Ontology-Based Access Control Module for Digital Product Passports Within Built Environment

Bincy Veena, vebi23qi@student.ju.se
Jönköping University, Jönköping 551 11, Sweden

Vineetha Shajan, shvi23yw@student.ju.se
Jönköping University, Jönköping 551 11, Sweden

Abstract
Digital Product Passport (DPP) is a digital identity card for products, components, and materials, which will store relevant information to support products' sustainability, promote their circularity and strengthen legal compliance. According to recent research, DPPs are developed to enhance transparency, traceability, circularity, and sustainability throughout a product's lifecycle. However, DPPs often contain sensitive product and operational data, managing secure and stakeholder specific access is a critical challenge. This study addresses the need for fine grained access control by implementing an Ontology-Based Access Control (OBAC) approach within a modular DPP architecture. The method combines a systematic literature review and expert interviews to identify access control requirements and inform the development of a security-focused ontology module. The OBAC framework integrates semantic rules and role-based constraints using OWL and SWRL to enforce dynamic, policy-driven access. The model was evaluated through selected DPP use case and validated via reasoning, SHACL constraint checking, and expert review. The findings demonstrate that OBAC can effectively enable secure, role-sensitive data exchange in DPP systems, while supporting FAIR data principles and regulatory alignment. This work contributes a reusable semantic framework for secure DPP implementation in the built environment.
Keywords
Digital Product Passport, Ontology Based Access Control, Ontology Engineering, Semantic Web, SHACL, SWRL, Modular Ontology Modeling, Circular Economy in Construction, RDF/OWL Knowledge Graph.

1 Introduction

The built environment significantly contributes to global economic growth through infrastructure, urbanization, and innovation (Newton & Newman, 2015). As sustainability becomes increasingly important in this sector, Digital Product Passports (DPPs) have emerged as key tools for managing structured, interoperable lifecycle data to support circular economy strategies like reuse and compliance (Voulgaridis et al., 2024). Ontologies have gained attention for DPP implementation due to their ability to standardize data and enable semantic reasoning (Kebede et al. (2024); E.M. Sauter et al. (2019); Gligoric et al. (2019); Kedir et al. (2021)). Notably, Kebede et al. (2024) proposed a modular DPP ontology to overcome monolithic model limitations by reusing core ontologies and design patterns.
DPPs are designed to model comprehensive data for the circular economy, raising concerns about data security and the need for controlled access (Jansen et al. (2023); Kebede et al. (2024)). Studies identify key threats, including unauthorized access to proprietary information, data breaches exposing trade secrets, and interoperability gaps that compromise security across platforms (Jansen et al. (2023); Voulgaridis et al. (2024)). In multi-stakeholder ecosystems, access needs vary by actor and lifecycle stage, making robust, flexible access control essential. Traditional models like RBAC and ABAC lack the semantic interoperability and context-awareness required in DPPs (Brewster et al. (2020); Kirrane et al. (2017a)). Ontology-Based Access Control (OBAC) offers a dynamic, context-sensitive alternative, enabling inference-driven permissions based on roles, context, and evolving policies (Brewster et al., 2020). However, OBAC's application in DPPs, especially within the built environment, remains underexplored. This creates a critical research gap.
To address this gap, this study aims to develop an Ontology-Based Access Control Module (OBACM) integrated with the modular DPP ontology proposed by Kebede et al. (2024), tailored for the built environment. This ontology module aims to demonstrate a flexible, semantic access control mechanism that ensures secure, context-sensitive stakeholder access to product lifecycle data.
The following are the research questions developed for this study.
RQ1: What are the access control requirements associated with DPPs within built environment?
RQ2: How can an Ontology-Based access control module be developed to incorporate the necessary access control policies in DPP?
The structure of the paper is as follows: section 2 discusses the conceptual background needed for the study, gathered from literature study. Section 3 presents the research methods employed for the conduct of this study; section 4 presents the results and section 5 presents the discussion.

2 Theoretical Framework

This section outlines key theoretical concepts, DPPs in the built environment, digital access control, and relevant standards, forming the foundation for understanding how OBACM supports data governance in DPP ecosystems.

2.1 Digital Product Passport (DPP)

A DPP is defined by the European Commission (EC) as a set of data specific to a product and is accessible via electronic means through a data carrier (Regulation (EU) 2024/1781, 2024). Psarommatis & May (2024) describe it as an emerging data system that aggregates key lifecycle information to enhance transparency, traceability circularity and sustainability, while addressing the diverse informational needs of manufacturers, distributors, regulators, and end-users.These records aim to support CE practices by enabling traceability, transparency, and data-driven decision-making across the value chain. Recognizing their importance, the European Union formally introduced DPPs through Regulation (EU) 2024/1781, which mandates DPPs as part of eco-design requirements for sustainable products. In the built environment, where construction materials significantly contribute to resource consumption and waste, DPPs are positioned as a transformative tool for sustainable infrastructure development (Regulation (EU) 2024/1781, 2024). Due to the complexity and volume of lifecycle data, managing DPPs efficiently requires robust information systems (Kebede et al., 2024). Recent research by Kebede et al., (2024) advocates for a modular ontology modeling approach, breaking down the DPP into reusable modules such as Product, Material, and Environmental Impact. This approach enhances interoperability, maintainability, and alignment with industry ontologies like BOT, BPO, and MAT (Kebede et al., 2024)

2.2 Ontology Based Access Control (OBAC)

Access control systems regulate manage who is allowed to access which information and under what conditions (Kirrane et al., 2017). This is a critical requirement for DPPs which often contain sensitive business, environmental, and regulatory data (Kebede et al., 2024); (Jansen et al., 2023); (Voulgaridis et al., 2024). Traditional models such as Role-Based Access Control (RBAC) provide structured ways to define access permissions (Kirrane et al., 2017a). However, these models face limitations in dynamic, multi-stakeholder environments such as those enabled by DPPs (Brewster et al., 2020).
The study by Brewster et al. (2020) proposes OBAC which addresses these challenges, by building on RBAC, by leveraging Semantic Web technologies to add reasoning and flexibility. Rather than relying solely on predefined rules or static role assignments, OBAC enables access decisions to be inferred dynamically through ontological reasoning (Brewster et al., 2020). This allows policies to incorporate user roles, contextual metadata, and semantic relationships between entities to determine access permissions (Brewster et al., 2020). Brewster et al. (2020) demonstrate this approach in a law enforcement use case, where OBAC enables controlled access to sensitive data based on roles and metadata patterns.

