Protect

ODRL Profile for Expressing Consent through Granular Access Control Policies in Solid

Beatriz Esteves, beatriz.gesteves@upm.es, OEG – UPM
Harshvardhan J. Pandit, pandith@tcd.ie, ADAPT Centre –TCD
Víctor Rodríguez-Doncel, vrodriguez@fi.upm.es, OEG – UPM

This project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº813497

Overview

- Introduction to Solid
- Motivation
- Related Work
- ODRL Profile for Solid's ACL
- Implementation & Architecture
- Challenges
- Conclusion

ODRL Profile for Access Control in Solid

Release 12 April 2021

Latest editor's draft:
https://w3id.org/oac/

Editors:
Beatriz Esteves (Ontology Engineering Group, Universidad Politécnica de Madrid)
Harshvardhan J. Pandit (ADAPT Centre, Trinity College Dublin)
Víctor Rodríguez-Doncel (Ontology Engineering Group, Universidad Politécnica de Madrid)

Participate:
GitHub profile
File a bug
Commit history
Pull requests

Abstract

This document presents a new profile, the ODRL Profile for Access Control in Solid, that extends Solid's ACL mechanism by using the ODRL Vocabulary and Expression specification to define 'sticky policies' that express permissions and / or prohibitions associated with data stored in a Solid pod and utilises DPV as a controlled vocabulary for invoking privacy and data protection-specific terms.

Introduction to Solid

https://solidproject.org

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

Ownership

Interoperability

Solid's Access Control Authorizations

Beatriz has full access to one of her web resources, located at https:// beatriz.databox.me/docs/file1

```
<#authorization1>
    a acl:Authorization;
    acl:agent <https://beatriz.databox.me/profile/card#me>;
    acl:accessTo  <https://beatriz.databox.me/docs/file1>;
    acl:mode acl:Read, acl:Write, acl:Control.
```

WebID

Motivation

GDPR's Articles 13 and 14

provide information regarding

Identity
Purpose
Personal data categories
Processing categories
Legal bases
Recipients

→ **Consent**

Introspect use of personal data

Store consent and authorisations

Determine data sharing preferences

→ **How can Solid's ACL be extended to specify and enforce an individual's data sharing preferences?**

