Towards defining Data Usage Restrictions in the Built Environment

Gonzalo Gil[0000−0002−8988−4986] and Iker Esnaola-Gonzalez[0000−0001−6542−2878]

TEKNIKER, Basque Research and Technology Alliance (BRTA)
Iñaki Goenaga 5, 20600 Eibar, Spain
gonzalo.gil@tekniker.es, iker.esnaola@tekniker.es

Abstract. The building sector consumes about 40% of global energy, which is largely caused by buildings' operations. Research showed that providing users with detailed consumption and appliance-usage data may engage them in energy efficiency activities. To do so, data analytic services must be deployed by third parties. These services require a huge amount of data from the users in order to offer high quality services. Nevertheless, users are usually reluctant to share their data especially if its private. This is the case of those measurements performed inside the buildings, as they may be an indicative of the occupants' behaviour. In these scenarios, data sovereignty plays a key role because it provides to data owners a way to define data usage requirements and verify their compliance in a trustworthy way. In consequence, the owners' predisposition to exchange their data is expected to increase. This article takes a step forward in the development of a trustworthy ecosystem for the built environment where data sovereignty is provided. Specifically, an approach is proposed to formally specify data usage requirements for the built environment based on ontologies. Furthermore, this approach has been implemented in a real world home use case.

Keywords: Buildings · Ontology · Distributed Data Usage Control · Policy Specification

1 Introduction

The European Commission agreed a set of binding legislation inside the EU 2020 package in order to meet the energy sustainability and minimize the climate change. One of the spotlighted sectors regarding this package is the building sector which, according to the UNEP (United Nations Environment Programme), consumes about 40% of global energy and is responsible for 36% of CO_2 emissions in the EU. This energy consumption, and specially energy demand peaks, have a negative impact on operational cost and environmental aspects due to the carbon-intense generation plants that are deployed to satisfy them [3]. Certainly, demand peaks are largely caused by buildings' operations, including space and water heating, followed by appliances, cooking and lighting [2].

Demand side management activities such as load curtailment or reallocation have a huge potential to minimize these peaks, especially in the residential sector which has traditionally been largely untapped. In this regard, the increasingly penetration of Renewable Energy Sources (RES) in the energy production side, and their combination with Demand Response (DR) programs and improvement in energy storage options, could also contribute to significantly reduce peak demands. DR can be understood as the set of technologies or programs that concentrate on shifting energy use to help balancing energy supply and demand [15], and they are introduced into the smart grids so that reliable and economical operation of power systems are ensured. However, the full capabilities of the DR are yet to be unlocked in the residential sector. This is mainly caused by the heterogeneous group of end-users that conform this sector, who do not easily stay engaged with DR programs.

Research showed that providing users with historical consumption information and detailed appliance-specific consumption information contributed to the reduction of the energy consumption in the residential sector [14, 10, 1]. As a matter of fact, offering usable and attractive services may further engage users with DR programs. The quality of these services depends largely both on the quality and on the amount of data provided by the user. Additionally, shared data may also be exploited for other purposes apart from energy management, such as the development of new business models[1] including the data monetization. However, even though home occupants are aware of the benefits of these services, they may still be reluctant to share their personal data [12], specially if data sovereignty is not assured. Data sovereignty is defined as the self determination that individuals and organizations have regarding the usage of their data [8]. In order to ensure the sovereignty of exchanged data, a trustworthy ecosystem must be developed where data usage is controlled in a distributed way and the data provenance is ensured.

Traditional access control standard XACML[2] (eXtensible Access Control Markup Language) has been established as the de-facto standard for data control. However, access control mechanisms only provide control at the time of the request on provider side when the consumer requests a resource in a specific way (e.g. write or read). That is, once data access is granted, there is no control over its usage at consumer systems. In other words, access control is limited to past and present data restrictions and cannot cope with future control.

Distributed data usage control extends access control mechanisms by controlling how data is used by distributed consumers once access is granted as shown in Figure 1. Moreover, distributed data usage control is not limited to the fulfillment of a set of conditions (e.g. time-based restrictions or usage purpose). As a matter of fact, it extends to the enforcement of obligations throughout data usage. These obligations consist in a set of actions that can range from data modifications (e.g. anonymization) to system interactions (e.g. data deletion).