2.3 Standards and Regulations

The Ecodesign for Sustainable Products Regulation (ESPR) is a legislative framework introduced by the EU, aiming to establish a comprehensive set of ecodesign requirements applicable to the widest possible range of products, components, and intermediate goods. ESPR mandates that DPPs provide both machine-readable information and enforce access control based on stakeholder roles. Stakeholders such as consumers, manufacturers, recyclers, and authorities are granted different levels of access rights (Regulation (EU) 2024/1781, 2024).
FAIR Data Principles (Findability, Accessibility, Interoperability, Reusability) ensure that DPP data can be efficiently discovered, accessed, reused, and linked across systems (Wilkinson et al., 2016). These principles are crucial for DPP ecosystems which rely on distributed data and multi-stakeholder access.

2.4 SWRL and SHACL

The Semantic Web Rule Language (SWRL) is designed as a Horn-like rule-based extension that integrates OWL DL or OWL Lite with RuleML, enabling more expressive semantic reasoning on the web (Ian Horrocks et al., n.d.). Building on this foundation, SWRL enhances the expressiveness of OWL by enabling the formulation of logical rules that go beyond the capabilities of Description Logic (Parsia et al., 2005).
The Shapes Constraint Language (SHACL) is a W3C-recommended language used to validate RDF data against a set of predefined constraints, known as shapes, which are themselves expressed in RDF (Holger Knublauch & Dimitris Kontokostas, n.d.).

3 Research Method

3.1 Literature Review

A literature review was conducted to establish a theoretical foundation and identify key information requirements (IRs) for access control and semantic security in DPPs within the built environment. The search covered Scopus, ScienceDirect, Web of Science, and Google Scholar, focusing on peer-reviewed papers from 2020–2025, with additional sources included

via cross-referencing and manual selection. Figure 1 presents the PRISMA flow diagram, and Supplementary Information 1 outlines the search strategy.

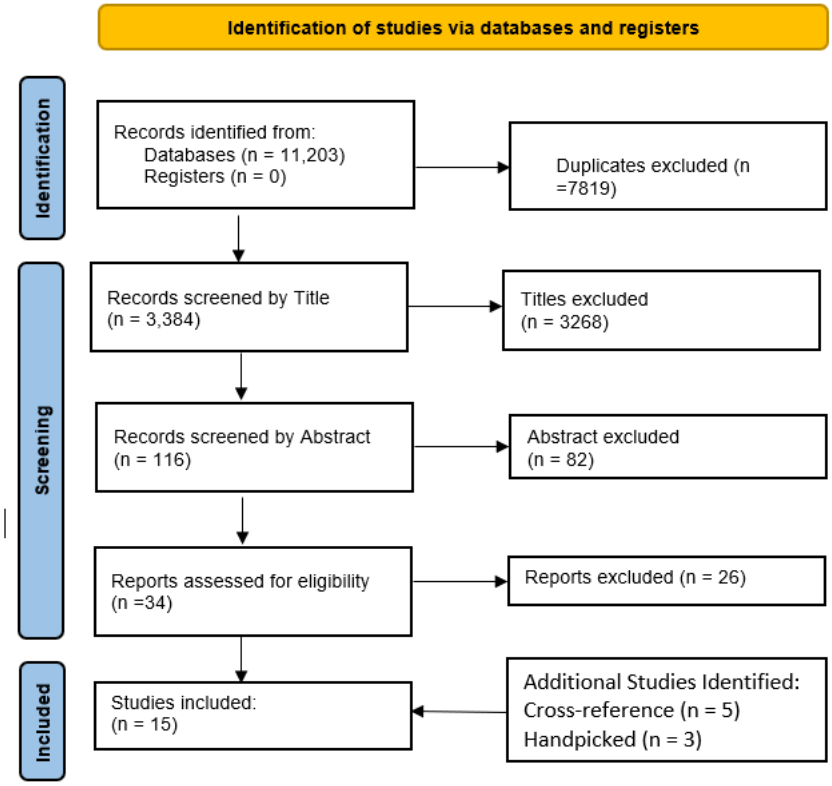

Figure. 1: PRISMA Flow diagram

3.2 Expert Interview

A semi-structured interview with predefined and open-ended questions was used to gather additional insights. The interview's objectives, participants, questions, ethics, and data analysis are outlined below.

Interview Objective and Participants

The interviews aimed to gather expert insights on access control models, policies, and user expectations for secure DPP data access. This helped identify current practices, stakeholder concerns, and areas for improvement. Experts from two domains were selected: cybersecurity professionals (preferably with ontology expertise) and those working in shared data environments like DPPs. Six experts with 2 to 40 years of experience participated. Participant details are provided in Supplementary Information 2.

Interview Questions

The interview questions were designed to align with the study's aims, with two sets tailored to the experts' backgrounds. Interviews began with general questions about participants' roles and DPP knowledge, followed by open-ended prompts to encourage detailed responses. The full list of questions is provided in Supplementary Information 3.

Ethical Considerations, Data Evaluation and Analysis

All interviews were recorded with participant consent, and confidentiality rights were communicated in advance. After transcription, response summaries were shared with participants for validation, allowing them to clarify, add, or retract information. The final responses were manually analyzed using thematic analysis, following the approach of Naeem et al. (2023). The themes identified are utilized for the conceptualization of OBACM.

