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
beatriz.gesteves@upm.es
[2] ADAPT Centre, Trinity College Dublin, Ireland
[3] Inrupt, Inc., United States

Abstract. This demo shows an ODRL editor where RDF policies can be defined and enforced to grant access to personal data stored in Solid Pods. Policies are represented using OAC, the ODRL profile for Access Control, which allows the definition of complex, fine-grained permissive and prohibitive policies that are aligned with GDPR requirements regarding the processing of personal data. In addition, a second demonstrator is presented to simulate an app's request for data and examples of policies and consent record modelling are showcased.

Keywords: ODRL · Policy modelling · Access control · Solid

1 Introduction

Currently, 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 Web, and in particular to decentralize the storage of data, such as Solid[4], Hub of All Things[5] and so on, have appeared in recent years. In particular, the Solid specification[6] relies on interoperable data formats and protocols such as the Linked Data Platform[7] or the ACL (Basic Access Control)[8] ontology. However, as we are dealing with personal data, this decentralized storage system falls on the sphere of the General Data Protection Regulation (GDPR)[9] [1] and therefore ACL-based access control policies are not expressive enough for applications to define more complex policies and deal with GDPR requirements regarding the specification of purposes or legal bases for the processing of personal data. In addition, by using semantic web vocabularies such as the Open Digital Rights Language (ODRL) [3] and the Data

[4] https://solidproject.org/
[5] https://www.hubofallthings.com/
[6] https://solidproject.org/TR/protocol
[7] https://www.w3.org/TR/ldp/
[8] http://www.w3.org/ns/auth/acl#
[9] https://eur-lex.europa.eu/eli/reg/2016/679/oj

Privacy Vocabulary (DPV) [4], users can easily define more elaborated policy-type preferences when it comes to accessing resources stored in their personal information management system, i.e., to state that only contacts who attended the same university as the user can see their photos.

In this demo[10], we showcase:

- An ODRL editor (SOPE - Solid ODRL access control Policies Editor) which allows for the generation of ODRL policies based on OAC – the ODRL profile for Access Control[11] – to define declarative policies that express permissions and / or prohibitions associated with data stored in a Solid Pod.
- A demonstrator where developers can issue an app request for personal data and receive the respective response based on the architecture and on the access request's authorization algorithm previously described by the authors in [2].

This paper is structured as follows: Section 2 presents a description of the demonstration; Section 3 details the data modelling used in the work, which relies essentially on OAC, ODRL and DPV; and Section 4 concludes the paper and provides future lines of work.

2 Demonstration

The UML sequence diagram in Figure 1 highlights the components of this demo. The demo set-up consists of two Solid apps that consume and produce Solid Pod resources. SOPE[12] is a Solid ODRL access control Policies Editor for users of Solid apps who wish to define more fine-grained access control policies over their Solid Pod resources. It allows the users to define ODRL policies, based on the OAC profile, to govern the access and storage of Pod resources. To start using SOPE, users need to log into their Solid Pod as the policies will be saved in a private Solid container. Following this step, users only need to choose which type of policy they will be modelling (an ODRL permission or prohibition), select the categories of personal data and purposes to which the policy applies and the access control modes permitted/prohibited by the policy. Finally, the RDF policy will be automatically generated and stored in their Pod under the "/private" container, in a specific sub-container for ODRL policies.

A second app was developed to simulate the process of an app requesting access to certain types of personal data for a specific purpose. It allows Solid app developers to create and launch an access request for specific personal data categories and purposes. This app will match the request's personal data categories, access modes and purposes with the ODRL policies stored in a user's Pod. If a policy exists to authorize the access to such personal data categories then URL paths to Solid Pod resources that contain said personal data categories will be returned.

[10] https://protect.oeg.fi.upm.es/eswc-demo/
[11] https://w3id.org/oac/
[12] Source code is available on https://github.com/besteves4/solid-sope