[1] https://op.europa.eu/en/publication-detail/-/publication/2d6d436e-4832-11e8-be1d-01aa75ed71a1/language-en
[2] http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

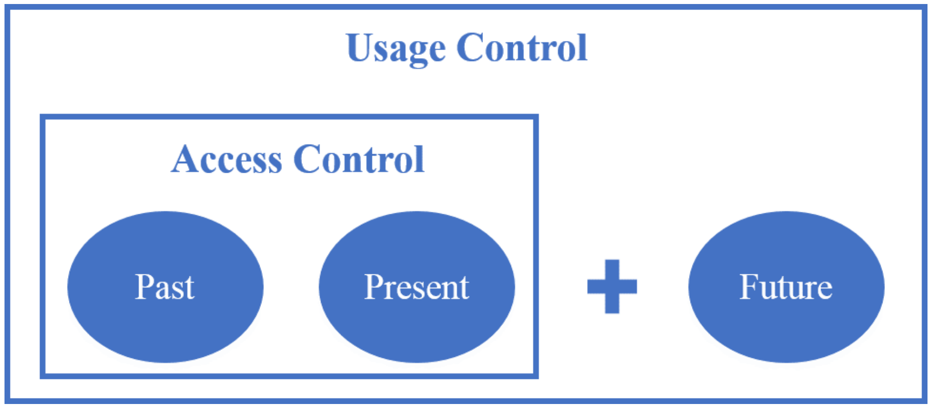

Fig. 1. Usage Control: an extension of Access Control.

Therefore, the development of a trustworthy ecosystem where data sovereignty is provided must face new challenges [7] related to distributed data usage control that are not addressed in the access control mechanisms:

- Data Usage Requirements Specification and Implementation: Human-readable data usage requirements are not directly implementable in scenarios where data is provided, exchanged and used between machines instead of humans. Therefore, the compliance with data usage requirements cannot be fully guaranteed and will only depend on the consumer's trust. To solve this issue, first, all possible human-readable data usage requirements must be specified in a formal way as a set of conditions and obligations to be readable and interpretable by machines. Second, these formal specified requirements must be translated into specific data usage policy languages in a technology-dependent way. Finally, these policies must be implemented and attached to the corresponding data at the provider side.
- Data Usage Policies Enforcement: Distributed data usage control solutions must be able to enforce all the conditions and obligations that have been previously specified and implemented, in every distributed consumer system.
- Reliability: Unlike access control, in distributed data usage control, data usage requirements are enforced at external and distributed systems where the provider has no control. Therefore, trustworthy guarantees about data usage requirements compliance must be provided to providers.

The International Data Spaces Association[3] (IDSA) is working on the development of a trustworthy open data platform where business-to-business relationships can be searched and established to provide and consume data under easily customised data usage requirements guaranteeing data sovereignty. To reach this goal, distributed data usage control plays a key role. Therefore, IDSA is working on the research of the challenges defined above.

[3] https://www.internationaldataspaces.org/

This article takes an step towards the development of a trustworthy ecosystem for the built environment where data sovereignty is provided. Regarding the aforementioned challenges, focus is placed on the data usage requirements specification. Therefore, data usage requirements implementation, enforcement and reliability related challenges are out of scope.

Data usage requirements specification recognize three issues to be solved. Firstly, the formal specification of human-readable data usage requirements in a domain-agnostic way to be readable and interpretable by machines. In nowadays digitized world, data is provided, exchanged and consumed by machines instead of humans. Therefore, if human-readable data usage requirements are not implemented on such machines, there will be no reliable way to guarantee a provider that its data is actually being used as it was originally agreed. Secondly, the assets identification and specification for specific domains, as data usage control is oriented to data sets rather than data points. Assets are economic goods generated by a participant, that can classified data points based on its value and usage requirements among others. These assets, must be formally specified for the corresponding domain. Thirdly, the formal specification of domain-agnostic data usage requirements in specific domains. In this way, data usage requirements will be applicable for a specific domain.

