HEDGE-IoT

Holistic approach towards Empowerment of the Digitalization of the Energy Ecosystem through adoption of IoT solutions

D4.1
HEDGE-IoT Interoperability Framework and Integrated Solution (First release)

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

DOCUMENT CONTROL SHEET

PROJECT INFORMATION

Project Number	101136216		
Project Acronym	HEDGE-IoT		
Project Full title	Holistic Approach towards Empowerment of the Digitalization of the Energy Ecosystem through adoption of IoT solutions		
Project Start Date	01 January 2024		
Project Duration	42 months		
Funding Instrument	Horizon Europe Framework Programme	Type of action	HORIZON-IA HORIZON Innovation Actions
Call	HORIZON-CL5-2023-D3-01-15		
Topic	Supporting the green and digital transformation of the energy ecosystem and enhancing its resilience through the development and piloting of AI-IoT Edge cloud and platform solutions		
Coordinator	European Dynamics Luxembourg SA		

DELIVERABLE INFORMATION

Deliverable No.	D4.1							
Deliverable Title	HEDGE-IoT Interoperability Framework and Integrated Solution (First release)							
Work-Package No.	WP.4							
Work-Package Title	Digital Interoperability Framework and Integrated Solution							
Lead Beneficiary	DST							
Main Author	DST							
Other Authors	ED TNO TRIALOG INESC KONC VUA							
Due date	M15							
Deliverable Type		Document, Report (R)		Data management plan (DMP)		Websites, press & media action (DEC)		Other X

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Dissemination Level		Public (PU)X		Sensitive (SEN)		Classified
	PU: Public, fully open SEN: Sensitive, limited under the conditions of the Grant Agreement Classified R-UE/EU-R – EU RESTRICTED under the Commission Decision No2015/444 Classified C-UE/EU-C – EU CONFIDENTIAL under the Commission Decision No2015/444 Classified S-UE/EU-S – EU SECRET under the Commission Decision No2015/444					

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Document Revision History

Version	Date	Description of change	List of contributor(s)
0.1	24/01/2025	Table of Contents (ToC) draft	Antonella Cadeddu (DST) Giovanni Natale (DST)
0.2	30/01/2025	ToC revisions	All WP4 partners
0.3	07/02/2025	Final ToC, structure and guidelines	Antonella Cadeddu (DST) Giovanni Natale (DST)
0.4	26/02/2025	First contributions	Antonella Cadeddu (DST) Giovanni Natale (DST) Apostolos Kapetanios (ED) Lenos Peratitis (ED) Cornelis Bouter (TNO) Laura Daniele (TNO) Wouter Vandenberg (TNO) Fábio Coelho (INESC) Léo Cornec (TRIALOG) Josipa Stegić (KONC) Ivan Krajnović (KONC)
0.5	28/02/2025	Consolidation	Antonella Cadeddu (DST) Giovanni Natale (DST)
0.6	14/02/2025	Final partner's contributions	Antonella Cadeddu (DST) Giovanni Natale (DST) Apostolos Kapetanios (ED) Lenos Peratitis (ED) Cornelis Bouter (TNO) Laura Daniele (TNO) Wouter Vandenberg (TNO) Fábio Coelho (INESC) Léo Cornec (TRIALOG) Josipa Stegić (KONC) Ivan Krajnović (KONC)
0.7	17/03/2025	Consolidation and final touches	Antonella Cadeddu (DST) Giovanni Natale (DST)
0.8	24/03/2025	Review by RWTH	Katharina Wehrmeister (RWTH) Marjorie Hoegen (RWTH) Taeyoung Kim (RWTH)
0.9	25/03/2025	Review by UNIZG	Tomislav Antić (UNIZG)
0.10	27/03/2025	Processing of reviewers' comments and Full complete version	Antonella Cadeddu (DST) Giovanni Natale (DST)
1.0	07/04/2025	Completed Final Review	Lenos Peratitis (ED) Nikos Bilidis (ED)

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

PARTNERS

Participant number	Participant organisation name	Short name	Country
1	EUROPEAN DYNAMICS LUXEMBOURG SA	ED	LU
2	RHEINISCH-WESTFAELISCHE TECHNISCHE HOCHSCHULE AACHEN	RWTH	DE
~~3~~	~~ENGINEERING - INGEGNERIA INFORMATICA SPA~~	~~ENG~~	~~IT~~
4	EREVNITIKO PANEPISTIMIAKO INSTITOUTO SYSTIMATON EPIKOINONION KAI YPOLOGISTON	ICCS	EL
5	INESC TEC - INSTITUTO DE ENGENHARIADE SISTEMAS E COMPUTADORES, TECNOLOGIA E CIENCIA	INESC	PT
6	NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO	TNO	NL
7	TAMPEREEN KORKEAKOULUSAATIO SR	TAU	FI
8	TEKNOLOGIAN TUTKIMUSKESKUS VTT OY	VTT	FI
9	TRIALOG	TRIALOG	FR
~~10~~	~~CYBERETHICS LAB SRLS~~	~~CEL~~	~~IT~~
11	CENTRO DE INVESTIGACAO EM ENERGIA REN - STATE GRID SA	NESTER	PT
12	INTERNATIONAL DATA SPACES EV	IDSA	DE
13	ELIA TRANSMISSION BELGIUM	ETB	BE
14	HRVATSKI OPERATOR PRIJENOSNOG SUSTAVA D.D.	HOPS	HR
15	UNIVERSITATEA TEHNICA CLUJ-NAPOCA	TUC	RO
16	CLUSTER VIOOIKONOMIAS KAI PERIVALLONTOS DYTIKIS MAKEDONIAS	CLUBE	EL
17	F6S NETWORK IRELAND LIMITED	F6S	IE

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

18	SOCIAL OPEN AND INCLUSIVE INNOVATION ASTIKI MI KERDOSKOPIKI ETAIREIA	INCL	EL
19	ABB OY	ABB	FI
20	ENERVA OY	ENERV	FI
21	JARVI-SUOMEN ENERGIA OY	JSE	FI
22	DIMOSIA EPICHEIRISI ILEKTRISMOU ANONYMI ETAIREIA	PPC	EL
23	DIACHEIRISTIS ELLINIKOU DIKTYOU DIANOMIS ELEKTRIKIS ENERGEIAS AE	HEDNO	EL
24	INDEPENDENT POWER TRANSMISSION OPERATOR SA	IPTO	EL
25	ELLINIKO HRIMATISTIRIO ENERGEIAS	HENEX	EL
26	HARDWARE AND SOFTWARE ENGINEERING EPE	HSE	EL
27	QUE TECHNOLOGIES KEFALAIOUCHIKI ETAIREIA	QUE	EL
28	ARETI S.P.A.	ARETI	IT
29	APIO S.R.L.	APIO	IT
30	ACEA ENERGIA SPA	AE	IT
~~31~~	~~VOLKERWESSELS ICITY B.V.~~	~~VWICI~~	~~NL~~
32	ARNHEMS BUITEN BV	AB	NL
33	STICHTING VU	VU	NL
34	COOPERATIVE ELECTRICA DO VALE DESTE CRL	CEVE	PT
35	REN - REDE ELECTRICA NACIONAL SA	REN	PT
36	MC SHARED SERVICES SA	SONAE	PT
37	ELES DOO SISTEMSKI OPERATER PRENOSNEGA ELEKTROENERGETSKEGA OMREZJA	ELES	SI
38	ELEKTRO GORENJSKA PODJETJE ZA DISTRIBUCIJO ELEKTRICNE ENERGIJE DD	EG	SI
39	OPERATO DOO	OPR	SI

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

40	SVEUCILISTE U ZAGREBU FAKULTET ELEKTROTEHNIKE I RACUNARSTVA	UNIZG	HR
41	INSTITUT JOZEF STEFAN	JSI	SI
42	KONCAR - DIGITAL DOO ZA DIGITALNE USLUGE	KONC	HR
43	DS TECH SRL	DST	IT
44	CYBERSOCIAL LAB SRL IMPRESA SOCIALE	CSL	IT

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

DISCLAIMER

COPYRIGHT NOTICE

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

EXECUTIVE SUMMARY

HEDGE-IoT (Holistic Energy Decentralized Grid for Enhanced IoT) is a flagship project funded by the European Union's Horizon Europe research and innovation program. The initiative aims to develop a state-of-the-art, interoperable digital framework for the energy sector, enabling the seamless deployment of Internet-of-Things (IoT) assets across the energy ecosystem—from Transmission System Operators (TSOs) to behind-the-meter applications.

This document provides a professional and comprehensive summary of the progress and key achievements within Work Package 4 (WP4) of the HEDGE-IoT project. WP4 is focused on addressing critical technical challenges by developing interoperability frameworks, integrating advanced semantic technologies, coordinating cloud and edge systems, and implementing robust cybersecurity measures to support the evolution of IoT ecosystems.

WP4 is structured around several key tasks. Task 4.1 focuses on creating an Open Services Catalogue and App Store, which facilitates access to and management of Data Apps. This includes essential operations such as registration, publication, and provisioning, and supports the creation of innovative data-driven services.

Task 4.2 emphasizes the development of a middleware designed to ensure secure, seamless, and standardized data exchange across both edge and cloud levels. By leveraging established frameworks like FIWARE, and adhering to IDSA principles, this task enhances interoperability across diverse systems, adhering to the concept of Data Spaces.

Task 4.3 aims to improve semantic interoperability through the Interconnect Semantic Interoperability Framework (SIF). By extending ontologies such as SAREF to cater to specific use cases, this task promotes decentralized knowledge sharing and more effective communication between systems.

In Task 4.4, guidelines and roadmaps are developed to support the integration of tools, components, and platforms. This ensures smooth and interoperable interactions among IoT and Edge nodes within the HEDGE-IoT framework, creating a cohesive operational environment.

Finally, Task 4.5 is dedicated to defining practices that prioritize trustworthiness, security, and privacy by design. This includes addressing safety concerns related to AI and implementing strategies to mitigate risks like adversarial attacks and data poisoning.

Together, these tasks lay the foundation for a robust, secure, and interoperable IoT framework, supporting the project's overarching goal of advancing next-generation energy ecosystems. This deliverable represents the first in a series of three reports - D4.1, D4.2, and D4.3- with subsequent deliverables detailing further progress and outcomes of WP4.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

TABLE OF CONTENTS

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

LIST OF TABLES

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

LIST OF FIGURES

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

ABBREVIATIONS

Abbreviation	Full description
AI	Artificial Intelligence
API	Application Programming Interface
BUC	Business Use Case
CEEDS	Common European Energy Data Space
CIM	Common Information Model
CoC	Code of Conduct
CRA	Cyber Resilience Act
DAPS	Dynamic Attribute Provisioning Service
DFD	Data Flow Diagram
DSA	Digital Service Act
DSP	Data Space Protocol
DSSC	Data Space Support Centre
EC	European Commission
EDC	Eclipse Dataspace Component
EDSCP	Energy Data Space Cluster Projects
EIF	European Interoperability Framework
ESA	Energy Smart Appliance
ETSI	European Telecommunication Standardization Institute
EU	European Union
GDPR	General Data Protection Regulation
GOOSE	Generic Object-Oriented Substation Event
GUI	Graphical User Interface

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

HEDGE-IoT	Holistic Energy Decentralized Grid for Enhanced Iot
HTTP	Hyper Text Transfer Protocol
HTML	Hyper Text Markup Language
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technologies
IDSA	International Data Spaces Association
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Intellectual Property
IPTO	Independent Power Transmission Operator
ISC	Integration Services Component
ISTQB	International Software Testing Qualifications Board
JRC	Joint Research Centre
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
LOT	Linked Open Terms
LN	Logical Nodes
ML	Machine Learning
MMS	Manufacturing Message Specification
MVD	Minimum Viable Dataspace
MVP	Minimum Viable Product
OCI	Open Container Initiative
ODBC	Open Database Connectivity
ODC	Ontology-Driven Constraint
OWL	Web Ontology Language

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

PPC	Public Power Corporation
PSP	TRIALOG Privacy and Security Plan
P2P	Peer to Peer
QoS	Quality of Service
REST	Representational State Transfer
RDF	Resource Description Framework
SAREF	Smart Applications REFerence Ontology
SDK	Software Development Kit
SGAM	Smart Grid Architecture Model
SIF	Semantic Interoperability Framework
STH	Semantic TreeHouse
SUC	System Use Case
SV	Sampled Values
TRL	Technology Readiness Level
TSO	Transmission System Operator
UI	User Interface
URI	Uniform Resource Identifier
WP	Work Package
X-CCP	Cross-Cutting Characteristics Plan
XML	eXtensible Markup Language

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

1 INTRODUCTION

The HEDGE-IoT project is aiming to revolutionize the way data and digital services interact in distributed environments, with a particular emphasis on the energy sector. By leveraging Artificial Intelligence (AI), Internet of Things (IoT), and cloud/edge computing, the HEDGE-IoT project aims to create an interoperable and intelligent data-sharing ecosystem. Its primary goals are to enhance data-driven decision-making and optimize energy management by enabling seamless data exchange, processing, and analysis across various stakeholders. Central to this approach is the concept of Data Spaces, which ensures that organizations remain in full control of their data while facilitating secure, standardized, and efficient interoperability.

A key element in realizing this vision is Work Package 4 (WP4), which focuses on developing the interoperability framework and integrated solutions that underpin the HEDGE-IoT ecosystem.

WP4 is responsible for defining and implementing digital enablers that allow heterogeneous services and platforms to communicate effortlessly.

This includes creating an open and modular architecture capable of integrating various IoT, AI, and data-sharing solutions, ensuring cohesive and secure collaboration across different systems and stakeholders. Several fundamental components at the core of this deliverable play a crucial role in establishing this interoperability.

Key components of this framework include the Interoperability Middleware, featuring the Eclipse Dataspace Connector (EDC). The EDC plays a pivotal role in enabling seamless data exchange between different entities, adhering to European Data Spaces principles and ensuring compliance with sovereignty and security requirements. The EDC-based architecture is engineered to facilitate scalable and decentralized data sharing, empowering data providers and consumers to interact effortlessly while maintaining control over their assets.

Another critical component is the Open Services Catalogue and App Store, which serves as a centralized registry for digital services within the HEDGE-IoT ecosystem. This catalogue enables service providers to register, manage, and expose their applications, ensuring easy discovery and integration of interoperable services. The App Store complements this by streamlining deployment and management, fostering collaboration between different stakeholders and enabling cross-sector data utilization.

A crucial aspect of this deliverable is ensuring semantic interoperability, achieved through the adoption of standardized ontologies and data models, such as ETSI SAREF and IEC CIM. These standards enable a uniform data representation and exchange across different systems. The semantic layer facilitates automated reasoning, data alignment, and seamless communication between heterogeneous IoT and AI-driven applications, ensuring that services can interpret and process data ambiguity.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Cybersecurity and privacy are foundational elements of the interoperability framework. Given the sensitivity of energy data and the inherent risks associated with IoT environments, WP4 prioritizes secure data exchange, access control, and threat mitigation strategies. This includes deploying advanced security protocols, conducting risk assessments, and ensuring compliance with European cybersecurity standards.

This deliverable represents the first major milestone in the development of the HEDGE-IoT interoperability framework and delivers an operational version of key enablers laying the groundwork for future iterations. The components introduced here will be validated, expanded, and refined in subsequent project phases, ensuring that HEDGE-IoT evolves into a robust, scalable, and widely adopted solution for next-generation energy and data-sharing ecosystems.

1.1 Purpose of the Document

This document, Deliverable D4.1, represents the first major milestone in the HEDGE-IoT journey towards creating a robust, scalable, and interoperable framework for the IoT energy ecosystem. The main objective of this document is to provide a comprehensive foundation for the development of an integrated solution that connects diverse IoT platforms, stakeholders, and services through a trusted and interconnected Data Space.

Specifically, the purpose of this document is to:

- Present the initial design and implementation of the interoperability framework, detailing key components such as the Interoperability Middleware, Semantic Interoperability Framework, and Open Services Catalogue.
- Describe the architecture and technical specifications necessary to facilitate secure, scalable, and standardized data exchange among the various actors and technologies within the HEDGE-IoT ecosystem.
- Outline the methodologies, tools, and standards adopted to ensure compliance with European regulations on data sovereignty, security, and privacy, as well as alignment with state-of-the-art practices in interoperability and semantic data exchange.
- Establish a baseline for monitoring progress and guiding future iterations, which will focus on enhancing the framework and integrating additional components and functionalities in subsequent phases of the project.

1.2 Document Structure

The document is structured into distinct but interrelated sections, each addressing a critical aspect of the HEDGE-IoT project's interoperability framework. This approach ensures a logical progression and facilitates understanding of the concepts, methodologies, and technologies described.

- Chapter 1-Introduction: This section provides an overview of the HEDGE-IoT project, emphasizing its role in advancing data-driven decision-making and energy management through an interoperable IoT ecosystem. It highlights the objectives of Work Package 4

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

(WP4) and its significance in achieving the project's overarching goals.Chapter 2- Interoperability Middleware: This chapter delves into the design and functionality of the Eclipse Dataspace Connector (EDC), which is central to enabling secure and policy-driven data exchanges within the ecosystem. It discusses the architecture, key features, and integration with European Data Space principles, ensuring compliance with sovereignty and security requirements.

- Chapter 3-Open Services Catalogue and App Store: This section introduces the Open Services Catalogue and App Store, which act as centralized registries for managing and distributing Data Apps. It explains how these components facilitate the discovery, deployment, and integration of interoperable services, fostering collaboration among stakeholders and supporting data-driven applications.
- Chapter 4- Semantic Interoperability: The document explores the adoption of standardized ontologies and semantic models, such as ETSI SAREF and IEC CIM, to achieve seamless and unambiguous data exchange across diverse IoT platforms. It also details the methodologies used to develop, publish, and maintain these ontologies, ensuring consistency and alignment with best practices.
- Chapter 5-IoT Cloud/Edge System Integration: This chapter outlines the strategies and methodologies employed to integrate IoT devices, edge nodes, and cloud systems within a unified framework. It includes a discussion on system interfaces, component catalogues, and the roadmap for achieving full interoperability.
- Chapter 6- Security and Privacy: Given the sensitivity of energy data and the vulnerabilities associated with IoT environments, this section focuses on the cybersecurity measures and privacy-preserving mechanisms implemented within the framework. It highlights strategies for threat mitigation, data access control, and compliance with European cybersecurity standards.
- Chapter 7-Conclusions: The final section summarizes the deliverable's achievements, emphasizing the progress made in developing the HEDGE-IoT interoperability framework. It also outlines the next steps for validating, refining, and expanding the framework in subsequent project phases.
- Appendix A**–** Provides supplementary details.

This structure ensures that the document is comprehensive yet accessible, offering a clear narrative that guides readers through the technical and conceptual aspects of the interoperability framework while aligning them with the HEDGE-IoT project's strategic vision.

1.3 Relationship with other Work Packages and Tasks

Work Package 4 (WP4) plays a crucial role in heterogeneous platforms while maintaining security, scalability, and compliance with data space principles. This involves the development of an Open Services Catalogue, a Middleware solution, an EDC-based Connector, Semantic Interoperability mechanisms and IoT Cloud/Edge integration for HEDGE-IoT to ensure seamless interoperability between the different components and services of the project. It focuses on building a data-sharing framework that enables communication across cybersecurity enablers.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Since interoperability is a cross-cutting requirement, WP4 interacts directly with several other work packages, supporting their implementation and ensuring that all technical developments can work together effectively. Below is an overview of how WP4 connects with other key areas of the project.

Relationship with WP3 (Technological Enablers Specification, Design and Development)

WP3 is responsible for defining and developing AI-driven services, which will be integrated into the HEDGE-IoT ecosystem. WP4 ensures that these services can communicate, exchange data, and operate efficiently in a distributed and federated environment.

- Task 3.1 (Extension of demo specific IoT proprietary digital interfaces, platforms and tools) provides the necessary data models, APIs, and interoperability standards that WP4 implements in its middleware and connector to enable seamless cross-platform interactions.
- Task 3.2 (AI/IoT Enabled User-Centric Services Specification) defines the functional and technical specifications of the AI services that WP4 later onboards and integrates using the Open Services Catalogue and Middleware.
- Task 3.5 (AI Service Orchestration and Lifecycle Management Computational Orchestration to ensure the cloud-edge continuum) relies on WP4's interoperability solutions to manage the deployment, execution, and scaling of AI services, ensuring that applications can efficiently operate across edge and cloud environments.

Relationship with WP5 (Demonstration Across Technologies and Scenarios)

WP5 is dedicated to testing and validating the HEDGE-IoT infrastructure in real-world pilot scenarios. WP4 plays a critical role by enabling secure and efficient data exchange across pilot sites, allowing different components to work together within the pilots.

- Task 5.1 (Demos' preparation, evaluation framework and baseline analysis) depends on WP4's connectivity mechanisms and interoperability enablers to integrate pilot services. The EDC-based connector is particularly important for ensuring secure data transactions between pilot infrastructures.

Relationship with WP2 (– Stakeholders Requirements and System Specifications)

WP2 provides fundamental guidelines for WP4's development, ensuring that the interoperability framework aligns with the overall project architecture, security standards, and functional requirements.

- Task 2.6 (Functional specifications for interoperability and standardised data integration) delivers use case-driven requirements, which WP4 translates into functional and technical solutions.
- Task 2.7 (Operational Framework Design-Interoperable EDS-aligned RA) defines the high-level architecture that WP4 follows to ensure seamless integration of its interoperability components.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Relationship with WP7 (Dissemination, Exploitation, Standardization)

WP7 ensures that the developments in HEDGE-IoT contribute to industry's best practices and standardization efforts. WP4 collaborates with W7 to align its interoperability framework with European data-sharing initiatives.

> Task 7.4 (Contribution to standards) by integrating IDSA principles, the Data Space Protocol, and semantic interoperability standards such as SAREF and IEC CIM, WP4 ensures that HEDGE-IoT's middleware and connector are compliant with state-of-the-art data-sharing standards.

WP4 serves as a central enabler in HEDGE-IoT, connecting AI services, pilot infrastructures, and data-sharing components to ensure smooth operation and secure interoperability. Its close collaboration with WP2, WP3, WP5, and WP7 highlights its key role in achieving the project's overarching goal: creating an interoperable, AI-driven IoT ecosystem that ensures data sovereignty and seamless cross-platform interaction.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

2 INTEROPERABILITY MIDDLEWARE

At the outset of the HEDGE-IoT project, the OneNet Connector was initially selected to address the project's interoperability requirements. However, the project's evolving focus on ensuring full compliance with the Data Space Protocol, as defined by the International Data Spaces Association (IDSA), underscored the need for a more suitable solution.

In response to these developments, the Technical Board of the project undertook a comprehensive review and selected the Eclipse Dataspace Connector (EDC) as the preferred solution. At the same time the OneNet connector will also be used in specific use cases in order to showcase the interoperability and scalability of the HEDGE-IoT ecosystem, which is able to interoperate with multiple systems in a technology agnostic manner. This decision reflects the necessity for a reliable, interoperable, and compliant connector that aligns with the dynamic requirements of the HEDGE-IoT ecosystem.

In this deliverable and in the Sections that follow a complete description of the Eclipse Data Space Connector is presented. As the project evolves and matures the use of the OneNet Connector will be framed more accurately. Specific use-cases within certain pilots will be identified in order to showcase how the HEDGE-IoT ecosystem can work with other connectors as well and support data exchanges through data spaces in a technology-agnostic manner. In the next deliverables of WP4 a description of the OneNet Framework will be included and more specific details on the usage and the added value will be elaborated.

The selection of EDC was guided by several key considerations:

- **Compliance with IDSA Standards:** EDC fully adheres to the Data Space Protocol, facilitating a decentralized, sovereign data exchange model that ensures robust data privacy, security, and control.
- **Scalability and Flexibility:** EDC's modular architecture provides a scalable and adaptable solution capable of seamlessly integrating with diverse IoT and AI services, making it well-suited to the evolving needs of the HEDGE-IoT project.
- **Enhanced Security and Governance:** EDC incorporates a contract-based data exchange model, enabling fine-grained access control and ensuring secure, compliant transactions across multiple stakeholders in the energy ecosystem.
- **Open-Source Sustainability and Continuous Improvement:** As an open-source project, EDC benefits from ongoing contributions and updates from a growing community, ensuring its long-term sustainability and alignment with industry best practices.

The adoption of the Eclipse Dataspace Connector positions the HEDGE-IoT project to not only comply with international standards but also to strengthen its role within the IoT ecosystem by offering a secure, scalable, and fully interoperable data exchange solution. This strategic decision underscores the project's commitment to innovation, security, and sustained success

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

2.1 Connector Architecture

2.1.1 Eclipse Dataspace Connector (EDC)

EDC operates within a decentralized network where data remains under the owner's control until explicitly shared under agreed-upon terms. This is achieved through a policy enforcement mechanism that governs data usage, transfer, and access permissions. By leveraging secure communication protocols and advanced identity verification mechanisms, EDC ensures that only authorized entities can access shared data while maintaining compliance with legal and regulatory requirements.

A key feature of EDC is its compliance with the principles established by the International Data Spaces Association (IDSA)[1], which promotes secure and standardized data sharing across different organizations and industries. Furthermore, EDC aligns with the Dataspace Protocol, a specification that defines the handling of transactions in data ecosystems to foster interoperability and trust among stakeholders.

The framework's modular design allows for seamless integration with various deployment environments, including cloud-based, on-premises, and hybrid infrastructures. Its core functionalities encompass secure transfer, policy negotiation, contract enforcement, and identity management, making it a robust solution for building trusted data-sharing ecosystems.

EDC serves as a critical enabler for organizations seeking to participate in data spaces, ensuring structured and interoperable data exchange while safeguarding privacy and security. Its implementation in industry-wide initiatives lays the foundation for a scalable and collaborative approach to leveraging data across diverse domains.

2.1.2 EDC in HEDGE IoT

Within the HEDGE-IoT project, the Eclipse Dataspace Connector (EDC) serves as a cornerstone for enabling secure and interoperable data exchanges among stakeholders while ensuring compliance with data sovereignty principles. Given the project's emphasis on AI-driven services, edge-cloud integration, and interoperability, EDC serves as the key enabler for implementing a standardized and controlled data-sharing mechanism between IoT devices, cloud platforms, and external data sources.

HEDGE-IoT employs EDC to establish a federated data-sharing environment where participants retain full control over their data while allowing selective and policy-driven exchanges. This approach aligns with the project's need for a scalable and modular framework, allowing multiple organizations with distinct infrastructures and policies to securely share information without compromising ownership or confidentiality.

[1] https://docs.internationaldataspaces.org/ids-knowledgebase/idsa-rulebook/idsa-rulebook/2_guiding_principles

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Specifically, EDC is being integrated into the HEDGE-IoT architecture to manage data movement across various computational layers, from edge devices to centralized cloud infrastructures. It enforces well-defined access policies, contracts, and authentication mechanisms, in accordance with the principles established by the International Data Spaces Association (IDSA) and the Dataspace Protocol. This compliance guarantees that the HEDGE-IoT data-sharing framework adheres to industry standards while remaining adaptable to future advancements in data space technologies.

Moreover, EDC empowers HEDGE-IoT to establish a trusted ecosystem where AI-based services can efficiently access and process data in a decentralized manner. By providing standardized interfaces and integration capabilities, the connector ensures seamless interaction between different system components, enhancing the overall interoperability of the platform.

In the context of the project's initial release, EDC is being deployed as the central middleware component responsible for handling secure data transfers between a provider and a consumer. This first implementation focuses on establishing the fundamental capabilities of the connector, including policy negotiation, contract enforcement, and secure data exchange. Future iterations aim to expand its capabilities to include more complex integrations with additional partners and services, further strengthening the HEDGE-IoT interoperability framework.

2.1.3 Repository and handles

As part of the HEDGE-IoT project, the Eclipse Dataspace Connector (EDC) framework is being utilized to establish the interoperability layer. The EDC framework provides a modular and extensible approach to data exchange in trusted environments, adhering to the principles of the International Data Spaces Association (IDSA) and the Data Space Protocol (DSP).

The following repositories and handles are crucial for our implementation:

Main Repositories:

1) **HEDGE-IoT Repository:** All the code and transfer flows mentioned and described in this document can be found in the HEDGE-IoT/MVD repository
- GitLab Link: https://git.dstech.info/hedge-iot/mvd/-/tree/master

2) **Eclipse Dataspace Connector (EDC) Main Repository:** This repository contains the core framework and modules required to implement a compliant data space connector.
GitHub Link: https://github.com/eclipse-edc/Connector

3) **EDC Samples Repository:** This repository provides example implementations and reference configurations that serve as the foundation for our Minimum Viable Product (MVP) development.
- GitHub Link: https://github.com/eclipse-edc/Samples

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Handles Used in HEDGE-IoT:
Specific handles are employed to configure and manage the EDC-based data-sharing infrastructure, enabling data transfer, negotiation, and policy enforcement:

1) **Transfer Process Handles:** Responsible for overseeing the lifecycle of data transfer requests between providers and consumers. These handles ensure policy compliance and verify contract agreements before data exchange can occur.
2) **Catalogue and Contract Handles**: Facilitate the publication and discovery of data offers, allowing consumers to identify available datasets from providers. These handles support the negotiation of access conditions for each data transaction.
3) **Endpoint and API Handles:** Provide REST API endpoints that enable communication between various EDC instances. They support interactions such as contract negotiation, transfer initiation, and event monitoring.

Together, these repositories and handles form the technical backbone of the HEDGE-IoT data-sharing infrastructure, enabling secure, standardized, and scalable data transactions across multiple entities.

2.2 Technical Components

2.2.1 Transfer Layer (Negotiation, Consumer-pull, Provider-push, Event-consumer)

The Transfer Layer in the Eclipse Dataspace Connector (EDC) is central to facilitating secure, governed, and decentralized data exchanges. In the context of moder data space, data-sharing transcends simple transfer mechanisms, requiring structured negotiation, access control, and compliance mechanisms. These mechanisms ensure data sovereignty and enforceable agreements between participants. To achieve this, EDC follows a structured contract-based transfer model, which includes multiple phases:

1. **Negotiation Phase: Defining and Discovering Data Assets**

The negotiation process begins with data providers defining which assets they wish to share. Each data asset is registered within EDC along with its metadata, access control policies, and associated terms of use.
This process includes:

- **Asset Registration:** Provider registers data assets via an HTTP request to the EDC connector, specifying metadata such as data type, origin, and intended purpose.
- **Access Policy Definition:** Policies define under what conditions a consumer can request the asset, specifying constraints such as time-limited access, role-based permissions, or contractual obligations.
- **Contract Definition:** A contract template is created linking data assets with policies, ensuring that any access request complies with pre-established governance rules.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

On the consumer side, the participant browses the catalogue of available data assets through a request to the provider's connector, which returns a list of data offers that can be negotiated.

Before data can be exchanged, the Consumer must establish a contract with the Provider (see TABLE 1).

Figure 1, Figure 2 and Figure 3 illustrate the workflow of the negotiation phase.

TABLE 1 NEGOTIATION PHASE ENDPOINT

Type	***Path***	***Description***
POST	/catalog	The Consumer requests the available data assets.
POST	/contract-negotiations	Initiates contract negotiation based on available assets.
GET	/contract-negotiations/{id}	Polls the contract negotiation status.

