Capturing Requests and Context for ODRL-based Access and Usage Control

Beatriz Esteves[1,*], Wout Slabbinck[1], Yassir Sellami[2], Andrea Cimmino[3], Víctor Rodríguez-Doncel[3] and Ruben Verborgh[1]

[1] *IDLab, Department of Electronics and Information Systems, Ghent University – imec, Ghent, Belgium*
[2] *Gaia-X, Brussels, Belgium*
[3] *Ontology Engineering Group, Universidad Politécnica de Madrid, Madrid, Spain*

Abstract

Trusted data exchange between parties requires robust mechanisms for governing how data is requested and accessed in a transparent and accountable manner across contexts. To achieve this, data exchange systems must support the interoperable expression, interpretation, and enforcement of access and usage control policies. While the W3C Open Digital Rights Language (ODRL) can capture complex policies for technical, societal and legal requirements, it currently lacks a mechanism to express requests for such data, and the context in which to evaluate the policies and requests. To address this issue, we derived key requirements for policy-based access and usage control systems to specify terms for describing: *i)* evaluation requests (formal descriptions of requested actions), and *ii)* the state of the world (knowledge representing real-world information relevant to the evaluation of the target policy or policies). We propose ontology design patterns using these terms to describe evaluation requests and the state of the world, which, in conjunction with policies, are necessary inputs for ODRL evaluators to assess which rules are active and which prohibitions and obligations have been violated or fulfilled. We demonstrate the expressiveness of our approach by analysing its coverage of the ODRL standard: while we conclude that there is no direct 1:1 mapping between ODRL concepts and the proposed request and state of the world terms, full coverage of the ODRL left operand constructs is achievable using the proposed ontology. Hence, our proposal provides the formalism required by ODRL evaluators to represent contextual information as inputs for policy evaluation, which can be used by current state of the art implementations to interoperably interpret and enforce ODRL policies. Future work includes the integration of our approach into the formal semantics work being developed in the context of the W3C ODRL Community Group, as well as its real-world usage in ODRL evaluator implementations.

Keywords

Policy evaluation, access and usage policies, context, evaluation requests, state of the world, ODRL

1. Introduction

Interoperability is paramount for the digital economy [1, 2]. Amongst others, it ensures that heterogeneous systems can consistently interpret and enforce access and usage control policies, thus enabling scalable, vendor-agnostic data integration and safeguarding against fragmentation, e.g., through the usage of open standards at both data and service levels. As described in the European Commission's European Interoperability Framework [3], interoperability governance encompasses not just the management of organisational structures, roles and responsibilities, but also refers to the administration of *"policies, agreements and other aspects of ensuring and monitoring interoperability at national and EU levels"*. Hence, to ensure its correct implementation, digital services must comprise multiple interoperability layers; from legal and organisational, to semantic and technical interoperability. Given the focus

16th Workshop on Ontology Design and Patterns (WOP 2025), co-located with the 24th International Semantic Web Conference 2025 (ISWC 2025), November 2–6, 2025, Nara, Japan

*Corresponding author.

beatriz.esteves@ugent.be (B. Esteves); wout.slabbinck@ugent.be (W. Slabbinck); yassir.sellami@gaia-x.eu (Y. Sellami); andreajesus.cimmino@upm.es (A. Cimmino); vrodriguez@fi.upm.es (V. Rodríguez-Doncel); ruben.verborgh@ugent.be (R. Verborgh)

https://w3id.org/people/besteves (B. Esteves); https://woutslabbinck.com (W. Slabbinck); http://www.cosasbuenas.es (V. Rodríguez-Doncel); https://ruben.verborgh.org/ (R. Verborgh)

0000-0003-0259-7560 (B. Esteves); 0000-0002-3287-7312 (W. Slabbinck); 0000-0002-8596-222X (R. Verborgh)

on policy-based access and usage control, this work specifically aims to address semantic and technical interoperability — while semantic interoperability ensures that the intended meaning of exchanged data is preserved and accurately interpreted by all parties involved in the exchange, technical interoperability includes the infrastructure needed to connect and integrate services, including standards for data exchange and communication [3]. Drawing on these principles, the European Commission recommends the prioritisation of metadata management, and the usage of open standards, as indispensable factors to ensure interoperability.

In this context, the Open Digital Rights Language (ODRL) [4, 5], as a W3C standard for policy expression, is already employed in various domains and initiatives, such as Solid [6, 7] and Data Spaces [8, 9, 10], primarily based on ODRL version 2.2, to define access and usage control policies. However, the policy expression alone is insufficient for accurate evaluation and enforcement. Contextual information is required to interpret a policy meaningfully. If a payment has to be made in order to play a song, the payment state needs to be verified. If a policy is valid when the policy consumer is in Spain, the consumers' location must be represented. Furthermore, if a certain action is requested, then information about the concrete request, including its requesting party or the target of the request, must be evaluated along with existing policies. Finally, context information is also required in the context of legal compliance. For instance, in the context of personal data usage, data protection regulations, such as the General Data Protection Regulation (GDPR) [11], frequently mandate the specification of a purpose to request or establish valid consent for data processing. As such, for any party creating or relying on ODRL policies, it is essential to ensure that ODRL evaluators behave deterministically, meaning they must produce identical outcomes when provided with the same contextual inputs. For example, because of missing real-world context, evaluator A could conclude that a certain mandatory action has already been performed and, hence, that the related duty was fulfilled, while evaluator B could conclude the contrary and thus resulting in a violation. Consequently, a foundational step in achieving such interoperability — and the *main contribution of this paper* — is to formally define contextual inputs of an ODRL evaluator.

