interconnect

interoperable solutions
connecting smart homes,
buildings and grids

WP5 – Digital Platforms and Marketplace

D5.1

Concept, design and architecture of the interoperable marketplace toolbox

DOCUMENT INFORMATION

DOCUMENT	D5.1 – Concept, design and architecture of the interoperable marketplace toolbox
TYPE	Report
DISTRIBUTION LEVEL	Public
DUE DELIVERY DATE	09/30/2020
DATE OF DELIVERY	09/30/2020
VERSION	V1.0
DELIVERABLE RESPONSIBLE	SENSI
AUTHOR (S)	WP5 Partners
OFFICIAL REVIEWER/s	VLF, INESC TEC, VITO, SENSI, CYB, Trialog

DOCUMENT HISTORY

VERSION	AUTHORS	DATE	CONTENT AND CHANGES
0.1	Eliana Valles (Sensinov)	15/06/2020	Provided initial draft of the ToC
0.1.1	Sensinov, INESC TEC, VLF, TNO, VITO, cyberGRID	30/06/2020	Final ToC
0.2	Fabio Coelho (INESC TEC)	14/08/2020	Section 4 - Interoperability of platforms first draft
0.2.1	Eliana Valles (Sensinov)	14/08/2020	Section 2 - SoTA analysis - first draft
0.2.2	Fabio Coelho (INESC TEC), Milenko Tosic (VLF)	28/08/2020	Section 3 - Digital platform catalogue - first draft
0.3	Milenko Tosic (VLF)	02/09/2020	Section 5 - Interoperability framework specification - first draft
0.4	Eliana Valles (Sensinov) Milenko Tosic (VLF)	09/09/2020	Section 6 - Interoperability requirements for pilots - first draft
0.4.1	Amelie Gyrard (Trialog)	15/09/2020	Content for section 2, 5 and 6
0.4.2	Laura Daniele, Barry Nouwt (TNO)	15/09/2020	Content for section 5
0.5	Sensinov, INESC TEC, VLF, TNO, VITO, cyberGRID, Trialog	18/09/2020	Final draft for sections 2, 3, 4 and 5
0.5.1	Eliana Valles (Sensinov) Milenko Tosic (VLF)	21/09/2020	Final draft for sections 1, 6 and 7

0.5.2	(Sub-)Pilot leaders (INESC-TEC, VITO, Yncrea, GridNET, Planet Idea, Hyrde, VITO, Th!nk-E, 3E, OpenMotics, VUB, ThermoVault, EEBUS, Uni Kassel, IEE)	25/09/2020	Updates to section 6
1.0	Eliana Valles (Sensinov), Milenko Tosic (VLF), Fabio Coelho (INESC TEC)	28/09/2020	Integrated document ready for QA review
1.1	Eliana Valles (Sensinov), Milenko Tosic (VLF), Fabio Coelho (INESC TEC)	30/09/2020	Final version addressing QA comments - ready for submission

ACKNOWLEDGEMENTS

NAME	PARTNER
Ruben Baetens	3E NV
George Lyberopoulos	Cosmote
Cami Dodge-Lamm Andraž Andolšek	cyberGRID
Lieven Demolder	DUCOOP
José Manuel Terras	EDP DISTR
Josef Baumeister Ulrich Bartsch	EEBUS
Sebastian Wende Von Berg Lars-Peter Lauven	Fraunhofer
Donatos Stavropoulos	GRIDNET S.A.
Esteban Municio	IMEC
Fabio Coelho	INESC TEC
Stefano Fava	Planet Idea
Miguel Gonçalves	Schneider Electric Portugal
Eliana Valles Mahdi Ben Alaya	Sensinov
Amandio Ferreira	SONAE (Elergone)
Arnor Van Leemputten	TH!NK E
Pol Olivella	ThermoVault
Kristian Helmholt Laura Daniele Barry Nouwt Wilco Wijbrandi Joost Laarakkers	TNO
Amélie Gyrard Olivier Genest	Trialog
Lars Lauven Sebastian Wende-von Berg	UNI KASSEL
Dominic Ectors Jung Georg	VITO

Chris Caerts Enrique Rivero Puente	
Milenko Tosic Dragan Boscovic Ognjen Ikovic	VIZLORE LABS FOUNDATION
Kim Verheij (Hyrde)	VOLKERWESSELS ICITY B.V.
Dieter Roefs Thierry Coosermas	VUB
Andreas Georgakopoulos Vassilis Foteinos Ilias Romas	WINGS
Anaïs Galligani Stephane Vera	Yncréa Méditerannée

DISCLAIMER:

The sole responsibility for the content lies with the authors. It does not necessarily reflect the opinion of the CNECT or the European Commission (EC). CNECT or the EC are not responsible for any use that may be made of the information contained therein.

EXECUTIVE SUMMARY

This document introduces the deliverable D5.1 Concept, design and architecture of the interoperable marketplace toolbox. It is the first deliverable produced by WP5 - Digital Platforms and Marketplace [M7-M48]. The InterConnect Project received funding from the European Union's Horizon 2020 Research and Innovation program under the Grant Agreement (GA) number 857237.

This deliverable is part of the outcome of the work carried out in task T5.1 - Interoperability Framework and Service Store Architecture and specification [M7-M12]. It uses and develops the output and ongoing work of other WPs. Hence, this deliverable and its related task:

- **Compiles a catalogue of all digital platforms** brought by the project partners and used for realization of the project pilots and use cases;
- Utilizes the High-Level Use Cases developed within WP1 to **analyse and specify each (sub-)pilot's preliminary architectural implementation;**
- **Provides high level specification of the InterConnect interoperability framework and toolbox** based on the InterConnect's Secure Interoperable IoT Smart Home/Building and Smart Energy Reference Architecture (SHBERA);
- Contributes to the **specification of the preliminary Semantic Interoperability Layer**, developed within WP2, to identify the set of connectors and adapters required for ensuring interoperability on a syntactic and semantic level;
- Collaborates closely with WP3 on **defining the set of interoperable services and applications needed for pilot implementation** and validation of results, due to take place within WP7.

More precisely, D5.1 is a key entry point for all other tasks in WP5, namely:

- It **provides the overall framework used in T5.2 to develop, test, and deploy the interoperable endpoints**, based on the WP2's Secure Interoperable IoT Smart Home/Building and Smart Energy Reference Architecture;
- It **provides an overview of the security mechanisms to be integrated into the resulting framework**; further developed within T5.3, in charge of developing the actual security and privacy practices and policies for the interoperability framework;
- Provides an **overview of the project's P2P marketplace enablers**, which are the focus of T5.4;
- Defines a **set of tools to be made available within the project's Interoperable Framework**, that will later help T5.5 to define the scope of the open calls organized by WP8 as well as procedures for maintaining and managing the interoperability framework instantiated within project pilots.

These concepts and the methodology used to achieve these results are described in detail in the next sections.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS AND ACRONYMS

IoT	Internet of Things
API	Application Program Interface
B2B/C	Business-to-Business / Commerce
BEMS	Building Energy Management System
BUC	Business Use Case
CA	Consortium Agreement
CIM	Core Information Model
DMS	Distribution Management System
DR	Demand Response
DRES	Distributed Renewable Energy Sources
DSF	Demand Side Flexibility
DSO	Distribution System Operator
EDSO	European Distribution System Operators
ESCo	Energy Service Company
EV	Electric Vehicle
FHP	Flexible Heat and Power
GDPR	General Data Protection Regulation
HEMS	Home Energy Management System
HLA	High Level Architecture
IC	InterConnect
ICT	Information and Communication Technologies
IEC	Internal Electrotechnical Commission
ISO	International Organization for Standardization
KPI	Key Performance Indicators

M2M	Machine to Machine
MQTT	Message Queuing Telemetry Transport
NIST	National Institute of Standard and Technology
OneM2M	Global Standards Initiative for Machine to Machine Communication
SAREF	Smart Appliances Reference ontology
SCADA	Supervisory Control and Data Acquisition
SDK	Software Development Kit
SDO	Standards Development Organisations
SPINE	Smart Premises Interoperable Neutral-Message Exchange
TRL	Technology Readiness Level
TSO	Transmission System Operator
UC	Use Case

1. INTRODUCTION

1.1 WP5 OBJECTIVES

Within the InterConnect project, WP5 [M7 - M48] is in charge of carrying out the following activities and attaining the following objectives [26]:

- Establish interoperability between project stakeholders (platforms, services, IoT devices) by leveraging the ontologies, standards and designed specifications (T5.1);
- Demonstrate via the interoperability framework how several technologies can create a pluggable and transparent approach, while focusing in interfacing functionality-by-design (T5.2);
- Provide security-enabled and a privacy-by-design architecture, by considering a mix of cloud-enabled services and legacy systems (T5.3);
- Leverage on the interoperability toolbox to provide P2P marketplace enablers between stakeholders (T5.4);
- Lastly, provide a description of the platforms, devices and services to be exploited in WP7 (T5.5).