3.3 Ontology Development

The ontology development in this study followed the Modular Ontology Modeling (MOMo) methodology proposed by Shimizu et al. (2023), which offers a structured and iterative approach for building modular, reusable, and interoperable ontologies. Table 1 shows the MOMo workflow adpetd from Shimizu et al. (2023).

Table 1: MOMo worflow adapted from Shimizu et al. (2023)

Step	Description	Output
Define use case	This step includes identifying the specific issue that the ontology tries to solve.	Use case description
Gather competency questions (CQs)	List natural-language questions the ontology should help answer. These clarify requirements and test if the ontology can support key queries.	List of competency questions
Identify key notions and patterns	Pinpoint central concepts that will become modules. These are derived from use cases, data, and competency questions. Also search for reusable design templates from curated libraries (like ODRL) that align with the key notions identified.	List of key notions and selected ODP(s)
Create schema diagram and conceptualization	Draft schema diagrams for each module. Visual modeling is used to facilitate communication and consensus among the team.	Schema Diagram
Document modules and axioms	Write documentation for each module, including diagrams, formal OWL axioms, and natural language explanations. This ensures clarity and reusability.	Documentation with diagrams and axioms
Creating OWL file	Translate the conceptual model into a formal OWL ontology file, typically using tools like CoModIDE or Protégé, ready for publication and use.	Final OWL file for use and publication

Protégé was used for ontology development with OWL 2 as the formal language. Existing Ontology Design Patterns like PROV-O and ODRL were reused. Classes and properties were annotated with rdfs:label and rdfs:comment, and axioms were defined using Description Logic. SWRL rules enabled dynamic permission inference, and the Pellet reasoner ensured consistency and classification. To simulate access control, semantically accurate synthetic instances reflecting ESPR policies were created.

3.4 Analysis and Evaluation Methods

The ontology was subjected to multiple validation and evaluation procedures to ensure logical consistency, structural soundness, and functional correctness of the access control logic.

Internal Consistency and Reasoning Validation

The internal consistency of the ontology was tested using the Pellet reasoner within the Protégé environment. Logical inconsistencies, such as contradictory class definitions or unsatisfiable classes, were automatically detected and then resolved.

SHACL Validation

SHACL was used to validate the ontology structure and detect missing classes that prevented the SWRL rules from executing as intended.

SPARQL Querying

SPARQL queries were used to test whether the ontology could answer the competency questions identified during early design. Executed in Protégé, the results were checked to confirm they reflected the intended semantic inferences and rules, validating OBACM's role as a policy-aware access control knowledge base.

4 Results

4.1 Literature review findings

Using a PRISMA-based approach, eight peer-reviewed articles, along with four cross-referenced and three handpicked documents, were reviewed to identify key access control requirements for OBACM. The review done by Kirrane et al. (2017a) highlighted RBAC's structured, scalable approach, but also it has limitations in dynamic, context-aware environments (Brewster et al., 2020).

To overcome these limitations, Brewster et al. (2020) proposed OBAC as a metadata-driven approach where access policies are defined over ontologies, allowing reasoning over user roles, resource types, and contextual metadata. OBAC enables fine-grained, context-sensitive access decisions and aligns well with the FAIR principles by improving semantic interoperability and auditability of access decisions (Brewster et al., 2020). Brewster et al., (2020) suggested access control decisions can be inferred from the ontology structure itself, enabling highly dynamic and modular security policies.

In addition, regulations such as the ESPR suggests the inclusion of role-based permissions in DPPs to make lifecycle data available to stakeholders for better decision making. Several access permission policies suggested by ESPR were identified for modeling in the OBACM. The following are two examples of the access control policies retrieved from ESPR. More access control policies are added as supplementary information 4.

- Recyclers are permitted to view end-of-life data
- A manufacturer is permitted to create, update, and manage the DPP for any product it places on the market.

This legislative requirement reinforces the need for a formalized and enforceable access control mechanism grounded in stakeholder roles.

The literature review also informed the identification of key access concepts used in Brewster et al (2020), including:

- User: Agent requesting access
- Role: A label representing responsibilities
- Context: user metadata (certification)
- Resource: the data being protected
- Access Policy: A rule mapping roles and contexts to allowed actions.

In summary, the literature provided both theoretical and practical guidance on defining a policy-driven access control module suitable for the evolving and multi-stakeholder nature of DPP systems. These insights directly shaped the ontology classes, properties, and rules embedded in OBACM.

4.2 Expert interview results

Table 2 shows the themes identified from the analysis. The detailed report of thematic analysis is given in the supplementary information 6.

Table 2: Themes identified using thematic analysis

Theme	Constituent codes	Description
Theme 1: Sensitivity and control of product data	Data sensitivity, trust	Emphasizes the need for regulating access to proprietary or sensitive product data to ensure confidentiality and integrity
Theme 2: limitations of traditional access models	Access models limitations	Critiques rigid role-based models like RBAC and their inability to adapt to complex stakeholder environments.
Theme 3: Demand for flexible, context aware access	Flexibility and granularity	Highlights the importance of dynamic, ontology-based access mechanisms tailored to specific roles and contexts.
Theme 4: Demand for flexible, context aware access	Security threats	Addresses the risks of data manipulation, unauthorized access, and fake DPPs, underscoring the need for strong validation system.
Theme 5: Implementation and adoption challenges	Implementation barriers, Governance	Reflects concerns around technical complexity, low industry readiness, and lack of standardized practices in deploying advanced access controls.

4.3 Development of ontology

Using MOMo methodogy, an ontology tailored to OBACM was developed, drawing on IRs identified from both literature reivew and interviews. Use case description, competency questions, keynotions and patterns and creation of owl file is described in the following subsections.