To address this need, we introduce two complementary models. The *State of the World* model represents contextual information relevant to policy enforcement, including temporal, spatial, and historical aspects. The *Evaluation Request* model provides a formal description of the action to be assessed against an ODRL policy. Together, these models enhance the precision, interoperability, and practical applicability of ODRL policy evaluation in real-world data exchange scenarios. Accordingly, this article presents the first proposal of its kind to formally model contextual inputs for ODRL-based access and usage control.

The remainder of this article is structured as follows: Section 2 provides a background on ODRL, its formal semantics and existing ODRL evaluator implementations, as well as an overview of related work on Ontology Design Patterns (ODPs) related to policies. In Section 3, we define the requirements for the development of an ontology to represent evaluation requests and contextual information about the state of the world. Section 4 contains the proposed ontology and the defined ontology patterns. Section 5 discusses the expressiveness of the proposed ontology to cover ODRL 2.2 policies, as well as challenges related to dynamic constraints and the behaviour of policy-based systems. Finally, Section 6 concludes the paper and provides pointers to future research.

2. Background & Related Work

ODRL is specified in two W3C Recommendations: the *ODRL Information Model 2.2* [4] and the *ODRL Vocabulary and Expression 2.2* [5]. In addition, supplementary documents published by the community define *ODRL profiles* — extensions tailored for specific domains — propose good practices, or formalise the semantics of the language [12].

The official charter of the W3C *Permissions and Obligations Expression (POE)* Working Group — which produced ODRL 2.2 — explicitly excluded the definition of access control or enforcement mechanisms. Consequently, essential elements such as the *evaluation request*, *state of the world contextual information*, and the *evaluation result* were not specified. This omission has led to mutually incompatible implementations. By contrast, the legacy system XACML [13] represents context in the *Request Context*, an XML/JSON structure that encodes attributes of the subject, resource, action, and environment for policy evaluation. Nonetheless, this structure does not provide the necessary parameters to evaluate and enforce usage control, such as concepts to represent current time or location, focusing on access control.

The list of ODRL public implementations[1] includes the *Open Digital Rights Enforcement (ODRE)* [14] for policy enforcement in both Python and Java, the *Gaia-X Policy Decision Point*[2], the *marketdata.md* platform for managing critical business data[3], a JavaScript implementation for news information[4], *ODRL-PAP*[5], the *MOSAICrOWN* policy engine[6], the *MYDATA Control Technologies* policy engine created by Hosseinzadeh *et al.* [15], the *Prometheus-X ODRL manager*[7], *Polival*[8], and the *ODRL Evaluator* from Slabbinck *et al.* [16]. Although all of these implementations perform ODRL evaluation, they lack a common vocabulary to represent evaluation requests and state of the world information, resulting in heterogeneous implementations that do not interoperate [16]. The need for a complete representation of all the elements involved in ODRL evaluation has also been recognised by other researchers [17]. Akaichi *et al.* proposed a policy framework in which the "state of affairs" is essential [18], while Bonatti *et al.* emphasised the importance of mapping all relevant information into a formal logic system [19]. As such, the models proposed in this article represent a first step towards having interoperable representations of the contextual inputs necessary to evaluate ODRL policies.

Ontologies provide a well-established means of representing this contextual information in a structured, interoperable, and machine-readable way. By defining shared vocabularies and formal semantics, ontologies enable heterogeneous systems to interpret contextual facts — such as temporal constraints, spatial conditions, or agent roles — in a consistent manner. This semantic grounding facilitates reasoning, supports richer policy conditions, and allows the integration of data from multiple sources. Time-related aspects can be represented using temporal ontologies, locations through geospatial ontologies, and organisational roles through domain-specific vocabularies, all of which can be combined with policy models. If it is known that I am in Madrid, policies that allow me to do something in Spain will be valid because the system can reason that Madrid is in Spain.

Ontology Design Patterns (ODPs) further support this goal by providing reusable modelling solutions to recurring representation problems [20]. ODPs exist for modelling events, provenance, and spatial information, which can be adapted to capture elements of the *state of the world* relevant to policy evaluation. The use of ODPs can help ODRL evaluators adopt common, interoperable models for contextual information, reducing ambiguity, and improving cross-system compatibility. In particular, an evaluation request model enriched with well-chosen ODPs would allow implementers to express both the requested action and the relevant contextual facts using established, interoperable patterns, paving the way for deterministic and semantically robust ODRL policy evaluation.

Early work in this domain includes the *Licensing Ontology Design Pattern* [21], proposed in 2013 to capture licensing terms and constraints in a consistent manner. Building upon this foundation, the *OntCAAC (Ontology-based Context-Aware Access Control)* framework adopted semantic technologies to model dynamic contexts and their corresponding access control policies, incorporating a specialized context model tailored for access control scenarios [22]. Complementing these efforts, Mustafa *et al.* proposed an ontology-based access control model for the JADE platform, effectively combining Semantic Web technologies with context-aware policy mechanisms [23]. Similarly, Priebe *et al.* [24] extended the XACML standard by defining context information associated with access control management

[1] https://www.w3.org/community/odrl/implementations/
[2] https://wizard.lab.gaia-x.eu/policyStepper
[3] https://marketdata.md/
[4] https://github.com/nitmws/odrl-wprofile-evaltest1/
[5] https://github.com/wistefan/odrl-pap
[6] https://github.com/mosaicrown/policy-engine
[7] https://github.com/Prometheus-X-association/odrl-manager
[8] https://codeberg.org/elbtech/Polival

policies through basic operators represented in OWL, enabling more expressive authorisation evaluation requests and results. More recently, Brewster *et al.* [25] advanced this line of research by proposing *Ontology-Based Access Control (OBAC)* policies for data access based on assigned metadata, leveraging Semantic Web technologies to enhance the expressiveness and interoperability of security policies. These approaches collectively demonstrate the effectiveness of ontological representations in capturing the complex contextual elements involved in policy-based authorisation systems, including user attributes, environmental conditions, resource characteristics, and temporal constraints that influence authorisation decisions.

