Semantic Interoperability, a Key Enabler for Good Quality Distributed Usage Control

Gonzalo Gil[1] [0000-0002-8988-4986], Iker Esnaola-Gonzalez[1] [0000-0001-6542-2878]

[1] Tekniker, Basque Research and Technology Alliance (BRTA), Iñaki Goenaga 5, 20600 Eibar, Spain
gonzalo.gil@tekniker.es

Companies operating in different sectors and of different sizes have already highlighted the great benefits that Business-to-Business (B2B) data sharing presents to enhance their activities [5]. These include, among others, the improvement in the design of their products and services as well as the generation of new business models. Thus, the European Commission is promoting the creation of distributed and collaborative European Data Spaces [8] in which data owners could provide their data to end users under specific restrictions in a trustworthy way. As a result, data economy, competitiveness and innovation would be boosted at European level.

One of the main factors that may jeopardize the adoption of data spaces is the reluctance of data owners to share their data. This is motivated by the fact that they lose the control over their data once this reach the end user infrastructure to be exploited. Therefore, the self-determination of individuals and organizations regarding the usage of their data or also called data sovereignty [6] emerges as a fundamental need. In this regard, enabling technologies focus on the extension of Access Control (AC) towards Distributed Usage Control (DUC) [1]. However, the development of good quality DUC technologies that optimally ensures data sovereignty presents a set of challenges that must be addressed.

The AC research literature [7] has already identified that the implementation of policies without mistakes or also called good quality policies highly impact on the quality of AC. This is due to the relationship that low quality policies have on the appearance of first, security breaches leading to unauthorized data disclosure and denial of legal access and second, performance issues requiring longer policy enforcement time. Understanding DUC as an extension of AC, the quality of the policies is further affected by additional challenges. In particular, the extended expressiveness of the DUC model and the complexity introduced in the B2B policy implementation process are the most important.

To face these challenges, guaranteeing the semantic interoperability is essential. The semantic interoperability ensures that the meaning of the information exchanged is understandable by any other application that was not initially

developed for such purpose. In this way, systems can combine the policies received from several resources and process them by exploiting their underlying semantics. The natural way to achieve the interoperability of information at a semantic level is to annotate such information with ontologies or vocabularies, which allows to a better representation, structuring them and establishing formal types, relations, properties, and constraints between them. Furthermore, a piece of information annotated with ontologies is provided with explicit and unambiguous semantic, which is key for ensuring a common understanding in data exchange scenarios.

To make a more comprehensive analysis of the importance of semantic interoperability for good quality DUC, we present below a wind energy usage case in which data sovereignty is ensured by implementing DUC in a trusted IDSA (International Data Spaces Association) ecosystem. From this use case, we describe the issue that the expressiveness of the DUC model introduces for good quality policy implementation. Finally, we demonstrate how this becomes even more critical in the process of implementing B2B policies.

Wind Energy Use Case

In the wind energy domain, the wind farm competitiveness is closely connected with the maintenance of the wind turbines. In turn, the gearbox is one of the components that has a major impact on the wind turbine performance. Thus, sharing gearbox related data, which is often retained by wind farm operators and OEMs, with other stakeholders of the value chain such as the component supplier is of great interest, for example, to improve the component design.

In Figure 1, we present a use case in which gearbox health status data is estimated at the edge from condition data that has been monitored at the gearbox lubrication system.