Co-funded by the European Union

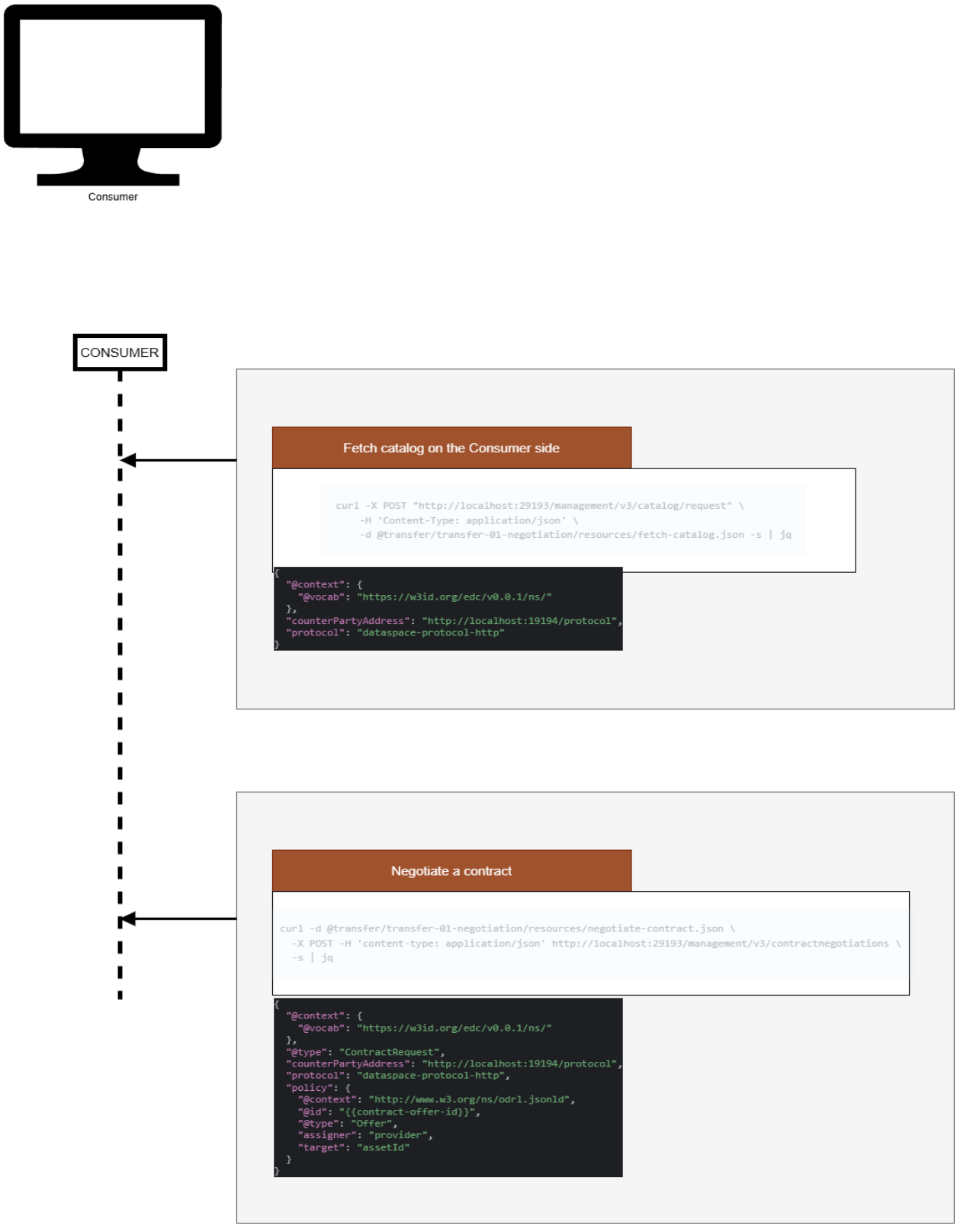
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

FIGURE 1 NEGOTIATION PHASE WORKFLOW_STEP1

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

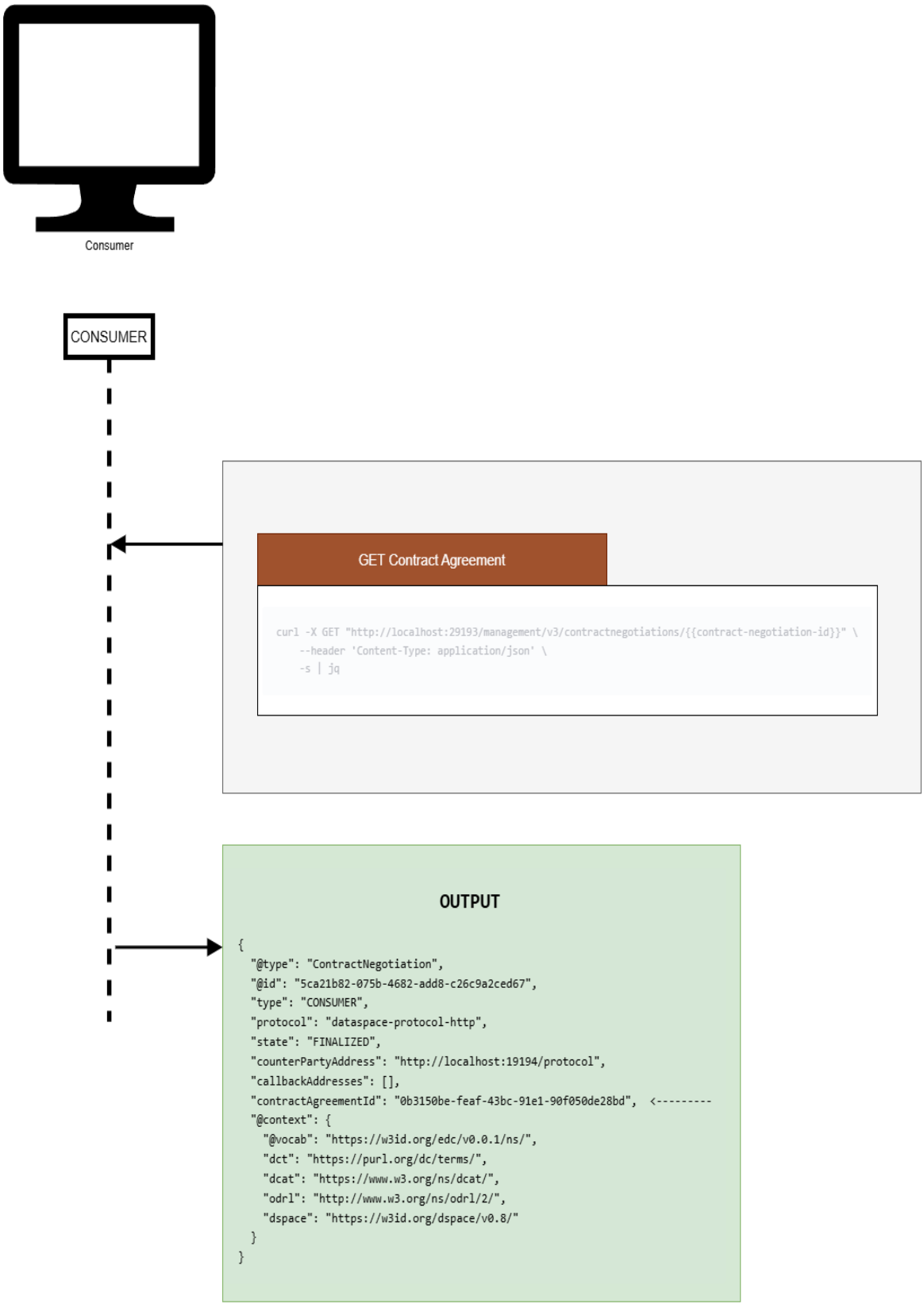
FIGURE 2 NEGOTATION PHASE WORKFLOW_STEP2



Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

FIGURE 3 NEGOTATION PHASE WORKFLOW_STEP3



Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

2. **Contract Agreement: Establishing Secure and Governed Data Exchange**

Once the consumer identifies an asset of interest, a contract negotiation process begins.

This follows a structured workflow:

1) The consumer submits a request to initiate a contract negotiation for a selected dataset.
2) The provider reviews and validates the request against its pre-defined policies.

If the request meets the provider's policies, a contract agreement is established between the two parties, which defines:

- Who has access to the data
- For how long data access is granted
- What data processing activities are permitted
- Any additional conditions (e.g., monetization models, compliance with GDPR regulations, etc.)

Once the agreement is finalized and signed digitally, data transfer can proceed under the established conditions.

Once the consumer identifies an asset of interest, a contract negotiation process begins (see Table 2)

TABLE 2 CONTRACT AGREEMENT ENDPOINT

Type	*Path*	*Description*
POST	/contract-negotiations	Requests a contract based on the selected asset.
GET	/contract-negotiations/{id}	Polls the contract negotiation status.
200 OK	Response	Returns the finalized contract once negotiation is complete.

3. **Data Transfer Execution: Multiple Models for Flexible Exchange**

EDC supports various transfer models, allowing providers and consumers to exchange data based on their infrastructure setup, security policies, and latency requirements.

The primary modes of data exchange include:

1) **Consumer Pull**: The consumer actively requests and retrieves data from the provider's storage. This model is typically used when consumers need data on-demand, allowing them to control when and how data is retrieved.

The consumer actively requests and retrieves data from the provider's storage (see Table 3). Figure 4, Figure 5 and Figure 6 illustrate the workflow of the consumer pull.

TABLE 3 CONSUMER PULL ENDPOINT

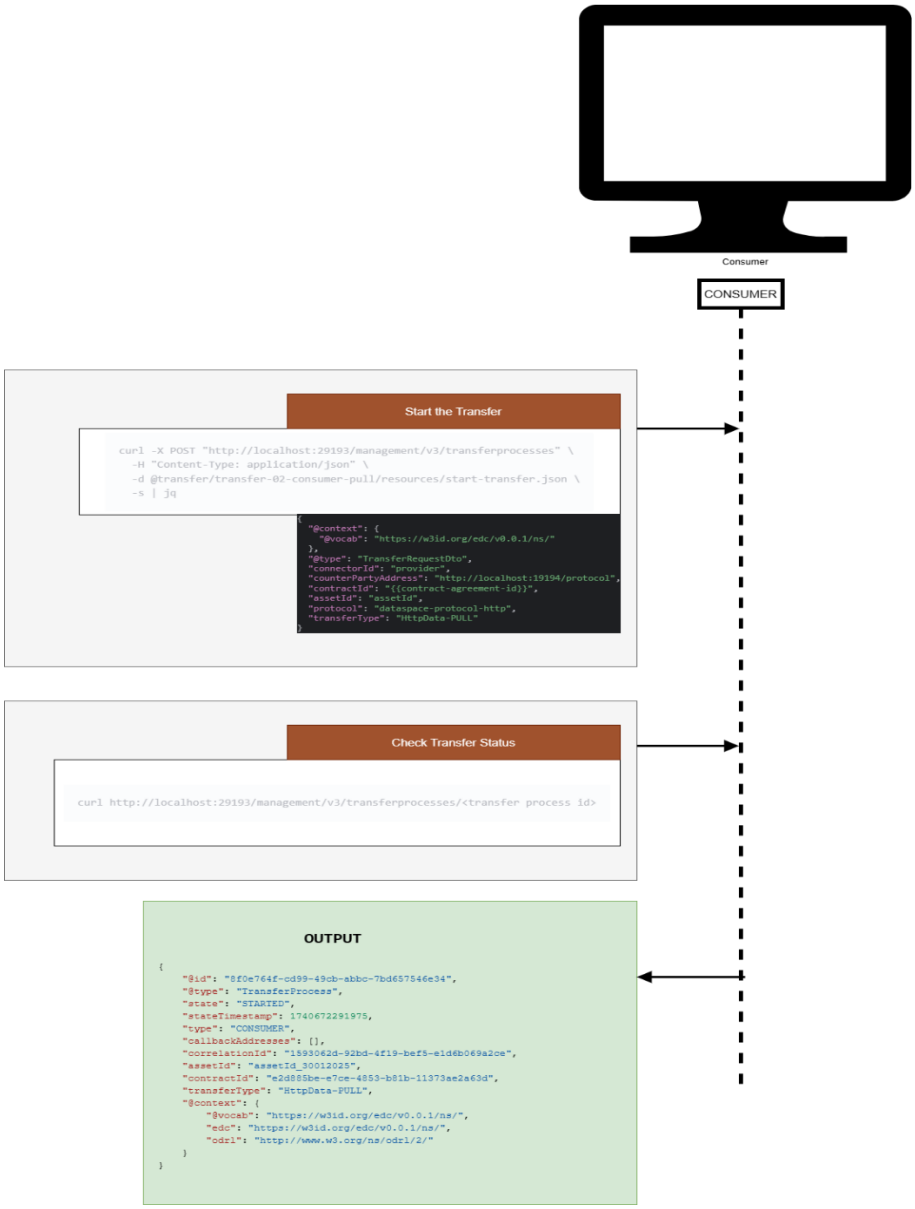
Type	*Path*	*Description*
GET	/catalog	Retrieves the list of available assets and contract definitions.
POST	/transfer-process	Requests data transfer using the contract agreement ID.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

GET	/transfer-process/{id}	Polls the status of the transfer process.
GET	/data	The Consumer retrieves data from the Provider.

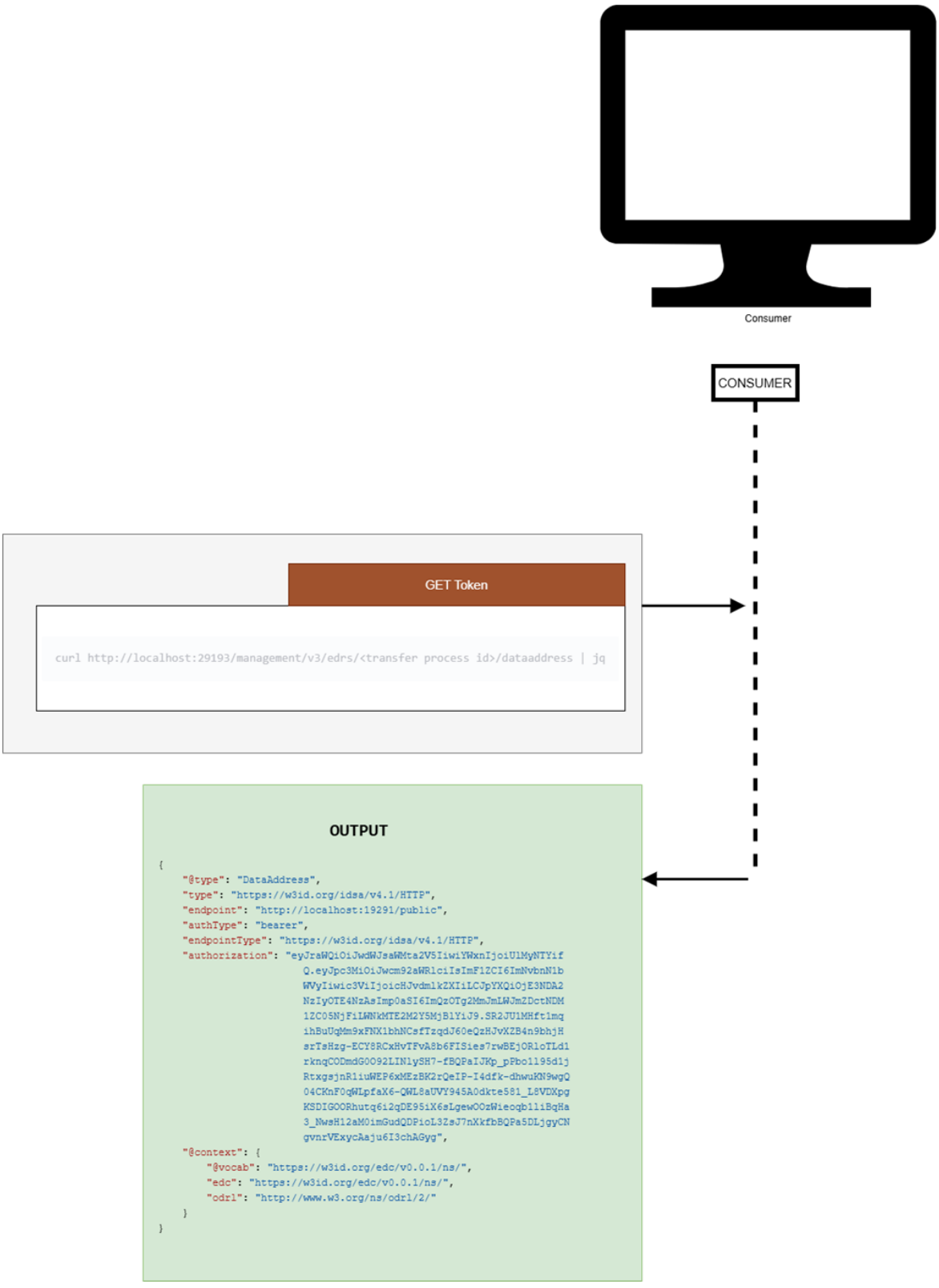
FIGURE 4 CONSUMER PULL WORKFLOW_STEP1



Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

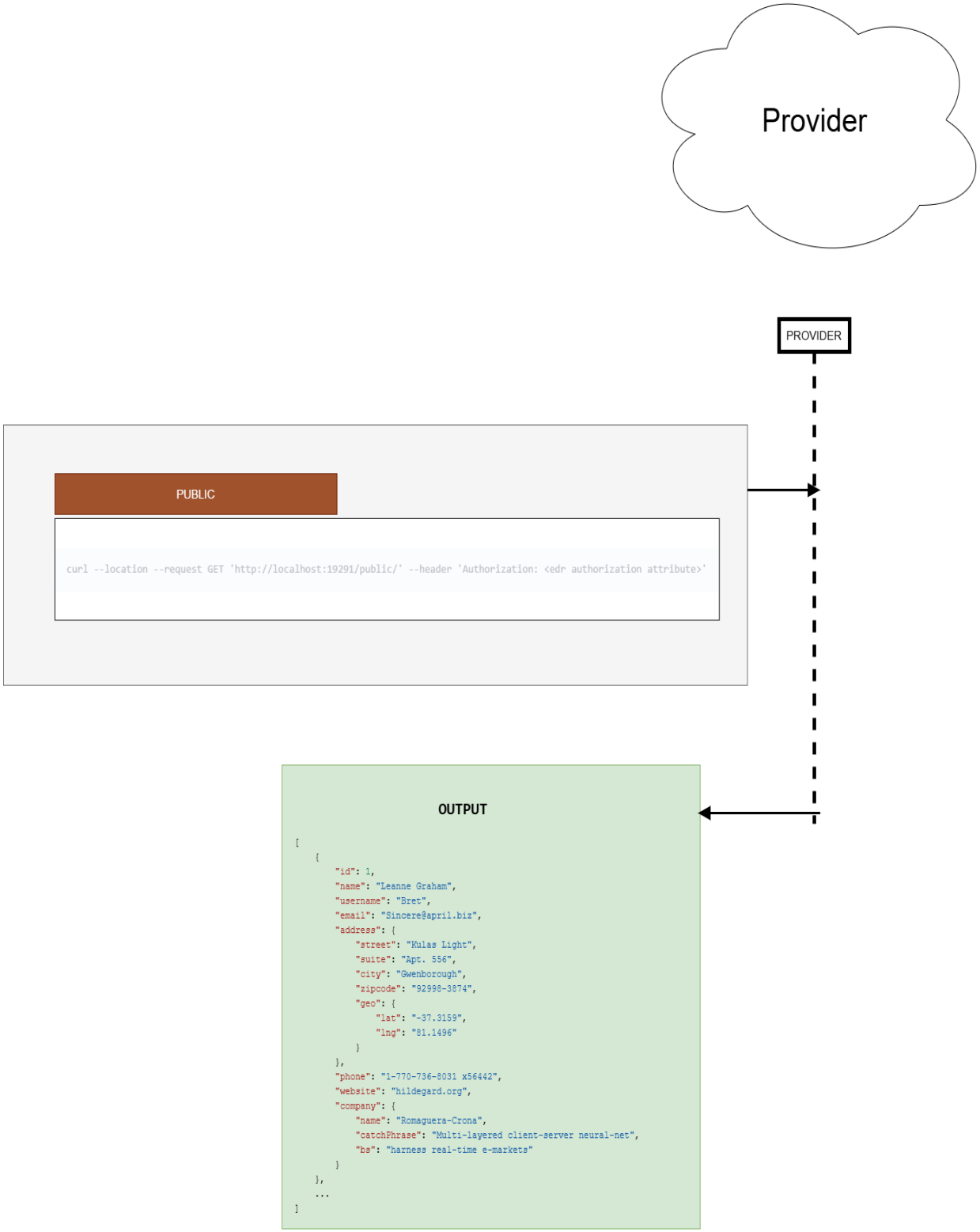
FIGURE 5 CONSUMER PULL WORKFLOW_STEP2



Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

FIGURE 6 CONSUMER PULL WORKFLOW_STEP3



Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

2) **Provider Push**: The provider proactively sends data to the consumer's designated endpoint. This approach is useful for real-time streaming applications where data updates must be pushed immediately.

The provider proactively sends data to the consumer's designated endpoint. (see Table 4)

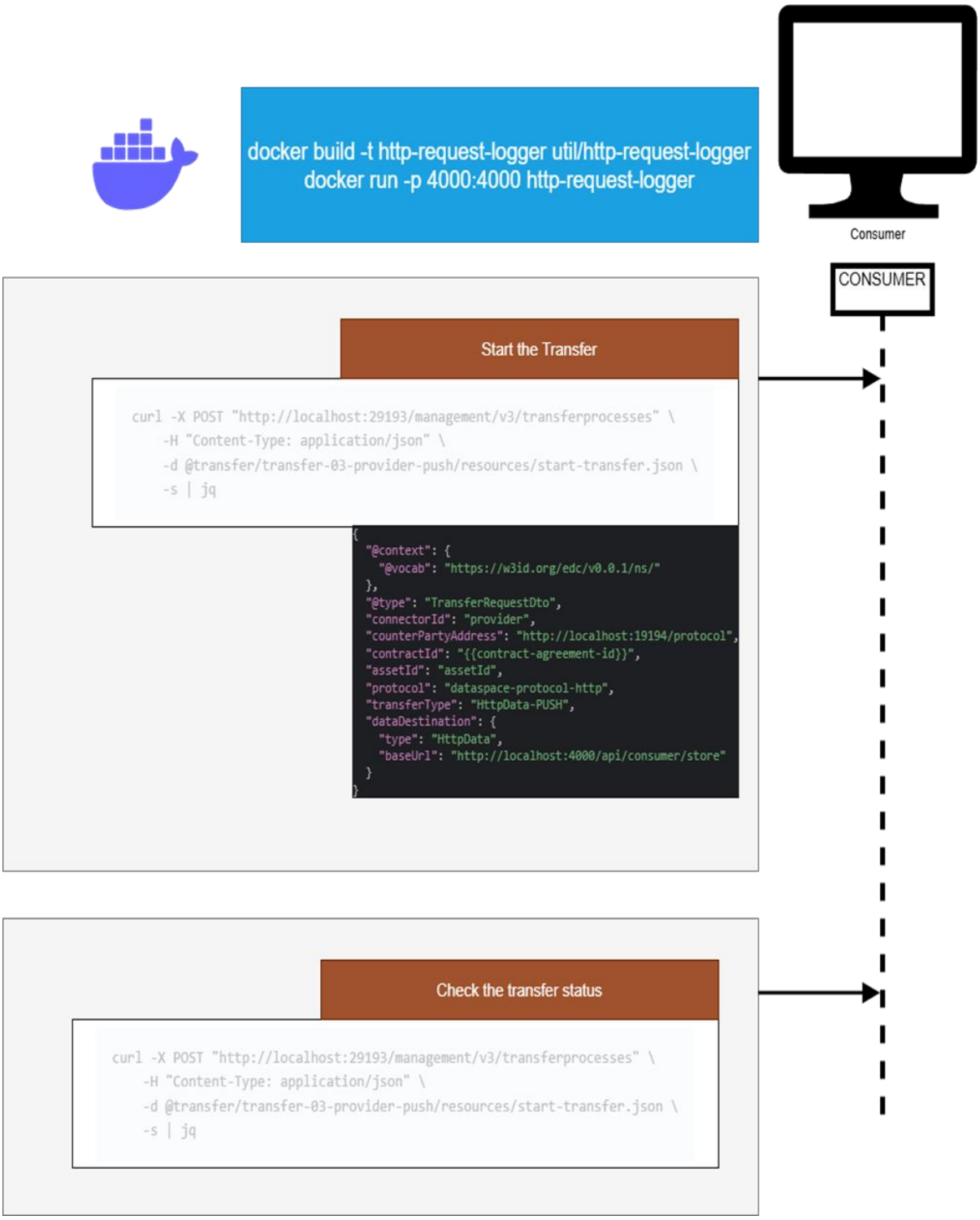
TABLE 4 PROVIDER PUSH ENDPOINT

Type	*Path*	*Description*
POST	/transfer-process	Requests a data transfer using the contract agreement ID.
GET	/transfer-process/{id}	Polls the status of the transfer process.
POST	/data	The Provider sends data to the Consumer's HTTP endpoint.
200 OK	Response	The Consumer acknowledges receipt of the data.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

FIGURE 7 PROVIDER PUSH WORKFLOW

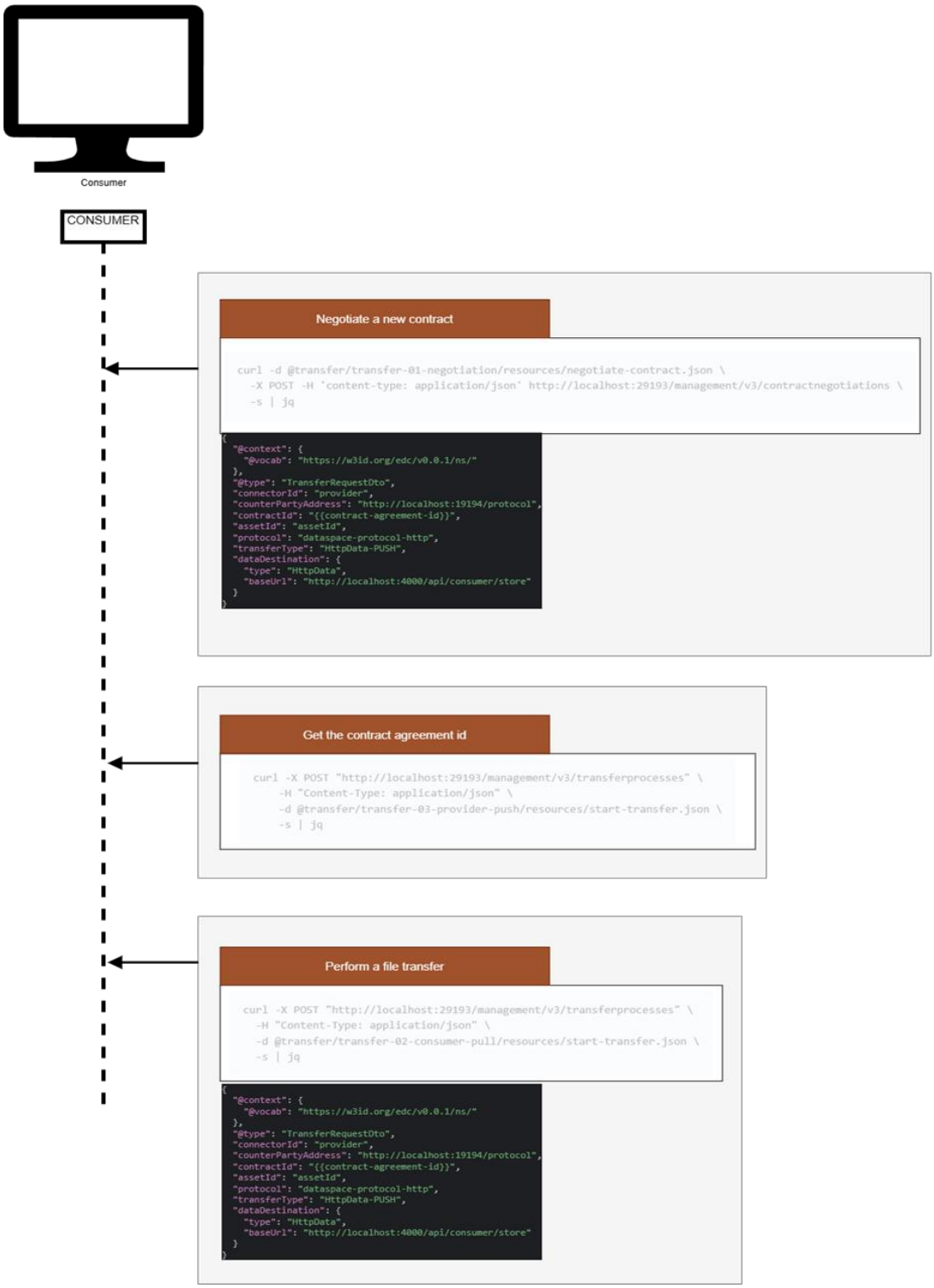


Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

3) **Event-Based Transfer:** Consumers subscribe to event notifications triggered by the provider, allowing them to receive data whenever specific conditions occur (e.g., new data availability). Figure 8 illustrates the workflow of the event-based transfer.

FIGURE 8 EVENT BASE TRANSFER WORKFLOW



Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

4) **Cloud-to-Cloud Transfer:** EDC can facilitate direct data movement between cloud storage solutions (e.g., Azure to AWS), ensuring secure, policy-compliant cross-cloud transfers.

Each transfer mode is secured using authentication mechanisms, encryption protocols, and compliance checks, ensuring that data movement is traceable, verifiable, and aligned with regulatory requirements.

EDC facilitates direct data movement between cloud storage solutions (e.g., Azure to AWS). (see Table 5)

TABLE 5 CLOUD-TO-CLOUD TRANSFER ENDPOINT

Type	*Path*	*Description*
POST	/assets	Registers an asset representing a file stored in Azurite.
POST	/transfer-process	Requests data transfer using the contract agreement ID.
GET	/transfer-process/{id}	Polls the status of the transfer process.
GET	/blob/{filename}	Fetches the file from the Azure Blob Storage emulator.
PUT	/minio/{bucket}/{filename}	Writes the file to the S3-compatible MinIO storage.

5) **Integrity and Compliance Checks: Ensuring Data Trustworthiness**

To ensure that transferred data remains secure, unaltered, and compliant, EDC implements several integrity measures, including:

- **End-to-End Encryption:** Protecting data in transit through secure TLS connections, preventing unauthorized access.
- **Data Provenance and Logging:** Tracking the entire transfer history to maintain an audit trail of data movements.
- **Policy Enforcement at Runtime:** Before data is shared, EDC dynamically validates access conditions to ensure compliance with the agreed terms.
- **Integration with Cybersecurity Frameworks:** EDC supports security extensions, including HashiCorp Vault for credential management and ETSI SAREF-based semantic models for context-aware security.

These security controls align with data sovereignty principles, ensuring that organizations retain control over who accesses their data, under what conditions, and for what purposes.

EDC Transfer Layer within HEDGE-IoT: Enabling Interoperability and Secure IoT Data Sharing

In the context of the HEDGE-IoT project, the EDC Transfer Layer is a key enabler of secure interoperability between IoT-Edge and Cloud-based services.

The project leverages decentralized data-sharing to achieve:

- Real-time data exchange between IoT devices, cloud platforms, and AI-driven applications.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- Policy-driven data governance, ensuring that IoT-generated data adheres to sovereignty principles.
- Standardized data-sharing mechanisms, compliant with IDSA and Dataspace Protocol standards to enable cross-organization collaboration.

EDC acts as a trusted intermediary, allowing different stakeholders, services, and devices to share data while ensuring that privacy, compliance, and security are preserved. This is particularly relevant in smart grid applications, predictive maintenance, and AI-powered IoT analytics, where sensitive operational data must be securely exchanged across diverse infrastructures.
Through the integration of EDC's Transfer Layer, HEDGE-IoT ensures a scalable, auditable, and policy-compliant data-sharing infrastructure, paving the way for a trusted and efficient IoT data economy.

2.3 MVP Description

As part of the first release of the HEDGE-IoT interoperability framework, a Minimum Viable Product (MVP) is being developed to establish a foundational mechanism for data exchange within the project. The MVP leverages the Eclipse Dataspace Connector (EDC) Minimum Viable Dataspace (MVD) repository, which offers a pre-configured environment for setting up secure and governed data-sharing infrastructures. By using MVD, the project adopts a standardized approach to ensure that data transactions between providers and consumers are both reliable and policy driven.

MVD is designed as a lightweight, modular framework that streamlines the deployment of data-sharing components. Its predefined configurations and integration patterns enable organizations to quickly establish functional data-sharing environments without the need for extensive customization.

1. **Predefined Connector Configurations**: MVD provides ready-to-use configurations for deploying consumer and provider connectors, reducing setup complexity and allowing seamless integration between different entities.
2. **Built-in Data Cataloguing and Asset Management:** The system includes data asset registration and discovery functionalities, enabling providers to expose their available datasets while allowing consumers to browse and request access to them.
3. **Contract-Based Data Exchange**: Before any data is shared, a structured contract negotiation takes place. Providers define access conditions, and consumers request and agree to the specified terms. This ensures that all transactions are transparent and regulated.
4. **Multiple Data Transfer Mechanisms**: MVD supports various transfer models, including consumer pull, provider push, and event-driven exchanges, allowing flexible adaptation to various use cases and infrastructure requirements.

For the HEDGE-IoT MVP, the focus has been on implementing the transfer layer within the MVD framework. This includes setting up contract negotiation mechanisms, policy enforcement layers, and data transport components to enable seamless interaction between data providers and

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

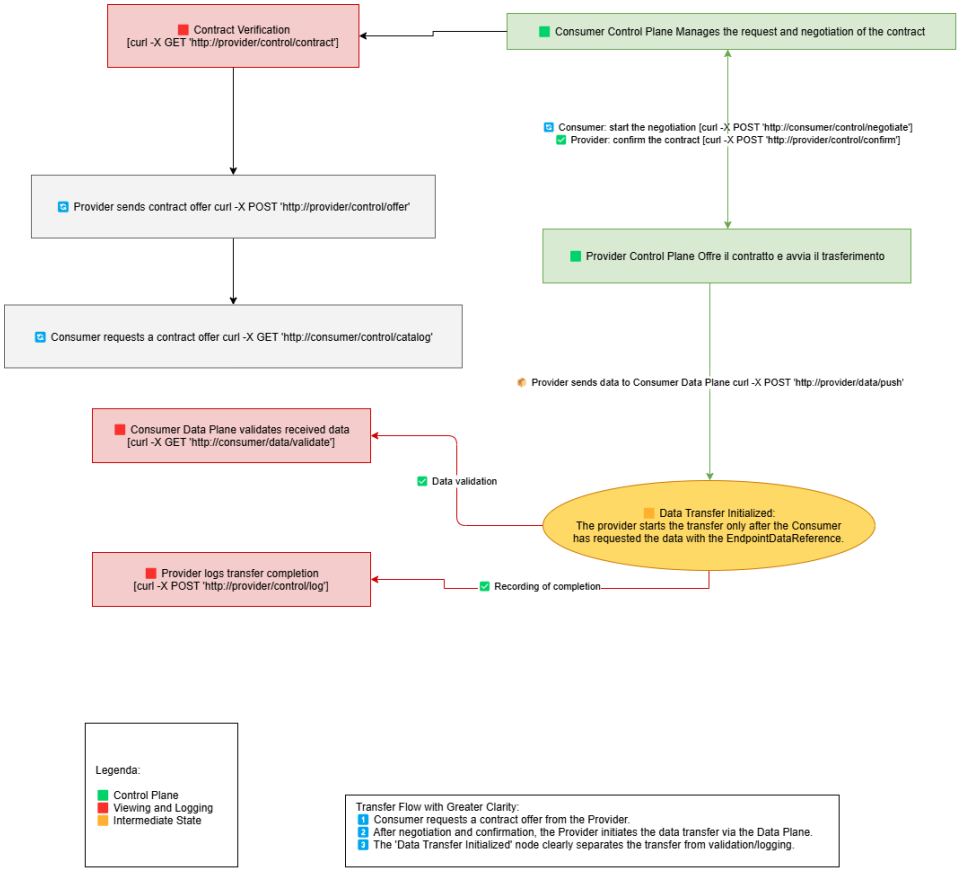
consumers. By leveraging MVD, the project benefits from a robust and well-defined architecture that can be expanded and integrated with additional components over time.

