Enershare

The Energy Data Space for Europe

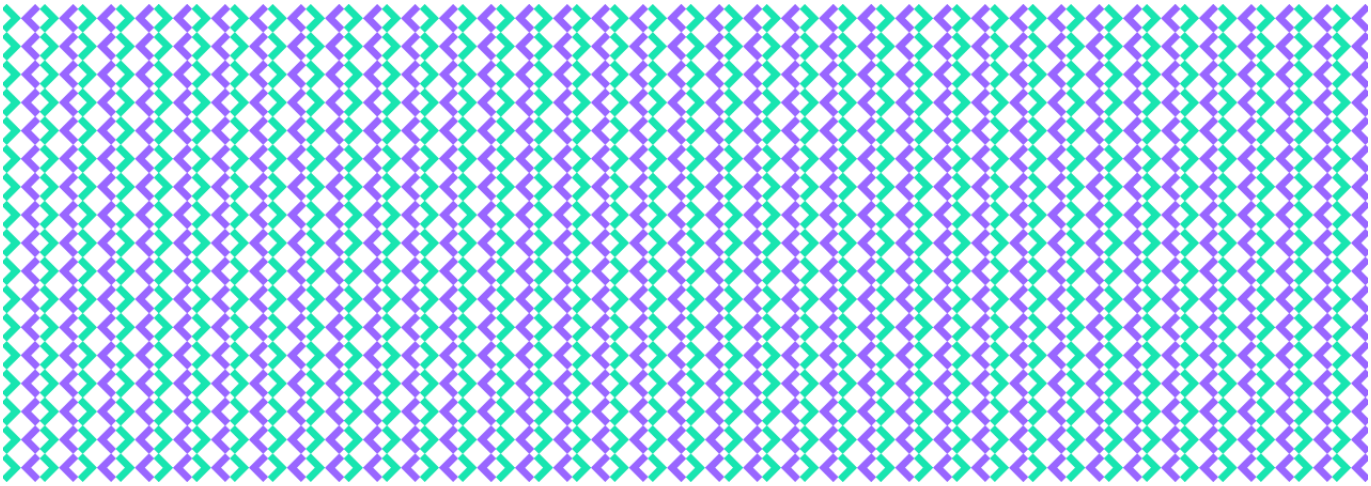
European Common Energy Data Space Framework Enabling Data Sharing - Driven Across – and Beyond – Energy Services

www.enershare.eu

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

D4.1 ENERSHARE Trust and sovereignty building blocks

Alpha version




Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Publication details

Grant Agreement Number	101069831
Acronym	ENERSHARE

Full Title	European Common Energy Data Space Framework Enabling Data Sharing-Driven Across — and Beyond — Energy Services
Topic	HORIZON-CL5-2021-D3-01-01 'Establish the grounds for a common European energy data space'
Funding scheme	HORIZON-IA: Innovation Action
Start Date	Jul 1, 2022
Duration	36 months
Project URL	https://enershare.eu
Project Coordinator	Engineering
Deliverable	D4.1. – ENERSHARE Trust and sovereignty building blocks. Alpha version
Work Package	WP4 – Trust and sovereignty enabling framework and building blocks
Delivery Month (DoA)	M11
Version	1.0
Actual Delivery Date	July 17, 2023
Nature	Report
Dissemination Level	PU
Lead Beneficiary	TNO

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Authors	Sonia Jimenez (IDSA), Alessandro Rossi (ENGINEERING), Rizwan Mehmood (FRAUNHOFER), Rieks Joosten, Simon Dalmolen, Maarten Kollenstart, Michiel Stornebrink (TNO), David Campo (FIWARE), Idoia Murua (TECNALIA), Xabier Yurrebaso Asua (TECNALIA), Fábio Coelho (INESC TEC)
Quality Reviewer(s)	Volker Berkhout (FRAUNHOFER) and Vincenzo Croce (ENGINEERING)
Keywords	Identy and access management, usage control, trust, sovereignty, full stack integrity, blockchain, ledger

Document history

Ver	Date	Description	
0.1	Mar 30	Table of content	
0.5	April	Contents for sections on IAM, Usage control	
0.6	May	Contents for sections FSI and DLT	
0.8	May 22	Introduction + conclusions, combining pilots requirements on document level	
0.9	May 24	Consolidated version ready for review	
0.99	June	Review comments processed	
1.0	July 17	Final version	

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Table of Contents

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

1 Introduction

1.1 About the project

The overall vision of ENERSHARE is to develop and demonstrate a European Common Energy Data Space which will deploy an '**intra-energy**' and '**cross-sector**' interoperable and trusted Energy Data Ecosystem. Private consumers, business (energy and non-energy) stakeholders and regulated operators will be able to **access, share and reuse**, based upon voluntary agreements (or legal obligations where such obligations are in force): (a) Large sources of currently fragmented and dispersed data; (b) Data-driven cross-value chain (energy and non-energy) services and Digital Twins for various purposes.

1.2 About this document

This deliverable, which is the first of a series of 3 (alpha, beta and final version), presents the preliminary results of the work in WP4, whose focus is on the framework and building blocks providing trust and sovereignty in the energy data space.

This deliverable accompanies the software components that are provided to WP8 for the integration in the energy data space.

Furthermore, this deliverable outlines the next steps and design for the 2nd technology release of the trust and sovereignty building blocks.

1.3 Intended audience

The intended audience for this deliverable is:

- All project partners that are involved in WP4. This document contains the (high-level) designs of the building blocks for the next technology release
- All project partners from other WPs (especially WP5). This document contains the scope and building blocks that are considered part of the trust and sovereignty framework. It allows others to understand what building blocks can and cannot be expected from WP4.
- All project partners involved in integration (WP8) and pilot implementations (WP9). This document addresses what building blocks are provided as part of the 1st technology release and how and which pilot requirements are addressed.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- External stakeholders to the project that would like to be part of the ENERSHARE energy data space and need to integrate and deploy trust and sovereignty building blocks.

1.4 Reading recommendations

This document is divided into 8 chapters.

- Chapter 1 is this introduction.
- Chapter 2 provides an overview and context information about how we define trust and sovereignty and scope the building blocks.
- Chapter 3 provides the link with the pilot requirements for trust and sovereignty.
- The chapters 4 to 7 address the work carried out the the four tasks of WP4 and elaborating on the task objectives, the state of the art and the high level designs and plans for the second technology release.
- Chapter 8 provides the conclusion of this deliverable, including an overview of the (software) components for the alpha release and summarizes work to be carried out for the second technology release.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

2 Overview Trust and Sovereignty

2.1 Introduction to OPENDEI

OPENDEI is an initiative that describes a soft infrastructure for European data spaces. This soft infrastructure consists of 12 building blocks that are divided into four groups as shown in Figure 1.

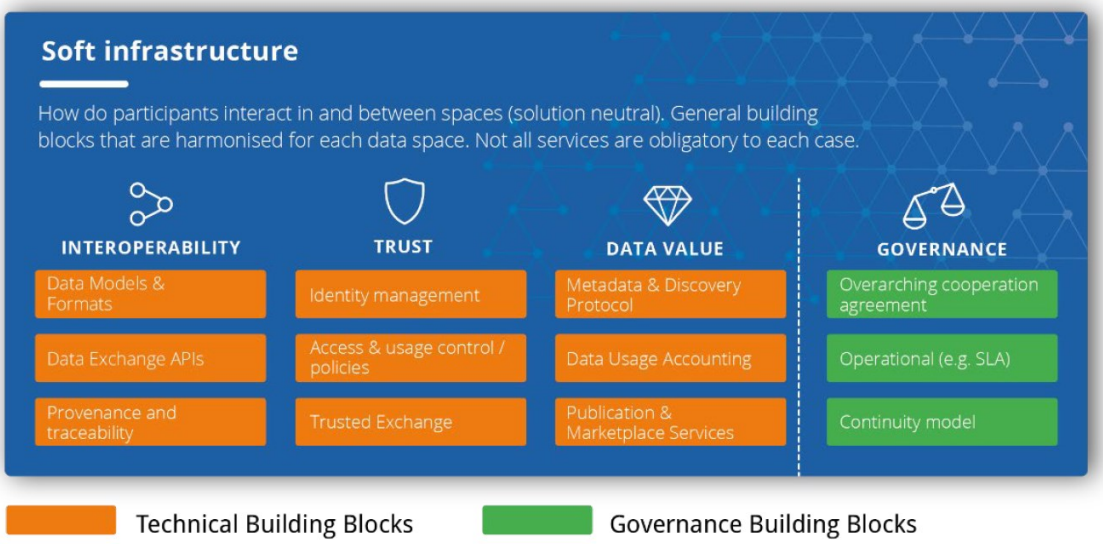


FIGURE 1: OPENDEI DATA SPACE BUILDING BLOCKS

Source: Design Principles for Data Spaces [1]

One of the groups of building blocks that are shown in Figure 1 is Trust. This group contains three building blocks that facilitate trust and data sovereignty, and are relevant for the current deliverable.

The first building block in Trust is Identity Management (IM), which enables identification, authentication, and authorisation of parties in a data space. The second building block is Access and Usage Control/Policies. The aim of this building block is to guarantee the enforcement of data access and -usage policies. The third and last building block is Trusted Exchange, which, as the name suggests, facilitates the trusted exchange of data between parties in terms of trusted identities and compliance with defined rules/agreements.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

2.2 Data space connectors as starting point

A data space consists of a network of parties and components. In the International Data Spaces Reference Architecture Model (IDS-RAM) this network is formed by connectors. In other words, each component or service in a data space is represented by a connector.

An IDS connector allows and enables the exchange of data within a data space. It provides a number of core functions that are extended with business logic inside a data app. Among the Connector Core Service(s) are the means for Authentication, Contract Negotiation and Trusted Data Exchange[1].

One example of the Connector Core Services is the TNO Security Gateway (TSG)[2] Core Container. This container serves as a foundation for core data space components[3] and can be enhanced with data apps. These data apps can implement business logic for both data providers and consumers. Additionally, an alternative implementation called the TRUE[4] connector is also available. In the Enershare project, both implementations will be utilized, and they are designed to be interoperable with each other through the dataspace protocol.

Connectors play a crucial role in data spaces, such as international data spaces, for several reasons:

1. Data Integration: Connectors enable the integration of diverse data sources and systems within a data space. They provide the necessary interfaces and protocols to connect and exchange data between different platforms, applications, and organizations. By establishing interoperability, connectors facilitate seamless data sharing and collaboration.
2. Standardization: Connectors help enforce standardized data formats, protocols, and security measures across the data space. They ensure that data can be understood and processed consistently, regardless of the source or destination. Standardization promotes data quality, reduces errors, and enables efficient data exchange between participants.
3. Data Governance: Connectors play a crucial role in implementing data governance policies within a data space. They help enforce access controls, data usage agreements, and privacy regulations. Connectors enable organizations to define and enforce rules

[1] https://docs.internationaldataspaces.org/ids-ram-4/layers-of-the-reference-architecture-model/3-layers-of-the-reference-architecture-model/3_5_0_system_layer/3_5_2_ids_connector
[2] https://tno-tsg.gitlab.io/
[3] such as the Identity Provider, the Metadata Broker, the Clearing House, the Vocabulary Hub and the App Store
[4] https://github.com/Engineering-Research-and-Development/true-connector

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

for data sharing, ensuring compliance with legal, regulatory, and contractual obligations.

4. Scalability and Flexibility: Connectors provide a scalable and flexible architecture for data spaces. They allow for the addition or removal of data sources and applications without disrupting the overall data ecosystem. Connectors enable the expansion of the data space, accommodating new participants and data types, and adapting to evolving business requirements.
5. Data Security: Connectors play a vital role in establishing secure connections and protecting data integrity within a data space. They facilitate encrypted data transmission, authentication mechanisms, and authorization protocols. Connectors enable secure data access and transfer, mitigating the risks associated with unauthorized data exposure or breaches.
6. Interoperability: Connectors enable data interoperability by facilitating the seamless flow of data between different systems, platforms, and technologies. They bridge the gap between diverse data sources, ensuring compatibility and enabling data exchange across various formats, structures, and standards. Interoperability allows organizations to leverage data from multiple sources, unlocking new insights and value.

In summary, connectors are essential in data spaces like international data spaces as they enable data integration, standardization, data governance, scalability, data security, and interoperability. They facilitate seamless data sharing and collaboration, empowering organizations to leverage the full potential of their data assets and drive innovation.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

3 Pilot requirements on trust and sovereignty

3.1 Building blocks identified

Based on the use case descriptions and the analysis of the information provided by the pilots, ENERSHARE D2.1 [2] created a list of technical building blocks of data spaces with the number of scenarios that require these building blocks.

TABLE 1 - LIST OF TECHNICAL BUILDING BLOCKS OF DATA SPACES WITH THE NUMBER OF SCENARIOS THAT REQUIRE THESE BLOCKS

Building Block Category	Building Block name	Number of Scenarios
Technical	Data Models and Formats	22
	Data Exchange APIs	22
	Identity Management	21
	Trusted Exchange	21
	Data Processing	15
	Metadata and Discovery Protocol	16
	Access and Usage control / Policies	16
	Publication and Marketplace Services	13
	System Adaptation	9
	Provenance and traceability	7
	Data Visualisation	5
	Data Analytics Engine	4
	Workflow Management Engine	3
	Data Routing and Preprocessing	3
	Data Usage Accounting	1

As shown in the table, building blocks for Trusted Exchange and Identity Management are required in 21 scenarios and Access and Usage control /Policies is required in 16 scenarios. These building blocks are in scope for WP4.

The data space connector implementations, as described in section 2.2 will enable the secure/trusted exchange of data. The connectors are at the basis of data sharing in the energy

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

data space. The building block Identity Management is addressed in chapter 4 and the building block for Access and Usage control / Policies is addressed in both chapter 4 and 5.

3.2 Requirements on access and usage policies

To understand more about the access and usage policies that ensure large part of the trusted exchange, we looked into 4 use cases in more details. The following sections elaborate on the requirements these pilots have regarding access and usage policies.

3.2.1 P1-ES: Wind farm integrated predictive maintenance and supply chain optimization

Pilot #1 “Wind farm integrated predictive maintenance and supply chain optimization” will require the support of complex rules that will be a combination of the following policy patterns, to specify the usage restrictions to be fulfilled by the consumers:

- Connector-restricted Data Usage: allow data usage for specific connectors associated to the companies that will take part in the pilot.
- Interval-restricted Data Usage: allow data usage during the interval corresponding to the duration of the ENERSHARE project, that is, till 30th June 2025.
- Purpose-restricted Data Usage Policy: allow data usage within the scope of ENERSHARE project.

3.2.2 P2-PT-A: Leveraging on consumer-level load data to improve TSO’s operational and planning procedures.

Pilot #2-A will use behind-the-meter data to improve operational and planning procedures of the Portuguese transmission system operator (TSO), using smart devices from the Energy Data Space. Thus, it will require a combined set of rules to limit the recipients and use of data. The specific usage rules follow:

- Connector-restricted Data Usage: allow data usage for specific connectors associated to the companies that will take part in the pilot.
- Interval-restricted Data Usage: allow data usage during the interval corresponding to the duration of the ENERSHARE project, that is, till 30th June 2025.
- Purpose-restricted Data Usage Policy: allow data usage within the scope of this pilot within ENERSHARE project.
- Personal Data: filter out the contents of the data according to the data subject´s consents, particularly stemming from consumers at the community.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

3.2.3 P2-PT-B: Instantiation of energy communities and digital simulation of business models.

Pilot #2-B will use cross-silo data stemming from several data owners to improve operational and planning procedures of a Renewable Energy Community using smart devices from the Energy Data Space. Thus, it will require a combined set of rules to limit the recipients and use of data. The specific usage rules follow:

- Connector-restricted Data Usage: allow data usage for specific connectors associated to the companies that will take part in the pilot.
- Interval-restricted Data Usage: allow data usage during the interval corresponding to the duration of the ENERSHARE project, that is, till 30th June 2025.
- Purpose-restricted Data Usage Policy: allow data usage within the scope of the ENERSHARE project.
- Anonymize: Specific JSON property values are modified.
- Personal Data: filter out the contents of the data according to the data subject´s consents, particularly stemming from consumers at the community.