3. Requirements

In this section, requirements for policy-based access and usage control systems were analysed, in particular considering technical requirements for the interoperable evaluation of ODRL policies. Although the W3C ODRL Community Group has been developing a specification for the formal semantics of ODRL [12], this specification has so far defined how an ODRL evaluator should behave, especially focusing on determining what should be the output of such systems. However, to effectively compute such an output, an ODRL evaluator needs not only to consider policies, but also other contextual information. Consider this example policy: *Company X allows employees to access documents during weekdays only, from the EU.* To evaluate whether such a policy is in effect or not, an ODRL evaluator needs to use the previously mentioned policy, but also needs information about the current date and time to evaluate whether the access is being attempted on a weekday, information about the employee's whereabouts — and whether the person is actually an employee of Company X —, as well as the employee's ability to actually request said data. As such, in the following subsections, we will explore concrete requirements for both evaluation requests and state of the world contextual information.

3.1. Requirements for Evaluation Requests Representation

Considering an access control scenario, beyond the policies that specify the conditions of access of users to certain resources, an ODRL Evaluator requires a formal way to describe the action being requested, as well as the party requesting it, the targetted resource, or other contextual information. We refer to such a concept as a **Evaluation Request**.

Definition 1 (Evaluation Request)**.** *Formal description of a requested action by an assignee on a target asset, which can be enriched with further contextual information.*

While traditional access control systems focused on the first three mentioned properties, i.e., *(action, party, target)*, as the basis for the expression of access policies, modern access control systems need to be more expressive, in particular if they are to tackle more complex use cases. Namely, to cater to legal requirements, such as the transparency requirements described in the EU's GDPR [11] for the processing of personal data or in the Data Act [26] for accessing data generated through the use of connected products or related services, there is the need to express additional concepts, such the purpose of the access or the legal ground that justifies said access. As such, the possibility of expressing additional contextual constraints should also be considered as a requirement for evaluation requests. To answer these requirements, the following competency questions were formulated to guide the development of our proposed ontology:

CQR1. What is the requested action?

CQR2. Who is the party issuing the evaluation request?

CQR3. What is the target asset of the evaluation request?

CQR4. When was the evaluation request issued?

CQR5. What additional contextual information can be included in the evaluation request to further constrain it?

3.2. Requirements for State of the World Representation

Furthermore, if the policies under evaluation include *constraints* (such as temporal or spatial restrictions), involve *memberships* to asset or party collections, or require the *history* of performed actions to assess whether a duty was fulfilled or not, additional information needs to be provided to the evaluator at the time of the request. We refer to such contextual information as the **State of the World** (SotW).

Definition 2 (State of the World)**.** *Knowledge representing real-world information aiding the evaluation of ODRL Policies.* (Adapted from Slabbinck *et al.* [16]).

As such, the following competency questions were formulated to guide the development of our proposed ontology:

CQS1. What is the current time?

CQS2. What is the location of a party?

CQS3. What assets are part of the asset collection of the policy that is being evaluated?

CQS4. Which parties are part of the party collection of the policy that is being evaluated?

CQS5. What actions were already performed or attempted?

CQS6. How many times has a rule been exercised?

CQS7. What information is available about an event that has occurred?

CQS8. How long has a rule been exercised?

CQS9. Which recipients or categories of recipients can receive the result of the rule that has been exercised?

CQS10. Has a financial payment been made? What was the amount paid?

The SotW concept is quite broad and can be used to cover information about anything that might be needed for a policy evaluator to compute its output. We focused on providing a minimal list of concepts by looking at the ODRL standard, to later analyse the proposed model in terms of its coverage of the ODRL 2.2 terms. Hence, this is a non-exhaustive list of requirements, which can be further improved with demands from real-world implementations, as well as by considering additional constraints defined in ODRL profiles.

4. An Ontology for Evaluation Requests and SotW

As covered in the previous sections, there is a gap in the representation of knowledge needed to evaluate policies that determine data access and usage. In particular, when looking at the ODRL standard and the recent developments on its formal semantics, the formalisation of evaluation requests and SotW information is required to determine the output of an ODRL evaluator in an interoperable and deterministic manner. Hence, using the requirements identified in Section 3, we present an ontology, and respective *Ontology Design Patterns (ODPs)*, which include terms for the representation of such concepts.

The development of the ontology followed the *Linked Open Terms (LOT)* methodology [27], which provides a structured approach for the specification, implementation, publication, and maintenance of ontologies. This methodology builds upon established practices in Semantic Web technology development and aligns with the typical lifecycles of software engineering and research projects. The ontology is published through the *w3id.org*[9] service, which provides permanent identifiers for the Web, as well as

[9]https://w3id.org

content negotiation capabilities. This enables the delivery of both human-readable documentation and machine-readable representations from a single, stable URI. The source code is hosted on GitHub[10], with version control managed using the Git system. The ontology is available at https://w3id.org/force/sotw, under the CC BY-SA 4.0 license, and reuses available terms from the ODRL, Compliance Report [16] and DCMI Metadata vocabularies, in line with FAIR (Findable, Accessible, Interoperable, Reusable) principles.

In the next subsections, the ODPs for evaluation requests and SotW information are described in detail, and examples of their usage are provided.

