Report on Data Enforcement Policies Design for Sovereignty preserving data access

D5.7

Authors:

Ferdinando Bosco (ENG)

Vincenzo Croce (ENG)

Denisa Ziu (ENG)

Angelo Triveri (ENG)

Responsible Partner	ENG
Checked by WP leader	**Ferdinando Bosco (ENG)** - Date: 18/03/2022
Verified by the appointed Reviewers	**Konstantinos Kotsalos (ED)** – Date 23/03/2022 **Apostolos Kapetainos (ED)** – Date 23/03/2022 **Marko Petron (Cybernetica)** – Date 23/03/2022
Approved by Project Coordinator	**Stephan Gross (FhG)** – Date: 28/03/2022

Dissemination Level		
PU	Public	X
CO	Confidential, only for members of the consortium (including the Commission Services)	
CI	Classified, as referred to in Commission Decision 2001/844/EC	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Issue Record

Planned delivery date	31/03/2022
Actual date of delivery	
Status and version	V1.0

Version	Date	Author(s)	Notes
0.1	21/01/2022	Ferdinando Bosco (ENG)	Table of Contents
0.2	08/02/2022	Ferdinando Bosco (ENG) Denisa Ziu (ENG)	First Draft of the deliverable (Ch.2 and Ch.3)
0.3	14/03/2022	Ferdinando Bosco (ENG) Vincenzo Croce (ENG) Angelo Triveri (ENG)	First Consolidate version of the deliverable. All chapters concluded.
0.4	18/03/2022	Ferdinando Bosco (ENG)	Deliverables ready for review.
0.5	25/03/2022	Ferdinando Bosco (ENG)	Feedback from the reviewers addressed. Deliverable ready for quality check.
1.0	28/03/2022	Ferdinando Bosco (ENG)	Final version

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

About OneNet

OneNet will provide a seamless integration of all the actors in the electricity network across Europe to create the conditions for a synergistic operation that optimizes the overall energy system while creating an open and fair market structure.

The project OneNet (One Network for Europe) is funded through the EU's eighth Framework Programme Horizon 2020. It is titled "TSO – DSO Consumer: Large-scale demonstrations of innovative grid services through demand response, storage and small-scale (RES) generation" and responds to the call "Building a low-carbon, climate resilient future (LC)".

While the electrical grid is moving from being a fully centralized to a highly decentralized system, grid operators have to adapt to this changing environment and adjust their current business model to accommodate faster reactions and adaptive flexibility. This is an unprecedented challenge requiring an unprecedented solution. For this reason, the two major associations of grid operators in Europe, ENTSO-E and EDSO, have activated their members to put together a unique consortium.

OneNet will see the participation of a consortium of over 70 partners. Key partners in the consortium include: already mentioned ENTSO-E and EDSO, Elering, E-REDES, RWTH Aachen University, University of Comillas, VITO, European Dynamics, Ubitech, Engineering, and the EUI's Florence School of Regulation (Energy).

The key elements of the project are:

1. Definition of a common market design for Europe: this means standardized products and key parameters for grid services which aim at the coordination of all actors, from grid operators to customers;
2. Definition of a Common IT Architecture and Common IT Interfaces: this means not trying to create a single IT platform for all the products but enabling an open architecture of interactions among several platforms so that anybody can join any market across Europe; and
3. Large-scale demonstrators to implement and showcase the scalable solutions developed throughout the project. These demonstrators are organized in four clusters coming to include countries in every region of Europe and testing innovative use cases never validated before.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

List of Figures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

List of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

List of Abbreviations and Acronyms

Acronym	Meaning
ABAC	Attribute-based Access Control
API	Application Programming Interface
DAC	Discretionary Access Control
DAP	Data Access Policy Framework
DoA	Description of Actions
EVM	Ethereum Virtual Machine
GE	Generic Enabler
IDS	International Data Space
IDSA	International Data Space Association
MAC	Mandatory Access Control
NGSI-LD	Next Generation Service Interface – Linked Data
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
PMP	Policy Management Point
PoW	Proof-of-Work
PXP	Policy Execution Point
RBAC	Role-based Access Control
UC	Usage Control
UI	User Interface
WP	Work Package
XACML	eXtensible Access Control Markup Language

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Executive Summary

One of the main goals of the OneNet project is to facilitate the integration and cooperation of all energy stakeholders across Europe for optimizing the overall energy system while creating an open and fair market structure.

OneNet project proposes an IT solution, namely OneNet Framework, which leverages on the implementation of a decentralized solution for the integration of the platforms, tools and services that require secure and trusted data exchange.

This concept is completely aligned with the concept of a common European data space, already defined by the European commission for the creation of **"seamless digital area with the scale that will enable the development of new products and services based on data".**

In this context, the topic of data sovereignty assumes an aspect of fundamental importance and more particularly the possibility of managing the control of access and usage of data, following well-defined and incontrovertible rules.

This document is therefore focused on the concepts of data sovereignty, data access control and its evolution of enforced data usage control and how all these concepts will be implemented in the OneNet Solution.

The OneNet Framework and in particular the OneNet Connector are strictly related to the IDS reference model and FIWARE architecture. In fact, the OneNet Connector consists of a hybrid solution that includes the usage of IDS Connector and FIWARE Context Broker for ensuring a high level of standardization, interoperability, scalability, and reuse of OneNet solution.

The analysis of the IDS reference model for usage control mechanisms was fundamental and it proved to be absolutely compatible with the implementation needs of the OneNet solution. For this reason, the IDS reference model of the OneNet Data Access Polices Framework (DAP), the main result of this deliverable,

In addition, this document also suggests possible alternative technologies that can be approached during the implementation of the components necessary to manage the access and use control to data in WP6: open-source FIWARE Generic Enablers and blockchain technologies.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

1 Introduction

This chapter describes the context in which the activities of WP5, and more specifically the T5.7, are placed and how they are coordinated and linked within the other project activities. In addition, a detailed description of the structure and objectives of this document is provided.

1.1 Scope

OneNet will develop an open and flexible architecture to transform the actual European electricity system, which is often managed in a fragmented country- or area-level way, into a pan-European smarter and more efficient one, while maximizing the consumer capabilities to participate in an open market structure. According to OneNet Description of Action (DoA), WP5 contributes to the direction of fulfilling the OneNet envision by striving to attain two objectives; First, to design an open conceptual architecture for effective yet seamless operation of a smarter pan-European electricity system where market and network technical operations are coordinated closer to real-time across countries, and second to provide requirements, functional and technical specifications, together with interoperable and standardisable interfaces for an open scalable decentralized interconnection of platforms, technology agnostic adaptable and flexible IT reference architecture which fully support the OneNet concept and provides the necessary backbone for the WP6 subsequent implementation of the OneNet data sovereignty-preserving working space.

The WP5, together with WP6, act as IT pillar of the overall OneNet project. The IT pillar it is closely linked to all the other pillars of the project, as shown in Figure 1. It takes into consideration all the results provided in the Market Pillar (WP2 and WP3) as well as the Operation Pillar (WP4). In addition, the OneNet Solution, implemented in WP6 will be tested and evaluated in 4 Demonstration Clusters and the results of the evaluation will be used for adapting, improving, and enhancing the OneNet Solution.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

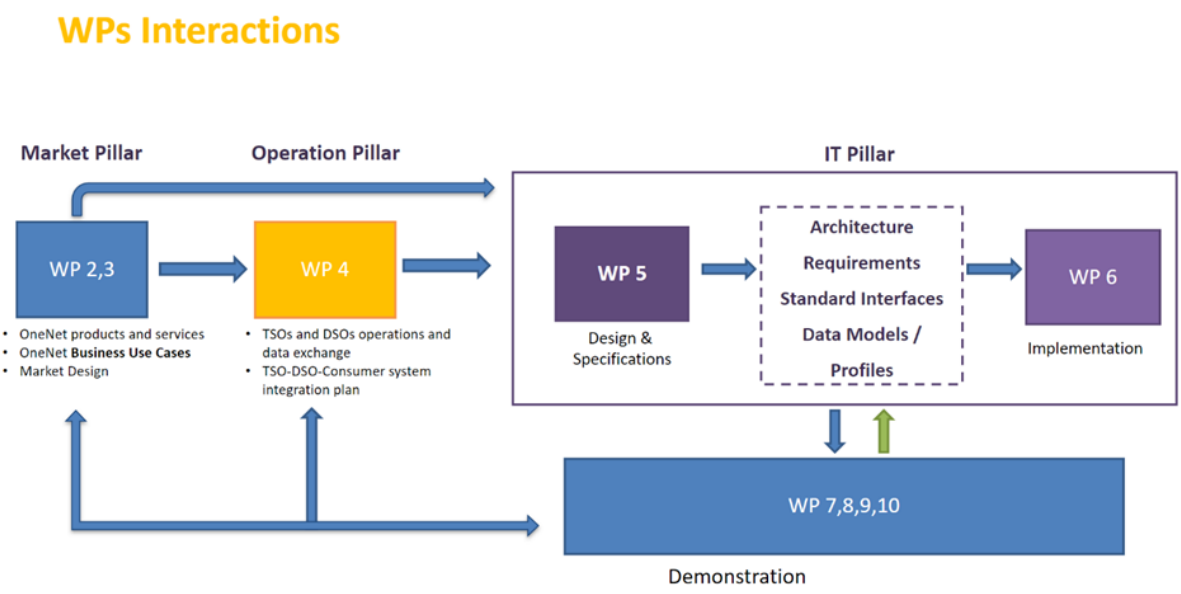

Figure 1: WP5 interactions

1.2 Task 5.7

Within the context just described in Section 1.1, the main goal of the Task T5.7 is to define a OneNet Data Access Policies Framework (DAP) in order to support the data access and usage control in full data exchange cycle within the OneNet System.

Task 5.7, started at M3 of the OneNet projects, investigate on the data management concept and how much is the data access control important for defining a common European data space. In particular the evolution of the data access control concept in a more enhanced data usage control, is the base for the definition of the OneNet Data Access Policies Framework.

The T5.7 foresees two important results:

- the release of the **report on the data enforcement policies design for sovereignty preserving data access** in the Deliverable D5.7 (this document) in March 2022, M18 of the project
- the release of the **final report on the data enforcement policies design for sovereignty preserving data access**, in the Milestone MS10 in September 2022, M24 of the project

The results of this task are fundamental for the implementation of data access and usage control mechanisms in the OneNet Middleware within WP6.

1.3 Outline of the deliverable

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

This deliverable is structured in 6 different chapters.

Chapter 2 analyses the different concepts related to data sovereignty, data management and access control.

Chapter 3 reports the most used and commons technologies for addressing the data access and usage control mechanisms.

Chapter 4 describes how the OneNet System will implement the data access and usage control in the OneNet Middleware and defines the OneNet Data Access Policies Framework.

Finally, chapter 5 concludes the document.

To facilitate the readability of D5.7, it might be useful to refer to D5.2 for the main concepts of the OneNet Architecture and OneNet Middleware component.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

2 Data Sovereignty and Access Control

2.1 Introduction and main concepts

Data sovereignty is a term that refers to the guidelines for the use and processing of data. Data sovereignty is also closely linked to data protection, cloud computing and technology sovereignty. Data sovereignty, more generally, intervenes in any interaction based on data and concerns aspects of protection, security, transfer and storage of the data. Usually, to address the issues related to this area, we can refer to the following questions:

- Who does the data belong to?
- Who is authorized to keep the data?
- How can the data be stored?
- How can the data be used?
- How should the data be protected?
- What happens if the data is used illegally?

The wide-spread adoption of cloud computing services, as well as new approaches to data storage including object storage, have broken down traditional approaches for the management of the data sovereignty.

The benefits of cloud computing are well known. But as soon as the data is not stored on site, but on external servers, or these are exchanged between one location and another, issues of security and management of data ownership arise.