The MVP will serve as a testbed for refining data-sharing processes and enhancing interoperability among IoT, cloud, and AI-driven services within HEDGE-IoT. Planned enhancements include:

- Extending MVD functionalities to support more complex data-sharing scenarios.
- Integrating advanced security features to meet evolving compliance requirements.
- Aligning the framework with the broader interoperability goals of the project.

By building on the structured foundation provided by MVD, HEDGE-IoT aims to create a scalable and secure data-sharing ecosystem that accelerates innovation across IoT and AI domains. FIGURE 9 illustrates the overall MVP workflow.

FIGURE 9 MVP OVERALL WORKFLOW



Co-funded by the European Union

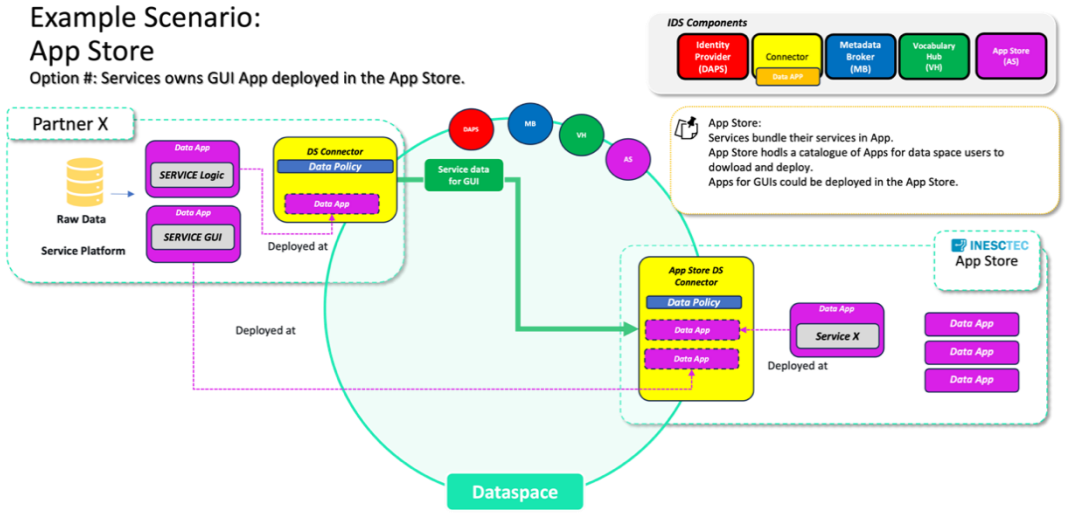
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

3 OPEN SERVICES CATALOGUE AND APP STORE

3.1 Component description and IDS alignment

The App Store integrates into the IDSA ecosystem as one of its main building blocks. It interfaces with the IDS Connector and enables Data Apps to be distributed within the data space. Data Apps are reusable applications that are used to process or transform data before or after the data is exchanged. Users access the App Store to browse the available Apps and verify their requirements/ functionalities before downloading them. When users download Data Apps, these are instantiated in the user's IDS Connector instance. Users also acess the App Store to publish their own Data Apps so they can be used by other users. Moreover, users use the App Store to fast prototype new Data Apps, focusing on the business-related data acquisition or data transformations, while ensuring key data acquisition and integration with the IDS connector environment is taken care of.

FIGURE 10 IDS APP STORE POSITIONING TOWARDS DATA SPACE COMPONENTS



3.2 App Store and the EDC connector

The HEDGE-IoT App Store builds on a former version in which data apps are isolated applications running in OCI containers. Each of these containers held a fully-fledged application that exposed its own API, which gets detected by the core container architecture, establishing the necessary links to make authentication, authorization and all remaining connector interactions work, namely: publishing data assets, requesting usage certificates and requesting data exchange in scope of a given connector.

The new data space protocol migrates connector implementations to strictly separate control and data operations in two separate stages, among other changes. Dataspace connectors adopting the vision of the new protocol establish two key planes: the control plane and the data plane. The control plane handles asset publication, the establishment of data usage policies (including custom ones

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

defined by organizations) and manages authorization and authentication of contract request procedures. The data plane oversees implementation of specific data sync operations, to integrate with several data sources. Thus, the data plane can be viewed as a driver or custom client that enables a connector to interface with ODBC databases, S3 cloud storage, specific communication protocols or data storage software.
The App Store architecture evolves to abide by the usage of the newer generation of dataspace connectors, using the new data space protocol and thus having a control and data plane architecture. In this case, data apps are shaped as client software, bundled too as an OCI compliant container, holding client code that reaches for the connector's control plane administration API and a custom (if needed) data plane installation that interfaces with organizations' data and makes it available in the wider data space. Moreover, specific data usage policies may also be embedded in the software container and loaded during the app's booting process to make it available in the data space.

3.3 Reference Architecture and Functional Specifications

3.3.1 Actors

The HEDGE IoT App Store design shapes a web-based application that will embody the identified functionalities. The concept includes 6 key actors, as depicted in TABLE 6

TABLE 6 APP STORE SYSTEM ACTORS

Actors		
Actor Name	***Actor Type***	***Actor Description***
App Store	System	App Store Backend System
App Store Frontend	System	App Store Frontend System
IDS Connector	System	IDS compliance connector (integrated as part of Backend)
User	People	The user that interacts with the App Store
Identity Provider	System	Provided and verifier of identity within the data space
Container Registry	System	System that holds App containers available in the App Store.

Each system actor plays a specific role in fulfilling a set of scenarios, covering the required actions, what triggers them to accomplish the functionalities identified and what are the expected results/outputs, being the result of processing data or a trigger to other functionalities.

3.3.2 Scenarios and Diagrams

The following tables summarize the key characteristics for each scenario, namely the event sequence number, the name and description of the event and the related actors. The scenarios covered include:

- The Boot process of the App Store, TABLE 7
- Publishing a data app, TABLE 8
- Browse and retrieve data apps, TABLE 9

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

TABLE 7 *APP STORE BOOT PROCESS SCENARIO*

Scenario name: Boot process					
Step No.	**Event**	**Name of process/ activity**	**Description of process/ activity**	**Information producer (actor)**	**Information receiver (actor)**
1.1	App Store Boots	App Store boots	The App store process starts and relays to the container registry and underlying IDS connector to also boot.	App Store	Container Registry, IDS connector
1.2	App Store request identity certificate	Collect Identity Certificate	The App Store requests an identity certificate from the Identity provider.	App Store	Identity Provider
1.3	Identity Provider assigns certificate in the App Store	Provide Identity Certificate	The identity Provider validates the identity request and assigns identity certificate.	Identity provider	App Store

TABLE 8 *APP STORE PUBLISH DATA APPS SCENARIO*

Scenario name: Publish Data Apps					
Step No.	**Event**	**Name of process/ activity**	**Description of process/ activity**	**Information producer (actor)**	**Information receiver (actor)**
2.1	Send App Container Image	Push App Container to App Store	The IDS connector pushes the app container image to the app store container registry.	IDS Connector	App Store
2.2	Send App Metadata	Send App Metadata to App Store	The IDS Connector sends app metadata to the app store,	IDS Connector	App Store
2.3	Process and store app metadata	Process and store app metadata	The App Store receives and processed app metadata	AppStore	AppStore
2.4	Create app record	Create App record in App Store	An App record is created in the App Store	AppStore	AppStore
2.5	Add app container image to registry	Process and add app container image	The app container image is processed and added to the app store container registry	AppStore	AppStore
2.6	Push app container image	Push container image	The Data App container is pushed to the container registry	AppStore	Container Registry

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

			and is validates.		

TABLE 9 *APP STORE BROWSE AND RETRIEVE DATA APPS SCENARIO*

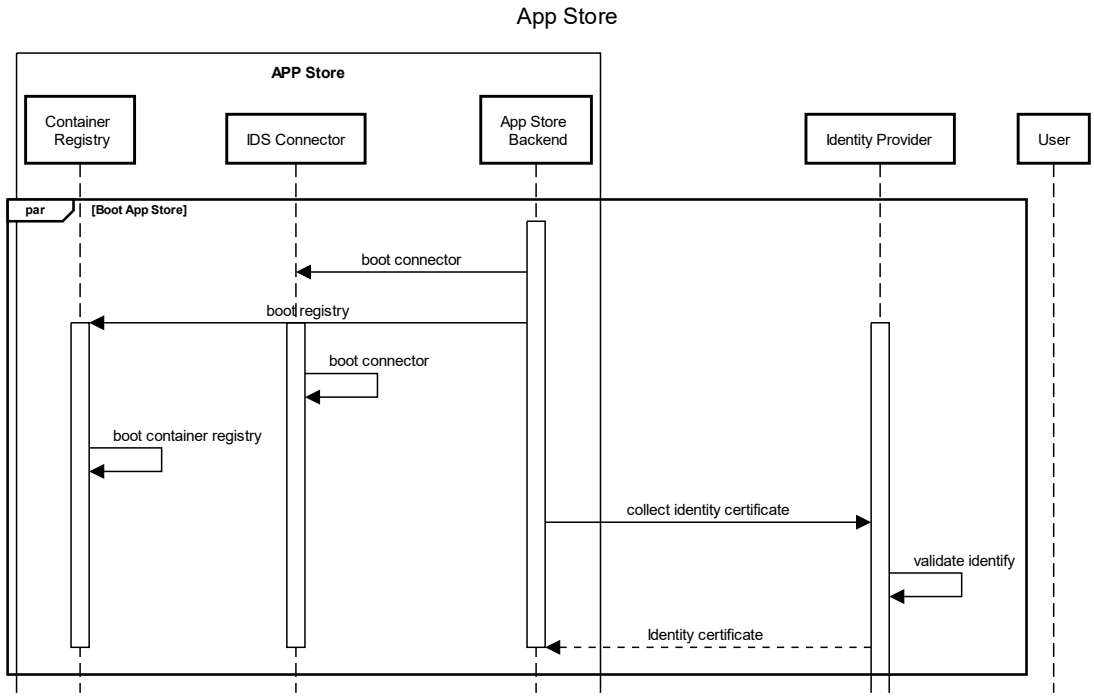
Scenario name: Browse and Retrieve Data Apps					
Step No.	**Event**	**Name of process/ activity**	**Description of process/ activity**	**Information producer (actor)**	**Information receiver (actor)**
3.1	User searches app	Search Apps	The User navigates the App store UI and searches for the intended Data App	App Store	User
3.2	App Store request App Metadata	Query App list	The App Store frontend reaches for its backend to search for app metadata.	App Store	App Store
3.3	Request for app metadata	Request images Metadata	The App Store contacts its container registry of data apps to request metadata about Data Apps	Container Registry	App Store
3.4	Validate App Metadata	Verify App Containers	The container registry verifies the validity of Data Apps, including those that are certified and those that are not certified.	Container Registry	Container Registry
3.5	Data App is selected for download	Select Data App	A specific Data App is marked for download.	App Store	User
3.6	Data App is selected for download	Select Data App	A specific Data App is marked for download.	App Store	App Store
3.7	Data App is selected for download	Request Data App	A given data app container is found and selected for download	Registry	App Store
3.8	Data App is set for validation	Validate Data App	Before provisioning, a Data App is validated.	Registry	Registry
3.9	Data App is set for collection	Collect Data App	Data Container is retrieved from registry	Registry	Registry

The detailed scenarios shape the overall diagram of all interactions that make up the App Store system. These are depicted in FIGURE 11 and FIGURE 12.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

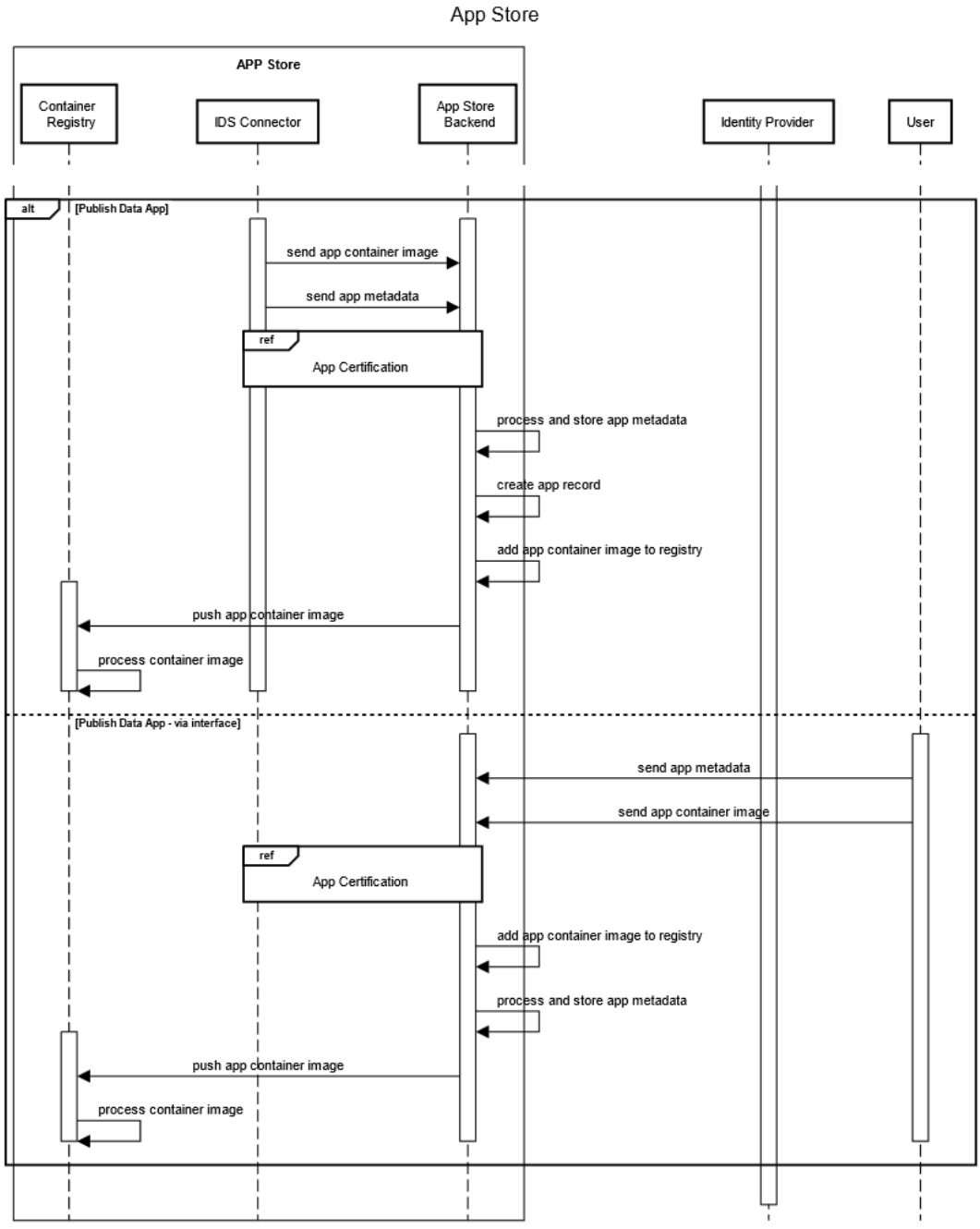
FIGURE 11 APP STORE BOOT PROCESS SEQUENCE DIAGRAM



Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

FIGURE 12 APP STORE PUBLISH DATA PROCESS SEQUENCE DIAGRAM

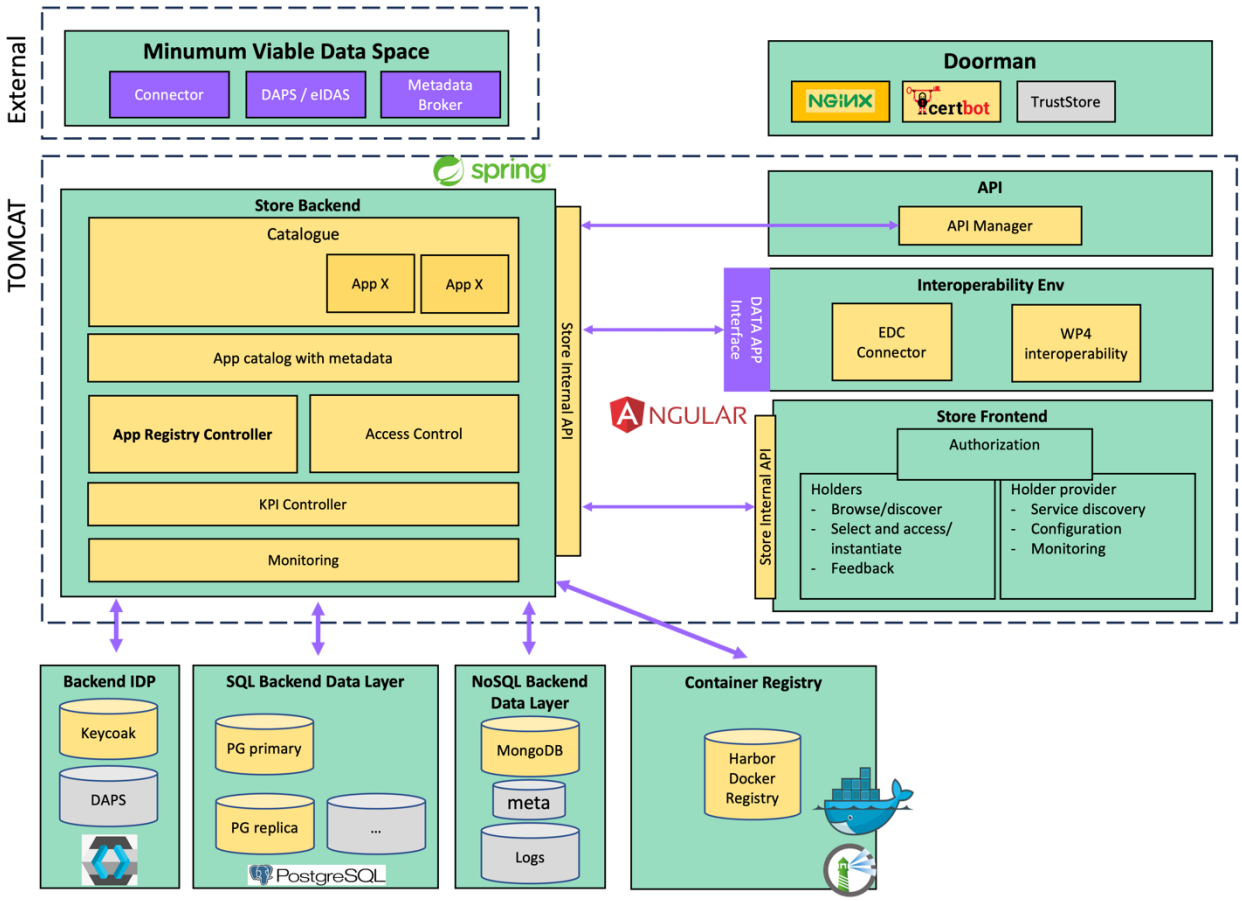


3.3.3 App Store Architecture

The architecture of the App Store is depicted in FIGURE 12. It is split into two sub-components, the App Store Backend and the App Store Frontend. As a web-based application, the App Store architecture follows a Model-View-Controller design pattern where the Model and Controller dimensions are in scope of the backend sub-component, while the View dimensions are in scope of the frontend sub-component.

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

FIGURE 13 APP STORE ARCHITECTURE



The App Store backend departs from an IDS compliant connector, providing the key integration with a data space instantiation. The embedded connector will link with identity provisioning of the App Store itself, also taking part in the identity validation for all other interactions with foreign data connectors.

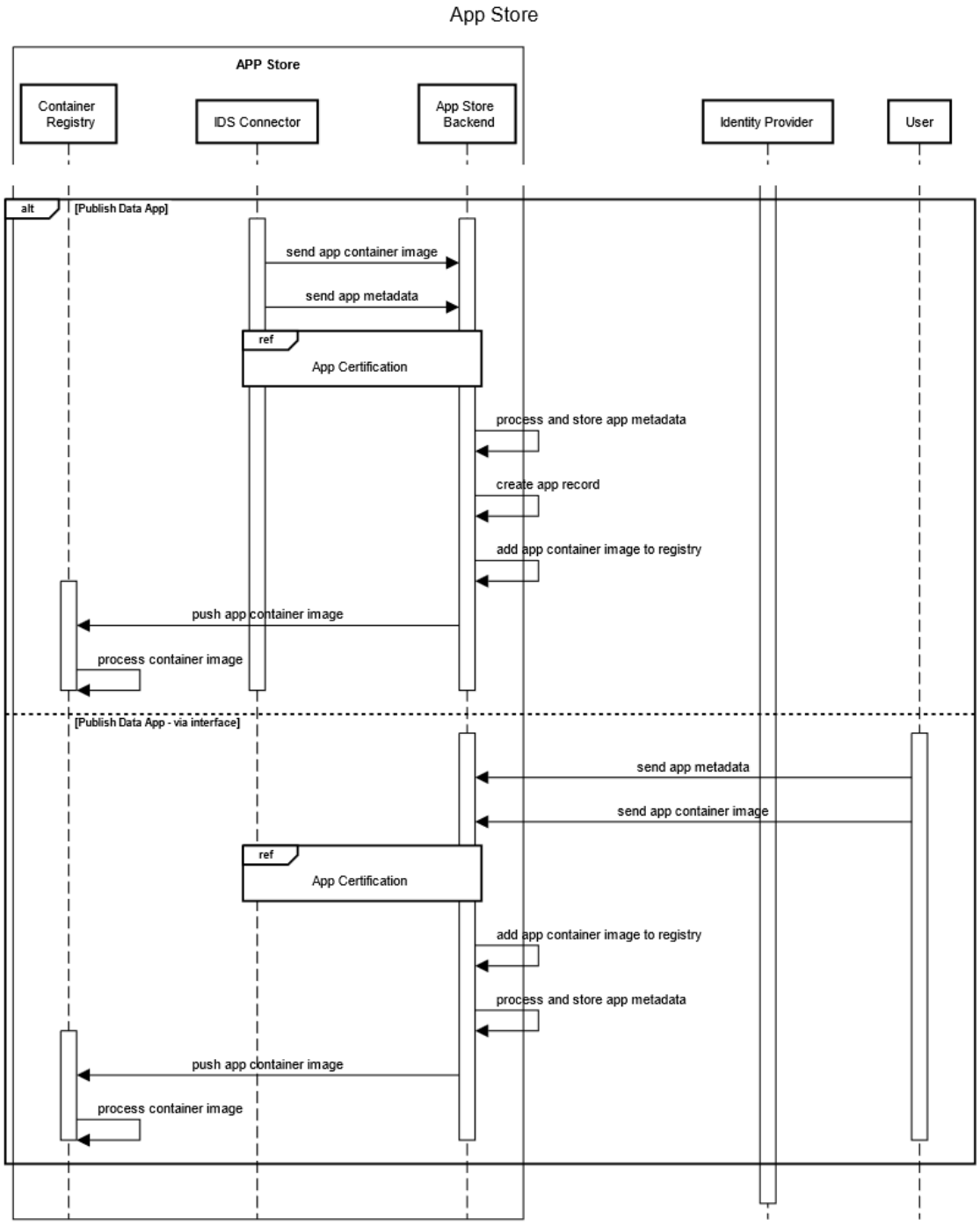
As a catalogue of available Apps, the App Store includes an App registry module, holding container images of apps as assembled by their owners. The registry only links with the App Store backend system that forwards it to the data connector interface. Metadata from app descriptions is currently handled by the App Store internal data model as a support for the application development. The next release will move forward and consider the use of the metadata broker to support management and querying data assets. The next release will also consider the Clearing House as a complement to assist the process where a payment is considered to unlock the transfer process of a data app. Finally, other modules assist the workflow of using the App Store, such as the monitoring module that records operations or the access control module that links with the DAPS system of the data space.

The frontend sub-component provides user interfaces to browse the catalogue of apps, upload and download apps. Moreover, it also assists the process of uploading app metadata (key for searching apps).

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

FIGURE 14 APP STORE PUBLISH DATA PROCESS SEQUENCE DIAGRAM



3.3.4 Component Diagram

The App Store component view is composed of several modules as depicted in FIGURE 15- A summary for each module is provided in TABLE 10.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

FIGURE 15 IDS APP STORE COMPONENT VIEW

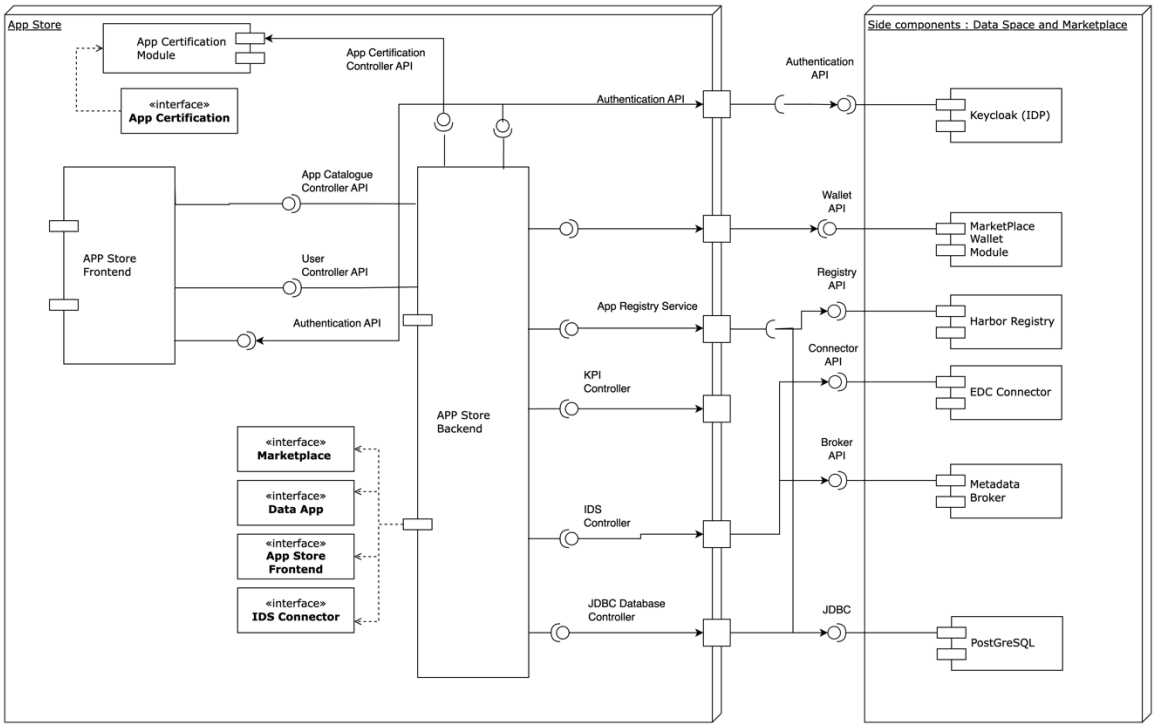


TABLE 10 *APP STORE COMPONENT DETAIL*

Component Detail	
Module Name	**Detail**
App Store Backend	Includes all the sub-modules that expose the identified interfaces and embody the business logic for managing data apps.
App Store Frontend	Includes a single page application all the view needed to export the information exported by the App Store Backend.
App Certification	Includes all the functionalities and exports a certification API to be adopted by an entity that certifies data apps.
Dynamic Attribute Provisioning Service (DAPS)	External module that handles identities in the IDS Dataspace (for connectors and organisations)
Keycloak	Standard, open-source Identity provider system
EDC Connector	Dataspace Compliant Connector from EDC distribution.
Broker	Dataspace Metadata Broker needed to instantiate a Dataspace.
Docker Registry	External Registry for the App Images, rendered a OCI container Images.
PostGreSQL	Relational Database Management System for operational purposes.

3.4 App Store API

The App Store integrates into the IDS ecosystem as one of the building blocks. It interfaces with the IDS Connector and enables Data Apps to be distributed within the data space. Data Apps are

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

reusable applications that are used to process or transform data before or after the data is exchanged. Users consider the App Store to browse the available Apps, verifying their requirements/ functionalities before downloading them. When users download Data Apps, they are instantiated in the user's IDS Connector instance. Users also consider the App Store to publish their own Data Apps so they can be used by other users. These apps focus on business-related data acquisition or data transformations, while ensuring key data acquisition and integration with the IDS connector environment is taken care of. TABLE 11 introduces the component identity card.

TABLE 11 IDENTITY CARD COMPONENTS_STEP1

IDS App Store		
Framework Sub-System	Interoperable components	
Responsibility	Distribute IDS Apps (Push and Pull), App Catalogue, Manage APP KPIs	
Required Interface	**Docker Registry Controller**	
	Pull App Docker Image	
	Description	Pulls one image from the docker registry
	Provided to	IDS App Store Frontend, Connector Controller
	End-point	/api/{vX}/app/images
	Protocol used	HTTP
	Allowed Methods	GET
	Push App Docker Image	
	Description	Pushes one image to the docker registry
	Provided to	IDS App Store Frontend, Connector Controller
	End-point	/api/{vX}/app/images
	Protocol used	HTTP
	Allowed Methods	PUT
	App Container Controller	
	Download App	
	Description	Downloads one app from the App Store container registry
	Provided to	App store frontend, IDS Connector
	End-point	/api/{vX}/app/image/{imageId}
	Protocol used	HTTP
	Allowed Methods	GET
	Get Apps	
	Description	Returns all apps available.
	Provided to	App store frontend
	End-point	/api/{vX}/app/all
	Protocol used	HTTP
	Allowed Methods	GET
	Get App Metadata	
	Description	Returns metadata for one specific app
	Provided to	App store frontend
	End-point	/api/{vX}/app/{appId}/metadata
	Protocol used	HTTP
	Allowed Methods	GET

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

TABLE 12 IDENTITY CARD COMPONENTS_STEP2

IDS App Store		
Framework Sub-System	Interoperable components	
Responsibility	Distribute IDS Apps (Push and Pull), App Catalogue, Manage APP KPIs	
	Toggle App Visibility	
	Description	Toggles the current visibility for this app.
	Provided to	App store frontend
	End-point	/api/{vX}/app/{appId}/toggleVisibility
	Protocol used	HTTP
	Allowed Methods	POST
	Edit app metadata	
	Description	Edit details for this app
	Provided to	App store frontend
	End-point	/api/{vX}/app/{appId}/edit
	Protocol used	HTTP
	Allowed Methods	POST
	Create App	
	Description	Create a record for a new App
	Provided to	App store frontend
	End-point	/api/{vX}/app/
	Protocol used	HTTP
	Allowed Methods	PUT
	Get My Apps	
	Description	Get Apps for the active user.
	Provided to	App store frontend
	End-point	/api/{vX}/app/
	Protocol used	HTTP
	Allowed Methods	GET
	Delete App	
	Description	Remove one App and all its images
	Provided to	App store frontend
	End-point	/api/{vX}/app/{appId}
	Protocol used	HTTP
	Allowed Methods	DELETE
	Delete App Image	
	Description	Delete one specific Image from an App
	Provided to	App store frontend
	End-point	/api/{vX}/app/{appId}/image/{imageId}
	Protocol used	HTTP
	Allowed Methods	DELETE

TABLE 13 IDENTITY CARD COMPONENTS_STEP3

IDS App Store		
Framework Sub-System	Interoperable components	
Responsibility	Distribute IDS Apps (Push and Pull), App Catalogue, Manage APP KPIs	
	Authentication Controller	
	User Login	
	Description	Allows a user to enter the service
	Provided to	App store frontend
	End-point	/api/{vX}/users/login

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

	Protocol used	HTTP
	Allowed Methods	POST
	User Verification	
	Description	Verifies recently created accounts.
	Provided to	App store frontend
	End-point	/api/{vX}/users/verification
	Protocol used	HTTP
	Allowed Methods	POST
	Forgot Password	
	Description	Allows the user the claim a new password
	Provided to	App store frontend
	End-point	/api/{vX}/users/forgot-password
	Protocol used	HTTP
	Allowed Methods	POST
	Reset Password	
	Description	Allows a user to enter a new password after claiming it as forgotten
	Provided to	App store frontend
	End-point	/api/{vX}/users/reset-password
	Protocol used	HTTP
	Allowed Methods	POST
	Change Password	
	Description	Allows the use to change its current password
	Provided to	App store frontend
	End-point	/api/{vX}/users/change-password
	Protocol used	HTTP
	Allowed Methods	POST
	Get User	
	Description	Retrieves the user profile details from one user.
	Provided to	App store frontend
	End-point	/api/{vX}/users/{userId}
	Protocol used	HTTP
	Allowed Methods	POST
	SignUp	
	Description	Creates one account for one user.
	Provided to	App store frontend
	End-point	/api/{vX}/users/signup
	Protocol used	HTTP
	Allowed Methods	POST
	Notification Controller	
	Create Notification	
	Description	Create a new notification
	Provided to	App store frontend
	End-point	/api/{vX}/notification
	Protocol used	HTTP
	Allowed Methods	PUT
	Get Notifications	
	Description	Retrieves all notifications
	Provided to	App store frontend
	End-point	/api/{vX}/notification/all
	Protocol used	HTTP
	Allowed Methods	GET

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

TABLE 14 IDENTITY CARD COMPONENTS_STEP4

IDS App Store		
Framework Sub-System	Interoperable components	
Responsibility	Distribute IDS Apps (Push and Pull), App Catalogue, Manage APP KPIs	
	Get Notification	
	Description	Retrieves one notification
	Provided to	App store frontend
	End-point	/api/{vX}/notification/{notificationId}
	Protocol used	HTTP
	Allowed Methods	GET
	Delete Notification	
	Description	Removes one notification
	Provided to	App store frontend
	End-point	/api/{vX}/notification/{notificationId}
	Protocol used	HTTP
	Allowed Methods	DELETE
	Mark Notification as Read	
	Description	Toggle status of notification from read/unread
	Provided to	App store frontend
	End-point	/api/{vX}/notification/{notificationId}/toggleRead
	Protocol used	HTTP
	Allowed Methods	POST
	GetConnectors	
	Provided by	Metadata broker
	Description	Transfers information about all available connectors.
	Pull Docker Image	
	Provided by	Docker-Registry
	Description	Pulls an OCI image on an App

TABLE 15 Identity Card Components_Step5

IDS App Store		
Framework Sub-System	Interoperable components	
Responsibility	Distribute IDS Apps (Push and Pull), App Catalogue, Manage APP KPIs	
	KPI Controller	
	Get all App KPIs (download metrics, upload metrics and releases)	
	Description	Retrieves the list with all KPIs
	Provided to	App Store Frontend
	End-point	/api/{vX}/kpi/all
	Protocol used	HTTP
	Allowed Methods	GET

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

	Get KPI by ID	
	Description	Retrieve one specific KPI
	Provided to	App Store Frontend
	End-point	/api/{vX}/kpi/get
	Protocol used	HTTP
	Allowed Methods	GET
	Post KPI	
	Description	Insert one KPI
	Provided to	App Store Frontend
	End-point	/api/{vX}/kpi
	Protocol used	HTTP
	Allowed Methods	POST
	Post KPI Historic	
	Description	Insert readings for one specific KPI
	Provided to	App Store Frontend
	End-point	/api/{vX}/kpi/{kpi_Id}/historic
	Protocol used	HTTP
	Allowed Methods	POST
	Remove KPI	
	Description	Removes one specific KPI
	Provided to	App Store Frontend
	End-point	/api/{vX}/kpi/{kpi_Id}
	Protocol used	HTTP
	Allowed Methods	DELETE
	Get KPI History	
	Description	Retrieves all the history reading for one KPI
	Provided to	App Store Frontend
	End-point	/api/{vX}/kpi/{kpi_Id}/historic
	Protocol used	HTTP
	Allowed Methods	GET

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

4 SEMANTIC INTEROPERABILITY

4.1 Background

4.1.1 Interoperability levels

The main challenge on the Internet of Things (IoT) is the existence of a plethora of different platforms, protocols, and standards [1]. This fragmentation makes it hard for devices from different companies to work together and for consumers to connect them to each other. To avoid this problem, we need to ensure that devices and platforms can connect and share information easily. This concept is referred to as cross-platform interoperability. Another important challenge is making sure that devices and platforms in different domains, like smart buildings and energy systems, can work together, as sharing data across domains can unlock new possibilities. This is called cross-domain interoperability. Both cross-platform and cross-domain interoperability are of great importance for the HEDGE-IoT project.