Moreover, this WP is responsible for designing the set of interoperable endpoints offered by InterConnect, using a scalable, and modular approach. These are based on the ontology and the Semantic Interoperability Layer specifications introduced in WP2 and should enable pilot-specific instantiations of the use cases developed within WP1. WP5 will also focus on the deployment of distributed ledger technologies, tailored for supporting distributed operations, like trading and transactions management activities by enabling the establishment of P2P marketplaces.

1.2 RELATION TO OTHER WPS

As shown in Figure 1, the work carried out in WP5 is based on the work carried out in other technical WPs, while at the same time providing key enablers for the same WPs, namely:

- From WP1, this WP utilizes the use case requirements to infer the architectural requirements the IC Interoperability Framework needs to consider;
- From WP2, which is itself primarily based on the work carried out in WP1, it utilizes and develops the concepts and functions (data models, interfaces, protocols, security and privacy requirements) introduced by the project's Secure Interoperable IoT Smart Home/Building and Smart Energy Reference Architecture;
- WP3 provides interoperable/adapted energy and non-energy services while WP5 provides to WP3 the service store specification and generic adapter for achieving semantic interoperability of the services;
- WP4 provides interoperable interfaces towards energy markets and especially DSOs while WP5 provides integration with the interoperability framework and services;

- WP5 will provide WP7 pilots with the interoperable digital platforms and supporting services necessary for realizing the project use cases, while the WP7 pilots will provide feedback necessary for updating and maintenance of the interoperability framework;
- WP5 will provide cascade funding projects/partners (WP8) with interoperability toolbox necessary for making their platforms and services interoperable with the interoperability framework and established pilots.

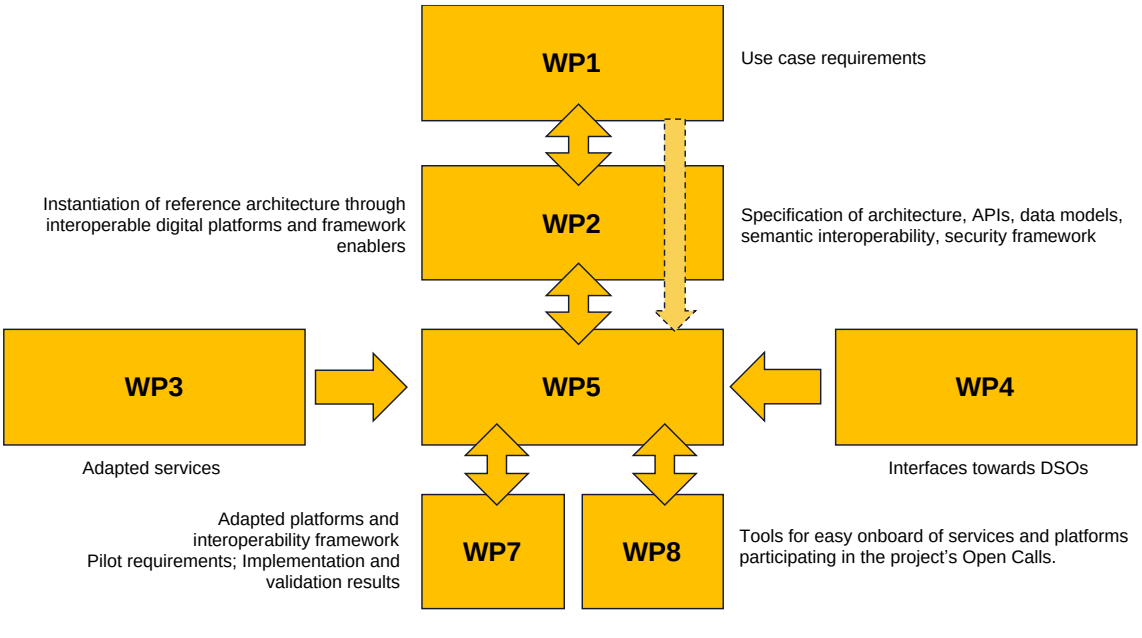


FIGURE 1 - RELATION OF WP5 TO OTHER WPS

1.3 D5.1 OBJECTIVES

This deliverable is part of the result of the work carried out by T5.1 - Interoperability framework and service-store architecture and specification [M7 - M12]. Its main objectives can be detailed as follows:

- Carry out a detailed analysis of the project's digital platforms and services and their interoperability capabilities and requirements;
- Provide an initial overview of each (sub-)pilot's architectural implementation;
- Specify Interconnect's Interoperability Framework and other interoperable resources and services;
- Contribute to the specification of the Semantic Interoperability Layer, by identifying the set of connectors and adapters required for ensuring interoperability on a syntactic and semantic level.

To attain these objectives, the present document introduces:

- An overview and analysis of other European initiatives that have provided a framework for cross-platform and cross-domain interoperability. To be considered, initiatives

providing a marketplace and a set of services and enablers to achieved interoperability were privileged.

- A catalogue containing a description of all digital platforms available within InterConnect's consortium. This catalogue is used as a basis for discussing the services, main properties and technologies that shall later be assembled and made interoperable.
- The specification of InterConnect's IC Interoperability Framework Architecture, identifying the set of tools and services which are required to enable existing digital platforms and services, operated by the consortium partners, to achieve semantic interoperability without an intermediary platform.
- An overview of each pilot and sub-pilot use cases, and more particularly those requiring cross-platform interoperability. Once identified, a first high-level overview of the type of data that will be collected and the commands that need to be supported for ensuring interoperability is established. This exercise is the first step towards identifying the actual architectural implementation for each (sub-)pilot, an ongoing activity within several WPs.

As stated earlier, this document can be viewed as an entry point for all other tasks and activities carried out in WP5. Therefore, the work presented here should not be considered static nor exhaustive, but rather the structure upon which all other WP5 tasks will further specify the IC Interoperability Framework.

1.4 DOCUMENT STRUCTURE

This document is the deliverable D5.1 Concept, Design and Architecture of the Interoperable Marketplace toolbox.

This introduction is part of **Chapter 1**. Its followed by the table of common definitions used within this document and other technical and non-technical deliverables published by the InterConnect project.

Chapter 2 - State of the Art, collects and analyses other European initiatives focused on creating an interoperable ecosystem, namely through the creation of a marketplace. It concludes by offering a synthetic view of each project's key features and compares them to the InterConnect project.

Chapter 3 - Digital Platforms Catalogue provides an overview of all the digital platforms available within the project. The results shown in this chapter are derived from an internal survey that highlights their general architectures and interoperability indicators.

Chapter 4 - Interoperability of platforms, analyses the elements presented in Chapter 3, namely the services offered by the digital platforms, their main functionalities, and their need (or not) for external services for supporting the SAREF ontology. It concludes by discussing the interoperability requirements for supporting ICT technologies and the availability of interfaces deployment capabilities for virtual and scalable environments.

Chapter 5 - InterConnect Interoperability Framework Architecture introduces the tools and services that will enable existing digital platforms, operated by the consortium partners, to achieve semantic interoperability. This chapter also provides the first overview of InterConnect's approach to semantic interoperability and the enabling technologies being considered for the project's future proof design.

Chapter 6 - Pilot's interoperability requirements and implementations strategy provides an overview of each pilot and sub-pilot's use cases, particularly those requiring cross-platform interoperability. The results shown in this chapter are derived from an internal survey that allowed us to collect the first high-level description of which type of data and commands are needed to implement the pilot's use cases. This chapter concludes by providing a first view on the architecture and early mapping of interoperability adapters.

1.5 GLOSSARY AND TERMINOLOGY

The glossary table will be maintained throughout the project. Presented definitions might be updated to accommodate project progress and key results from the technical WPs. New terminology definitions might be added in future deliverables.

CONCEPT	DEFINITION
InterConnect Framework-related terminology	
IoT platform (provider)	A collection of tools, software and hardware that makes it possible to connect 'things' (i.e. sensors, actuators or other types of physical devices) to the Internet. Also used for managing the connection to the devices as well as the devices themselves.
(The) IC Framework	A collection of tools and enablers that describes and prescribes how to interconnect devices from different vendors and services from different providers, enabling interoperability and the intelligent interaction of many devices and services from different domains (e.g. home automation, energy management, etc.). The IC Framework includes services, like service store for all interoperable services, p2p marketplace enablers, access control mechanisms, generic interoperability adapters, reasoning and compliance tests.
(An) IC Platform	A digital platform that complies with IC Framework requirements in terms of software and/or hardware that enables the actual interconnection of devices and services. Often implemented on the basis of an IoT platform.
Project Pilot	A collection of tools, software, hardware, building and users that provide a working demonstration one of more aspects of the generic IC Framework in one or more EU countries in terms of platform interconnected devices and services.
Project Use Case	A demonstration of application of the generic IC Framework in terms of using a specific set of services and a specific set of devices, that are interconnected by the platform, in a specific way.
Service-related terminology	
Technical Service Provider	A hardware or software component, possibly representing other components, that is capable of offering certain functionality in the form of an (IC) Service to other components. The other component could be owned by the same actor or by a different actor.