Related Work

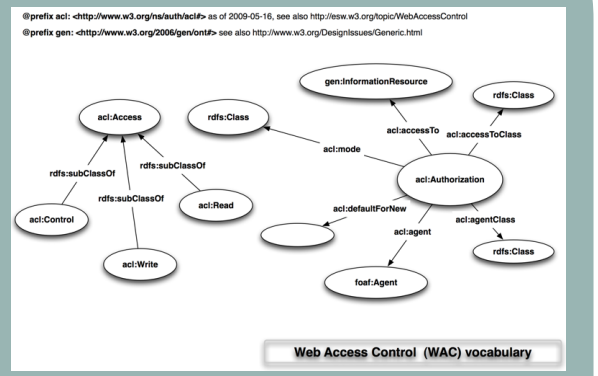
Access Control using Linked Data

W3C

WebID 1.0

Web Identity and Discovery

W3C Editor's Draft 05 March 2014



OASIS

eXtensible Access Control Markup Language (XACML) Version 3.0

OASIS Standard

22 January 2013

ODRL Information Model 2.2

W3C Recommendation 15 February 2018

W3C

Specifying Personal Data and Processing

SPECIAL

BPR 4 GDPR

GDPRtEXT

Release 2020-03-31

GConsent

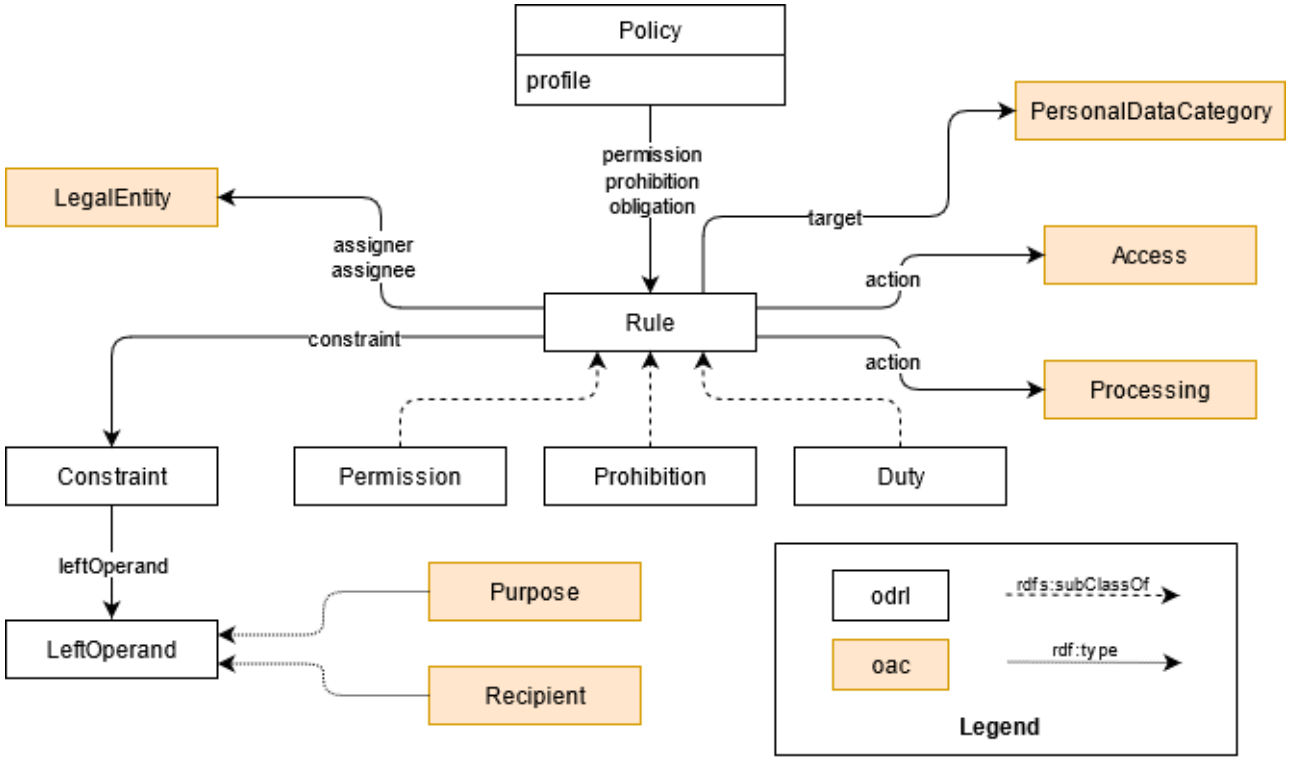
A consent ontology based on the GDPR

Data Privacy Vocabulary (DPV)

version 0.2

Draft Community Group Report 28 July 2021

ODRL Profile for Solid's ACL



Extension of Solid's ACL mechanism using the ODRL specification to define "sticky 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.