3.2.4 P2-PT-C: Detect irregularities in energy consumption in households with seniors living alone.

Pilot #2-C will use data stemming from EMSs in houses with senior residents to trigger alarms taken from abnormal energy consumption patterns. Thus, it will require a combined set of rules to limit the recipients and use of data. The specific usage rules follow:

- Connector-restricted Data Usage: allow data usage for specific connectors associated to the companies that will take part in the pilot.
- Interval-restricted Data Usage: allow data usage during the interval corresponding to the duration of the ENERSHARE project, that is, till 30th June 2025.
- Purpose-restricted Data Usage Policy: allow data usage within the scope of the ENERSHARE project.
- Anonymize: Specific JSON property values are modified.
- Personal Data: filter out the contents of the data according to the data subject´s consents, particularly stemming from consumers at the community.
- Usage notification: the data provider is notified periodically if and for what purpose was its data used.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

3.2.5 P2-PT-D: Improve quality of living and energy consumption in households by detecting higher energy consumptions of appliances early on and increase energy efficiency by suggesting maintenance or replacement of appliances.

Pilot #2-D will use disaggregated data to offer a preventing maintenance service for home appliances. Thus, it will require a combined set of rules to limit the recipients and use of data. The specific usage rules follow:

- Connector-restricted Data Usage: allow data usage for specific connectors associated to the companies that will take part in the pilot.
- Interval-restricted Data Usage: allow data usage during the interval corresponding to the duration of the ENERSHARE project, that is, till 30th June 2025.
- Purpose-restricted Data Usage Policy: allow data usage within the scope of the ENERSHARE project.
- Anonymize: Specific JSON property values are modified.
- Personal Data: filter out the contents of the data according to the data subject´s consents, particularly stemming from consumers at the community.
- Usage notification: the data provider is notified periodically if and for what purpose was its data used.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

4 Identity and access management

4.1 Task objectives

Trust is one of the main pillars of data spaces and Identity and Access Management is a key building block that fosters trust. This task will provide the necessary building blocks for allowing identification, authentication, and authorization of the EnerShare partipants.

The objectives of T4.2 - Identity and Access Management (IAM) can be summarized as follows:

- Analysis of existing IAM building blocks
- Evaluation of IAM requirements for EnerShare
- Definition of reference IAM implementation to establish a certificate mechanism to identify entities and/or devices in a secure manner.
- Implementation of the process of validating the data against the issued certificates

The primary expected outcome for this task is to provide the necessary building blocks to enable identification, authentication, and authorization of stakeholders operating within the EnerShare Data Space.

Throughout the initial months of the project, our focus has been on exploring and analyzing existing definitions, specifications, and implementations of IAM building blocks. Additionally, we have conducted an initial evaluation of the IAM requirements specific to the EnerShare pilots. In this chapter, we will delve into the details of the identified building blocks and implementations that we plan to consider for EnerShare, along with an outline of our roadmap for the upcoming months.

4.2 State of the art

We have selected and documented the building blocks provided by the DSBA and its integrating partners (mainly IDSA and FIWARE) as the overall architecture of EnerShare will be aligned with these two initiatives and they already provide specifications and documented implementations of these building blocks. Additionally, we will leverage and further develop the work conducted by the InterConnect project.

4.2.1 IDS components involved in IAM (Data connectors, CA, DAPS, ParIS)

To be able to make access control related decisions that are based on reliable identities and properties of participants, a concept for Identity and Access Management (IAM) is mandatory. To access resources in the IDS, aspects of identification (i.e., claiming an identity),

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

authentication (i.e., verifying an identity), and authorization (i.e., making access decisions based on an identity) need to be defined.

The Identity Provider (IdP) in the IDS consists of three complementary components: Certificate Authorities (CAs) issue and manage technical identity claims, the Dynamic Attribute Provisioning Service (DAPS) provides short-lived tokens with up-to-date information about connectors, and the Participant Information Service (ParIS) provides business-related information of IDS Participants in machine- and human-readable manners.

Certificate Authorities (CAs)

One or multiple CAs issue identity certificates for connector instances by signing Certificate Signing Requests (CSRs) that have been handed in by valid connector instances. Each connector instance is made up of:

- The platform the IDS connector instance depends on. A platform consists of hardware, firmware, operating system and (container) run-time environment.
- The Connector Core Services (CCS) software artifacts that provide management functionality and IDS interoperability.
- The configuration of an IDS connector (defined data routes, configured Usage Control (UC) framework).
- The IDS Apps or other services (e.g., Clearing House (CH) services) that are bound to this connector instance.

The CAs revoke certificates that become invalid and, for higher trust levels, assure that private keys are properly stored in hardware modules, such as a Trusted Platform Module (TPM) or Hardware Security Module (HSM). They are essential trust building entities responsible for ensuring that only registered organizations may operate components in the IDS.

Dynamic Attribute Provisioning Service (DAPS)

A DAPS enriches connector identities by issuing up-to-date information in the form of signed claims. It embeds them into Dynamic Attribute Tokens (DATs) which are handed out to requesting IDS connector instances. The DAPS verifies the current status/validity of Software Manifests (SM) and Company Descriptions (CD) which contain metadata regarding passed IDS certifications (see 4.1.2). Simultaneously it delivers dynamic attributes, such as device location or currently supported transport certificates, which may dynamically change over time and are linked to the connector identity based on the DAT. Thus, a DAPS is used to provide dynamic, up-to-date attribute information about participants and IDS connectors.

Using a service to hand out attributes in a dynamic fashion reduces the need for certificate revocation and enables more flexible attribute handling for participants in International Data

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Spaces. This allows dynamic assignment of attributes and status flags to IDS connector instances. Exemplary use cases are:

- Tracking of temporary changes of a participant's level of trustworthiness.
- Assigning membership status to a workflow with contractors.
- Information about known vulnerabilities in utilized software stacks.
- Information about available newer versions of software components.
- Revocation of issued certification for components or operational environments.

This concept avoids revocation of Connector identity certificates in most cases, as it allows to include or change attributes if need arises. The DAPS is used as part of the bootstrapping of trust and is not a connector itself but an external service, such as the Public Key Infrastructure (PKI) services.

Participant Information Service (ParIS)

The ParIS provides business-related information about participants in the IDS that have been checked by the Support Organization.

From a system layer view, the internal architecture components and endpoints of a ParIS are very similar to the ones of an IDS Metadata Broker. Both need to receive, persist, and make IDS Self-Descriptions (SD) available for other IDS Connectors to query them. The main difference is the type of SD they manage – IDS connectors and Resources by the Metadata Brokers and Participants by the ParIS.

Interactions between IDS Connectors and Identity Components

To establish a trusted connection, each connector needs the identity information of the corresponding connector to perform access and usage control decisions. The interactions can be depicted as follows:

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

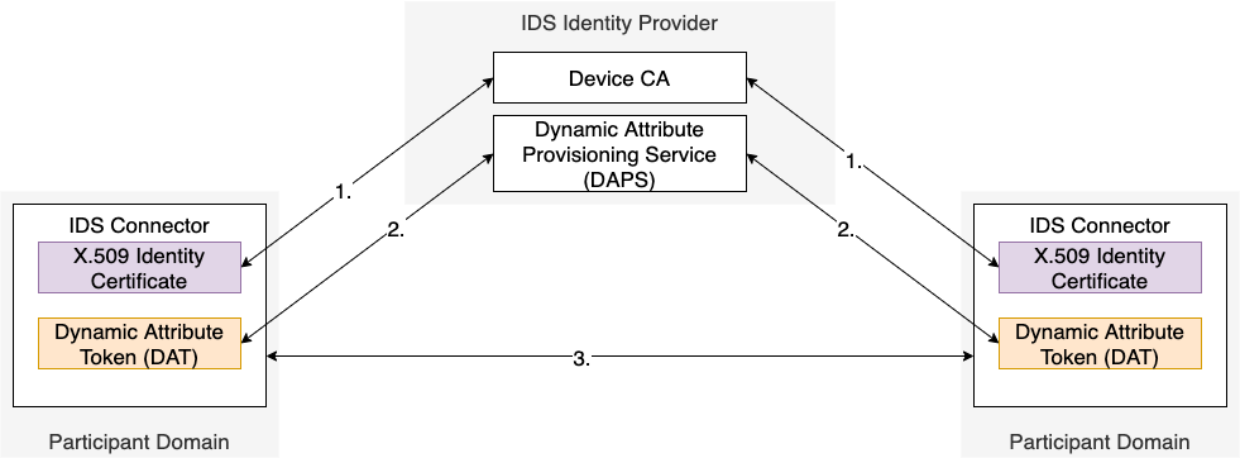


FIGURE 2 - INTERACTION BETWEEN IDS CONNECTORS AND IDENTITY COMPONENTS

In Figure 2, the interaction between IDS connectors and identity components:

1. Each IDS Connector acquires a valid identity certificate from the IDS Device CA.
2. Each IDS Connector requests a current Dynamic Attribute Token from DAPS.
3. When establishing communication, the DAT of both IDS Connector instances is exchanged. This is also matched with the used TLS certificate.

4.2.2 DSBA Architecture Alignment: IDSA, Gaia-X, FIWARE

In September 2021, the Big Data Value Association (BDVA), FIWARE Foundation, Gaia-X and the International Data Spaces Association (IDSA) decided to join forces and formed the Data Spaces Business Alliance (DSBA) aimed at driving the adoption of data spaces across Europe and beyond.

They have defined a digital convergence document[5] with the shared vision on Data spaces, how to approach interoperability and how to achieve trust and data sovereignty. Besides this, in this document it can also be found a shared vision on the data value creation in data spaces and a practical example of their implementation.

DSBA architecture defines an Identity and Access Management (IAM) framework based on:

[5] https://data-spaces-business-alliance.eu/wp-content/uploads/dlm_uploads/Data-Spaces-Business-Alliance-Technical-Convergence-V2.pdf
[2] Home - EBSI - (europa.eu)

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- A set of Verifiable Credential issuing protocols (OpenID Connect for Verifiable Credential Issuance, Self-Issued OpenID Provider v2 (SIOPv2), via DIDComm channel, etc)
- A set of verifiable presentation protocols (ex: OpenID Connect for Verifiable Presentations (OIDC4VP), Presentation Exchange, etc)
- An ABAC (Attribute Based Access Control) framework based on Verifiable Credentials, comprising components implementing PEP, PDP, PAP/PMP, and PIP functions

For authentication DSBA proposes to use the same mechanism as in the European Blockchain Services Infrastructure (EBSI²) and the EUDI Wallet for online flows, namely using OpenID Connect for Verifiable Presentations (OID4VP) and Self-Issued OpenID Provider v2 (SIOPv2), which leverages the proven, robust and secure standards of OpenID Connect protocols to:

- Transport Verifiable Credentials/Presentations in the flows of OpenID Connect, so, Relying Parties can use well known mechanisms to issue and receive Verifiable Credentials.
- Enable all participants (via SIOPv2) to send identity data and Verifiable Credentials to other participants without the requirement for big and centralized Identity Providers as it is unfortunately common in implementations of standard OpenID Connect.

This way DSBA implements a distributed, fault-tolerant, trustful and efficient IAM system avoiding the existence of centralized Identity Providers (IdPs). Using widely implemented standards like OIDC and W3C Verifiable Credentials provides a very low barrier of entry to participants implementing IAM.

Using OIDC for transporting Verifiable Credentials enables integration of the attested data inside the credential for sophisticated and flexible authorization schemes. Participants implementing this Decentralized Identity and Access Management Framework can use credential data for advanced RBAC/ABAC access control and policy enforcement.

The authorization phase corresponds to interactions (5) to (8) in Figure 3.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

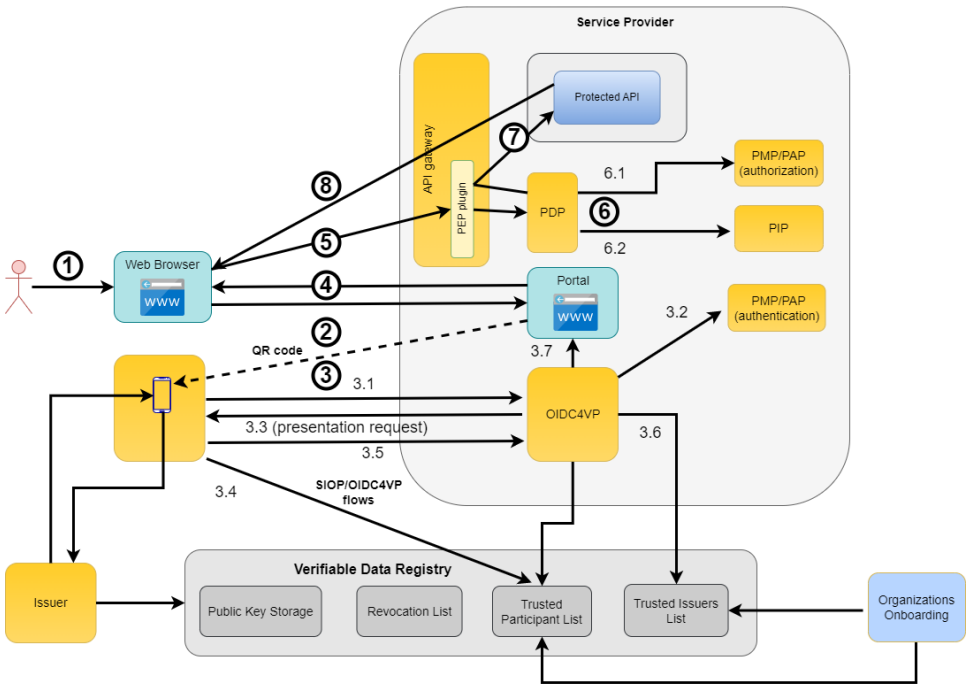


FIGURE 3 – COMPONENT DESIGN

The detailed descriptions with a concrete example can be found in section 6 of the version 2 of the digital convergence document. Furthermore, the IAM Framework can be used by participants not just to interact with the data space and marketplaces but they can adopt it and use it for peer-to-peer interactions between participants in the ecosystem without the involvement of central entities (except for initial onboarding and certification processes).

4.2.3 Interconnect: Federated user access control capability

The Interconnect Semantic Interoperability Framework (SIF) facilitates operational data forwarding between services/endpoints equipped with interoperability adapters. while not storing any privacy sensitive information exchanged between endpoints participating in realization of project use cases. Stakeholders participating in the data exchange adhere to the privacy protection rules through the operation of their legacy services and the adoption of the SIF's Generic Adapters (i.e., service provider or digital platform operator), supporting semantic reasoning and discovery following access control rules defined by service providers.

The goal of the InterConnect security and privacy protection framework is to ensure that the access control mechanisms and privacy protection rules established by participating endpoints (services and platforms) are followed in the SIF. To this end, InterConnect provides access control enablers which integrate with the access control and privacy protection mechanisms into the semantic reasoning procedures. Semantic discovery, reasoning, and data translation

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

between legacy and SAREF based data models includes specified access control and privacy protection rules.

InterConnect access control introduces a concept of InterConnect authorized user and endpoint. End users and services can be authorized for accessing data and services which are part of the InterConnect interoperability ecosystem:

- InterConnect users register on the InterConnect Service Store (catalogue of interoperable services) and are recognized as authorized users for accessing the SIF. InterConnect user features:
    - A user ID for authentication, authorization for attribute-based access control.
    - All collected information will be encoded and stored in the InterConnect user database.
- An InterConnect endpoint (services, devices) is recognized as an authorized endpoint to participate in the SIF and access the framework services.
    - Interoperable endpoints will have authorization ID for attribute-based access control.

Figure 4 shows the specification of the InterConnect authentication, authorization, and access control mechanism as part of the SIF. The goal is to implement access control authority for the complete interoperability framework and integrate it with already existing authentication and access control policies and services residing on interoperable digital platforms and within the InterConnect service store. The aim is to utilize OAuth2 authentication standard (RFC 6749) for delegating user authentication towards their host digital platforms. It delegates user authentication to the digital platform or service that hosts the user account and authorizes third-party applications/services to access the user account. OAuth2 provides authorization flows for web and desktop applications, mobile devices, and smart devices.