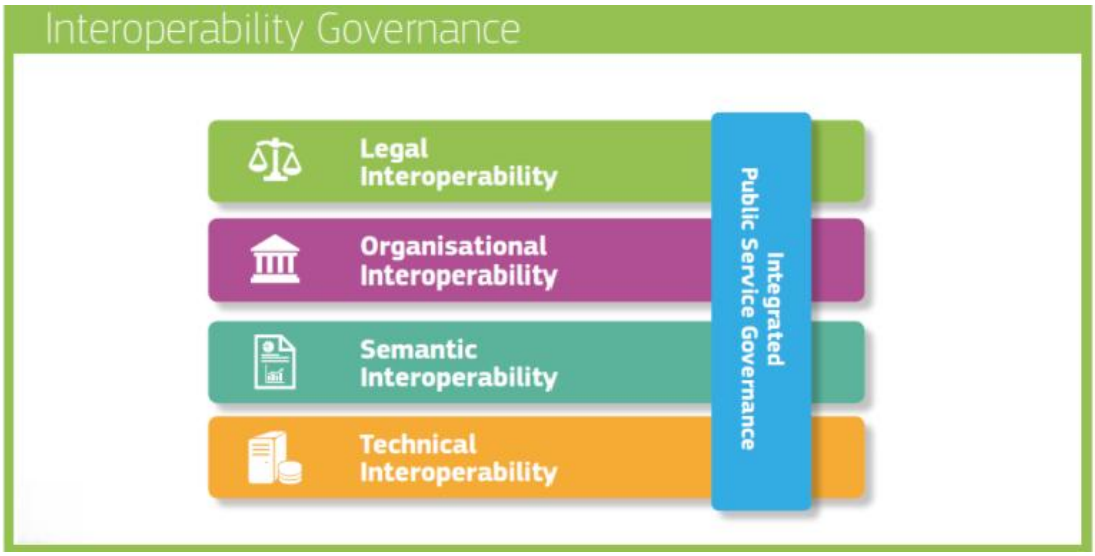
Several frameworks exist that can help to understand interoperability. For example, Figure 16 shows the European Interoperability Framework (EIF) Toolbox[2], provided by the EC, to be used when designing and implementing digital public services. The EIF Toolbox outlines several layers of interoperability. Starting from the bottom, technical interoperability covers the technical aspects of linking systems and services, including interfaces, protocols, and data formats. Semantic interoperability ensures that the precise meaning of exchanged data is preserved and understood by all parties. Organizational interoperability aligns business processes, responsibilities, and expectations among public administrations to achieve common goals. Legal interoperability ensures that organizations operating under different legal frameworks can work together effectively. In addition to these four layers, the EIF Toolbox also includes integrated public service governance, a cross-cutting component that integrates the four layers, and interoperability governance, a background layer that supports the overall governance of interoperability.

[2] https://interoperable-europe.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/solution/european-interoperability-framework-eif-toolbox

Co-funded by the European Union

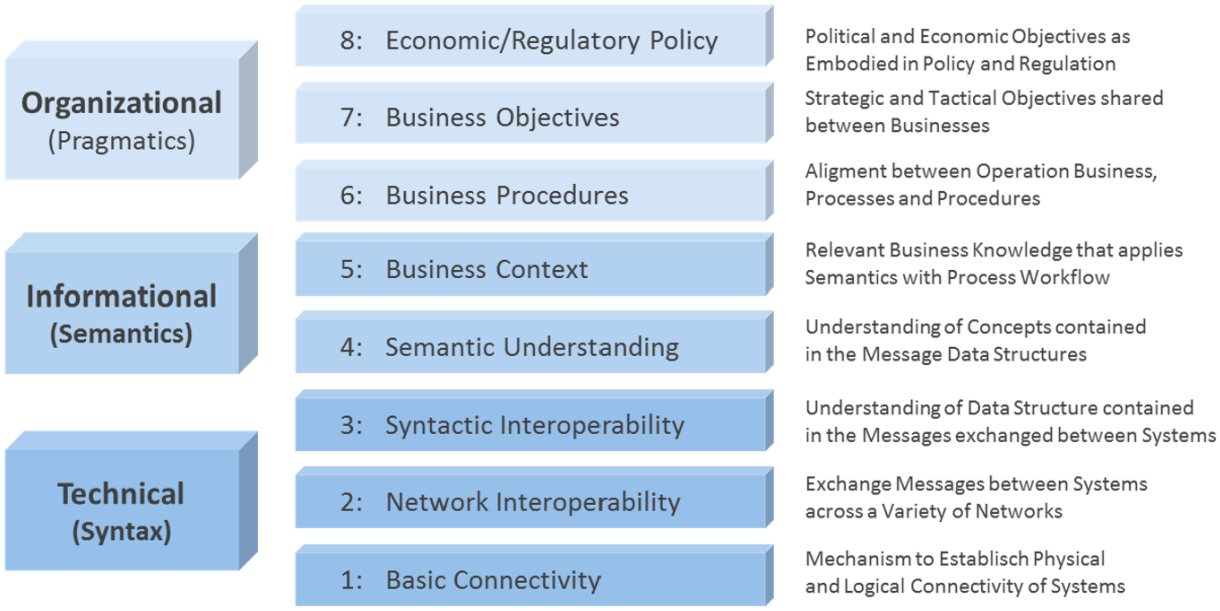
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

FIGURE 16 *THE MAIN LEVELS OF INTEROPERABILITY AS DEFINED BY THE EUROPEAN INTEROPERABILITY FRAMEWORK (EIF)*



A similar interoperability framework that is relevant for HEDGE-IoT, as it targets more system's architects and integrators, rather than public administrations and services, is provided by Gridwise [2], which specifies three main levels of interoperability: technical, informational, and organizational, and it is shown in FIGURE 17. Technical interoperability is about making sure that systems/ devices can connect and communicate. Informational interoperability is about making sure the information exchanged is understood correctly. Organizational interoperability is about making sure businesses and organizations can work together smoothly.

FIGURE 17 *THE THREE MAIN LEVELS OF INTEROPERABILITY AND EIGHT INTEROPERABILITY CATEGORIES AS DEFINED IN [2], WITH EXAMPLES OF EACH CATEGORY*



Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

When looking further at technical interoperability, basic connectivity is about establishing a reliable communication path. Network interoperability is about transporting information across different networks. Syntactic interoperability is about using the same format and structure for sharing information. When moving up to informational interoperability, semantic understanding is about making sure the information is interpreted correctly, which is also the scope of Task 4.3 in HEDGE - IoT. To achieve semantic interoperability, systems need to use a shared reference model, like ontology, which defines the meaning of the information exchanged, ensuring that systems can understand and act on it correctly. This helps resolve conflicts and ensures smooth communication between different systems.

4.1.2 The ontology

Semantic interoperability facilitates seamless communication between (software) agents without the need to convert or otherwise process incoming and outgoing messages. This form of interoperability can be achieved by requiring all parties involved to speak the same language, and by having a shared vocabulary from which to draw words when constructing messages. This shared vocabulary is also often called an ontology and ensures that the same message conveys the same meaning to all agents.

Formally, an ontology is an explicit specification of a shared conceptualization that is held within a particular context [3]. In practice, ontologies can be thought of as documents or files that define the minimal set of classes and properties that are necessary to model the knowledge in a certain domain with. This distinction, between the specific instances and the abstract concepts that are used to model them, is like the distinction between the data level and schema level in relational database management systems, or between assertion data and terminology data in formal systems.SAREF[3] is an example of an ontology for the IoT domain. First published by ETSI[4] in 2015, SAREF provides a large collection of classes to model, amongst others, devices, sensors, and measurements, as well as provide the necessary properties that relate these classes to one another. Ever since, SAREF has been further improved and extended to various subdomains, including energy and smart buildings. Other popular ontologies include Dublin Core[5], which provides numerous concepts for modelling metadata with, and GeoSPARQL[6], used for representing locations and geometries.

Separating the abstract concepts from the specific instances has the benefit that the same ontologies can be used to model other instances, if these are part of the same domain. Because of this reusability, ontologies also lend themselves well to being shared amongst the community, or, more general, to be published online for others to use. This process of publishing and reusing shared ontologies has resulted in a common set of popular and online-available ontologies that form the *de facto* standard for modelling knowledge from a wide range of domains. It is considered good

[3] https://w3id.org/saref/
[4] www.etsi.org
[5] www.dublincore.org
[6] www.ogc.org/publications/standard/geosparql/

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

modelling practice to reuse the ontologies in this popular set, unless these fail to cover the use case in question.

FIGURE 18 A SCHEMATIC OVERVIEW OF THE SEPARATION BETWEEN THE ONTOLOGY (GREEN) AND THE INSTANCES CREATED USING SAID ONTOLOGY (BLUE). NOTE THAT, FOR SIMPLICITY, ONLY SOME OF THE PROPERTIES USED ARE DEPICTED IN THE ONTOLOGY.

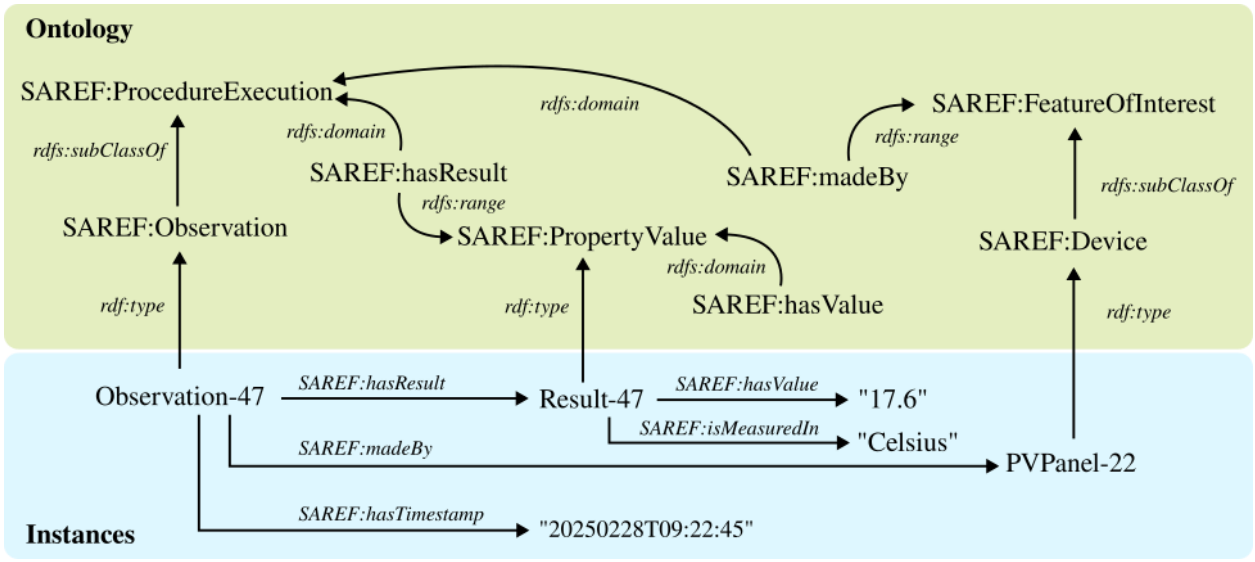


Figure 18 depicts the separation between the ontology (green) and instance level (blue), here shown for a single observation (*Observation-47*, with associated measurement *Result-47*) from a photovoltaic panel *(PVPanel-22)*. Together, these instances describe a single data point (17.6° Celsius) that has been observed at a certain moment in time. All other observed data points, both future and past, can reuse these same classes and properties. By following the links from the instances to these classes, it can be inferred that the observation is of the type *SAREF:Observation*, and that this type is a subclass of the type SAREF:ProcedureExecution. Similarly, the photovoltaic panel can be inferred to be of the type SAREF:Device, and the measurement of the type SAREF:PropertyValue. The same can be done for the properties, inferring their type of hierarchy, domain (source), and range (target). FIGURE 19 shows this for some of the used properties, including SAREF:hasResult and SAREF:madeBy.

Ontologies can be published as text or web documents, aimed at human readers, or they can be shared as machine-readable files, facilitating semantic validation and reasoning if needed. Ideally, both versions are made available, each catering to the needs of their human or machine audience and fostering seamless and unambiguous communication.

4.1.3 Ontology engineering methodology

In HEDGE-IoT, the Linked Open Terms (LOT) methodology (https://lot.linkeddata.es) is employed. This approach, also adopted by ETSI for the development of the SAREF ontologies, as documented in the ETSI EN 303 760 on "SAREF Guidelines for IoT Semantic Interoperability; Develop, apply and evolve Smart Applications ontologies". The methodology encompasses key steps for ontology

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

engineers, domain experts and software developers when creating ontology, including ontology requirements specification, implementation, publication and governance.

Requirements specification. The first activity of the requirement specification consists of extracting the set of requirements that will guide the creation of an ontology. The requirements are extracted from the following sources:1) use cases specified by domain experts and software developers; and 2) existing documentation about the domain of interest in terms of manuals, API specifications, datasets and standards. The second activity is carried out by the ontology development team in collaboration with users and domain experts and consists of defining the purpose and scope of (the modules of) the ontology under development. The ontology development team is then able to propose a set of ontological requirements in terms of Competency Questions or natural language sentences to be further verified with domain experts. The requirements can be finally formalized in an Ontological Requirement Specification Document (ORSD) and taken as input by the ontology implementation activity.

Implementation. During the implementation, the ontology development team first makes a conceptualization (or visualization) that captures the information collected in the requirement specification activity. This conceptualization is then encoded using a formal representation language, such as OWL, which makes the ontology computable by machines. The best practice during this activity is the reuse of existing ontologies, rather than creating all the required concepts from scratch.

Publication. The ontology publication activity aims to provide online ontology accessible both as human-readable documentation and a machine-readable file from its URI. The process includes evaluation to ensure readiness for use, documentation generation in collaboration with domain experts, and publication on the web. The documentation includes an HTML description of the ontology, metadata, and diagrams, while the online ontology is accessible via its namespace URI using content negotiation.

Governance. In the governance activity, the ontology artefact is prepared for sustainability and exploitability. This includes documenting the design choices behind the ontology, prescribing who can maintain and evolve it, choosing a proper platform to host it, and a group to govern it (for example, a standardization body such as ETSI, like in the case of the SAREF ontology). The process of maintenance can include updating the ontology according to new requirements or solving bugs reports, or if a new version of the ontology needs to be generated.

4.2 HEDGE-IoT Approach

This section outlines the approach adopted in Task 4.3 to achieve the intended results.

The HEDGE-IoT approach takes the SAREF ontology and the CIM as the core models to check the pilots' requirements and to extend these models wherever is needed. After the requirements elicitation phase (see section 4.1.3), we perform a gap analysis between the requirements of the

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

pilots and the coverage of SAREF and its various extensions. In section 4.3 we describe the various semantic models we expect the pilots to use, but other models can be used where appropriate. Given the extensive scope that SAREF already has, we expect the resulting HEDGE-IoT ontologies to be small modular additions to existing models instead of another large independent semantic model.

To specify the data models used per project pilot in their information exchange, we envision the use of Semantic Treehouse (STH) as a vocabulary hub. STH is particularly suited for this role as it supports both top-down modelling starting from SAREF/CIM and bottom-up modelling starting from pilot data. Whatever the approach, the outcome is available on the platform to all project partners, so that further collaborative development and maintenance of the semantic specifications in the project is made possible. Any mappings and comparisons between different specifications (for example between different pilot data models, or between a pilot and SAREF/CIM) can be visualized to show overlaps and gaps. It generates technical artifacts needed for implementation - such as graph patterns for the Semantic Interoperability Framework (SIF), which is introduced later in this chapter.

Since the T3.1 survey identified SAREF and the CIM as the most widely used semantic models among the partners, additional effort will focus on investigating whether and how SAREF and CIM can be aligned with each other to reinforce each other's strengths. Among the partners in the project are various CIM experts as well as several SAREF experts.

We see the following stages in the work to be done in T4.3 until August 2026:

- **September 2024 – April 2025**: TNO has scheduled biweekly meetings to get all partners up to speed about the ideas behind semantic interoperability and to get all the partners acquainted with the various tools and technologies that can enable semantic interoperability.
- **March 2025 – August 2025:** the partners have now gathered enough knowledge about the various tools at our disposal to decide which tools or technologies they should employ in their pilot. Members of task 4.3 initiate the use of the vocabulary hub to specify pilot data models in collaboration with pilot partners, followed by initial comparisons of said models to the SAREF and CIM standards.
- **August 2025 – July 2026:** the partners apply and integrate the chosen tools and technologies to solve the use cases they have identified for their pilots. Task 4.3 is a place to gather common problems and to find & create solutions to those problems. Task 4.3 members coordinate the refinement and maintenance of data model specifications in the vocabulary hub.
- **April 2026 - August 2026:** prepare input for T7.4 for possible contributions for standardisation to an appropriate standardisation group, for example the groups governing CIM and SAREF.

4.3 Overview of Semantic interoperability enablers

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

4.3.1 Standardized semantic models

4.3.1.1 ETSI SAREF and extensions

The Smart Applications REFerence (SAREF) ontology is a framework of ontologies standardized and maintained by the European Telecommunications Standards Institute (ETSI) designed to enable interoperability between various IoT solutions from different providers and across different sectors. The framework includes the core SAREF ontology and 12 domain-specific extensions. The main goal of the SAREF framework is to provide a common language that allows different IoT devices and systems to understand and communicate with each other effectively. This helps to overcome the fragmentation in the IoT landscape and promotes a more integrated and efficient digital market. The main concepts of SAREF core include devices, tasks, functions, commands, states, properties, and features of interest. A device is a tangible object designed to accomplish a particular task, such as a light switch, temperature sensor, or washing machine. The task refers to the specific activity or goal that a device is designed to accomplish, like washing clothes for a washing machine. Functions describe the specific actions or operations that a device can perform to accomplish its task, such as starting or stopping a wash cycle. Commands are instructions given to a device to perform a specific function, like turning on a light switch. The state refers to the current condition or status of a device, such as a light switch being "on" or "off." Properties are the characteristics or attributes of a device, including model, manufacturer, or specific measurements like temperature or energy consumption. Features of interest are aspects or elements of the environment that a device can measure or control, such as the temperature of a room monitored by a temperature sensor.

SAREF4ENER is an extension of SAREF specifically designed for the energy domain. It focuses on demand response scenarios, where customers can offer flexibility to the Smart Grid by managing their smart home devices through a Customer Energy Manager (CEM). The CEM is a logical function that optimizes energy consumption and production, which can reside either in the home gateway or in the cloud. This extension helps standardize communication between energy smart appliances and energy management systems, ensuring efficient energy use and integration. SAREF4ENER is based on several key standards to ensure interoperability in the energy domain. It primarily relies on the CENELEC standards EN 50631 series, which includes a set of data elements called SPINE and SPINE IoT resources. Additionally, it incorporates elements from the EN 50491-12-2 standard, which defines S2 resources. These standards provide the necessary framework for creating a common language that allows different energy systems and devices to communicate effectively.

SAREF4GRID is an extension of the SAREF ontology specifically designed for the Smart Grid domain. It aims to create a common core of general concepts for smart grid data oriented towards the Internet of Things (IoT) field.

It is based on the following standards:

- IEC 62056-1-0 ("Electricity metering data exchange - The DLMS/COSEM suite - Part 1-0: Smart metering standardisation framework");
- IEC 62056-6-1 ("Electricity metering data exchange - The DLMS/COSEM suite - Part 6-1: Object Identification System (OBIS)");

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- IEC 62056-6-2 ("Electricity metering data exchange - The DLMS/COSEM suite - Part 6-2: COSEM interface classes").

This extension includes various classes, properties, and individuals to represent different aspects of smart grids, such as meters, firmware, network interfaces, clocks, breaker states, scripts, scheduled actions, activity calendars, power line properties, and services.

SAREF4BLDG is an extension of SAREF specifically designed for the building domain. It was created to enable interoperability among various actors and applications involved in managing building information throughout different phases of a building's life cycle, such as planning, design, construction, operation, and demolition. SAREF4BLDG is based on the Industry Foundation Classes (IFC) standard for building information, developed by buildingSMART International and published as the ISO 16739 standard. The main goal of SAREF4BLDG is to ensure that smart appliances and devices within buildings can communicate effectively, regardless of the manufacturer. It achieves this by providing a common language for describing devices and their interactions within building spaces. This extension includes classes and properties that represent buildings, building spaces, and physical objects, allowing for a standardized way to share and manage building information.

4.3.1.2 IEC CIM

The Common Information Model (CIM) is a standardized framework for facilitating interoperability and data exchange in electrical power systems domain. Defined by IEC standards (IEC 61970, IEC 61968, and IEC 62325), CIM ensures consistent modelling of power system components, operational data, and market processes [5][6][7][8][9][10][11][12][13].

The model consists of three key elements:

- CIM Model (complete dictionary of elements).
- CIM Profile (subset tailored for specific exchanges).
- CIM Serialization (how data is formatted for exchange).

CIM allows for detailed and complete modelling of electrical grid (realistic model is needed for simulations and security analysis). Advantage of CIM is also standardization of extending the CIM when CIM is not enough to model needed data.

TSOs manage high-voltage grids and ensure system stability, security, and market operations. CIM supports TSOs in network modelling, real-time monitoring, and data exchange through the Common Grid Model Exchange Standard (CGMES), as mandated by ENTSO-E. This allows for coordination in state estimation, contingency analysis, and dynamic stability assessments, improving cross-border energy management. CIM profiles such as Equipment (EQ), Steady State Hypothesis (SSH), and State Variables (SV) facilitate structured data exchange, ensuring consistency across different system operators.

DSOs oversee medium- and low-voltage networks, ensuring efficient energy distribution and decentralized energy resource (DER) integration. CIM enables Advanced Distribution Management Systems (ADMS), Geographic Information Systems (GIS), and Meter Data Management Systems

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

(MDMS) to interoperate efficiently. By implementing IEC 61968-3 for Network Operations and other related profiles, DSOs improve visibility, forecasting, and asset management, supporting grid modernization and smart grid initiatives.

CIM plays an almost indispensable role in digital transformation by enabling automated, standardized, and scalable data exchange.

4.3.1.3 IEC 61850

IEC 61850 is a globally recognized standard for communication networks and systems in substations, primarily used in electrical power automation. The standard defines the communication protocols, data models, and system architecture for substations, ensuring interoperability between different vendors' equipment. When viewed as a semantic model, IEC 61850 represents the relationships and semantics of various components in the substation automation system.

Following a brief overview of IEC 61850 semantic model:

- **Semantic Representation of Substation Elements**: IEC 61850 provides a formalized structure for electrical power system components (e.g., transformers, circuit breakers, switches). Each component is described with specific attributes, such as measurements, control functions, status, and diagnostic information.
- **Logical Nodes (LN)**: The semantic core of IEC 61850 is based on "Logical Nodes" (LN), which represent a functional entity or a device in the power system. Each LN is identified with a unique name and provides a specific set of data objects or services. For example, an LN might represent a protection relay or a measurement unit.
- **Data Objects and Attributes**: Each Logical Node contains a set of "Data Objects" (DOs), which are variables or parameters used to describe the state, performance, or measurements of the physical system. These objects represent specific attributes like voltage, current, or status flags.
- **Data Classes and Services**: The standard defines several data classes such as **Control**, **Status**, **Measurement**, and **Settings**. These classes determine the type of data and its meaning in the context of power system operations. Additionally, IEC 61850 defines services like reading, writing, and controlling these data objects for communication and control.
- **Communication Protocols**: IEC 61850 also specifies communication protocols like MMS (Manufacturing Message Specification), GOOSE (Generic Object Oriented Substation Event), and SV (Sampled Values) that enable data exchange between devices in real-time. These protocols support efficient, high-speed communication across substations.
- **Modeling Power System Functionality**: The semantic model also includes a functional layer where multiple Logical Nodes are combined to represent higher-level functions, such as protection, monitoring, control, and automation. These functions are structured hierarchically, supporting complex interrelationships among devices and sub-functions.
- **Extensibility**: IEC 61850 supports extensibility in its semantic model. New Logical Nodes, Data Objects, and Services can be introduced as the needs of the technology or the power system evolve. This flexibility enables the standard to remain relevant over time.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- **Interoperability**: One of the primary objectives of IEC 61850 as a semantic model is ensuring interoperability between different vendors' equipment and systems. The consistent and standardized representation of power system elements and their behaviours ensures that devices from different manufacturers can exchange information and work together seamlessly.

In essence, IEC 61850 as a semantic model defines how power system components, their attributes, and services are represented, communicated, and controlled within a substation automation system. The model is structured to support both current and future needs of the electrical power grid while facilitating interoperability and efficient operation.

4.3.2 Semantic platforms, tools and relevant initiatives

4.3.2.1 Semantic Interoperability Framework (SIF)

The Semantic Interoperability Framework (SIF) is a framework for distributed semantics-based data exchange in a uniform and secure manner. It consists of several components, including the Knowledge Engine, Generic Adapter, Service Store and the P2P marketplace. The goal of SIF is to enable communication between smart appliances and energy management systems, allowing data sharing between digital platforms from different manufacturers and service providers. It was developed during the H2020 InterConnect project.

The Knowledge Engine helps to intelligently exchange data in a semantically interoperable way between various systems, such as sensors, APIs, databases, and services. This is done by using a description of each system that defines the data that it produces and consumes. This description is expressed using an ontology. The Knowledge Engine then intelligently combines information from all systems in the network to ensure seamless data exchange across multiple information systems from different vendors and organizations, without using a centralized database.

The Service Store is a web application that serves as a single stop for all providers and adopters of interoperable services from energy and non-energy domains. Users can register new interoperable services at the Service Store and browse existing ones. Moreover, it also provides all the information for accessing and utilizing these services.

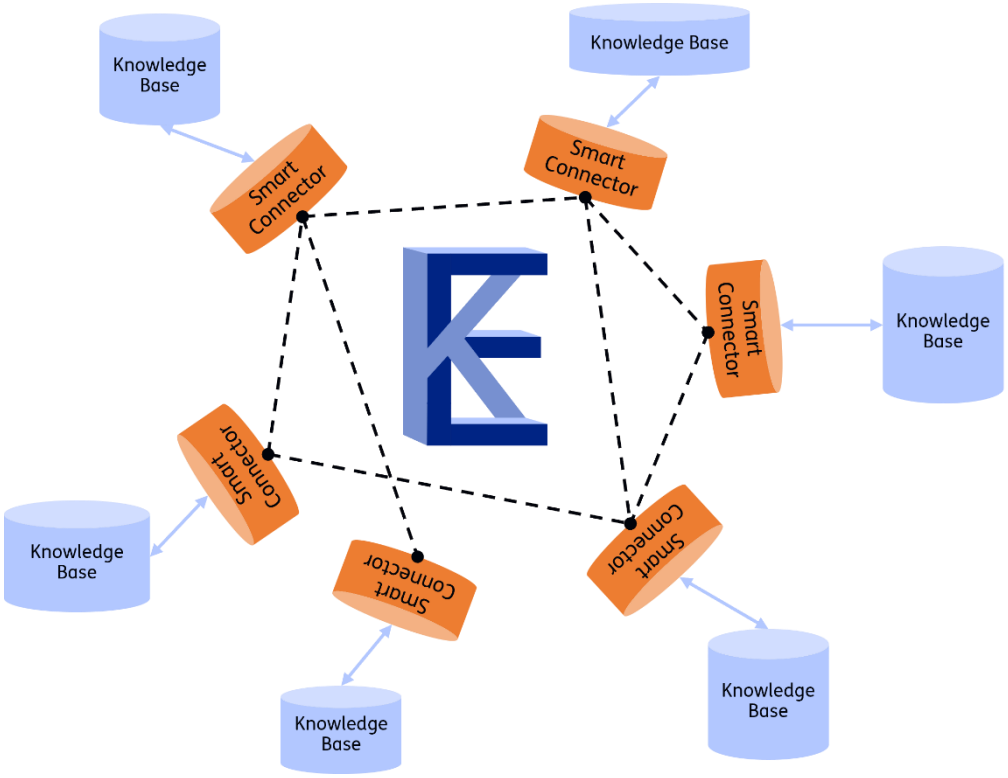
The Generic Adapter ties the Knowledge Engine and Service Store together and, as such, is a generic software component that acts as a gateway for secure and trusted integration into a wider interoperability framework instance. It enables a unified and secure communication interface. Moreover, it makes deployment more flexible based on Docker.

In the SIF, we assume that there are multiple knowledge bases who form a network together:

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

FIGURE 19 INTERACTIONS BETWEEN KNOWLEDGE BASES AND SMART CONNECTORS IN SIF



Knowledge bases can be data producers (e.g. a temperature sensor), data consumers (e.g. a dashboard or data storage), and/or a type of service (e.g. an anomaly detection algorithm). Each knowledge base can receive data and/or send data to others in the network by using a connector. Each participant tells its own connector which knowledge it wants to send/receive based on a shared ontology. Any ontology can be used for this purpose, including SAREF and its extensions. The connector will then take care of the data sharing with other participants in the network.

The SIF is ideal when one wants to share data with multiple parties, in a shared domain where the parties that exchange data may change over time. It has been implemented such that data stays at the source as much as possible. It also supports both querying and publish-subscribe interactions, providing a flexible means of communication. Moreover, it can automatically infer new facts and intelligently link systems to answer more complex questions.