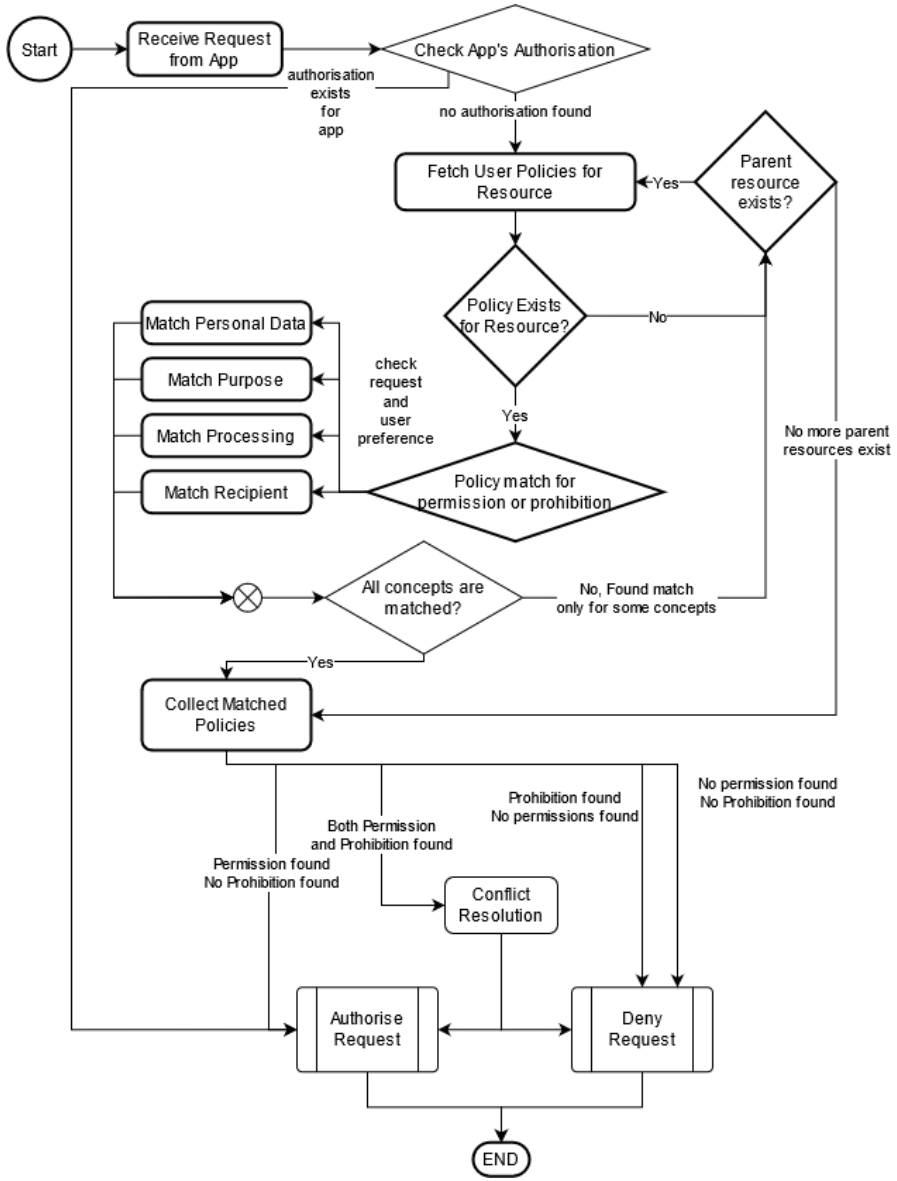
https://w3id.org/oac/

Requisites

R1. Support specifying user preferences as policies.
R2. Incorporate vocabulary specifying or aligned to legal concepts.
R3. Support specifying permissions and prohibitions at arbitrary granularity.
R4. Support identifying and resolving conflicts based on scope.
R5. Record (store) policies used to authorise access.
R6. Support querying policies and authorisations for introspection of data use.

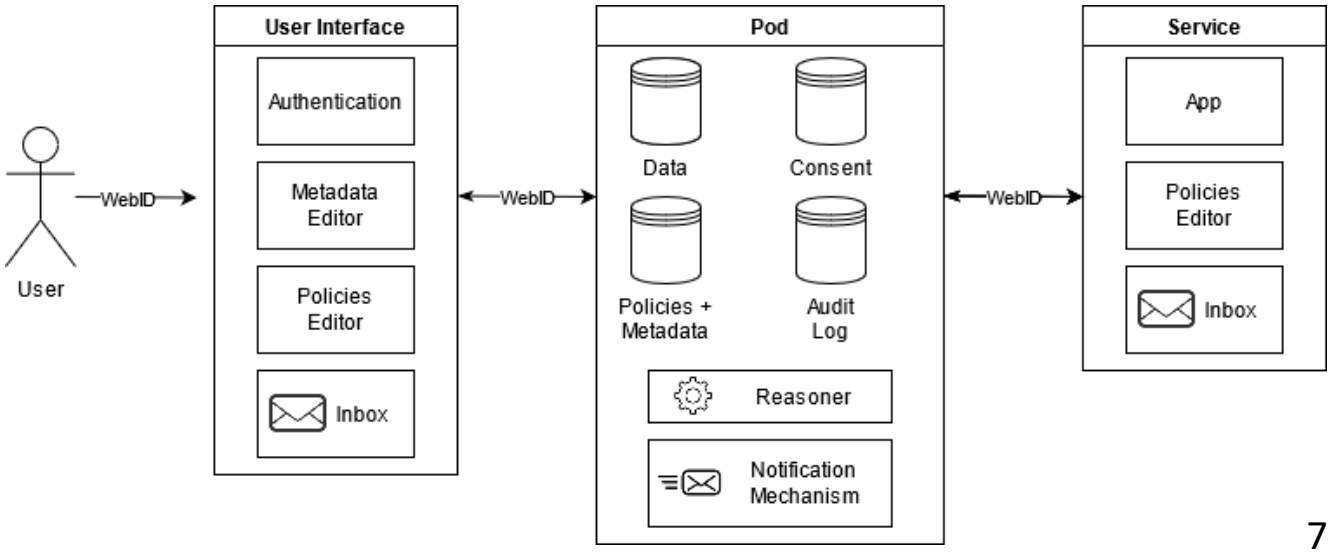
```
:example-1 a odrl:Policy ;
        odrl:permission [
                odrl:action oac:Read
                odrl:target oac:Contact
                odrl:assigner [
                        a oac:DataSubject ;
                        cert:key "https://beatriz.webID/card#me"
                ] ;
                odrl:constraint [
                        odrl:leftOperand oac:Purpose ;
                        odrl:operator odrl:isA ;
                        odrl:rightOperand dpv:AcademicResearch
                ]
        ] .
```