Commercial Service provider	A business actor that provides a service to another actor (e.g. consumer, but also another commercial service provider).
Service user	An entity that uses a service as provided by another entity. This can be from a commercial viewpoint or a more technical one (e.g. 'software using services offered by other technical components'). The context of this term determines the viewpoint.
Customer	A business actor that uses/consumes a service and in return (generally) rewards the (commercial) service provider for the use of that service.
Service Level Agreement (SLA)	Agreement between (commercial) service providers and users/customers
Service Level Management (SLM)	Management of agreements and commitments between (commercial) service providers and users/customers through tracking and documentation of service level delivery and usage.
(IC) Service	The offering of certain functionality from one entity/component to another authorized entity/component (e.g. service or software component) using (standardized) interfaces, compliant to certain IC Framework requirements.
(IC) Regular services	IC Services that are offered via, not by, the IC Framework. Regular services are listed in the IC Service Store.
Service interface	An (technical) interface that exposes the functionalities of an IC Service. Within the IC Framework, this includes a metadata interface for exposing service capabilities
Meta data interface	Part of a (technical) service interface in the IC Framework, that provides functionality for interacting with service at a 'meta' level. This part of the interface can be used for example to interrogate the service about its capabilities and semantical framework. Thus, it can be used for reasoning about using a service.
IC Framework Service	A service that supports offering and using services on an IC platform, as prescribed by the IC framework. Examples are registration and discovery services for interfaces, enabling humans and technical entities to find a particular regular service offered through an IC platform.
Energy service	A service that offers the ability to accomplish an objective (mainly in) in the domain of energy, like balancing demand and supply or the reduction of energy usage. This is a special category of services within the IC Framework, as energy services (often) require the coordination of tasks across different Smart Homes and Smart Buildings across the Smart Grid and thus requires multiple levels and domains of control to be interconnected.
Non-energy service	Non-energy service are services that do not relate to energy and/or do not enable clients to accomplish and energy objective (as a main objective). Examples of non-energy services are services that have as objective comfort, well-being, entertainment or safety of their users. Non-energy services can be used by and/or 'become part of' an Energy service. For example, a non-energy service that sends events when a door remains open, can be used by an Energy service to reduce loss of heat in a house by closing doors.
Technical service implementation related terminology	
Software as a Service (SaaS)	A software licensing and delivery model in which software is licensed on a subscription basis and is hosted (de)centrally. It is sometimes referred to as "on-demand software". SaaS applications are also known as Web-based software, on-demand software and hosted software. The term "software as a Service" (SaaS) is considered to be part of the nomenclature of cloud computing.
Local / Remote Services	Software services can be either implemented as code that is run at 'remote' server (i.e. on the cloud), or on a 'local' server, i.e. as code that runs on a digital platform that is in a Smart Building or Smart Home.

IC Service run-time platform	Code that is hosted on a digital platform and acts as an abstraction layer for the underlying software platform (e.g. specific operating systems). The digital platform hosting the IC service run-time platform can be any kind of digital platform, ranging from resource constrained embedded systems up to (virtual) cloud servers. IC services compliant with the IC service run-time platform are called IC² service and digital platform agnostic as they interface with IC service run-time abstraction layer and not directly with the underlying software platform.
(IC) Native Service	A service implemented as software/code that runs on a specific vendor's digital platform, making use of specific functions and characteristics of this specific platform.
(IC) IC² Service	A service implemented as software/code that runs on top of the IC service run-time platform.
Semantic and Syntactic Interoperability-related terminology	
Semantics	Semantics is the study of meaning, i.e., the meaning of the data being exchanged via the IC Framework
Semantic Interoperability	Semantic Interoperability concerns the exchange of meaningful information on the basis of agreed, formalized and explicit semantics
(IC) Semantic Interoperability Layer	A logical concept within the IC Framework that enables semantic interoperability. The semantic interoperability layer comprises ontologies, interoperability adapters and smart connectors with supporting orchestration enablers.
Ontology	The formal specification of a conceptualization, used to explicit capture the semantics of a certain domain of discourse. In the IC Framework, ontologies like SAREF are used to capture the agreed, formalized and explicit semantics for the exchange of meaningful information via the semantic interoperability layer.
IoT Platform specific Information Model	In a specific IoT platform, it is a representation of concepts and the relationships, constraints, rules, and operations to specify data semantics for a chosen domain of discourse, related to a specific IoT platform.
(IC) Sarefized Services	A Software Service whose capabilities and data for the Service Interface are expressed using the SAREF ontologies. (IC) Sarefized Services are automatically recognized by the IC Semantic Interoperability Layer. The capabilities of an (IC) Sarefized Service automatically become available to other Sarefized Services/Devices.
(TNO's) Knowledge Engine	An open-source, ontology-agnostic software component that is being developed by TNO in cooperation with VU Amsterdam. The Knowledge Engine helps improve interoperability by making data exchange more dynamic and smarter through orchestration and semantic reasoning. It creates a new way for software and devices to communicate with each other.
Knowledge Directory	A central component that registers the knowledge offered and requested by Smart Connectors. It does not perform any reasoning.
IC (Smart) connectors	Generic software responsible for orchestration and reasoning. The Smart Connectors are peers, that can communicate directly with each other through SPARQL+. Based on the information in the Knowledge Directory, each Smart Connector can perform orchestration and reasoning for itself. Smart Connectors configured to use the same Knowledge Directory can communicate with each other through SPARQL+.
IC adapters	The Interoperability Framework provides a set of adapters to allow vendors that are already compliant with industry standards to quickly connect their device/service to the Interoperability Framework. Ideally, for each industry standard (i.e., SPINE, WoT, modBUS, S2) an adapter would be available.

	IC adapter includes IC connector and also the underlying mapping of legacy data models and interfacing functionalities onto the InterConnect unifying protocol (SPARQL+) and SAREF based data model.
Knowledge IO	A description of a type of interaction that a Knowledge Base supports. There are five types of interactions, each with a Graph Pattern associated with it. The Function KnowledgeIO has two (one for input, one for output). A Knowledge Base typically has multiple KnowledgeIO's of different types. KnowledgeIO's are registered in the Knowledge Directory.
SPARQL+	Unifying interfacing protocol for the InterConnect semantic interoperability layer. It comprises the SPARQL standard and additional interfacing functionalities required for realization of the project use cases ("+" in the name).
IC Interoperability Framework-related terminology	
(IC) Service store	Complete catalogue of all interoperable services from energy and non-energy domains. The service store is implemented as a web application providing frontend interface for onboarding new interoperable services and browsing existing (already onboarded services) by category and other metadata parameters. The service store is part of the interoperability framework and can be utilized by local reasoners to find appropriate remote services (running on 3rd party platforms) needed for completing a task at hand. Service store enables users or local reasoners to find interoperable services of interest and provides them with information on how to access the services running on their hosting digital platforms.
(IC) Deployment Orchestrator	This is integral part of the service store responsible for facilitating instantiation of interoperable services packaged as containers for specific runtime environments including the service store sandbox.
P2P marketplace enablers	Set of enablers for P2P marketplaces include: Hyperledger Fabric configuration as blockchain basis for trusted data access and transaction management; set of smart contract templates representing supported transactions, reports and audits; white labeled web application utilizing blockchain network through integrated smart contract interfaces. These enablers can be configured and deployed for specific use case, on the level of a pilot or on the level of the whole project.
IC security and data protection framework	Set of best practices for ensuring data and privacy protection in integration/interoperability scenarios between two or more stakeholders with digital platforms, services, end users and databases. On the level of the project, a specific access control mechanism will be implemented with user/service/platform authentication and authorization procedures directly integrated with semantic interoperability layer (discovery and reasoning).
Interoperability compliance certification	Set of automated tests of achieved interoperability minimum defined for each service and platform category. The tests will include dummy data exchanges to showcase that defined data models are properly parsed and understood and services are capable of exchanging information through unifying communication layer/protocol. The interoperability compliance test will be part of the service onboarding process in the IC service store. After successful compliance test, a certification of interoperability compliance will be issued and written in immutable record of all interoperable endpoints based on Hyperledger Fabric blockchain established on the level of the IC project.

2. STATE OF THE ART

This chapter aims to provide an overview of various European initiatives, focusing on achieving an interoperable ecosystem across IoT platforms, services, and stakeholders. Projects that featured an interoperable marketplace – where users can register, discover, and interact with the available services – were of particular interest for this analysis.

The next sections will provide information about the following project's core functional components and their interaction. Privacy and security practices are also briefly examined to offer a complete overview of their different approaches. Finally, information models (or lack thereof) are discussed, allowing us to differentiate each initiative's take on interoperability.

The following paragraphs introduce the IoT architectures discussed in this section and some of their key features.

symbIoTe offers a middleware framework covering all seven layers of the IoT Architecture[1]. Existing IoT platforms and services can use symbIoTe's Core Services to register and discover other functions. One of symbIoTe's key features is its flexible and incremental approach to interoperability; ranging from purely syntactic and semantic to full ecosystems where smart objects can interact, project stakeholders could choose which interoperability level they wished to support. Security mechanisms are based on resource access schemes and identity management.