The access control policies and identity attributes are stored on the hosting digital platforms. We also plan to explore implementation options where certain access control policies and identity attributes are stored within the interoperability framework enabler for semantically interoperable authorization and access control, as shown in Figure 4. Options for authorizing users with well-known OAuth2 providers like Google and Github. One of the main requirements to ensure privacy protection for any identity attributes that are transferred between interoperable authorization entities. The mechanism integrates the authentication and authorization mechanism within the SIF Generic Adapters so that the semantic reasoning and discovery follow the established access control rules.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

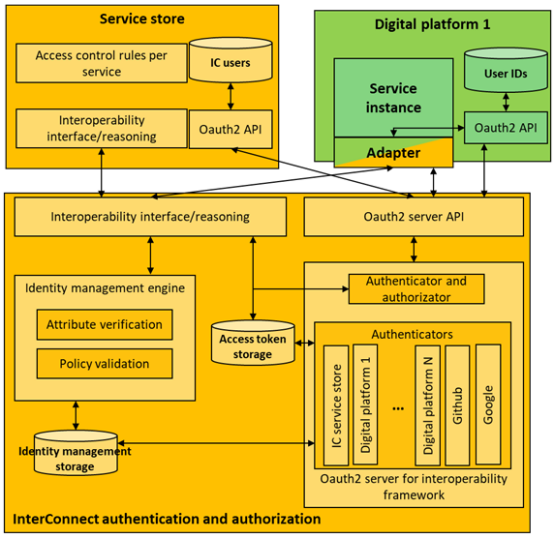


FIGURE 4 - ARCHITECTURE OF THE INTERCONNECT AUTHORIZATION AND ACCESS CONTROL ENABLER

Figure **5** shows a typical pilot architecture for Interconnect with two digital platforms, each with its own set of access control rules and data protection frameworks. The SIF interconnects the two platform and their services. Users registered on the digital platform 1 can access only the services of the host digital platform. The same stands for a user of digital platform 2. An InterConnect user is authorized to access all interoperable services (if not specifically constrained by interoperable service provider). The InterConnect access control mechanism will enable end users of interoperable platforms to be authorized as InterConnect users. With the user profile from the home digital platform, user can access interoperability framework services and other interoperable services available in the service store.

The InterConnect access control will allow service providers to enforce access control rules in line with their data protection policies and business models.

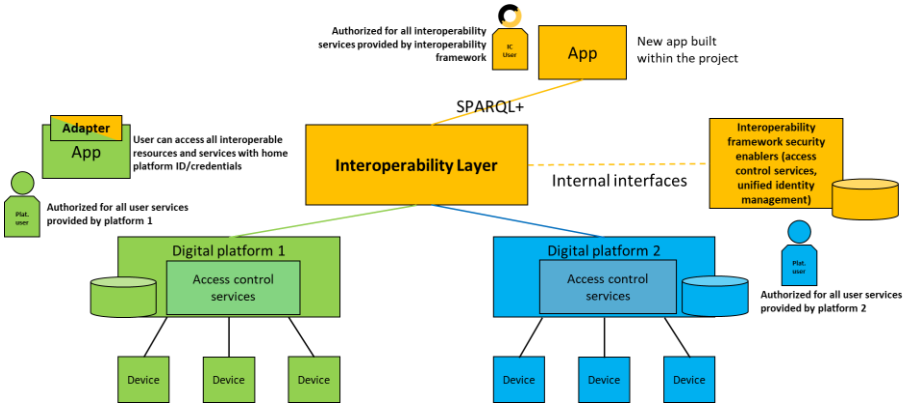


FIGURE 5 - INTERCONNECT ACCESS CONTROL MECHANISM INTEGRATED WITH THE SIF

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

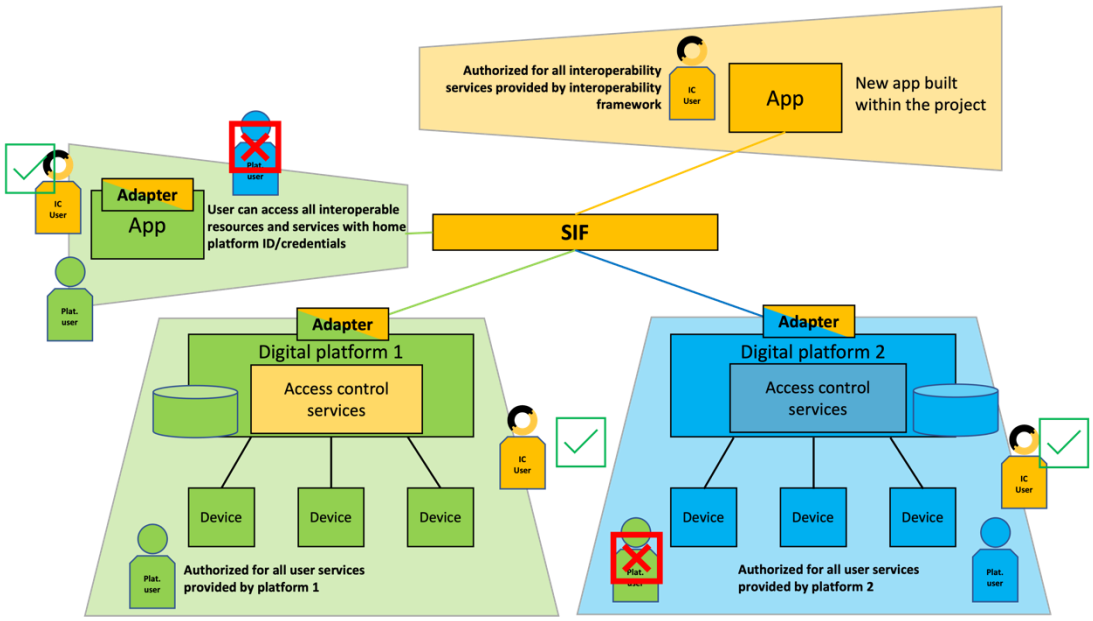


FIGURE 6 - INTERCONNECT DATA DOMAINS AND DATA BOUNDARIES

Figure **6** highlights the data and user authorization domains that are intrinsic to the scenario depicted in Figure 6. Each colorful area surrounding a digital platform or app represents its data domain (*e.g.,* home, energy), that is, the area into which data from that platform is naturally allowed, together with the realm in which a user that is authorized for that platform can operate. The green and blue domains, respectively referring to digital platforms 1 and 2 cover the standard approach, that is, without user roaming capabilities (*i.e.,* a user that can access multiple platforms with the same credentials). This implies that a green user, authorized for the green domain is not able to access the capabilities for the remainder domains, as illustrated. The happens in the opposite direction regarding the user authorized for the blue domain.

The provision of a mechanism for user roaming allows for the IC user, depicted in yellow, to be able to access all resources via the generic adapters. Nevertheless, access control rules can be applied to this roaming concept to eventually block users from accessing particular services classes but allowing an IC user to be mapped to an internal standard one via the adoption of the generic adapter.

In the same way as with use access and control, each digital platform or service implements restrictions of the data is possible to be exported (*i.e.,* sent to another platform or service outside its domain). This is due to data privacy, eventual service level agreements and, most importantly, user consent via the General Data Protection Regulation (*i.e.,* GDPR). Likewise, the colorful domains also address the realms where specific data protection measures are installed. The generic adapters will also work as data boundaries, collecting from the service configuration

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

which data can be forwarded or not. This refers either to operational data or metadata supporting the service execution.

In the interest of interoperability, the required data movement needs to be addressed by each digital platform and according to each service type. This indicates that for services, data can be aggregated at the level of the digital platform and pushed to the destination platform, without compromising the overall goals for the service. Moreover, operational data, which can become the most critical in terms of data privacy is only forwarded between pairs of generic adapters. This means that the required data flow holding operational data will not be forwarded to other proxy-like intermediate structures, and if does, data will not be stored, being just forwarded between parties.

The technical dimension of authorization, accounting and the federation of user access are provided by the integration of the open source IDP system Keycloak, external authenticator services and custom validation between the SIF's Generic Adapters and Service Store.

4.2.4 eSSIF-Lab components for SSI

One way to ensure that data comes from a particular participant is request such data from a connector component that acts on that participant's behalf. Another way is to obtain data that (allegedly) has been issued by (or on behalf of) that participant, and that data is tamper evident and comes with a (cryptographic) proof of its authorship. This is illustrated in Figure 7. Where currently IDS connectors use the first way, components that we will refer to as 'SSI components' would use the second way.[6]

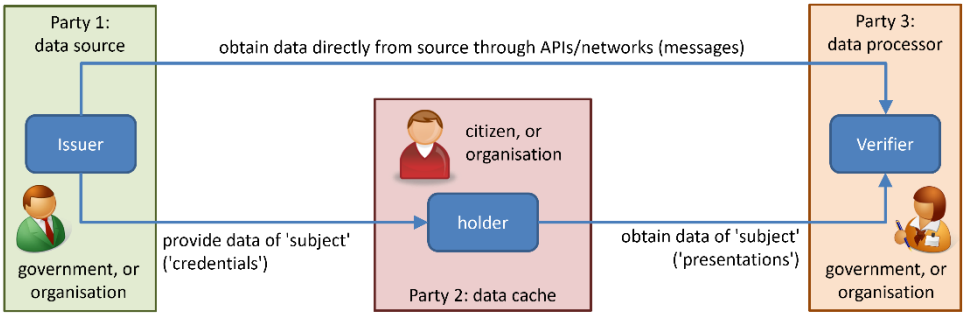


FIGURE 7 - THE TWO WAYS OF EXCHANGING DATA

Note that either way, the communications between the parties must be secured, i.e., encrypted. This requires the communicating parties to identify and authenticate themselves, which typically requires parties to have PKI (X509) certificates. Today, other mechanisms (self-certifying identifiers) have been devised that no longer require certificate authorities to issue

[6] Different people have a different idea about what is, and what is not SSI. Our take on this is just one of many, and equally (in)valid as any of the other views.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

certificates to certify one's key.[7] DIDs are perhaps the best-known example thereof. The similarities and differences between them are discussed in the next section.

In fact, there are various other issues. In the context of decentralized identity (SSI) discussions, there are many and persistent misunderstandings about the overlaps between important technologies such as OpenID Connect (OIDC)[8], Credential Handler API[9], (CHAPI), Decentralized Web Nodes[10] (DWN, and similar initiatives around secure storage of sensitive data), and DIDComm messaging[11] [12]. Such misunderstandings make it difficult for people that are not in the middle of such developments to understand what is going on, and what (not) to use for particular purposes.

In this section, we explore a variety of what some call SSI components, hinting at what they do, and providing pointers for those that want to know more about particular ones. For practical reasons, we will limit ourselves mostly to SSI components that have been produced in the NGI eSSIF-Lab project [3], and references to such components are designated by [eSSIF-Lab, page *n*] (with *n* the page number where the component is described). Also, we note that such components typically request/provide so-called verifiable credentials (VCs[13]), which are tamper-evident data in the form of claims about one or more entities, that are digitally signed by the party that has asserted what is claimed.

Typical SSI components will have one or more of the following capabilities:

- the verifier-capability, i.e., to create and send a request for particular kinds of VC/issuer combinations, receiving a response to such a request and verifying it (i.e., check the integrity of the response and the signatures therein).
- The holder-capability, i.e.
    - to receive a request from a verifier, produce a response (called a (verifiable) presentation or VP), and send it to the requester;
    - to create and send a request for a particular kind of VC to an issuer, receiving a VC of that kind, verifying it, and storing it.

[7] A good and very readable explanation is given by Daniel Hardman in chapter 5 "SSI architecture: The big picture" of A. Preukschat, D. Reed, et. al. "Self-Sovereign Identity". Manning. 2021.
[8] https://openid.net/connect/
[9] https://w3c-ccg.github.io/credential-handler-api/
[10] https://identity.foundation/decentralized-web-node/spec/
[11] https://identity.foundation/didcomm-messaging/spec/
[12] Daniel Hardman explains this in his article "Sentries, Confessionals, Vaults, and Envelopes" (2023).
[13] It also includes verifiable presentations (VPs), but for the purpose of this document, we can ignore that here.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- The issuer-capability, i.e., to receive a request (for a VC) from a holder, deciding whether or not to issue a VC of the requested type, and act accordingly (sending the VC if appropriate).

A wallet is typically taken to be a component that has holder capabilities and has (access to) a storage capability in/from which it can store/retrieve VCs.

Capabilities such as these may come as existing components but can also come in the form of a software library that requires integration in components. Examples of this include the Evernym Open Sourcing project [eSSIF-Lab, p12], Walt.id's wallet kit [eSSIF-Lab, 20], eOrigin wallet [eSSIF-Lab, p43], or TNO's EASSI gateway [eSSIF-Lab, p63]

Also, capabilities that are necessary to create verifier, holder or issuer capabilities may come in the form of libraries, e.g., for creating signatures or creating and verifying VCs and/or VPs. Examples of this include, e.g., Datarella's "Go Aries!" [eSSIF-Lab, p4]

Then there are additional, supportive and/or extension capabilities that may (not) be strictly SSI but could play a supportive role. Examples of this are depicted in this table:

eSSIF-Lab Reference	Capability
[eSSIF-Lab, p6]	facilitation of payments for VCs
[eSSIF-Lab, p10]	capability-based authorization system
[eSSIF-Lab, p11]	a DNS-based mechanism for dealing with trust lists
[eSSIF-Lab, p13]	FIDO2
[eSSIF-Lab, p14]	advanced or qualified electronic signatures , a universal verifier interface
[eSSIF-Lab, p16]	a universal verifier interface
[eSSIF-Lab, p18]	consented data exchange with auditable data agreements
[eSSIF-Lab, p19]	DIF Presentation Exchange protocols
[eSSIF-Lab, p21]	VC building blocks
[eSSIF-Lab, p23]	exchanging data over NFC
[eSSIF-Lab, p24]	authority delegation and verifiable mandates
[eSSIF-Lab, p26]	devices
[eSSIF-Lab, p28]	a decentralized key management infrastructure
[eSSIF-Lab, p32]	user-frendly mnagement interfaces for verifier policies
[eSSIF-Lab, p40]	universal backup services for SSI agents
[eSSIF-Lab, p41]	corss-border transactions
[eSSIF-Lab, p44]	electronic contracting
[eSSIF-Lab, p45]	universal DID SaaS
[eSSIF-Lab, p50]	Key Event Rotation Infrastructure (KERI)
[eSSIF-Lab, p51]	system approach
[eSSIF-Lab, p59]	a system for portable membership between cooperatives

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

This summary of SSI solutions shows that there is a large variety of such services. With the current state of the EnerShare requirements on the one hand and the high-level technical specification of these solutions from the booklet, it makes no sense to try and map them at this point in time. This may change when the needs of EnerShare pilots become more apparent.

4.2.5 Current work on alignment x.509 certificates & DIDs

The current way in which data spaces (as per the IDSA framework) operate is by using x.509 certificates for asserting an identity[14] for a person, organization or other kinds of entities) and possibly also various (rather static) attributes. This obviously requires related infrastructure and (administrative) processes for issuing (and revoking, if necessary) such certificates. The merits and drawbacks are well-known, as this framework has been around for several decades.

Decentralized Identifiers (DIDs) are a new type of identifier that enables individuals and organizations to create and manage their own digital identities without relying on centralized authorities like governments or corporations.

DIDs are typically, but not always, built using blockchain or other distributed ledger technologies and provide a way to create a unique identifier for an individual, device or entity that is both cryptographically secure and independent of any particular system or organization.

DIDs are designed to be self-sovereign, meaning that the party that controls the DID (and can cryptographically prove that) also determines the DID semantics, i.e., determines what/who is identified by that DID[15]. A DID is associated with precisely one so-called 'DID document', i.e., data that is said to describe the DID subject, but basically consists of a set of public keys that have designated purposes, and service endpoints that serve to contact the DID subject and/or controller. Only the controller can modify the DID document[16], and as such resembles what a CA does for a PKI certificate. A DID can be shared with arbitrary others, who can then resolve that DID to obtain the DID document and from there get all the (public) key related information that it would otherwise would have gotten from a PKI certificate. While DIDs do not require a central authority or service provider to manage such information, they do require assurances regarding the implementation of the services for creating, reading (or resolving), updating, and deleting (or tombstoning) DIDs and their associated DID documents.[17] Nevertheless, DIDs can

[14] This is what many people call it; it was, however, better referred to as 'identifier'.
[15] The entity identified by a DID is called the DID subject.
[16] The controller can delegate such functions or specify that control can only be exerted by a (sub)set of designated parties. This implies that controlling a DID is not that straightforward as one might think.
[17] The security around DIDs should not be taken for granted, as illustrated by Appelcline, Sgalam, Sills, and Stocker: "Taking out the CRUD: Five Fabulous DID Attacks".

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

provide greater privacy and security, and new forms of digital interaction and trust between individuals and organizations.

Decentralized Identifiers (DIDs) and X.509 certificates serve different purposes and have different strengths and weaknesses. Here are some of the pros and cons of using DIDs compared to X.509 certificates.