This article focuses on the formal specification of data usage requirements for the built environment based on IDSA's domain-agnostic approach.

The rest of the article is structured as follows. Section 2 introduces the challenges when specifying data usage requirements. Section 3 introduces a use case to illustrate the data usage control needs in a built environment scenario. Section 4 describes the proposed approach for satisfying the identified needs. Finally, conclusions of this work are described in Section 5.

2 Data Usage Requirements Specification

Traditionally, textual contracts have been enough for setting data exchange agreements between business partners. Nevertheless, in nowadays digitized world where interactions are performed between machines instead of humans, data usage requirements must be autonomously translated to be machine-understandable. Otherwise, their compliance cannot be guaranteed. Therefore, higher degrees of formalization are needed to autonomously negotiate, specify, implement and enforce data usage requirements. Figure 2 represents different degrees of formalization for data usage requirements. The first or lowest level of formalization belongs to traditional human-readable textual-contracts whose limitations have been previously identified. The second level comprises the descriptive policies which refer to machine-readable representations of these contracts (e.g. in JSON or XML format). However, the content of these policies must be manually translated to be at least interpretable by machines. In the third level, the formal policies extend these machine-readable policies by including specifications such as a consistent semantic provided by, for example, RDFs (Resource Description Frameworks). Even though formal policies are interpretable by enforcement points, they must be translated into specific data usage policy languages of existing technologies to be enforceable. In the fourth level, the enforceable policies are made based on translations from formal policies in a technology-dependent way in order to be autonomous enforceable. Finally, the autonomously negotiated policies allow the negotiation of data usage requirements without human interactions. This article focuses on reaching the level of formalization related to formal policies for the built environment.

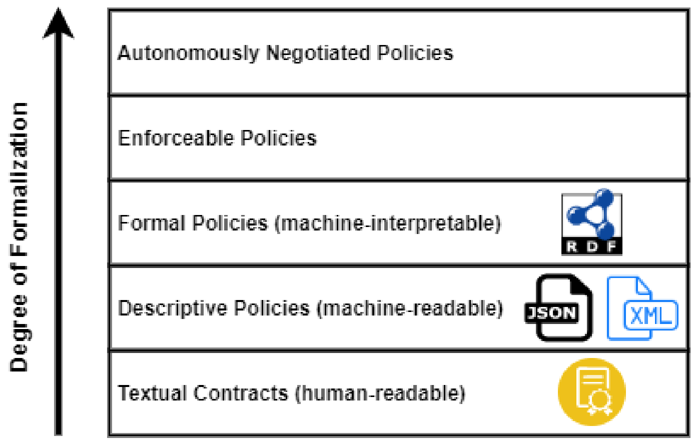

Fig. 2. Degree of formalization of business process contracts.

2.1 IDSA Approach

The IDSA defines the IDS Information Model[4], a domain-agnostic common language for the semantic description of the participants and components within the IDSA, which includes the specification of data usage requirements. This Data usage requirement specification is based on the ODRL (Open Digital Rights Language) Information model 2.2[5], a W3C recommended policy expression language that provides a vocabulary and data model for the description of machine-readable contracts. Moreover, the IDS Information Model extends it towards data usage control descriptions and enforcement.

IDSA define the concept of contract (*ids:Contract*), a subclass of a Policy (*odrl:Policy*), that is an abstract set of rules (*ids:Rule*) which are comprised of permissions (*ids:Permission*), prohibitions (*ids:Prohibition*) and duties (*ids:Duty*). Each of these rules describes an action (*ids:Action*) that stakeholder (*ids:Participant*) might be permitted or prohibited to do on a digital content