Additional resources:

- SIF: https://gitlab.inesctec.pt/groups/interconnect-public/-/wikis/home#interconnect-interoperability-framework
- Knowledge Engine: https://github.com/TNO/knowledge-engine

4.3.2.2 Semantic Treehouse (STH)

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Semantic Treehouse is an open-source platform that helps data sharing communities to agree on, define and improve shared data models. It serves as a vocabulary hub that makes semantic specifications findable and accessible while providing services to facilitate their adoption by data owners and consumers. The platform supports both top-down and bottom-up approaches to semantic interoperability:

Top-down approach: Users start established semantic models like SAREF or CIM and use the STH wizard functionality to create use case specific API specifications and schemas. The wizard guides users through:

1. the selection of appropriate ontologies for their use case,
2. creating a data model by selecting relevant classes/properties, and, optionally,
3. the generation of schemas (XML, JSON, RDF/SHACL) and API specifications

Bottom-up approach: Starting from existing data samples or schemas, users can create initial data models of their specific use case that can be further developed and aligned with common semantic models. This approach is particularly useful when there are no suitable existing semantic models, or users are not yet familiar with semantic modelling, or when quick results are preferred over careful semantic alignment (for the time being).

Other functionalities of Semantic Treehouse are:

Collaborative development and maintenance of specifications through version control and issue tracking. (STH is to common data models what platforms GitHub/Gitlab are to software.)
Integrated validation support for developers tasked with implementing the data models
Support for showing mapping and comparison between different specifications (e.g. "how does pilot A's data model here relate to the model specified by pilot B?" "How does pilot A's data model compare to the popular SAREF ontology?

Semantic Treehouse has been in active development since 2016. Its design is continuously aligned with standards and best practices, in particular with the IDSA family of documents (IDS RAM, position paper on semantic interoperability), the Data Space Support Center (DSSC) blueprint and toolbox, and the Common European Energy Data Space (CEEDS) blueprint. The code base is openly available at https://gitlab.com/semantic-treehouse, while documentation is provided at https://www.semantic-treehouse.nl/docs. TNO provides a deployed instance of Semantic Treehouse to function as an Energy data spaces vocabulary at https://energy.vocabulary-hub.eu.

4.3.2.3 Ontology-Driven Constraint Tester (ODC-Tester)

The Ontology-Driven Constraint Tester (ODC-Tester) focuses on ensuring technology-neutral ontology-based interoperability. It aims to support engineers to verify, ensure and validate the interoperability compliance of data exchange between various systems with ontologies (e.g., SAREF at the moment). The testing methodology is based on the Joint Research Center (JRC) initiative for a Code of Conduct (CoC) for Energy Smart Appliance (ESA) [14] interoperability test method. The

Co-funded by the European Union

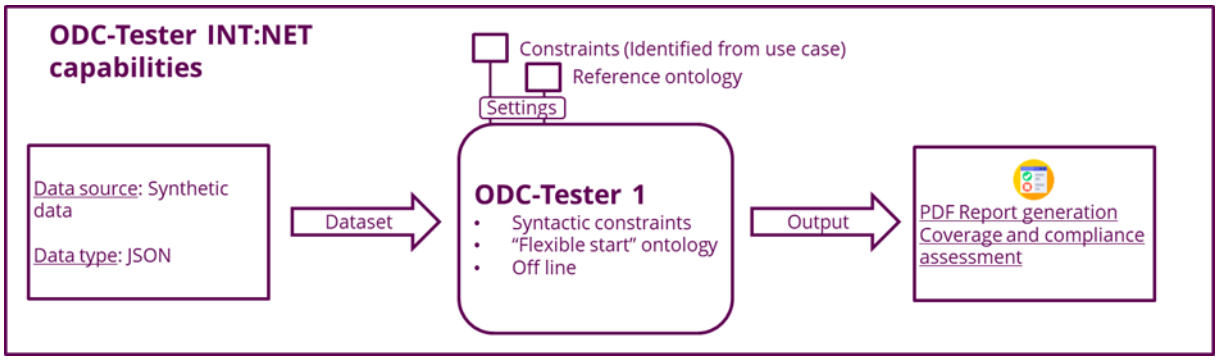
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

ODC-Tester proof of concept has been initiated in the INT:NET project [15] to get insight on the feasibility of an interoperability assurance program. It includes the use of ontology-based testing tools and also supports JRC CoC ESA interoperability.

The existing proof-of-concept supports several functions:

- Ontology compliance: validating the compliance of a simulated dataset to an ontology which is part of the SAREF ecosystem.
- Interoperability support: providing execution logs to support testers and engineers in identifying the interoperability issues.
- Report generation: generating a report compiling results and recommendations for improvement.

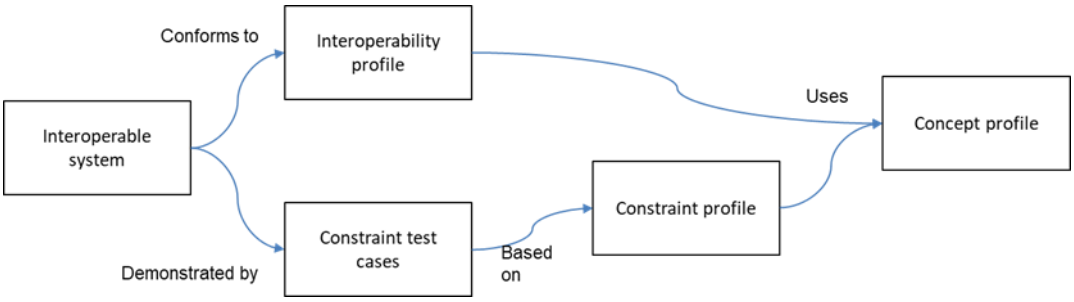
FIGURE 20 ODC-TESTER INT:NET CAPABALITIES



Technically, the ODC-Tester uses SHACL shape constraints to validate the semantic data of the system under test. The validation is achieved by an ontology engine implemented into a web application supporting the tool. A technical presentation of the proof of concept developed in INT:NET is available in the paper "Design of an Ontology-Driven Constraint Tester (ODCT) [16]. The current version of the ODC-Tester was also presented during the workshop on Energy Management Interoperability of Energy Smart Appliances, which was organized in 2024 by the JRC and DG ENER.[17]

In HEDGE-IoT, TRIALOG will contribute to two activities, the SAREFisation process and the demonstration of testing capabilities based on the ODC-Tester. SAREFisation is the process of defining reusable ontologies in a domain governed by a SAREF community. This will include a focus on the methodology to define concept profiles (or ontology profiles) and constraints profiles.

FIGURE 21 CONSTRAINT PROFILE



Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

The ODC-Tester will showcase the test of constraints specific to HEDGE-IoT pilots. A use case (and the associated SHACL shape constraints) will be implemented based on at least one pilot need regarding smart appliances use cases, that could also support the work of the JRC CoC ESA initiative.

New functions will be explored in the context of the HEDGE-IoT study such as performing ontology compliance verification using real datasets, performing behavioural compliance verification, extending and improving the tool's support with additional visualisation capabilities and supporting additional data formats as input to facilitate the data exchange with diverse systems under test. This study could also identify new relevant test cases that could support the JRC CoC ESA.

4.3.2.4 PowerCIM

PowerCIM is a digital platform designed for the efficient exchange and management of electrical power system information, fully aligned with the IEC CIM (Common Information Model) standards (IEC 61968, IEC 61970, IEC 62325). It enables seamless data integration, versioning, and advanced network model management, empowering grid operators and stakeholders with a unified and standardized approach to handling complex energy system network model data. The platform incorporates rapid model assembly, validation, import/export and Version Control System (VCS) functionalities, allowing for flexible and scalable data management.

A core feature of PowerCIM is its smart versioning and model management, which allows for storing only changes (deltas) rather than entire dataset snapshots. This approach optimizes storage, improves retrieval efficiency, and ensures historical accuracy without data loss. The platform employs bi-temporal versioning, enabling users to make corrections without erasing history and to maintain multiple future scenarios simultaneously. With multi-repository support, PowerCIM enables diverse workflows for different power system models, allowing for interdependent or independent branches that facilitate easy model data maintenance and integration of various data sources. While CIM does not define a strict hierarchy, PowerCIM enables inferred hierarchies, ensuring a structured approach to data modelling.

The architecture of PowerCIM is designed for high performance and modularity. The core library provides essential functionalities such as in-memory storage, indexing, model versioning, and data validation. Surrounding this core, PowerCIM incorporates adapters, which enable integration with external systems and ensure interoperability with different formats and protocols.

At its core, the platform relies on PostgreSQL for persistence, using JSON structures for equipment data and specialized blobs for other data types. The backend of PowerCIM is built using .NET Core, ensuring a high level of performance and compatibility, while the frontend is implemented in React, offering a user-friendly interface for data visualization and interaction.

With optimized indexing and filtering mechanisms, the PowerCIM platform ensures high-speed query execution and in-memory processing and can handle large-scale network model datasets efficiently without performance bottlenecks. Furthermore, its built-in geolocation capabilities allow performant spatial data management and geoindexing, supporting standard WKB/WKT and GeoJSON geometric formats.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

PowerCIM finds practical applications in various power transmission and distribution business processes, enabling easy model data management and application development without reimplementing the complex CIM standard and model versioning functions. In the context of the HEDGE-IoT project, PowerCIM enables a standardized data format that can be integrated into various digital platforms for power system management. This allows network operators to utilize the models while also supporting the development of advanced applications and algorithms for analytics and optimization. Through unified data exchange, PowerCIM serves as a foundation for enhancing interoperability and driving digital transformation in the energy sector.

4.3.3 IDSA Energy Interoperability TF

The IDSA Energy Interoperability Task Force, comprising experts from the Energy Data Space Cluster Projects (EDSCP), namely OMEGA-X, ENERSHARE, DATA CELLAR, EDDIE, and SYNERGIES, along with their associated Coordination and Support Action (CSA, Int:net), plays a crucial role in promoting cross-data space interoperability. While the task force primarily focuses on achieving technical and semantic interoperability, it also addresses organizational and legal aspects to ensure a comprehensive approach. As outlined in the position paper "Interoperability Framework in Energy Data Spaces [4], the task force leverages existing reference architectures like the Common Information Model (CIM) and the Smart Grid Architecture Model (SGAM), while proposing enhancements tailored for energy-specific applications. The framework emphasizes interoperable data formats, exchange protocols, and identity management systems, alongside standardized legal and organizational practices, to facilitate secure and efficient collaboration.

To demonstrate cross-data space interoperability, the EDSCP have defined 5 System Use Cases (SUC), which have been described in the position paper. These include 4 technical ones (onboarding, data discovery, contracting, data exchange) and 1 semantic SUC. Semantic interoperability within energy data spaces ensures that exchanged data retains its meaning, enabling seamless integration and collaboration among diverse stakeholders. This is particularly vital for smart meter data, where discrepancies in data models and terminologies can obstruct efficient data sharing. To address this, sister projects such as of the EDSC have adopted the IEC 61968-9 Ed 3 (EUMED Metering profile) as a common data model, with each project mapping its internal data accordingly. As part of the EDSCP, a semantic interoperability test, supported by Int:net and the BRIDGE Data Management Working Group, was conducted to ensure unambiguous data exchange across five dataspaces, focusing on metering data. The Common Semantic Data Model (CSDM), developed in OMEGA-X and incorporating the EUMED module, serves as the foundation for this initiative. Three integration strategies—native support, ontology alignment, and transformation services—are implemented to align project data with the EDSCP Common Data Model, ensuring seamless cross-domain interoperability.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

5 IOT CLOUD/EDGE SYSTEM INTEGRATION

5.1 Integration Methodology

5.1.1 Intended Output

The primary goal of Task 4.4 "IoT Cloud/Edge System integration" is to support the integration of the technology components developed to support interoperability, trust & sovereignty, and data process flows as depicted by functional requirements. By providing the necessary service orchestration and a Dataspace technological framework, these components will form the reference implementation for HEDGE-IoT. The outcome will also involve the inclusion of processes, services, communication channels, and interfaces based on the demonstrator scenarios. The integrated Data Space will manage data access for various stakeholders within the energy ecosystem, as well as external services/platforms, in an interoperable way. In summary, the integration methodology can be categorized as follows:

- **Integration Guidelines:** Defined integration guidelines outline the path for incorporating middleware software components by detailing the processes and methodologies, assigning responsibilities, and most importantly, creating an activity plan with clear objectives, milestones, and interdependencies. This effort will ensure successful implementation alignment and convergence, ultimately bringing the HEDGE-IoT technical framework to life.
- **Contingency Plan:** A detailed methodology with mitigation strategies designed to address integration risks, scheduling delays, or other potential issues.
- **Service Orchestration:** Service orchestration will oversee the configuration and coordination of activities related to managing available software and services. A key aspect of this process will be the integration of various stand-alone software subsystems into a unified system that delivers consistent results. This task will also include monitoring the alignment of the integration procedure with the Data Space integration guidelines and the Eclipse MVD (Minimum Viable Dataspace) implementation.
- **Actual integration and deployment of the HEDGE-IoT Data Space:** The practical integration and deployment of the HEDGE-IoT Data Space involves establishing a fully operational digital ecosystem that incorporates the processes and services defined in WP2. This will be achieved through communication channels and API interfaces. Simultaneously, the integrated framework will ensure seamless data access management for various stakeholders in a genuinely interoperable and decentralized manner.
- **A comprehensive testing process:** Each integrated version (technological release) will undergo testing to identify and resolve any technical issues arising from the integration. The goal is to develop a fully functional platform by integrating all components, ultimately delivering a prototype suitable for validation.

5.1.2 Pilot Requirements

The development of the HEDGE-IoT platform will be guided by a well-defined set of requirements, ensuring a structured and efficient integration process. These requirements will not only dictate

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

how various components are incorporated but will also align with the broader principles outlined in technical WPs. The integration process will focus on the following key objectives:

1. **Ensuring seamless interoperability** between components and stakeholders.
2. **Guaranteeing data privacy, security, and sovereignty** throughout the system.
3. **Achieving full GDPR compliance** to uphold data protection regulations.
4. **Minimizing risks of privacy breaches** through robust security measures.
5. **Preventing misuse and abusive practices** in data sharing.
6. **Adhering to cybersecurity best practices** to enhance system resilience.
7. **Leveraging System Use Cases** to ensure practical applicability.
8. **Defining clear Demo requirements** for validation and implementation.
9. **Integrating technologies that are usable, useful, and desirable** for stakeholders.
10. **Employing tools and technologies that are accessible, applicable, acceptable, and adoptable.**
11. **Assessing the technological maturity of the Pilot** to ensure feasibility.
12. **Maintaining inclusiveness** with well-defined eligibility criteria.
13. **Prioritizing Quality of Service (QoS), performance, and scalability** in the system.
14. **Enhancing the user experience** for intuitive and efficient interaction.
15. **Streamlining processes** to simplify implementation and usability.

By adhering to these principles, the HEDGE-IoT Data Space will establish a robust, secure, and user-centric data-sharing environment that meets both technical and regulatory standards.

5.1.3 Definitions

5.1.3.1 Successful Software Delivery

As quality software is an essential part of successful implementation and delivery[7], the need for faster release cycles, higher quality, and robust security — especially data security—has never been more critical. Modern software demands are non-negotiable, driving a fundamental shift in how software is developed and delivered. Established technical organizations are overhauling their software development life cycles, businesses that once treated IT as a cost center are now making significant software investments, and a surge of startups is entering the market to tackle longstanding challenges across various industries. The energy sector, stands to benefit from this transformation. The adoption of cloud computing, digital transformation, DevOps, DevSecOps, and chaos engineering is rapidly gaining momentum, reshaping how software solutions are designed, deployed, and managed.

[7] https://www.harness.io/blog/best-practices-software-delivery

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

The success of software delivery is often linked to user requirements and technological infrastructure. However, four key success factors can be defined:

- Velocity – Modern software delivery demands rapid deployment and continuous delivery.
- Governance – Ensuring alignment with business objectives and adherence to project specifications.
- Quality – A high-quality and adaptable delivery process is essential, with user experience and simplicity playing a crucial role.
- Efficiency – Optimizing resource utilization to achieve a streamlined and effective delivery process.

According to existing literature[8] a successful software delivery process requires:

- Data-Driven Approach – Utilizing KPIs and metrics to quantify results, enhance productivity, and improve process quality.
- Agile-Oriented Process – Implementing an iterative, goal-driven approach that remains flexible and responsive to feedback, ensuring alignment with business and functional requirements.
- Microservices Framework – Enabling faster and higher-quality software delivery by adopting a microservices architecture, where each loosely coupled service fulfills a specific function.
- Source Control and Testing Strategy – Establishing a structured source control process with defined branching, code reviews, and merge procedures. Implementing a robust testing framework (potentially automated) focused on quality, integration, functionality, and user experience, following a shift-left testing approach.
- Continuous Integration (CI) – Allowing multiple developers to contribute to a shared codebase while maintaining a stable, well-tested product. The CI process should include unit testing, security scans, dependency management, compilation, build, and packaging.
- Continuous Deployment (CD) and Continuous Verification – Automating deployment activities to create a repeatable and sustainable process while mitigating risks throughout the release cycle.
- Security-First Development – Integrating security from the initial code development phase, tracking it through artifact management, and reinforcing it at every deployment stage. This includes implementing security scans in CI/CD pipelines, conducting code analysis, and enforcing well-defined security standards throughout the release process.

5.1.3.2 Software Distribution, Packaging, and Integration Methodology

This section explores two interconnected yet distinct topics: software component distribution and packaging, and a fundamental approach to software integration. The integration methodology is designed around HEDGE-IoT, which functions as a federation of energy-related stakeholders aiming to share data to enhance operational efficiency.

Software Packaging and Distribution: Software component packaging and publication are essential steps in the deployment process. Packaging involves bundling executable files,

[8] https://www.oreilly.com/library/view/accelerate/9781457191435/

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

documentation, and necessary resources into a structured format that facilitates deployment. To ensure accessibility, a distribution mechanism is required, enabling external users to retrieve the packaged software. Today, public repositories serve as centralized storage solutions for application code, with platforms like GitHub[9], GitLab[10], and Bitbucket[11] being widely used for hosting and managing repositories.

Containerization with Docker: Docker[12] is a widely adopted open platform for developing, shipping, and running applications within containers. A Docker image includes all the essential components needed to execute an application, such as code, dependencies, libraries, and tools. These images can be deployed across multiple container instances, ensuring consistency and scalability. Public repositories play a crucial role in hosting and distributing Docker images. Docker Hub[13], for example, provides a platform for storing and sharing containerized applications. It functions as a registry, a system for storing and delivering named Docker images in multiple tagged versions. Users can opt for free public repositories for sharing images openly or subscribe to private repositories for restricted access. By leveraging modern distribution channels, containerization technologies, and integration frameworks, organizations can streamline software deployment while maintaining flexibility, scalability, and security.

5.1.3.3 Understanding System Integration

Integration is the process of combining individual components into a cohesive, functional unit. In the IT domain, it involves merging different systems to ensure seamless data exchange, enabling a more efficient and interconnected environment. The primary goal is to create a unified system where data can be shared quickly and effortlessly when needed. To achieve this, organizations often develop a customized reference architecture, incorporating both new and existing hardware, software, and other technological components[14]. System integration can also be viewed as a data management process, where software facilitates automated information exchange between multiple subsystems. An integrator serves as an intermediary, translating data between systems, as each may be built using different programming languages and structures. Generally, there are four primary methods for integrating third-party services within service management software, each with its own advantages and challenges, depending on the specific use case.

Application Programming Interfaces (APIs)

An **Application Programming Interface[15] (API)** is one of the most widely used tools for connecting different applications. APIs come in various forms, both public and private, but they all serve the same fundamental purpose—facilitating interaction between systems. APIs use a standardized code language to define functionalities and establish protocols, enabling seamless data exchange between applications. By leveraging these interconnections, APIs ensure automated and efficient data transfer. API integration provides end-to-end visibility across systems and processes,

[9] https://github.com/
[10] https://gitlab.com/
[11] https://bitbucket.org/
[12] https://www.docker.com/
[13] https://hub.docker.com/
[14] https://www.techtarget.com/searchcustomerexperience/definition/integration
[15] https://blog.postman.com/intro-to-apis-history-of-apis/

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

enhancing data tracking, monitoring, and reporting capabilities. Additionally, it supports the transfer of complex and large datasets with minimal errors, improving overall efficiency and accuracy.

Webhooks

Through a **webhook**[16] (web call-back) applications provide real-time information. For webhooks, implementation is often not code based. They have modules that are programmable within a web application. Instead of being request-based, webhooks are event-based. They only trigger when specific events occur within a third-party service.

Integration Service Component (ISC)

Unlike code-based integrations, the **Integration Services Component (ISC)** operates directly on a local server. It acts as a bridge between on premise tools—such as directories, asset management systems, and business intelligence (BI) tools—eliminating the need for manual file imports, particularly for handling large datasets.

Orchestration

Orchestration represents the most automated form of integration. It involves automating the interaction between multiple systems and services by consolidating repetitive tasks. Teams typically use software configuration management tools to build these orchestrations. These tools provide various methods, such as snap-ins or hosting APIs, to connect with applications and manage the automation workflow. The orchestration process automates the necessary tasks to handle connections and operations across workloads on both private and public clouds. Its goal is to improve production efficiency and streamline information flow. By automating the integration of multiple software and processes, users can easily connect with any service to access data. However, like APIs, this method requires in-depth knowledge of coding and software development.

5.1.4 Integration Process

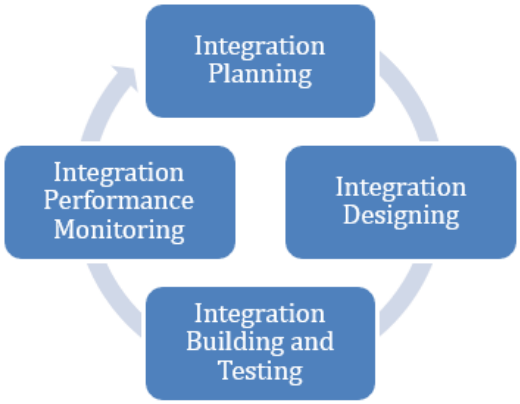
FIGURE 22 below visualises the overall integration methodology that will be followed in the project.

[16]https://www.vivantio.com/blog/4-types-of-integration-methods-with-your-it-service-management-software/

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

FIGURE 22 INTEGRATION PROCESS



The integration process is broken down into four key phases:

- **Planning Phase:** This phase involves dividing the entire integration process into smaller, manageable tasks, focusing on timelines, team organization, and resource allocation for activities.
- **Integration Design Phase:** In this phase, we define the overall integration strategy and determine the most effective approach to achieve the goals set out in the integration plan.
- **Integration Building and Testing Phase:** This is the actual execution phase where integration takes place. It is essential to ensure that all integration requirements are met and that all components are properly integrated and functioning. A critical objective of integration is ensuring functional interoperability, which is achieved through specialized connectors that guarantee security, trust, and sovereignty. API integration plays a vital role here, involving the development and deployment of API interfaces. API development often follows standards like OpenAPI or Swagger, which provide automated documentation and code generation for SDK clients. During testing, we assess whether the integrated components comply with the Reference Architecture and meet functional specifications such as Quality of Service (QoS), accessibility, security, scalability, and performance.
- **Monitoring Phase:** The final phase focuses on evaluating the integration process from a system perspective, ensuring that it aligns with functional requirements and performs as expected.

5.1.5 Contingency Plan

The Contingency Plan for HEDGE-IoT is structured around: i) Design, ii) Development and iii) Deployment & Testing. This plan outlines the measures to mitigate potential risks that may arise during any phase of the system's development and integration. These mitigation strategies are incorporated into the Integration Plan and the HEDGE-IoT Framework, ensuring they are considered throughout the design, development, testing, deployment, and documentation phases.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

TABLE 16 CONTINGENCY PLAN

Kind of Risk	Description	Impact	Mitigation Measures
Overall Development Management	The implementation and deployment of the HEDGE-IoT digital ecosystem is critical to the success of the project, as it serves as the system that enables and promotes the data sharing and exchange process among stakeholders	High	Ongoing communication with stakeholders through regular and ad-hoc teleconferences, emails, and document exchanges
Timing	Timing refers to efficient alignment of actions. The project's complexity requires that all participants follow the agreed schedule or communicate as early as possible on possible deviations	High	Ongoing communication through the established channels within the project will ensure that any deviations from the planned integration process are identified promptly. The integration plan's timeline will be revised as needed to minimize the impact of these deviations
Stakeholders' engagement	Demos are regarded as the ultimate beneficiaries of the project. Therefore, their continuous involvement throughout the various phases, from design to testing, is essential	High	In addition to communication, key activities include distributing evolving documentation, conducting live system presentations from the early development phase, and establishing structured communication channels (e.g., GitHub)
Design			
Scope (SUCs) accuracy & variations	The System Use Cases serve as the foundation for HEDGE-IoT's design. Their accuracy and efficiency directly contribute to the creation of a precise and effective Data Space and the HEDDGE-IoT system in general. However, since HEDGE-IoT's scope is new to the involved stakeholders and beneficiaries, there is a possibility that the Use	Very high	Early involvement of stakeholders' specialists during SUCs design. Detailed documentation of SUCs, usage of good practices or standards

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

	Cases may require revision or adaptation during the detailing and development phases. A significant risk arises if this revision process extends beyond the testing timeframe, especially if the development encounters changes or integrations affecting core system components—such as the data model, APIs, and processes—rather than just limited operational aspects		
Differences among Pilots	HEDGE-IoT aims to be a unified system rather than a customized solution for each Pilot. Consequently, certain design elements, particularly System Use Cases (SUCs), are expected to be shared across all pilots. However, variations in similar characteristics among the demos add complexity to the design and development process	High	Convey development progress to the pilots through: • Updated documentation • Component prototyping • System presentations and discussions from the users' perspective
Users' acceptance	User acceptance is crucial for the system's success. This requires the system to effectively fulfil its intended functions while being intuitive and user-friendly. The risk lies in users struggling to adapt to the system or finding that it does not meet their reasonable expectations and requirements	High	Same as above
Development			
Timing	Ensuring the timely delivery of development outcomes and intermediate results is essential. Delays, particularly in critical components, could impact both	High	Adhere to and monitor the development timeline, ensuring intermediate results are shared with other development teams as early as possible. Utilize established communication channels for smooth

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

	the overall project timeline and the system's quality		collaboration and respond promptly to feedback from participants
Specifications' fulfilment	All functional and non-functional requirements must be met during development	High	A Requirements Traceability Matrix (RTM) will be created for the 2nd and final release. Corresponding tests, following the Testing Guidelines, will validate the fulfilment of the requirements
Tools & Technology Stack	Utilize tools and technologies that ensure easy access for deployment for beneficiaries and users without requiring expertise beyond the standard IT infrastructure used in the electricity sector	High	Choose standard, and where possible, open-source tools and technologies. Notify the demos of the proposed technology stack as early as possible
Integration			
Local Services & Local Components	If integration with local services and components is not seamless, meaning the correct information is not exchanged at the right time, the system integration will effectively fail.	High	Develop the required middleware to integrate local components and services with the core system, following a thorough API definition, implementation, and testing process.
APIs Documentation	Incomplete API Documentation might hinder integration of local actors and systems	High	Provide detailed API documentation
APIs accessibility	APIs accessibility should be ensured for the users that need to access them	High	Documentation and extensive testing shall ensure that APIs are indeed accessible for authorised users
Deployment			
Hosting Infrastructure	The hosting infrastructure must be sufficient to support the technologies and payload required by the system	High	Select a Technology Stack which provides for a hosting environment that covers all appropriate requirements

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Network Security	The security of the hosting infrastructure is critical, as the HEDGE-IoT system is exposed to the Internet	High	Follow the project's Cybersecurity guidelines
Logging & Debugging	A new IT system may encounter programming errors (bugs) or malfunctions that arise during extensive user testing and its integration with external systems, particularly under various edge conditions and parameter settings	High	Incorporate a comprehensive (and expandable) logging and reporting system into the HEDGE-IoT system. Develop a debugging strategy for each demo during the integration, testing, and piloting phases

5.2 Integration testing activities

5.2.1 Introduction

Software testing is the process of assessing a software product to determine if it meets the required specifications and to ensure it is free of defects. It involves executing software or system components using manual or automated tools to evaluate specific properties of interest. The goal of software testing is to identify errors, gaps, or missing requirements when compared to the actual specifications. Testing is essential for detecting issues early in the development process before the software version is released to customers or end-users. The key benefits of testing include:

- **Software Quality**: A critical requirement for any software system aimed at delivering high-quality products to end-users and key stakeholders.
- **Cost Minimization**: Timely testing helps save both money and time in the long run. The earlier bugs are identified, the less expensive they are to fix, leading to fewer iterations between developers and customers (such as the pilot demonstrators in our use case).
- **Customer Satisfaction**: The primary goal of any product is to satisfy customers, boost engagement, and enhance the overall user experience.

Testing is traditionally divided into three main categories: Functional, Non-Functional, and Maintenance. While there are over 150 types of testing methods, the most used ones (which we will address in HEDGE-IoT) include:

- **Functional Testing**: UI Testing, API Testing, Integration Testing
- **Non-Functional Testing**: Performance Testing
- **Maintenance Testing**: Regression Testing

In the first development phase, we focus primarily on functional testing.

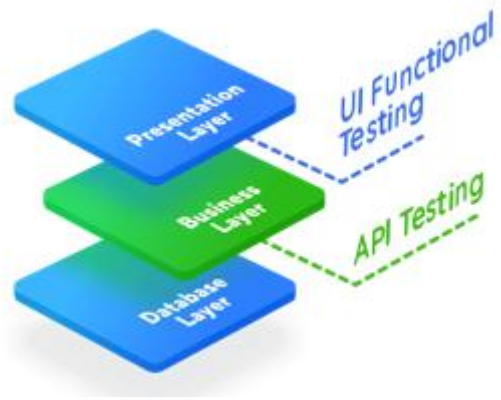
Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

5.2.2 Introduction

Functional testing is a form of black box testing that assesses whether a system or component meets its specified functional requirements. It focuses on what the system does, verifying that all the application's functionalities work as expected and are ready for release. As black box testing, the tester does not have knowledge of the app's internal structure or source code. The development team creates functional test cases based on user and business requirements, while testers define the functionality requirements from the user's perspective. Functional testing can be performed manually or automated. In the context of the project, functional testing will be based on the HEDGE-IoT Functional Requirements. These high-level requirements outline the technical functionalities expected from the Data Space components, which can be further broken down into smaller sub-requirements. The project will address three types of functional testing: UI Testing (frontend), API Testing (backend), and Integration Testing (frontend-backend). This approach aligns with the typical web application architecture, which consists of three separate layers: the presentation layer (user interface), the business layer (where business logic is handled), and the database layer (for data modelling and manipulation).

FIGURE 23 THE THREE LAYERS OF THE HEDGE IOT PLATFORM



UI Testing is conducted at the presentation layer and focuses on evaluating the features that users interact with directly. This type of testing typically examines visual components to ensure they meet specified requirements for both functionality and performance. UI testing is primarily concerned with two aspects: first, verifying how the application responds to user actions via input devices like the keyboard, mouse, and other peripherals; and second, confirming that visual elements are displayed and function properly. Examples of aspects tested during UI testing include:

- **Menu Items** – Ensure only valid menu items are displayed based on the current application state.
- **Navigational Elements** – Verify that all navigation buttons work correctly and redirect users to the appropriate pages or screens.
- **Data Type Validation** – Confirm that only valid data types (e.g., currency, dates) can be entered into fields.
- **Field Widths** – Ensure text boxes clearly indicate character limits and prevent the entry of excessive data.

Co-funded by the European Union

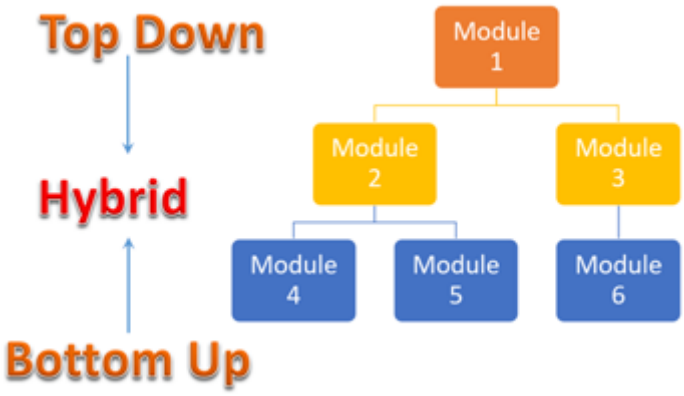
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

API Testing, performed at the business layer, involves testing the application's core logic and the transactions between the user interface and database layers. This testing evaluates the functionality, reliability, performance, and security of APIs. It is an essential part of integration testing, allowing for quick validation of the system's logic. Rather than using standard user inputs, software tools are used to send requests to the API, receive responses, and assess how the system reacts. API testing is different from GUI testing, as it focuses on the software's business logic layer rather than its user interface. Examples of API testing include:

- **Return Values Based on Input Conditions** – Test the API's response to defined inputs and validate the output.
- **Triggering Other APIs/Events** – If an API triggers another event or interrupt, these events should be monitored.
- **Resource Modification** – Verify that if an API call modifies resources, the changes are reflected and validated within the system.

Integration Testing is a type of testing where different software modules, developed by various programmers, are logically integrated and tested as a group. This phase focuses on identifying issues that arise when these modules interact. In the case of HEDGE-IoT, integration testing will focus on ensuring the frontend and backend components work together to meet all functional requirements from start to finish. Given the project architecture, integration testing will follow the **sandwich testing strategy**, where both frontend and backend are tested in conjunction with each other, ensuring smooth interaction between the various system layers.