TABLE 2 – PROS AND CONS OF X.509 CERTIFICATES VS DIDS

	Pros	Cons
X.509	• **Wide adoption**: X.509 certificates have been in use for many years and are widely adopted, making them a well-established solution for digital identity. • **Easy to implement**: Implementing and managing X.509 certificates is relatively straightforward and can be done using a variety of tools and technologies. • **Trust**: X.509 certificates are backed by trusted certificate authorities (CAs), which can provide an additional level of trust for users.	• **Centralization**: X.509 certificates rely on centralized CAs, which can create a single point of failure or attack. • **Limited flexibility**: X.509 certificates are primarily used for authentication and may not be well-suited for other types of digital identity use cases. • **Privacy concerns**: X.509 certificates typically require users to share a lot of personal information with CAs, which can raise privacy concerns.
DIDs	• **Self-sovereignty**: DIDs give individuals complete control over their digital identity, allowing them to share only the information they choose and with whom they choose. • **Decentralization**: DIDs are not tied to any particular organization or service provider, making them more resistant to single points of failure or attack. • **Flexibility**: DIDs can be used in a variety of contexts, including personal identity, IoT devices, and verifiable credentials, making them a versatile solution for digital identity.	• **Complexity**: Implementing and managing DIDs can be more complex than traditional digital identity solutions, requiring knowledge of blockchain and other distributed ledger technologies. • **Lack of adoption**: DIDs are still a relatively new technology and have not yet been widely adopted, which may limit their usefulness in some contexts. • **Security**: While DIDs are designed to be secure, the use of blockchain and other distributed ledger technologies can introduce new security risks that need to be carefully managed.

Having said that, it is easy to imagine that X.509v3 certificates can be extended with a field that contains a DID of which the party that the certificate identifies is expected to control that DID. Whether or not the keys that control the DID (and mentioned as such in the corresponding DID document) would be the same as the public key mentioned in the X.509 v3 certificate is not yet clear. Also, it remains to be seen if other key material would or should need to be made available through that DID document.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

From reviewing the state-of-the-art solutions on identity management, we conclude that X.509v3 certificates, as are currently used in the IDS connectors, suffice for the first technology release. This covers the requirements from chapter 3, and could be expanded/later to accommodate any additional needs as they may arise.

4.3 Design for 2nd technology release

4.3.1 Implementation of SSI tech in identity solution/process

One of the problems that organizations face is to provide policies that their IT components (e.g., connectors) can use to determine whether or not to service a request that is received, and if that is permitted, what the response can(not) be. Some of these issues can be solved by enhancing IAM functionality.

One issue is that there are different kinds of organization identifiers in use, such as Decentralized identifiers (DIDs), Global Location Numbers (GLN), Data Universal Number System (DUNS), Bank Identifier Codes (BIC), Taxpayer Identification Numbers, ISB-numbers, Legal Entity Identifiers (LEI), Social Security Numbers (or something similar, depending on where you live), etc. Also, numbers that typically serve specific purposes, such as telephone numbers (for calling someone), or public keys (for encrypting messages, or verifying digital signatures), are known to be also used as identifiers (the person that owns the phone, or that controls the private key).

One cannot necessarily tell from a text, e.g., 'Alice', '+31622901317', 'localhost', or 'did:example:12345', whether or not it is an identifier, or what kind it would be. Also, a specific text (e.g., 'localhost') may be used to identify e.g., a specific computer service on a specific computer in one context, while in another context it could identify the concept of having local services on computers, and in even other contexts, it may identify the host of some local community. While it is obvious that one needs to know what kind of identifier one is dealing with, the question is who determines that. And the answer is: the one that expresses it.

In one of the upcoming releases, we intend to come to grips with this issue, which means that it will become possible to use all sorts of different identifiers or different purposes, and for parties to learn what the type of an identifier is and thereby how to properly dereference it, that is: as its author intended it.

Another issue is related to authorizations. If an organization authorizes another organization to use specific data that it provides (possibly limited to particular purposes), and a connector that is deployed by the first organization receives a request from another connector, then how will it know that this other connector has the authority to make such a request? Obviously, when the connector is deployed by the other organization (which can be seen from its certificate),

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

that could readily be the case. But what if that connector were deployed in the cloud (by some cloud provider), which provides the connector service as a SaaS offering to the other organization? While one could think this SaaS connector to have multiple certificates, how would it choose the one that needs to accompany the request? And what if the other organization has authorized a third organization to process data on its behalf, which would mean that the connector of that third organization should be recognized (by the connector of the first party) as having the authority to make such a request. How would that come to pass?

In the upcoming release(s), we intend to come to grips with this issue, which means that it will become possible for organizations to mandate other organizations and/or their IT-components to perform actions on their behalf. We will use the term 'mandate' to refer to data that specifies the rights and duties that a party (that has such right and duties – the mandator) transfers to another party, an employee or an IT-component (the mandatee). It seems obvious that this data should be tamper evident and come with a (cryptographic) proof of its authorship (i.e.: the mandator), which make VCs a natural choice for mandates.

We intend to develop a conceptual model for mandating, i.e. define a precise language that we can use to express how mandates are created, updated, revoked, and how they can be exchanged by means of connectors (or by other communication means, e.g. in a human-to-human setting that would also be relevant within the context of ENERSHARE), and subsequently used by people or IT alike to decide whether or not a request that is received has been made by a person or IT component that is properly mandated.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

5 Usage control policies

5.1 Task objective

Effective usage control is critical for companies and systems as they protect privacy, maintain data integrity, and guarantee regulatory compliance. Organizations may achieve an appropriate balance between authorizing allowed data usage and protecting individuals' privacy rights by carefully designing and enforcing the policies.

The objectives of this task are summarized as following:

- Analyse and design privacy-preserving data-driver exchange architecture and implementation within the project platforms (e.g., FIWARE, IDSA).
- Development and demonstration of a “usage control”. Define usage rights and control the validity to ensure compliance with privacy regulation (incl. GDPR).
- Design for an ontology for pre-processing data within the connector to ensure certain policies.
- Establish a certification infrastructure for user applications that will deal with sensible/confidential data. Building blocks that can used as starting point are: MYDATA Control Technologies; Consent management and clearance for GDPR enforcement over consumer’s metering data (H2020 Integrid); IDS Usage Control App; LUCON, logic-based usage control.

5.2 State of the art

The modern world of data-driven businesses relies heavily on the constant exchange of important and confidential information among partners. To ensure its security, data is typically protected through access control measures. Once access to the data is granted, it can be utilized without additional limitations, allowing for actions such as alteration, copying, and dissemination. But this not sufficient to establish a trustworthy and secure data exchange. So, Data Spaces are established to fulfill these requirements. IDSA and Firware are working closely to establish technology standards which will help in communication and fulfill the key success factor of data sovereignty. Data-driven organizations realize that complete data protection is not the most effective answer; instead, they aim at maintaining control over their data. Now according to different requirements, standard rules, legal obligation, and European Union General Data Protection Regulation (EU-GDPR) make it difficult to implement solution for secure data exchange. Considering these future objectives, the integration of usage control policies is important that can meet these objectives. The is a standard which is used in

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

implementation of data sovereignty framework and data connectors. In the next section, the reference architectures of IDS and Firware and how usage control works in connectors are discussed.

Various research works propose solutions for data Usage Control (UCON) by using different approaches depending on the application field. The xDUCON framework provides a general perspective for policy enforcement and specification, while other proposals use the UCON model and Policy Definition Languages (PSLs) like XACML and PPL to enforce and define mechanisms for access and Usage Control. Recent works offer solutions based on the XACML reference architecture for dealing with IoT, cloud, and smart home environments. However, these overtures lack coverage of cross-domain data exchange, data governance, and trust environments, highlighting the need for a flexible framework that can adapt to mixed data ecosystems. The International Data Space (IDS) is a European initiative with the goal of creating an interoperable and decentralized data infrastructure for data exchange between different organizations and systems.

5.2.1 IDS Architecture

The concept of international data spaces revolves around the core principle of data sovereignty. The *IDS reference architecture* for International Data Spaces (IDS-RAM)[18] establishes a benchmark for constructing data-driven ecosystems, products, and services, providing a standardized framework for development and implementation. The general overview IDS architecture is discussed below:

- **Data spaces:** Decentralized and autonomous data storage and processing environments managed by various organizations or individuals are known as data spaces.
- **Data contracts:** are agreements that establish the terms and conditions under which data can be shared between data spaces, including data types, usage conditions, and other relevant terms.
- **Data brokers:** are intermediaries that facilitate data exchange between different data spaces by matching data providers with consumers, negotiating data contracts, and enforcing contract terms.
- **Data marketplaces:** are platforms that enable the discovery and exchange of data between different data spaces, providing centralized access to data providers and consumers, and offering additional services like data analytics and storage.

[18] https://www.fraunhofer.de/content/dam/zv/de/Forschungsfelder/industrial-data-space/IDS_Referenz_Architecture.pdf

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

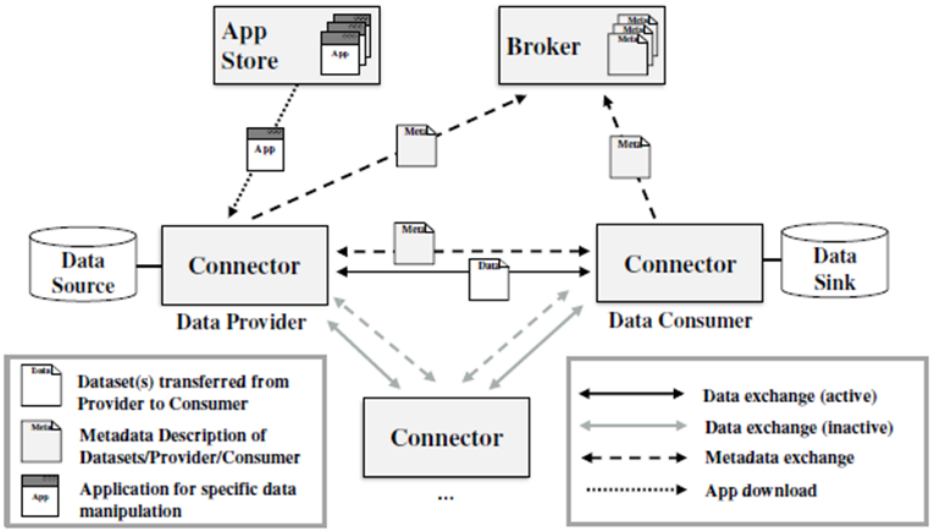


FIGURE 8 – IDS INTERACTION COMPONENTS

5.2.2 FIWARE Architecture

The FIWARE platform provides a set of open-source technologies and standards that enable the development of smart applications and solutions in various domains, such as smart cities, agriculture, industry 4.0. The Fiware architecture shown in Figure 9 and Figure 10 architecture schemas which are derived from a hybrid model based on the Data Privacy Directive 95/46/EC[19] and the IDS reference architecture[20] and it is divided in three essential parts: Data Provider, Data Consumer and Data Controller.

Data Consumer:

- **Apache Flink Cluster**: Big Data Processing Engine in which client jobs are run. The data consumer may write real-time data processing jobs using Flink for Scala and the FIWARE Cosmos Orion Flink Connector[21] in order to have a direct ingestion of data from Orion in the processing engine.

Data Provider/Controller:

- **Orion Context Broker**: Component that allows to manage the entire lifecycle of context information
- **IdM Keyrock**: Component for defining Access and Usage Control Policies

[19] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046
[20] https://www.fraunhofer.de/content/dam/zv/de/Forschungsfelder/industrial-data-space/IDS_Referenz_Architecture.pdf
[21] https://github.com/ging/fiware-cosmos-orion-flink-connector

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- **PEP (Policy Enforcement Point) proxy**: Component for enforcing Access Control Policies
- **PTP (Policy Translation Point)**: Component for translating the FI-ODRL Policies into a program that checks compliance in real time
- **PXP/PDP (Policy Execution/Decision Point)**: Component with complex event processing capabilities (CEP) for analyzing the logs in order to verify the compliance of the obligations defined in the IDM and enforce the punishments.

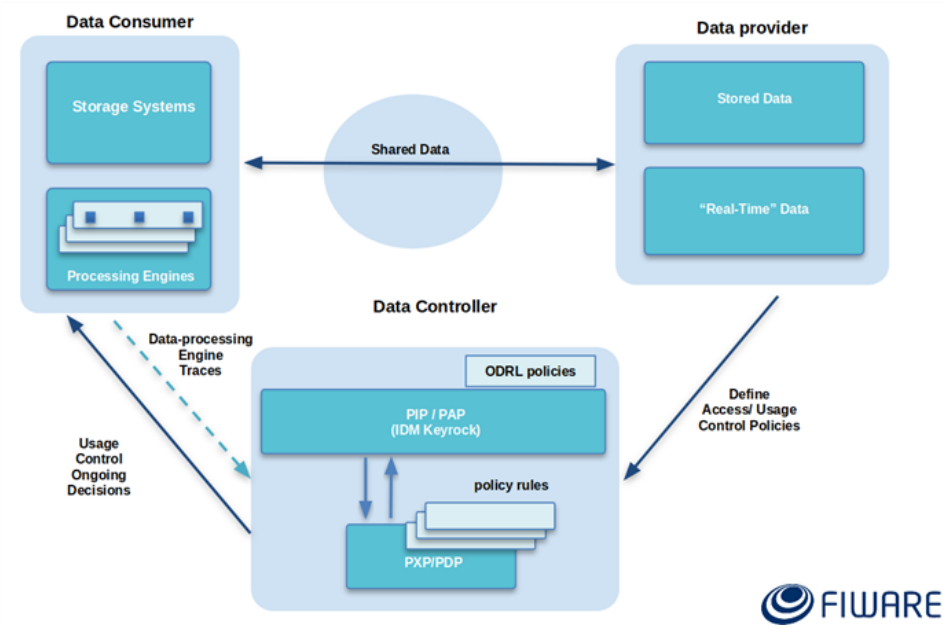


FIGURE 9 - THREE STAKEHOLDER ARCHITECTURE

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

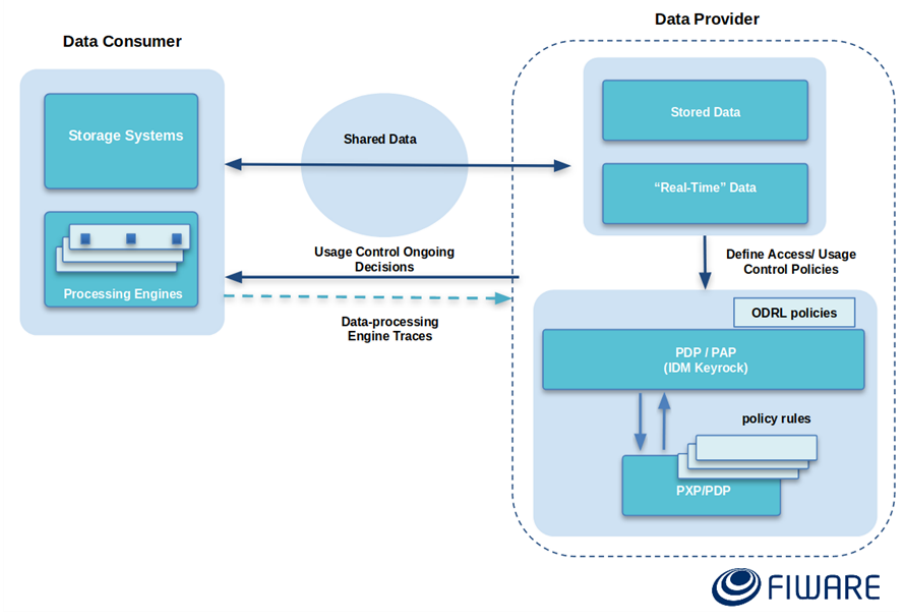


FIGURE 10 - TWO STAKEHOLDER ARCHITECTURE

5.2.3 Usage Control

Usage control, also known as data usage regulation, is a security measure that goes beyond controlling data access and focuses on governing how data can be utilized. This approach is commonly employed in situations where there are specific requirements or restrictions regarding the handling of sensitive information, such as intellectual property or personal data. In addition to access control (refer to Figure 11), the concept of usage control entails establishing rules and guidelines for data processing, which may include prohibiting certain actions or mandating the implementation of specific safeguards. Furthermore, it involves the active monitoring and enforcement of these rules to ensure compliance with the established regulations (Jung, 2022).