Use case description

The use case addressed in this study is as follows. “Design an ontology based access control module suiable for a modular ontology based DPP proposed by Kebede et al.(2024). The ontology manages permission to access requests from a user to DPP modules based on role-based access policies. The policies will be add conditions based on context of users to further extend the models flexibility. the policies in ontology define who can view, add, or edit specific types of DPP data, ensuring that access control is semantically transparent, and aligned with regulatory and operational requirements in the built environment”. The system architecture for OBACM, shown in Figure 2, introduces a security layer over DPP data. When a user attempts access, OBACM initiates request validation and provenance logging by capturing key credentials such as user identity, role/context, requested action, and requested asset/data. It then retrieves relevant access control policies and evaluates permissions. SWRL rules perform the policy matching, and if conditions are met, access is granted and the user is redirected to the requested DPP resource.

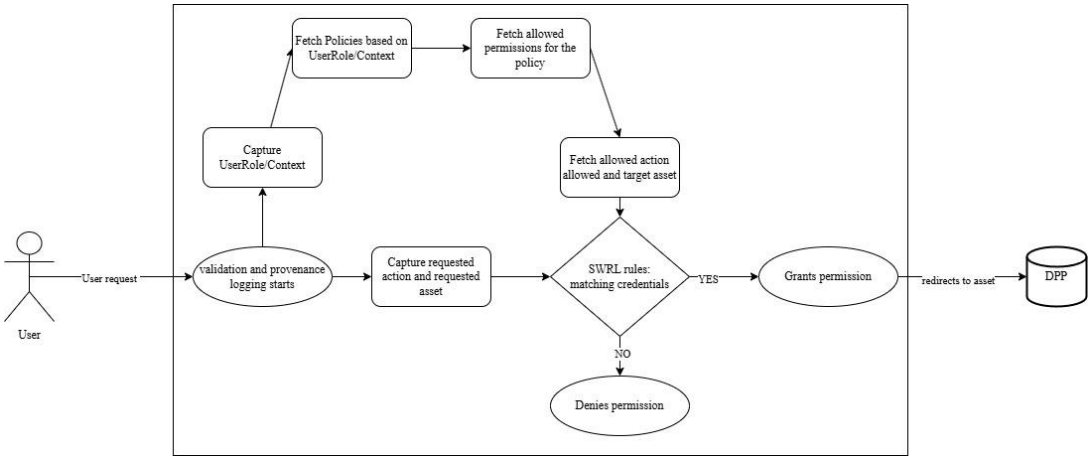

Figure. 2: System Architecture

Competency Questions

Based on the results of the literature review and interview analysis, a set of core competency questions was formulated to guide the ontology development process. These questions were designed to reflect the access control requirements of various stakeholders interacting with DPP data across the product lifecycle. More competency questions can be found in the OBACM documentation.

CQ1: What role is assigned to a user?
CQ2: What context is associated with a user?
CQ3: What are the role and context assigned to a specific policy?
CQ4: Which access control policies are assigned to a specific asset?
CQ5: What permissions does a policy have?
CQ6: What actions does a permission allow?
CQ7: Which role is allowed to do what action to which asset?
CQ8: What types of actions are modelled within OBACM?
CQ9: Who is the assignee of a specific policy?
CQ10: When does a request started?

Key notions and Pattern identification

The implementation of Ontology-Based Access Control Module (OBACM) within the modular ontology framework for Digital Product Passports (DPPs) is anchored in a set of foundational semantic notions. These notions were identified through an in-depth literature review and expert interviews, reflecting essential components required to model access control in multi-stakeholder DPP ecosystems. The table 3 shows key notions identified.

Table 3: Keynotions

Key notion	Description
User	An agent (person, organization, or system) attempting to interact with the DPP system.
Role	A designated label or classification that reflects the authority, responsibilities, or permissions granted to a user.
Action	The actions that a user or role is allowed to perform on a given resource.
Resource	The target of access, typically referring to product-related data stored within the various modules of a DPP.
Access Policy	A rule-based mechanism that assigns permissions to roles, optionally constrained by context.
Context	Additional information related to a user (e.g., certifications, organizational affiliation, regulatory compliance status) used to influence access control decisions.
Resource	The data which is being protected
User request	A request from the use to access the data within DPP

To implement these notions within a semantic web framework, two core Ontology Design Patterns (ODPs) were adopted. They are ODRL information model (W3C recommendation) and PROV-O ontology (W3C recommendation)

ODRL Information Model (W3C recommendation)

The ODRL 2.2 information model was selected as the foundational pattern for modeling access permissions and policies. It provides a flexible vocabulary for expressing policies, permissions and actions involved in a policy (Kirrane et al., 2017). The concepts of OBACM and ODRL were found matching so it can be used for modelling the policies for OBACM. Key ODRL concepts used in the study is shows in Table 4.

Table 4: Key ODRL concepts identified

Classes	Description	Matching keynotion
odrl:Policy	A container for permission statements governing access rules.	Access Policy
odrl:Permission	A statement that allows a specific action on a resource.	

odrl:Action	Actions that can be permitted/prohibitted (e.g., read, modify, write, writeTo).	Action
odrl:Assignee	The agent receiving the permission	Represents a user
odrl:Asset	The data or module being protected	The resourse

PROV-O Ontology (W3C Recommendation)

To support provenance tracking of user access and data modification events, the PROV-O ontology was adopted. It enables capturing when, how, and by whom access decisions are made, which is critical for auditability and regulatory compliance. Key PROV-O concepts used in the study is shown in the Table 5.

Table 5: Key concepts from PROV-O ontology

Classes	**Description**	**Matching keynotion**
prov:Entity	A data object or document involved in acces	Access Policy
prov:Activity	The action performed by a user	User request
prov:Agent	The user or system responsible for initiating an activity	User

Together with these patterns custom classes and properties were created according to the requirement, which is explained in conceptualizion.

Schema diagram and conceptualization

Figure.3 shows the schema diagram developed for OBACM, following the graphical conventions of Shimizu et al. (2023).