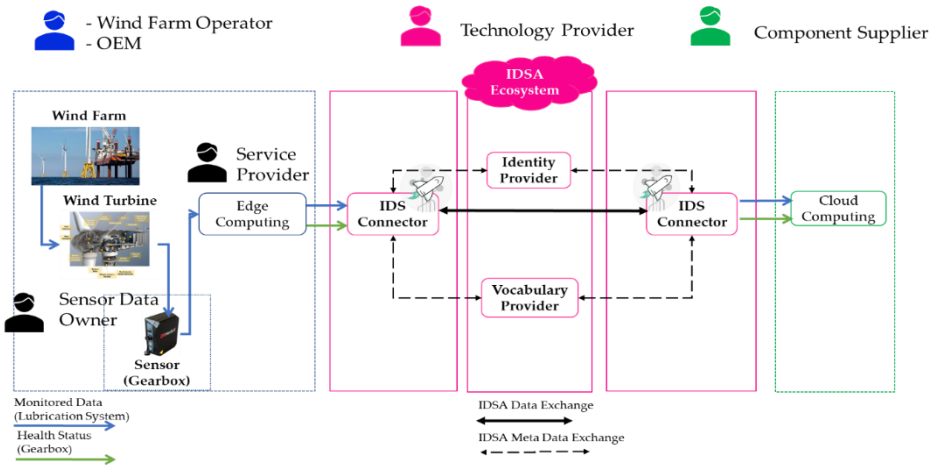

Fig. 1. IDSA Wind Energy Use Case

To promote the sharing of this data between a data owner and, for example, a component supplier, two IDS (International Data Spaces) DataSpace Connectors[1] are deployed and integrated in a trustworthy IDSA ecosystem through the Identity Provider. The IDS Connectors are the technical components responsible for the correct data exchange by providing data sovereignty through the implementation of DUC. On the one hand, in the role of the data provider, the IDS Connector is responsible for the implementation of good quality DUC policies for the resources described through a domain-specific Wind Farm Ontology (WFOnt[2]) that is integrated in a Vocabulary Provider. For this purpose, policies are implemented following the IDSA UPL (Usage Policy Language). On the other hand, once the policy quality is ensured, both IDS Connectors in the role of the data provider and consumer are responsible for enforcing policies correctly.

DUC Model

DUC is about the implementation and enforcement of restrictions regulating what must happen to data [9]. Thus, as shown in Figure 2, it extends data access restrictions, called provisions, to restrictions that pertain to data processing, called obligations [3].

[1] https://international-data-spaces-association.github.io/DataspaceConnector/
[2] https://w3id.org/wfont

Fig. 2. DUC: an extension of AC towards obligations

In practice, from the novel UCON model [2] to more recent models such as ODRL [4] or the IDSA UPL [9], AC models are extended by supporting the following features:

- Context-aware control: permissions and prohibitions on data usage are refined through different conditions. Conditions are Boolean expressions which, based on context-information, permit, or prohibit data usage if they are satisfied. Whereas conditions may apply to non-dependent domains being complementary, such as time or location, dependent conditions are highly expressive.

- Action requirements: to further control data usage, permissions are refined by supporting duties that define actions that must be executed before and after a permission is granted. Furthermore, how these actions must be performed is also defined by conditions in the form of Boolean expressions.

As a result, DUC models become much more expressive than AC models. While gearbox related data usage may be controlled by policies refined through dependent and highly expressive conditions such as those related to time and expressed in time intervals (e.g., 2022-01-01 to 2023-01-01), specific events (e.g., maintenance), etc. different duties such as a payment may be included and refined by conditions defined in terms of a payment method, currency, etc.

This fact further expands the probability of policies related to gearbox data that may not satisfy policy quality requirements such as consistency (permission and prohibition respectively implemented for an overlapping time interval and maintenance period) or redundancy (permissions for overlapping time periods). This leads to security breaches or performance issues. In this regard, providing a formal and common controlled vocabulary for the implementation of policies by policy administrators is of utmost importance for policy analysis. In the presented use case, this issue is solved by implementing a policy analysis method in the IDS Connector deployed at the data provider that analyses the policies implemented following the IDSA UPL such as those represented in Figure 3 for time-interval conditions and Figure 4 for event-based condition.

```
"ids:constraint": [{
                    "@type": "ids:Constraint",
                    "ids:leftOperand": {"@id": "idsc:POLICY_EVALUATION_TIME"},
                    "ids:operator": {"@id": "idsc:DURING"},
                    "ids:rightOperand": [{
                                        "@type": "ids:interval",
                                        "ids:begin": {
                                                            "@type": "ids:Instant",
                                                            "dateTime": {
                                                                                "@value": "2022-01-01T00:00:00Z",
                                                                                "@type": "xsd:dateTimeStamp"
                                                            }
                                        },
                                        "ids:end": {
                                                            "@type": "ids:Instant",
                                                            "dateTime": {
                                                                                "@value": "2023-01-01T00:00:00Z",
                                                                                "@type": "xsd:dateTimeStamp"
                                                            }

                                        }
                    }]
}]
```