The **BIG IoT** initiative focuses on the upper layers of the IoT architecture, through its API for resource sharing and discovery. BIG IoT's Marketplace offers additional resources to expand the project's ecosystem, such as billing, subscription, and accounting. Some flexibility was included in the project after identifying different types of IoT platforms and their specific requirements (e.g., always-on, constrained device, etc.). Semantic and syntactic interoperability is achieved via the definition of a core model, extended with domain-independent and domain-specific vocabularies.

INTER-IoT focuses on six layers of the IoT Architecture, covering aspects ranging from physical components, network connectivity to QoS, and resource catalogue for service

[1] This model was introduced at the 2014 IoT World Forum, a research and innovation symposium showcasing IoT research. It is commonly used to illustrate the various system layers of an IoT architecture:

- The first level consists of the physical devices or “Things” in IoT, to which sensors and Intelligent Edge Nodes can be attached (if not already integrated) so that they can be managed;
- The second level, Connectivity, deals with the connectivity and transport of data, spanning from an Edge Node device to a local-based or cloud-based server. Multiple solutions can be considered at this stage (e.g., Wi-Fi, LPWAN, etc.);
- The third level, Edge Computing, interfaces the data with higher layers of cloud, SaaS, or proprietary software containing software functions and/or logic;
- The fourth level, Data Accumulation, handles data storage for processing;
- The fifth level, Data Abstraction, is an abstraction layer that organizes the upstream and downstream flows of data;
- The sixth level, Application Layer, is where the application logic resides. It allows the execution of functions such as monitoring, notification management, etc.;
- Finally, the seventh level, Collaboration and Processes, covers human interactions with lower layers of the IoT system.

A detailed description can be found here: http://cdn.iotwf.com/resources/72/IoT_Reference_Model_04_June_2014.pdf.

registering and discovery. A practical approach to security was privileged in this project, including multiple control points based on best practices. Interoperability is achieved by translating each IoT platform's resources to INTER-IoT's common ontology model and its extensions.

SynchroniCity aims to build a city-wide interoperable ecosystem of IoT solutions. Focusing on the upper layers of the IoT architecture, SynchroniCity offers a rich catalogue of services and functions via its IoT Data Market Place and compliable Smart City applications and services. Security mechanisms, such as authentication, authorization, and accounting are integrated through an overarching approach. SynchroniCity's data model is based on OASC's reference information meta-model and its extensions.

VICINITY addresses the five upper layers of the IoT Architecture and builds around the concept of "virtual neighborhoods" to achieve interoperability across distributed (i.e., P2P) IoT ecosystems. VICINITY's semantic and syntactic interoperability approach is based on a single common ontology - defined by the project - and extended through domain-specific ontologies, guided by the project requirements and defined use cases.

FIESTA-IoT focuses on six layers of the IoT Architecture, covering aspects ranging from physical components, network connectivity to resource catalogue thanks to FIESTA-IoT's WEB Browsing & Configuration graphical interface. Within the project, each IoT platform and service is represented as a Virtual Entity (VE), advertising a set of functionalities through an interoperable endpoint. The latter uses the project's core ontology model, based on popular IoT ontologies.

AGILE IoT provides a flexible and modular hardware and software solution for building interoperable IoT solutions. The software modules cover functions such as device management, communication networks, and solution for distributed storage. The hardware module focuses on extending the Raspberry Pi platform's capabilities by including additional radio sockets and expanding its connectivity options.

bIoTope follows a system-of-system approach for building an open, interoperable ecosystem, allowing for rapid use case implementation. bIoTope's architectural framework is built around a set of scalable micro-services. Interoperability is achieved via the implementation of the Open Messaging Interfaces (O-MI) and the Open Data Format (O-DF), defined by The Open Group.

The following sub-sections describe the details of the IoT architectures mentioned above.

2.1 SYMBIOTE

The symbIoTe initiative (symbioses of smart objects across IoT environments) is an EU H2020 funded project. It aims to provide a middleware framework to facilitate the creation of an interoperable IoT ecosystem, allowing for cross-platform interaction and the development of new domain-specific applications.

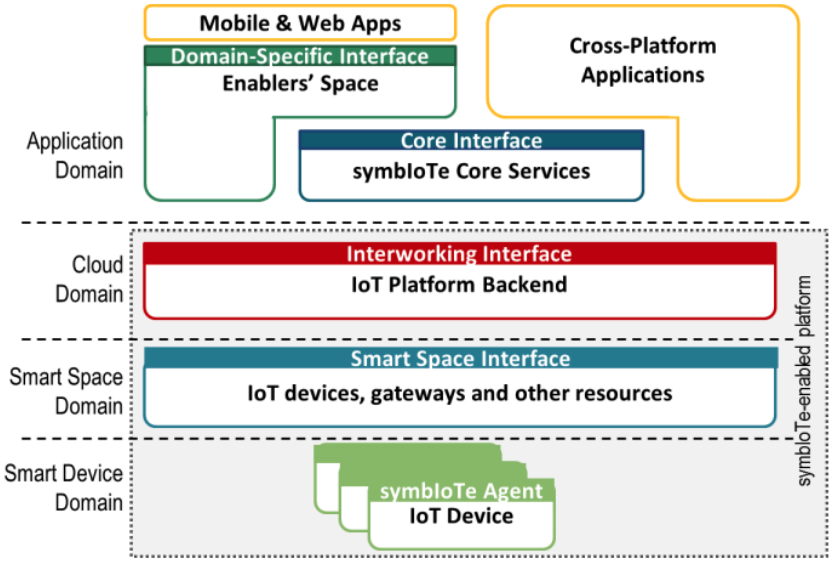


FIGURE 2 - SYMBIOTE'S HIGH-LEVEL ARCHITECTURE [1]

As presented in Figure 2, the symbIoTe architecture is based on a hierarchical four-layered IoT stack, covering the following domains [1]:

- The **Smart Device domain,** including various physical entities (i.e., IoT devices) communicating through heterogeneous technologies (e.g., Zigbee, 6LoWPAN) deployed within a Smart space, i.e., a physical environment where IoT platforms can discover and interact with smart devices, following predefined access policies.
- The **Smart Space domain** offers the required services to enable dynamic discovery, device configuration for local smart environments, and uniform interfaces for data consumption.
- The **Cloud domain** provides open interworking interfaces (API) where two or more platforms can securely collaborate and exchange resources.
- The **Application domain** provides symbIoTe's Core Services, particularly IoT device registry and discovery functions. The latter is, however, limited to storing and managing resource's metadata. Underlying IoT platforms are responsible for exposing core data in a unified manner through symbIoTe's Interworking Interface, based on symbIoTe's Core Information Model (CIM). Benefiting from these mechanisms, additional enablers provide high-value services and applications, exposing domain-specific interfaces upon which third parties can develop mobile & web applications.

In terms of security, symbIoTe's security mechanisms are incorporated into various architectural domains, based on resource access schemes and identity management [1]. To this end, symbIoTe implements Attribute-Based Access Control (ABAC) mechanisms, where access rights are granted to users (i.e., client application or resources within a system) possessing the exact set of attributes that match the predefined access policy.

Each access policy can be defined as a combination of attributes (i.e., user, resource, environment, etc.), allowing for complex policies based on Boolean logic (IF, THEN) and inclusive/exclusive logic (AND, OR).

2.1.1 SYMBIOTE'S COMPLIANCE LEVELS

Figure 3 depicts symbIoTe's flexible and incremental approach to interoperability. Based on the architecture's layered view, symbIoTe introduces four compliance levels (CLs), each representing different stages of interoperability that platform providers can choose to support [1]:

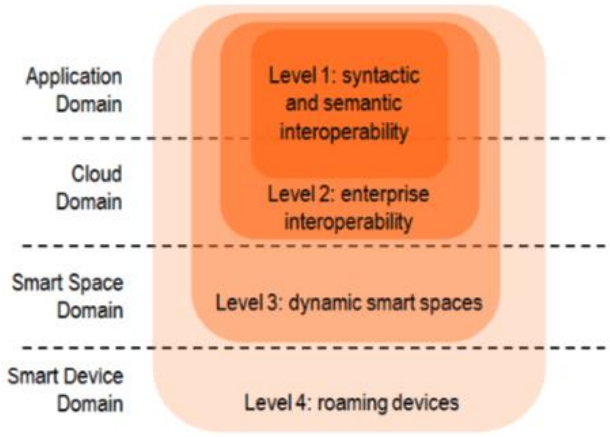


FIGURE 3 - SYMBIOTE COMPLIANCE LEVELS (CLS) [1]

- **Level-1 symbIoTe Compliant Platform (L1 Platform):** Platforms integrate the project's ecosystem by promoting and offering virtualized resources through symbIoTe's Interworking Interface in a unified manner, based on symbIoTe's unified information model for syntactic and semantic interoperability, further detailed in the next section.
- **Level-2 symbIoTe Compliant Platform (L2 Platform):** L1 platforms can federate to attain L2, which includes additional functionalities (e.g., sharing/bartering devices) that facilitate enterprise-level interoperability.
- **Level-3 symbIoTe Compliant Platform (L3 Platform):** L3 compliance mainly involves configuring platform and device software to integrate symbIoTe's component. The goal here is to facilitate IoT device integration and dynamic reconfiguration of smart spaces (i.e., a device is reconfigured on the fly to become part of another platform within the smart space).
- **Level-4 symbIoTe Compliant Platform (L4 Platform):** Building on L1, L2, and L3 compliance levels, L4 requires that platforms support device roaming, which can enable smart object interaction (i.e., devices from one platform can use another registered platform's infrastructure, following an SLA between the two platforms).