FIGURE 24 SANDWITCH TESTING STRATEGY FOR HEDGE IOT



The Integration testing process, is summarized in the following steps:

1. Prepare the Integration Test Plan.
2. Design the Test Scenarios/Cases.
3. Select the appropriate framework and write the tests.
4. Execute the test cases and report any defects found.
5. Track and re-test any defects.

Co-funded by the European Union

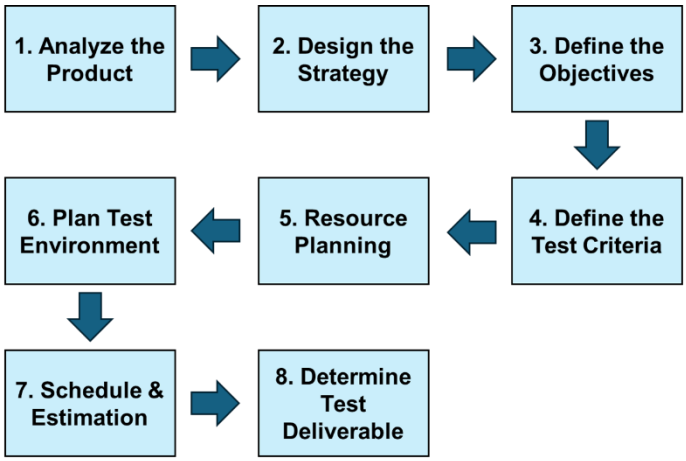
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

6. Repeat steps 3 and 4 until the integration is successfully completed.
7. (Optional) Choose a suitable automation framework to automate the tests.

5.2.3 Test Plan

A test plan is a document describing the scope, approach, resources and schedule of intended testing activities as per ISTQB definition. The test plan serves as a blueprint to conduct software testing activities as a defined process. The seven tests for a successful test plan as per IEEE 829 are shown in the figure below. Every step will be analysed and adapted specifically to the HEDGE-IoT purposes and needs.

FIGURE 25 TEST PLAN



Analyse the Software Component: This phase focuses on answering key questions such as "Who are the component users?", "What is the component used for?", and "How will the component function?".

Develop Test Strategy: During this critical phase, the testing scope is defined, the appropriate testing methods are selected, risks and issues are documented, and test logistics are established. In the first development phase of HEDGE-IoT, the focus will solely be on **Functional Testing**, excluding other types like Performance Testing. The selected testing methods for this phase are UI Testing, API Testing, and Integration Testing.

Define Test Objectives: The third step involves setting the test objectives, which are the overall goals for the test execution. At the initial development phase, these objectives may not be fully defined since technical requirements are still being developed.

Define Test Criteria: Test criteria are critical for assessing whether a test cycle can proceed. If a significant number of test cases (e.g., 30%) fail, the testing cycle is paused until the development team resolves the issues causing the failures. Once the issues are addressed, the testing cycle resumes. **Exit criteria** specify when a test phase is considered successfully completed, and in our case, a 95% pass rate for critical test cases will be set as the exit criterion.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Resource Planning: In this phase, the required resources, both human and system-related, are clearly defined to complete testing tasks. Each technical partner is responsible for determining the resources needed for their respective teams.

Plan Test Environment: This step involves setting up the software and hardware environment for executing test cases. In HEDGE-IoT, testing is planned to be conducted in an automated environment using Continuous Integration/Continuous Delivery (CI/CD) tools, specifically with a dedicated GitLab server.

Schedule and Estimation: In this phase, the entire project is broken into smaller tasks, and time estimates are assigned to each task.

Determine Test Deliverables: The final step is to define the test deliverables, which include all necessary documents, tools, and components that need to be created and maintained to support the testing effort.

5.3 Component Catalogue Template and System Interfaces

The aim of this section is to provide the methodological approach for the identification and definition of relevant subsystems and components as building blocks of the HEDGE-IoT technological platform, as well as their interdependencies. Input from all Technical Work packages at Task level will follow the template below:

TABLE 17 COMPONENT CATALOGUE TEMPLATE

Service (Software) Component	Functions	I/O data format	TRL & release plan	Software details	Integration with HEDGE-IoT Data Space
Overall description	Identification of the description of the functions (e.g., optimization calculation functions, data processing, ML/AI)	Description of I/O data format / APIs, data transfer architecture, how to run the service	TRL level for the different technical releases (M13, M20, M29)	Use of third-party software (and licenses), programming language, DB, docker, job scheduling, etc.	Describe level of integration and development time-schedule

Moving forward towards the 2nd technological release, this live document will catalogue all software components and their related information.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

5.4 Integration Plan and Roadmap

5.4.1 Generic Project Time Schedule

The implementation efforts along with the integration process will be split into three distinct development phases according to the project time-plan, taking into consideration the WP4 deliverables and milestones along with the actual technical WPs development.

TABLE 18 WP4 DELIVERABLES & MILESTONES

Deliverables & Milestones		
Phase A: First Integration		
MS4	HEDGE-IoT Interoperability Framework and Integrated Solution – First Release	M15
D4.1	HEDGE-IoT Interoperability Framework and Integrated Solution (First release)	M15
Phase B: Intermediate integration		
MS6	HEDGE-IoT Interoperability Framework and Integrated Solution – Intermediate Release	M21
D4.2	HEDGE-IoT Interoperability Framework and Integrated Solution (Intermediate release)	M21
Phase C: Final integration		
MS8	HEDGE-IoT Interoperability Framework and Integrated Solution – Final Release	M32
D4.3	HEDGE-IoT Interoperability Framework and Integrated Solution (Final release)	M32

5.4.2 Integration Requirements

The integration process will be guided by the preliminary functional requirements for HEDGE-IoT, which will be defined throughout the project's implementation. These requirements will serve as the foundation for the development scope, alongside the specification of the Data Space as a unified platform. The initial requirements will focus on the following areas:

- Definition and review of general functional requirements
- Evaluation of pilot-specific functionalities based on business use cases
- Analysis of requirements for data integration and homogenization
- Examination of interoperability requirements
- Specifications for data access and usage control

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- Edge-Level Services requirements
- Edge-Level Operation requirements
- Computational orchestration requirements
- EDC building blocks and data services
- Legal and regulatory requirements

As a general principle, the functional requirements will be based on the analysis of the following:

- Business rules
- Data exchange processes, including adjustments and cancellations
- Administrative functions
- Authentication and authorization levels
- Monitoring and audit tracking
- Data services and external interfaces
- Certification requirements and historical data
- Analytics and KPIs requirements

5.4.3 Plan Overview

TABLE 19 DEVELOPMENT & INTEGRATION PLAN

A/A	DESCRIPTION	START	END
A	First Development & Integration Phase	M6 31/06/24	M18 30/06/25
A.1	General Functional Requirements Definition - First version		M13 31/01/25
A.1.1	Functional Requirements definition & review		M12 31/12/24
A.1.2	Assessment of pilot specific functionalities based on business use cases		M13 30/01/23
A.1.3	Analysis of requirements on Data integration & homogenization		
A.1.4	Analysis of requirements for interoperability		
A.1.5	Data Access and Usage control specifications		
A.1.6	Analysis on Edge-Level Services requirements		
A.1.7	Analysis on Edge-Level Operation requirements		
A.1.8	Examination on Computational Orchestration requirements		
A.1.9	EDC building blocks and Data Services		
A.1.10	Legal and Regulatory requirements		
A.2	HEDGE-IoT Integrated Platform 1st version		M15 31/03/25
MS4	HEDGE-IoT Interoperability Framework and Integrated Solution – First Release		M15 31/03/25
A.2.1	Open Services Catalogue and App Store		M15 31/03/25
A.2.2	Interoperability Middleware - Open Data Connector		
A.2.3	Semantic Interoperability Enablers		
A.2.4	IoT Cloud/Edge System integration		

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

A.2.5	Cybersecurity considerations and AI safety		
Deliverable dependencies			
D2.1	Requirements on an IoT Cloud/Edge System for the Energy Ecosystem		M8 31/08/24
D2.2	Functional Specifications of the HEDGE-IoT system		M10 31/10/24
D3.1	HEDGE-IoT interfaces and tools for interoperability		M13 30/06/23
D3.3	HEDGE-IoT Technological Enablers (First release)		M13 30/06/23
D4.1	HEDGE-IoT Interoperability Framework and Integrated Solution (First release)		M15 31/03/25
A.3	Integration and Testing: First iteration		M18 30/06/25
A.3.1	Integration plan update		M15 31/03/25
A.3.2	Initial Lab Testing		M17 31/05/25
A.3.3	Ensure functional requirements compliance		M18 30/06/25
B	Second Development & Integration Phase	M15 31/03/25	M24 31/12/25
B.1	General Functional Requirements Definition - Final version		M18 30/06/25
B.1.1	HEDGE-IoT Functional requirements evolution towards second version		M18 30/06/25
B.1.2	HEDGE-IoT non-functional requirements analysis		M18 30/06/25
B.1.3	Concluding Contingency plan & Risk management		M18 30/06/25
B.2	HEDGE-IoT Integrated Platform 2nd version		M21 30/09/25
MS6	HEDGE-IoT Interoperability Framework and Integrated Solution – Intermediate Release		M21 30/09/25
B.2.1	Open Services Catalogue and App Store		M21 30/09/25
B.2.2	Interoperability Middleware - Open Data Connector		M21 30/09/25
B.2.3	Semantic Interoperability Enablers		M21 30/09/25
B.2.4	IoT Cloud/Edge System integration		M21 30/09/25
B.2.5	Cybersecurity considerations and AI safety		M21 30/09/25
Deliverables Dependencies			
D2.3	HEDGE-IoT Reference Architecture (First Release)		M18 30/06/25
D3.2	HEDGE-IoT interfaces and tools for interoperability 2		M19 31/07/25
D3.4	HEDGE-IoT Technological Enablers (Intermediate release)		M19 31/07/25

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

D4.2	HEDGE-IoT Interoperability Framework and Integrated Solution (Intermediate release)		M21 30/09/25
B.3	Integration and Testing: Second iteration		M24 31/12/25
B.3.1	Testing individual components		M22 31/10/25
B.3.2	Testing APIs & interfaces		M22 31/10/25
B.3.3	Integration of all components		M22 31/10/25
B.3.4	Integrated platform lab testing		M23 30/11/25
B.3.5	Integrated platform field testing		M23 30/11/25
B.3.6	Intermediate Hedge-IoT prototype demo testing		M24 31/12/25
C	Final Development & Integration Phase	M24 31/12/25	M36 31/12/26
C.1	Functional Requirements Evolution		M32 30/06/26
C.1.1	HEDGE-IoT Functional requirements evolution after testing		M31 31/07/26
C.1.2	HEDGE-IoT non-functional requirements final version		M32 31/08/26
C.2	HEDGE-IoT Integrated Platform 2nd version		M32 31/08/26
MS8	HEDGE-IoT Interoperability Framework and Integrated Solution – Final Release		M32 31/08/26
C.2.1	Open Services Catalogue and App Store		M32 31/08/26
C.2.2	Interoperability Middleware - Open Data Connector		M32 31/08/26
C.2.3	Semantic Interoperability Enablers		M32 31/08/26
C.2.4	IoT Cloud/Edge System integration		M32 31/08/26
C.2.5	Cybersecurity considerations and AI safety		M32 31/08/26
Deliverables Dependencies			
D2.4	HEDGE-IoT Reference Architecture (Final Release)		M28 30/04/26
D3.5	HEDGE-IoT Technological Enablers (Final release)		M30 30/06/26
D4.3	HEDGE-IoT Interoperability Framework and Integrated Solution (Final release)		M32 31/08/26
C.3	Integration and Testing: Final iteration		M36 31/12/26
C.3.1	Integration of all components		M34 31/10/26
C.3.2	Integrated platform lab testing		M34 31/10/26
C.3.3	Integrated platform field testing		M35

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

			30/11/26
C.3.4	Final HEDGE-IoT prototype pilot testing		M36 31/12/26

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

6 SECURITY AND PRIVACY

This section lays the foundations for Task 4.5, which ensures that cybersecurity, data privacy and AI trustworthiness is adequately managed in HEDGE-IoT demonstrators. It will also support the reference architecture of HEDGE-IoT on privacy and cybersecurity and explore the definition of HEDGE-IoT trustworthiness profiles.

6.1 State of art

6.1.1 Privacy

In the field of privacy, regulation and standardisation are evolving since the adoption of the GDPR [18], proposed by Article 29 data protection Working Party and the European Parliament becoming official in 2016 and entering into force from May 2018.

6.1.1.1 Regulation

Between 2011-2012, the EDPS (European Data Protection Supervisor) and Article 29 Working Party agreed and proposed the GDPR (General Data Protection Regulation) to the European Commission. In 2014, the European Parliament adopted the new regulation, which entered into force in May 2018. National data protection and privacy laws have been adapted to this EU Regulation, with minimal differences. It can be said that the transposition is a reality in most of the EU countries.

GDPR brings to the individuals more rights but also defines new roles in the data protection and data processing. Although the GDPR is a European Union regulation, non-EU organisations with offices in EU countries or that collect, store, and process the personal data of EU data subjects (individuals living in the EU) are still required to understand its implications and ensure they are in compliance.

GDPR 7 Guiding Principles

- *Lawfulness, fairness and transparency of the personal data processing.* Establish specification for determining the controller, the type of personal data subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing.
- *Purpose Limitation.* Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.
- *Data minimisation.* Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- *Accuracy*. Personal data shall be accurate, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- *Storage limitation.* Personal data shall be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed.
- *Integrity and confidentiality (security).* Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- *Accountability.* The controller shall be responsible for and be able to demonstrate compliance with.

New Rights introduced

- *Right to erasure (to be forgotten):* A data subject has the right to have personal data permanently deleted. (Art. 12, 17)
- *Right to data portability:* A data subject has the right to move, copy or transfer personal data from one data controller to another, in a safe and secure way, in a commonly used and machine-readable format. Wherever technically possible, this also includes the right to have the data transferred directly from one controller to another without the data subject having to handle the data. (Art. 12, 20)
- *Right to be informed:* Before data is collected, a data subject has the right to know how it will be collected, processed, and stored, and for what purposes. (Art. 12, 13, 14)
- *Right to access:* After data is collected, a data subject has the right to know how it has been collected, processed, and stored, what purposes. (Art. 12, 15)

New Roles introduced

- Data Protection Officer (DPO). This new position shall have the following tasks:
    - to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions.
    - to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits.
    - to provide advice when requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35.
    - to cooperate with the supervisory authority (Data Protection Authority).
    - to act as the contact point for the supervisory authority on issues relating to processing.
- *Data Controller:* The data controller determines the purposes and the means by which personal data in processed. It could be an organization or joint-organizations.
- *Data Processor:* the one that processes the personal data on behalf of the controller. It could be a third party external to the controller. The duties of the processor towards the controller must be specified in a contract or another legal act. It could also be joint-organizations.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

From 2019 until nowadays, new regulations affecting Data Protection, Privacy and (Cyber) security have arrived, such as:

- Cybersecurity Act (2019) [19]
- Data Governance Act (2022) [20]
- NIS2 Directive (2022) [21]
- Data Act (2023) [22]
- AI Act (2024) [23]
- Cyber Resilience Act (CRA) (2024) [24]

The CRA (2024) continues the regulation started in 2019 (Cybersecurity Act) with the goal to achieve a high-level cybersecurity, cyber resilience and trust within the EU. NIS2 Directive (2022) aims to achieve a high common level of cybersecurity across the EU by improving the functioning of the internal market.

Data Act (2023) and Data Governance Act (2022) go in the direction of harmonizing access and use of data and specific data categories held by public sector bodies.

6.1.1.2 Standardisation

The Standardisation landscape is very wide but it can be narrowed, by taking into account, which ones are relevant for privacy and which could impact it:

- **IoT Security & Privacy:**
  - ISO/IEC 27400 Security and privacy guidelines for IoT
  - ISO/IEC 27402 – IoT security and privacy – device baseline requirements
  - ISO/IEC 27403 IoT security and privacy – guidelines for IoT domotics
  - NISTIR 8200 Interagency report on the status of international cybersecurity standardization for the Internet of Things
- **Privacy:**
  - Risk management:
    - ISO/IEC 29134 Guidelines for privacy impact assessment: a guide method for PIAs (Privacy Impact Assessments)
    - NISTIR 8062 Introduction to privacy engineering and risk management in federal systems.
- **Information systems:**
  - ISO/IEC 27002 for privacy information management – Requirements and guidelines.
    - Microsoft data protection/privacy mapping project
  - Lifecycle and ecosystems:
    - NIST Privacy Framework: the NIST methodology with different concepts.
    - ISO/IEC 27570 Privacy guidelines for smart cities: a base for the X-CCP methodology.
    - ISO/IEC 27556 User-centric framework for the handling of PII based on privacy preferences.

  Engineering:
    - ISO/IEC 27550 – Privacy engineering for system life cycle processes
    - ISO/IEC 31700 Privacy-by-Design for consumer and goods and services

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

        - ISO/IEC 27561 Privacy operationalisation model and method for engineering (POMME).
- **Cybersecurity:**
    - Risk Management:
        - ISO/IEC 27005 Information security risk management
    - SC 42 Artificial Intelligence:
        - ISO/IEC 23894 AI Risk management
    - Information systems:
        - ISO/IEC 27002 Information security controls
    - Lifecycle and ecosystems:
        - NIST Cybersecurity framework
        - ISO/IEC 27110 Cybersecurity framework development guidelines
- **Architecture:**
    - ISO/IEC 30141 IoT reference architecture
    - AIOTI reference architecture
- **Domains:**
    - IEC 62443 series
    - NIST 7628 guidelines for smart grid cyber-security
- **Trustworthiness:**
    - ISO/IEC 30141 IoT reference architecture - Trustworthiness view
    - ISO/IEC 30149 IoT trustworthiness principles
    - ISO/IEC 30147 Trustworthiness in IoT lifecycle processes
- Study on trustworthiness reference architecture
    - SC 42 Artificial intelligence:
    - ISO/IEC 24028 AI Trustworthiness
    - ISO/IEC 24368 Overview of ethical and societal concerns.

6.1.2 Cybersecurity

Cybersecurity is characterised by a dual nature with: a highly technical aspect involving security protocols or creating innovative attack techniques, and on the other broad policies applied to organisations through regulations. As the objective of the cybersecurity analysis on HEDGE-IoT is to raise partner awareness and build a secure ecosystem, this landscape will focus on the latter, mainly regulations and standardisation.

6.1.2.1 Regulation

The European Union is creating a regulatory framework aiming to raise awareness about cybersecurity issues and create an ecosystem where they are systematically considered in the development of products and services. To this end, the EU has issued the following regulations:

- the Cybersecurity Act of June 2019 creates a framework for certification schemes under the purview of ENISA. The main schemes are EUCC (based on Common Criteria) and EUCS (for cloud services) which are not fully operational yet.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- the NIS2 directive highlights critical economic sectors (such as Healthcare, Energy, Transports or Telecommunications) which must be able to disclose cybersecurity incidents and coordinate with cybersecurity authorities to monitor their resolution.
- the Cyber Resilience Act of October 2024 provides requirements for hardware and software products manufacturers such as secure by default settings, vulnerability management and security updates.

6.1.2.2 Standardisation

To facilitate the deployment of cybersecurity best practices in organisations, extensive standardisation efforts have been made, like in the ISO 27000 series of standards published by ISO. Some important standards in this series are:

- ISO 27001 [28] detailing how to handle cybersecurity on an organisational level and building a security policy
- ISO 27002[29] detailing general organisational and technical cybersecurity controls
- ISO 27005 [30] detailing a risk analysis process allowing to define security objectives and manage risks associated to them

Complementing the formal standards, frameworks and knowledge bases are also published by different organisations.

As an example, NIST publishes the Cybersecurity Framework [31] which describes cybersecurity activities along 5 main pillars (Identify, Protect, Detect, Respond and Recover) linked together by governance activities. Another example is the STRIDE [32] taxonomy published by Microsoft which helps identify potential attacks during a risk analysis by classifying them into broad categories (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges).

On the other hand, MITRE uses data from actual vulnerabilities and attacks to produce knowledge bases like CWE, which presents potential weaknesses in software and hardware which can lead to exploitable vulnerabilities, and ATT&CK [33], which compiles attack techniques and strategies used by attackers targeting a system, with different objectives being highlighted depending on whether the attacker is doing reconnaissance for a further attack, covering their activities, actively trying to disrupt operations, etc.

6.1.3 Artificial intelligence trustworthiness

With the increase of functions in systems, their complexity also grows dramatically. Such a system may fail, cause harm, or expose Personal Identifiable Information (PII) (and worst, sensitive data) leading to serious consequences for individuals and undoubtedly a loss of confidence in the systems and/or organisations. As a result, building trustworthy systems has become both vital and challenging.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Trustworthiness is the "ability to meet stakeholder's expectations in a verifiable way" (ISO/IEC TS 5723 – section 3.1.1)

Note: Depending on the context or sector, and also on the specific product or service, data, technology and process used, different characteristics apply and need verification to ensure stakeholders' expectations are met.

Note: Trustworthiness is an attribute that can be applied to services, products, technology, data and information as well as to organizations.

The list of trustworthiness cross-cutting characteristics can vary according to the level of expectation. For instance, TABLE 20 presents both a simple and an extended vision with additional characteristics.

TABLE 20 EXAMPLE OF DIFFERENT TRUSTWORTHINESS CHARACTERISTICS

Expectation Level	Trustworthiness cross-cutting characteristics
Simple vision	Reliability Resilience Safety Security Privacy Transparency Reliability
Extended vision	Simple vision characteristics + Robustness Availability Integrity Controllability Quality Authenticity Usability Accountability

Definition of the Trustworthiness characteristics

IEC/ISO TS 5723 [34] defines the previously mentioned characteristics as follows below.

- Accountability: "state of being accountable"
- Authenticity: "property that an entity is what it claims to be"
- Availability: "property of being accessible and usable on demand by an authorized entity"
- Controllability: "property of a system that a human or other external agent can intervene in the system's functioning"
- Information security: "preservation of confidentiality, integrity and availability of information"
- Security: "resistance to intentional, unauthorized act(s) designed to cause harm or damage to a system"
- Integrity: "<data> property whereby data have not been altered in an unauthorized manner since they were created, transmitted, or stored"

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- Privacy: "freedom from intrusion into the private life or affairs of an individual"
- Quality: "<data> degree to which the characteristics of data satisfy stated and implied needs when used under specified conditions"
- Reliability: "<system> ability of an item to perform as required, without failure, for a given time interval, under given conditions"
- Resilience:
  "<system> capability of a system to maintain its functions and structure in the face of internal and external change, and to degrade gracefully when this is necessary"
  "<governance> ability to anticipate and adapt to, resist, or quickly recover from a potentially disruptive event, whether natural or man-made<governance> ability to anticipate and adapt to, resist, or quickly recover from a potentially disruptive event, whether natural or man-made"
- Robustness: "ability of a system to maintain its level of performance under a variety of circumstances"
- Safety: "property of a system such that it does not, under defined conditions, lead to a state in which human life, health, property, or the environment is endangered"
- Transparency:
  "<systems> property of a system or process to imply openness and accountability."
  "<information> open, comprehensive, accessible, clear and understandable presentation of information"
- Usability: "extent to which a system product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use"

Each trustworthiness characteristic is covered by one or many standards and verification of trustworthiness can be achieved by an assurance plan.

Main trustworthiness standards

Published:

- ISO/IEC 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence
- ISO/IEC 30147:2021 Information technology — Internet of things — Methodology for trustworthiness of IoT system/service
- ISO/IEC TS 5723:2022 Trustworthiness — Vocabulary
- ISO/IEC TS 30149:2024 Internet of Things (IoT) — Trustworthiness principles
- ISO/IEC 30141:2024 IoT Internet of Things (IoT) — Reference architecture - Trustworthiness view
- ISO/IEC 24368:2022 Information technology — Artificial intelligence — Overview of ethical and societal concerns

Under development:

- ISO/IEC AWI 31303 Trustworthiness — Overview and concepts
- Cen-cenelec JTC21 AI Trustworthiness framework

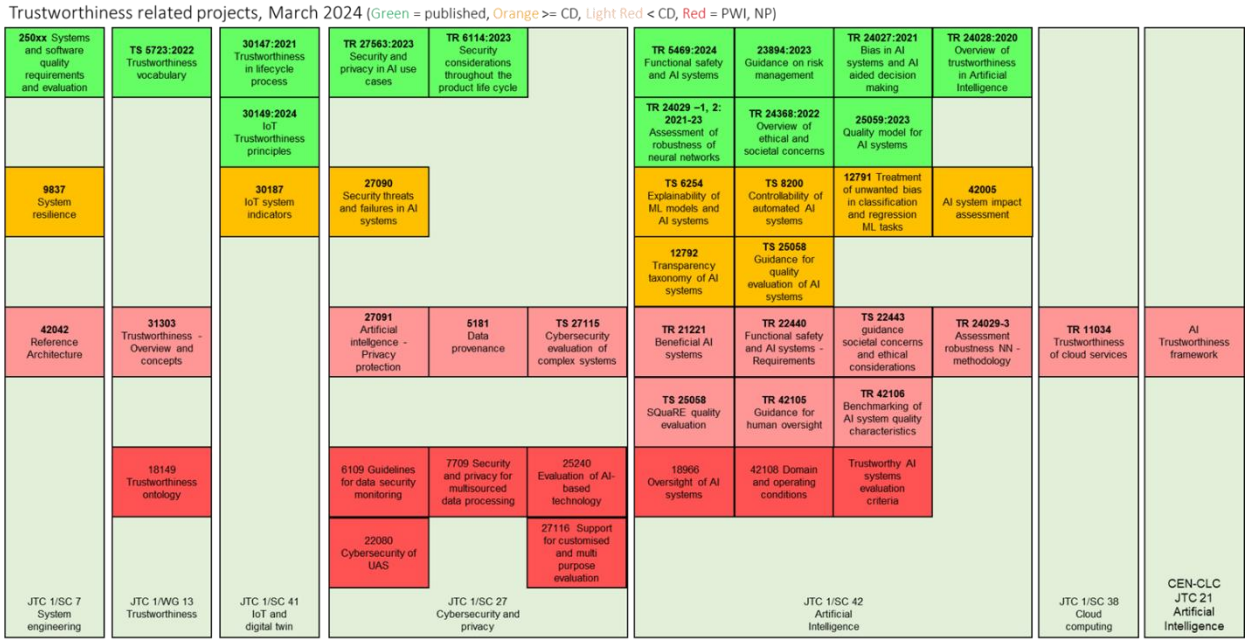
Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- ISO/IEC JTC 1/SC 42 - ISO/IEC 42005 Information technology – Artificial intelligence – AI system impact assessment

It then relies on a wide range of standards to deep dive into each trustworthiness characteristic. For example, AI risk management is discussed in Trustworthiness standards and then relies partly on ISO/IEC 23894 information technology on Artificial intelligence. Guidance on risk management is required to go further. It shows how trustworthiness characteristics can be fragmented and consequently covered by many standards as depicted below.

FIGURE 26 STANDARDISATION PERSPECTIVE ON TRUSTWORTHINESS (PREPARED BY ANTONIO KUNG (TRIALOG) IN THE CONTEXT OF A STANDARDISATION MEETING)



Trustworthiness assurance

Trustworthiness assurance refers to the set of processes, practices, and measures designed to verify that a system is trustworthy. It aims to validate the trustworthiness of a system.

The main challenge of trustworthiness assurance is:

- How to analyse the trustworthiness of a system during the design phase as well as after its realization? Assurance cases could be a solution.

From ISO/IEC 15026-2 Systems and software engineering — Systems and software assurance [35] defines an assurance case as an "auditable artefact that provides a convincing and sound argument for a claim on the basis of tangible evidence under a given context" and "assurance cases are generally developed to support claims in areas such as safety, reliability, maintainability, human factors, operability, and security".

Trustworthiness and AI

Trustworthiness is essential in AI systems, which influence critical decisions in domains such as energy, healthcare, finance, and security. Applying trustworthiness to AI ensures that systems are

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

reliable, fair, and secure. By applying trustworthiness principles, we ensure trustworthy AI can remain a responsible and valuable tool for society.

AI trustworthiness specific characteristics and definition

- Accountable: "answerable for actions, decisions, and performance" from ISO/IEC 22989 3.4.1. [36]
- Bias: "systematic difference in treatment of certain objects, people, or groups in comparison to others" from ISO/IEC 22989 3.4.4.
- Explainability: "property of an AI system to express important factors influencing the AI system (3.1.4) results in a way that humans can understand" from ISO/IEC 22989 3.4.6.
- Predictability: "property of an AI system that enables reliable assumptions by stakeholders about the output" from ISO/IEC 22989 3.4.7.
- Resilience: "ability of a system to recover operational condition quickly following an incident" from ISO/IEC 22989 3.4.9.
- Safety: "freedom from unacceptable risk" from ISO/IEC 22989 3.4.12.
- Transparency: "property of an organization that appropriate activities and decisions are communicated to relevant stakeholders in a comprehensive, accessible and understandable manner" from ISO/IEC 22989 3.4.14.

6.1.3.1 AI trustworthiness Regulation

AI is impacting industries, economies and societies at an unprecedented pace. In response to its rapid development, the European Union (EU) has taken an active approach to regulate AI. It aims to balance innovation with fundamental rights and safety. AI Act was defined specifically for AI systems but not for other regulations like GDPR or the CRA. However, some AI systems could fall under their scope.

Artificial Intelligence (AI) Act – 2024 [23]

The AI Act came into force on August 1st of 2024. This regulation is the first comprehensive legal structure of its kind in the world. It classifies the AI system based on the level of risk and implements strict requirements on high-risk applications. This regulation aims to ensure transparency, accountability and ethical AI, promoting confidence in the European market. It applies to all AI developed in and out of the EU market. In the context of HEDGE-IoT and European projects, it is important to mention that it does not apply to:

- AI systems specifically developed and put into service for the sole purpose of scientific research and development,
- any research, testing or development activity regarding AI systems prior to their being placed on the market or put into service,
- any systems released under free and open-source licences, unless they are placed on the market or put into service as high-risk AI system or as an AI system that falls under Article 5 (prohibited AI practices) or Article 50 (transparency obligations for providers and deployers of certain AI systems) of the AI Act.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

This regulation applies to AI systems providers, deployers, importers, distributors and affected persons that are located in the EU.

AI Act defines four risk categories: minimal risk, limited risk, high-risk, and unacceptable risk. TABLE 21 describes them and provides some insights about the associated requirements.

TABLE 21 AI ACT CATEGORIES

AI category	Description	Requirements
Minimal risk	AI systems that do not raise risks to safety or fundamental rights. Examples: - AI in video games - Spam filters - Recommendations based on AI for entertainment (e.g., movies)	No requirements but still recommended to follow general principles such as human oversight, non-discrimination, and fairness.
Limited risk	AI systems that do not raise risks to safety or fundamental rights but still require some transparency obligations to ensure that users are well informed about the nature and the function of an AI system. Examples: - Chatbots - Deepfake content	AI Act – Chapter 5 – Section 2 Transparency requirements: - Clear disclosure to the users - AI content should be labelled (e.g., deepfakes)
High-risk	AI Act – Chapter 3 - Article 6 and Annex 3 "AI systems that are intended to be used as safety components in products or that are themselves products covered by Union harmonization legislation shall be classified as high-risk." (Article 6, AI Act) It includes the following areas: Biometrics - Critical infrastructure - Education and vocational training - Employment, workers' management and access to self-employment - Access to and enjoyment of essential private services and essential public services and benefits - Law enforcement - Migration, asylum and border control management - Administration of justice and democratic processes	AI Act – Chapter 3 - Section 2 and 3 Respects of AI trustworthiness, the specifically mentioned characteristics are: - Risk management system (Article 9) - Data and data governance (Article 10) - Technical documentation (Article 11) - Record keeping (Article 12) - Transparency and provision of information to deployers (Article 13) - Human oversight (Article 14) - Cybersecurity (Article 15) - Accuracy (Article 15) - Robustness (Article 15) Additional requirements apply in Chapter 3 – Section 3. Here some examples:

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

	HEDGE-IoT highlight: critical infrastructure includes: "AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity." (AI Act – Annex 3)	- Quality management system (Article 17) - Documentation keeping (Article 18) - Keep automatically generated logs (Article 19) - Fundamental rights impact assessment - Submission of a request of information upon the registration of high-risk AI systems. The list of requested documents is available in AI Act - Annex 8 and 9.
Unacceptable risk	AI Act – Chapter 2 - Article 5 This article describes a long list of prohibited AI practices. These AI systems are banned due to their unacceptable risks to fundamental rights and democracy. Examples: - Social scoring - Manipulation AI systems - Mass biometric identification in public spaces	AI systems of this category are prohibited.

GDPR - General Data Protection Regulation (EU 2016/679) [18]

This regulation aims to regulate the collection and the use of personal data, including for AI systems. If an AI system processes irreversibly anonymised data, the GDPR does not apply. If the data are only pseudonymised, they could still be re-identifiable. In this case GDPR remains in force.

Cyber Resilience Act (CRA) – 2023 [24]

This regulation aims to ensure the cybersecurity of digital systems and software, including AI systems. It requires AI system providers to guarantee cybersecurity by design, to maintain security updates throughout the product's lifetime, to be able to prove the robustness against cyber-attacks, and to report security vulnerabilities and incidents to the European Cyber Agency (ENISA).