Within the European Union, companies and services that process third party data are obliged to ensure the highest level of data security, verifiable data protection and compliance with modern guidelines [2].

Data used in cloud services can take the following forms:

- Data-in-use: data currently in use
- Data-in-motion: data being transmitted
- Data-at-rest: data stored locally or in the cloud

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Before increasing digitization, data sovereignty was primarily discussed in relation to data-at-rests, i.e., stored data. Today other standards apply: data security, audit security and data sovereignty apply regardless of where the data is stored, especially when the data is processed by external services. It is therefore essential to manage data sovereignty for all three phases.

In this document, following the OneNet scope, the concept of data sovereignty is mainly focused on the application and maintenance of the data sovereignty in the transactional data flow, that is strictly related with the concept of data access control and policy access definitions.

In fact, ensuring data sovereignty for the owner of the data presupposes the possibility to unambiguously defines data usage policies at each level of the data value chain. Ensuring the data sovereignty requires an appropriate technical and conceptual framework that facilitates agreements on the use of data, such as allowing (or disallowing) the processing, linkage or analysis of data and allowing (or disallowing) third parties access to data.

2.2 Data Space and Usage Control

In recent years, the strategy of European companies and the European Commission itself has focused a lot on the importance of data and how it is fundamental to generate business value [4]. Data is an essential resource for economic growth, competitiveness, innovation, job creation and societal progress in general.

The European strategy for data aims at creating a single market for data that will ensure Europe's global competitiveness and data sovereignty. The definition of Common European data spaces will ensure that more data becomes available for use in the economy and society, while keeping the companies and individuals who generate the data in control [3].

The term Data Space usually refers to a **"seamless digital area with the scale that will enable the development of new products and services based on data"**. According to the more recent EC's Digital Europe Work Programme [4], a data space is **"data infrastructure with tailored governance mechanisms that will enable secure and cross-border access to key datasets in the targeted thematic area."**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

In the context of defining a data space, as an ecosystem enabled for sharing and reusing data, it is important to define the following aspects

- Definition of the data value chain (from production to use, but also to processing)
- Definition of roles (who are the actors involved in the entire data value chain)
- Definition of data access and control rules

2.3 Data Access Control Mechanisms and policies definition

Data access control is a mechanism in computer security that regulates access to the system resources. The rights of subjects to access such resources are typically expressed through access control policies, which are evaluated at access request time against the current access context.

Several access control models exist, such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-based Access Control (RBAC), Attribute-based Access Control (ABAC), etc. Among all these approaches, the RBAC and the ABAC is mostly used in modern IT organizations.

RBAC is a security and authorization model for securing access to computer resources. Sometimes referred to as “Role-Based Security,” RBAC access is based on roles as defined by the business using them. In the RBAC model, roles are created and then sets of permissions for resources are assigned to the role. Users are then granted one or more roles to receive access to resources. ABAC, on the other hand, stands for Attribute-Based Access Control. As suggested by the name, ABAC relies on user attributes for authorization decisions. ABAC policies are rules that evaluate access based upon four sets of attributes. These include: Subject Attributes, which are attributes concerning the person or actor being evaluated; Resource Attributes, which are attributes of the target or object being affected; Action Attributes, which describe the action to be performed on the Resource; and, Environment Attributes, which include attributes such as the time of the day, IP subnet, and others that do not relate to either the Subject or the Resource.

Each of these models has its weakness and benefits. The main benefits of RBAC are:

- It is deterministic. An RBAC approach makes it easy to know who has access to what at any moment in time;
- It is more direct and easier to visualize. Security admins can visualize the actors and resources they will affect when creating or modifying a policy;
- It is inherently auditable. With RBAC assignments it is simple for business owners to certify or attest to access granted, as the consequences of that access are visible. This visibility contrasts with ABAC where a “before the fact audit" is not possible and the effects of a rule are not easy to grasp;

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

- RBAC can be simpler than ABAC. For example, with RBAC, bundles of access can be directly assigned to a user. To do this in ABAC requires the creation of a new rule.

RBAC's primary weaknesses are:

- It requires advance knowledge of the Subjects and Resources and typically does not support making on-the-fly contextual decisions;
- An RBAC-only approach can result in a huge number of roles to accomplish fine-grained authorization;
- Resource Owners must know something about the roles and their intended purpose to grant access to those roles accurately;
- Resources must be organized into collections to facilitate delegation;
- Given a substantial number of roles and collections of resources, a correspondingly large number of delegations would need to be created and managed.

On the other hand, also ABAC has advantages and disadvantages. The principal advantages of ABAC are:

- It enforces centralized management of authorization policies;
- It makes it easy to specify access rules as simple queries;
- ABAC rules can be extremely fine-grained and contextual;
- ABAC rules can evaluate attributes of Subjects and Resources that are not inventoried by the authorization system;
- ABAC rules need less maintenance and overhead because they do not require the creation or maintenance of the structure on which an RBAC model depends (e.g., roles and resource locations.)

ABAC's principal weaknesses are:

- It makes it extremely difficult, if not impossible, to perform a "before the fact audit" and determine the permissions available to a specific user. Potentially, a huge number of rules might need to be executed, and in the same order in which the system applies them, to successfully determine access. As a result, it could be impossible to determine risk exposure for any given employee position;
- It can lead to a "Rule Explosion" (somewhat in the same way as RBAC can create a "Role Explosion) as a system with N number of attributes would have 2N possible rule combinations;
- ABAC systems (which don't pre-calculate the net result of access rights) can be unacceptably slow to answer authorization queries unless rules are kept extremely simple and do not access data from multiple source systems.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The XACML (eXtensible Access Control Markup Language) Standard [5] is commonly used for describing access control rules. The main building blocks of the language are subject, action, resource and environment. The subject describes who is accessing a data asset (e.g., a user). The action describes what the subject wants to perform on the data asset (e.g., read, write). The resource describes the data asset. Finally, the environment specifies the context (e.g., time, location). Figure 2 illustrates the data-flow model of XACML and the main actors or components to implement it: Policy Enforcement Point (PEP), Policy Decision Point (PDP), Policy Information Point (PIP), and Policy Administration Point (PAP).

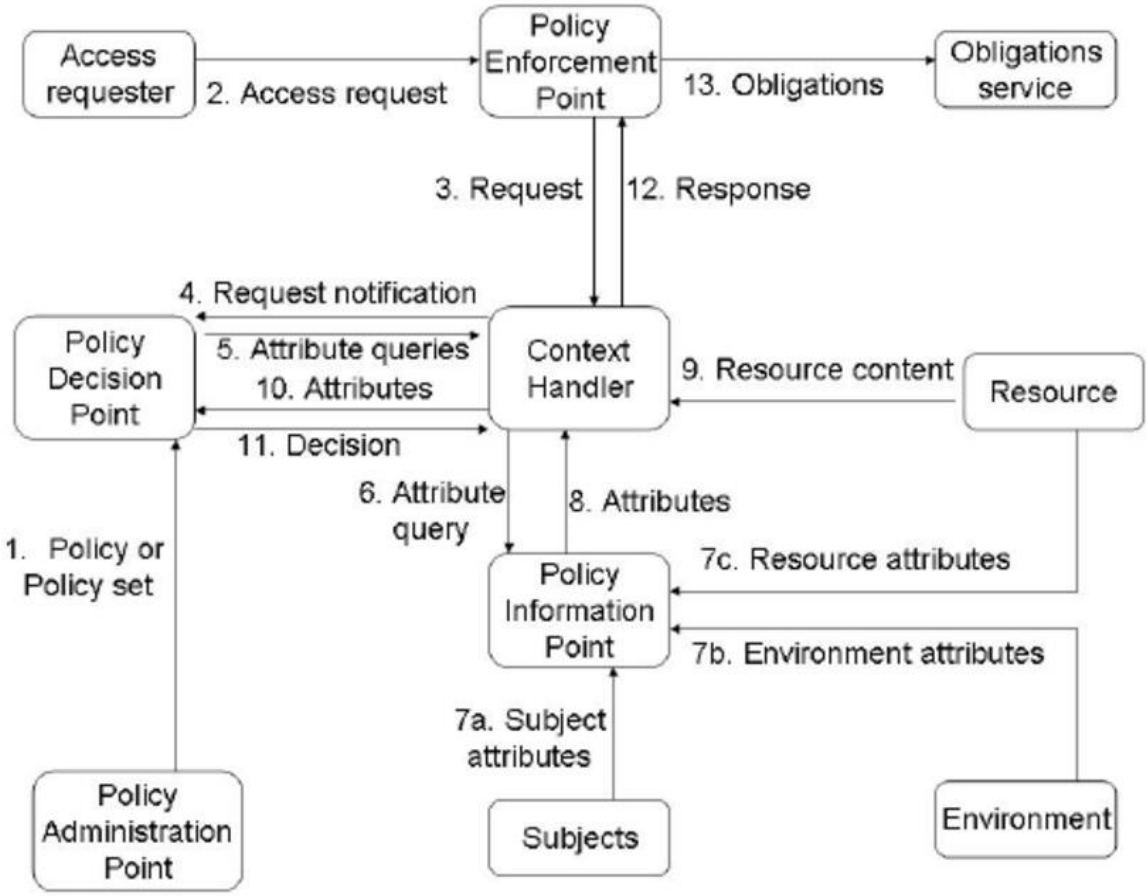

Figure 2: XACML data flow model [6]

In general, attributes can describe anything and anyone, but tend to split into four categories:

- Subject attributes: Attributes that describe the user by e.g., age, role, or clearance.

- Action attributes: Attributes that describe the action attempted e.g., read, delete, or view.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

- Resource (or object) attributes: Attributes that describe the resource itself e.g., object type, location, or classification.

- Contextual (environment) attributes: Attributes that address time, location, or other dynamic aspects.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3 Technologies for Data Access Control

3.1 IDSA and Usage Control

The International Data Spaces Association (IDSA) [7] is a non-profit organization founded jointly by business, politics, and research with the mission of establishing both the development and the use of a Reference Architecture Model for secure data spaces and sovereign data sharing on a European and International level. More than 130 members from different kind of industries, sizes and organizations aim to establish a worldwide standard for data exchange.

International Data Spaces (IDS) can be considered the more important European initiative related to Data Spaces and it has the main mission to leverage existing standards and technologies, for facilitating and establishing a secure, standardized and sovereign system of data exchange in a trusted Business Ecosystem.

IDSA vision is guided by the demand for digital sovereignty, and it aims to create a network of trusted data.

Key features of IDS are:

· Sovereignty of data assets: The data owner establishes individual usage policies for their data assets, regarding both data usage and data users (such as the specific release or blocking of data for certain users).

· Security of data exchange: A protection level concept regulates the data protection requirements, in particular during the exchange of data.

· Decentralized organization and federal architecture: International Data Spaces combines all end points that use an IDS connector for participation in the data space of International Data Spaces. Thus, there is no central authority for data management or data governance tasks. This makes International Data Spaces an alternative architecture design, compared for example to central data management concepts (including data lakes) on the one hand and decentralized data networks without shared rules on the other hand.

· Governance and shared rules: Due to the decentralized architecture of International Data Spaces and thus the lack of a central supervisory authority, data governance principles are developed as shared rules. They determine the rights and obligations for data management and are derived from the requirements of the users.

· Network of platforms and services: International Data Spaces connects data providers and data users. Data providers can be companies, but also individual entities on the Internet of things such as vehicles, machines, means of transport, and equipment.

· Scaling and network effects: International Data Spaces provides data services for the secure exchange and straightforward linking of data. By connecting the participants via the IDS connectors, the infrastructure has

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

a decentralized character which makes International Data Spaces scalable without a central authority. Furthermore, the scaling and network effects as such develop through the growing availability of data, not only from individual participants but also entire ecosystems.