2.1.2 SYMBIOTE'S INFORMATION MODEL

symbIoTe's Core Information Model (CIM) is depicted in Figure 4. It consists of a set of basic concepts shared across participating platforms, capable of providing a high-level understanding of all available resources relevant to symbIoTe (i.e., classes and their interrelations). The set of definitions can be augmented using platform-specific concepts that extend the CIM, thus providing semantic and syntactic transformation as a common interoperability service. As such, we can describe the interoperability patterns as supporting:

- **Interoperability by standardization** (in this case, partial), where platforms use a common vocabulary to describe available resources and facilitate out-of-the-box interoperability.
- **Interoperability by mapping**, which allows platforms to maintain their own internal vocabulary by providing a mapping between their model and other platform-specific extensions (PIM). In this case, internal information models are exchanged in a transparent manner to allow platforms to interoperate efficiently.

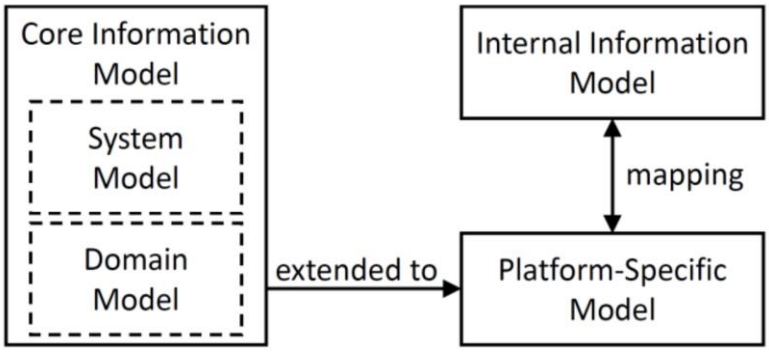


FIGURE 4 - CONCEPTUAL STRUCTURE OF SYMBIOTE'S CIM [2]

Thus, platforms wishing to become symbIoTe-compliant mush expose their data following this pattern. For that, symbIoTe defined Interworking Interfaces as RESTful APIs with JSON payload, following Open Data Protocol (OData) standards and best practices [2]. Information models created within this project are realized as OWL ontologies and made publicly available[2].

By favouring this approach, symbIoTe provides a minimalistic but flexible core information model, promoting widespread platform adoption. However, such flexibility can come at a high cost, since supporting complex scenarios will require the definition of domain-specific extensions and mappings that need to be understood and agreed upon by various platforms.

2.2 BIG IOT

The BIG IoT (Bridging the Interoperability Gap of the Internet of Things) is an EU H2020 funded project. Its goal is to help overcome technological market entry barriers in the IoT domain by enabling cross-standard, platform, and domain interworking of IoT services and applications. Moreover, the project aimed to demonstrate key findings by deploying BIG IoT's interoperability solution and ecosystem in three different pilot sites (Barcelona, Berlin/Wolfsburg, and Piedmont).

[2] https://github.com/symbiote-h2020

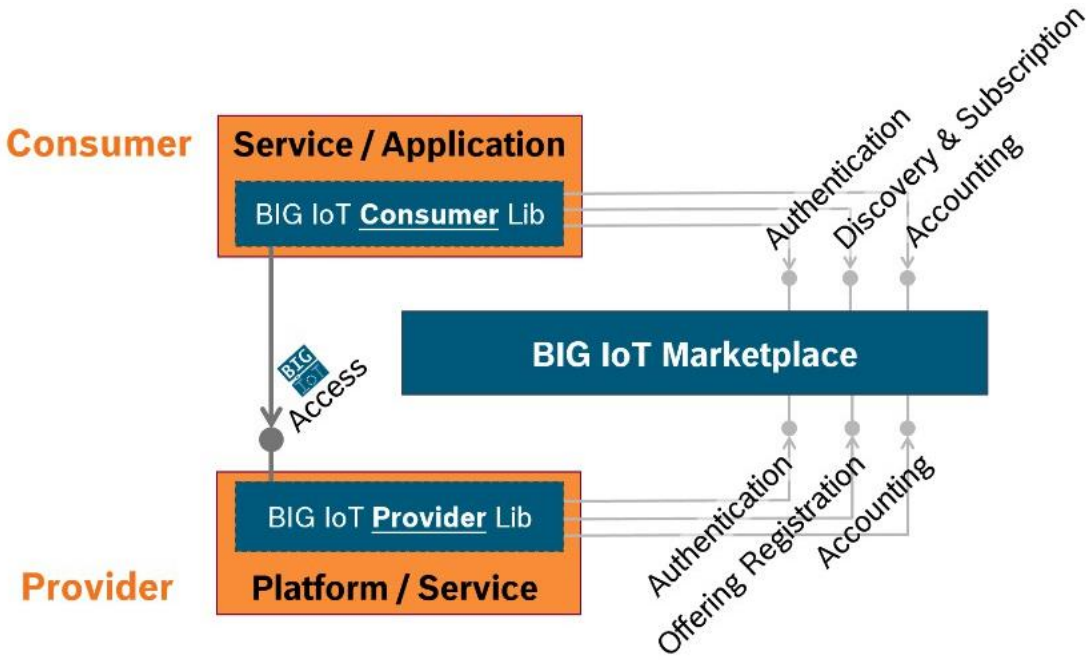


FIGURE 5 - BIG IOT'S SIMPLIFIED HIGH-LEVEL ARCHITECTURE [3]

As depicted in Figure 5, BIG IoT's architecture is based on the following building blocks and their interactions:

- **The BIG IoT Applications / Platforms / Services**, consisting of the set of compliant applications, platforms and services available within the project's scope. The latter are responsible of implementing the project's API for resource (i.e., information or functions) discovery and sharing within BIG IoT's Marketplace. The project offers four different integration modes, based on the project's ecosystem (i.e., cloud-based, constrained or unconstrained device-level IoT platform, etc.).
- **The BIG IoT Library or SDK**, which can be defined as programming interfaces for integrating and developing new BIG IoT compliant services and applications. Existing Platforms or services implement the BIG IoT Provider Lib, which allows them to authenticate themselves and register their offerings to the Marketplace. and Applications wishing to discover, and access available resources implement the BIG IoT Consumer Lib.
- **The BIG IoT Marketplace** hosts the set of resources that can be traded within the BIG IoT ecosystem. It also provides a set of standard web APIs, covering BIG IoT's primary interactions, i.e., authentication, registration, discovery, subscription, and accounting. The latter is one of BIG IoT's specific features, allowing to monetize the consumption of available resources [4]. Another one of such features is the "Recipe Cooker", providing users a graphical user interface to discover, download, and upload new instances of semantic descriptions to the marketplace.

2.2.1 BIG IOT'S COMPLIANCE MODES

The full set of interactions and core building blocks supported by BIG IoT is shown in Figure 6. As mentioned earlier, the project offers four different integration modes [3], following the identification of five types of IoT platforms available within the project, namely:

