

# Authentication and authorization in Data Spaces: A relationship-based access control approach for policy specification based on ODRL

Irene Plaza-Ortiz<sup>1,†</sup>, Andres Munoz-Arcentales<sup>1,†</sup>, Joaquin Salvachua<sup>1,†</sup>, Carlos Aparicio<sup>1,†</sup>, Gabriel Huecas<sup>1,†</sup> and Enrique Barra<sup>1,\*,†</sup>

<sup>1</sup>*Departamento de Ingeniería de Sistemas Telemáticos, Information Processing and Telecommunications Center, ETSI Telecomunicación, Universidad Politécnica de Madrid*

## Abstract

Data has become a crucial resource in the digital economy, fostering initiatives for secure and sovereign data sharing frameworks such as Data Spaces. However, these distributed environments require fine-grained access control mechanisms that balance openness with sovereignty and security. This paper proposes an extension of the Open Digital Rights Language (ODRL) standard, the ODRL Data Spaces (ODS) profile, aimed at supporting authorization—and complementing existing authentication mechanisms—throughout the data lifecycle. Additionally, a policy execution engine is introduced to translate ODRL policies into executable formats, enabling effective enforcement. The approach is validated through a use case involving OpenFGA, demonstrating its applicability to relationship-based access control scenarios.

## Keywords

Data Spaces, Data Sovereignty, Policy Execution, Access Control, ReBAC, ODRL

## 1. Introduction

The European Union's Data Spaces aim to facilitate secure, decentralized data exchange based on trust and sovereignty. However, effective governance requires enhanced mechanisms for access and usage control [1]. ODRL has emerged as a key standard for managing digital rights in these environments [2].

Nevertheless, ODRL existing vocabulary presents limitations when addressing the complex requirements of decentralized and federated environments. This work addresses these challenges by proposing the ODRL Data Spaces (ODS) profile, an extension specifically designed to enhance ODRL's applicability to cover the life cycle of a data within Data Spaces [3].

Moreover, as ODRL policies are not inherently executable, this paper introduces a policy execution engine capable of compiling ODRL specifications into executable formats. The integration of these two contributions supports the realization of sovereign and controlled data sharing within dynamic and heterogeneous ecosystems. Additionally, this work explores how OpenFGA, an access control system, complements ODRL by enabling usage control [4].

While the main focus of this work is on fine-grained authorization, we assume authentication to be handled by existing identity management solutions, such as decentralized identifiers (DIDs) or federated identity providers, which supply trusted identities for policy evaluation.

The paper is structured as follows: Section 2 presents the ODS profile, Section 3 details the execution engine and the use case with OpenFGA, and Section 4 concludes the paper.

---

OPAL 2025: ODRL And Beyond: Practical Applications And Challenges For Policy-Base Access And Usage Control., June 01–02, 2025, Portorož, Slovenia

\*Corresponding author.

<sup>†</sup>These authors contributed equally.

✉ irene.plaza.ortiz@upm.es (I. Plaza-Ortiz); joseandres.munoz@upm.es (A. Munoz-Arcentales); joaquin.salvachua@upm.es (J. Salvachua); carlos.aparicio@upm.es (C. Aparicio); gabriel.huecas@upm.es (G. Huecas); enrique.barra@upm.es (E. Barra)

0009-0008-6382-7482 (I. Plaza-Ortiz); 0000-0003-1554-437X (A. Munoz-Arcentales); 0000-0002-7269-8079 (J. Salvachua); 0000-0002-6331-3296 (C. Aparicio); 0000-0001-5673-9312 (G. Huecas); 0000-0001-9532-8962 (E. Barra)



© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

**Table 1**  
ODRL additional vocabulary

Label	Parent class	Definition
ODS:Consumer	odrl:Party	The Party who acts as the intended user of the data under the Rule. Inherits semantics from odrl:assignee but is specialized for Data Space consumption roles. The Party who offers or shares the data asset under the Rule. Specialization of odrl:assigner for Data Spaces. The The Party who intermediates data exchanges between Providers and Consumers within the Data Space. The Party responsible for overseeing compliance with the Rule, without being directly involved in data usage.
ODS:Provider	odrl:Party	
ODS:Broker	odrl:Party	
ODS:Monitor	odrl:Party	
ODS:Train	odrl:Action	Action to train a machine learning model.
ODS:Subscribe	odrl:Action	Action to subscribe to a dataset, services, or data stream.
ODS:Request_data	odrl:Action	Action to request specific data from other participants in the data space.
ODS:Retention	odrl:Action	Action that defines the maximum data retention period before deletion or archiving.
ODS:Kill_job	odrl:Action	Action to kill the current executing job.

## 2. An ODRL Profile for Data Spaces

The proposed ODRL Data Spaces (ODS) profile builds upon existing efforts to enable fine-grained access control in decentralized environments. It extends the Open Access Control (OAC) profile for ODRL [5], which itself leverages the Data Privacy Vocabulary (DPV) [6]. DPV provides a rich ontology for expressing personal data categories, purposes of processing, and legal bases, facilitating granular policy specification aligned with privacy regulations such as GDPR [7].