FIGURE 11 - USAGE CONTROL – AN EXTENSION TO TRADITIONAL ACCESS CONTROL

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Usage control provides IDS participants with the ability to enforce architectural designs that respect data sovereignty, ensuring that no violations occur. Furthermore, by implementing usage control mechanisms, data flows are closely monitored, serving as an audit mechanism that generates evidence of compliant data usage. There are specific requirements for data sovereignty that cannot be fulfilled through traditional access control methods. Instead, data-centric usage control is necessary to address these requirements:

- **Data Secrecy:** Classified data can only be transmitted to nodes and services that possess the appropriate clearance or security level.
- **Data Integrity:** Trusted nodes or services are the only ones permitted to modify critical data.
- **Time to Live:** Data must be deleted or modified after a designated period of time.
- **Anonymization:** Before usage, (personal) data must undergo anonymization processes such as aggregation or replacement.
- **Separation of Duty:** Data sets, especially those belonging to competitive organizations, must remain separate. This means no joining operations or processing within the same service.
- **Usage Scope and Purpose:** Data can only be utilized within trusted nodes or services, and solely for specific usage purposes.
- **Context Awareness:** Data usage is restricted to meeting certain contextual conditions, such as being limited to company premises or specific geographical locations.

5.2.4 Usage Control Components and Communication Flow

For enforcing usage restrictions, data flows are monitored and intercepted by control points. The main components involved in the communication are listed below:

- **Policy Enforcement Point (PEP):** Data flow information is transmitted from the PEP component to the decision engine (Policy Decision Point, PDP) to determine whether the data flow should be allowed or denied. The decision made by the PDP may also include instructions to modify the data in an authorized data flow.
- **Policy Decision Point (PDP):** The PDP is responsible for evaluating incoming requests from the Policy Enforcement Points (PEPs) and making decisions based on the predefined policies.
- **Policy Information Point (PIP):** The Policy Information Point (PIP) retrieves missing information for policy evaluation in the PDP. It provides a standardized interface and encapsulates the logic for information retrieval.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- **Policy Execution Point (PXP):** The PXP executes supplementary actions according to deployed policies. Examples include sending emails when data is used or logging messages to a third-party logging system.

5.2.5 Categorization of Usage Restriction

There are two ways in which usage restrictions can be placed on data: sticky policies and centralized policies.

- **Sticky policies:** also called data-centric policies, are attached to data and enforced when it is accessed or used. Encryption is often used to ensure compliance with usage restrictions. This approach manages distribution of usage restrictions by applying policies directly to the data, enabling them to be enforced consistently wherever the data travels.
- **Centralized policies:** are stored separately from the data in a central component, such as a Policy Management Point or Policy Repository Point. Usage restrictions are exchanged between systems via this central management component, and policies are enforced there. This approach is efficient and manageable since policies are stored in a central location and can be easily updated. However, ensuring consistent enforcement across all systems may be more challenging.

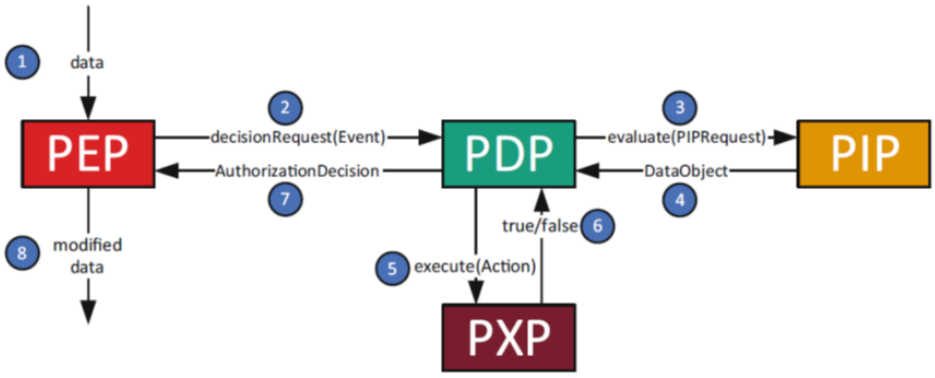


FIGURE 12 - USAGE CONTRL COMMUNICATION FLOW

5.2.6 Usage Control in Connector

A data connector with machine-readable data policies can help ensure that data is handled in accordance with the company's data sovereignty requirements, as the policies can be automatically enforced by the connector without the need for manual intervention. This can help streamline data exchange processes and reduce the risk of data breaches or other security issues. The different connectors which are currently available are reported in the IDSA Data Connector Report [4]. considering the requirement and scope of the project we need to identify

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

the suitable connector which provides the usage control for trust and sovereignty of users. The selection is narrowed down to the following connectors: Trusted Connector[22] maintained by Fraunhofer IESE, Dataspace Connector (DSC)[23] maintained by Sovity, TNO Security Gateway (TSG)[24] maintained by TNO (Netherlands Organization for Applied Scientific Research), and FIWARE TRUE Connector[25] maintained by Engineering .

5.2.6.1 IDS Trusted Connector

The IDS Trusted Connector is a specialized version of the IDS connector that focuses specifically on security and trust. It incorporates a range of features and capabilities to help ensure the security and integrity of the data exchange process, including:

Identity and trust management: The Trusted Connector provides tools and APIs for authenticating communicating parties and establishing trust relationships between partners.

A trusted platform: The Trusted Connector provides a secure, controlled execution environment for data services, helping to ensure the integrity and confidentiality of the data being processed.

Trustworthy communication: The Trusted Connector uses authenticated and encrypted connections to ensure the confidentiality and integrity of the data being exchanged.

Access and usage control: The Trusted Connector provides foundations for flexible access control and hooks for usage control frameworks, helping to ensure that data is accessed and used only by authorized parties.

Overall, the IDS Trusted Connector is intended to contribute to the security and integrity of data exchange and processing inside the IDS ecosystem. Some of the key features include:

- Message routing and conversion between protocols with Apache Camel
- Apps in isolated containers
- Data flow- and data usage control
- An Apache Camel component for secure communication
- Remote attestation between Connectors.

It's essential to understand that, while the connector provides strong protection, no system can ensure complete data security, especially with administrator access. The IDS ecosystem enables partners to efficiently perform their responsibilities and define trust and access requirements.

[22] https://github.com/Fraunhofer-AISEC/trusted-connector
[23] https://github.com/International-Data-Spaces-Association/DataspaceConnector
[24] https://gitlab.com/tno-tsg
[25] https://github.com/Engineering-Research-and-Development/true-connector

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

5.2.6.2 Dataspace Connector

Dataspace Connector is an implementation of an IDS connector originally developed by Fraunhofer ISST and currently being maintained by Soviety. It is a software component in the International Data Spaces (IDS) architecture that enables secure and standardized data exchange between data providers and users. Its design and functionalities are determined by the IDS Reference Architecture Model (RAM) and specified by the certification criteria. The metadata is described using the ontology of the IDS Information Model. The key advantage of utilizing the IDS reference architecture and employing an IDS Connector is the decentralized storage of data. This facilitates the integration of data from various sources and ensures that data access is exclusively granted through other IDS Connectors.

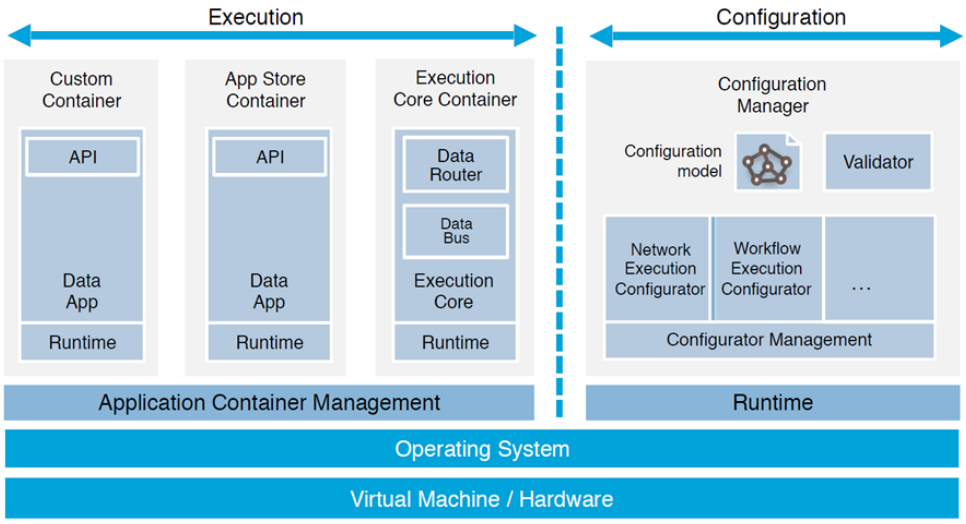


FIGURE 13 - CONNECTOR ARCHITECTURE FROM THE IDS REFERENCE ARCHITECTURE MODEL (RAM)

The IDS Connector provides several key features:

Data Access and Authorization: It controls data access by applying fine-grained access control policies. This ensures that specified data resources are only accessible to authorized people or systems.

Data Protection and Encryption: To protect data during transmission and storage, encryption mechanisms are employed to ensure confidentiality and integrity of the provided data.

Identity and Authentication: It authenticates individuals and systems requesting to access data resources, ensuring that only authenticated entities can participate in data exchanges.

Consent Management: It provides people and organizations control over how their data is used and shared by allowing them to define and maintain their data sharing preferences.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Interoperability: It facilitates system and platform interoperability, enabling simple integration and data interchange across heterogeneous environments.

Auditing and Monitoring: It provides monitoring and auditing capabilities to keep track of data access, usage patterns, and compliance with data sharing policies.

An IDS Connector is composed of various system services:

- Execution core container with message systems (message router/bus)
- Configuration Manager to configure the Connector (execution core container, application container management, network, firewalls, etc.)
- Data Apps for data processing and handling
- Application container management
- Hardware/Operating system

5.2.6.3 TNO Security Gateway (TSG)

The TNO Security Gateway (TSG) is a project developed by TNO (Netherlands Organization for Applied Scientific Research) that focuses on developing a secure and trusted data exchange ecosystem. It intends to make it possible for companies to safely communicate and collaborate on data while maintaining data sovereignty, privacy, and security. It is composed of up of several components:

Authentication and Authorization: TSG verifies user identities and authorizes access, ensuring only authorized individuals can interact with the gateway and access shared data.

Encryption and Data Protection: TSG encrypts data during transmission and storage, safeguarding its confidentiality and integrity from unauthorized access and tampering.

Access Control: TSG regulates data access by allowing organizations to define specific access rights and permissions, ensuring that only authorized users can retrieve or modify data.

Privacy-Preserving Protocols: TSG employs protocols to protect sensitive information, enabling data sharing while preserving individual privacy and confidentiality.

Data Governance and Policy Enforcement: TSG enforces data governance policies, enabling organizations to define usage conditions, data protection policies, and consent management rules to comply with regulations and principles.

Integration and Interoperability: TSG seamlessly integrates with existing systems, allowing organizations to leverage their infrastructure while benefiting from enhanced security and data sharing capabilities.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Monitoring and Auditing: TSG provides monitoring and auditing features to track data usage, access patterns, and security breaches, ensuring accountability and compliance.

5.2.6.4 FIWARE TRUE Connector

The FIWARE TRUE connector is a tool that allows developers to easily integrate applications with the FIWARE platform using a set of pre-defined APIs. The TRUE connector is designed to be used in conjunction with the FIWARE reference architecture, which provides a set of guidelines and best practices for building and deploying applications on the FIWARE platform. By using the TRUE connector, developers can take advantage of the scalability, security, and interoperability TRUE Connector features of the FIWARE platform to build innovative digital solutions.

Components:

- **Execution Core Container (ECC)[26]:** is responsible for facilitating data exchange within the IDS (International Data Spaces) ecosystem. This utilizes the IDS Information Model to represent data and establishes connections with an external Identity Provider to manage authentication and authorization processes. Additionally, it enables communication with an IDS Broker for tasks such as registering and querying information.
- **Back-End (BE) Data Application[27]:** It is in charge of processing incoming request and providedata on top of ECC component.
- **Usage-Control (UC) Data Application**[28]: It will check if those who are requesting the data have the grants to use that in a well-defined policy. (The FIWARE TRUE Connector integrates the Fraunhofer MyData Framework[29] for implementing the Usage Control. Details about the PMP and PEP components can be found here).

[26] https://github.com/Engineering-Research-and-Development/true-connector-execution_core_container
[27] https://github.com/Engineering-Research-and-Development/true-connector-basic_data_app
[28] https://github.com/Engineering-Research-and-Development/true-connector-uc_data_app_platoon
[29] https://www.mydata-control.de/

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

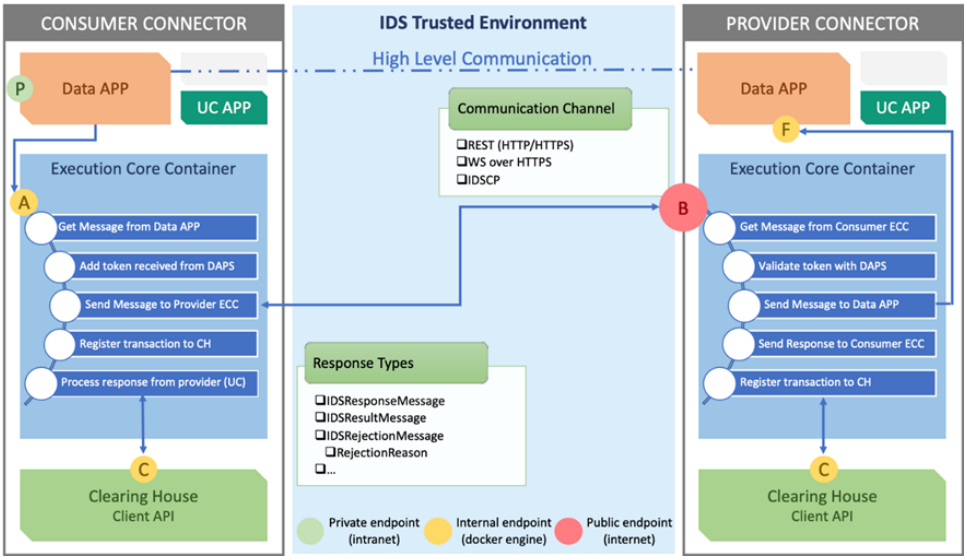


FIGURE 14 - FIWARE CONNECTOR ARCHITECTURE

5.2.6.5 Policy patterns defined by IDSA

Data Usage Control policies allows us to define the actions that the provider lets the consumer perform over the data consumed. These usage control policies must be agreed between the provider and the consumer when they establish the contract agreement. The table shows the overview of the policies pattern of IDSA which are supported in Data Space Connector (DSC), TNO Security Gateway (TSG) and TRUE Connector using MyData Usage Control and PLATOON Usage Control.

TABLE 3 - SUPPORT OF POLICY PATTERNS IN DIFFERENT CONNECTORS

No.	Policy Patterns	Data Space Connector	TNO Security Gateway (TSG)	True Connector with MyData Usage Control	True Connector with PLATOON Usage Control
1	Allow Usage of the Data	x	x	x	x
2	Connector-restricted Data Usage	x			
3	Application-restricted Data Usage				

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

4	Interval-restricted Data Usage	x	x	x	x
5	Duration-restricted Data Usage	x			x
6	Location Restricted Policy		x	x	
7	Perpetual Data Sale (Payment once)				
8	Data Rental (Payment frequently)				
9	Role-restricted Data Usage				x
10	Purpose-restricted Data Usage Policy			x	x
11	Event-restricted Usage Policy				
12	Restricted Number of Usages	x			x
13	Security Level Restricted Policy	x	x		
14	Use Data and Delete it After	x			
15	Modify Data (in Transit)			x	
16	Modify Data (in Rest)				
17	Local Logging	x			
18	Remote Notifications	x			
19	Attach Policy when Distribute to a Third-party				
20	Distribute only if Encrypted				
21	State Restricted Policy				

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

IDS has defined a policy language to express data usage restrictions. This policy language is based on the Open Digital Rights Language (ODRL) and its syntax is RDF. It has also predefined 21 policy patterns to express the most commonly data usage restrictions. A data Usage Control policy is a combination of one or more instances of these policy patterns. The description of these 21 policy patterns defined by IDSA can be found in **Appendix A** of the document[30]. Here we summarize them the table below.

TABLE 4 - IDS POLICY PATTERNS

No	Policy Pattern	Explanation
1	Allow or inhibit the usage of the data.	This pattern gives permission or prohibits to use the dataset.
2	Restrict the data usage to specific connectors.	This pattern restricts the usage of the dataset to a specific connector defined in the policy
3	Restrict the data usage to a group of systems or applications.	This pattern restricts the usage of the dataset to a specific system or application defined in the policy.
4	Restrict the data usage to a group of users.	This pattern restricts the usage of the dataset to a consumer member of the specified organization or that has a specific role defined in the policy.
5	Restrict the data usage to specific locations.	This pattern restricts the usage of the dataset to a consumer located on the location defined in the policy.
6	Restrict the data usage for specific purposes.	This pattern restricts the usage of data for the specific purpose defined in the policy. E.g.: if the purpose is risk management, then allow the usage of data.
7	Restrict the data usage when a specific event has occurred.	This pattern restricts the usage of data under specific conditions; in the circumstances that the usage of data must be restricted. E.g.: provide permission to a Data Consumer to use the data during the exhibition.