· Openness: The International Data Spaces initiative is user-driven and based on a participative development process, organizationally bundled in the International Data Spaces Association.

· Protection of trust: International Data Spaces participants must be able to rely on the identity of data providers and data users, and on the technical implementation of data sovereignty. To this end, a mandatory certification of the software ensures the protection of trust. Special IDS connectors with extended encryption are also available for the secure exchange of data.

International Data Spaces (IDS) relies and focuses on **data usage control** as a conceptual and technological solution to cope with data sovereignty challenges. In its position paper [8] IDS focusing on the difference between access control and usage control, the usage control concepts and related concepts such as digital rights management or user managed access, as well as the implementation of data usage control in the IDS

3.1.1 Usage Control Concepts and implementation on IDS

Data Usage control is an extension to traditional data access control descripted in Ch.2 It is about the specification and enforcement of restrictions regulating what must (not) happen to data. Thus, usage control is concerned with requirements that pertain to data processing (obligations), rather than data access (provisions). Usage control is relevant in the context of intellectual property protection, compliance with regulations, and digital rights management.

In addition to data access control, where only the access to specific resources is managed, the IDS architecture supports data-centric usage control. In general, the overall goal is to enforce usage restrictions for data after access has been granted. Therefore, the purpose of usage control is to bind policies to data being exchanged and to continuously control the way how messages may be processed, aggregated, or forwarded to other endpoints.

This data-centric perspective allows the user to continuously control data flows, rather than accesses to services. At configuration time, these policies support developers and administrators in setting up correct data flows. At runtime, the usage control enforcement prevents IDS connectors from treating data in an undesired way, for example by forwarding personal data to public endpoints. Thus, usage control is both a tool for system integrators to ensure they are not building an architecture that violates security requirements, and an audit mechanism, which creates evidence of a compliant data usage [8].

There are two main steps within the IDS to implement data usage control:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

- First, **the definition of IDS contracts** that contains the data usage restrictions using a policy language. The used policy language used must be descriptive, technology-independent and based on the Open Digital Rights Language (ODRL).
- Second, usage control technologies are developed for the **enforcement of the usage restrictions** at technical level.

Definition of IDS Contracts

An IDS Contract, as shown in Figure 3, is divided to two main sections: the contract specific metadata and the IDS Usage Control Policy of the contract. The contract specific information (e.g., date when the contract has been issued or references to the sensitive information about the involved parties) has no effect on the enforcement. However, the IDS Usage Control Policy is the key motive of organizational and technical Usage Control enforcement. Furthermore, an IDS Usage Control Policy contains several Data Usage Control statements (e.g., permissions, prohibitions, and obligations) called IDS Rules and is specified in the IDS Usage Control Language which is a technology independent language. The technically enforceable rules shall be transformed to a technology dependent policy (e.g., MYDATA [9]) to facilitate the Usage Control enforcement of data sovereignty [8].

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Figure 3: Example of IDS Contract with time restriction usage

The IDS Contract represents an agreement between the involved parties for addressing their needs and benefits. After all, the Data Usage Control statements of the agreement contract shall be transformed to a technology-dependent language which is interpretable by a Data Usage Control technology and can be enforced to the systems.

Enforcement

For enforcing usage restrictions, data flows need to be monitored and potentially intercepted by control points (i.e., PEPs). These intercepted data flows are given to the decision engine (i.e., the PDP) for requesting permission or denial of the data flow. In addition to just allowing or denying the data flow, the decision can also require a modification of data. A PEP component encapsulates the enforcement.

The enforcement relies on a decision. A Policy Decision Point (PDP) takes the responsibility to answer incoming requests (i.e., data flows) from a PEP with a decision (see Figure 4). The decision-making based on usage restrictions is also called (policy) evaluation.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

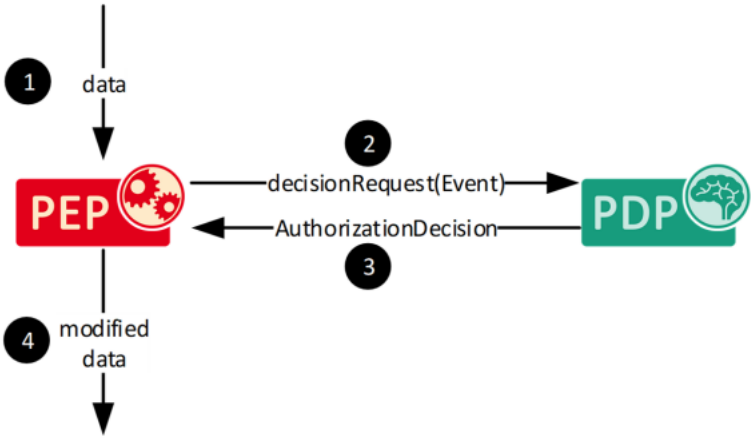

Figure 4: Illustration of a PEP intercepting data with decision making (PDP) [8]

The policy decision may also depend on additional information that is not present in the intercepted data flow itself. This includes information about contextual information such as previous data usages or the geographical location of an entity. There is also the possibility for pre- or post-conditions that have to hold before (e.g., integrity check of the environment) and after (e.g., data item is deleted after usage) the decision-making. In addition, there is the possibility to define on-conditions that have to hold during usage (e.g., only during business hours). These conditions usually specify constraints and permissions that have to be fulfilled before, during, and after using the data (see Figure 5).

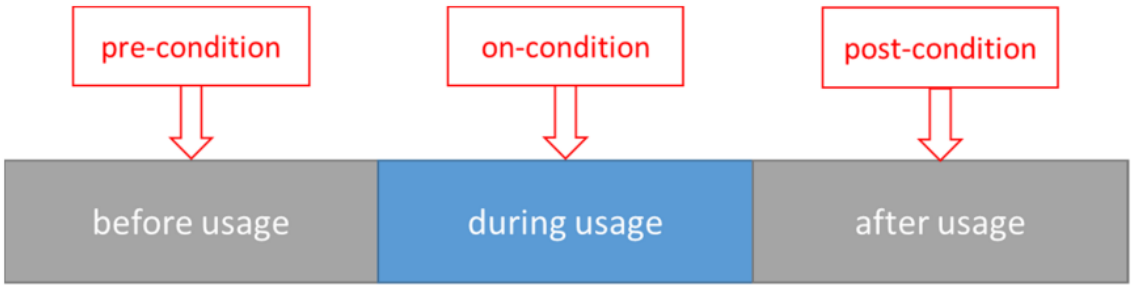

Figure 5: Types of conditions and when they are enforced [8]

A Policy Information Point (PIP) provides missing information for the decision making. In addition, we can use such a component to get contextual information for or about the intercepted system action (e.g., data flow information, geolocation of the requesting device). Finally, there is the concept of a Policy Execution Point (PXP). A PXP is used to perform additional actions based on the policy rules, such as sending an email when data is

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

used or writing to a specific log system. Figure 6 illustrates an exemplary sequence of all processing steps to enforce usage control restrictions on a data flow:

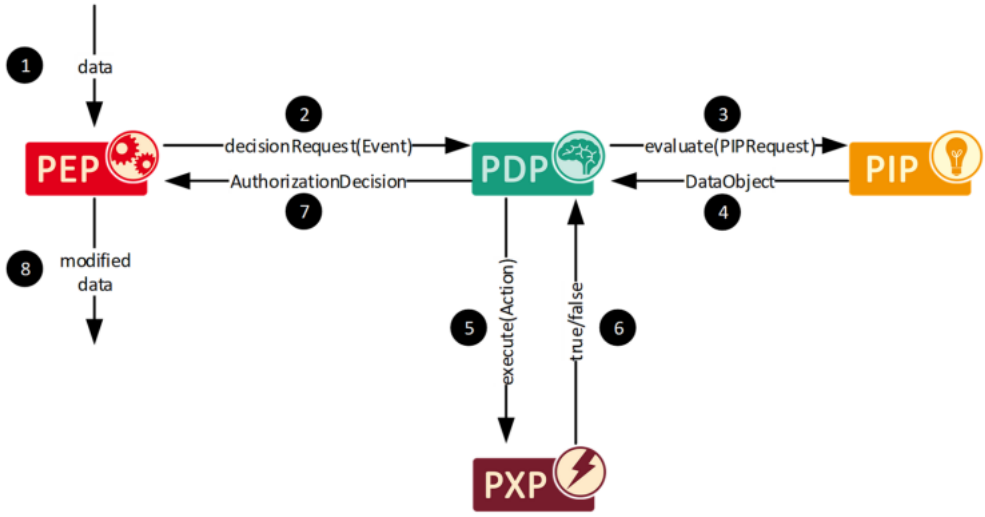

Figure 6: Full illustration of a usage-controlled data flow [8]

1. PEP intercepts the data flow
2. PEP transforms the data flow to a decision request and sends that decision request to PDP
3. PDP starts the policy evaluation and invokes a PIP to retrieve additional information
4. PIP responds with the requested data to the PDP
5. PDP triggers an additional action at a PXP
6. PXP confirms that the action succeeded to the PDP
7. PDP sends authorization decision to the PEP
8. PEP enforces the decision on the intercepted data flow

Implementation of the Usage Control

Usage control can be implemented in different ways. The solutions range from organizational rules or legal contracts to complete technical enforcement of usage restrictions. Intermediate levels may contain parts of both enforcement manifestations.

The following figure presents the different stages of usage control that we name the usage control onion, starting from the inner part of the onion, which is the IDS connector, and ending in the outer onion shells with external systems.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

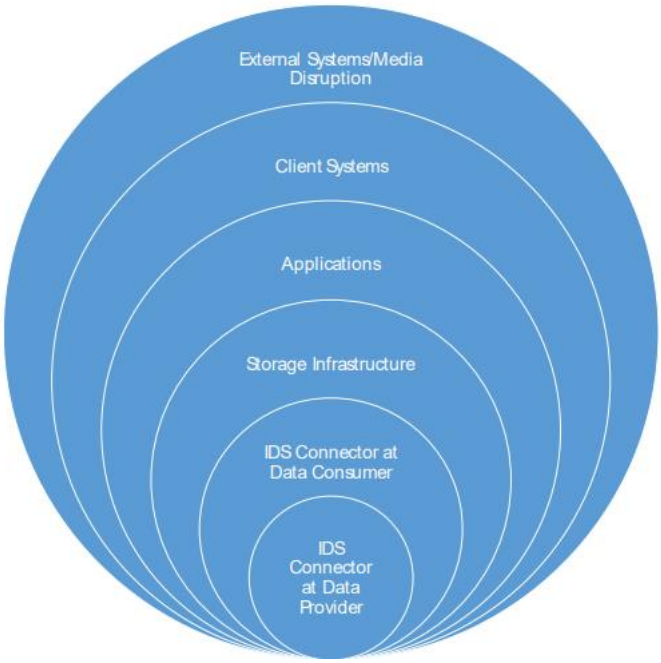

Figure 7: Usage Control "Onion" [8]

Usage Control within the IDS Connector

The inner part of the usage control onion is the IDS connector. Depending on the usage restrictions, they are applied at the data provider connector or at the data consumer connector. At the data provider connector, usage control enforces policies such as how often data can be accessed, at what times (e.g., only within business hours), or that data must be filtered or masked (e.g., anonymized) before leaving the company. The usage restrictions at data provider connector are usually provisions that are technically handled by a PEP. At the data consumer connector, usage control enforces policies that are usually obligations for the data consumer such as "data can only be used for fourteen days" or "data can only be used for the purpose of predictive maintenance". The technical enforcement is handled by a PEP or PXP, depending on the usage restriction. Limiting data flowing to a specific target system to ensure the correct usage purpose is handled by a PEP, the deletion of data in storage infrastructure outside the connector is handled by a PXP that performs the delete operation.

