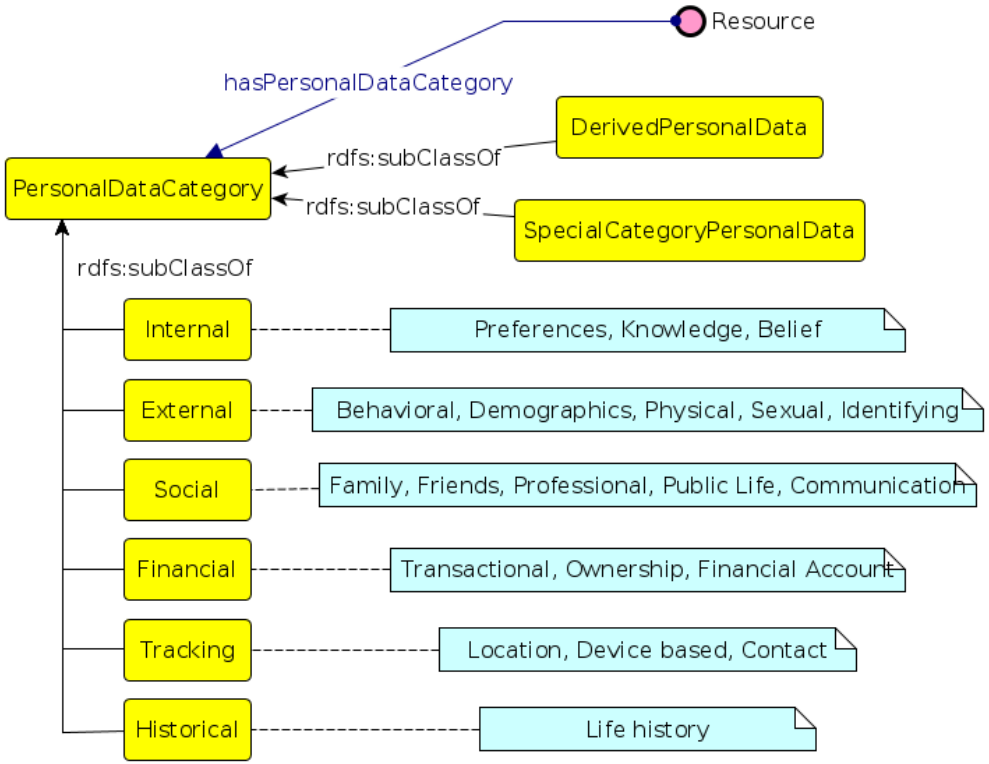
API Development



Esteves, B., Rodríguez-Doncel, V., Pandit, H. J., Mondada, N., & McBennett, P. (2022). Using the ODRL Profile for Access Control for Solid Pod Resource Governance. In European Semantic Web Conference (pp. 16-20). Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-031-11609-4_3