[30] https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Position-Paper-Usage-Control-in-the-IDS-V3..pdf.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

8	Restrict the data usage to the security level of the connectors	This pattern restricts the usage of data to connectors that offer the security level specified in the policy. The information model of IDS differentiates the connectors with respect to their security levels (i.e., base, trust and trust plus).
9	Restrict the data usage to a specific time interval.	This pattern restricts the usage of the dataset during the time interval specified in the policy.
10	Restrict the data usage to a specific time duration.	This pattern restricts the usage of the dataset to a specific duration of time (e.g.: two months).
11	Use the data not more than N times.	This pattern restricts the usage of the dataset the number of times specified in the policy.
12	Restricted Number of Usages	Use data and delete it after this pattern allows to use the data but the consumer has to delete the data after consuming it.
13	Modify data (in transit).	In all mentioned cases, the policies allow the users to use the entire data, without modifications, after the conditions are met. However, there might be cases where data must be modified or partially anonymized before it is allocated to the user. The data modification must be done before the permission to use the data is granted.
14	Modify data (in rest).	This class of policy demands for the data modifications or anonymizations before the permission to use the data is granted. In contrast to the previous policy class, it demands the modifications to be done when data is stored in a database. The Data Consumer is only allowed to use the data after certain modifications have been applied to the stored data.
15	Log the data usage information.	This pattern requests to log the information of transferring the data from the provider to the consumer.
16	Notify a party or a specific group of users when the data is used.	This pattern requests to notify that the data has been transferred from the provider to the consumer.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

17	Attach policy when distribute the data to a third-party.	If the consumer wants to distribute the received data, the consumer is obliged to pass the specified policy to the third-party and demand for an agreement before distributing the data.
18	Distribute the data only if it is encrypted.	This pattern demands the consumer to share the data only if it is encrypted.
19	Perpetual data sale restrictions:	this pattern is used when the provider wants to sell the data. This pattern addresses the conditions that are associated to a data sale contract.
20	Rental data restrictions	This pattern is used when the provider wants to rent the data. This pattern addresses the conditions that are associated to a data rental contract.
21	Restrict the data usage to specific state.	This pattern restricts the usage of the dataset when an environment state occurs. it is about the state of the contract and the connectors, e.g.: if the contract is terminated or if the firewall is activated.

5.2.7 Policy patterns supported by Dataspace connector

The Dataspace connector supports 9 of the 21 policy patterns defined by IDS. These policy patterns are defined by IDS. These patterns are specified in the documentation [31]. Here we summarize them:

1. **Provide Access**

Description: This policy simply grants access to the resource.

2. **Usage During Interval and Usage Until Deletion**

Parameters: start and end time (of type ZonedDateTime, a representation of an instant in the universal timeline)

[31] https://international-data-spaces-association.github.io/DataspaceConnector/Documentation/v6/UsageControl#provide-access

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Description: Both the policies Usage During Interval and Usage Until Deletion use the same parameters and behave in the same way. They check if the data access time is between the start and end time defined. The access time used is a ZonedDateTime, which represents an instant in the universal timeline, since it also contains date, time and zone information. The only difference is that the Usage Until Deletion rule should contain a postDuty field with a DELETE action and deletes the data after the interval has passed. The Usage Until Deletion policy should be used if it is desired that the resource be deleted after the time interval.

3. **Duration Usage**

Parameters: a duration, as specified by the Duration java class. (Example: “PT10H” stands for 10 hours, see more)

Description: This policy starts a duration for a resource: the resource can only be accessed in the specified period. The duration starts counting from the artifacts’ creation time. If the consumer tries to access the resource and the current time is over the allowed period, a PolicyRestrictionException is thrown, and the access is therefore denied.

4. **Usage Logging**

Prerequisites: clearing house url in connector configuration

Description: This defines the policy to send usage logs to the clearing house. The clearing house has to be defined in the connectors’ configuration. The logs are sent as IDS Messages to the clearing house with the path “clearingHousePath/agreementId”. The resource that is to be logged is sent in the payload. It is not possible to specify in the rule to which clearing house should be logged. If a clearing house is not specified or the message could not be delivered, the data access will still be granted.

5. **N Times Usage**

Parameters: a maximum number of accesses

Description: This policy counts the access number of the resource and denies access if the access number is greater than the maximum number of accesses. It is recommended to disable automatic contract negotiation if you plan on using this policy, so that the data consumer does not negotiate a new contract once the maximum number of accesses has been reached. To disable automatic contract negotiation change the field to policy.negotiation=false in application.properties. (How to negotiate a contract is shown here)

6. **Usage Notification**

Parameters: url to which usage notifications should be sent to (not limited to clearing house)

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Description: This policy is similar to Usage Logging but is not restricted to sending messages to a clearing house. In the post duty field of the rule, an url can be defined within a constraint to which the DSC will send usage notifications to. The payload of the logs sent contain target, issuer connector and access time. If the message could not be sent, the access will still be granted.

7. **Connector Restricted Usage**

Parameters: allowed connector URI defined in a rule

Description: This policy checks if the issuer connector is equal to a specified connector. The connector id that is used for this verification is the one provided in the config.json file. A similar check is performed when a contract is negotiated. For the negotiation the connector id is also checked to be the specified contract consumer.

8. **Security Profile Restricted Usage**

Parameters: required connector security profile (BASE_SECURITY_PROFILE, TRUST_SECURITY_PROFILE and TRUST_PLUS_SECURITY_PROFILE)

Description: This policy checks if the connector has a specific security profile. This is verified by analyzing the DAT claims of the message received.

9. **Prohibit Access**

Parameters: none

Description: This policy denies the access to the resource. A resource can't be shared if it is annotated with this policy.As specified in the documentation[32] https://international-data-spaces-association.github.io/DataspaceConnector/Documentation/v6/UsageControlhttps://raw.githubusercontent.com/Engineering-Research-and-Development/fiware-true-connector/master/docs/img/TRUE_Connector_Architecture.png, not all policies are enforced in both data access and provision. Data access policies are checked when the consumer tries to use the data. Data provision policies are checked before the data is sent from the data provider to the data consumer.

Policies enforced at data access currently are (at consumer side):

- PROVIDE_ACCESS
- USAGE_DURING_INTERVAL
- USAGE_UNTIL_DELETION

[32] https://international-data-spaces-association.github.io/DataspaceConnector/Documentation/v6/UsageControl

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- DURATION_USAGE
- USAGE_LOGGING
- N_TIMES_USAGE
- USAGE_NOTIFICATION

Policies enforced at data provision currently are (at provider side):

- PROVIDE_ACCESS
- PROHIBIT_ACCESS
- USAGE_DURING_INTERVAL
- USAGE_UNTIL_DELETION
- CONNECTOR_RESTRICTED_USAGE
- SECURITY_PROFILE_RESTRICTED_USAGE

5.2.8 Policy examples

The usage policies are written in the IDS Usage Control Language based on ODRL[33], in JSON-LD format. The "**provide-access**" usage policy example is shown in **Appendix A** of the document and more examples are available on the website [34].

5.2.9 Policy Patterns supported by True Connector with MyData Usage Control

When the True Connector is configured to work with MyData Usage Control, it supports the following policy patterns:

- Usage during interval
- Modify data in transit: the payload is modified. The current limitation is that the payload must be JSON string in order to be able to apply rules with modifiers.
- Anonymize: Specific JSON property values are modified.
- Delete: Specific Json properties are removed.
- Location based: restriction based on the consumer´s connector location (country).
- Purpose based:
- Complex rules: Rules can be composed in order to create complex permission definitions.

Some examples of these policy patterns can be found on GitHub[35].

[33] ODRL Information Model 2.2 (w3.org)
[34] https://international-data-spaces-association.github.io/DataspaceConnector/Documentation/v5/UsageControl
[35] https://github.com/Engineering-Research-and-Development/true-connector-uc_data_app#usagecontrol-examples

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

5.2.10 Policy Patterns supported by True Connector with PLATOON Usage Control

When the True Connector is configured to work with PLATOON Usage Control, it supports the following policy patterns:

- Allow the Usage of the Data provides data usage without any restrictions.
- Prohibit the Usage of the Data prohibits data usage.
- Interval-restricted Data Usage: provides data usage within a specified time interval.
- Duration-restricted Data Usage: allows data usage for a specified time period.
- Role-restricted Data Usage.
- Purpose-restricted Data Usage Policy.
- Restricted Number of Usages allows data usage for n times.
- Personal Data: filter out the contents of the data according to the data subject´s consents. To apply this rule, the Usage Control module interacts with CaPe.
- Complex rules: Rules can be composed in order to create complex permission definitions.

More information about this usage control is provided on GitHub[36].

5.2.11 Tools for policies creation

It is possible to write the policies with any text editor, but there are some policy editors available, that make this task easier:

- IDS Policy Editor[37]
- The DataSpace Connector also provides an endpoint to help creating the policies[38]

5.3 Design for 2nd technology release

In first technology release, the research was carried out to identify suitable technology framework which will be able to demonstrate the application of the usage control policies listed in the project. The current reference architecture was explained in the report and how these aligned to standards and usage control components. The data connectors are identified based on policies presented in chapter 3 and how these would be implemented and integrated into

[36] https://github.com/Engineering-Research-and-Development/true-connector-uc_data_app_platoon#platoondatausage
[37] https://odrl-pap.mydata-control.de/#/
[38] https://international-data-spaces-association.github.io/DataspaceConnector/Documentation/v6/UsageControl#usage-tips

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

the ENERSHARE project. In Table 5, the policy pattern required from pilot 1 and pilot 2 are listed and further pilot requirements will be added in future releases.

TABLE 5 - POLICY PATTERNS FROM PILOT REQUIREMENTS

No	Policy Pattern	Pilot 1	Pilot 2
1	Connector-restricted Data Usage	X	x
2	Interval-restricted Data Usage	X	x
3	Purpose-restricted Data Usage Policy	X	x
4	Security Level Restricted Policy		x
5	Modify Data (in Rest)		x
6	Local Logging		x
7	Remote Notifications		x

The Dataspace Connector (DSC) is designed to facilitate secure data sharing in decentralized environments. The usage policies defined International Data Space are 9 of 21 are supported and compliance with data exchange standards and protocols. Currently the DSC is maintained by Soviety and support of IDSCPv2 in the connector is still pending. The policy enforcement configuration needs to modular and interchangeable. Identity & Access Management which is an important feature in trust and sovereignty would be implemented in future. The data push is conceptually provided in the documentation, but the implementation has not been completed.

The TNO Security Gateway (TSG) connector has implemented remote attestation which is the process of providing and verifying proof of an application running in a secure environment. The IDSCPv2 protocol is a protocol used within IDS that supports remote attestation. The Policy Enforcement Framework is built upon XACML standards for data-flow model. The semantics of policies are based on the IDS policy language, a profile and ODRL standard. The Agreements are immutable and are stored in PAP and PDP makes decision based on the Agreements. The Usage Control in the IDS Position Paper[39] are used. The current components are developed in Kotlin and implementation in other languages would require additional configuration. In table 1, the policy pattern which are supported are presented and would be considered according to the project uses cases. The TSG Policy Enforcement Framework by TNO requires further development to support the usage policies which are defined by IDSA, and usage policies requirements in the project.

[39] https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Position-Paper-Usage-Control-in-the-IDS-V3.pdf

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

The FIWARE TRUE Connector integrates both the Platoon Usage Control Data App and MyData Usage Control Data App for enforcing the Usage Control .The connectors build upon the Information model 4.1.1 and works with HTTP/HTTPS, WS over HTTPS, and IDSCPv2. The TRUE Connector Usage Control Data App, based on IDS Usage Control App by Fraunhofer IESE. The Data Usage Control module of PLATOON has been developed by modifying IDS Dataspace Connector and does not handle Contract Negotiation. It is conducted separately, and the resulting Contract Agreements are supplied to the Usage Control module for enforcement. The additional features are given below:

- The REST services allow users to retrieve, upload, and delete Contract Agreements stored in the Contract Agreements storage. The format of these Contract Agreements adheres to the specifications outlined in the IDS Information Model. These contracts play a crucial role in enforcing Data Usage Control measures.
- This REST service applies Data Usage Control enforcement on the input data based on the Contract Agreements associated with the consumer-producer pair provided as input parameters. The service ensures that the data is handled and utilized in accordance with the terms and conditions specified in the corresponding Contract Agreements.
- The system now supports a new policy that identifies whether the data contains Personal Data. If Personal Data is detected, the module triggers CaPe (Consent-based Personal Data Protection) for each dataset associated with a specific data subject. CaPe is responsible for filtering out content that has been consented to by each individual data subject, ensuring that only authorized and approved data is processed or accessed.

In the next technology release, the policy requirements for Pilot 1 and Pilot 2 which are presented in Table 5 would be aligned to ODRL language and then these would be demonstrated using FIRWARE TRUE connector. The architecture design and communication process would be presented and deployed on the project Testbed.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

6 Full stack integrity

6.1 Task objective

The objective of Full Stack Integrity (FSI) is to ensure that during the entire data lifecycle (from provenance to removal), one can trust the components and layers involved in data at rest, in use or in transit over the complete technical infrastructure they run on (the edge-cloud continuum).

Confidential computing refers to a set of technologies and approaches aimed at protecting sensitive data and computations while they are being processed in an untrusted environment. It enables secure execution of applications or workloads in a way that preserves data confidentiality, integrity, and privacy.

Full stack integrity, on the other hand, refers to the assurance that the entire software stack and underlying infrastructure, including hardware, software, and firmware components, remain unaltered and free from unauthorized modifications throughout their lifecycle. It ensures that the system operates as intended without compromising its security, reliability, or functionality.

In essence, confidential computing focuses on protecting data and computations, while full stack integrity ensures the trustworthiness and integrity of the entire software and hardware stack. Both concepts are essential for ensuring the security and privacy of sensitive information in various computing environments.

Why is it important?

Confidential computing and full stack integrity are crucial topics in relation to data spaces due to the following reasons:

- **Data Security**: Data spaces often involve the storage, processing, and sharing of sensitive and confidential information, such as personal health records or financial data. Confidential computing technologies help protect the confidentiality of this data by ensuring that it remains encrypted and inaccessible to unauthorized parties, even during processing or analysis.
- **Data Privacy**: Data spaces typically involve multiple stakeholders and organizations collaborating and sharing data. Confidential computing enables privacy-enhancing techniques, such as secure multi-party computation or secure enclaves, which allow computations to be performed on encrypted data, preventing any party, including service providers, from accessing the raw data.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- **Trust and Integrity**: Full stack integrity is crucial in data spaces to maintain trust in the system. Ensuring the integrity of the entire software and hardware stack helps prevent unauthorized tampering or modifications that could compromise the security or reliability of the data and the overall system. It helps establish trust among participants by guaranteeing that the data and processes are executed in a secure and trustworthy environment.

By incorporating confidential computing and *full stack integrity* principles into *data spaces*, organizations and individuals can have greater confidence in the security, privacy, and trustworthiness of their data. These concepts provide the necessary safeguards to protect sensitive information, maintain data privacy, and ensure the integrity of the systems involved in data sharing and processing.

6.2 State of the art

Types of Full Stack Integrity

6.2.1 Homomorphic Encryption

Homomorphic encryption is a revolutionary cryptographic technique that allows computations to be performed on encrypted data without the need for decryption. In other words, it enables mathematical operations to be performed directly on encrypted data, preserving its confidentiality. Homomorphic encryption provides a means to securely process sensitive information while maintaining privacy and security. By leveraging this technique, data can remain encrypted at rest, in transit, and even during computation, minimizing the exposure of sensitive information to potential threats. Homomorphic encryption holds immense potential in various domains, such as secure cloud computing, privacy-preserving machine learning, and confidential data analysis. Although there are challenges related to performance and computational overhead, ongoing research and advancements in this field are paving the way for more efficient and practical homomorphic encryption schemes, thereby opening up new possibilities for secure and privacy-preserving data processing.

6.2.2 Secure Multi-Party Computation

Secure Multi-Party Computation (MPC) is a cryptographic technique that enables multiple parties to jointly compute a result without revealing their private inputs to one another. In MPC, each party holds private data and wishes to perform a computation on the collective data without exposing their individual inputs. The goal is to obtain the output of the computation while preserving the privacy and confidentiality of each party's data. Through the use of advanced cryptographic protocols, MPC allows parties to collaboratively compute the desired result without explicitly sharing their inputs. This technique has significant applications in

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

scenarios where data privacy is paramount, such as collaborative data analysis, privacy-preserving machine learning, and secure voting systems. By ensuring that no party can learn more than what is required for the computation, MPC empowers secure and privacy-preserving collaborations among multiple entities, fostering trust and enabling valuable insights to be derived without compromising data confidentiality.