4.1. ODP for Evaluation Request

Currently, the ODRL Core Vocabulary [5] does not provide the terms to describe an evaluation request. While it contains an `odrl:Request` concept in its Common Vocabulary, this concept is non-normative and, as such, not mandatory to be supported by ODRL evaluators. Moreover, this concept is a subclass of an ODRL policy, it is non-binding and could contain both permissive or prohibitive rules. Hence, since its semantics do not align with the provided description of an evaluation request, we define `EvaluationRequest` as a class in the proposed ontology with the following predicates:

Predicate	Usage
`requestedAction`	The requested action to be evaluated
`requestingParty`	The party requesting the action
`requestedTarget`	The asset on which the action is to be performed
`context`	Additional contextual information that MAY be included in the request

Since ODRL already includes a taxonomy of actions for rules, these should be reused to describe the requested actions, while the range of the properties `requestingParty` and `requestedTarget` are instances of the `odrl:Party` and `odrl:Asset` terms, respectively. Furthermore, ODRL's `Constraint` and `LogicalConstraint` structure, i.e., the *(left operand, operator, right operand)* construct and the logical operands to use multiple constraints simultaneously, can be reused to include further contextual information in evaluation requests, e.g., to give a purpose for the request or to specify the file format into which an asset will be transformed. Finally, as recommended in the ODRL standard to specify the issuance date of policies, the `dcterms:issued` property[11] can also be reused to register the time of issuance of the evaluation request. As an example[12,13], if Alice, `ex:alice`, requests to translate the asset `ex:document-1234` into French or Dutch, the `EvaluationRequest` in Listing 1 must be presented to an ODRL evaluator to determine whether this request is permitted or not.

```
ex:request a :EvaluationRequest ;
  dcterms:issued "2024-02-12T11:20:10.999Z"^^xsd:dateTime ;
  :requestedAction odrl:translate ;
  :requestingParty ex:alice ;
  :requestedTarget ex:document-1234 ;
  :context [
    odrl:leftOperand odrl:language ;
    odrl:operator odrl:isAnyOf ;
    odrl:rightOperand "fr", "nl" ] .
```

Listing 1: Evaluation Request representing Alice's wish to translate a document into French or Dutch.

[10] Source code of the ontology available at https://w3id.org/force/sotw/repo.
[11] DCMI Metadata Terms are published under the namespace http://purl.org/dc/terms/, with '`dcterms`' as its preferred prefix.
[12] The namespace https://example.org/, with '`ex`' as its preferred prefix, is being used throughout the paper for the examples.
[13] The empty prefix, '`:`', is used throughout the paper to represent the terms introduced by our ontology.

A visualisation of this pattern is presented in Figure 1.

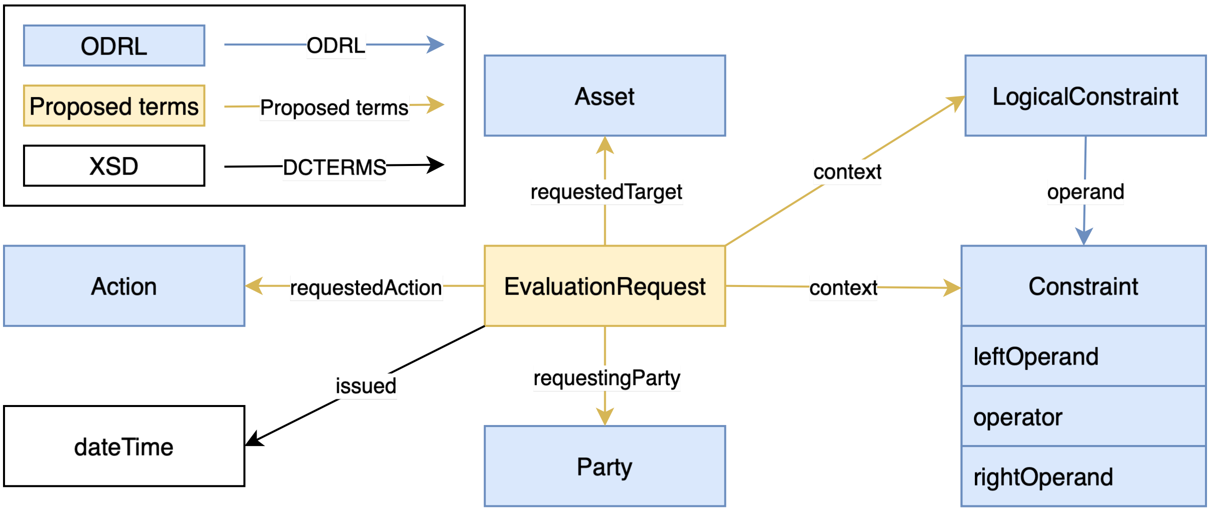

Figure 1: Evaluation Request proposed terms.

4.2. ODP for State of the World

In addition to pattern-based requests, as previously discussed in Section 3.2, formal descriptions of the state of the world are required to evaluate ODRL policies. Although it can be argued that the SotW can be represented in RDF with any relevant ontology, to promote interoperability and allow for easy extendability, we propose a core ontology of terms that cover the identified requirements. Thus, we define `SotW` as a class in the proposed ontology with the following predicates:

Predicate	Usage
`currentTime`	The current time of the state of the world
`currentLocation`	The current location of an ODRL party
`assetCollection`	An asset that is part of an ODRL asset collection
`partyCollection`	A party that is part of an ODRL party collection
`existingReport`	Existing reports from previously performed ODRL evaluations
`count`	The amount of times a rule has been exercised
`event`	Information about an event that has occurred
`accumulatedTime`	An accumulated amount of time a rule has been exercised
`recipient`	Information about a recipient of a rule that has been exercised
`paidAmount`	Information about a performed financial payment

A visualisation of this ontological pattern is presented in Figure 2. Since we do not wish to force the usage of certain vocabularies or resources to represent certain state of the world concepts, in particular for the specification of locations, recipients and events, their range is kept open to use URIs and/or strings. As an example, to evaluate a certain request, the ODRL evaluator requires information on the location of the requesting party, as well as on the recipient to which the asset is going to be transferred. Listing 2 provides an example of how such SotW can be modelled, by using the ISO 3166[14] standard to represent the location and the `dpv:AcademicScientificOrganisation` term[15] to specify which type of

[14]https://www.iso.org/iso-3166-country-codes.html, accessed on 28/July/2025.
[15]DPV [28] is published under the namespace https://w3id.org/dpv#, with 'dpv' as its preferred prefix.