API Development

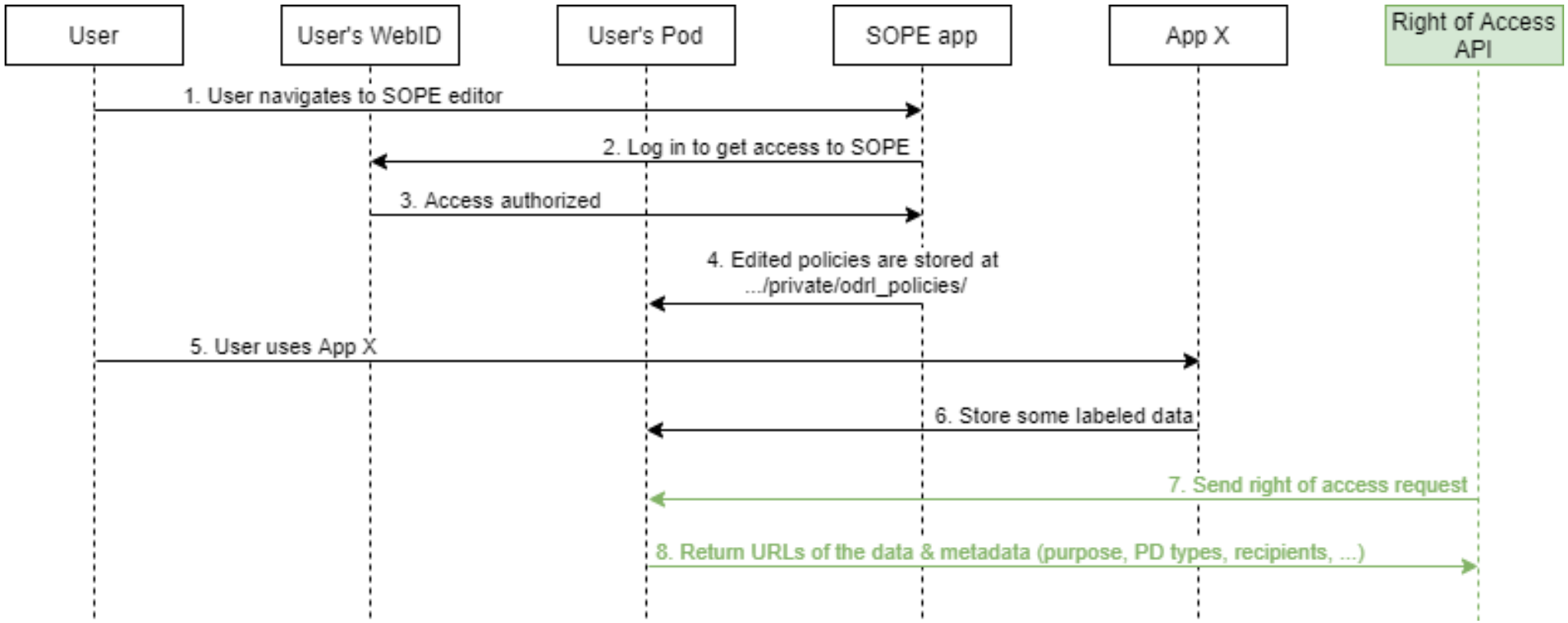




Esteves, B., Rodríguez-Doncel, V., Pandit, H. J., Mondada, N., & McBennett, P. (2022). Using the ODRL Profile for Access Control for Solid Pod Resource Governance. In European Semantic Web Conference (pp. 16-20). Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-031-11609-4_3