Actors Involved

According to the IDS information model, a Data Owner (Data Sovereign) is a core participant of IDS who has complete control over the data and makes it available in the IDS and defines the terms and conditions of use of the data. A Data Provider is another Core participant of IDS who exposes the Data Sources via a Connector. A Data Provider may be an enterprise or other organization, a data marketplace, an individual, or a "smart thing". Moreover, a Data Consumer requests and uses the data provided by a Data Provider and a Data User is an IDS participant that has the legal right to use the data of a Data Sovereign as specified by the usage policy.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Policy Definition

The Data Providers of the IDS need to specify their Data Usage Control policies, although, they are from different technical backgrounds. A policy specification dashboard can support the customers in the process of policy specification. Figure 8 illustrates the process of policy specification in IDS. The IDS Data Providers and Data Consumers shall use the IDS policy editors (i.e., Policy Administration Points) to specify their Data Usage Control policies and consequently, create their IDS Contracts.

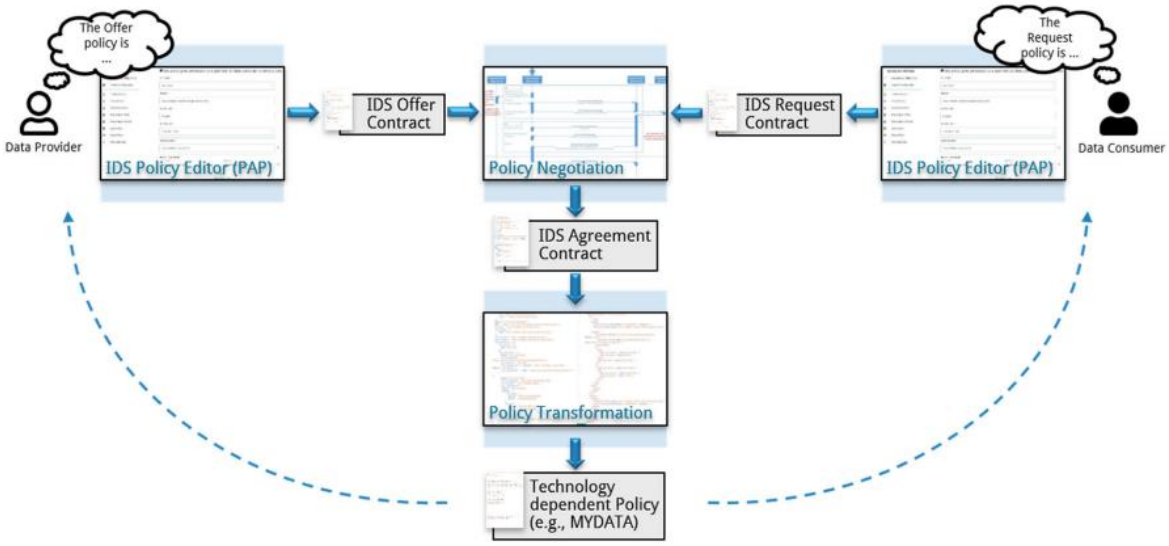

Figure 8: Policy Definition Process [8]

Policy Classes

A Data Usage Control policy, in general, may provide permission to an IDS Data Consumer to operate specified action(s) over a Data Asset or prohibit the operation of that specified action(s). Providing permission or prohibition of an operation is extended to variety of actions. A policy can be specified to provide permission to use the data. The action of using the data covers various operations over that piece of data such as displaying it, printing it, making calculation over it, and so on. In addition, a policy may address only a particular fine-grained action. For example, a policy that permits reading data, allows the act of obtaining the Data Asset from the data source without further restrictions, however, the action of printing data is not permitted. The Data Usage Control technologies in IDS context support the whitelisting approach to protect the data. It means that the access to the non-public data is prohibited by default. The studies on the requirements and use cases of the IDS projects shows that several restrictions shall apply when data is used. For example, an IDS Data Consumer may request to use the data in a specific time interval, or an IDS Data Consumer may restrict the usage of the data to a specific location. IDS categorizes these restrictions into 21 atomic templates called policy classes that are reported in Table 1. Eventually, a Data Usage Control policy is a combination of one or more instances of these

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

policy classes that is identified and is referring to a specific piece of data. Furthermore, the policy classes may evolve over the time in the context of IDS, depending on the stakeholders' demands as well as public rules and regulations.

Table 1: IDS Policy Classes [8]

No.	Title
1	Allow the Usage of the Data
2	Connector-restricted Data Usage
3	Application-restricted Data Usage
4	Interval-restricted Data Usage
5	Duration-restricted Data Usage
6	Location Restricted Policy
7	Perpetual Data Sale (Payment once)
8	Data Rental (Payment frequently)
9	Role-restricted Data Usage
10	Purpose-restricted Data Usage Policy
11	Event-restricted Usage Policy
12	Restricted Number of Usages
13	Security Level Restricted Policy
14	Use Data and Delete it After
15	Modify Data (in Transit)
16	Modify Data (in Rest)
17	Local Logging
18	Remote Notifications
19	Attach Policy when Distribute to a Third-party
20	Distribute only if encrypted
21	State Restricted Policy

3.1.2 IDS based Usage Control Technologies

In the IDS ecosystem, there are already several technologies for the implementation of the Data Usage and Access Control. The most relevant are bot proposed by Fraunhofer IESE: MYDATA Control Technologies and LUCON policy language.

A brief description of the technologies is reported below. For more details, please refer to the IDS Position Paper [8].

MYDATA

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

MYDATA Control Technologies (MYDATA for short) [9] is a technical implementation of data sovereignty, which represents an essential component for informational self-determination. It is based on the IND2UCE [10] framework for data usage control developed at Fraunhofer IESE. In general, MYDATA implements data sovereignty by monitoring or intercepting security relevant data flows. This enables fine-grained masking and filtering of data flows in order to make them anonymous, for example. Compared to classical access control systems, MYDATA can enforce partial filtering and masking of data, context and situation restrictions as well as restrictions on the purpose of use. From a functional perspective the MYDATA Usage Control Container includes at least a PEP, a PDP and a PMP (Policy Management Point) and it offers interfaces for calling the PEP interfaces and the PMP interfaces directly [8].

LUCON

LUCON (Logic based Usage CONtrol) [11] is a policy language for controlling data flows between endpoints. The Trusted Connector uses Apache Camel [12] to route messages between services (such as MQTT, REST, or OPC-UA endpoints). The ways how messages may be processed and passed around between services is controlled by LUCON, a simple policy language for message labelling and taint tracking. The LUCON policy language comes with an Eclipse plugin for syntax highlighting, code completion and compilation into a format that is understood by the policy decision point within the Connector. From a functional perspective, LUCON is able to intercept data flows and define policies for controlling it, but it is not yet able to perform the enforcement and modify the data. These additional features are still in development phase and even if LUCON is listed as IDSA suggested tools for implementing Data Usage Control, it still has too low maturity level (TRL 4) to be integrated into stable environments.

3.2 Data Usage and Access Control using FIWARE

In the OneNet context, where IDS Reference model and FIWARE smart energy architecture together form the basis for the implementation of the OneNet Middleware and the OneNet Connector, is interesting to analyse some possible alternative, based on FIWARE for the implementation of a Usage Control Framework.

As already widely discussed in the D5.2 [13], FIWARE is an open initiative whose mission is to ease the development of new Smart Applications in multiple sectors by providing a set of components, known as Generic Enablers (GE), that enable the connection among IoT devices and Context Information Management and other services such as security or big data analysis.

FIWARE catalogue offers several open-source Generic Enablers (GEs), that can be used for implementing a Data Usage Control Framework:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Keyrock

The Keyrock GE [14] is responsible for Identity Management. Keyrock enables OAuth 2.0 based authentication and authorization security to services and applications. In the context of Data Usage Control, Keyrock can play the role of the **Identity Manager**.

Wilma

The Wilma GE [15] enables the support of proxy functions within OAuth 2.0-based authentication schemas. It could implement PEP functions within an XACML-based Access Control schema.

AuthZForce

The AuthZForce GE [16] is the reference implementation of the Authorization PDP Generic Enabler (formerly called Access Control GE). It brings additional support to PDP/PAP functions within an Access Control schema based on the XACML standard. It could be used to create more advanced fine-grained authorization policies and to make decisions over requests received from PEPs

Orion Context Broker (with Linked Data Extensions)

The Context Broker (Orion) [17] manages the entire lifecycle of context information including updates, queries, registrations and subscriptions. The Context Broker offers the FIWARE NGSI-LD (Next Generation Service Interface with Linked Data Extension) [18] APIs and associated information model (entity, attribute, metadata) as the main interface for sharing data among stakeholders.

Cosmos

The Cosmos GE [19] simplifies Big Data analysis of context data and integrates with some of the many popular Big Data platforms like Apache Flink [ref] and Apache Spark [ref]

Draco

The Draco GE [20] is aimed at providing storage of historical context data, allowing the reception of data events and dynamically recording them with a predefined structure in several data storage systems.

3.2.1 Case study: Data Usage and Access Control in Industrial Data Spaces - Implementation Using FIWARE

The Universidad Politécnica de Madrid proposes an implementation of Data Usage and Access Control in Industrial Data Spaces using FIWARE [21].

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

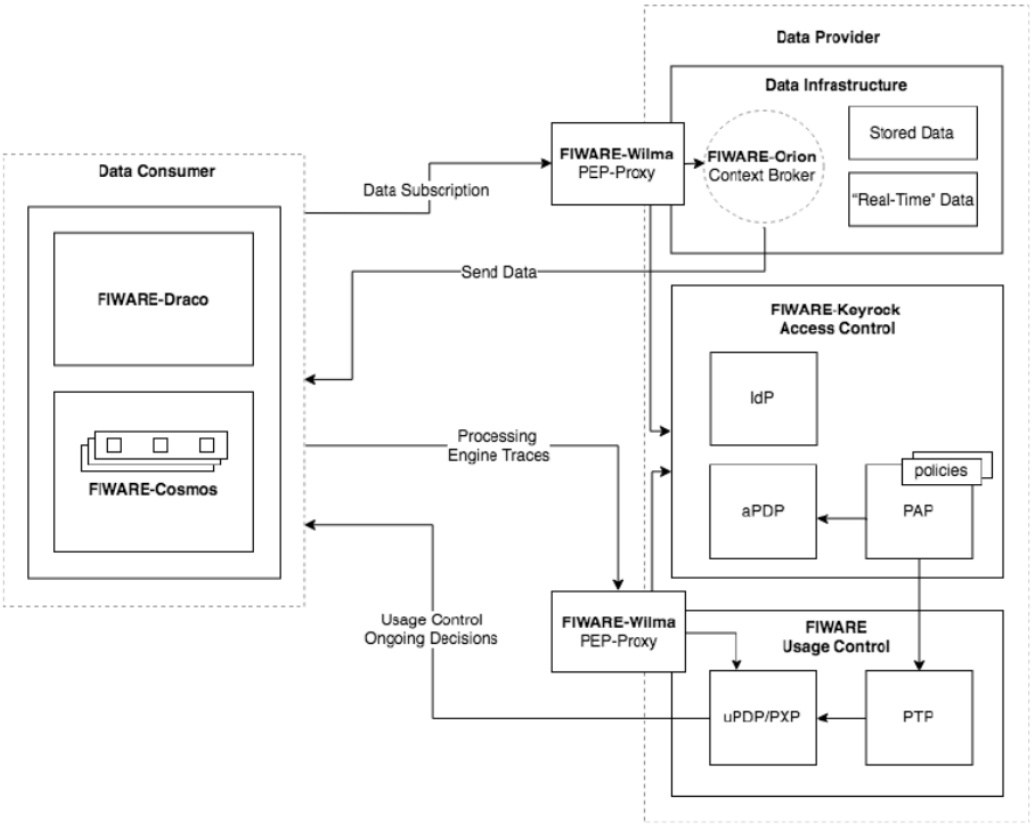

Figure 9: FIWARE based Data Usage Control Framework [21]

In this implementation, the FIWARE GEs provide all the features needed to implement the components on the Data Consumer side (processing engine and data storage), the Access Control components (PAP, PEP, and aPDP), the SDS, and the IdP.