[4] https://w3id.org/idsa/core
[5] https://www.w3.org/TR/odrl-model/

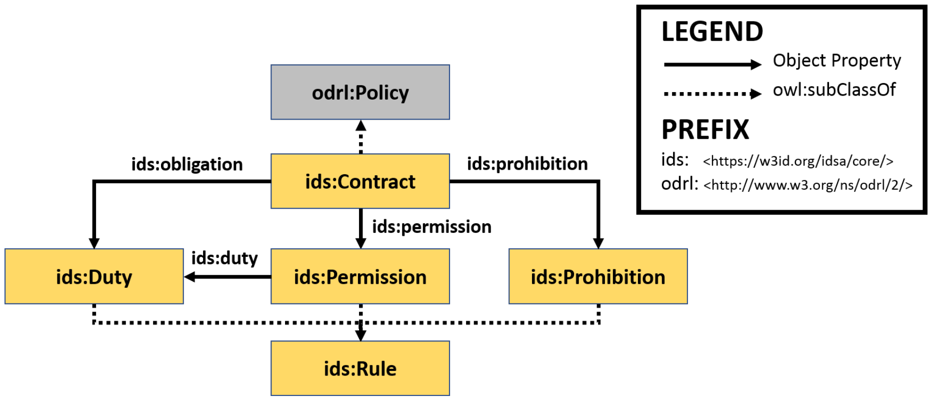

Fig. 3. IDS Policy Concept.

(*ids:DigitalContent*) under certain constraints (*ids:Constraint*). This basic contract representation is shown in Figure 3.

As previously mentioned, the IDS Information Model is generic, with no commitment to any particular domain. That is, the domain knowledge has to be modelled or imported from other existing vocabularies. In this article, focus is placed on the specification of data usage requirements for the built environment to define formal policies based on this IDSA's approach.

3 Use Case

The RESPOND H2020[6] project aims to deploy an interoperable energy automation, monitoring and control solution to deliver DR programs at a dwelling, building and district level to neighborhoods across Europe.

The use case presented in this article focuses on a home located in the Aran Islands (Ireland) participating in the RESPOND project (from now on referred to as Aran_01). In this use case, home occupants are provided with their household-related information via the RESPOND Mobile App[7] and they can interact with the devices deployed in the home such as switching appliances on or off. Among other relevant information, occupants can visualize the electrical consumption and comfort measurements during a specific time (both raw data or summarized as aggregated data), as well as the recommended optimal electrical consumption profile. This optimal profile is generated taking leverage of different data analytic services developed by technology providers, including the electricity demand forecasting, renewable energy production forecasting and optimization services. For the development of these analytic services, technology providers

[6] http://project-respond.eu/

[7] http://project-respond.eu/personal-energy-performance-assistant-version-1-13-released/

needs data that must be exchanged between the different stakeholders involved in this process. Therefore, some business relationships needs to be agreed.

Next, the stakeholders involved in the use case, the assets exchanged and the established agreements are described.

3.1 Stakeholders

The stakeholders identified in the Aran_01 use case play different roles as follows:

- Owner: The person or company that owns the home or the building.
- Occupant: The person who lives in the home. He/She may be the owner of the home or not, if it is rented. He/She is the data owner of the monitored data on building behaviour and the data consumer of the results received from the analytic services.
- Technology Provider: Third parties that provide hardware and/or software services. They can be classified into two different categories:
  - Data Acquisition Service Providers: The companies that provide the service needed to obtain and exchange data with other parties, but never use the data. They are the data providers.
  - Analytic Service Providers: The companies that provide data analytic services based on the data. They are the data consumers of the monitored data on building behaviour and the data owners/providers of the results obtained from the analytic services.

Regarding the stakeholders and their roles, the Aran_01 dwellers are the owners and the occupants of the home. Energomonitor SRO[8] from the Czech Republic, TEKNIKER[9] from Spain and Institut Mihajlo Pupin[10] (PUPIN) from Serbia are the technology providers. On the one hand, Energomonitor is a data acquisition service provider. Even tough Energomonitor provides the devices and the gateways that make and send measurements to data consumers, the Aran_01 user is the owner of this data. Therefore, the Aran_01 user has the right to define textual contracts related to home data. On the other hand, TEKNIKER and PUPIN are the analytic service providers. Their services include the generation of optimized energy profiles for electricity consumption management [6]. Moreover, TEKNIKER offers comfort services that will provide the average temperature of the home.