6.2.3 Trusted Execution Environments

Trusted Execution Environments (TEEs) are secure and isolated environments within a computer system that provide a high level of confidentiality and integrity for executing sensitive computations. TEEs are typically implemented using hardware-based security features, such as Intel Software Guard Extensions (SGX) or ARM TrustZone. These environments create a secure enclave where sensitive data and code can be processed in isolation from the rest of the system, including the operating system and other applications. The data and code within the TEE are encrypted and protected from unauthorized access or tampering, even by privileged software or operating system administrators. TEEs offer a trusted execution environment where critical operations, such as cryptographic key management, secure authentication, and secure storage, can be performed with a high degree of assurance. TEEs are increasingly being used in various applications, including secure mobile payments, digital rights management, secure cloud computing, and protecting sensitive data in Internet of Things (IoT) devices.

In summary, Multi-Party Computation enables secure joint computations among multiple parties, Trusted Execution Environments provide secure execution environments for sensitive computations, and Homomorphic Encryption allows for computations on encrypted data. Each technique has its own unique strengths and applications, and the choice of which to use depends on the specific requirements of the use case at hand.

6.3 Design for 2nd technology release

The first demonstration of remote attestation was performed with two TSG (https://tno-tsg.gitlab.io/pages/architecture/#high-level-overview) connectors that were able to proof to each other that they ran within a secured virtual machine. The two main aspects of this demonstration are: (1) trusted execution environments and (2) remote attestation.

The trusted execution environment used is based around Azure Confidential VMs[40], specifically the AMD virtual machines with Secure Encrypted Virtualization – Secure Nested Paging (SEV-SNP). This basically allows an application inside such an VM to be aware of its surroundings, including ways of proving to other parties that the application runs in a secure environment.

[40] https://azure.microsoft.com/en-us/solutions/confidential-compute/#overview

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Remote attestation is the process of providing and verifying proof of an application running in a secure environment. The IDSCPv2 protocol is a protocol used within IDS that supports remote attestation. The protocol is built around a finite-state machine, in which the remote attestation is an important aspect. The protocol is built in such a way that it can be easily extended with drivers for specific remote attestation mechanisms. An Azure Remote Attestation driver has been created that allows for requesting the proof that an application is executed within a AMD SEV-SNP virtual machine, together with the logic to verify such a proof.

The next steps include linking the remote attestation with an ephemeral key to ensure data can be encrypted in a way that only that specific application is able to decrypt that data. Also, remote attestation on application level, by using enclaves like Intel SGX, is planned to decrease the trusted compute base to make sure only the application itself needs to be trusted.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

7 Distributed Ledger Technology

7.1 Task objective

In the framework of WP4, DLT (Distributed Ledger Technology) and blockchain are being studied for studied inside Task 4.4. The main objective of this task is studying and analyzing the features offered by blockchain and smart contracts to assure that data assets (i.e., all data coming from the interested stakeholders, taking part in energy business processes) are managed according to specific policies ensuring data usage control privacy/GDPR compliance. Data Access Policies (DAP) may be put in place to control the access to different datasets dynamically and investigate the possibility of customizing the control policies according to information derived from the context. Suitable Smart Contracts have been specifically designed to be attached to Data Assets where DAPs are specified together with (if any) economic conditions for exploiting such data. Different approaches for hybrid data handling are being explored, ranging from in chain to off-chain storage. Additionally, the blockchain will be leveraged and adapted to support ex-post verification and compliance of provenance and traceability over data assets being exchanged.

7.2 State of the art

7.2.1 Web evolution from 1.0 to 3.0

In 1991 Tim Berners Lee created the World Wide Web. The first version of the Web 1.0 was mainly a read-only web. Web 1.0 was static and unidirectional, only a small portion of users could produce content while the remainder were only able to read content retrieved from the Web. In this first version of the Web, sites were created with static HTML pages that were updated very infrequently. With Web 2.0, in 2005, there has been a shift to a participative Web in which consumers can also produce content. The following table shows the main differences between Web 1.0 and Web 2.0.

TABLE 6 - A COMPARISON BETWEEN WEB 1.0 AND WEB 2.0[41]

Web 1.0	Web 2.0
Reading	**Reading/Writing**
Companies	**Communities**

[41] S. Aghaei, M. A. Nematbakhsh and H. K. Farsani, "EVOLUTION OF THE WORLD WIDE WEB: FROM WEB 1.0 TO WEB 4.0", International Journal of Web & Semantic Technology (IJWesT) Vol.3, No.1, January 2012

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Client-Server	**Peer to Peer**
Owning	**Sharing**
Web forms	**Web applications**
Screen scraping	**APIs**
Hardware costs	**Bandwidth cost**
Lectures	**Conversation**
Service sold over the web	**Web services**
Information portals	**Platforms**

The evolution of the web leads to the creation of a web with a data-centric view. In the new web, one thinks about connections between data rather than between hypertext documents. This new type of web is called the semantic web, and the main technologies include RDF, OWL and SPARQL.

The Web has also evolved in terms of decentralization. This is the case with Web3, a term coined by Ethereum co-founder Gavin Wood in 2016 and which identifies all digital innovations and applications that rely on blockchain technology. With this new type of Web they want to build an environment that is decentralized, permissionless, with native payments and without the need for trust. Distributed Ledger Technology (DLT) converts a ledger to a distributed version[42], which can then be updated and stored in a distributed manner. The following image shows the Web3 stack divided into 4 layers.

[42] M. Belotti, N. Božić, G. Pujolle and S. Secci, «A vademecum on blockchain technologies: When, which, and how,» IEEE Communications Surveys & Tutorials, vol. 21, p. 3796–3838, 2019.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

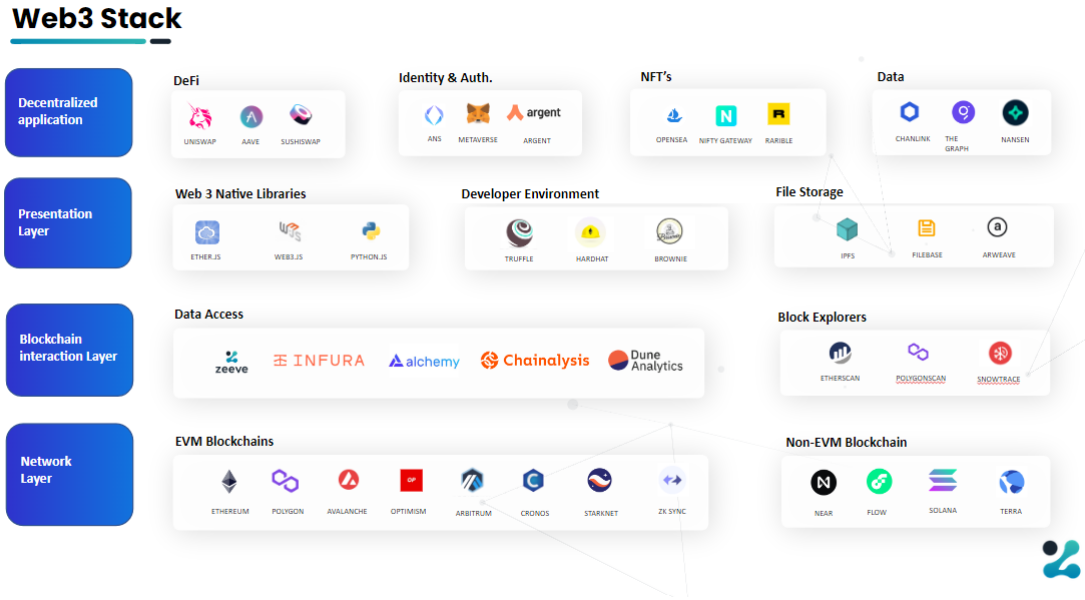


FIGURE 15 – THE WEB3 LAYERS

The first layer, the network layer, identifies the technologies on which decentralized applications can be built, such as the Ethereum blockchain or different blockchains not based on the Ethereum Virtual Machine (EVM).

The second layer provides the tools to read and write to the blockchain and analysis tools such as block explorers.

In the presentation layer are grouped all the technologies for accessing data from the underlying layers. These include traditional technologies such as React.js for building applications and presenting data or such as Ether.js and Web3.js, libraries for accessing the data in the blockchain.

Finally, the last layer shows all the major decentralized applications that provide the front-end for direct interaction with the end user.

As seen above, the focus of Web3 is blockchain. Blockchains, however, can be of different types; they can be divided into permissioned blockchain and permissionless blockchain. The main difference between these two types of Blockchains lies in the fact that while in the permissioned Blockchain restrictions are applied to be part of it and to the control procedures, in the permissionless one any entity can decide to participate with its own computers in the network.

7.2.2 The different consensus methods in DLT

In distributed environments, there is no central authority, so it is the network nodes themselves that control the network, authorizing, or denying activities within it. In order to make decisions

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

in a distributed manner without a central authority, it is necessary to have a consensus method among the network nodes. There are many different types of consensus mechanisms[43]. Among them the most used ones are the Proof of Work (PoW), the Proof of Stake (PoS) and the Proof of Authority (PoA).

The PoW was introduced with the Bitcoin Blockchain[44]. In PoW, users are required to complete complex computational calculations before submitting new transactions into the network.. This algorithm is used to confirm transactions and produce the new blocks on the chain; PoW incentivizes miners to compete in processing transactions, receiving a reward in return. Miners solve the problem, create to a new block, and confirm all transactions within it. The node that first solves the puzzle is entitled to place the block on the blockchain and gets a reward to incentivize continued work.

In the PoS every node of the networks can participate in network activity if it holds even a small amount of cryptocurrency. This consensus algorithm randomly assigns one them the possibility to validate the next block in order to get the transaction fees. Generally, the probability of being chosen is proportional to the amount of coins you have: the more coins you have, the higher the probability of validating the next block. The stake, the amount of cryptocurrency in staking, functions as a guarantee placed by the node for the proper performance of its work as a validator. Should a node make mistakes or fraudulent activities, it would lose all of its staked tokens.

In the PoA the set of validators consists of a group of approved accounts. This type of consensus algorithms provides high performance and fault tolerance. In PoA, rights to generate new blocks are awarded to nodes that have proven their authority to do so. To gain this authority and a right to generate new blocks, a node must pass a preliminary authentication. This makes it a useful consensus method in private environments since only enabled nodes can be an active part of the network. The nodes who have earned the right to be approved are incentivized to maintain a good reputation within the network.

[43] B. Lashkari and P. Musilek, «A comprehensive review of blockchain consensus mechanisms,» IEEE Access, vol. 9, p. 43620-43652, 2021.
44 S. Nakamoto, «Bitcoin: A peer-to-peer electronic cash system,» Decentralized business review, p. 21260, 2008.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

7.2.3 Ethereum and Hyperledger

The Ethereum blockchain supports full Turing-completeness[45] and implements a layer that allows users to use smart contracts to create their own rules on transitions[46]. In the Ethereum Blockchain the key points are that the transaction cannot be altered or deleted after it is recorded. The code executed by smart contracts cannot be altered by any entity and even if one node goes offline, the network will continue to operate thank to the decentralized nature of Ethereum.

These features, although very interesting, are not sufficient in some cases such as in the context of B2B applications. In these types of application Hyperledger provides different and interesting features. The following table shows the main differences between Ethereum features and Hyperledger ones.

TABLE 7 - A COMPARISON BETWEEN ETHEREUM AND HYPERLEDGER FEATURES

FEATURES	ETHEREUM	HYPERLEDGER
CONFIDENTIALITY	Public Blockchain	Private Blockchain
PURPOSE	Client-side B2C applications	Enterprise-level B2B applications
GOVERNANCE	Ethereum Developers	Linux Foundation
PARTICIPATION	Anyone	Organizations having Certificate of Authorization
PROGRAMMING LANGUAGE	Solidity	Golang, JavaScript, Java
CONSENSUS MECHANISM	PoW/PoS	Pluggable consensus mechanism
SPEED	Less	More
CRYPTOCURRENCY	Ether	None

The possibilities offered by both technologies can be exploited by using of Hyperledger Besu. Hyperledger Besu is an open source Ethereum client that can be run on the Ethereum public network or on private permissioned networks. One of the features of Hyperledger Besu is the different types of consensus mechanism available, for example PoS, PoW, PoA. The Hyperledger Besu's features include:

[45] V. Buterin and others, «A next-generation smart contract and decentralized application platform,» white paper, vol. 3, p. 2–1, 2014.
46 D. Vujičić, D. Jagodić and S. Ranđić, «Blockchain technology, bitcoin, and Ethereum: A brief overview,» in 2018 17th international symposium infoteh-jahorina (infoteh), 2018.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- The Ethereum Virtual Machine (EVM): that allows the deployment and execution of smart contracts.
- Various consensus Algorithms.
- Storage: Hyperledger Besu uses a RocksDB key-value database to persist chain data locally.
- P2P networking: Hyperledger Besu implements Ethereum's devp2p network protocols for inter-client communication.
- User-facing APIs: Hyperledger Besu provides mainnet Ethereum and EEA JSON-RPC APIs over HTTP and WebSocket protocols as well as a GraphQL API.
- Monitoring: Hyperledger Besu allows you to monitor node and network performance.
- Privacy: Privacy in Hyperledger Besu refers to the ability to keep transactions private between the involved parties.
- Permissioning: A permissioned network allows only specified nodes and accounts to participate by enabling node permissioning and/or account permissioning on the network.

Figure 16 shows the general architecture of Hyperledger Besu.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

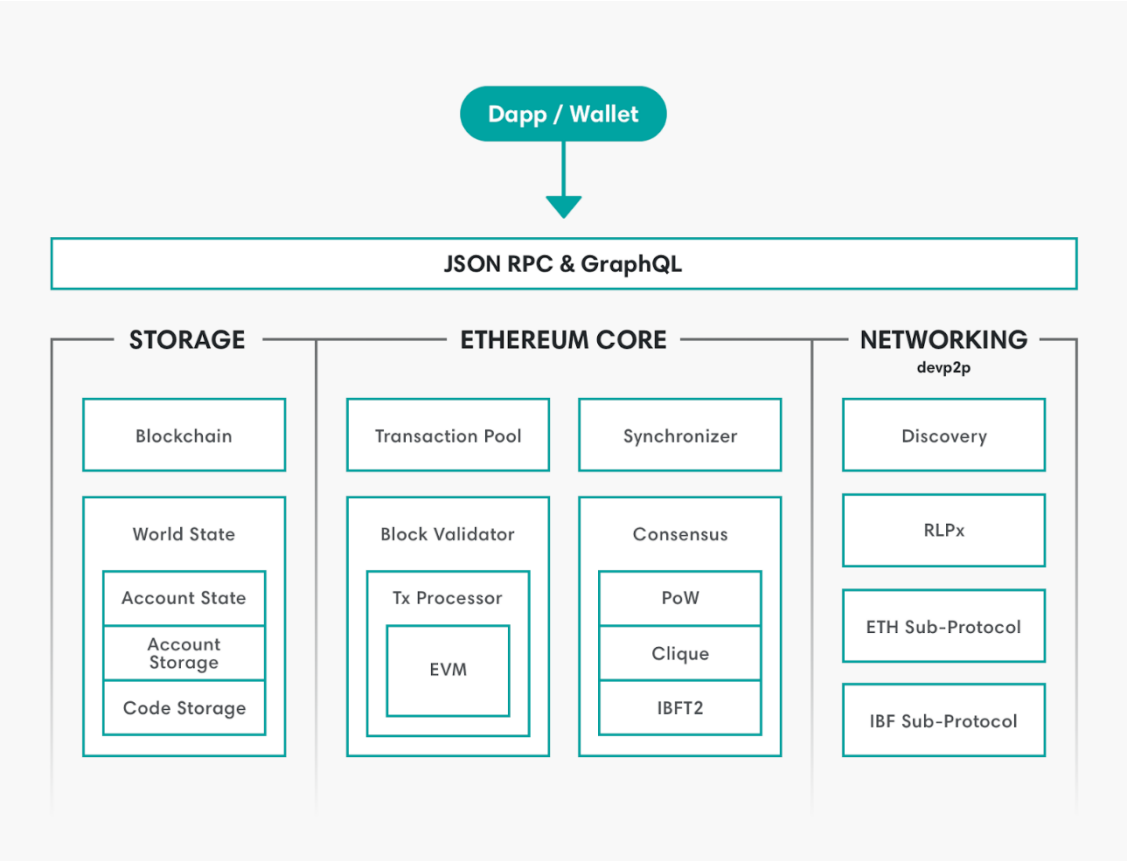


FIGURE 16 - HYPERLEDGER BESU'S GENERAL ARCHITECTURE

7.2.4 Blockchain enabled use cases

In order to exploit the DLT and blockchain for data access control, two main approaches have been analyzed and proposed. Before presenting the two approaches, a small introduction about the main uses cases for the exploitation of those technologies, is considered as opportune.