As the FIWARE catalogue lacks any GEs that aid in the implementation of Usage Control capabilities the framework includes additional component developed by the Universidad Politécnica de Madrid. In particular, they developed the PTP, uPDP and PXP components, planning to include them as a new FIWARE GE in the near future.

3.3 Blockchain-based data access control

Blockchain technology was considered in the latest years as an important opportunity to disrupt traditional products and services in many contexts. This is mainly due to features such as the absence of a single trusted third party, the immutability of the blockchain record, the distributed, decentralised nature of blockchains, and the ability to run smart contracts.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Some of the features of blockchain technology are consistent with features of the International Data Spaces architecture, such as the absence of a single trusted party (e.g., where all data is being stored) and the decentralized nature. Other features are complementary, such as the permanence of the blockchain record. This makes it highly interesting to explore how the blockchain technology could fit with the concept of the IDS Reference Architecture and how it could be exploited for implementing data access and usage control [22].

3.3.1 Blockchain Concept

Blockchain has been considered an innovative technology, identified as to be as disruptive as Internet was considered when it was first introduced. Blockchain promises innovation in the commercial and financial area which is comparable to the impact the web has had on communication [23]. It is revolutionising the way we interact based on these main key advantages:

• Traceability and data storage - decentralised and distributed system that becomes a secure way to track changes in information over time;

• Trust - the creation of trust among untrusted participants;

• Peer-to-peer transactions - the absence of intermediaries promotes democracy.

The Blockchain is a distributed ledger, based on a shared and distributed database, containing a log of transactions in chronological order. Transactions are grouped into blocks and chained through cryptographic hashes into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work [24] (Figure 10) The main purpose of blockchain technology is to remove the need for intermediaries and replace them with a distributed network of digital users, who work in partnership to verify transactions and safeguard the integrity of the ledger. Differently to centralised systems, every member of the blockchain network holds his copy of the ledger or can access it in the open cloud. As a result, anyone in the network can have access to the historic log of the system transactions and verify their validity, enabling a high level of transparency.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

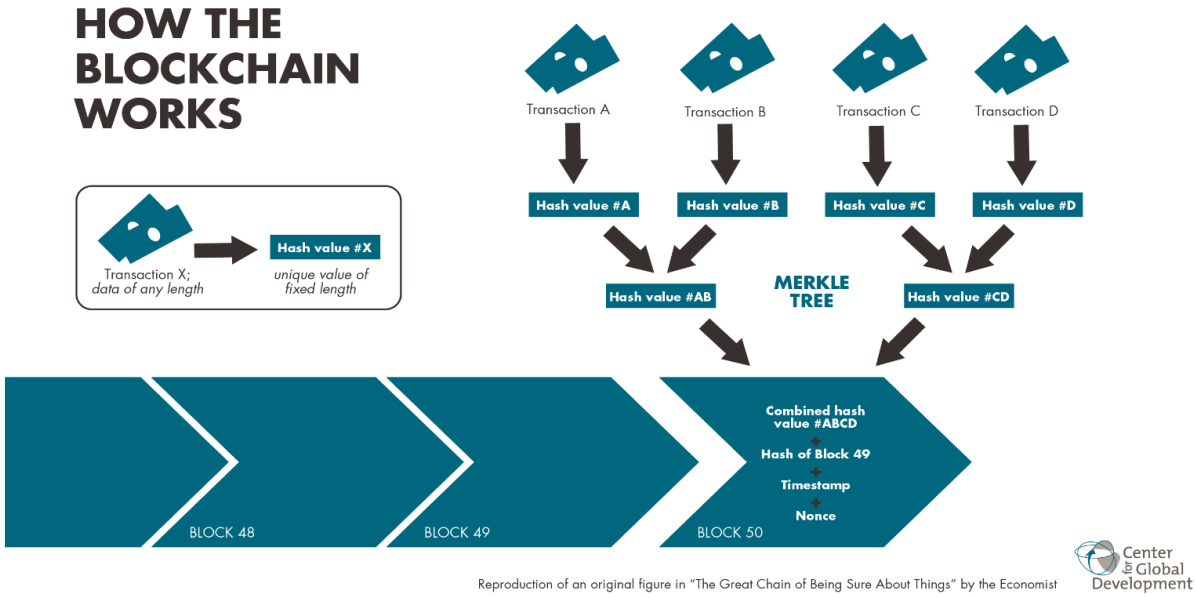

Figure 10: Blockchain technology (Reproduction of original figure in the "The Great Chain of Being Sure about Things" by the Economist)

3.3.2 Blockchains

The two most popular blockchains are Bitcoin and Ethereum. Bitcoin is the world's first cryptocurrency, established in 2009 following the public release of a paper by Nakamoto [24], an author whose real identity remains unknown. In this work it was proposed a distributed electronic cash payment system that uses P2P communication of anonymous and unknown Internet users. Digital cash transacted between users is not issued or controlled by a central bank, but by a network of computers that operate in collaboration and use cryptography to assure security. Bitcoins are created as a reward for a process known as mining. Bitcoin mining is performed by high-powered computers that solve complex computational mathematical problems; these problems are so complex that they cannot be solved by hand and are complicated enough to overload even incredibly powerful computers. The result of bitcoin mining is twofold. First, when computers solve these complex mathematical problems on the bitcoin network, they produce new bitcoins. And second, by solving computational mathematical problems, bitcoin miners make the bitcoin payment network reliable and secure by verifying transaction information.

Different blockchains may differ in the consensus mechanisms and programming capabilities.

Consensus Mechanisms

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Consensus mechanisms are protocols that make sure all blockchain nodes are synchronised with each other and agree on a single data value or a single state of the blockchain network.

These consensus mechanisms are crucial for a blockchain in order to function correctly. They make sure everyone uses the same blockchain at the same moment. Everyone can submit things to be added to the blockchain, so it is necessary that all transactions be constantly checked and that all nodes constantly audit the blockchain. Without good consensus mechanisms, blockchains are at risk of various attacks [25].

Before Bitcoin [26], there were many iterations of peer-to-peer decentralized currency systems that failed because they were unable to answer the biggest problem when it came to reaching a consensus. This problem is called “Byzantine Generals Problem” [27]. To solve this problem, Bitcoin introduced the Proof-of-Work (PoW) [28] consensus mechanism and other blockchains implemented and used other consensus mechanisms (such as Proof-of-Stake, Proof-of-Capacity, etc.) [29].

Considering the consensus mechanism, blockchains differ in the definition of the nodes’ participation in the distributed network and the roles that they can perform. In particular, it is possible to distinguish between public and private blockchains.

Public Blockchains (also called “permissionless”) are defined in this way because they require no authorization to access the network, perform transactions or participate in the verification and creation of a new block. Anyone can participate (read and write) in the blockchain network. Public blockchains are decentralised, no one has control over the network, and they are secure in the sense that the data cannot be changed once validated on the blockchain.

On the other hand, a private blockchain is a permissioned blockchain. Permissioned Blockchains are subject to a central authority that determines who can access is authorized to be part of the network. This authority defines what roles a user can play within it, also defining rules on the visibility of recorded data. The permissioned Blockchains therefore introduce the concept of governance and centralization in a network that is born as absolutely decentralized and distributed.

Programming capabilities

Considering the programming capabilities, we can differentiate between blockchains programmable via simple scripting (e.g., Bitcoin Blockchain) and blockchains providing Turing-complete computational capabilities, enabling the creation of “smart contracts” (e.g., Ethereum Blockchain).

Ethereum was the first blockchain supporting smart contracts and it is still the most notable example of a Turing-complete programmable blockchain, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state-transition functions. Smart contracts, cryptographic "boxes" that contain value and only unlock it if certain

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

conditions are met, can also be built on top of the platform, with vastly more power than that offered by Bitcoin scripting because of the added powers of Turing-completeness, value-awareness, blockchain-awareness and state [30].

Ethereum was proposed by Vitalik Buterin in 2013 [30] and a further detailed analysis was provided by Gavin Wood in the 'yellow paper' (Ethereum: A Secure Decentralised Generalised Transaction Ledger [31]). As the Ethereum website [32] reports, "Ethereum is a decentralized platform that runs smart contracts." These contracts run on the "Ethereum Virtual Machine" (EVM); a distributed computing network made up of all the devices running Ethereum nodes. Like other blockchains, Ethereum has a native cryptocurrency called Ether (ETH) and it has a double use: it is used as an incentive for the network "validators", but also to regulate the use of the blockchain computational resources.

The smart contracts are written in a low-level bytecode language interpreted by the EVM. High level languages whose programs can be compiled in EVM bytecode (producing a .bin file containing the binary of the compiled contract and an ". abi" file containing the contract interface specification) have also been developed to ease human smart contract coding. The most widespread of such languages is a JavaScript style language called Solidity [33].

It is important to remark that every transaction has to pay a fee proportional to its complexity to repay the miners for their effort of maintaining the EVM. To every single operation of the EVM is assigned (by the protocol) a price proportional to its burden to the users (i.e., the number of computational steps needed for its execution and its storage weight), this is called gas and the total gas of a transaction is the summation of all the gas of every single instruction it contains. This is the gas that is consumed by the transaction upon validation. The entity (either a user or a contract) creating the transaction needs to decide two parameters, the gas limit and gas price. The gas limit is the maximum amount of gas the transaction is allowed to consume, if it is exceeded all gas is spent but the execution effects on the state are eliminated. This is useful to avoid too long or even infinite computations that would stall the EVM. Furthermore, each block has associated a block gas limit to guarantee a limit to the amount of computation executed by all the transactions in that single block. The gas price is instead set by the user as the amount of ether the user is willing to pay for each unit of gas. Miners are free to choose what transaction to mine and so they can refuse the ones with a gas price too low.

3.3.3 Smart Contracts

The term smart contract was introduced in 1994 by Nick Szabo in [34], when he first described how the computer-based execution of contracts between two parties could be secured without requiring any third party: "A set of promises, including protocols within which the parties perform on the other promises. The protocols are usually implemented with programs on a computer network, or in other forms of digital electronics, thus

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

these contracts are 'smarter' than their paper-based ancestors". In the blockchain context, it is generally related to computer code that is stored on a blockchain and that can be accessed by one or more parties. These programs are often self-executing and make use of blockchain properties like tamper-resistance, decentralised processing, and so on. In this interpretation, used for example by the Ethereum Foundation, a smart contract is not necessarily related to the classical concept of a contract, but can be any kind of computer program. It is called a 'contract' because the code that runs on Ethereum can control valuable things like ETH, currency notes or other digital assets [35].

The possibilities are infinite for smart contracts. They can be used to code and automate business processes that can be shared and executed among multiple parties offering increased trust and reliability in the process, often with significant gains in efficiency and cost reduction. Smart contracts can also be used to hard-code agreements between parties involving value and other types of asset transfer and allow them to be very transparent and run automatically based on predetermined rules, making it impossible for a party to back out.

3.3.4 Case study: Blockchain for Data Access Control

Due to its main characteristics Blockchain and Smart Contracts could be a trustable alternative infrastructure for implementing a Data Access Control Framework. In literature there are several studies proposing to consider blockchain as an infrastructure for access control systems.

