

Beatriz Esteves¹, Víctor Rodríguez-Doncel¹, Harshvardhan J. Pandit²,
Nicolas Mondada³ and Pat McBennett³

1 - Ontology Engineering Group, Universidad Politécnica de Madrid, Spain
2 - ADAPT Centre, Trinity College Dublin, Ireland
3 - Inrupt, Inc., United States
beatriz.gesteves@upm.es | Twitter: @b_esteves4



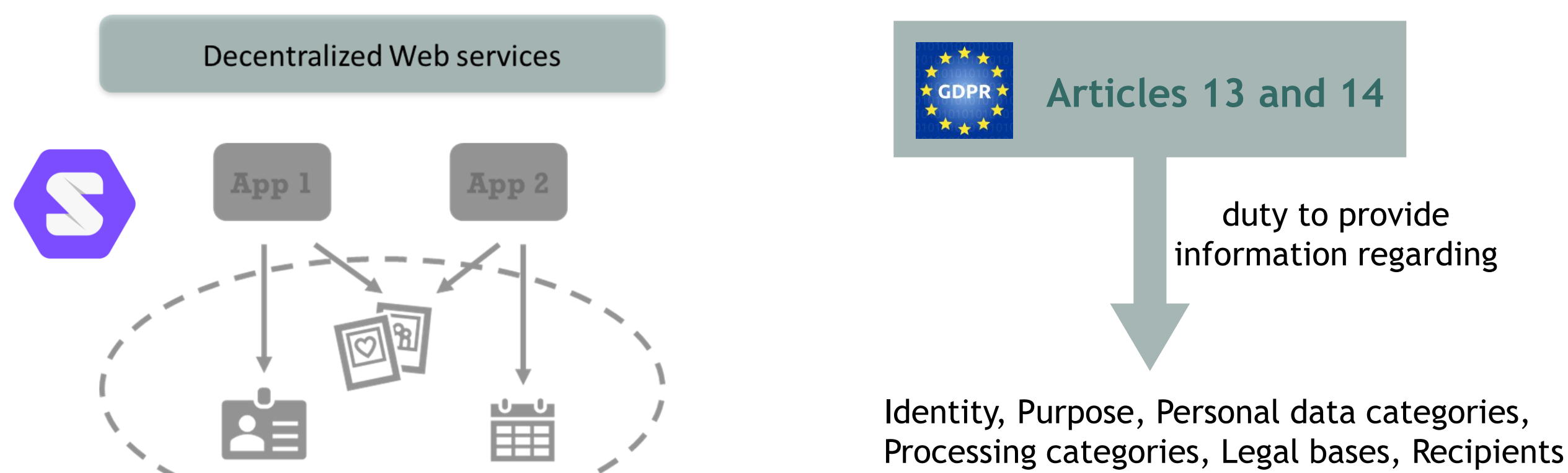
Motivation

Most companies whose business models depend on data, and especially on personal data, for the provision of Web services store the collected data in private data silos, far from the users' control.

In this context, a number of emergent solutions to decentralize the storage of data have appeared in recent years. However, as we are dealing with personal data, these decentralized storage systems fall on the sphere of the General Data Protection Regulation (GDPR) and therefore "read-write" access control policies are not expressive enough to define more complex policies and deal with GDPR requirements.