Digital Service Act (DSA) – 2022 [25]

This regulation aims to regulate digital platforms and their algorithms, including the ones based on or using AI systems.

6.1.3.2 AI trustworthiness standardisation

The standardisation of AI system is in full effervescence as can be seen in Figure 27, which is an overview of the standards published, under development or to be developed. Below a focus is done

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

on two key standards under development that will play an important role on the topics of AI trustworthiness and AI impact assessment.

Cen-Cenelec JTC21 AI trustworthiness framework [26]

Cen-Cenelec JTC21 is working under Commission's standardisation request to provide a harmonised standard named "AI Trustworthiness framework" supporting the AI Act and especially the requirements to ensure trustworthy AI systems. If this standard is validated and published, it could be used for conformity demonstration to the AI Act. This standard is still under development and covers today the following elements (non-exhaustive list):

- AI system lifecycle
- Risk management system for AI system
- Governance and quality datasets
- Record keeping through logging capabilities
- Transparency and explainability
- Human oversight of AI system
- Accuracy specifications of AI system
- Robustness specifications for AI system
- Cybersecurity specifications for AI system
- Quality management system for providers of AI systems including post-market monitoring process
- Conformity assessment for AI systems
- Requirements by lifecycle stages
- Requirements by AI Act Article

ISO/IEC JTC 1/SC 42 - ISO/IEC 42005 Information technology – Artificial intelligence – AI system impact assessment [27]

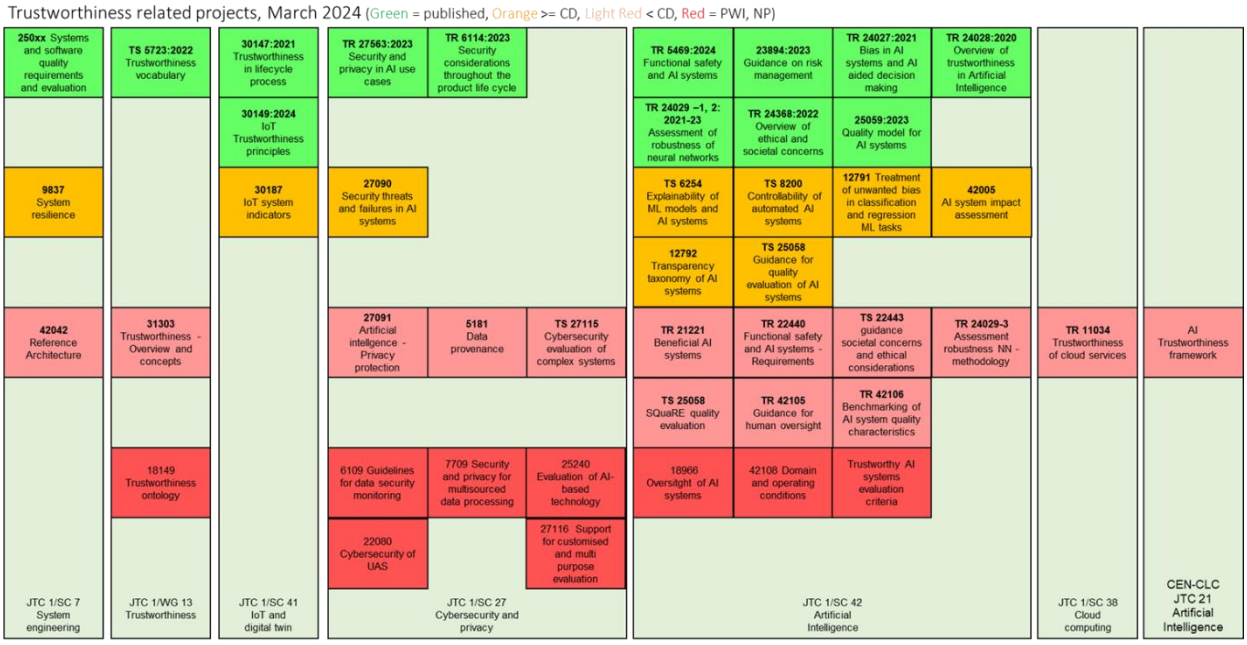
This standard is still under development. It provides guidance for organizations performing AI system impact assessments. It covers the following elements (non-exhaustive list):

- Implementing an AI system impact assessment process
- Documenting the AI system impact assessment
    - AI system information
    - Data information and quality
    - Algorithm and model information
    - Deployment environment
    - Relevant interested parties
    - Actual and potential impacts
    - Measures to address harms and benefits
- Example AI system impact assessment template

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

FIGURE 27 STANDARDISATION PERSPECTIVE ON AI (PREPARED BY ANTONIO KUNG (TRIALOG) IN THE CONTEXT OF THE SC27 AND SC24 LIAISON)



6.2 Task Strategy and Methodology

This chapter presents the strategy, the methodology and the activities to be carried out within task 4.5. This task aims to ensure robust cybersecurity, data privacy and AI trustworthiness through the project and its pilots.

To achieve this objective a Cross-Cutting Characteristics Plan (X-CCP) is under development and will be executed to address the targeted trustworthiness characteristics.

This plan will cover:

- Data privacy,
- Cybersecurity,
- AI Trustworthiness,
- Key Performance Indicators definition and
- A plan progress assessment.

X-CCP methodology objective:
Ensure that cybersecurity, data privacy and AI safety is adequately managed in HEDGE-IoT demonstrators, system-of-interest and its associated ecosystem.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

6.2.1 Cross-Cutting Characteristics Plan introduction

X-CCP introduction

This plan is based on an existing methodology developed by TRIALOG and successfully demonstrated in previous EU projects, e.g., InterConnect [37], Energica [38]. This method was initially named Privacy and Security Plan (PSP) and changed over time to Cross-Cutting Characteristics Plan (X-CCP) to consider additional characteristics like AI trustworthiness in HEDGE-IoT.

In the context of each project, the project and partners' needs are first identified. Then the plan is adapted, extended and customised accordingly to fit the project requirements before producing jointly with the pilots' partners the multi-domain preserving mechanisms which are the expected task 4.5 results. Indeed, each project has its own requirements, e.g., cybersecurity and privacy.

The concept is to perform a one-shot broad analysis of all characteristics targeted by the task for each pilot. The results of the analysis will support the project architecture definition on the same topics. Key Performance Indicators (KPI) will be defined by identifying the actual status and level of each pilot to later assess their progress. The implementation range during the project related to the identified multi-domain preserving mechanisms will obviously depend on the priorities and resources each pilot will consent to.

It is important to highlight X-CCP does not provide conformity to standards and/or regulations but supports pilots with knowledge and methodology to tend to conformity.

Based on the task scope this practice will also support the reference architecture definition at the privacy and cybersecurity level as well as the exploration of the HEDGE-IoT trustworthiness profiles.

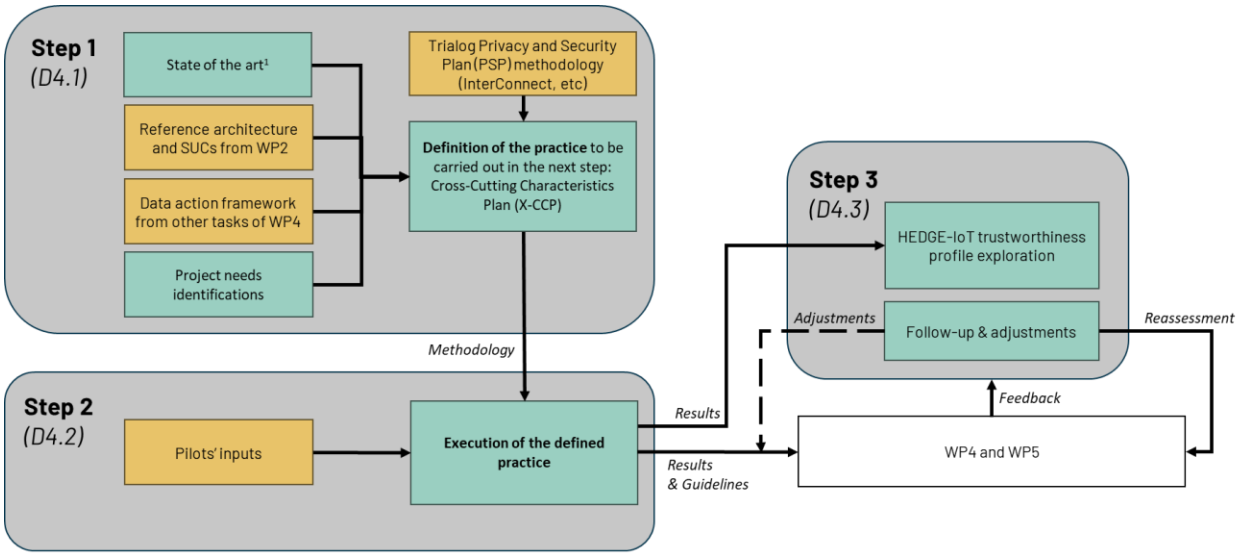
Figure 28 describes the task strategy and the three steps to go through.

- Step 1 refers to the preparation and definition of the practice based on state of the art, previous work in the project, pilots' answers to a questionnaire and the TRIALOG Privacy and Security Plan (PSP) methodology.
- Step 2 refers to the execution of the defined practice, also named Cross-Cutting Characteristics (X-CCP) in the project. For this step, the inputs of the pilots will be necessary.
- Step 3 refers to the HEDGE-IoT trustworthiness profile exploration and the adjustment of the action plan based on pilots' feedback and progress.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

FIGURE 28 TASK STRATEGY



[1]: ISO Standards (27xxx series), NIST guidelines for smart grid cyber-security (NISTIR 7628), EC recommendations on cybersecurity in the energy sector (SWD(2019)1240 final), EU network code on cyber security and existing work on AI trustworthiness (ISO/IEC/SC42).

The X-CCP practice expects to provide the following outputs to the project and pilots:

- Training sessions,
- results analysis reports for each pilot on privacy, cybersecurity and AI trustworthiness,
- pilots' maturity and security status and progress assessment,
- action plan for improvement,
- knowledge to tend to conformity based on the analysis reports,
- partners support (regular workshop and KPI monitoring) and
- tentative HEDGE-IoT Trustworthiness profile.

6.2.2 Project needs

A questionnaire was used to collect information from the pilots on their priorities and needs for the task. The structure of the questionnaire is the following:

1. Questionnaire information
    a. Filler's information
    b. Completion date
    c. Pilot name
2. Pilot information
    a. How many sub-pilot(s) do you have?
    b. What are the expected participants for each workshop?
    c. Have you already performed risk, privacy, cybersecurity, AI trustworthiness analysis for your system or pilot? Do you have sharable document(s) on this/these analysis/topics?
    d. Are the participants of the practice (to be executed by TRIALOG in T4.5 with the pilots' participation) experimented or trained on cybersecurity or privacy issues?

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

3. Project & Pilot needs
    a. What are the priorities on privacy, cybersecurity and AI trustworthiness for your pilot in the context of HEDGE-IoT?
    b. What are your needs and expectations on the privacy, cybersecurity and AI trustworthiness topics?
    c. According to you, what are the project needs on the privacy, cybersecurity and AI trustworthiness topics?
4. Privacy and Cybersecurity first overview
    a. Is your system handling Personally Identifiable Information (PII) data?
    b. Apart from tasks specifically dedicated to cybersecurity issues, what efforts are dedicated to implementing cybersecurity and privacy measures in the work to come?
    c. What cybersecurity and privacy features are already in place in your pilot?
    d. While developing/working/monitoring AI system(s) do you consider AI trustworthiness?
    e. Are there specific agreements in place within the existing pilots?
5. Other
    a. Do you have any other information to share?

Existing studies performed on the pilots

Almost all the pilots' replies show that they have not carried out analysis in the past. The few studies available are confidential.

Pilots priorities

TABLE 22 summarises the priorities of the pilots on privacy, cybersecurity and AI trustworthiness topics.

TABLE 22 SUMMARY OF THE PILOTS' PRIORITIES BASED ON QUESTIONNAIRE ASWERS

	Privacy	Cybersecurity	AI trustworthiness
Finnish pilot	Medium-High	High	High
Greek pilot	Medium-High	Medium-High	Medium-High
Italian pilot	High	High	Medium
Dutch pilot	Medium	High	Medium
Portuguese pilot	Medium	Medium	Low
Slovenian pilot	Low	Medium	Medium

Pilots' needs

Most of the partners raised the need for privacy, cybersecurity and AI trustworthiness analysis to assess the pilots and identify action plans for improvement during or beyond the project. TABLE 23 summarises the pilots' answers to their needs for this task. Training sessions and status assessments (security and maturity) were also mentioned.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

TABLE 23 SUMMARY OF PILOTS' NEEDS BASED ON QUESTIONNAIRE ANSWERS

	Finnish pilot	Greek pilot	Italian pilot	Dutch pilot	Portuguese pilot	Slovenian pilot
Training sessions	Yes		Yes		Yes	
Privacy analysis	Yes	Yes	Yes	Yes	Yes	Yes
Cybersecurity analysis	Yes	Yes	Yes	Yes	Yes	Yes
AI trustworthiness analysis	Yes	Yes	Yes	Yes	Yes	Yes
Control measures list		Yes	Yes	Yes	Yes	
Action plan for improvement	Yes	Yes	Yes	Yes	Yes	
Initial status assessment (security & maturity) and progress assessment later	Yes				Yes	
Implementation support			Yes			

Project needs raised by the partners

This questionnaire was a good opportunity for the pilots to brainstorm on the project needs regarding privacy, cybersecurity and AI trustworthiness.

Privacy:

- Compliance with GDPR and data protection regulations.
- Secure handling and storage of user data (encryption, anonymization).
- Clear privacy policies and user consent management.
- Network and operational data need to be private.
- End consumer data being accessed via authorized processes only.
- Dataspace and connector's deployment based on safe practices.

Cybersecurity:

- Secure authentication and authorization (e.g. role-based access control).
- Protection against common web threats (e.g., SQL injection, XSS, CSRF).
- Regular security audits, vulnerability assessments, and patching.
- Data security and secure API communication (HTTPS, OAuth, JWT).
- Secure connection between cloud and edge. Secure connection with IoT devices and other devices providing information about Power Quality etc.
- Horizontal analysis, assessment and testing applied to all pilots.

AI trustworthiness:

- Consideration of the trustworthiness requirements when developing AI systems.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- Information regarding the use of AI systems based on almost real-time interaction with users.
- Assessment AI in critical power grid/electricity applications.
- Reliable training sets.
- Replicability tests.

Specific agreements in place within some of the existing pilots:

- Data sharing and collection agreements
- Data analysis and integration agreement

The inputs collected through this questionnaire have supported the definition and adaptation of the X-CCP methodology that the next section will describe.

6.2.3 X-CCP methodology

This one-shot analysis should enable the pilots and solution providers to get a deep understanding of cybersecurity, privacy and AI Trustworthiness principles, based on relevant reference architectures, ISO standards (including Management standards & Management systems standards[39], 20889[40], 27xxx series [40][41][42][43][44][45][46] 29100 [47]29134[48], 31000 [49], 31700 [50], IEC standards 62443 series [52] ,NIST guidelines (NISTIR 7628 [53] and 8062 [54]) and privacy [55] and security frameworks, EC recommendations on cybersecurity in the energy sector (SWD (2019) 1240 final), LINDDUN privacy threat model [56]. STRIDE Threat modelling, MITRE Knowledge bases and the CNIL Privacy Impact Assessment Methodology.

TABLE 24, TABLE 25, TABLE 26 and TABLE 27 list the main references on which the X-CCP methodology is built. The other references above are used to support the technical discussions and results.

TABLE 24 MAIN REFERENCES USED FOR THE PRIVACY METHOD ANALYSIS

Reference	Description
ISO/IEC 29134 – Privacy Impact Assessment Guidelines [48]	This standard provides guidelines and recommendations for conducting a Privacy Impact Assessment (PIA), from understanding the benefits, objectives, and targets of a Data Privacy Impact Assessment (DPIA) to how to conduct the PIA process (e.g., risk assessment, risk treatment).
ISO/IEC 31000 – Risk management – Guidelines [49]	This standard provides guidelines supporting the risk management method used within the PSP.
LINDDUN methodology [56]	It is a PIA method that provides support to the elicitation and mitigation of privacy threats. LINDDUN: Linking, Identifying, Non-repudiation, Detecting, Data Disclosure, Unawareness, and Non-compliance.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

TABLE 25 MAIN REFERENCES USED FOR THE CYBERSECURITY METHOD ANALYSIS

Reference	Description
ISO/IEC 27005 – Information security risk management **[30]**	This standard provides the method and the structure for risk analysis.
ISO/IEC 27002 – Code practice for information security controls **[29]**	This standard provides a list of information security controls to be used during the risk analysis.
STRIDE method **[32]**	Methodology to analyse threats. It identifies and categorizes security threats that can lead to a cybersecurity breach of the target system.

TABLE 26 MAIN REFERENCES FOR AI TRUSTWORTHINESS ANALYSIS METHOD

Reference	Description
ISO/IEC JTC 1/SC 42, - ISO/IEC 42005 Information technology – Artificial intelligence – AI system impact assessment [27], under development	This standard provides a methodology and a template for AI system impact assessment.
ISO/IEC JTC 1/SC 42 - ISO/IEC TR 24028 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence**[57]**, 2020	These standard surveys: • approaches to establish trust in AI systems, • engineering pitfalls and associated threats and risks, • approaches to assess trustworthiness characteristics.
Cen-Cenelec JTC21 – AI Trustworthiness framework **[26]** under development	This standard provides the structure for AI trustworthiness analysis.
ISO/IEC JTC 1/SC 42 - ISO/IEC 23894 Information technology — Artificial intelligence — Guidance on risk management**[58]**, 2023.	This standard provides the methodology and structure for AI risk analysis.

The AI Trustworthiness module is based on a multitude of standards covering all AI Trustworthiness characteristics however, the four references in the table above are the starting points of the methodology.

TABLE 27 MAIN REFERENCES USED FOR THE KPI ASSESSMENT METHOD ANALYSIS

Reference	Description
IEC 62443 series – Part 2-1: Security program requirements for IACS asset owners **[52]**	The KPIs methodology to assess security and maturity levels is described in this standards series.

Co-funded by the European Union

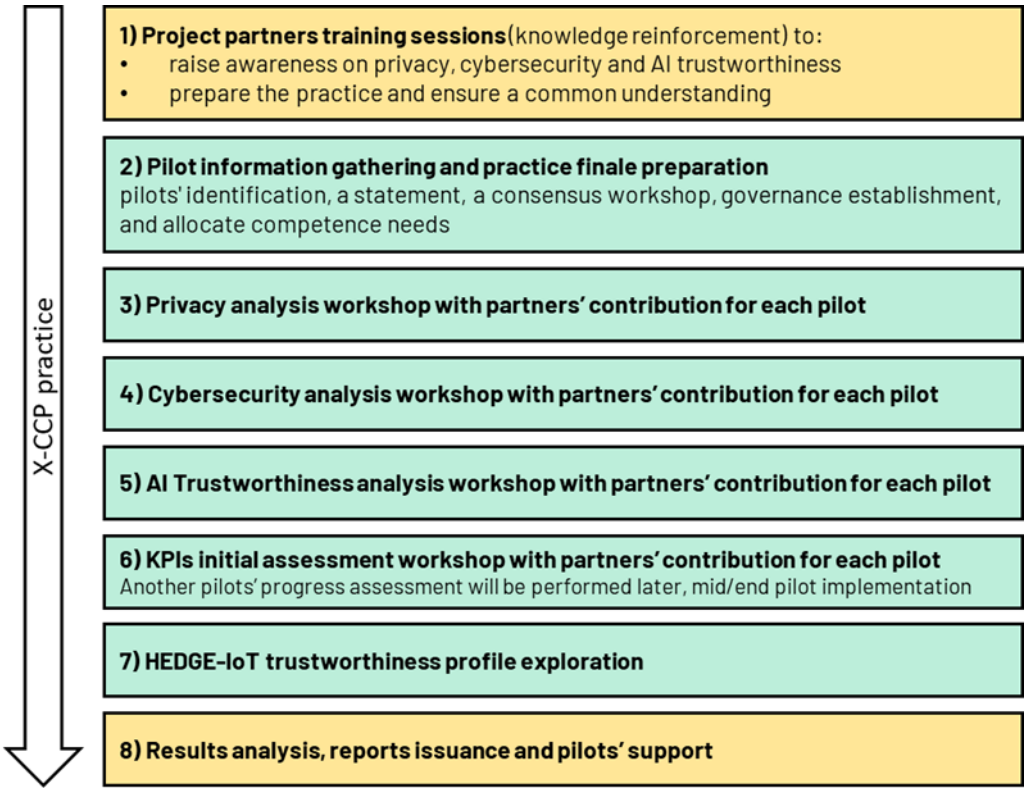
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

IEC 62443 series - Part 2-2: IACS protection levels **[52]**	Based on these two levels it defines the Security Program Rating (SPR) with a table.

X-CCP practice structure

The X-CCP methodology will be structured as described in FIGURE 29.

FIGURE 29 CROSS-CUTTING CHARACTERISTICS PLAN MAIN STEPS



Steps 1 to 6 constitute the X-CCP practice in HEDGE-IoT:

Project partners training sessions: Training sessions will be performed by TRIALOG to the task contributors to ensure a sufficient level of knowledge. The following subjects will be covered:

- Preparing a PSP
- Privacy analysis
- Security analysis
- AI trustworthiness
- Privacy and security program KPI

Pilot information gathering and practice final preparation: This step focuses on collecting all the information needed for the following analysis. Pilots will have to provide some elements like pilot architecture and data flow diagram. The BUCs and SUCs will serve as a basis as well. X-CCP needed inputs:

- BUCs & SUCs

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- Pilot architecture
- Data flow diagram (DFD)
- Past privacy and security analysis
- Data action framework
- Regulation and standardisation
- TRIALOG Privacy and Security Plan (PSP) methodology
- Pilots' participation and contribution during the task and workshops

The most extensive steps (3, 4 and 5) consist of a series of focused workshops for each pilot, gathering TRIALOG's experts and pilot leaders. These workshops enable targeted security, privacy and AI trustworthiness analysis to be carried out for each pilot. The number of workshops to be organised for each pilot will depend on the complexity of their Information and communication technologies (ICT) infrastructure. The participants of the workshop should have a good vision of the overall pilot architecture and use cases to be able to identify threats and breaches at the whole system level.

The KPIs definition is important as it will ensure an efficient monitoring of the improvements based on the results of the first analysis.

Steps 7 and 8 will build tangible results for HEDGE-IoT based on the previous steps outputs.

HEDGE-IoT trustworthiness profile exploration: This step will explore how the HEDGE-IoT trustworthiness profile could be defined, describing the most relevant characteristics/requirements needed. This work will be based on the RA (incl. components list) and standards (e.g. ISO/IEC 30149 - Internet of Things (IoT) Trustworthiness principles). This study will also support the HEDGE-IoT reference architecture development based on the trustworthiness profile and workshops results.

The last step covers the analysis of the results, the report issuance and the support to the pilots in the implementation of the recommendations and monitoring the progress thanks to the KPIs.

6.3 Task Schedule

Figure 30 describes the tentative schedule for task T4.5 following the methodology presented above.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

FIGURE 30 T4.5 Schedule

Tasks	2024				2025												2026								
	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
4.5 - Cybersecurity considerations and AI safety [M10-M32]																										
Step 1 - Preparation and definition of the Cross-Cutting Characteristics Plan (X-CCP)																										
Creation of the AI trustworthiness analysis module																										
Project needs identification																										
Definition of the practice methodology																										
Preparation and implementation of the practice																										
Deliverable 4.1 writing					Ds		D																			
Step 2 - Execution of the practice																										
Execution of the previously defined practice (X-CCP)																										
Deliverable 4.2 writing											Ds		D													
Step 3 - Follow-up & adjustments/corrections																										
Finalisation of the practice execution																										
Adjustment of recomendations																										
HEDGE-IoT trustworthiness profile exploration and support to RA development																										
Reassessment of pilots' progress through KPIs previously defined																										
Deliverable 4.3 writing																						Ds		D		

Legend:

Ds: Deliverable structure issuance and validation with partners

D: Deliverable submission

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

7 CONCLUSIONS

The initial release of the HEDGE-IoT interoperability framework marks a pivotal milestone towards establishing a secure, scalable, and interoperable ecosystem for IoT and cloud environments. This deliverable has outlined the foundational elements developed within WP4, addressing key aspects such as data connectivity, service discovery, semantic interoperability, security, and IoT integration. These components collectively form the backbone of seamless operation of data-driven AI services across diverse infrastructures in HEDGE-IoT.

One of the standout achievements in this phase is the creation of a Minimum Viable Product (MVP) for the interoperability framework, built around the Eclipse Dataspace Connector (EDC). This release introduces a functional data transfer layer – based on the Minimum Viable Dataspace (MVD) repository - that ensures secure and controlled data exchange between providers and consumers. Future iterations will enhance the connector's functionality, incorporate the Template Basic repository for customized distribution, and achieve full compliance with stringent security and data sovereignty standards.

Complementing this, the App Store and the Open Services Catalogue has been designed to streamline service discovery and registration across the HEDGE-IoT ecosystem. It provides a standardized approach for entities to register, manage, and integrate AI-driven services. Initial efforts have focused on defining the architecture and API functionalities of the catalogue. Future work will expand its capabilities, enhance automation, and integrate advanced service metadata to drive interoperability.

The semantic interoperability framework represents another critical achievement, ensuring effective communication among heterogeneous IoT systems. Through standardized ontologies such as SAREF and IEC CIM, the framework establishes a unified vocabulary for data exchange - addressing fragmentation across infrastructure. Ongoing efforts aim to refine data modelling techniques and broaden compatibility with additional semantic platforms and interoperability standards.

Cybersecurity and privacy are central to the HEDGE-IoT architecture. This deliverable outlines mechanisms for secure trusted data-sharing and compliance with European data protection regulations. Key measures include secure transmission protocols, access control policies, and tailored risk assessment methodologies. Moving forward, efforts will focus on strengthening end-to-end encryption, implementing fine-grained identity management, and integrating advanced risk monitoring tools to reinforce ecosystem security.

Finally, the IoT Edge/Cloud integration strategies outlined in this deliverable provide a framework for efficiently managing distributed computing resources. These strategies strike a balance between performance, scalability, and real-time processing. Subsequent phases will refine orchestration mechanisms, optimize workload distribution, and enhance AI-driven resource management within the edge-cloud continuum.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

In the next development cycle the focus will shift towards refining these components, resolving identified limitations, and progressing towards a fully integrated, production-ready solution. WP4 has laid a solid and robust foundation for an interoperable, secure, and scalable data-sharing ecosystem, aligned with the broader objectives of HEDGE-IoT and supporting the next generation of AI-powered IoT applications.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

8 REFERENCES

[1] ETSI TR 103 375, *"SmartM2M; IoT Standards landscape and future evolutions," 2016. [Online]. Available:https://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf*. [Accessed 2025].

[2] S. Widergren, D. Hardin, R. Ambrosio, R. Drummond, E. Gunther, G. Gilchrist and D. Cohen, "GridWise Interoperability Context-Setting Framework," 2008.

[3] Gruber, Thomas R. "Toward principles for the design of ontologies used for knowledge sharing?." International journal of human-computer studies 43.5-6 (1995): 907-928.

[4] International Data Spaces Association (IDSA), *Position Paper: Energy Interoperability Framework*, version 0.9.

[5] "IEC 61968-13:2021." Accessed: Feb. 20, 2025. [Online]. Available: https://webstore.iec.ch/en/publication/34213

[6] "IEC 61968-11:2013." Accessed: Feb. 20, 2025. [Online]. Available: https://webstore.iec.ch/en/publication/6199

[7] "IEC 61970-301:2020." Accessed: Feb. 20, 2025. [Online]. Available: https://webstore.iec.ch/en/publication/62698

[8] "IEC 61970-452:2021." Accessed: Feb. 20, 2025. [Online]. Available: https://webstore.iec.ch/en/publication/64844

[9] "IEC 61970-456:2021." Accessed: Feb. 20, 2025. [Online]. Available: https://webstore.iec.ch/en/publication/68054

[10] "IEC 61970-552:2016." Accessed: Feb. 20, 2025. [Online]. Available: https://webstore.iec.ch/en/publication/25939

[11] "IEC 61970-600-1:2021." Accessed: Feb. 20, 2025. [Online]. Available: https://webstore.iec.ch/en/publication/63866

[12] "IEC 61970-600-2:2021." Accessed: Feb. 20, 2025. [Online]. Available: https://webstore.iec.ch/en/publication/63867

[13]] "Common Information Model Primer: Tenth Edition." Accessed: Feb. 20, 2025. [Online]. Available: https://www.epri.com/research/products/000000003002029927

[14] JRC CoC ESA Website https://ses.jrc.ec.europa.eu/development-of-policy-proposals-for-energy-smart-appliances

[15]INT:NET project https://intnet.eu/

[16] Chy, T.M.R.H. et al. (2025). Design of an Ontology-Driven Constraint Tester (ODCT) and Application to SAREF and Smart Energy Appliances. In: Tiwari, S., Villazón-Terrazas, B., Ortiz-Rodríguez, F., Sahri, S. (eds) Knowledge Graphs and Semantic Web. KGSWC 2024. Lecture

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Notes in Computer Science, vol 15459. Springer, Cham. https://doi.org/10.1007/978-3-031-81221-7_13

[17] Presentation done by Trialog during the meeting to the JRC https://ses.jrc.ec.europa.eu/sites/default/files/2024-10/4.1_trialog_iop_standards_coc_ontology_tester_antonio_kung.pdf

[18] European Union, General Data Protection Regulation (GDPR):

[19] Regulation (EU) 2016/679, 2016. European Union, Cybersecurity Act - Regulation (EU) 2019/881.

[20] European Union, Data Governance Act, 2022.

[21] European Union, NIS 2 Directive (Directive (EU) 2022/2555), 2022.

[22] European Union, Data Act, 2023.

[23] European Commission, *AI Act: Regulation of the European Parliament and of the Council*, 2021.

[24] European Commission, *European Cyber Resilience Act (CRA)*, 2024.

[25] European Parliament and Council, Regulation (EU) 2022/2065, Digital Services Act, 2022.

[26] CEN-CENELEC JTC 21, AI Trustworthiness Framework.

[27] ISO/IEC JTC 1/SC 42, ISO/IEC 42005, Information Technology — Artificial Intelligence — AI System Impact Assessment.

[28] ISO/IEC 27001: Information Security Management Systems — Requirements, 2022

[29] ISO/IEC 27002: Information Security Controls, 2022

[30] ISO/IEC 27005: Information Security Risk Management, 2022

[31] National Institute of Standards and Technology (NIST), The NIST Cybersecurity Framework (CSF) 2.0, 2024

[32] Microsoft Corporation, STRIDE Threat Modeling Framework.

[33] MITRE Corporation, MITRE ATT&CK® Matrix.

[34] ISO/IEC JTC 1/SC 27, ISO/IEC TS 5723:2022 — Trustworthiness — Vocabulary, 2022.

[35] ISO/IEC JTC 1/SC 7: Document: ISO/IEC 15026-2 Systems and software engineering — Systems and software assurance

[36] ISO/IEC JTC 1/SC 42, ISO/IEC 22989: Information Technology — Artificial Intelligence — Artificial Intelligence Concepts and Terminology, 2022.

[37] interconnect : https://interconnectproject.eu/

[38] Energica : https://energica-h2020.eu/fr/

[39] ISO, Management System Standards, 2023. Available at: https://www.iso.org/management-system-standards.html

[40] ISO/IEC 20889:2018, Privacy Enhancing Data De-identification Terminology and Classification of Techniques, 2018. Available at: https://www.iso.org/standard/69373.html

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

[41] ISO/IEC 27701:2019, Security Techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management — Requirements and Guidelines, 2019. Available at: https://www.iso.org/standard/71670.html

[42] ISO/IEC TS 27570:2021, Privacy Protection — Privacy Guidelines for Smart Cities, 2021. Available at: https://www.iso.org/standard/71678.html

[43] ISO/IEC 27556:2022, Information Security, Cybersecurity and Privacy Protection — User-Centric Privacy Preferences Management Framework, 2022. Available at: https://www.iso.org/standard/71674.html

[44] ISO/IEC TR 27550:2019, Information Technology — Security Techniques — Privacy Engineering for System Life Cycle Processes, 2019. Available at: **https://www.iso.org/standard/72024.html**

[45] ISO/IEC CD 27561.2, Information Technology — Security Techniques — Privacy Operationalisation Model and Method for Engineering (POMME), Available at: **https://www.iso.org/standard/80394.html**

[46] ISO/IEC 27400:2022, Cybersecurity — IoT Security and Privacy — Guidelines, 2022. Available at: **https://www.iso.org/standard/44373.html**

[47] ISO/IEC 27559:2022, Information Security, Cybersecurity and Privacy Protection — Privacy Enhancing Data De-identification Framework, 2022. Available at: **https://www.iso.org/standard/71677.html**

[48] ISO/IEC 29100:2011, Information Technology — Security Techniques — Privacy Framework, 2011. Available at: https://www.iso.org/standard/45123.html

[49] ISO/IEC 29134:2017, Information Technology — Security Techniques — Guidelines for Privacy Impact Assessment, 2017. Available at: https://www.iso.org/standard/62289.html

[50] ISO 31000:2018 (en), Risk Management — Guidelines, 2018. Available at: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

[51]ISO 31700-1, Consumer Protection — Privacy by Design for Consumer Goods and Services — Part 1: High-Level Requirements. Available at: https://www.iso.org/standard/84977.html

[52] ISA/IEC 62443 Series of Standards. Available at: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[53] NISTIR 7628 Rev. 1, Guidelines for Smart Grid Cybersecurity. Available at: https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final

[54] NISTIR 8062, An Introduction to Privacy Engineering and Risk Management in Federal Systems. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

[55] Privacy Framework. Available at: https://www.nist.gov/privacy-framework

[56] LINDDUN Privacy Engineering. Available at: https://www.linddun.org/

[57] ISO/IEC TR 24028, Information Technology — Artificial Intelligence — Overview of Trustworthiness in Artificial Intelligence.