Maesa et al [36] proposes to use blockchain technology to represent the rights to access resources and to transfer them from one user to another. The study uses the attribute-based access control mechanism and eXtensible Access Control Markup Language (XACML) [5] to define policies. The policies and the rights exchanges are publicly visible on the blockchain; accordingly, any user can know at any time the policy paired with a resource and the subjects who currently have the rights to access the resource. This solution allows distributed auditability, preventing a party from fraudulently denying the rights granted by an enforceable policy. The approach has been validated through a reference implementation based on Bitcoin. In their recent study [36] the same authors refined and extended the previous approach by considering smart contracts to enforce access control policies instead of simple transactions. They have implemented a proof of concept using XACML policies and Ethereum platform. In order to evaluate the feasibility and performance of the represented system, they have defined a new scenario where smart contracts are considered as resources that need to be protected and access to them is restricted. They have concluded that applying Ethereum to their implemented system has brought benefits in terms of flexibility and efficiency.

In the field of cloud storage [37] proposes a data storage and sharing scheme for decentralized storage systems combining a decentralized storage system, the Ethereum blockchain and the Attribute-Based Encryption (ABE) technology. The only one who has access to the secret key is the data owner. Ethereum

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

blockchain has been applied for managing the private keys. Essentially there are two smart contracts: the Data Sharing contract that is deployed by the data owner and includes methods to register a user who need access to the specific data belong to the owner of the contract and Data User contract that is deployed by data requester to invoke the search function defined in data sharing contract to view the search results. In a similar way, this study [37] proposes a Reputation Based Knowledge Sharing system to protect the copyright using fine-grained access control. The system includes three main roles: Questioner, Answerer, and Bystander. The Questioner is the one who designs a question. The answerer is one who is an expert to answer the question and receives rewards from Bystander. The Bystander is the one who is willing to pay a small fee in order to get access to the shared knowledge.

In the IoT field the management of attributes (e.g., location, date, time, etc.) is significant to provide a decentralized, flexible, and fine-grained authorisation for IoT devices. Attributes are significant as they are used to express specified access policies by a target to decide if the requested entity fulfils the required privileges that are necessary for access. Blockchain is utilized in such cases that allow authentic and reliable credentials. In different studies [38] [39] [40] [41] it is proposed an attribute-based access control mechanism for IoTs that provides local access, authorization of clients, privacy, and interoperability by using smart contract data sharing and user-controlled encoded policies. The user can own their data and have authority to share it with other users. The ABAC model is used for its high compatibility and expressiveness.

Blockchain has desirable features that make it a trustable alternative infrastructure for access control systems. The distributed nature of blockchain solves the problem of single point of failure and other centralized management problems. Also, by eliminating third parties, we do not need to be concern about privacy leakage from their side. In addition, we can have access to a trustable and unmodifiable history log. Consensus mechanisms are applied, so only valid transactions are recorded on blockchain. Furthermore, by using smart contracts, we can monitor and enforce access permissions under complex conditions. All these features have motivated researchers to consider blockchain as an infrastructure for access control systems. Current access control methods which are static might be inadequate for future systems and more dynamic access control methods, one in which resources define their own access control, might be required. Integrating blockchain with dynamic access control approaches could be an interesting area to investigate in the future.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

4 OneNet Data Access Policies (DAP)

4.1 OneNet Connector and Usage Control App

As described in the OneNet Reference Architecture in D5.2 [13], the IDS reference model and FIWARE architecture, play a fundamental role for the implementation of the core components of the OneNet Solution: the OneNet Decentralised Middleware and the OneNet Connector.

The OneNet Connector consists of a hybrid solution that includes the usage of IDS Connector and FIWARE Context Broker for ensuring a high level of standardization, interoperability, scalability, and reuse of OneNet solution.

Roles and Actors

As already described in the D5.1 [42], the OneNet Concept foresees, in line with the IDS reference models, a set of actors involved in the data exchange process: the OneNet Participants.

A OneNet participant can be divided into data source, data provider, data consumer and service provider.

- **Data Source** is the more generic source of data that could be integrated within OneNet system. It could be represented by a Data Provider (see below), a single database, an IoT device, a file system etc.
- **Data Provider** is a specific OneNet participant that provide data to the system. To submit metadata to a Broker, or exchange data with a Data Consumer, the Data Provider uses software components (OneNet connector) that are compliant with OneNet System. To facilitate a data request from a Data Consumer, the Data Provider should provide proper metadata about the data the Broker Service Provider (see below).
- **Data Consumer** receives data from a Data Provider. From a business process perspective, the Data Consumer is the mirror entity of the Data Provider; the activities performed by the Data Consumer are therefore similar to the activities performed by the Data Provider. Before the connection to a Data Provider can be established, the Data Consumer can search for existing datasets by making an inquiry at Broker Service Provider. The Broker Service Provider then provides the required metadata for the Data Consumer to connect to a Data Provider.
- **Service Provider** is a specific OneNet participant that provides services or tools. The Service Provider registers its services in the OneNet Framework in order to be used, integrated and tested within any cross-platform integration or orchestration process.

Decentralised Approach

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The OneNet platform should make sure that data providers and data consumers can rely on the identity of the members of the data ecosystem between different security domains, leveraging in a complete decentralised approach and maintain a high level of interoperability and reusability.

The OneNet Connector, using both the design model of the IDS Reference and FIWARE ecosystem can ensure all these characteristics.

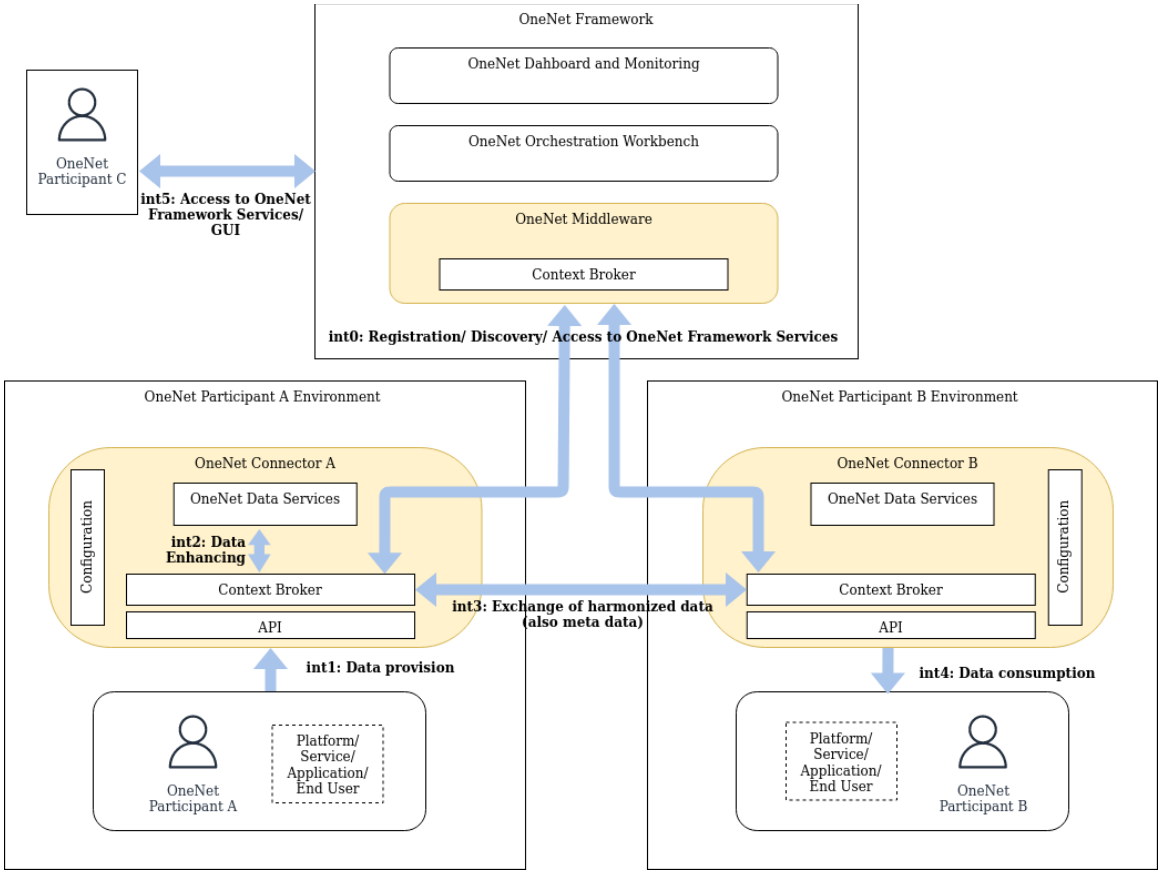

Figure 11: OneNet Decentralized Approach

OneNet Decentralised Middleware and the OneNet Connector are the core systems for enabling a seamless platforms integration and cooperation for cross-platform market and network operation services and at the same time makes available and accessible data from different sources (the OneNet Participants) in a secure and trusted way ensuring data ownership and privacy.

As described in D5.2 [13], while the OneNet Decentralised Middleware offers central features to all the OneNet participants like identity management, sources discovery, semantic annotation, vocabularies and ontologies, the OneNet Connector is a decentralised instance of the OneNet Middleware itself and is responsible for the execution of the complete data exchange process.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Each OneNet Participant will be able to deploy and configure its own connector that will include:

- UI Configuration tool
- Set of interoperable APIs for the connection with already existing Platform/Application/Services
- OneNet Data services (a detailed list of the Data Services is provided in D5.3 [43])

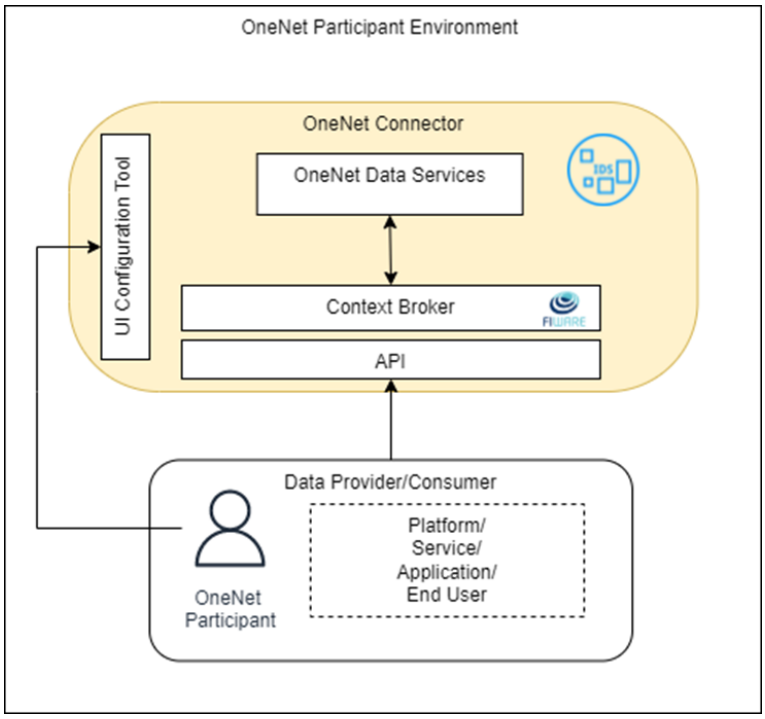

Figure 12: OneNet Connector High Level Concept

The OneNet Connector extends the reference implementation of a generic IDS connector and therefore follows the specifications and guidelines of the IDS Reference Model and therefore must ensure services such as:

- Identity Management
- Management of Metadata
- Clearing House
- **Access and Usage Control**
- Configuration

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

As described in Ch.3.1, access and usage control policies are fundamental aspect in the IDS. For supporting the definition of the policies, the OneNet Connector must support the IDS Usage Control Language based on ODRL [44].

4.1.1 Access and Usage Control

The OneNet Connector will be deployed and integrated in many platforms for implementing cross-platform services in which the data exchange plays a fundamental role. For implementing these cross-platform services in a secure and trusted manner will be fundamental to define data access and usage policies within each instance of the OneNet Connector.