- Classes: Orange rectangles with solid border
- Datatypes: Yellow ovals with solid borders
- Subclass relationships: Dashed lines with white-headed arrows (no label)
- Other relationships: Solid lines with labeled arrowheads indicating object or data properties

OBACM governs interactions between users and DPP modules using semantically defined access policies, while integrating provenance tracking and reasoning for traceability and automation. At the core is the UserRequestAction class, representing a user's request to perform an action on DPP data. Each request links to 'odrl:Action' via 'requestedAction', 'DPPModules' (a subclass of odrl:Asset) via 'requestedAsset' and 'User' via 'requestedBy'

Users may optionally be associated with 'UserRole' via 'hasRole' or 'Context' via 'hasContext'. Lacking both association will result in denied access by default and having either one of them allows access based on policy logic.

The identified access policies (modeled as instances of AccessControlPolicy, a subclass of odrl:Policy) connect to 'User' via 'odrl:assignee', 'UserRole' via 'assigneeRole', 'Context' via 'hasCondition' and 'odrl:Permission' via 'odrl:permission'. Each odrl:Permission links to 'odrl:Action' via 'odrl:action', and an instance of 'DPPModule' via 'odrl:target'. Finally, access decisions are recorded with the 'isPermitted' data property (type xsd:boolean) on 'UserRequestAction', inferred through SWRL rules based on role, context, and policy.

Provenance is modeled using PROV-O. 'UserRequestAction' is a subclass of 'prov:Activity', 'User' is a subclass of prov:Agent. Timestamps use prov:startedAtTime. Additionally, Outcomes are stored under prov:Entity as 'AccessDecisionEntity' and linked via 'prov:value' and 'prov:wasGeneratedBy'

This schema supports dynamic and policy-aware access to DPP data, aligned with Semantic Web principles and regulatory frameworks. Following is an example policy structure in OBACM.

Policy: Recyclers are permitted to view end-of-life data (Regulation (EU) 2024/1781, 2024)

RecyclerViewEndOfLifeDataPolicy a :AccessControlPolicy;
odrl:assignee : User;
:assigneeRole :RecyclerRole;
:hasCondition :CertifiedRecycler;
odrl:permission :ViewEndOfLifeDataPermission.

For this policy to work, we should also define the following:

RecyclerRole a :UserRole.
CertifiedRecycler a: Context.
ViewEndOfLifeDataPermisson a odrl:Permission;
odrl:action odrl:read;
odrl:target :EndOfLifeData.
EndOfLifeData a DPPModule.

SWRL rule based access decision:

Since the ODRL model requires the assignee of a policy to be a actual user but OBACM supports role based policies, a SWRL rules are used assign the role based-policy to the 'User'. The SWRL rule is as follows.

OBACM:User(?u) ^ OBACM:hasRole(?u, ?r) ^ OBACM:AccessControlPolicy(?p) ^ OBACM:assigneeRole(?p, ?r) -> odrl:assignee(?p, ?u)

Following is the example of SWRL rule which helps to infer the access permittion based on UserRole.

OBACM:UserRequestAction(?request)^OBACM:requestedBy(?request,?u)^OBACM:hasRole(?u,?r)^OBACM:AccessControlPolicy(?p)^OBACM:assigneeRole(?p,?r)^odrl:permission(?p,?per)^odrl:action(?per,?act)^OBACM:requestedAction(?request, ?act) ^ odrl:target(?per, ?asset) ^ OBACM:requestedAsset(?request, ?asset) ->OBACM:isPermitted(?request, true)

A similar rule for inferring access permission based on context is also present in the model. If both the SWRL rules did not fire, the request is denied, but the model does not explicitly set isPermitted to "false" by default. To address this, the following SWRL rule was added to record both permitted and denied outcomes under AccessDecisionEntity.
OBACM:UserRequestAction(?request)^OBACM:isPermitted(?request,true)^OBACM:generatedDecision(?decision,?request) -> prov:value(?decision, "Access granted")
Similarly, another rule is present in the model to store the denied permissions under 'AccessdecisionEntity'.