3.2 Assets

The assets are the data sets exchanged between the stakeholders. These, can be classified as follows:

- Temperature: Measurements related to the temperature in the home which includes:

[8] https://www.energomonitor.com/
[9] https://www.tekniker.es/
[10] http://www.pupin.rs/

  - Raw data: The temperature measured by a temperature sensor.
  - Comfort data: The average temperature of all the temperature sensors of the home.
- Electrical Demand: The measurements related to the electricity consumed by the home which includes:
  - Raw data: The electrical demand measured by an electricity meter.
  - Aggregated data: The average value of raw electrical demand data aggregated for a given period of time (e.g. 1h).
  - Forecast data: The predicted electrical demand based on one-hourly aggregated electrical demand data.
- Electrical Production: The measurements related to the electricity produced by the PV panels installed in the house, which includes:
  - Raw data: The electricity produced by the PV panels.
  - Forecast data: The predicted electrical production based on the raw electrical production data.
- Electrical Optimized Profile: The optimal electric demand curve with views to maximizing the renewable energy exploitation and minimizing electric demand peaks.

3.3 Agreements

To reach the main goal of the use case, the stakeholders identified need to establish agreements between them for data exchange. Figure 4 shows the assets exchanged in every agreement between the different stakeholders.

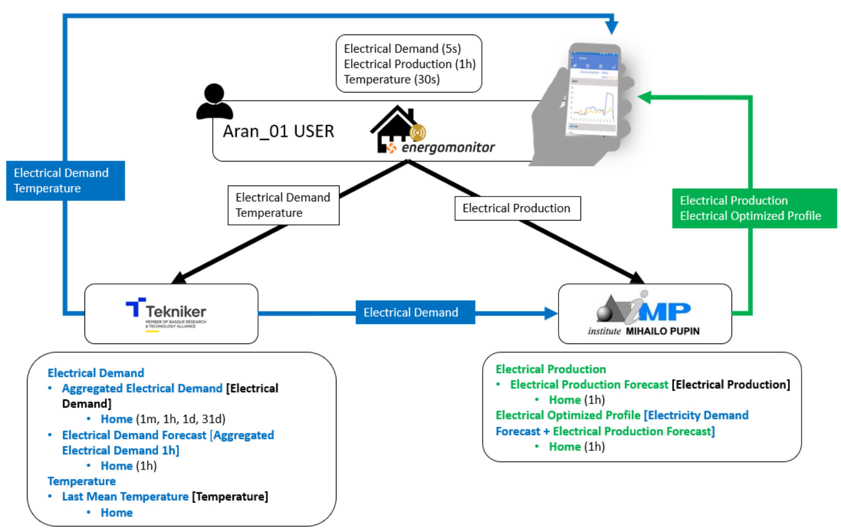

Fig. 4. Stakeholders business relationships.

Firstly, the Aran_01 user is the owner of the raw temperature measured every 30 seconds by the temperature sensors deployed in different rooms of the home, the raw electrical demand measured by the electricity meter every 5 seconds and the raw electrical production of the PV panels measured every hour. The Aran_01 user establishes a relationship with TEKNIKER and PUPIN for the exploitation of the data. On the one hand, TEKNIKER needs raw temperature data to provide the comfort service, and raw electrical demand for generating electrical demand aggregated data, which will be further used by TEKNIKER for the electrical demand forecasting service. For that purpose, the Aran_01 user grants TEKNIKER the raw temperature data usage for comfort purposes and electrical demand data usage for aggregation purposes, as long as this data is used before RESPOND project's ending date (i.e. 2021-01-01). Moreover, the Aran_01 user prohibits TEKNIKER from sharing the raw electrical demand data. On the other hand, PUPIN needs the electrical production raw data in order to provide the electrical production forecasting service. For that purpose, the Aran_01 user grants PUPIN the raw electrical production data usage for prediction purposes. Similar to the requirements set to TEKNIKER, PUPIN can only use the data prior to the RESPOND project's ending, and cannot share the data.