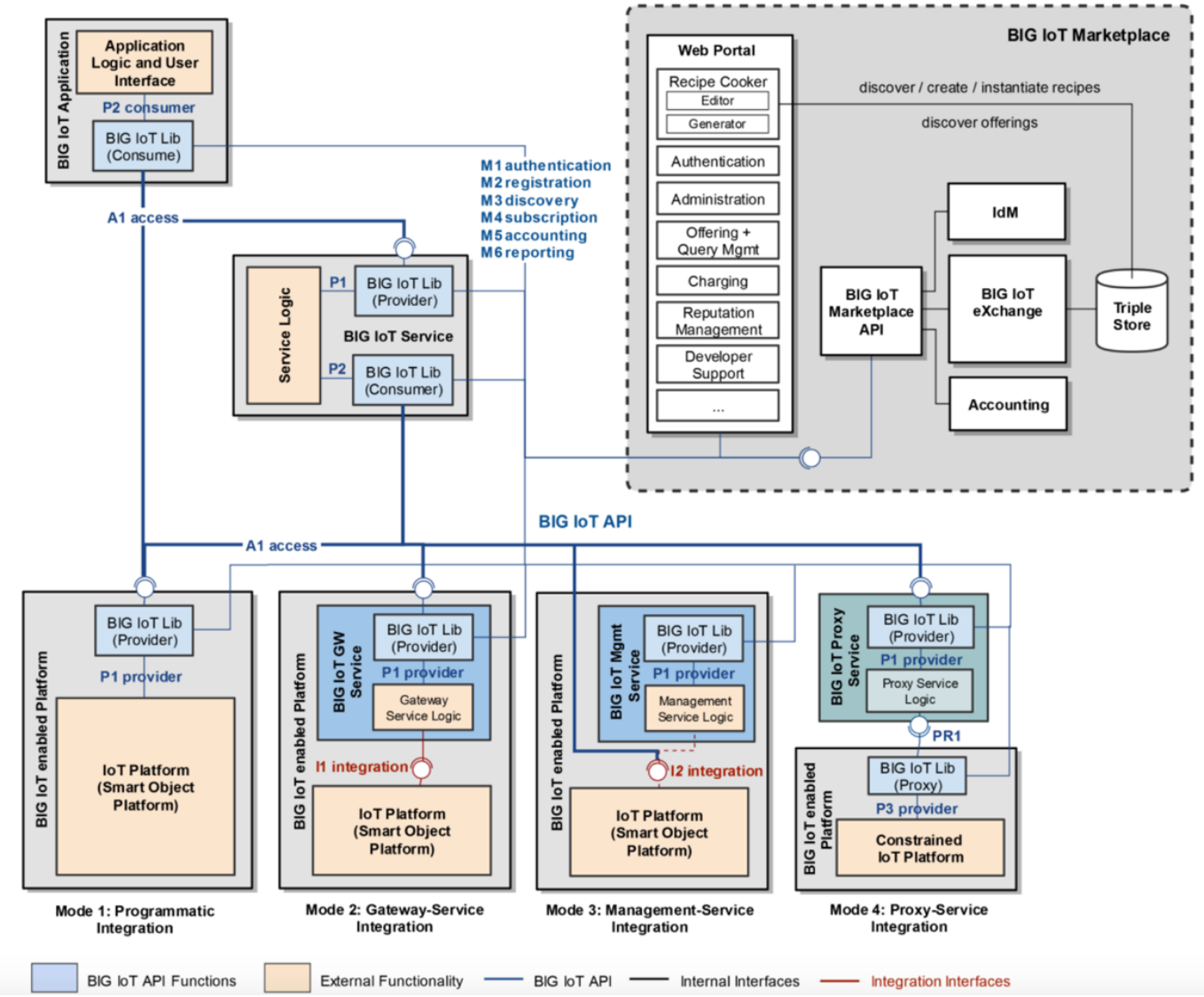


FIGURE 6 - BUILDING BLOCK VIEW OF THE BIG IOT ARCHITECTURE [3]

- **Cloud-based IoT platforms or Server Infrastructure**, accessible via the Internet and assumed as “always-on”,
- **Local-based IoT platforms, hosted on devices** that are unconstrained i.e., have no computational limits and are based on common Web/internet technologies supported by the project, such as HTTP and WebSockets (e.g., Raspberry Pi). These devices are also assumed to be “always-on”, and benefit from a flat-rate plan,
- **Local-based IoT platforms, hosted on devices** that are unconstrained but are not “always-on”,
- **Local-based IoT platforms, hosted on devices** that are unconstrained but are charged on a “pay-per-use” basis,
- **Local-based IoT platforms, hosted on devices** that are constrained with respect to their capacity to communicate or compute (e.g., micro-controller sensors).

Thus, the implementation of the BIG IoT architecture can be adapted following the infrastructure, computational capacity, availability of the resources, etc. The implementation modes can be detailed as follows:

- **Programmatic Integration (Mode 1):** Providers fully integrate BIG IoT's APIs to provide access and expose available resources. This mode assumes that existing platform providers and developers adapt their frameworks and programming languages to BIG IoT's supported access (e.g., request/response, streaming) and communication protocols (e.g., HTTP, WebSocket, MQTT).
- **Based on the BIG IoT Gateway Service (Mode 2):** Providers are required to develop and operate a gateway service based on the BIG IoT Provider Lib. Incoming communications and requests are translated so that the existing platform can support them. From the Marketplace or the end-user perspective, there is no difference between modes 1 and 2. This method allows existing (legacy) platform providers to avoid introducing changes in their current framework.
- **Based on the BIG IoT Management Service (Mode 3):** Providers can integrate the BIG IoT ecosystem via the projects Management Service, based on the BIG IoT Provider Lib. This scenario only covers basic interactions with the BIG IoT marketplace, i.e., resource registration and discovery. Thus, it imposes significant limitations in terms of interoperability: resources are exposed by the platform in an "*as-is*" manner, preventing further data enrichment or reformat. Furthermore, only consumers who are already registered with the platform provider can access their resources, since the platform's legacy interfaces handle access control policies.
- **Based on BIG IoT's Proxy Service (Mode 4):** Designed for constrained device-level IoT platforms, BIG IoT's Proxy Service allows them to extend their native capabilities by acting as an "always-on" proxy that stores information for dormant platforms. Thanks to this service, access requests can be queued until the host device reconnects/wakes up. Also, the Proxy Service allows for easy interaction with the Marketplace, allowing for basic interactions (e.g., registration and discovery) as well as more specialized functions, such as authentication and accounting (P3 interface). Hence, from the Marketplace or the end-user perspective, there is no difference between modes 1, 2, and 4.

2.2.2 BIG IOT'S APPROACH TO SEMANTIC INTEROPERABILITY

As shown in Figure 7, BIG IoT's information model uses a modular approach: the project specifies a core model, containing the minimal vocabulary required to describe the project's *Offerings* and *OfferingQueries*[3], that can be extended through domain-dependent or independent models.

More precisely, domain-dependent and independent models are used to annotate Input & Output data of Offering Descriptions and the OfferingCategory. For example, BIG IoT uses a Mobility Domain Model to annotate metadata specific to resources dealing with parking, traffic, etc. The data is then mapped to the BIG IoT Application model vocabulary.

[3] The term *Offering* refers to the resources (i.e., information or functions) offered or traded by the project's providers. Each *Offering* contains a semantic description (i.e., set of resources exchanged in the marketplace) and some meta-information (e.g., region, price, I&O's, etc.) associated with the resource. *OfferingCategory* allows for the classification of Offerings within the marketplace.

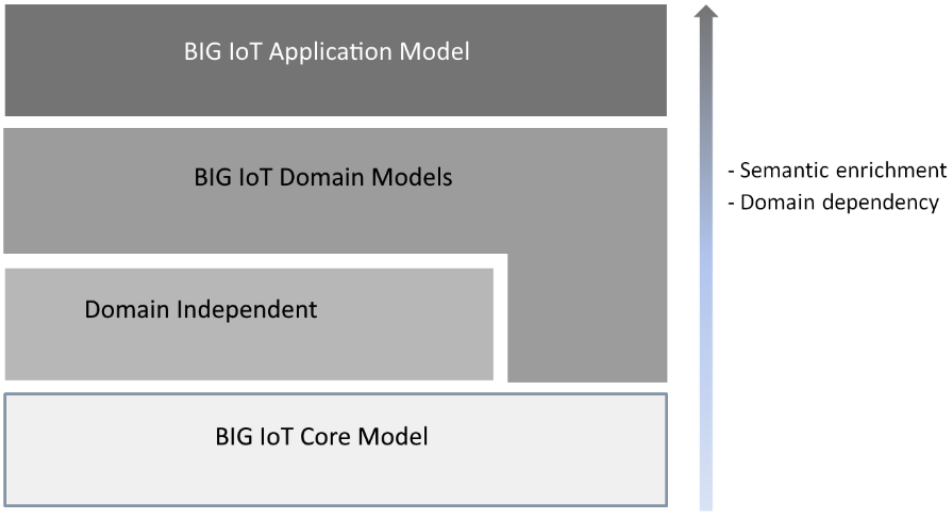


FIGURE 7 - BIG IOT'S INFORMATION MODEL (LAYERED VIEW) [3]

Data is stored in a triple store, following an RDF schema model. Once the data is expressed in a RDF-compliant format, it can be queried using GraphQL or SPARQL. This method allows for the implementation of an interoperable syntactic and semantic information model, where data can be enriched, queried, and inferred in some cases.

Data inference is achieved through the introduction of BIG IoT's Semantic Reasoner: a rule-based inference engine (based on a Jena inference subsystem[4]) that can generate new knowledge from data stored in triple stores.

2.3 INTER-IOT

INTER-IoT is an EU H2020 funded project, launched in 2016. It aims to develop an interoperability framework that provides seamless interworking between heterogeneous devices, services, applications, and IoT platforms. Furthermore, three large scale pilots were deployed to demonstrate cross-platform and cross-domain interoperability within the m-health, transportation, and logistics domains.