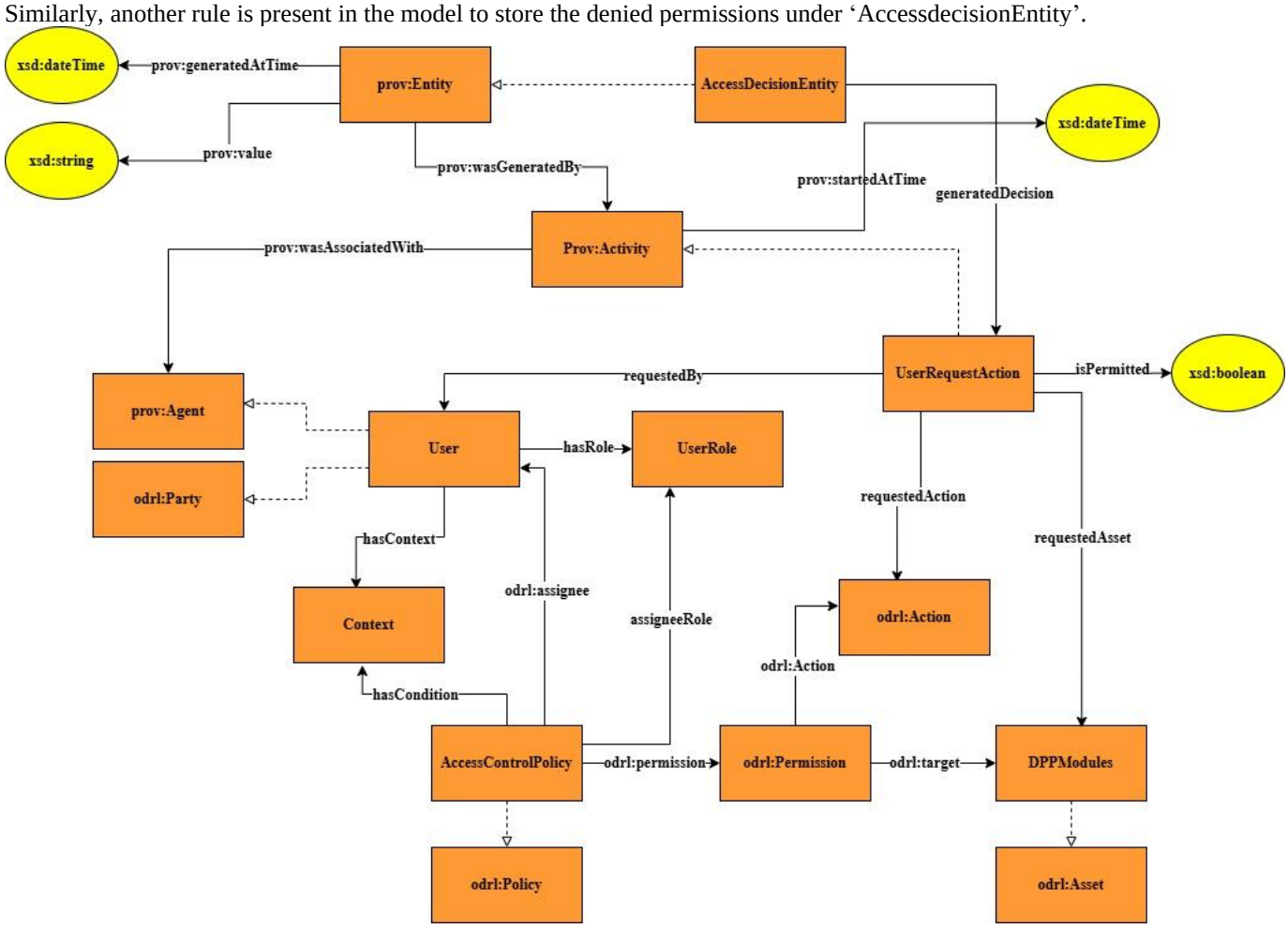

Figure. 3: Schema Diagram

Axiomatization

Since OBACM reuses ODPs, ODRL and PROV-O, the axiomatization for the model is derived from both those models. To maintain the semantic logic, minor adjustments were done in the axioms. Following Table 6 shows the adjustments made in axioms.

Table 6: Axiomatization in DL and explanation

Axiomatization in DL	Explanation
User ⊑ ∃ hasRole.UserRole ⊔ ∃ hasContext.Context	Each user must have at least one role, or one context, or both.
UserRole ⊓ odrl:Party ⊑ ⊥	UserRole and odrl:Party are disjoint (roles are not parties).

Creating OWL file

The ODRL ontology was imported first, to reuse it in the ontology, and then the owl file was created following the schema diagram. Brought in prov-o ontology later to do the required mapping. Any additional classes and properties were removed to maintain the OWL file clean and simple. The file then exported to .ttl format for further evaluation of the model. The documentation of the created ontology is attached as OBACM documentation.

4.4 Analysis and evaluation

Internal Consistency and Reasoning Validation Results

The model's internal consistency and reasoning were validated using the Pellet reasoner and SWRL rules. Access requests were created, SWRL rules executed, and the reasoner synchronized to check if the isPermitted property was correctly inferred. For example, a request by Recycler1 to view end-of-life data, assigned the role RecyclerRole and context CertifiedRecycler, successfully triggered inference of isPermitted (Refer Figure.4). Figure 5 shows the inference for decision outcome.

Recycler1 a :User;

:hasRole :RecyclerRole;
:hasContext :CertifiedRecycler.
Recycler1ViewEndOfLifeDataRequest a: UserRequestAction;
:requestedAsset :EndOfLifeData;
:requestedBy : Recycler1;
:requestedAction odrl:read.

Additional requests were created to test various scenarios, including users with only a role or context, no role or context, incorrect asset, or invalid action. All tests executed successfully, with no issues identified.

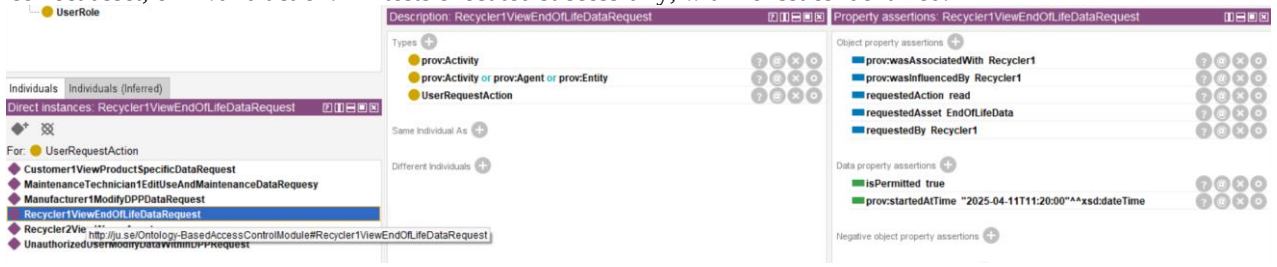

Figure. 4:Recycler1ViewEndOfLifeDataRequest after running SWRL rules

Figure. 5: Inference for decision outcome

SHACL Validation Results

A SHACL shape is created to ensure the structural completeness and correctness of access request data in OBACM ontology. The shape is used to validate all the instances of UserRequestAction by ensuring they include essential properties like requestedAction, requestedAsset, requestedBy, and a Boolean isPermitted value. Following figure shows the SHACL validation query and its results. The results shows out of 6 UserRequestAction, 4 of them violates constraints (refer Figure. 6).