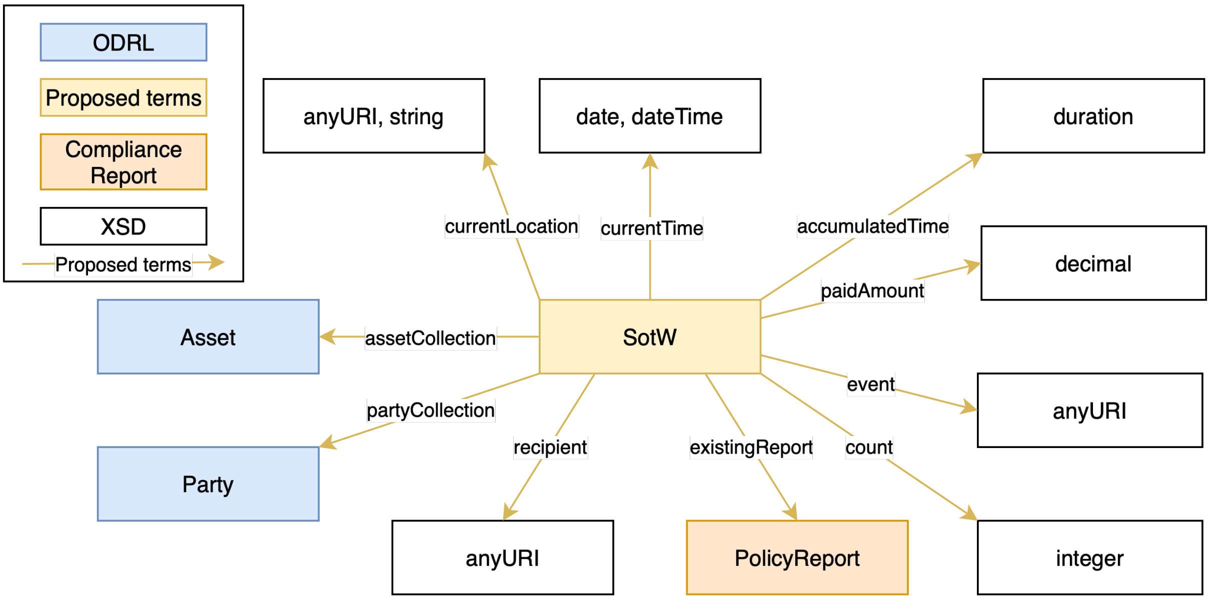

Figure 2: State of the World proposed terms.

recipient the `ex:recipient` is.

```
ex:sotw a :SotW ;
    :currentLocation <https://www.iso.org/obp/ui/#iso:code:3166:BE> ;
    :recipient ex:recipient .
ex:recipient a dpv:AcademicScientificOrganisation .
```

Listing 2: State of the world representing the location of a requesting party and a recipient.

For time-related, or numeric-bound, terms, such as the current or accumulated time and the count and paid amount terms, `dateTime`, `duration`, `integer` and `decimal` literals are expected to be used, though further information can be added if necessary though the usage of other vocabularies. Listing 3 provides an example of a SotW representation that contains a performed payment, where beyond the expected decimal value to represent the paid amount, DBpedia is used to represent the currency in which the payment was made.

```
ex:sotw a :SotW ;
    :paidAmount ex:payment .
ex:payment rdf:value "5.0"^^xsd:decimal ;
    <https://dbpedia.org/ontology/currency> <http://dbpedia.org/resource/Euro> .
```

Listing 3: State of the world representing information on a performed payment.

Moreover, to denote the memberships of party and asset collections, and as prescribed by the ODRL standard, the `odrl:partOf` property is used to assert that a certain party is a member of a certain party collection. Considering an example in which a policy states that *"Only members of Team A are allowed to read file X"*, to evaluate such a policy, the SotW needs to inform the ODRL evaluator on which team members belong to Team A. With the SotW represented in Listing 4, Alice, `ex:alice`, is allowed to read file X since she belongs to Team A, `ex:teamA`.

Finally, to represent information related to attempted and/or performed actions, e.g., to understand whether a certain duty has been fulfilled or a prohibited action performed, we propose the usage of

```
ex:sotw a :SotW ;
    :partyCollection ex:alice .
ex:alice odrl:partOf ex:teamA .
```

Listing 4: State of the world containing information on a party collection.

reports modelled with the compliance report model vocabulary[16]. This vocabulary is the state of the art resource for elaborating the output of an ODRL evaluation, as described in Section 2, since it contains the terms to describe the attempt and performance state of actions related to rules. Listing 5 presents an example of an existing report in which a duty, `ex:duty`, which states that party A needs to compensate party B, was performed, as indicated by the `report:Performed` concept, and, since this duty is active, as indicated by the `report:Active` concept, it was fulfilled by party A. If such a duty is a precondition for the execution of a permissive rule, e.g. the compensation duty needs to be fulfilled so party A can have access to a resource X, such a report needs to be provided in the SotW to the ODRL evaluator so that it has a way to check whether the duty has actually been performed.

```
ex:sotw a :SotW ;
    :existingReport ex:report .
ex:report a report:PolicyReport ;
    dcterms:created "2024-02-12T11:20:10.999Z"^^xsd:dateTime ;
    report:policy ex:policy ;
    report:ruleReport ex:dutyReport .
ex:dutyReport a report:DutyReport ;
    report:rule ex:duty ;
    report:activationState report:Active ;
    report:performanceState report:Performed ;
    report:deonticState report:Fulfilled .
ex:duty a odrl:Duty ;
    odrl:action odrl:compensate ;
    odrl:assigner ex:partyB ;
    odrl:assignee ex:partyA .
```

Listing 5: State of the world containing a report of a performed duty.