Secondly, TEKNIKER establishes a relationship with the Aran_01 user for comfort and forecasted data visualization, and with PUPIN for data exploitation purposes. On the one hand, the Aran_01 user is only allowed to use the electrical demand and the for mobile app visualization. Moreover, TEKNIKER forbids the Aran_01 user from sharing this data. On the other hand, PUPIN needs the electrical demand forecast data, in order to exploit it for providing the optimization service. Towards that goal, TEKNIKER allows PUPIN using the electrical demand forecast data only for optimization purposes, as long as it is used before the ending of the project. The sharing of this data is forbidden.

Finally, PUPIN establishes a relationship with the Aran_01 user for sending the results of the electrical production forecast service and the electrical optimized profile, so that they can be visualized in the RESPOND Mobile App. For this purpose, PUPIN allows the Aran_01 user visualizing the forecasted electrical production data and the optimized profile, but the sharing of this data is prohibited.

Therefore, as a result of the data exchanged between the different stakeholders, the Aran_01 user can visualize its own data, as well as aggregated, forecasted and optimized data provided by third parties.

4 The RESPOND approach

In order to represent and formalize the use case's data usage requirements, the IDS Information Model is used. However, as mentioned before, this ontology domain-agnostic, so it is not enough to represent the assets to which data usage requirements apply. Therefore, in order to represent all the necessary information, the RESPOND ontology [5] is used. The RESPOND ontology's core is developed by reusing and extending three well-known ontologies: BOT[11] [13] to represent the dwelling topology, and SAREF[12] [4] and SEAS Feature Of Interest[13] [9] ontologies to represent devices, features of interest and qualities monitored and controlled by sensors and smart appliances. However, there were other RESPOND requirements that remained unsolved and a set of new axioms had to be defined to satisfy them by extending the list of appliances, observed qualities or units of measurement to name a few. Figure 5 shows the main classes and properties of the RESPOND ontology.

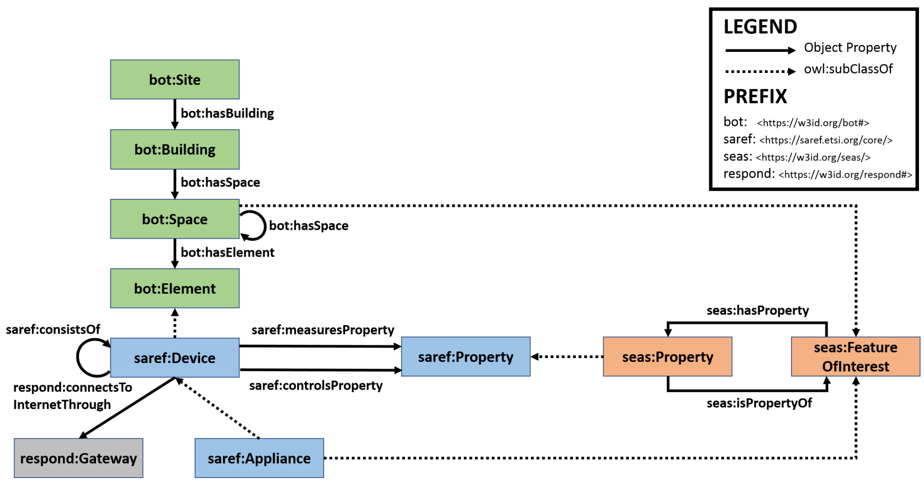

Fig. 5. RESPOND ontology's main classes and properties.

As part of other RESPOND project developments, every participant dwelling and neighbourhood is represented with appropriate ontological terms. This information remains accessible in an Openlink Virtuoso Server[14] version 07.20.3217 for its further exploitation by other services via SPARQL queries.