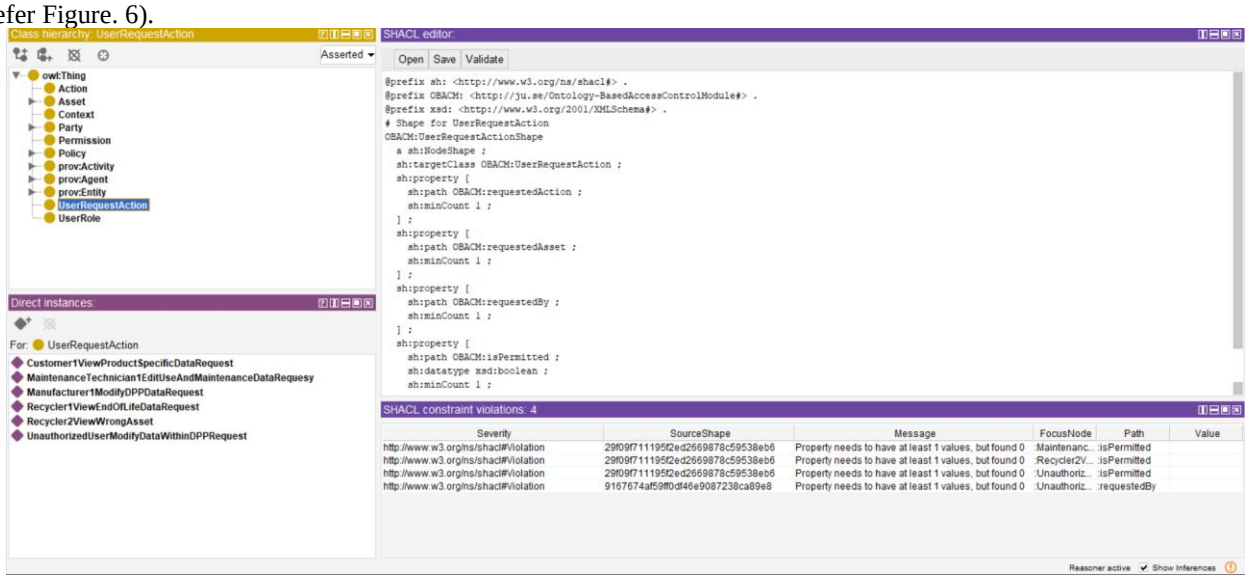

Figure. 6: SHACL Validation results

SPARQL Querying Results

The identified competency questions are formed as SPARQL queries to test the functionality of the model. An example query and result is explained below and the result obtain from the querying is shown in Figure 7.

CQ1: What role is assigned to a user?

```
PREFIX obacm: <http://ju.se/Ontology-BasedAccessControlModule#>
SELECT ?user ?role
WHERE {
  ?user a obacm:User ;
       obacm:hasRole ?role .
}
```

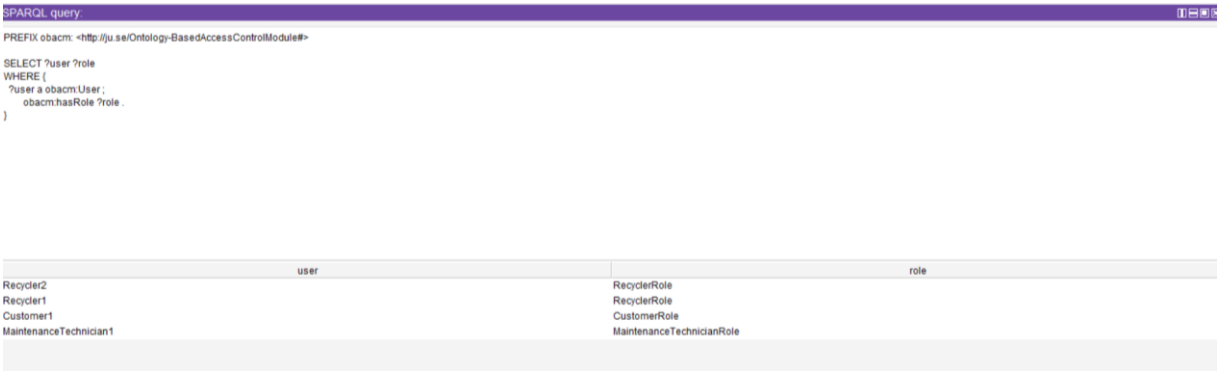

Figure. 7: Result of SPARQL Query

5 Discussion

This study explored the feasibility of OBACM as an ontology-based access control model for DPP in the built environment. Leveraging semantic technologies, ODRL 2.2, and PROV-O, OBACM enables dynamic, traceable, and flexible access decisions for sensitive data.

The primary research question examined access control requirements for DPPs in the built environment. Although direct research in this area is limited, insights were drawn from related domains through a literature review and expert interviews. Findings confirmed that role-based, policy-driven models suit data-rich systems like DPPs. However, as Brewster et al. (2020) noted, traditional RBAC lacks flexibility for dynamic contexts, a concern echoed by interviewed experts. To overcome this, Brewster et al. proposed a hybrid model combining RBAC with context-aware policies. This approach informed OBACM's design, which integrates role-based policies with contextual metadata (user's certification) for access decisions. OBACM's policies align with ESPR, which defines role-specific permissions, while its structural and functional design draws on Brewster et al.'s recommendations.

The second research question focused on developing a working OBACM prototype tailored to the modular ontology-based DPP by Kebede et al. (2024). This was achieved using Protégé, resulting in a consistent model capable of dynamically inferring permissions. Integration with PROV-O enables effective provenance tracking. The validation using Pellet and SWRL confirmed that the model is consistent since it infers the the property 'isPermitted', and successfully stores the dicision outcome. SHACL validation showed that 4 out of 6 test requests violated constraints. It was made intentionally to verify the correct inference of isPermitted = false, confirming proper system behavior. SPARQL query results further validated the model's functional performance.

This research presents a novel domain-specific extension of OBAC for DPPs in the built environment—the first of its kind. It demonstrates the use of Description Logic and SWRL for dynamic reasoning and offers a robust schema as a foundation for future implementation and broader adoption.

While the model shows strong potential, it has some limitations. Real-world access control policies may go beyond current ESPR provisions, potentially requiring structural updates to handle explicit prohibitions or conditional restrictions. The model's reliance on ODRL within Protégé may limit scalability, whereas languages like XACML, as suggested by Brewster et al. (2020), could offer more robust enforcement in complex environments. Additionally, broader expert input, particularly from DPP implementers or data owners, might have revealed more nuanced access control needs. Limited exposure to ontology-based systems among participants may have influenced the depth of responses, though the literature-based foundation helped mitigate bias.