5. Discussion

5.1. ODRL 2.2 Coverage

To demonstrate the expressiveness of our approach, Table 1 presents a mapping of our proposed terms to the requirements identified as competency questions in Section 3, as well as a mapping of the proposed terms to the ODRL concepts that can be covered by such terms.

As visible in this analysis, all competency questions can be answered using the defined terms, or in case of *CQR4* by reusing the `dcterms:issued` property to express the time of issuance of an evaluation request. When it comes to the coverage of the ODRL 2.2 standard, and in particular when looking at the mapping of the state of the world concepts to existing ODRL left operands, there is no direct 1:1 mapping for all ODRL concepts. For example, the proposed SotW `currentTime` term can be used to provide temporal information to the ODRL evaluator, which in turn can evaluate policies containing ODRL constraints with `dateTime`, `delayPeriod`, `elapsedTime`, or `timeInterval` left operands. On the

[16]Compliance Report Model is published under the namespace https://w3id.org/force/compliance-report#, with '`report`' as its preferred prefix.

Table 1
Mapping of proposed terms to the identified requirements, expressed as competency questions, and coverage of the ODRL 2.2 standard.

CQ	Proposed Terms	ODRL 2.2
CQS1	`currentTime`	`dateTime, delayPeriod, elapsedTime, timeInterval`
CQS2	`currentLocation`	`spatial, spatialCoordinates`
CQS3	`assetCollection`	`AssetCollection`
CQS4	`partyCollection`	`PartyCollection`
CQS5	`existingReport`	`Duty, Action`
CQS6	`count`	`count`
CQS7	`event`	`event`
CQS8	`accumulatedTime`	`meteredTime`
CQS9	`recipient`	`recipient`
CQS10	`paidAmount`	`payAmount`
CQR1	`requestedAction`	`Action`
CQR2	`requestingParty`	`Party`
CQR3	`requestedTarget`	`Asset`
CQR4	`dcterms:issued`	—
CQR5	`context`	`Constraint, LogicalConstraint`

contrary, SotW terms such as `count`, `event`, `accumulatedTime`, `recipient`, and `paidAmount` have a direct mapping to their ODRL left operand counterparts.

The left operand constructs that are not covered in the SotW contextual information can be utilised as constraints in evaluation requests. Consider the following use case: *Bob wants to have access to a certain video stream, but only needs access to minutes 4 to 9, for the purposes of an academic research project.* While this information needs to be available to the ODRL evaluator, so that it can determine if said access is permitted, they should be modelled as `odrl:absoluteTemporalPosition` and `odrl:purpose` constraints, respectively, and provided through an evaluation request and not as part of the SotW. However, due to their less defined semantics, ODRL left operands such as the `systemDevice` or the `virtualLocation` terms, defined as *"An identified computing system or computing device used for exercising the action of the Rule."* and *"An identified location of the IT communication space which is relevant for exercising the action of the Rule"*, respectively, are arguably possible to be represented in the SotW.

As such, we can conclude that the current proposed model, either by conveying contextual information through the evaluation request or the SotW, can be used to cover the ODRL 2.2 standard left operands. Future work on the integration of the proposed model into existing ODRL evaluator implementations, as well as the exploration of additional constraints specified in ODRL profiles, will provide further real-world evaluation of the expressiveness of our approach.

5.2. Dynamic Constraints

Representing values that may change over time, i.e., dynamic values, related to certain policy constraints is a challenging task. On the one hand, the ODRL ontology does not provide any means of representing values in policies, although researchers have already discussed the need for it [17]. On the other hand, representing these values directly as triples is not feasible for data such as current time or the GPS coordinates of a requesting party who is moving, since the mere action of including them as RDF triples in the SotW might already represent an incorrect value [29].

Nonetheless, handling such dynamic values is a challenge that needs to be tackled by ODRL-based systems. Some approaches rely on introducing a meta-language on top of the ODRL policies to represent variables that are injected on the fly during the evaluation [14, 30]. However, they lack an ontological representation of these variables and, therefore, their approach is not suitable for the sake of this article. To address this challenge, a similar approach to the ODRL dynamic constraint extension introduced by Akaichi *et al.* [31], which has been successfully implemented [32] in the Slabbinck *et al.* ODRL evaluator [16], can be adopted to resolve SotW dynamic values.

5.3. Behaviour of the System

Moreover, beyond the proposed contextual inputs, the inclusion of a third input parameter should also be discussed. In this case, an ODRL evaluator could also take as an optional input a parameter that specifies the behaviour of the system in case a requested or attempted action is neither permitted nor prohibited by the Policy input being evaluated. In such a scenario, this behaviour parameter could have three values:

- **open**: in case of an open system, anything that is not prohibited is permitted;
- **closed**: in case of a closed system, anything that is not permitted is prohibited;
- **default**: the default value is closed.

Such contextualization is under debate by the W3C's ODRL Community Group and can be integrated in a future iteration of this work.

6. Conclusions

In ecosystems that adopt ODRL as a policy definition language, interoperability is a hard requirement. This necessity arises from the inherent diversity of participants, who often originate from distinct domains, industries, and regulatory environments. In addition, it is increasingly common for individual actors to engage in multiple ecosystems simultaneously, further amplifying the need for consistent and interoperable policy interpretation and enforcement. Ensuring interoperability, therefore, is fundamental to enabling trust, compliance, and seamless interaction across heterogeneous systems that rely on ODRL-based access and usage control mechanisms.