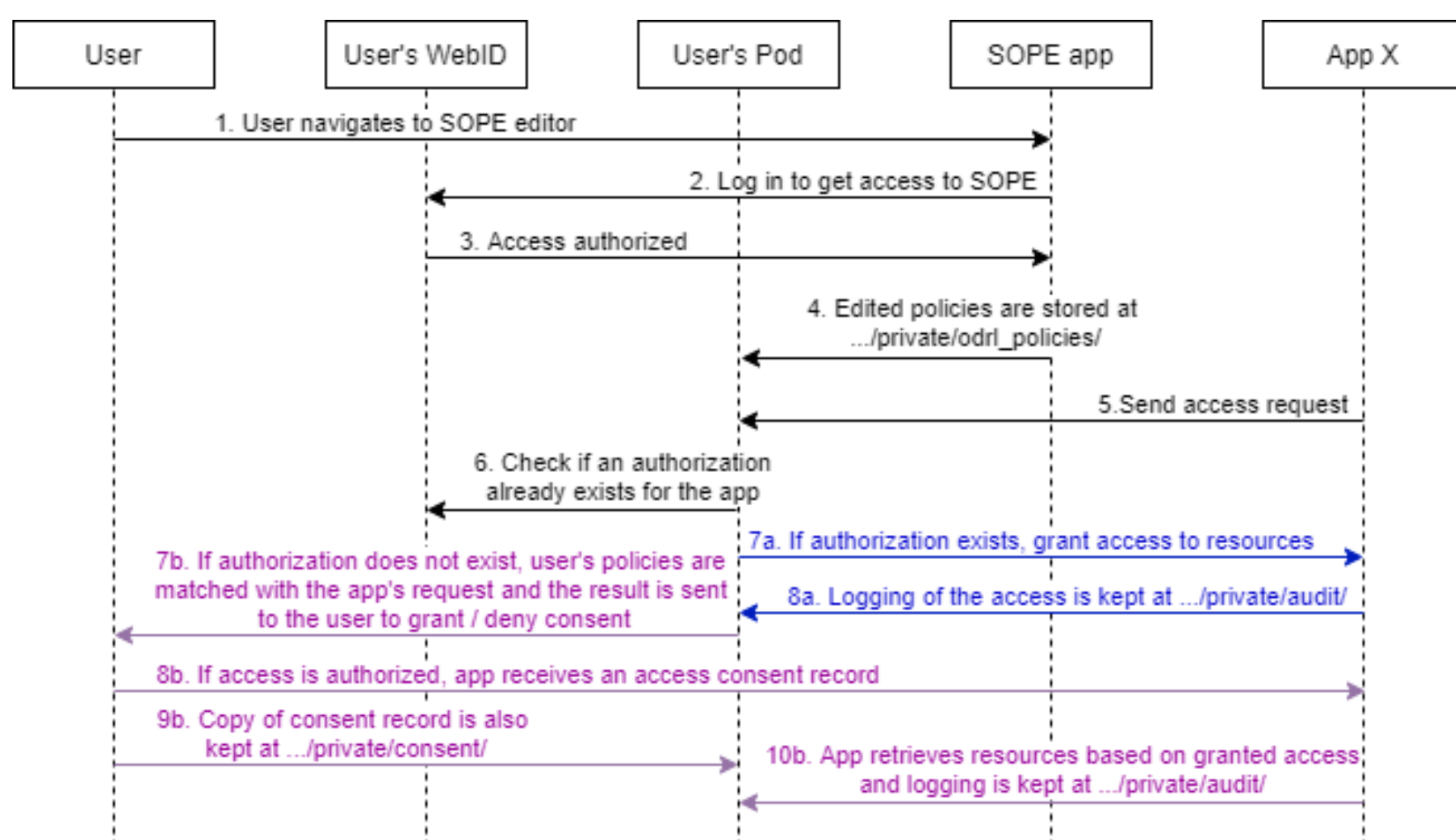
Contribution 1:
SOPE, a Solid ODRL access control Policies Editor to define policies applicable to resources stored in Solid Pods

Contribution 2:
A simulator that allows Solid app developers to create and launch an access request for specific personal data categories and purposes



Demonstration

Data Modelling



Sequence diagram of the proposed authorization algorithm demonstration

OAC - ODRL profile for Access Control [1]

Extension of Solid's access control mechanism using the ODRL[2] specification to define policies that express permissions and/or prohibitions associated with data stored in a Solid Pod and uses DPV [3] as a controlled vocabulary to invoke specific privacy and data protection terms.

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX odr: <http://www.w3.org/ns/odrl/2/#>
PREFIX oac: <https://w3id.org/oac/>
PREFIX dpv: <https://w3id.org/dpv#>
```

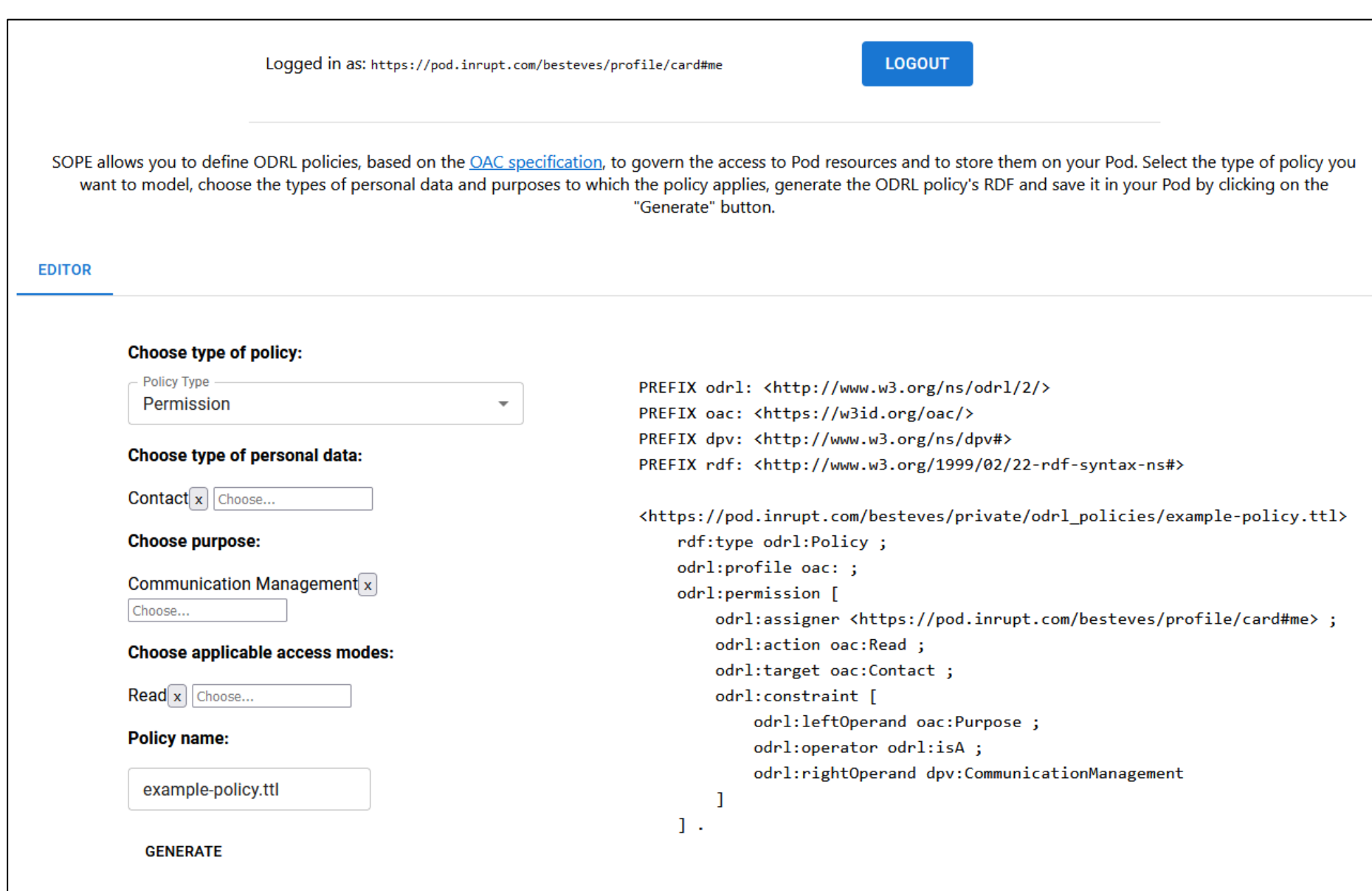
```
:policy-1 a odr:Policy ;
  odr:profile oac ;
  odr:permission [
    odr:assigner <https://anne.pod/profile/card#me> ;
    odr:action oac:Read, oac:Write ;
    odr:constraint [
      odr:leftOperand oac:Purpose ;
      odr:operator odr:isA ;
      odr:rightOperand dpv:AcademicResearch ] ] .
```