[4] https://jena.apache.org/documentation/javadoc/jena/org/apache/jena/reasoner/package-summary.html

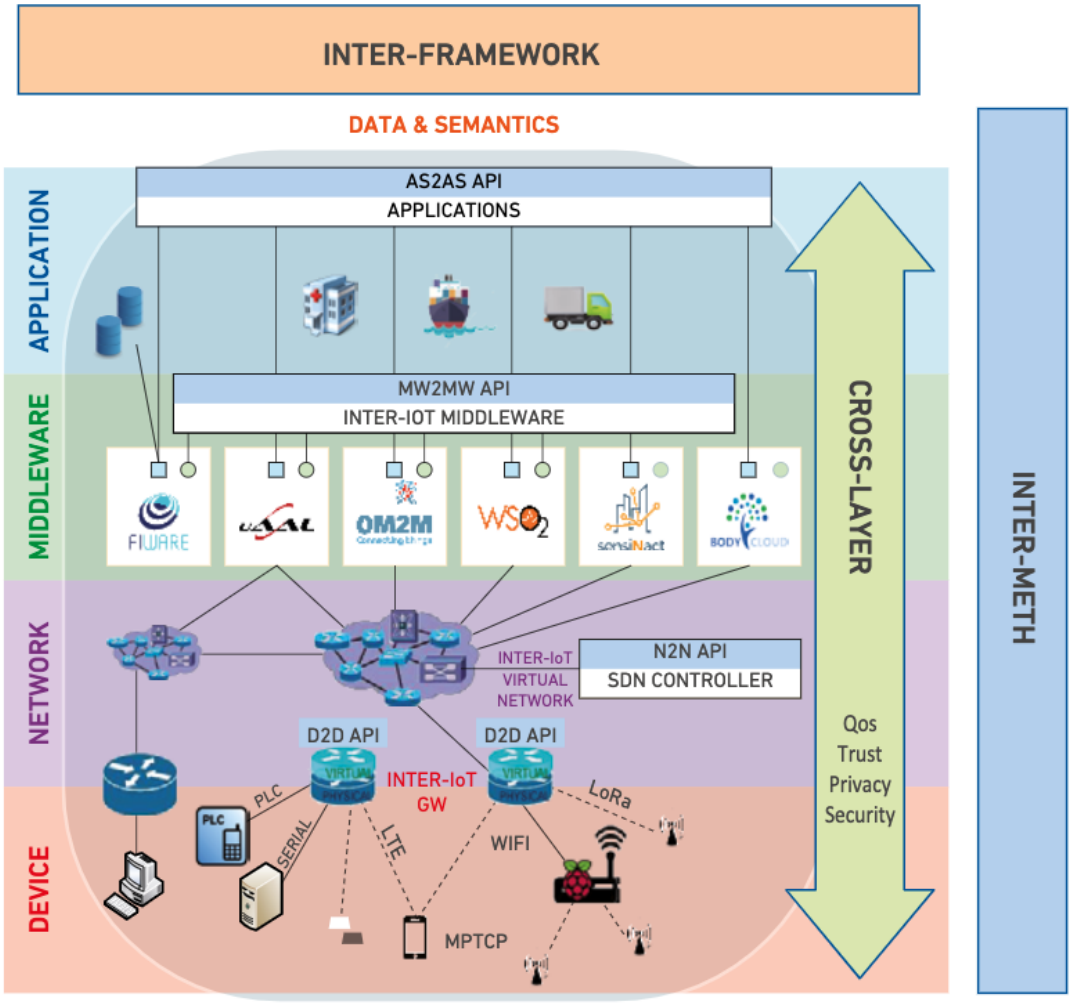


FIGURE 8 - INTER-IOT'S ARCHITECTURE [4]

INTER-IoT's layered architecture (shown in Figure 8) introduces the following main components:

- The **Device Layer (D2D)** includes the physical (i.e., hardware) and virtual (i.e., gateway virtualization) components required for device network access, communication, and gateway operations. Various communication technologies (e.g., LoRa, WIFI) and raw data forwarding is supported at this stage to improve the seamless integration of existing devices.
- The **Network Layer (N2N)** allows for Network-to-Network interoperability based on INTER-IoT's Virtual Network.
- The **Middleware Layer (MW2MW)** is an abstraction layer that handles resource discovery and management for IoT devices hosted across heterogeneous IoT platforms.
- The **Application and Services Layer (AS2AS)** consists of a set of services offered by IoT platforms, enabling resource discovery, catalogues, and new service/application development.
- The **INTER-FRAMEWORK** refers to the set of tools offered at each layer for achieving interoperability, accessible via API. The project also provides a virtualized version of each layer, via Docker.

- **INTER-METH** consists of general guidelines and methodology provided by INTER-IoT to facilitate implementation.

In terms of security, following the project's focus on potentially vulnerable sectors (e.g., the health sector handles personally identifiable data), a practical approach to cybersecurity was privileged. This can be translated by INTER-IoT's cross-layered approach for data confidentiality, integrity, availability, and overall quality of service (QoS).

The resulting framework (SecurIoTy) provides a scalable security protocol, covering all architectural components, ranging from secure data traffic from/to devices to encrypted data storage for applications. To achieve this, INTER-IoT provides multiple control points, based on industry best practices and standard protocols (e.g., HTTPS(S), WebDAV, REST, TCP).

2.3.1 INTER-IOT'S APPROACH TO SEMANTIC INTEROPERABILITY

INTER-IoT's semantic solution is based on the semantic translation of each platform's proprietary ontology to the project's common ontology model **(Generic Ontology for IoT Platforms or GOIoTP)**. The latter is based on W3C's core ontology SOSA (Sensor, Observation, Sample and Actuator) and its extension, the Semantic Sensor Network (SSN)[5].

The core ontology adopts a modular approach and can be extended to include additional classes, properties and individuals via the Generic Ontology for IoT Platforms Extended (**GOIoTPex**). The core ontology and its extension is publicly available at https://inter-iot.github.io/ontology/.

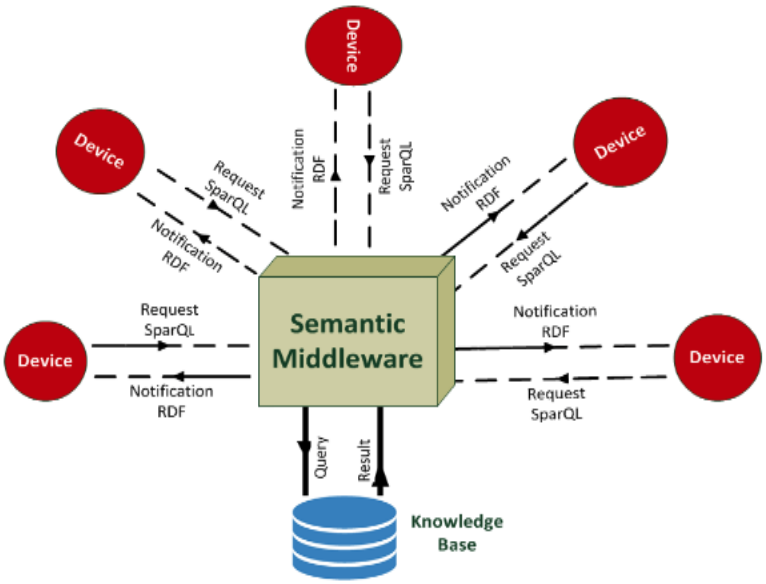


FIGURE 9 - INTER-IOT'S SEMANTIC MIDDLEWARE [5]

Figure 9 depicts the basic functioning of INTER-IoT's semantic middleware, which acts as a knowledge directory interacting with the project's knowledge base. Data is stored following an RDF schema model and can be queried through SPARQL. Some of the main features

[5] https://www.w3.org/TR/vocab-ssn/

supported by the semantic middleware are introduced in [5], namely: notify on device or service state change, subscription, support for scalable architectures, generating potentially massive amounts of real-time data streams, and support P2P private messaging interactions.

2.4 SYNCHRONICITY

SynchroniCity is an EU-funded project developed within the H2020 initiative. It aims to build an interoperable ecosystem for IoT-enabled smart city solutions. SynchroniCity's Single Digital City Market for Europe was deployed around eleven reference zones, covering over thirty-four partners, eleven different countries, and four continents.

The project's reference architecture is built around a set of logical components, following the Open & Agile Smart Cities (OASC) principles [6]. Figure 10 depicts these components and their interactions, which can be detailed as follows:

- The **City resources** module covers the primary data sources, platforms, and devices within the project's scope.
- The **IoT management** module covers interactions between IoT Agents (i.e., software modules implementing the project's interfaces) and devices. Existing heterogeneous protocols and technologies supported at this stage are made interoperable via the southbound interfaces (i.e., context management API).
- The **Context Data Management** module handles existing context information. It acts as a middleware that exposes heterogeneous data in a unified manner to its consumers. Additional functionalities, such as data enrichment, event detection, and resource query/subscription, are also offered at this stage.
- The **Data Storage Management** module handles data storage and access for heterogeneous sources so that the latter can be accessed in a unified manner. To achieve this, functionalities such as configuration, provision, etc. are proposed. Data security and quality are guaranteed by integrating aspects such as data anonymization and categorizing (i.e., public/open or private data).
- The **IoT Data Marketplace** handles interactions between the project's data suppliers and consumers. Some of the key features supported at this stage are asset management catalogue, license management, revenue management, etc. Services and applications can interact with a set of northbound interfaces providing an additional interoperability "entrance point".
- The **Northbound interfaces** module regroups the actual implementation of the logical interfaces (interoperability endpoints) offered by SynchoniCity. The different APIs are based on a HTTP RESTful approach, covering the following functions: context management API, responsible for managing the context entities; data storage API, which provides access to historical and open data; the marketplace API, which handles monetization of digital assets; the security API, based on OAuth2 protocol, providing security functionalities for the project's services.
- The **Monitoring and platform management** module offers additional functionalities covering platform configuration, monitoring (i.e., metrics for performance, usage, etc.). The project's quantitative and qualitative metrics (KPIs) are based on measures collected at this stage.