[58] ISO/IEC 23894, Information Technology — Artificial Intelligence — Guidance on Risk Management.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

APPENDIX 1 - OPEN SERVICE CATALOGUE

SERV-01 - Federated Learning for Energy Forecasting & Disaggregation		
a/a	***Field***	***Value***
	Service Provider	
1	Provider Name(s)	ICCS
2	Provider Contact(s)	
	BUC	
3	Related BUC_ID	
4	BUC Owner	
	Service Information	
5	Service ID	SERV-01
6	Service Name	Federated Learning for Energy Forecasting & Disaggregation
7	Service Description	This solution is designed to enhance energy management by providing accurate predictions of energy consumption and production, coupled with detailed energy disaggregation capabilities. It uses a decentralized horizontal federated learning approach to ensure privacy by keeping raw data localized on local IoT devices, such as smart meters, while enabling centralized model training. The approach leverages advanced time-series models like LSTM and BiLSTM for forecasting and NILM techniques for disaggregating energy consumption at the device level. It aligns seamlessly with the HEDGE-IoT interoperability framework, by adopting the project's open data connectors and semantic interoperability protocols.
8	Service Type	Decentralized energy forecasting and disaggregation (ML / Analytics)
9	Energy Domain	Electricity consumption and production forecasting (inc. device-level disaggregation)
	Data	
10	Data Profile	Inputs: • Time-series energy consumption (residential, device-specific) • Time-series energy production data • Weather data (temperature, humidity, etc.) • Contextual metadata (e.g. appliance types)

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

		Outputs: • User-level energy consumption and production forecasts • Disaggregated device-specific consumption timeseries
11	Data Format (Input)	• JSON • CSV
12	Data Format (Output)	• JSON
13	Data Availability	• Raw data remains on local devices • Only model updates are exchanged, minimizing bandwidth requirements. Updates or gradients are exchanged using MQTT • Secured with TLS
	Technical Specifications	
14	Software Tools	• Forecasting models: LSTM / BiLSTM • Disaggregation models: FHMM • Non-Intrusive Load Monitoring (NILM) techniques
15	Standard/protocol compliance	• MQTT • TLS
16	Deploying Environment	• Central server plus local nodes (e.g., Shelly 3EM meters)
17	Integration Requirements	• Integration with HEDGE-IoT interoperability framework via EDS Connector and semantic data standards • Data exchange through MQTT
18	Security Standards	
19	General Comments	• Current TRL: 2 (Technology concept formulated) • Target TRL: 7 (System prototype demonstrated in operational environment) • Pilot with ~100 residential apartments in Greece

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

SERV-02 - Vector Autoregressive Model for Energy Time Series Forecasting		
a/a	***Field***	***Value***
	Service Provider	
1	Provider Name(s)	INESC
2	Provider Contact(s)	
	BUC	
3	Related BUC_ID	BUC-PT-01
4	BUC Owner	
	Service Information	
5	Service ID	SERV-02
6	Service Name	Vector Autoregressive Model for Energy Time Series Forecasting
7	Service Description	This service employs a vertically federated learning approach to perform short-term energy predictions while preserving data privacy. By keeping data localized on devices and leveraging privacy-preserving encryption, the method allows data owners to collaboratively estimate VAR model coefficients without sharing sensitive information. The approach leverages VAR's multivariate component to extract relevant correlations with non-energy data, such as weather forecasts and humidity. LASSO regularization enables efficient variable selection and model optimization, addressing the high-dimensional nature of energy data. The integration with HEDGE-IoT's interoperability framework will be done via the adoption of the project's open data connector, ensuring secure and interoperable data exchanges.
8	Service Type	FL-based, energy forecasting
9	Energy Domain	Short-term energy consumption forecasting in residential or energy community settings
	Data	
10	Data Profile	Inputs: • Timestamps from time series • Anonymized local data (household energy consumption and related variables) • Random matrices for encryption • Rho and lambda hyperparameters for VAR model

Co-funded by the European Union
This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

		Outputs: • Encrypted coefficients (intermediate) • Final energy time series forecast for a specified horizon
11	Data Format (Input)	
12	Data Format (Output)	
13	Data Availability	• Data is kept on local devices • Only encrypted data / coefficients are shared • Privacy-preserving encryption techniques
	Technical Specifications	
14	Software Tools	• Python: LASSO-VAR approach and encryption • Cython
15	Standard/protocol compliance	• EDC Framework
16	Deploying Environment	• Lab environment simulation
17	Integration Requirements	• Integration with the Energy Community Management Platform • Adoption of EDS Connector for interoperability within HEDGE-IoT
18	Security Standards	
19	General Comments	• Current TRL: 4 (validated with large-scale data in a lab environment) • Expected TRL: 5 by M30 upon full implementation in the pilot • Future enhancements aim at scalability, parallelization, and integration with pilot environments

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

SERV-03 - Enhanced Network Management and Planning		
a/a	***Field***	***Value***
	Service Provider	
1	Provider Name(s)	UNZIG
2	Provider Contact(s)	
	BUC	
3	Related BUC_ID	
4	BUC Owner	
	Service Information	
5	Service ID	SERV-03
6	Service Name	Enhanced Network Management and Planning
7	Service Description	This service utilizes a combination of machine learning techniques to address anomaly detection, distributed energy resource (DER) capacity assessment, and forecasting of electrical quantities in secondary substations. Focused on improving planning and operational efficiency for DSOs, the service operates on edge devices to minimize reliance on centralized data storage and cloud computing. With all calculations performed close to the data source, this approach ensures low-latency decision-making and enhances data privacy. Interoperability is achieved through the PowerCIM tool for data exchange between energy stakeholders and by integrating with the project's interoperability framework.
8	Service Type	Edge-to-Cloud
9	Energy Domain	Planning and operation of distribution networks
	Data	
10	Data Profile	Inputs: • Weather data (wind speed, wind direction, temperature, solar irradiance, pressure, relative humidity, rain intensity) • Secondary Substation measurements (current, voltage, active power, reactive power) Outputs: • DER production/consumption values (intermediate) • Active power forecasts (intermediate)
11	Data Format (Input)	
12	Data Format (Output)	
13	Data Availability	• Data is sourced from IoT devices in secondary substations • Edge-level calculation avoids continuous data transfer to a

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

		central cloud • Substation identifiers are anonymized; location data is limited
	Technical Specifications	
14	Software Tools	• ML algorithms (anomaly detection, DER capacity detection, forecasting) • Central/cloud-based model training • Edge-level computing
15	Standard/protocol compliance	• Data exchange via MQTT • Data space connectors (EDS) for interoperability (EDC Framework) • Semantic interoperability with a specific CIM-based approach
16	Deploying Environment	• Tested in a controlled lab environment • Future operational deployment with edge-level computations
17	Integration Requirements	• Access to real-time measurements and weather data • Edge computing capability within secondary substations • Potential for central training before deployment to edge
18	Security Standards	
19	General Comments	• Current TRL: 4 (lab-tested with synthetic data) • Target TRL: 7 with full operational environment deployment by a DSO • Uses data from pilot demonstration sites to validate real-world performance

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

SERV-04 - DTR-DLR on the Edge		
a/a	***Field***	***Value***
	Service Provider	
1	Provider Name(s)	JSI
2	Provider Contact(s)	
	BUC	
3	Related BUC_ID	BUC-SI-0 • SUC-SI-01.1 • SUC-SI-01.2
4	BUC Owner	
	Service Information	
5	Service ID	SERV-04
6	Service Name	DTR-DLR on the Edge
7	Service Description	is an edge service that utilizes dynamic thermal rating algorithms to optimize the capacity and operational efficiency of overhead lines and transformers by leveraging real-time weather and operational data. Using IoT devices like the maxx GW-4100 gateway, the service performs localized computations for ampacity, thermal states, and short-term forecasts, providing a contribution to decentralizing the grid. The service integrates the notion of interoperability through the SUMO bus, which uses standardized protocols (e.g., IEC 61850) to enable real-time data exchange with other grid components. This decentralized and interoperable approach reduces latency and ensures secure operation within DSO and TSO infrastructures.
8	Service Type	Machine learning-based, real-time dynamic rating (DTR, DLR) with edge computation
9	Energy Domain	Electricity distribution and transmission
	Data	
10	Data Profile	Inputs: • Weather data (wind speed, wind direction, ambient temperature, solar irradiance, pressure, relative humidity, rain intensity) • Operational data (current) • Validation data (skin temperature, top oil temperature) Outputs: • Ampacity (current)

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

		• Temperature • Time to overheat
11	Data Format (Input)	
12	Data Format (Output)	
13	Data Availability	• Edge-level collection from local weather stations and metering devices • user-level access controls and encryption • No dependence on external data sources for ampacity computation
	Technical Specifications	
14	Software Tools	• DLR simulation engine based on CIGRE, IEEE standards, DTR on a three-mass thermal model for transformers • ML-based local weather forecast for short-term predictions • Edge gateway (IoT maxx GW-4100) for real-time computation
15	Standard/protocol compliance	• SUMO bus with standardized communication protocols (e.g., IEC 61850) • Additional encryption on data channels
16	Deploying Environment	• Deployed on IoT maxx GW-4100 gateways (edge devices) • Central servers for aggregating data and training global ML models
17	Integration Requirements	• SUMO bus for data exchange with other grid components • Local weather station interface (API) • Local database for operational measurements
18	Security Standards	
19	General Comments	• Current TRL: 5 (tested in controlled environments) • Target TRL: 7 by project end (fully operational in real-world deployments) • Suitable for both DSOs and TSOs to optimize asset utilization in real-time

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

SERV-05 - Anomaly Detection and Predictive Maintenance on the Grid		
a/a	*Field*	*Value*
	Service Provider	
1	Provider Name(s)	VU
2	Provider Contact(s)	
	BUC	
3	Related BUC_ID	
4	BUC Owner	
	Service Information	
5	Service ID	SERV-05
6	Service Name	Anomaly Detection and Predictive Maintenance on the Grid
7	Service Description	This service is designed to identify anomalies and faults in the local grid through real-time analysis of streaming data from IoT devices. The AI algorithm of the service learns the nominal behavior of energy nodes through online learning, allowing it to adapt to new environments and detect anomalies in both structural and non-structural graph data. The service implements semantic interoperability by using the SAREF ontology combined with TNO's Knowledge Engine as a semantic data broker. By leveraging SAREF-compliant Smart Connectors, the service integrates with the HEDGE-IoT Interoperability Framework, facilitating transparent data exchange and ensuring compatibility with third-party dashboards.
8	Service Type	AI-driven anomaly/fault detection and predictive maintenance
9	Energy Domain	Local grid monitoring and maintenance
	Data	
10	Data Profile	Inputs: • Continuous stream of graph data (RDF format) describing IoT device states via TNO's Knowledge Engine Outputs: • A corresponding stream of RDF graphs containing anomaly/fault detection reports, error codes, and explanations
11	Data Format (Input)	• RDF
12	Data Format (Output)	• RDF

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

13	Data Availability	• Real-time analysis of current and past broadcast from registered energy nodes/IoT devices • Brokered by TNO's Knowledge Engine for data exchange
	Technical Specifications	
14	Software Tools	• Under development in Python • Uses RDF, SAREF, REST standards
15	Standard/protocol compliance	• SAREF • REST API
16	Deploying Environment	• Cloud-based (service + TNO's Knowledge Engine) • Edge sensors for data collection
17	Integration Requirements	• Compatible with TNO's Knowledge Engine for incoming/outgoing RDF graph data • Streams data in real-time via SAREF
18	Security Standards	
19	General Comments	• Current TRL: 3 • Expected to reach higher TRL once validated and containerized

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

SERV-06 - APIO IoT Platform		
a/a	*Field*	*Value*
	Service Provider	
1	Provider Name(s)	APIO
2	Provider Contact(s)	
	BUC	
3	Related BUC_ID	
4	BUC Owner	
	Service Information	
5	Service ID	SERV-06
6	Service Name	APIO IoT Platform
7	Service Description	This service is a cloud-native, multi-tenant platform designed for managing time-series data and supporting machine learning applications in the energy domain. It integrates edge devices like PGUIs (Power Grid User Interfaces) that aggregate, sign, and securely transmit data from the edge to the cloud, without running any local algorithms themselves. Moreover, the PGUIs power consumption will be estimated by analyzing the behavior of the SoC (System on Chip) under several conditions, ensuring that the energy consumption of edge devices stays low. Data privacy is ensured through encryption protocols (CHAIN2 and MQTTS), rotating credentials, and strict access controls, safeguarding the integrity of data throughout its journey. The integration with the HEDGE-IoT Interoperability Framework will be achieved by applying SAREF-based ontologies to the platform's data and by adopting the project's open data connectors.
8	Service Type	IoT data management and ML forecasting platform
9	Energy Domain	Time-series Energy Data Management
	Data	
10	Data Profile	Inputs: • Main Meter data (Active/Reactive Energy) • Storage data (SoC, Capacity, SelfConsumptionEnergy) • Sunmeter data (Irradiation) • EMS/Inverter data (Solar Power, Solar Energy, String currents/voltages, Module Temperature) Outputs:

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

		• Forecast data (Produced Energy, Absorbed Energy) • Time-series predictions (load or generation)
11	Data Format (Input)	• Parquet
12	Data Format (Output)	• Parquet • JSON
13	Data Availability	• Real-time collection from edge devices (PGUIs) • Securely transmitted via MQTTS to the cloud • Historical data retained for ML training and analysis
	Technical Specifications	
14	Software Tools	• APIO IoT Platform • Edge suite for data collection and secure forwarding (PGUIs) • ML models: Prophet, ARIMA, LSTM, TimeGPT/transformers • Object storage + Parquet file format
15	Standard/protocol compliance	• CHAIN2 • MQTTS • SAREF • EDC Framework (considered)
16	Deploying Environment	• Cloud-based IoT platform and centralized ML pipeline • PGUIs at the edge for data acquisition
17	Integration Requirements	• Adoption of SAREF-based ontologies for semantic data alignment • EDC Framework (considered)
18	Security Standards	• CHAIN2 • MQTTS
19	General Comments	• Current TRL: 4 (validated in a research environment) • Goal: Achieve TRL 6 by implementing a full ML pipeline and validating with real-time data • Low-maintenance PGUIs, already deployed in large-scale contexts (e.g., RomeFlex)

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

SERV-07 - Anomaly Detection and Fault Forecasting to Increase Distribution Network Resilience		
a/a	***Field***	***Value***
	Service Provider	
1	Provider Name(s)	VTT
2	Provider Contact(s)	
	BUC	
3	Related BUC_ID	
4	BUC Owner	
	Service Information	
5	Service ID	SERV-07
6	Service Name	Anomaly Detection and Fault Forecasting to Increase Distribution Network Resilience
7	Service Description	This service enhances grid resilience by analyzing high-resolution, real-time data streams from Intelligent Electronic Devices (IEDs) within substations. The service uses advanced deep learning to establish a baseline of the grid's normal status and uses a Convolutional Neural Network (CNN) as a primary anomaly detection model. A Deep Reinforcement Learning (DRL) model is used for fault forecasting, to identify deviations from the grid's normal state and predict the faults before they occur. By processing data locally on the edge devices, the service ensures data privacy and does not rely on central storage. To secure interoperability with grid management systems, the service uses IEC 61850 and open data standards and will also leverage the project's interoperability framework. Currently, the service is at TRL 4 having been validated using historical and synthetic data.
8	Service Type	AI-based anomaly detection and fault forecasting for distribution grids
9	Energy Domain	MV distribution network resilience
	Data	
10	Data Profile	Inputs (High Resolution Streamed Data: • Current (A) • Voltage (V) • Harmonics (Hz) Outputs:

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

		• Green/Red/Yellow indicator (Integer) • Triggered values (Text) • Trigger signal (Integer)
11	Data Format (Input)	• IEC 61850-9-2
12	Data Format (Output)	
13	Data Availability	• Edge-based local processing
	Technical Specifications	
14	Software Tools	• CNN models • Deep Reinforcement Learning Model • IEC 61850 protocol interface
15	Standard/protocol compliance	• IEC 61850 • Open data standards for interoperability with HEDGE-IoT framework
16	Deploying Environment	• Edge devices within substations, capable of real-time, high-resolution data processing • Central server (historical data, model training)
17	Integration Requirements	• Must interface with Real-Time Data Link (e.g. IEC 61850) • Compatible with existing SCADA/DSO systems
18	Security Standards	
19	General Comments	• Current TRL: 4 (validated with synthetic and historical data) • Targets real-time fault warning for MV feeders and substations • Next steps: develop initial models for real-time data, test with pilot demonstration site, integrate operator feedback for DRL self-learning

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

SERV-08 - Real-Time Congestion Management		
a/a	*Field*	*Value*
	Service Provider	
1	Provider Name(s)	TAU
2	Provider Contact(s)	0
	BUC	
3	Related BUC_ID	BUC-FI-02 • SUC-FI-02.03 •SUC-FI-02.04
4	BUC Owner	
	Service Information	
5	Service ID	SERV-08
6	Service Name	Real-Time Congestion Management
7	Service Description	This service is a tool to manage grid congestion by gathering real-time data from primary substations and using edge nodes with significant computational power. Its modular architecture is designed to facilitate the development of algorithms. The system integrates microservices for load and generation estimation, state estimation, and congestion management. By combining active and passive grid management approaches, the service enables grid operators to use flexibility resources effectively while improving grid observability. In terms of flexibility, the service adopts the Eclipse data space connector to ensure secure and interoperable data exchanges between edge nodes and the cloud. Moreover, its data is based on the IEC61850 standard.
8	Service Type	Edge Solution for real-time congestion management
9	Energy Domain	MV distribution networks congestion management for DSO
	Data	
10	Data Profile	Inputs: • Real-time IEC 61850 data (voltages, currents, sampled values) from primary substation and feeder merging units •Historical load and generation profiles •Market price data and FSP data Outputs: • Logging of real-time CM results into data storage • Congestion warnings or recommendations for operator

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

		visualization • Potential control signals if integrated with DSOs or FSPs
11	Data Format (Input)	
12	Data Format (Output)	
13	Data Availability	• Edge node at the primary substation obtains real-time substation data. • Cloud-hosted historical data, accessible via Eclipse Data Space Connector • FSP data for flexibility resources via secure data exchange
	Technical Specifications	
14	Software Tools	• Real-time data link for IEC 61850 • Microservices for load/generation estimation, state estimation, and CM • Edge-cloud data adapter (EDS)
15	Standard/protocol compliance	• IEC 61850 • EDC Framework
16	Deploying Environment	• Edge server located at/near the primary substation
17	Integration Requirements	• Cloud-edge connectivity via EDS • Visualization for operator decisions
18	Security Standards	
19	General Comments	• Currently at TRL 4 • Future steps involve data preparation, edge-cloud connection, microservices implementation, testing, and piloting

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

SERV-09 - EdgeConnect		
a/a	*Field*	*Value*
	Service Provider	
1	Provider Name(s)	INESC
2	Provider Contact(s)	
	BUC	
3	Related BUC_ID	BUC-PT-01
4	BUC Owner	
	Service Information	
5	Service ID	SERV-09
6	Service Name	EdgeConnect
7	Service Description	This service provides an ecosystem for stakeholders across the flexibility value chain, enabling integration, qualification and market participation, to unlock flexibility potential. The service facilitates onboarding and certification of users, registration and pre-qualification of flexible assets, sharing of flexibility needs, baselines and bids and activation and settlement of flexibility services, allowing consumers to actively participate in energy markets. EdgeConnect ensures data privacy with role-based data access, while having critical information anonymized. Service to service data exchange interoperability is guaranteed via the integration of the project's data space connector. Furthermore, semantic interoperability will be integrated using the approach defined in the project. Currently, the service is at TRL 6, having already been tested in a controlled environment in a different European project.
8	Service Type	Cloud-Based Platform for managing flexibility markets and operations
9	Energy Domain	Flexibility Services • demand response • grid management • aggregator
	Data	
10	Data Profile	Inputs: • Stakeholder and user registrations (e.g., owners, aggregators, DSOs, TSOs) • Flexible asset information (asset IDs, power capacities, connectivity, divisibility)

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

		• Flexibility needs, baselines, bids (UUIDs, time intervals, prices, quantities) • Market results and activation signals Outputs: • Bids status updates (accepted, rejected, etc.) • Activation instructions (flexibility setpoints) • Settlement and remuneration calculations • Logs and notifications regarding each transaction
11	Data Format (Input)	• JSON
12	Data Format (Output)	• JSON
13	Data Availability	• Data exchanged via an EDS connector for interoperability
	Technical Specifications	
14	Software Tools	
15	Standard/protocol compliance	• EDC Framework • OAuth 2.0
16	Deploying Environment	
17	Integration Requirements	• Must connect to external processes (market clearing, aggregator systems) • Requires data space connector for service-to-service data exchange • Optional integration with HEDGE-IoT's Knowledge Engine and semantic data frameworks
18	Security Standards	
19	General Comments	• Current TRL: 6 (tested in a controlled environment) • Target TRL: 7 by integrating bilateral agreement features, leveraging HEDGE-IoT interoperability, and demonstrating in large-scale pilots • Provides a single ecosystem for multi-stakeholder collaboration, bridging local energy communities and global markets

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

SERV-10 - Flexibility Optimization Service		
a/a	*Field*	*Value*
	Service Provider	
1	Provider Name(s)	ICCS / HENEX
2	Provider Contact(s)	
	BUC	
3	Related BUC_ID	
4	BUC Owner	
	Service Information	
5	Service ID	SERV-10
6	Service Name	Flexibility Optimization Service
7	Service Description	This service is comprised of four modules that enable consumers to participate and place bids in local flexibility markets: 1) short and long-term forecast for energy demand and production; 2) calculation of incentives optimization and formulation of optimal bid; 3) communication of flexibility requests to consumers and 4) submission of bids in the local flexibility market. The service ensures data privacy by enforcing encryption and access control mechanisms like Attribute-Based and Role-Based Access Control (ABAC and RBAC). Currently, the service is at TRL 3 and the focus is on establishing the foundational architecture.
8	Service Type	AI-driven flexibility optimization for local energy markets
9	Energy Domain	Demand response and flexibility management
	Data	
10	Data Profile	Inputs: • Consumer energy consumption (kWh) • PV production data (kWh) • Battery capacities (kWh) and control levels (%) • Weather data (numeric / categorical) • Electricity prices (€/kWh) • Incentive limits (€/kWh) • Historical consumption / production data (kWh) • Acceptance probabilities (%) Outputs: • Forecasted production / consumption (kWh) • Flexibility offers (kWh, €) • Bid price (€/kWh) • Bid quantity (kWh)
11	Data Format (Input)	
12	Data Format (Outpout)	
13	Data Availability	• Data collected from IoT sensors and user inputs • Edge-cloud architecture with encryption and access

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

		control • Historical data and real-time streaming combined
	Technical Specifications	
14	Software Tools	
15	Standard/protocol compliance	
16	Deploying Environment	
17	Integration Requirements	
18	Security Standards	• ABAC • RBAC • Data encryption (storage + transport)
19	General Comments	• Current TRL: 3 (foundational architecture stage) • Targets improved demand/production forecasting, real-time incentive calculation, and local flexibility market bidding • Next steps include prototype implementation, synthetic data tests, validation with real pilot data

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

SERV-11 - Real-Time Reserve Market Simulator		
a/a	*Field*	*Value*
	Service Provider	
1	Provider Name(s)	NESTR
2	Provider Contact(s)	
	BUC	
3	Related BUC_ID	
4	BUC Owner	
	Service Information	
5	Service ID	SERV-11
6	Service Name	Real-Time Reserve Market Simulator
7	Service Description	This service is designed to emulate manual Frequency Restoration Reserve (mFRR) and automatic Frequency Restoration Reserve (aFRR) market operations, providing TSOs and Balancing Service Providers with a platform to test and optimize bidding strategies. The simulator validates bids, performs market simulations, and delivers outputs such as settlement curves and activation setpoints. The main advantage of the tool is enabling real-time market simulations with real consumer and TSO data, but without needing to comply with the full restrictions of the actual market. The tool will integrate HEDGE-IoT's interoperability framework by adopting the project's data space connector and performing data exchanges with the previously mentioned EdgeConnect service. Currently, the application is containerized using Docker and deployed in AWS
8	Service Type	Cloud-based reserve market simulation for mFRR/aFRR operations
9	Energy Domain	Balancing / Ancillary Services
	Data	
10	Data Profile	Inputs: • Bid documents (XML) from BSPs • Historical market data (from ENTSO-E Transparency Platform) • System and market parameters (reserve requirements, FAT, activation requests) Outputs: • Validation results for bids

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

		• Scheduling and activation signals for cleared bids • Simulation outcomes (revenues, imbalances, performance metrics)
11	Data Format (Input)	• XML
12	Data Format (Outpout)	• JSON
13	Data Availability	• Real-time simulation in the cloud (AWS ECS) • Containerized service accessible via REST endpoints • Integrates with EdgeConnect (HEDGE-IoT data space connector)
	Technical Specifications	
14	Software Tools	
15	Standard/protocol compliance	• RESTful API • EDC Framework
16	Deploying Environment	
17	Integration Requirements	• Must receive bids in XML • Exchanges data with EdgeConnect to broadcast or receive relevant market data • Access to ENTSO-E data for historical context
18	Security Standards	
19	General Comments	• Current TRL: 5 (validated in relevant environment) • Target TRL: 7 by real pilot demonstration • Ongoing updates are aFRR implementation, enhanced settlement, further integration in Portuguese demo

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

SERV-12 - Predictive Congestion Management		
a/a	***Field***	***Value***
	Service Provider	
1	Provider Name(s)	TAU
2	Provider Contact(s)	
	BUC	
3	Related BUC_ID	BUC-FI-02 • SUC-FI-02.01 • SUC-FI-02.02
4	BUC Owner	
	Service Information	
5	Service ID	SERV-12
6	Service Name	Predictive Congestion Management
7	Service Description	This service is composed of several micro-services for load, generation and grid state forecasting with the aim of enabling grid operators to procure flexibility. It uses 3 data sources: weather, market, and historical grid data to make predictive analyses and foster market participation. The service will implement the project's data space connector, therefore integrating its interoperability framework. Currently, the service is still at the design stage, as no implementation work has started yet.
8	Service Type	Cloud-based predictive congestion management and flexibility procurement
9	Energy Domain	Distribution grid operation and congestion management
	Data	
10	Data Profile	Inputs: • Weather data • Historical load and generation data • Grid data • Market data Outputs: • Predictive congestion analysis/results, logged to data storage for visualization • Potential flexibility requests issued to the nominal electricity market operator
11	Data Format (Input)	
12	Data Format (Outpout)	

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

13	Data Availability	• Cloud-based data processing • Edge-cloud connectivity via EDS Connectors
	Technical Specifications	
14	Software Tools	• Load/generation forecasting, state forecasting, predictive CM • Cloud-based approach requiring significant computational resources
15	Standard/protocol compliance	• EDC Framework
16	Deploying Environment	• Cloud-based micro-services architecture • Future synergy with real-time CM at the edge
17	Integration Requirements	• Weather API requests • Historical load/generation data • Edge-cloud interoperability for integrated CM
18	Security Standards	
19	General Comments	• Currently in design phase; implementation not started • Enhances existing real-time CM, forming a robust proactive + reactive approach • Will be simulated in the Finnish pilot (not fully piloted in real ops)

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

SERV-13 - Energy Community Management Service for Frequency Restoration Reserve		
a/a	***Field***	***Value***
	Service Provider	
1	Provider Name(s)	INESC
2	Provider Contact(s)	
	BUC	
3	Related BUC_ID	BUC-PT-01 • SUC-PT-01 • SUC-PT-02 • SUC-PT-03
4	BUC Owner	
	Service Information	
5	Service ID	SERV-13
6	Service Name	Energy Community Management Service for Frequency Restoration Reserve
7	Service Description	This service enables Renewable Energy Communities (RECs) to participate in Balancing Service Markets (BSMs) by provisioning mFRR and aFRR, using a set of modules to manage an energy community, including sizing, energy management and settlement. Since they act as natural aggregators, this service can coordinate a REC's members' flexibility while adhering to strict TSO requirements for frequency restoration reserve markets. The service will integrate HEDGE-IoT interoperability framework by adopting the project's data space connector, which will be used for interoperable data exchanges with other frequency restoration reserve market stakeholders. Currently, the frequency restoration reserve service is at TRL 2, while the underlying energy community management platform is at TRL 4, having been tested in a lab environment in the scope of another project.
8	Service Type	Energy community management andFR market participation
9	Energy Domain	REC operations and Balanving Services (mFRR/aFRR)
	Data	
10	Data Profile	Inputs: • Energy curve forecasts (JSON) • pre-qualified assets and REC members (JSON) • Activation setpoints received from the System Operator

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

		(JSON) • Settlement values from the SO (JSON) Outputs: • Baseline (flexibility baseline) (JSON) • Flexibility bid (offered to market) (JSON) • Metering data for settlement (JSON)
11	Data Format (Input)	• JSON
12	Data Format (Output)	• JSON
13	Data Availability	• Data stored in RECreation's database
	Technical Specifications	
14	Software Tools	• RECreation platform • Additional module for (mFRR/aFRR) provisioning
15	Standard/protocol compliance	• EDC Framework
16	Deploying Environment	• Cloud-based platform (RECreation) integrated with pilot IoT data • Lab tests (TRL 4 for the platform) • Eventually demonstrated in a full-scale Portuguese pilot
17	Integration Requirements	• Receives data from TSO, DSOs, aggregator services, and the real-time market simulator • Connects to EdgeConnect for discovering and integrating with external flexibility stakeholders
18	Security Standards	
19	General Comments	• Current TRL of Service: 2 • Planned TRL: 7 by M30 (demonstration in a large pilot with ~30 residential users) • Part of a broader platform (RECreation), which is at TRL 4 (tested in a different European project) and will likewise progress in maturity

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

SERV-14 - Computational Orchestration Framework		
a/a	***Field***	***Value***
	Service Provider	
1	Provider Name(s)	TUC
2	Provider Contact(s)	
	BUC	
3	Related BUC_ID	
4	BUC Owner	
	Service Information	
5	Service ID	SERV-14
6	Service Name	Computational Orchestration Framework
7	Service Description	This service ensures a streamline, homogenous and efficient cloud-to-edge computational effort, a swarm-based computation orchestration framework is developed in the project and its first specification is provided in this document. This framework has two main goals: 1) edge offloading for low-latency data processing for energy cloud services and 2) to orchestrate federated learning and distributed computing processes across the edge-fog-cloud continuum. Built on KubeEdge, the framework extends Kubernetes capabilities to edge environments, incorporating swarm-based heuristics to optimize resource allocation. Regarding data privacy, it integrates blockchain for secure and transparent service management, taking advantage of smart contracts and tokens for traceability. A monitoring system using Kube Prometheus will be established, supporting real-time infrastructure insights. It integrates HEDGE-IoT's interoperability framework by 1) considering the set of data-driven cloud services available in the project's App Store, 2) by using semantic annotation to expose edge devices computation capabilities and 3) by adopting the project's data space connector to perform interoperable data exchanges with the edge devices that also adopt it.
8	Service Type	
9	Energy Domain	
	Data	
10	Data Profile	Inputs: • Service specifications (from the Open Service Catalogue)

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

		• Node metrics (CPU, memory, network usage) collected by Node Exporter, cAdvisor, Prometheus • Local and global models for federated learning processes • Blockchain ledger entries (service tokens, smart contract references) Outputs: • Scheduling decisions and deployment logs (resource allocation, offloading) • Blockchain records of service deployments, migrations, token references • Federated learning model updates (aggregated, hyperparameter tuning results) • Monitoring alerts and performance dashboards (via Grafana)
11	Data Format (Input)	
12	Data Format (Output)	
13	Data Availability	• Real-time or near-real-time from edge to cloud • Node-limited metrics (edge or fog) aggregated centrally via Kube Prometheus
	Technical Specifications	
14	Software Tools	• KubeEdge • Swarm-based scheduling • Blockchain • Kube Prometheus (Node Exporter, cAdvisor, Prometheus, Grafana)
15	Standard/protocol compliance	• Kubernetes / KubeEdge • Blockchain-based traceability • EDC Framework
16	Deploying Environment	• Kubernetes • KubeEdge • Docker containers • Prometheus, Grafana
17	Integration Requirements	
18	Security Standards	• Smart contracts and blockchain-based resource tracking
19	General Comments	• Current TRL: 5, with plan to reach TRL 6 by the project's conclusion • Next steps include integration of swarm-based offloading, advanced hyperparameter optimization, and broader interoperability with HEDGE-IoT frameworks

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

HEDGE-IoT

Holistic Approach towards Empowerment of the Digitalization of the Energy Ecosystem through adoption of IoT solutions