As described in the state of the art section, the blockchain technology was born for a specific purpose, i.e., cryptocurrency, making use of already existent technologies, such as DLT and cryptography, in an innovative way. Then, with the advent of Ethereum and Smart Contracts in 2014, this technology saw a growing adoption also in different domains exploiting its disrupting characteristics, especially in terms of security and distributed calculation power. New use cases and scenarios emerged for the exploitation of the blockchain, as it can be schematically reported in the following figure.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

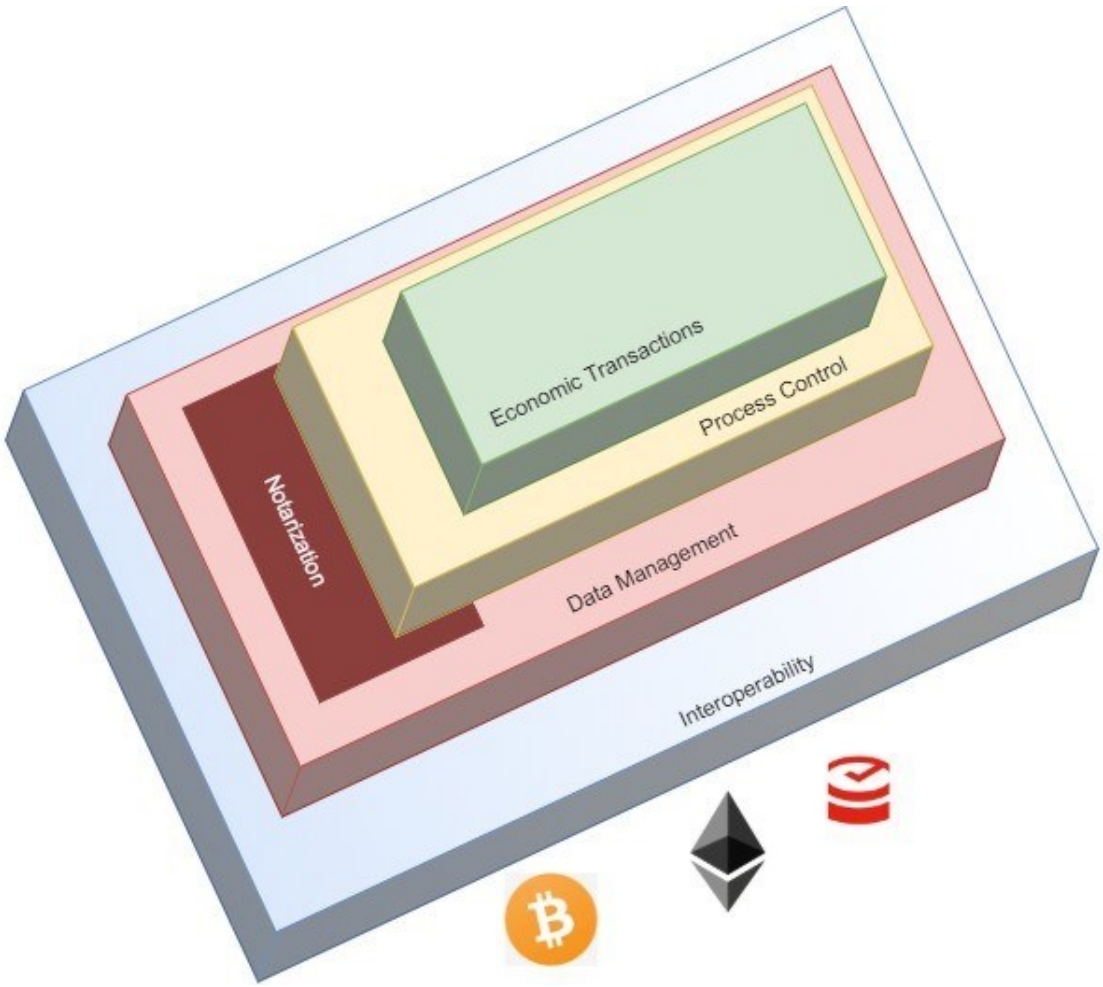


FIGURE 17 - USES CASES POWERED BY BLOCKCHAIN TECHNOLOGY

The DLT and Blockchain technology can provide a single source of data truth for the data-driven application, as one trusted and distributed system of recording information. Data coming from different heterogeneous data sources can be collected and registered into a distributed blockchain ledger, allowing the distributed applications to read and optionally write this trusted shared storage system and leverage the information validated by the technology itself.

When multiple stakeholders are involved (i.e., different applications, business units, or even corporate entities), a distributed blockchain allows credentials-based access management for secure collaboration on the shared trusted distributed data storage. If data can be trusted and verified at its operational layer, data pipelines can be built to its relevant consumers without frictions.

In general, concerning data management and exchange, the main use cases which can beneficially exploit blockchains and smart contracts can be categorized as it follows:

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- **Economic Transaction**: blockchain smart contracts for payments between two (or more) actors. Token as digital representation of a value for assets, used to reward (or penalise) users. (e.g., incentivisation of actors involved in DR programs according to their behaviour).
- **Process Control**: blockchain smart contracts used to manage inter-processes activities (e.g., the control DR flexibility services and energy transactions, thanks to the application of smart contracts to prosumers' flexibility aggregation and local peer-to-peer energy trading, making the transactions trackable and tamper-proof).
- **Data Management**: blockchain Hybrid approaches for data storage minimise the costs and assure the necessary scaling up. Distributed databases and off-chain approached used to improve the storage capabilities without losing the advantages provided by a distributed system.
- **Notarization**: Hashing timestamped occurrences of files and/or data on public blockchain notarizes them immutably.
  Interoperability: Interledger Protocols used to reduce the entry barrier for new players, leading to a more competitive environment of products and services. Integration with any type of ledger with a variety of higher-level protocols, maintaining the advantages provided by the distributed ledgers of transparency, security and trust.

7.3 Design for 2nd technology release

In particular, the first approach we propose in Task 4.4 focuses on the notarization. This first approach is strictly connected to Task 4.3 outcomes, for the notarization of the rule definition produced inside that task. As best practice, the blockchain should be used to register only encrypted data (technically speaking, the digest of a cryptographic function, commonly referred as "hash"), considering also the impossibility of deleting block data once transactions are confirmed. The rule definition can be then verified for its integrity by means of the blockchain itself. This provides the necessary level of privacy and anonymity of data, as well as security and reliability of the data exchanged, requested to the task.

Beside this first approach, which assumes the control is performed within Task 4.3 and verified in Task 4.4, we propose also a second approach, more Web 3.0 oriented, which can be tested in parallel with the standard methodologies already put in practice. In this second approach, smart contracts can be used to directly authorize reading or writing operations on data. To do that, the necessary condition is that each data owner is provided with an own Ethereum address, and so does the data consumer. Ethereum addresses are directly derived from a cryptographic public key associated to a private key that can belong only to the owner. In this sense, Ethereum addresses can be considered as a secure and trustful instruments for data

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

access. Technically speaking, it is "computationally impossible" that a malicious node, controlled by a hacker, can modify the blockchain status without being spotted and the node excluded from the network. So, once the owner of data publishes his or her smart contract into the blockchain, his or her Ethereum address is registered into the blockchain once and forever (in particular, as data attached to the block created after the confirmation of the transactions by the majority of the nodes). In simple words, this means that nobody can realistically replace the owner of the smart contract and modify its status, with the maximal theoretical computational power known so far.

Provided that technical premise, due for the sake of completeness, the second approach we propose can be illustrated and depicted as in the following figure.

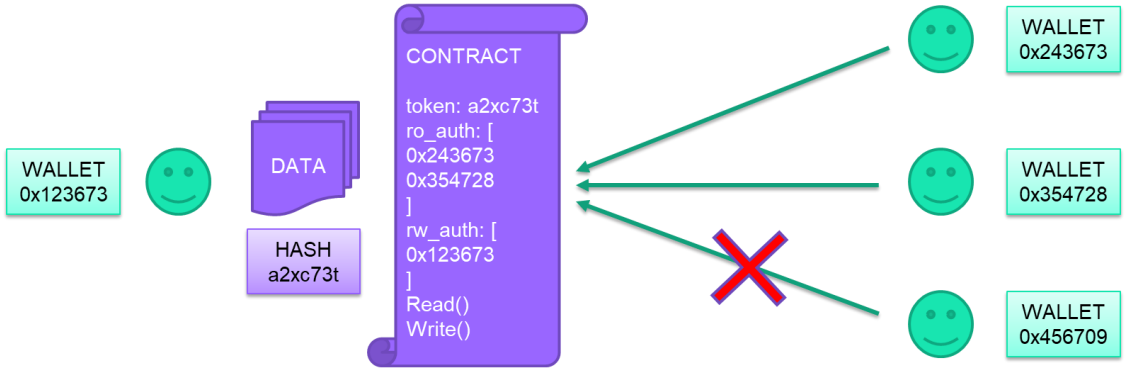


FIGURE 18 – DATA ACCESS CONTROL VIA BLOCKCHAIN

The owner of the data instantiates a new smart contract, associated to his or her Ethereum address (included into an Ethereum wallet). Then, whenever each data or asset is created, it or its reference is tokenized, e.g., using the same hash function used for the first approach. For simplicity, in the figure a single token is associated to the smart contract: in real cases, inside the smart contract, also a list of tokens can be registered, but it should have complicated the graphical representation. The most important thing is that inside the contract, for each token, two lists of Ethereum addresses are stored and maintained: the list of the user (identified by their Ethereum addresses) allowed to read the data, and the list of users allowed to read and write the data. For all the technical considerations described so far, nobody can replace neither the data owner nor the data consumers, completely defusing the possibility of cybersecurity attacks like Man-In.The-Middle or DDoS (Distributed Denial of Service) without being spotted and automatically excluded from the blockchain network.

It is worth noting that with tokenization of data, only encrypted data are registered inside the blockchain, in thus ensuring the fulfillment of privacy requirement. This however entails the further need of having and maintaining an external "off-chain" database, for the storage of the raw unencrypted data (or reference to that data). In general, this database can be provided by the data owners themselves, e.g., a local database used by pilots for their own monitoring data.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

According to each specific case, the first or the second approach can be followed, considering the tradeoff between completeness of solution versus its complexity of implementation. In most cases, the first approach, can be adopted to exploit the reliability of the blockchain, to verify the integrity of the access rule definition, in a much easier but still effective way.

In the next technology release, the two smart contracts will be developed, tested and reported.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

8 Conclusions

8.1 List of (software) components of alpha version

In the first technical release WP4 provides two essential building blocks for the energy data space: a data space connector implementation and an identity provider. Together with the metadata broker (WP5), these components allow for a minimal viable data space.

8.1.1 Connector implementation

The data space connector is the basis for trust and sovereignty. It provides secure peer-to-peer data exchange with IAA (Identification, Authentication, Authorization). Section 2.2 elaborated on the importance of the data space connector.

TNO Security Gateway (TSG)	
Description	IDS-based HTTP Multipart communication. See: Message Flows, Deployment. And the Playground to play around with the connector
Software details	Written in Kotlin, built into Docker images. Default deployment based on Kubernetes & Helm.
Codebase	• https://gitlab.com/tno-tsg/core-container • https://gitlab.com/tno-tsg/helm-charts/connector

TRUE Connector	
Description	IDS-based connector implementation consisting of a execution core container, a data app and usage control component.
Software details	Written in Java, built into Docker images. Docker compose and kubernetes manifests available for deployment.
Codebase	• https://github.com/Engineering-Research-and-Development/true-connector

8.1.2 Identity provider (CA + DAPS):

The certificate authority (CA) issues identity certificates for connector instances by signing Certificate Signing Requests (CSRs) that have been handed in by valid connector instances. It revokes certificates that become invalid and, for higher trust levels, assure that private keys are properly stored in hardware modules (such as a TPM or HSM).

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

The DAPS component provides dynamic, up-to-date attribute information about Participants and Connectors in form of signed claims and embeds them into Dynamic Attribute Tokens (DATs).

TSG DAPS (includes CA)	
Description	Implementation of an IDS Dynamic Attribute Provisioning Service (DAPS) v2, combined with certificate authority capabilities to sign certificate signing requests (CSR)
Software details	Written in Typescript. Both backend and generic frontend application.
Codebase	• https://gitlab.com/tno-tsg/daps • https://tno-tsg.gitlab.io/docs/daps/

IDS Identity provider	
Description	Intermediary offering services to create, maintain, manage and validate identity information of and for Participants in the International Data Spaces.
Software details	Implementation consisting of two components: the Certificate Authority (CA) and Dynamic Attribute Provisioning Service (DAPS).
Codebase	• https://github.com/International-Data-Spaces-Association/IDS-testbed/tree/master/CertificateAuthority • https://github.com/International-Data-Spaces-Association/omejdn-daps

8.2 Plans for second technology release

For tasks T4.1 to T4.4 this report outlines the plans and high level components designs for the second technology release. In short:

- For Identity and access management (T4.2) we'll integrate self-sovereign identity (SSI) concepts into the identity provider component. For more details see section 4.3.
- For Usage control policies (T4.3) several use case policies identified in the pilots will be implemented and demonstrated in the TRUE connector. For more details see section 5.3.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- The concept of full stack integrity (T4.1) will be integrated in the TSG connector and next steps are taking in linking remote attestations about the trusted execution environment with usage control.
- Finally we'll implement a component using distributed ledger technology (T4.4) to notarize access and usage policies, e.g. those that are defined by T4.3.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

9 References

[1] Nagel L., Lycklama D. (2021): Design Principles for Data Spaces. Position Paper. Version 1.0. Berlin

[2] ENERSHARE D2.1 Use cases' descriptions and list of minimum Data Space building blocks required for pilots

[3] The NGI eSSIF-Lab project is an H2020 project under grant agreement no 871932. An overview of these components is given in eSSIF Booklet 23.
Link: https://essif-lab.eu/wp-content/uploads/2023/01/essif-booklet-23.pdf

[4] IDSA Data Connector Report v1 (November 2022).
Link: https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Data-Connector-Report-November-2022.pdf

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Appendix A – Usage policy example


```
{
   "@context":{
      "ids":"https://w3id.org/idsa/core/",
      "idsc":"https://w3id.org/idsa/code/"
   },
   "@type":"ids:ContractAgreement",
   "@id":"https://w3id.org/idsa/autogen/contractAgreement/52272512-dcbd-4b15-8f1f-f409327a4a9a",
   "ids:permission":[
      {
         "@type":"ids:Permission",
         "@id":"https://w3id.org/idsa/autogen/permission/59b0a20a-11bd-4276-8341-af40c8960e98",
         "ids:target":{
            "@id":"https://w3id.org/idsa/autogen/artifact/8e3a5056-1e46-42e1-a1c3-37aa08b2aedd"
         },
         "ids:title":[
            {
               "@value":"Example Usage Policy",
               "@type":"http://www.w3.org/2001/XMLSchema#string"
            }
         ],
         "ids:description":[
```


Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

```
            {
               "@value":"provide-access",
               "@type":"http://www.w3.org/2001/XMLSchema#string"
            }
         ],
         "ids:action":[
            {
               "@id":"idsc:USE"
            }
         ]
      }
   ],
   "ids:provider":{
      "@id":"https://w3id.org/idsa/autogen/baseConnector/7b934432-a85e-41c5-9f65-669219dde4ea"
   },
   "ids:consumer":{
      "@id":"https://w3id.org/idsa/autogen/baseConnector/7b934432-a85e-41c5-9f65-669219dde4ea"
   },
   "ids:contractDate":{
      "@value":"2021-02-18T10:15:21.137Z",
      "@type":"http://www.w3.org/2001/XMLSchema#dateTimeStamp"
   },
   "ids:contractStart":{
      "@value":"2021-02-18T10:15:21.137Z",
```


Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

```
      "@type":"http://www.w3.org/2001/XMLSchema#dateTimeStamp"
   },
   "ids:contractEnd":{
      "@value":"2022-02-18T10:15:21.137Z",
      "@type":"http://www.w3.org/2001/XMLSchema#dateTimeStamp"
   }
}
```


Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831