The formalisation of fundamental concepts such as the *Evaluation Request* and the *State of the World* represents a crucial first step towards enabling seamless and reliable evaluation of ODRL policies, independent of the underlying evaluator architecture or implementation technology. These concepts are currently part of the ongoing discussions within the W3C ODRL Community Group, particularly in the context of the Formal Semantics document.

Establishing such common ground not only provides a practical foundation for addressing most common use cases but also sets clear and consistent targets for the development of ODRL evaluation engines. By aligning around shared definitions and semantics, the community can cover a broader scope of the evaluation process, fostering greater interoperability, reusability, and clarity in real-world deployments. This approach complements the already extensive set of available ODRL policies, thereby advancing the standard's utility and adoption across diverse application domains.

Future work will focus on *(i)* integrating these ontologies into the works of the W3C ODRL Community Group, namely in the context of the Formal Semantics specification, to have a stable resource that reflects the consensus of the community, *(ii)* incorporate them in existing evaluators, with implementations already planned for ODRE [14], Gaia-X Policy Decision Point, and Slabbinck *et al.* ODRL Evaluator [16], and, finally, *(iii)* test them in real-world use cases.

Acknowledgments

This research was partially funded by SolidLab Vlaanderen (Flemish Government, EWI and RRF project VV023/10), and by the HARNESS project, which has received funding from the EU's Horizon 2020 research and innovation programme under grant agreement no. 101169409, https://www.harness-network.eu; and the Next Generation EU through the STICS project (09I02-03-V01).

Declaration on Generative AI

During the preparation of this work, the author(s) used Grammarly in order to: Grammar and spelling check. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the publication's content.

References

[1] M. Bourreau, J. Kraemer, M. Buiten, Interoperability in Digital Markets, Technical Report, 2022. URL: https://sitic.org/wordpress/wp-content/uploads/Interoperability-in-Digital-Markets.pdf.

[2] W. Kerber, H. Schweitzer, Interoperability in the Digital Economy, Journal of Intellectual Property, Information Technology and E-Commerce Law 8.1 (2017) 39–58. URL: https://www.jipitec.eu/jipitec/article/view/190.

[3] European Commission: Directorate-General for Digital Services, New European interoperability framework: promoting seamless services and data flows for European public administrations, Publications Office of the European Union, 2017. URL: https://data.europa.eu/doi/10.2799/78681.

[4] R. Iannella, S. Villata, ODRL Information Model 2.2 – W3C Recommendation, 2018. URL: https://www.w3.org/TR/odrl-model/.

[5] R. Iannella, M. Steidl, S. Myles, V. Rodríguez-Doncel, ODRL Vocabulary & Expression 2.2 – W3C Recommendation, 2018. URL: https://www.w3.org/TR/odrl-vocab/.

[6] B. Esteves, V. Rodríguez-Doncel, H. J. Pandit, N. Mondada, P. McBennett, Using the ODRL Profile for Access Control for Solid Pod Resource Governance, in: European Semantic Web Conference, Springer, 2022, pp. 16–20.

[7] W. Slabbinck, J. A. Rojas Meléndez, B. Esteves, R. Verborgh, P. Colpaert, Enforcing Usage Control Policies in Solid Using a Rule-Based Software Agent, in: Proceedings of the Second Solid Symposium, 2024. URL: https://ceur-ws.org/Vol-3947/short15.pdf.

[8] H. Drees, D. O. Kubitza, J. Lipp, S. Pretzsch, C. S. Langdon, Mobility data space – first implementation and business opportunities, in: ITS World Congress, 2021. URL: https://www.researchgate.net/profile/Johannes-Theissen-Lipp/publication/351519610_Mobility_Data_Space_-_First_Implementation_and_Business_Opportunities/links/610101882bf3553b29174ee6/Mobility-Data-Space-First-Implementation-and-Business-Opportunities.pdf.

[9] L. Nagel, D. Lycklama, Design Principles for Data Spaces – Position Paper, Technical Report, 2021. doi:10.5281/zenodo.5105744.

[10] V. Siska, V. Karagiannis, M. Drobics, Building a Dataspace: Technical Overview, 2023. URL: https://www.gaia-x.at/wp-content/uploads/2023/04/WhitepaperGaiaX.pdf.

[11] 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. URL: ttp://data.europa.eu/eli/reg/2016/679/oj.

[12] N. Fornara, V. Rodríguez-Doncel, B. Esteves, S. Steyskal, B. Whittam Smith, Y. Sellami, ODRL Formal Semantics – Draft Community Group Report, 2025. URL: https://w3c.github.io/odrl/formal-semantics/.

[13] B. Parducci, H. Lockhart, E. Rissanen, eXtensible Access Control Markup Language (XACML) Version 3.0, 2013. URL: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-en.html.

[14] A. Cimmino, J. Cano-Benito, R. García-Castro, Open Digital Rights Enforcement framework (ODRE): From descriptive to enforceable policies, Computers & Security 150 (2025). doi:10.1016/j.cose.2024.104282.

[15] A. Hosseinzadeh, A. Eitel, C. Jung, A Systematic Approach toward Extracting Technically Enforceable Policies from Data Usage Control Requirements:, in: Proceedings of the 6th International Conference on Information Systems Security and Privacy, SCITEPRESS - Science and Technology Publications, Valletta, Malta, 2020, pp. 397–405. doi:10.5220/0008936003970405.