However, while OAC and DPV enable detailed modeling of purposes and obligations related to data use, they do not explicitly define the roles, actions, and operational constraints specific to federated Data Spaces. The ODS profile addresses this gap by introducing specialized Party and Action terms tailored to common Data Space scenarios, such as differentiated roles or operational actions like Subscribe, Retention, and Train. These additions support a clearer and more enforceable policy structure in complex data exchange environments.

Furthermore, the ODS profile is designed to complement existing Data Space architectures, particularly those informed by standards like the International Data Spaces Association (IDSA) Information Model [8].

Table 1 includes some of the main terms of the profile, along with a brief description and their alignment with the ODRL vocabulary.

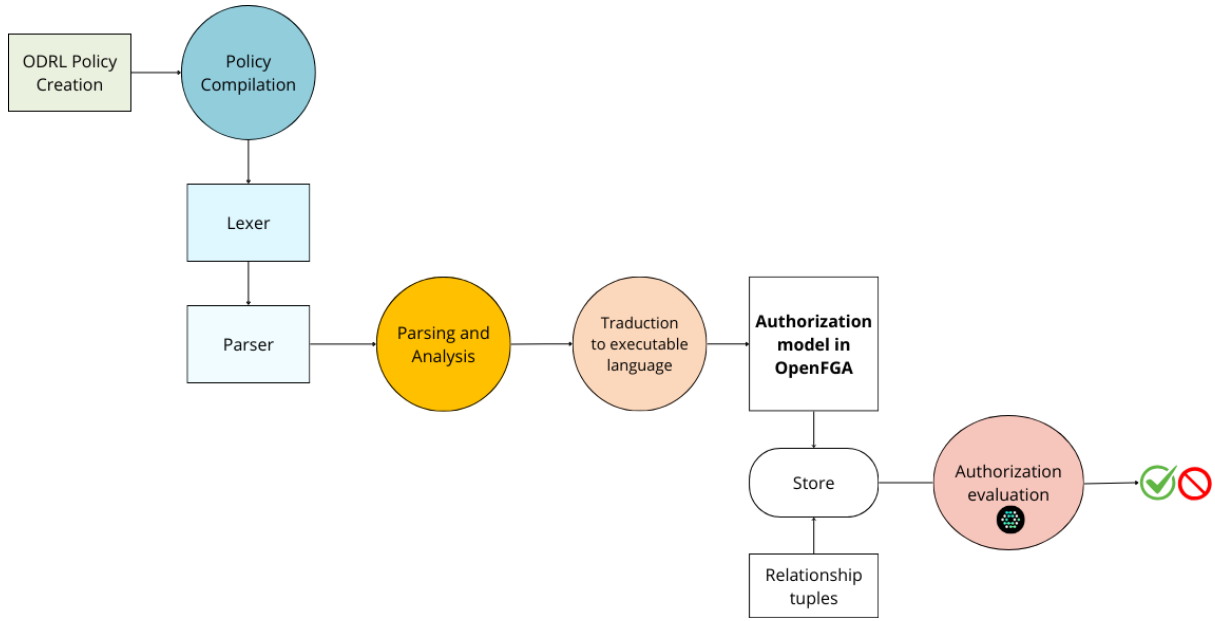
## 3. Policy Execution Engine

While ODRL provides a robust framework for policy specification, its lack of a native execution model limits its applicability in operational environments. To address this, we propose a conceptual policy execution engine that bridges ODRL-based policies with enforcement mechanisms. The approach focuses on compiling ODRL specifications into formats suitable for relationship-based access control systems.

In our prototype, we use OpenFGA—an authorization engine inspired by Google’s Zanzibar—to demonstrate how policies expressed using the ODS profile can be translated into executable rules. OpenFGA is a modern authorization engine designed to be scalable, flexible, and easily integrated into distributed architectures. It supports access policies based on relationships between entities, making it a suitable choice for dynamic and decentralized environments. Moreover, its compatibility with federated identity providers simplifies the authentication of identities, which are mapped to relationships that drive access decisions.

Figure 1 shows the workflow for this use case according to the following process:

1. **ODRL Policy Creation:** The first step is to define the access policy using the ODRL language. The policy is set following the previously defined ODS profile.
2. **Policy Compilation & Parsing and Analysis:** Once the policy is defined in ODRL, it is fed into the policy execution engine, which is responsible for processing and transforming the policy into different executable formats.
3. **Transformation to executable languages:** The runtime uses the compiler to translate the ODRL policy into multiple languages. Among these languages, one of the generated formats is compatible



**Figure 1:** Workflow for a use case with OpenFGA

with OpenFGA. Although OpenFGA supports both a DSL and a JSON to define authorization models, JSON is the executable format required by OpenFGA.

4. **Store the Authorization Model:** Once the JSON authorization model has been generated, it is stored in the Store. The uploaded model includes the access rules that OpenFGA will use to make authorization decisions.
5. **Store the Permission Tuples:** Next, the relationship tuples are written, defining the relationships between users and resources, and stored along with the authorization model in the Store.
6. **Authorization Evaluation:** Using the OpenFGA API, permission tuples are queried to assess whether a user has access to a specific resource. The API checks the relationships and rules defined in the authorization model to determine whether access should be granted.
7. **Authorization result:** Finally, OpenFGA returns a response indicating whether or not the user has the necessary permission to access the requested resource.