```
PREFIX dpv: <https://w3id.org/dpv#>
PREFIX dct: <http://purl.org/dc/terms/>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX dpv-pd: <https://w3id.org/dpv/dpv-pd#>
```

```
:consentRecord-1 a dpv:Consent ;
  dct:hasVersion "v1" ;
  dpv:hasIdentifier <https://anne.pod/private/consent/record1> ;
  dpv:hasDataSubject <https://anne.pod/profile/card#me> ;
  dpv:hasProvisionBy <https://anne.pod/profile/card#me> ;
  dpv:hasProvisionTime "2022-03-01T09:27:58"^^xsd:dateTime ;
  dpv:hasPersonalDataHandling [
    a dpv:PersonalDataHandling ;
    dct:language "en" ;
    dpv:hasPolicy :policy-1 ;
    dpv:hasPurpose [
      a dpv:AcademicResearch ;
      dpv:hasLegalBasis dpv:Consent ;
      dpv:hasPersonalData dpv-pd:Demographic ;
      dpv:hasProcessing dpv:Use, dpv:Store ;
      dpv:hasDataController [
        a dpv:DataController ;
        dpv:hasName "Company A" ;
        dpv:hasContact "companyA@example.com" ] ] ] .
```

Conclusions & Future Work

- SOPE provides Solid users with a tool to edit policies in a user-friendly manner, without the need to know about the inner workings of ODRL.
- The request demonstrator application allows Solid developers to simulate a request for access for specific categories and purposes of personal data and obtain the URIs of the resources for which the request is authorized.
- SHACL shapes should be defined to validate the policies.
- Usability testing must be performed to assess the design choices included in SOPE.
- Other user interfaces beyond this proof of concept should be developed.
- Semantic reasoners should be leveraged in different scenarios where inferred knowledge might simplify validating a policy.



Screenshot of the SOPE application

References:

- 1 - Esteves, B. et al.: ODRL Profile for Expressing Consent through Granular Access Control Policies in Solid. In: 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 298-306 (2021).
- 2 - Iannella, R. et al.: ODRL Vocabulary & Expression 2.2 (2018), <https://www.w3.org/TR/odrl-vocab/>, W3C Recommendation.
- 3 - Pandit, H.J. et al.: Data Privacy Vocabulary (DPV) 0.7 (2022), <https://w3id.org/dpv>, Draft Community Group Report.



Acknowledgements: This research has been supported by European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 813497 (PROTECT). Harshvardhan J. Pandit has received funding from the Irish Research Council Government of Ireland Postdoctoral Fellowship Grant#GOIPD/2020/790. The ADAPT SFI Centre for Digital Media Technology is funded by Science Foundation Ireland through the SFI Research Centres Programme and is co-funded under the European Regional Development Fund (ERDF) through Grant#13/RC/2106_P2.