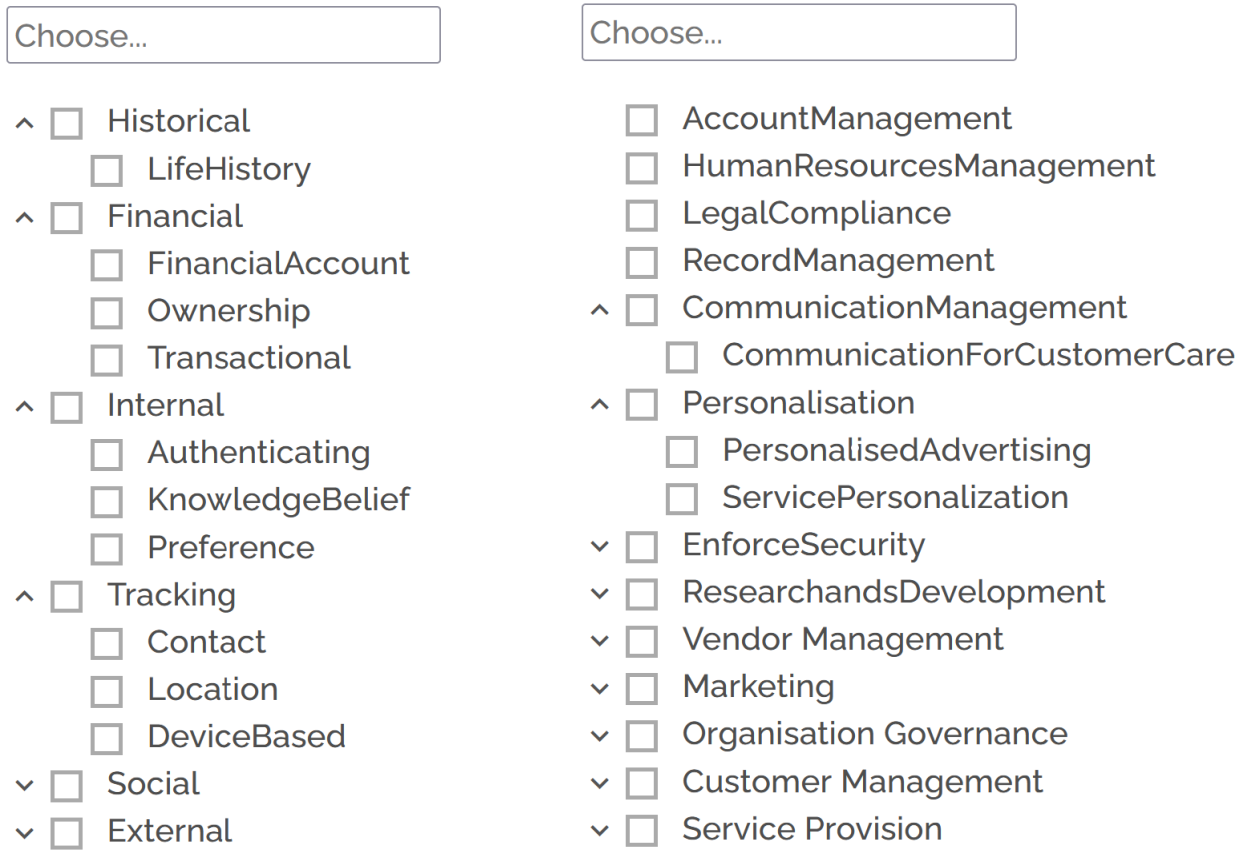
https://w3id.org/dpv/dpv-pd

API Development



https://github.com/besteves4/access-right-api

Exercising the Right of Access in Solid



https://github.com/besteves4/access-right-solid

Exercising the Right of Access in Solid

Choose...

- Historical
  - LifeHistory
- Financial
  - FinancialAccount
  - Ownership
  - Transactional
- Internal
  - Authenticating
  - KnowledgeBelief
  - Preference
- Tracking
  - Contact
  - Location
  - DeviceBased
- Social
- External

Choose...

- AccountManagement
- HumanResourcesManagement
- LegalCompliance
- RecordManagement
- CommunicationManagement
  - CommunicationForCustomerCare
- Personalisation
  - PersonalisedAdvertising
  - ServicePersonalization
- EnforceSecurity
- ResearchandsDevelopment
- Vendor Management
- Marketing
- Organisation Governance
- Customer Management
- Service Provision

https://github.com/besteves4/access-right-solid

https://pod.inrupt.com/ricardomld/public/File7

The category of the file is: LifeHistory

The recipients are:

The duration is: For as long as it is on the pod under a policy.

The policies are:

Name: Twopurposes gives permission for category: LifeHistory

RecordManagement - Write,Read

LegalCompliance - Write,Read

AccountManagement - Write,Read

Name: HistopAccMan gives permission for category: Historical

AccountManagement - Append,Write,Read

Download the folder contents.

Conclusions and Future Work

- Provide a copy of the data in an automated manner
- Metadata (purpose of the processing, personal data types, policies) is returned
- “Fine-grained” right of access for specific purposes and/or personal data types

Code

Conclusions and Future Work

- Provide a copy of the data in an automated manner
- Metadata (purpose of the processing, personal data types, policies) is returned
- "Fine-grained" right of access for specific purposes and/or personal data types

Code

- Return more metadata in the reply to the DSAR
- New parameters to filter requested data
- Mantain logs for auditing
- Reply to other data subject rights

Protect

Thanks for your attention and looking forward to your comments!

Beatriz Esteves, Víctor Rodríguez-Doncel, Ricardo Longares
Ontology Engineering Group, Universidad Politécnica de Madrid, Spain

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.