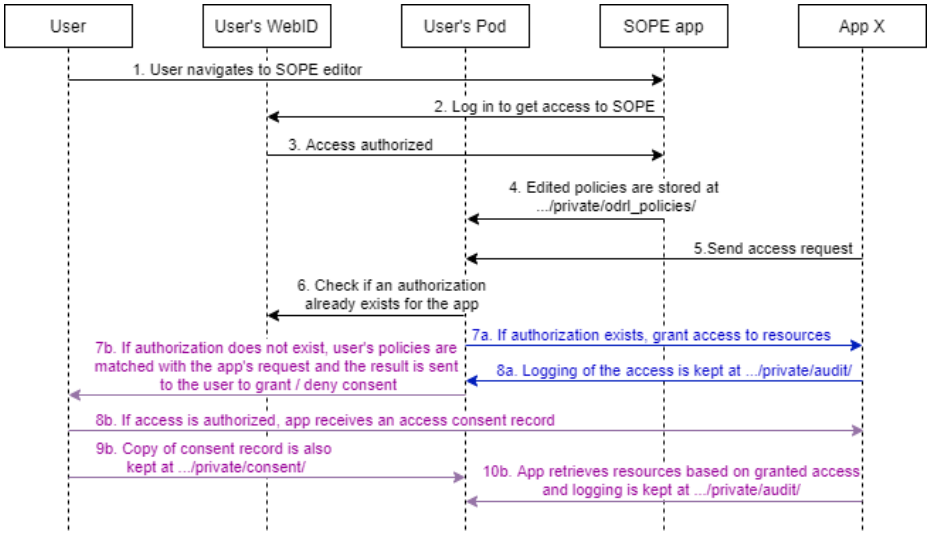

Fig. 1. Sequence diagram of the proposed authorization algorithm demonstration.

3 Data Modelling

In this demo, ODRL[13] is used to define access control policies for the governance of access to resources stored in Solid Pods. In particular, we leverage our previous work, related to the specification of OAC, an ODRL profile to express consent through granular access control policies in Solid [2], and on DPV[14], to invoke specific privacy and data protection terms.

To demonstrate the modelling of policies and consent records, we present two examples in Listings 1.1 and 1.2. In Listing 1.1, a permission over demographic data is set by Anne for the purpose of academic research, which permits read and write access operations over her personal data. In Listing 1.2, a consent record related to an authorized access request, to use and store demographic data for academic research, is specified.

Listing 1.1. Read-Write policy for Demographic data for Academic Research purposes

```
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 [
        a odrl:Permission ;
        odrl:assigner <https://anne.databox.me/profile/card#me> ;
        odrl:target oac:Demographic ;
        odrl:action oac:Read, oac:Write ;
        odrl:constraint [
```

[13] http://www.w3.org/ns/odrl/2/
[14] https://w3id.org/dpv#

```
            odrl:leftOperand oac:Purpose ;
            odrl:operator odrl:isA ;
            odrl:rightOperand dpv:AcademicResearch ] ] .
```

Listing 1.2. Consent record of an authorized access request

```
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.databox.me/private/consent/record1> ;
    dpv:hasDataSubject <https://anne.databox.me/profile/card#me> ;
    dpv:hasProvisionBy <https://anne.databox.me/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"
            ] ;
        ] ;
    ] .
```

4 Conclusions and Future Work

In this demo, we presented a first-of-its-kind web application to generate ODRL policies using the ODRL Profile for Access Control (OAC) and a demonstrator to simulate a Solid app request and the matching authorization mechanism. With SOPE, Solid users have a tool to edit policies in a user-friendly manner, without the need to know about ODRL's inner workings, and with the demonstrator Solid developers can model access requests and obtain the personal data if said request is authorized.

This method is an important advance over the current Solid access control model, enabling richer personal data access policies to be represented and enforced. Moreover, although in the context of this particular work the OAC profile is applied to the governance of access to Solid Pod resources, its use is not limited to the Solid ecosystem, as it does not rely on any Solid-specific terms whatsoever, and it can be applied to other Linked Data platforms in future lines of work.

The system is yet to be complemented by future endeavours: (i) SHACL shapes should be defined to validate the policies, (ii) usability testing must be performed to assess the design choices included in the editor, (iii) other user interfaces beyond this proof of concept should be developed (e.g., UIs to annotate resources with the types of personal data they contain) and (iv) the inferencing power of semantic reasoners should be leveraged in different scenarios where inferred knowledge might simplify validating a policy.

Funding 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.

References

1. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016)
2. Esteves, B., Pandit, H.J., Rodríguez-Doncel, V.: 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). https://doi.org/10.1109/EuroSPW54576.2021.00038, ISSN: 2768-0657
3. Iannella, R., Steidl, M., Myles, S., Rodríguez-Doncel, V.: ODRL Vocabulary & Expression 2.2 (2018), https://www.w3.org/TR/odrl-vocab/, publication Title: W3C Rec.
4. Pandit, H.J., Polleres, A., Bos, B., Brennan, R., Bruegger, B., Ekaputra, F.J., Fernández, J.D., Hamed, R.G., Kiesling, E., Lizar, M., Schlehahn, E., Steyskal, S., Wenning, R.: Creating a Vocabulary for Data Privacy: The First-Year Report of Data Privacy Vocabularies and Controls Community Group (DPVCG). In: Panetto, H., Debruyne, C., Hepp, M., Lewis, D., Ardagna, C.A., Meersman, R. (eds.) On the Move to Meaningful Internet Systems: OTM 2019 Conferences. vol. 11877, pp. 714–730. Springer International Publishing (2019). https://doi.org/10.1007/978-3-030-33246-4_44, http://link.springer.com/10.1007/978-3-030-33246-4_44, series Title: Lecture Notes in Computer Science