In order to showcase the machine-interpretable definition of formal policies, the contract between the Aran_01 user and TEKNIKER (described in the previous section) has been considered. This contract comprises two rules: a permission and a prohibition. This is represented with the following triples:

```
:contract002AZ63 rdf:type ids:Contract;
    ids:permission :permission25;
    ids:prohibition :prohibition43.
:permission25 rdf:type ids:Permission.
:prohibition43 rdf:type ids:Prohibition.
```

[11] https://w3id.org/bot
[12] https://saref.etsi.org/core
[13] https://w3id.org/seas/FeatureOfInterestOntology
[14] https://virtuoso.openlinksw.com/

The permission defines that TEKNIKER can use the Aran_01 user's demand data for aggregation purposes until the end of the project, that is, prior to the year 2021. This permission is represented with the following triples:

```
:permission25 ids:action ids:READ;
    ids:assignee :partner_TEKNIKER;
    ids:assigner :aran_01:
    ids:constraint :constraint_p25_01;
    ids:constraint :constraint_p25_02;
    ids:targetContent :aran_01_demand.
:constraint_p25_01 rdf:type ids:Constraint;
    ids:leftOperand ids:purpose;
    ids:operator idsa:EQ;
    ids:rightOperand "Aggregation Purposes"^^xsd:String.
:constraint_p25_02 rdf:type ids:Constraint;
    ids:leftOperand ids:now;
    ids:operator idsa:BEFORE;
    ids:rightOperand "2021-01-01T00:00:00Z"^^xsd:dateTimeStamp.
```

As it can be seen, the contract defined using the IDS Information Model ontological terms is assigned to the *aran_01_demand* individual, which represents the electrical demand of Aran_01. As mentioned before, Aran_01 and the rest of the RESPOND participant dwellings are described and stored in the Virtuoso triplestore. Next, a simplified RDF representation of Aran_01 is shown:

```
:irishSite rdf:type bot:Site;
    bot:hasBuilding :aran_01.
:aran_01 rdf:type bot:Building;
    bot:hasElement :aran_01_electricityMeter.
:aran_01_electricityMeter rdf:type saref:Device;
    saref:measuresProperty :aran_01_demand.
:aran_01_demand rdf:type saref:Property.
```

Regarding the second rule of the aforementioned usage restriction, it defines that TEKNIKER cannot share the Aran_01 user's electrical demand data. This rule can be represented with these triples:

```
:prohibition43 ids:action ids:DISTRIBUTE;
    ids:assignee :partner_TEKNIKER;
    ids:assigner :aran_01:
    ids:targetContent :aran_01_demand.
```

5 Conclusions

Nowadays, the inefficient operation of buildings makes the building sector responsible for the consumption of about 40% of the global energy. According to recent research, this consumption could be reduced if building occupants are informed about their energy consumption and appliance-usage, as this information could improve the user engagement in energy efficiency activities. Furthermore, the data collected by the smart home solutions could then be exploited to provide users with added-value services to further engage them in this kind of activities. However, users are not eager to share their data unless data sovereignty is ensured.

With the proposed approach, which is based on IDSA's domain-agnostic data usage requirements specification approach, it has been demonstrated that machine-interpretable formal policies can be defined in a built environment scenario for every relationship established between stakeholders. In this way, a step towards the development of a trustworthy ecosystem in the built environment has been taken. Therefore, not only B2B data exchange models are boosted, but also, high-quality analytic services and the energy consumption optimization as a consequence.

5.1 Future Work

The presented work paves the way towards future research in two different aspects.

Both practice and research suggests the use of a graph-based format to capture building data, nevertheless keeping numeric data explicitly out of the semantic graph for computational performance reasons [11]. Without having the semantic representation of those numeric data, the definition of assets must be done at a quality level (e.g. temperature or humidity), thus a more fine-grained asset definition is not possible. Therefore, stakeholders cannot specify policies at a measurement type level (e.g. raw temperature, aggregated temperature or forecasted temperature data). This research line is worth being further investigated.

The IDSA approach is limited to the semantic representation of human-readable usage control requirements into machine-interpretable policies. In the line of research related to the automatic specification and implementation of human-readable data usage requirements, two main challenges will be studied. On the one hand, the development of user-friendly templates which will autonomously specify the data usage requirements based on the formal specification proposed. On the other hand, before the implementation of data usage policies in a technology-dependent way, a translation must be done in order to make specified data usage requirements enforceable by specific technologies. The LUCON open source usage control technology[15] is not able to translate machine-intepretable policies into enforceable policies. LUCON will be studied in order to develop a translator which will allow the implementation of technology-dependent policies from the specified data usage requirements.