Future research should involve a broader range of stakeholders especially data owners and DPP practitioners to uncover additional access concerns and refine policy definitions. The current model, while functional in Protégé using SWRL rules, could benefit from more advanced reasoning tools like Prolog or Answer Set Programming, which offer richer logic capabilities for handling complex rules, prohibitions, and conflict resolution. Lastly, validating the prototype on real DPP datasets within BIM or product lifecycle systems would strengthen its practical applicability.

6 Conclusions

This study demonstrated that ontology-based access control can effectively manage stakeholder permissions in modular Digital Product Passports (DPPs) within the built environment. By integrating standards like ODRL 2.2 and PROV-O, the proposed OBACM model offers a flexible, traceable, and semantically rich framework for enforcing access policies. This contributes a novel, domain-specific solution that aligns with emerging regulatory demands under the European Ecodesign framework. While the prototype provides a strong foundation, future enhancements may involve logic-based reasoning and validation with real-world DPP datasets. Ultimately, this research supports secure and transparent data sharing across complex supply chains, an essential step toward realizing the goals of a circular economy and sustainable construction practices.

References

Brewster, C., Nouwt, B., Raaijmakers, S., & Verhoosel, J. (2020). Ontology-based access control for fair data. *Data Intelligence*, *2*(1–2), 66–77. https://doi.org/10.1162/dint_a_00029

E.M. Sauter, R.L.G. Lemmens, & P. Pauwels. (2019). *CEO & CAMO Ontologies: a circulation medium for materials in the construction industry*.

Gligoric, N., Krco, S., Hakola, L., Vehmas, K., De, S., Moessner, K., Jansson, K., Polenz, I., & van Kranenburg, R. (2019). SmartTags: IoT Product Passport for Circular Economy Based on Printed Sensors and Unique Item-Level Identifiers. *Sensors*, *19*(3), 586. https://doi.org/10.3390/s19030586

Holger Knublauch, & Dimitris Kontokostas. (n.d.). *Shapes Constraint Language (SHACL)*. W3C Recommendation. Retrieved May 14, 2025, from https://www.w3.org/TR/shacl/

Ian Horrocks, Peter F. Patel-Schneider, Harold Boley, Said Tabet, Benjamin Grosof, & Mike Dean. (n.d.). *SWRL: A Semantic Web Rule Language Combining OWL and RuleML*. Retrieved May 14, 2025, from https://www.w3.org/submissions/SWRL/

Jansen, M., Meisen, T., Plociennik, C., Berg, H., Pomp, A., & Windholz, W. (2023). Stop Guessing in the Dark: Identified Requirements for Digital Product Passport Systems. *Systems*, *11*(3). https://doi.org/10.3390/systems11030123

Kebede, R., Moscati, A., Tan, H., & Johansson, P. (2024). A modular ontology modeling approach to developing digital product passports to promote circular economy in the built environment. *Sustainable Production and Consumption*, *48*, 248–268. https://doi.org/10.1016/j.spc.2024.05.007

Kedir, F., Bucher, D. F., & Hall, D. M. (2021). *A Proposed Material Passport Ontology to Enable Circularity for Industrialized Construction*. 91–98. https://doi.org/10.35490/EC3.2021.159

Kirrane, S., Mileo, A., & Decker, S. (2017a). Access control and the Resource Description Framework: A survey. In *Semantic Web* (Vol. 8, Issue 2, pp. 311–352). IOS Press. https://doi.org/10.3233/SW-160236

Kirrane, S., Mileo, A., & Decker, S. (2017b). Access control and the Resource Description Framework: A survey. In *Semantic Web* (Vol. 8, Issue 2, pp. 311–352). IOS Press. https://doi.org/10.3233/SW-160236

Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2023). A Step-by-Step Process of Thematic Analysis to Develop a Conceptual Model in Qualitative Research. *International Journal of Qualitative Methods*, *22*. https://doi.org/10.1177/16094069231205789

Newton, P., & Newman, P. (2015). Critical connections: The role of the built environment sector in delivering green cities and a green economy. *Sustainability (Switzerland)*, *7*(7), 9417–9443. https://doi.org/10.3390/su7079417

Parsia, B., Sirin, E., Cuenca Grau, B., Ruckhaus, E., & Hewlett, D. (2005). *Cautiously Approaching SWRL*.

Psarommatis, F., & May, G. (2024). Digital Product Passport: A Pathway to Circularity and Sustainability in Modern Manufacturing. *Sustainability (Switzerland)*, *16*(1). https://doi.org/10.3390/su16010396

Regulation (EU) 2024/1781. (2024). *REGULATION (EU) 2024/1781 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2024 establishing a framework for the setting of ecodesign requirements for sustainable products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC (Text with EEA relevance)*. http://data.europa.eu/eli/reg/2024/1781/oj

Shimizu, C., Hammar, K., & Hitzler, P. (2023). Modular ontology modeling. *Semantic Web*, *14*(3), 459–489. https://doi.org/10.3233/SW-222886/FORMAT/EPUB

Voulgaridis, K., Lagkas, T., Angelopoulos, C. M., Boulogeorgos, A. A. A., Argyriou, V., & Sarigiannidis, P. (2024). Digital product passports as enablers of digital circular economy: a framework based on technological perspective. In *Telecommunication Systems* (Vol. 85, Issue 4, pp. 699–715). Springer. https://doi.org/10.1007/s11235-024-01104-x

Wilkinson, M. D., Dumontier, M., Aalbersberg, Ij. J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J. W., da Silva Santos, L. B., Bourne, P. E., Bouwman, J., Brookes, A. J., Clark, T., Crosas, M., Dillo, I., Dumon, O., Edmunds, S., Evelo, C. T., Finkers, R., … Mons, B. (2016). Comment: The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data*, *3*. https://doi.org/10.1038/sdata.2016.18