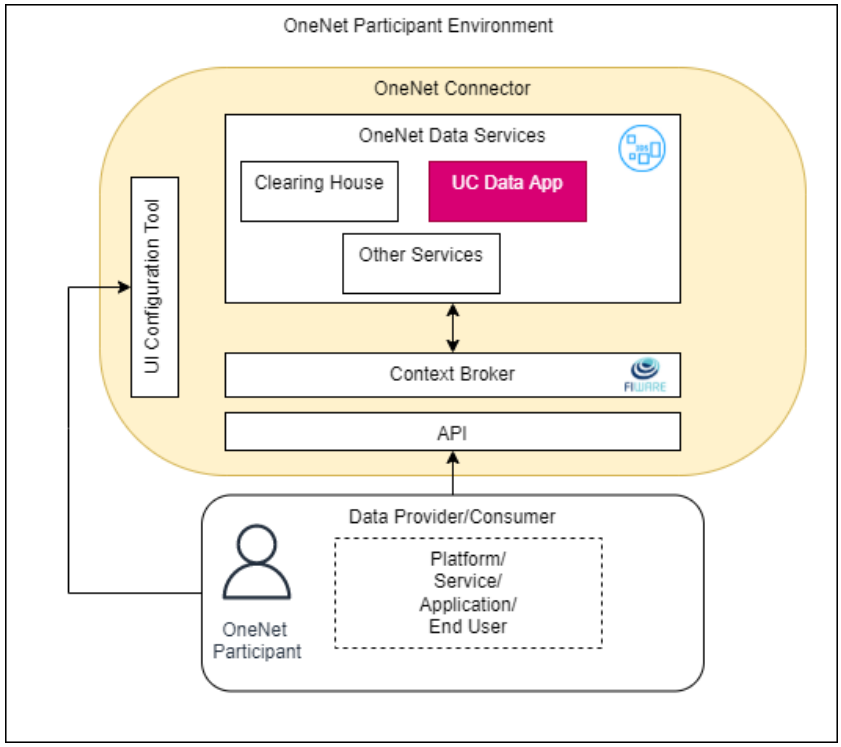

Figure 13: OneNet Connector and Usage Control App

As shown in Figure 13 The OneNet Connector will integrate a series of OneNet Data services, among which a **Usage Control App (UC App) for implementing the Access and Usage Control in OneNet**

Based on the analysis of the Access and Usage Control concepts conducted in the previous paragraphs, mainly focusing in the IDS guidelines and specifications, the implementation of the UC App should cover three main aspects:

- Data Control Management

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

- Data Policies Definition
- Data Policies Enforcement

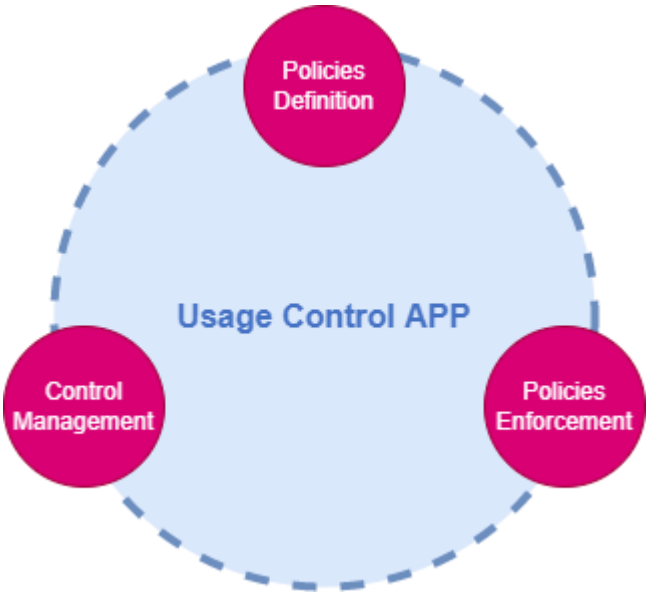

Figure 14: Usage Control App design concept

Data Control Management

The UC App should be able to apply all the defined policies to any data exchange interacting with the OneNet Connector and should allow the possibility to administrate the overall data access and usage control process.

Policy Definition Dashboard

OneNet Participant that acts as Data Provider must be able to create at runtime its Data Usage Control policies, to be applied to different data exchanges. A policy specification dashboard should support the Data Provider in the process of policy specification.

The Policy Definition Dashboard should be offered as a GUI for facilitating the creation and management of the policies.

As an example, the following rule, shown in Figure 15, describes the time interval in which it is allowed to access the resource with a specific identifier defined using the “target” property of the rule.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

```
{
    "@context": "http://www.w3.org/ns/odrl.jsonld",
    "@type": "ids:ContractAgreement",
    "uid": "http://example.com/policy/restrict-access-interval",
    "profile": "http://example.com/ids-profile",
    "target": "http://w3id.org/engrd/connector/artifact/1",
    "provider": "http://example.com/party/my-party",
    "consumer": "http://example.com/party/consumer-party",
    "permission": [{
            "action": "ids:use",
            "constraint": [{
                    "leftOperand": "ids:datetime",
                    "operator": "gt",
                    "rightOperand": {
                        "@value": "2020-10-01T00:00:00Z",
                        "@type": "xsd:datetime"
                    }
                },
                {
                    "leftOperand": "ids:datetime",
                    "operator": "lt",
                    "rightOperand": {
                        "@value": "2021-10-31T23:59:59Z",
                        "@type": "xsd:datetime"
                    }
                }]
        }]
}
```

Figure 15: Time-Based Interval Policy

Policy Enforcement Tool

As described on Ch.3.1.1, for implementing policy enforcement is necessary to intercepts events or data flows and enforces a decision based on specified policies. The Policy Enforcement Tool should be able to monitor, filter and mask data based on the predefined rules (e.g., anonymize personal data, remove specific information, send notifications and alerts). It should also be able to add additional enforcement rules based on external information like location, context and purpose.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The OneNet Connector will definitely include the Usage Control Data App for covering all the aspects described above. Following the analysis conducted about already existing technologies for implementing IDS based Access and Usage control, it would be an important advantage if the OneNet connector, through its Usage Control App, was compatible with the most used and promising technologies, like MYDATA (see Ch.3.1.2)

As an example, the following rule, shown in Figure 16, describes an enforcement policy for anonymization of the payload. In this case, the enforcement policy will modify the payload response.

```
{
    "@context": "http://www.w3.org/ns/odrl.jsonld",
    "@type": "ids:ContractAgreement",
    "uid": "http://example.com/policy/anonymize-in-transit",
    "profile": "http://example.com/ids-profile",
    "target": "http://w3id.org/engrd/connector/artifact/2",
    "provider": "http://example.com/party/my-party",
    "consumer": "http://example.com/party/consumer-party",
    "permission": [
        {
            "action": "ids:use",
            "preobligation": [{
                    "action": [{
                            "rdf:value": {
                                "@id": "ids:anonymize"
                            },
                            "refinement": [
                                {
                                    "leftOperand": "ids:modificationMethod",
                                    "operator": "eq",
                                    "rightOperand": {
                                        "@value": "http://example.com/anonymize/replace",
                                        "@type": "xsd:anyURI"
                                    },
                                    "replaceWith": {
                                        "@value": "xxxx",
                                        "@type": "xsd:string"
                                    },
                                    "jsonPath": "$.dateOfBirth"
                                }]
                        }]
                }]
        }]
}
```

Figure 16: Anonymization Enforcement Policy

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

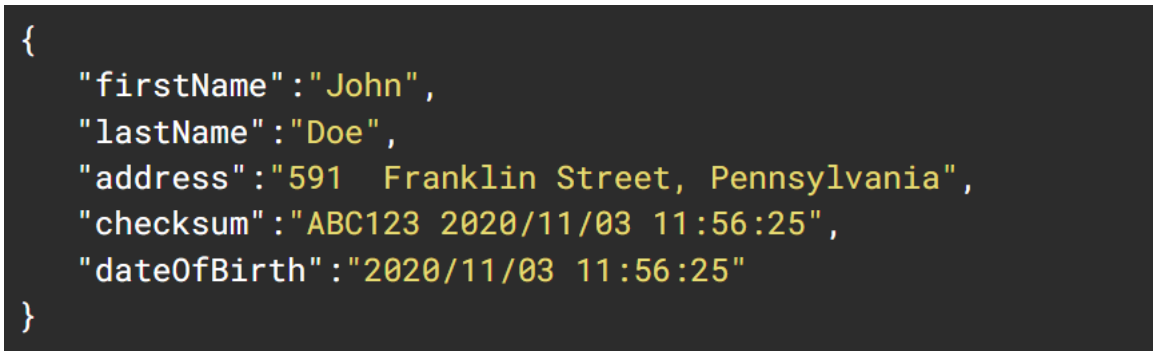

Figure 17: Original Payload

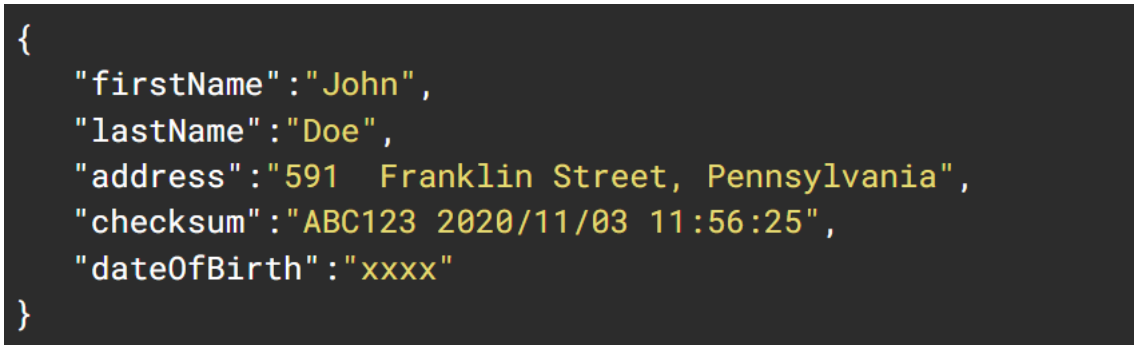

Figure 18: Anonymized Payload

4.2 OneNet Data Access Policies (DAP) Framework

The approaches proposed by IDS, specification of Data Policies and technical enforcement, are aligned with the demanded concepts for OneNet Data Enforcement Policies Design and for defining the OneNet Data Access Policies Framework.