Implementation & Architecture



Extension of the existing Solid Pod specification

- Consent datastore – keep a record of the consent actions
- Audit Log – store metadata related to logins, access requests, changes in policies and consent authorisations
- Notification Mechanism – allow to update or revoke requests regarding consent
- Metadata and Policies Editors – assist users to craft granular policies for the management of access to their Pod



Challenges

Efficiency and performance

- Deal with large collection of policies in the form of preferences, requests, and authorisations

Complexity of ODRL policies

- The more data is transmitted in policies and requests, the more time and resource-consuming will be the authorization mechanism
- Deal with conflicting policies, i.e., global prohibitions outweigh local permissions

Limit ODRL features to ensure optimal performance

Storage and Management of Policies

- Where to store requests and user policies
- Discovery of policies that refer to a given resource
- How to craft valid ODRL policies

- Create a separate area of the Pod to store the policies and metadata declarations
- Create a Policies Editor component that supports users in drafting the policies, without having the need for previous ODRL knowledge

Challenges

Legal Implications of Requests

- Deal with other legal bases, i.e., compliance with a legal obligation or legitimate interests

- Discuss whether access to resources in the pod should be automated
- Challenge that is unlikely to be satisfactorily addressed

Legal Interpretation of Request and Preferences

- Map policies, requests, and preferences with their legal interpretation
- Deal with different jurisdictions

Consent

- To ensure that consent is informed and explicit, specific information items should be provided and recorded in the Pod
- Allow users to update or revoke consent
- Discuss whether the implicit consent from the established user preferences is enough to provide automated access to non-sensitive personal data

- Allow users to choose which data types, and purposes, they are comfortable with enabling automation and which not
- Have a queryable Consent datastore which can be easily updated

Conclusion

Solid's shortcomings

- Expression of more complex policies beyond a yes/no
- Alignment with GDPR requisites

Can be overcome by using

ODRL Information Model 2.2
W3C Recommendation 15 February 2018

Data Privacy Vocabulary (DPV)
version 0.2

Draft Community Group Report 28 July 2021

Future Work

- Implement reasoners that can efficiently perform the authorization decision.
- Define the RDF SHACL shapes that determine which ODRL expressions can be evaluated.
- Declare mappings to other languages that grant interoperability with compliance tools.
- Grant seamless operation with non-ODRL Solid Pods.

Protect

ODRL Profile for Expressing Consent through Granular Access Control Policies in Solid

Q & A

Beatriz Esteves, beatriz.gesteves@upm.es, OEG – UPM
Harshvardhan J. Pandit, pandith@tcd.ie, ADAPT Centre –TCD
Víctor Rodríguez-Doncel, vrodriguez@fi.upm.es, OEG – UPM

This project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº813497