Using the ODRL Profile for Access Control for Solid Pod Resource Governance

Beatriz Esteves[1*], Víctor Rodríguez-Doncel[1], Harshvardhan J. Pandit[2], Nicolas Mondada[3] and Pat McBennett[3]

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 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 should support 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.

Decentralized Web services

App 1   App 2

Personal data store

GDPR

Articles 13 and 14

Duty to provide information regarding

Identity, Purpose, Personal data categories, Processing categories, Legal bases, Recipients
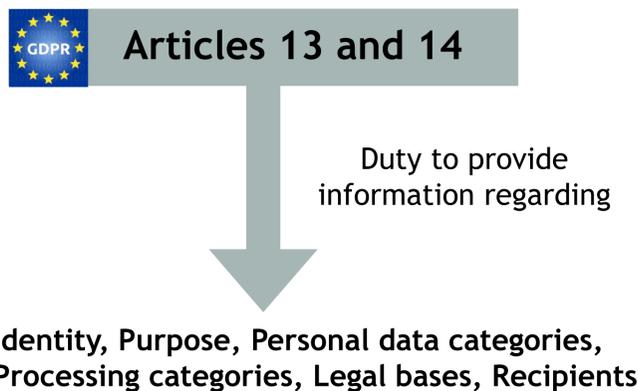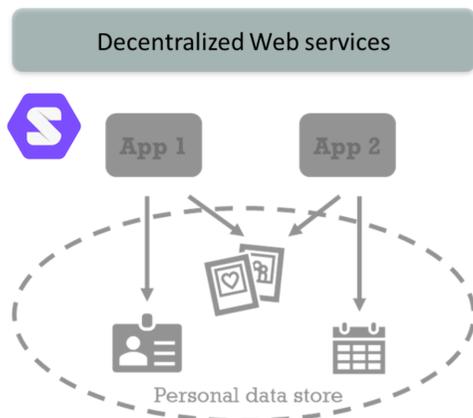
CONTRIBUTION 1
SOPE, a Solid ODRL access control Policies Editor to define policies applicable to resources stored in Solid Pods

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

Demonstration
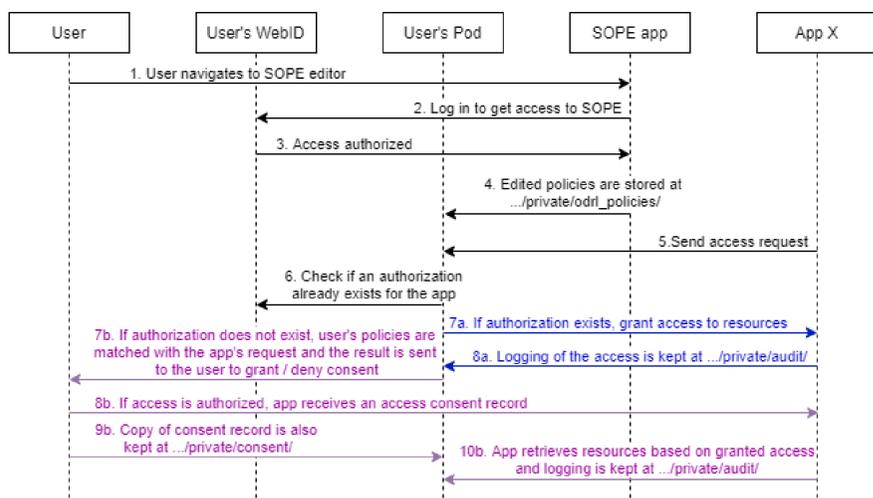
Figure 1. Sequence diagram of the proposed authorization algorithm demonstration

Logged in as: https://pod.inrupt.com/besteves/profile/card#me   LOGOUT

SOPE allows you to define ODRL policies, based on the OAC specification, to govern the access to Pod resources and to store them on your Pod. Select the type of policy you want to model, choose the types of personal data and purposes to which the policy applies, generate the ODRL policy's RDF and save it in your Pod by clicking on the "Generate" button.

EDITOR

Choose type of policy:
Policy Type
Permission

Choose type of personal data:
Contact x Choose...

Choose purpose:
Communication Management x
Choose...

Choose applicable access modes:
Read x Choose...

Policy name:
example-policy.ttl

GENERATE

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

<https://pod.inrupt.com/besteves/private/odrl_policies/example-policy.ttl>
    rdf:type odrl:Policy ;
    odrl:profile oac: ;
    odrl:permission [
        odrl:assigner <https://pod.inrupt.com/besteves/profile/card#me> ;
        odrl:action oac:Read ;
        odrl:target oac:Contact ;
        odrl:constraint [
            odrl:leftOperand oac:Purpose ;
            odrl:operator odrl:isA ;
            odrl:rightOperand dpv:CommunicationManagement
        ]
    ] .
```

Figure 2. Screenshot of the SOPE application

Data Modelling

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 odrl: <http://www.w3.org/ns/odrl/2/#>
PREFIX oac: <https://w3id.org/oac/>
PREFIX dpv: <https://w3id.org/dpv#>

:policy-1 a odrl:Policy ;
    odrl:profile oac: ;
    odrl:permission [
    odrl:assigner <https://anne.pod/profile/card#me> ;
        odrl:target oac:Demographic ;
        odrl:action oac:Read, oac:Write ;
        odrl:constraint [
            odrl:leftOperand oac:Purpose ;
            odrl:operator odrl:isA ;
            odrl: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.
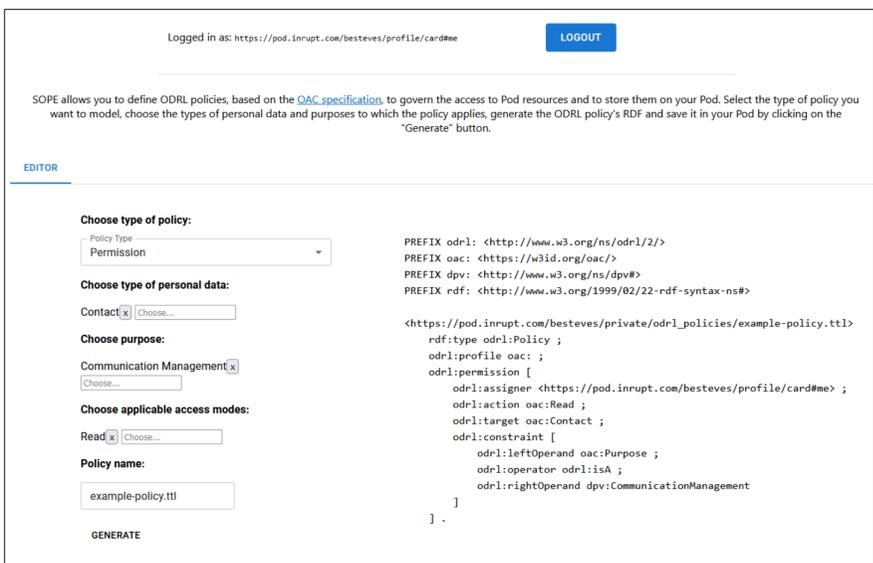
References:
1 – Esteves, B. et al.: ODRL Profile for Expressing Consent through Granular Access Control Policies in Solid. In: 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). pp. 298-306 (2021).
2 – Iannella, R. et al.: ODRL Vocabulary & Expression 2.2 (2018), https://www.w3.org/TR/odrl-vocab/, W3C Recommendation.
3 – Pandit, H.J. et al.: Data Privacy Vocabulary (DPV) 0.7 (2022), https://w3id.org/dpv, Draft Community Group Report.