For this reason, the OneNet Data Access Policies Framework will be defined following the IDS Usage Control concept and will be implemented at Connector Level (see Ch.3.1.1).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

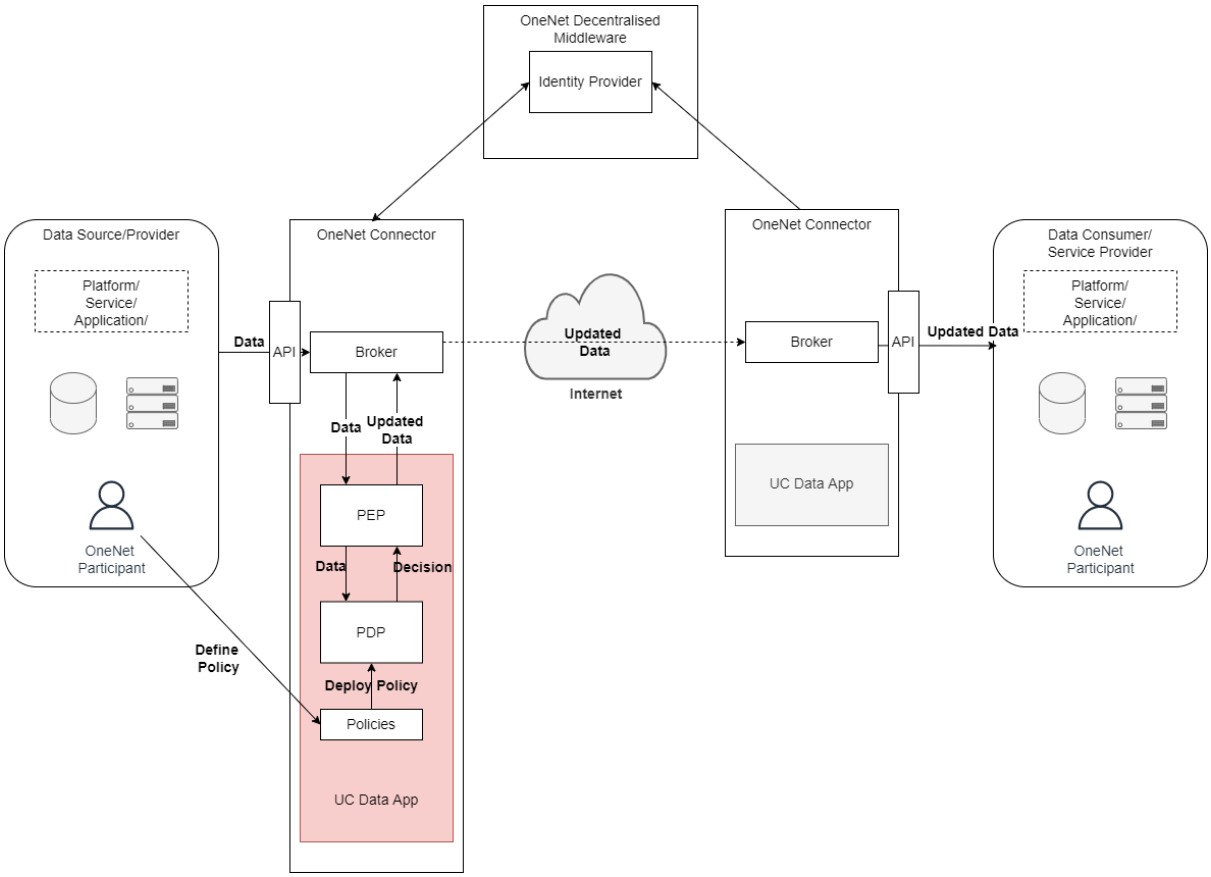

Figure 19: OneNet Data Access Policies Framework (DAP)

In the Figure 19 above, is represented the architecture of the OneNet Data Access Policies Framework (DAP). The Usage Control at Data Provider Side is applied whenever data is processed by the OneNet Connector. The OneNet connector is responsible to manage the data exchange and integrates the Usage Control App that is able to intercept the data exchanged. To ensure full data control, the Usage Control App has to be invoked last before data is leaving the OneNet Connector at Data Provider Side.

Within the Usage Control App, the PEP intercepts the data flow, transform it to a decision request and send it to the PDP for the policy evaluation. At the same time, the OneNet Participant is able to define the policies that will be deployed in the PDP in the form of IDS contracts. The PDP evaluates the decision request using the specific policy and returns the authorization decision to the PEP. Finally, the PEP enforces the decision in the intercepted data flow and send back the data (accordingly updated).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

5 Conclusions

The OneNet system is manly focused on data exchange and aims to create a shared data space at a European level for energy stakeholders. Thus, it needs to implement a management of access control and use of data, during any data exchange.

In this context, starting from an analysis of the concept of standard data access control, which therefore only provides control on the data access by the consumers (based on RBAC roles, or ABAC attributes), it immediately became clear how the concept of Data Usage Control provided by IDS was more fitting with the objectives and technologies proposed by OneNet.

The reference model proposed by IDS is in line with that foreseen for the OneNet system and in particular the management of a data control at the OneNet Connector level was considered the most suitable for the needs of the system.

Starting from the reference model of IDS and the architectural design of the OneNet Middleware and the OneNet Connector, a OneNet Data Access Policies (DAP) Framework has been proposed for the management of access control and use of data which includes a Usage Control App within the connector itself and therefore available to every OneNet Participant. This ensures that every platform connected to the OneNet system uses the UC App and that the policies defined by the data provider are applied to every data exchange.

The policies can be defined by the Data providers based on the classes suggested by the IDS reference model through a configuration dashboard. The UC App included within the OneNet Connector will give the possibility to create at least a series of policies defined as basic for the project and for the various demos and use cases but will be extensible with new policies and new classes (see Table 1).

The technologies to be used for the implementation of the UC App will be decided in the implementation phase, but this document clearly provides an overview of the most used technologies that offer greater benefits (e.g., compatibility with MYDATA Framework), based on completely open-source technologies (FIWARE Architecture) or which may be more innovative (use of Blockchain technology).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

6 References

[1] European Commission - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Energy Roadmap 2050 - COM(2011) 885/2 – http://ec.europa.eu/energy/energy2020/roadmap/doc/com_2011_8852_en.pdf (last accessed: DATE)

[2] E. Commission, «European Commission adopts new tools for safe exchanges of personal data,» 4 June 2021. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/it/ip_21_2847.

[3] E. Commission, «A European Strategy for data,» 23 February 2022. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/strategy-data.

[4] E. Commission, «Commission Implementing Decision on the financing of the Digital Europe Programme and the adoption of the multiannual work programme for 2021 - 2022,» 10 November 2021. [Online]. Available: https://ec.europa.eu/newsroom/repository/document/2021-46/C_2021_7914_1_EN_annexe_acte_autonome_cp_part1_v3_x3qnsqH6g4B4JabSGBy9UatCRc8_81099.pdf.L. STÄHLER, «A Close Look at European Data Spaces and Usage Control: DRM for Data?,» 15 February 2022. [Online]. Available: https://www.law.kuleuven.be/citip/blog/a-close-look-at-european-data-spaces-and-usage-control/.

[5] O. OPEN, «OASIS eXtensible Access Control Markup Language (XACML) TC,» 2020. [Online]. Available: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.

[6] Chadwick, David & Otenko, Sassa & Nguyen, Tuan Anh. (2006). Adding Support to XACML for Dynamic Delegation of Authority in Multiple Domains. 67-86. 10.1007/11909033_7.

[7] «International Data Space,» [Online]. Available: https://internationaldataspaces.org/.

[8] IDSA, «Usage Control in the International Data Spaces - Position Paper,» March 2021. [Online]. Available: https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Position-Paper-Usage-Control-in-the-IDS-V3..pdf.

[9] Fraunhofer IESE, «MYDATA Control Technologies,» [Online]. Available: https://www.mydata-control.de/.

[10] Fraunhofer IESE, «IND2UCE Framework,» [Online]. Available: https://www.iese.fraunhofer.de/en/services/security/ind2uce-framework.html.

[11] J. Schütte e G. S. Brost, «LUCON: Data Flow Control for Message-Based».

[12] «Apache Camel,» [Online]. Available: https://camel.apache.org/.

[13] OneNet Deliverable 5.2 “OneNet reference architecture” (Confidential deliverable)

[14] FIWARE, «FIWARE Identity Manager - Keyrock,» [Online]. Available: https://fiware-idm.readthedocs.io.

[15] FIWARE, «FIWARE PEP Proxy - Wilma,» [Online]. Available: https://fiware-pep-proxy.readthedocs.io/en/latest/.

[16] FIWARE, «AUTHZFORCE CE,» [Online]. Available: https://authzforce-ce-fiware.readthedocs.io.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

[17] FIWARE Academy, «FIWARE Orion-LD - Linked Data Context Broker,» [Online]. Available: https://fiware-academy.readthedocs.io/en/latest/core/orion-ld/index.html.

[18] FIWARE, «FIWARE NGSI-LD,» [Online]. Available: https://ngsi-ld-tutorials.readthedocs.io/en/latest/.

[19] FIWARE, «FIWARE Cosmos,» [Online]. Available: https://fiware-cosmos.readthedocs.io/en/latest/.

[20] FIWARE, «FIWARE Draco,» [Online]. Available: https://fiware-draco.readthedocs.io/en/latest/.

[21] Muñoz, Jose & López-Pernas, Sonsoles & Pozo Huertas, Alejandro & Alonso, Alvaro & Salvachua, Joaquin & Huecas, Gabriel. (2020). Data Usage and Access Control in Industrial Data Spaces: Implementation Using FIWARE. Sustainability. 12. 3885. 10.3390/su12093885.

[22] IDSA, «IDSA Position Paper Blockchain Technology in IDS,» March 2019. [Online]. Available: https://zenodo.org/record/5675962/files/IDSA-Position-Paper-Blockchain-Technology-in-IDS.pdf.

[23] "Could Blockchain Have as Great an Impact as the Internet?," [Online]. Available: https://www.jpmorganchase.com/news-stories/could-blockchain-have-great-impact-as-internet.

[24] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[25] A. Rosic, "Blockchain Consensus: A Simple Explanation Anyone Can Understand," [Online]. Available: https://blockgeeks.com/guides/blockchain-consensus/.

[26] "Bitcoin - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Bitcoin.

[27] "Byzantine Fault - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Byzantine_fault.

[28] "Proof-of-Work - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Proof_of_work#Bitcoin-type_proof-of-work.

[29] Different Blockchain Consensus Mechanisms," 10 November 2018. [Online]. Available: https://hackernoon.com/different-blockchain-consensus-mechanisms-d19ea6c3bcd6.

[30] "Ethereum Whitepaper," July 2019. [Online]. Available: https://ethereum.org/en/whitepaper/.

[31] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger," [Online]. Available: http://gavwood.com/paper.pdf.

[32] "Ethereum website," [Online]. Available: https://ethereum.org/en/.

[33] "Solidity documentation," [Online]. Available: https://docs.soliditylang.org/en/develop/.

[34] N. Szabo, "The Idea of Smart Contracts," Nick Szabo's Papers and Concise Tutorials, vol. 6.

[35] "How Ethereum works," [Online]. Available: https://ethereum.org/en/learn/#how-ethereum-works.

[36] D. D. F. Maesa, P. Mori and L. Ricci, "Blockchain Based Access Control," IFIP International Conference on Distributed Applications and Interoperable Systems, pp. 206-220, 2017.

[37] S. Wang, Y. Zhang and Y. Zhang, "A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems," IEEE Access, vol. 6, 2018.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

[38] S. Zaidi, M. Shah, H. Khattak, C. Maple, H. Rauf, A. El-Sherbeeny and M. El-Meligy, "An Attribute-Based Access Control for IoT Using Blockchain and Smart Contracts," Sustainability, 2021.

[39] L. Song, M. Li, Z. Zhu, P. Yuan and Y. He, "Attribute-Based Access Control Using Smart Contracts for the Internet of Things," Procedia Computer Science, vol. 174, pp. 231-242, 2020.

[40] H. Liu, D. Han and D. Li, "Fabric-iot: A Blockchain-Based Access Control System in IoT," IEEE Access, vol. 8, pp. 18207-18218, 2020

[41] Y. Zhang, B. Li, B. Liu, J. Wu, Y. Wang and X. Yang, "An Attribute-Based Collaborative Access Control Scheme Using Blockchain for IoT Devices," Electronics, 2020.

[42] OneNet Deliverable 5.1 "OneNet Concept and Requirements" https://onenet-project.eu/public-deliverables/

[43] OneNet Deliverable 5.3 "Data and Platform Assets Functional Specs and Data Quality Compliance" (Confidential deliverable)

[44] W3C, «ODRL Information Model 2.2,» [Online]. Available: https://www.w3.org/TR/odrl-model/.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

This paper reflects only the author's view and the Innovation and Networks Executive Agency (INEA) is not responsible for any use that may be made of the information it contains.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739