## 4. Conclusions and Future work

This work presents a novel extension of the ODRL framework through the ODS profile, enabling advanced authentication and authorization capabilities tailored to the requirements of Data Spaces. Furthermore, the development of a policy execution engine capable of translating ODRL policies into executable formats provides a practical solution for operationalizing governance mechanisms in decentralized environments.

Future research will focus on further refining the ODS profile to encompass additional aspects of the data lifecycle [9], integrating compliance with emerging privacy regulations, and optimizing the performance of the policy execution engine in large-scale deployments. One of the key aspects to be incorporated into the profile is the control of data usage, which will be based on the architecture defined in [10].

Another relevant aspect that has not been covered in this article is the study of possible privacy leaks derived from the use of ODRL policies. Although these policies generally do not involve the processing of personal or sensitive data, it is crucial to point out the possibility of privacy leaks through metadata. [11]. Special attention will be given to mitigating such privacy risks by carefully managing metadata within policy descriptions, ensuring compliance with the GDPR and similar regulatory frameworks.

By advancing both the expressiveness and enforceability of access control policies, this work contributes to the realization of secure, sovereign, and interoperable Data Spaces.

## Acknowledgments

The authors would like to acknowledge the support of the FUN4DATE (PID2022-136684OB-C22) project funded by the Spanish Agencia Estatal de Investigacion (AEI) 10.13039/501100011033, and the EUNOMIA Strategic Project: “Solutions for sovereignty, trust and security in data spaces” (C.128.23), result of the collaboration agreement signed between INCIBE and UPM. This initiative is carried out within the framework of the funds of the Recovery, Transformation and Resilience Plan, financed by the European Union (Next Generation). <https://eunomia.dit.upm.es>.

## Declaration on Generative AI

During the preparation of this work, the authors used Writefull-AI and DeepL in order to: Grammar and spelling check. After using these tools/services, the authors reviewed and edited the content as needed and takes full responsibility for the publication’s content.

## References

- [1] F. Eimear, M. Marco, K. Alexander, S. G. Josep, T. Brooke, M. Marina, P. S. Monica, S. Serena, T. Alessio, B. C. Jaime, et al., European Data Spaces-Scientific Insights into Data Sharing and Utilisation at Scale, Technical Report, Joint Research Centre, 2023.
- [2] S. Meckler, R. Dorsch, D. Henselmann, A. Harth, The web and linked data as a solid foundation for dataspaces, in: Companion Proceedings of the ACM Web Conference 2023, 2023, pp. 1440–1446.
- [3] I. Akaichi, W. Slabbinck, J. A. Rojas, C. Van Gheluwe, G. Bozzi, P. Colpaert, R. Verborgh, S. Kirrane, Interoperable and continuous usage control enforcement in dataspaces, in: The Second International Workshop on Semantics in Dataspaces, co-located with the Extended Semantic Web Conference, 2024.
- [4] A. Cimmino, J. Cano-Benito, R. García-Castro, Open digital rights enforcement framework (odre): from descriptive to enforceable policies, *Computers & Security* 150 (2025) 104282.
- [5] B. Esteves, H. J. Pandit, V. Rodríguez-Doncel, Odrl profile for expressing consent through granular access control policies in solid, in: 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), IEEE, 2021, pp. 298–306.
- [6] W3C, W3c data privacy vocabulary, 2025. URL: <https://w3c.github.io/dpv/2.1/dpv/>, accessed on March 25, 2025.
- [7] H. J. Pandit, B. Esteves, G. P. Krog, P. Ryan, D. Golpayegani, J. Flake, Data privacy vocabulary (dpv) – version 2.0, in: The Semantic Web – ISWC 2024, Springer Nature Switzerland, Cham, 2025, pp. 171–193.
- [8] C. Mader, J. Pullmann, N. Petersen, C. L.-B. Steffen Lohmann, F. IAIS/EIS, F. FIT, W3c international data spaces information model, 2025. URL: <https://international-data-spaces-association.github.io/InformationModel/docs/index.html#>, accessed on April 28, 2025.
- [9] D. M. Mustafa, A. Nadgeri, D. Collarana, B. T. Arnold, C. Quix, C. Lange, S. Decker, From instructions to odrl usage policies: An ontology guided approach, *Proceedings of the VLDB Endowment*. ISSN 2150 (2024) 8097.
- [10] A. Munoz-Arcentales, S. López-Pernas, A. Pozo, Á. Alonso, J. Salvachúa, G. Huecas, An architecture for providing data usage and access control in data sharing ecosystems, *Procedia Computer Science* 160 (2019) 590–597.
- [11] H. J. Pandit, B. Esteves, Enhancing data use ontology (duo) for health-data sharing by extending it with odrl and dpv, *Semantic Web* 15 (2024) 1473–1498.