[16] W. Slabbinck, J. Rojas Meléndez, B. Esteves, P. Colpaert, R. Verborgh, Interoperable Interpretation and Evaluation of ODRL Policies, in: E. Curry, M. Acosta, M. Poveda-Villalón, M. van Erp, A. Ojo, K. Hose, C. Shimizu, P. Lisena (Eds.), The Semantic Web, Springer Nature Switzerland, Cham, 2025, pp. 192–209. doi:10.1007/978-3-031-94578-6_11.

[17] A. Cimmino, N. Fornara, Improving ODRL 2.2: current limitations and theoretical solutions, in: ODRL and Beyond: Practical Applications and Challenges for Policy-based Access and Usage Control (OPAL 2025), co-located with the Extended Semantic Web Conference 2025 (ESWC 2025), 2025. URL: https://ceur-ws.org/Vol-3977/OPAL2025-6.pdf.

[18] I. Akaichi, G. Flouris, I. Fundulaki, S. Kirrane, GUCON: A Generic Graph Pattern Based Policy Framework for Usage Control Enforcement, in: A. Fensel, A. Ozaki, D. Roman, A. Soylu (Eds.), Rules and Reasoning, Lecture Notes in Computer Science, Springer Nature Switzerland, Cham, 2023, pp. 34–53. doi:10.1007/978-3-031-45072-3_3.

[19] P. A. Bonatti, N. Fornara, A. Harth, Towards a Formal Semantics of the Open Digital Rights Language (ODRL 2.2), in: ODRL and Beyond: Practical Applications and Challenges for Policy-based Access and Usage Control (OPAL 2025), co-located with the Extended Semantic Web Conference 2025 (ESWC 2025), 2025. URL: https://ceur-ws.org/Vol-3977/OPAL2025-4.pdf.

[20] A. Gangemi, Ontology Design Patterns for Semantic Web Content, in: Y. Gil, E. Motta, V. R. Benjamins, M. A. Musen (Eds.), The Semantic Web – ISWC 2005, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005, pp. 262–276.

[21] V. Rodríguez-Doncel, M. C. Suárez-Figueroa, A. Gómez-Pérez, M. Poveda-Villalón, License Linked Data Resources Pattern, in: A. Gangemi, M. Gruninger, K. Hammar, L. Lefort, V. Presutti, A. Scherp (Eds.), Proceedings of the 4th Workshop on Ontology and Semantic Web Patterns co-located with 12th International Semantic Web Conference (ISWC 2013), volume 1188 of *CEUR Workshop Proceedings*, CEUR-WS.org, Sydney, Australia, 2013. URL: https://ceur-ws.org/Vol-1188/paper_7.pdf.

[22] A. Kayes, J. Han, A. Colman, Ontcaac: An ontology-based approach to context-aware access control for software services, The Computer Journal 58 (2015) 3000–3034. doi:10.1093/comjnl/bxv034.

[23] B. S. Mustafa, N. Aldabagh, OJADEAC: An Ontology Based Access Control Model for JADE Platform, International Journal of Advanced Computer Science and Applications 5 (2014). URL: http://dx.doi.org/10.14569/IJACSA.2014.050506. doi:10.14569/IJACSA.2014.050506.

[24] T. Priebe, W. Dobmeier, N. Kamprath, Supporting attribute-based access control with ontologies, in: First International Conference on Availability, Reliability and Security (ARES'06), 2006, pp. 8–472. doi:10.1109/ARES.2006.127.

[25] C. Brewster, B. Nouwt, S. Raaijmakers, J. Verhoosel, Ontology-based access control for FAIR data, Data Intelligence 2 (2020) pp. 66–77. doi:10.1162/dint_a_00029.

[26] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (2023). URL: http://data.europa.eu/eli/reg/2023/2854/oj.

[27] M. Poveda-Villalón, A. Fernández-Izquierdo, M. Fernández-López, R. García-Castro, LOT: An industrial oriented ontology engineering framework, Engineering Applications of Artificial Intelligence 111 (2022). doi:10.1016/j.engappai.2022.104755.

[28] H. J. Pandit, B. Esteves, G. P. Krog, P. Ryan, D. Golpayegani, J. Flake, Data Privacy Vocabulary (DPV) – Version 2.0, in: G. Demartini, K. Hose, M. Acosta, M. Palmonari, G. Cheng, H. Skaf-Molli, N. Ferranti, D. Hernández, A. Hogan (Eds.), The Semantic Web – ISWC 2024, Springer Nature Switzerland, Cham, 2024, pp. 171–193. doi:10.1007/978-3-031-77847-6_10.

[29] A. Cimmino, J. Cano-Benito, R. García-Castro, Practical challenges of ODRL and potential courses of action, in: Companion Proceedings of the ACM Web Conference 2023, 2023, pp. 1428–1431.

[30] J. Cano-Benito, A. Cimmino, R. García-Castro, Injecting data into ODRL privacy policies dynamically with RDF mappings, in: Companion Proceedings of the ACM Web Conference 2023, 2023, pp. 246–249.

[31] I. Akaichi, W. Slabbinck, J. A. Rojas, C. V. Gheluwe, G. Bozzi, P. Colpaert, R. Verborgh, S. Kirrane, Interoperable and Continuous Usage Control Enforcement in Dataspaces, in: 2nd International

Workshop on Semantics in Dataspaces (SDS 2024), co-located with the Extended Semantic Web Conference 2024 (ESWC 2024), 2024. URL: https://ceur-ws.org/Vol-3705/paper10.pdf.
[32] W. Slabbinck, J. R. Meléndez, B. Esteves, R. Verborgh, P. Colpaert, May the FORCE be with you? A framework for ODRL rule compliance through evaluation, in: 2nd NeXt-generation Data Governance workshop (NXDG 2025), co-located with the 21th SEMANTiCS conference, 2025.