References

1. Abrahamse, W., Steg, L., Vlek, C., Rothengatter, T.: The effect of tailored information, goal setting, and tailored feedback on household energy use, energy-related

[15] https://industrial-data-space.github.io/trusted-connector-documentation/docs/usage_control/

behaviors, and behavioral antecedents. Journal of environmental psychology **27**(4), 265–276 (2007)
2. Agency, I.E.: Transition to Sustainable Buildings (2013). https://doi.org/https://doi.org/https://doi.org/10.1787/9789264202955-en, https://www.oecd-ilibrary.org/content/publication/9789264202955-en
3. Collins, L.D., Middleton, R.H.: Distributed demand peak reduction with non-cooperative players and minimal communication. IEEE Transactions on Smart Grid (2018). https://doi.org/10.1109/TSG.2017.2734113
4. Daniele, L., den Hartog, F., Roes, J.: Created in close interaction with the industry: the smart appliances reference (saref) ontology. In: International Workshop Formal Ontologies Meet Industries. pp. 100–112. Springer (2015). https://doi.org/10.1007/978-3-319-21545-7_9
5. Esnaola-Gonzalez, I., Diez, F.J.: Integrating building and iot data in demand response solutions. In: Proceedings of the 7th Linked Data in Architecture and Construction Workshop (LDAC 2019). vol. 2389, pp. 92–105. CEUR (2019)
6. Esnaola-Gonzalez, I., Diez, F.J., Pujic, D., Jelic, M., Tomasevic, N.: An artificial intelligent system for demand response in neighbourhoods. In: Proceedings of the Workshop on Artificial Intelligence in Power and Energy Systems (AIPES 2020) (Under Review)
7. Gil, G., Arnaiz, A., Higuero, M.: Towards assesment of existing frameworks for data usage control: Strength and limitations with respect to current application scenarios. In: IoT Connected World Semantic Interoperability Workshop (IoT-CWSI) (2019)
8. Jarke, M., Otto, B., Ram, S.: Data sovereignty and data space ecosystems. Business Information Systems Engineering **61** (08 2019). https://doi.org/10.1007/s12599-019-00614-2
9. Lefrançois, M.: Planned etsi saref extensions based on the w3c&ogc sosa/ssn-compatible seas ontology patterns. In: Proceedings of Workshop on Semantic Interoperability and Standardization in the IoT, SIS-IoT, (July 2017)
10. Peschiera, G., Taylor, J.E., Siegel, J.A.: Response–relapse patterns of building occupant electricity consumption following exposure to personal, contextualized and occupant peer network utilization data. Energy and Buildings **42**(8), 1329–1336 (2010)
11. Petrova, E., Pauwels, P., Svidt, K., Jensen, R.L.: In search of sustainable design patterns: Combining data mining and semantic data modelling on disparate building data. In: Advances in Informatics and Computing in Civil and Construction Engineering, pp. 19–26. Springer (2019)
12. Ranade, V.V., Beal, J.: Distributed control for small customer energy demand management. In: 2010 Fourth IEEE International Conference on Self-Adaptive and Self-Organizing Systems. pp. 11–20. IEEE (2010)
13. Rasmussen, M.H., Pauwels, P., Hviid, C.A., Karlshøj, J.: Proposing a central aec ontology that allows for domain specific extensions. In: Joint Conference on Computing in Construction. vol. 1, pp. 237–244 (2017). https://doi.org/10.24928/JC3-2017/0153.
14. Ueno, T., Sano, F., Saeki, O., Tsuji, K.: Effectiveness of an energy-consumption information system on energy savings in residential houses based on monitored data. Applied Energy **83**(2), 166–183 (2006)
15. Warren, P.: A review of demand-side management policy in the uk. Renewable and Sustainable Energy Reviews **29**, 941 – 951 (2014). https://doi.org/10.1016/j.rser.2013.09.009