Fig. 3. Interval-based IDSA UPL Condition


```
"ids:constraint": [{
                    "ids:leftOperand": {"@id":"idsc:EVENT"},
                    "ids:operator":  {"@id": idsc:SAME_AS"},
                    "ids:rightOperandReference": {"@id": "maintainance"},
                    "ids:pipEndpoint": {"@id": "?eventPipURI"}
}]
```


Fig. 4**. Event-based IDSA UPL Condition**

Policy Implementation in DUC

In DUC, while the data owner implements restrictions on data usage as offered policies in its corresponding IDS Connector, restrictions on how data would like to be used are also implemented as requested policies by the data user on its IDS Connector. Thus, offered and requested policies are negotiated and final agreed policies implemented at both IDS Connectors so that they can be enforced afterwards during data sharing.

To ensure the implementation of good quality agreed policies, both the offered and request policies need to be understood to be analysed at policy negotiation. Although in the presented use case, the IDSA UPL is followed for the implementation of policies, since a scenario where both data providers and consumers use the same set of ontologies can be unrealistic, having a harmonized ontology ecosystem where different ontologies and vocabularies are aligned and interrelated helps overcoming the semantic interoperability hurdle. This would consequently avoid security breaches and performance issues on data sharing, thus providing data sovereignty through a good performance.

Acknowledgments

This research was partly supported by the project HODEI-X (KK-2021/00049), funded by SPRI-Basque Government through the ELKARTEK program.

References

1. R. Sandhu and J. Park, “Usage control: A vision for next generation access control,” in Computer Network Security, edited by V. Gorodetsky, L. Popyack, and V. Skormin (Springer Berlin Heidelberg, Berlin, Heidelberg, 2003) pp. 17–31
2. Jaehong Park and Ravi Sandhu. 2004. The UCON ABC usage control model. ACM Transactions on Information and System Security (TISSEC) 7 (02 2004), 128–174. https://doi.org/10.1145/984334.984339
3. Alexander Pretschner, Manuel Hilty, and David Basin. 2006. Distributed Usage Control. Commun. ACM 49, 9 (Sept. 2006), 39–44.
4. R. Iannella, M. Steidl, S. Myles und V. Rodríguez-Doncel, ”ODRL Vocabulary & Expression 2.2,“ 15 02 2018. [Online]. Available: https://www.w3.org/TR/odrl-vocab/. [Zugriff am 16 08 2019].
5. Study on data sharing between companies in Europe 2018 [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en.
6. M. Jarke, B. Otto, and S. Ram, “Data sovereignty and data space ecosystems,” Business & Information Systems Engineering 61 (2019), 10.1007/s12599-019-00614-2
7. A. A. Jabal, M. Davari, E. Bertino, C. Makaya, S. Calo, D. Verma, A. Russo, and C. Williams, “Methods and tools for policy analysis,” ACM Comput. Surv. 51 (2019)
8. A European Strategy for Data 2020 [Online]. Available: https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy.
9. Eitel, Andreas & Jung, Christian & Brandstädter, Robin & Hosseinzadeh, Arghavan & Bader, Sebastian & Kühnle, Christian & Birnstill, Pascal & Brost, Gerd & Gall, Mark & Bruckner, Fabian & Weißenberg, Norbert & Korth, Benjamin. (2021). Usage Control in the International Data Spaces 3.0.