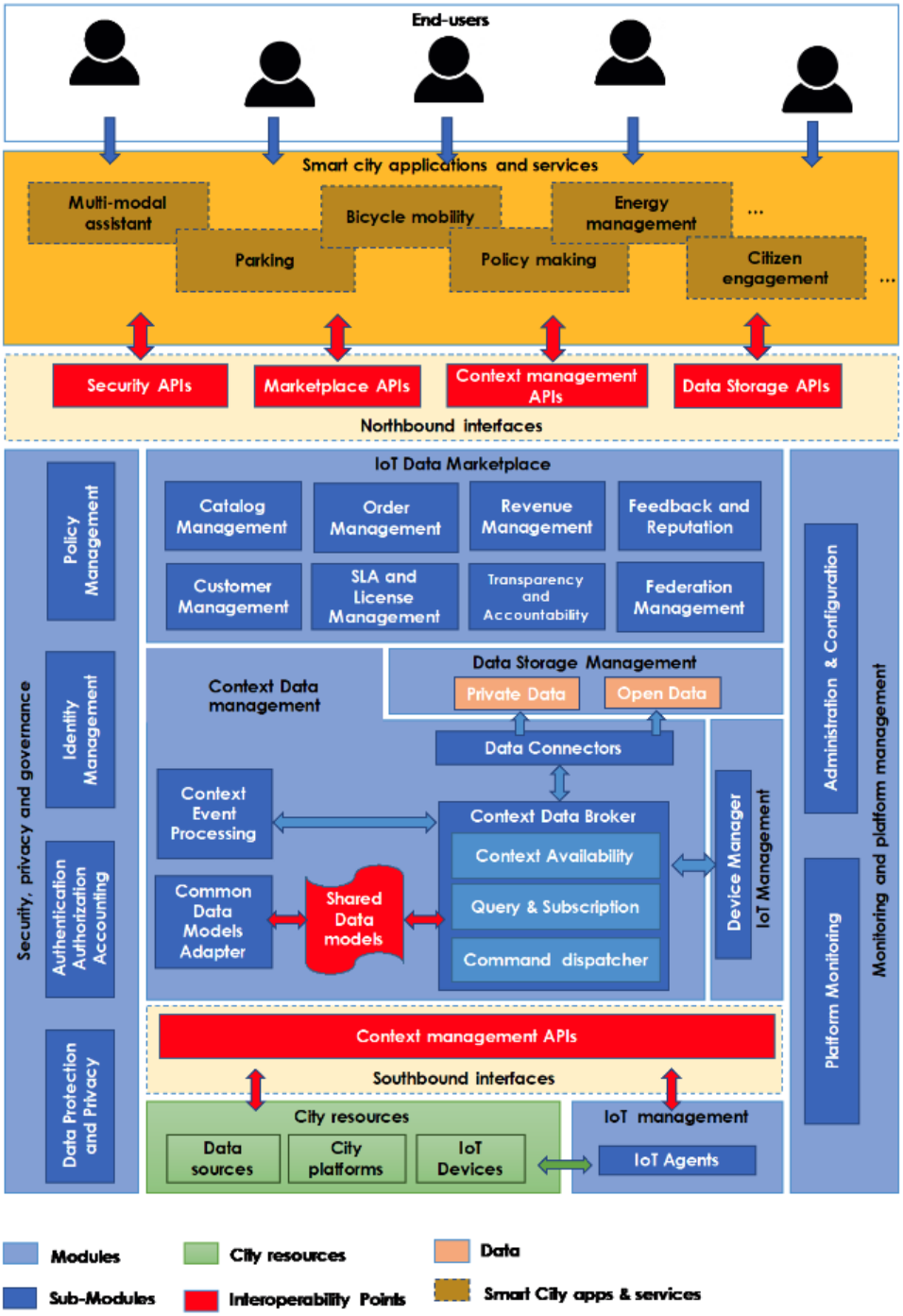


FIGURE 10 - SYNCHRONICITY'S REFERENCE ARCHITECTURE [6]

In terms of security, SynchroniCity privileges an overarching approach, based on three pillars: data, IoT infrastructure, and platform services. Each of these elements contains a set of transversal modules, covering the following aspects:

- **Data protection and privacy**, providing cryptographic mechanisms for data authentication and transit. Data collected can be managed (i.e., deleted, updated) by data subjects, thus enforcing data protection, transparency, and accountability.
- **Identity and Authentication Management** provides required functions for user registration, identification and authentication.

- **Authorization and Accounting** handles user's rights to a particular resource and stores access information for billing purposes.
- **Policy management** consists of a central, unified management point for all of SynchroniCity's governance and management policies. As such, this module can interact with all previous components to provide enforceable policies.

2.4.1 SYNCHRONICITY'S APPROACH TO SEMANTIC INTEROPERABILITY

SynchroniCity's data model builds on OASC's reference information meta-model (OMA NGSI meta-model, shown in Figure 11), commonly used on smart city projects [7].

OMA NGSI meta-model consists of three main elements: entities, which represent a thing, i.e., physical or logical objects such as sensors, or a person; attributes, which are a property of an entity, identified by a combination of its id and type; and metadata, which can further describe an attribute by specifying an entity's optional values. The core model can be extended through a catalogue of domain-specific data models for various Smart City application domains. Moreover, guidelines for creating new data models within the scope of the project are described in [7].

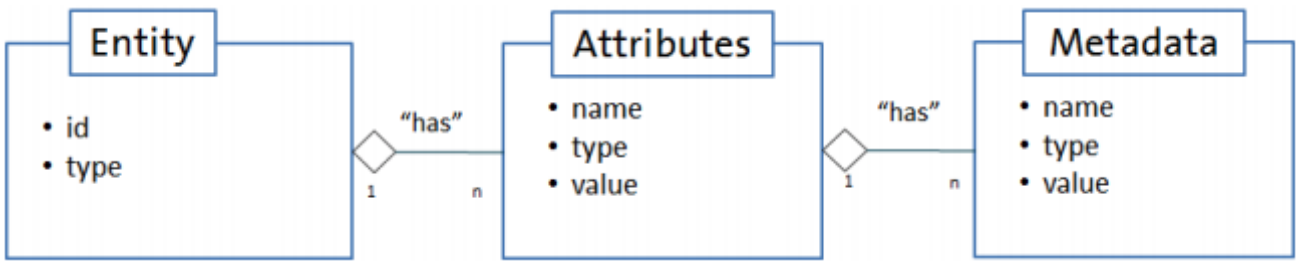


FIGURE 11 - OMA NGSI META-MODEL [7]

2.5 VICINITY

VICINITY is an EU H2020 funded project, launched in 2016. It tackles the subject of lack of interoperability across distributed IoT ecosystems. VICINITY's "interoperability as a service" concept is based on a high-level architecture built around virtual neighbourhoods (i.e., integrated IoT infrastructures and services). The project's reference framework and approach was demonstrated through a large-scale deployment site, connecting eight IoT ecosystems across seven European countries.

As shown in Figure 12, VICINITY's architecture is based on a peer-to-peer (P2P) network of nodes, allowing for secure data access and sharing amongst the project's participants. Below, a brief description of each component and their expected interactions [8]:

- **VICINITY Nodes** are a set of software components facilitating the integration of IoT infrastructure and services into the VICINITY Cloud. Each node is composed of the following VICINITY logical components: Communication Node (i.e., allows secure data traffic within the VICINITY P2P Network), Gateway API (i.e., for exposing and

consuming IoT object data), and Agent/Adapter (i.e., semantic translation and node description).

- The **VICINITY P2P Network** is the distributed network architecture containing VICINITY Nodes, registered within the VICINITY Cloud Services. The latter offers node-to-node (i.e., nodes request information to peer nodes) or cloud-to-node communication for data exchange, based on pre-defined access rules. Other services, such as encryption and privacy features are also offered at this stage.
- The **VICINITY Cloud** offers a set of services allowing for configuration of distributed virtual neighbourhoods, semantic search and discovery, service auditing, user notifications, etc. Based on these services, the VICINITY Cloud can be decomposed in the following VICINITY logical components: the Neighbourhood Manager (i.e., organizes virtual neighbourhood search, access rules, node configuration, etc.), the Semantic discovery and agent configuration platform (i.e., semantic search, registry and mapping of IoT objects), the Communication Server (i.e., handles P2P network transactions between cloud components), and the Gateway API Services (i.e., for semantic search of IoT objects).

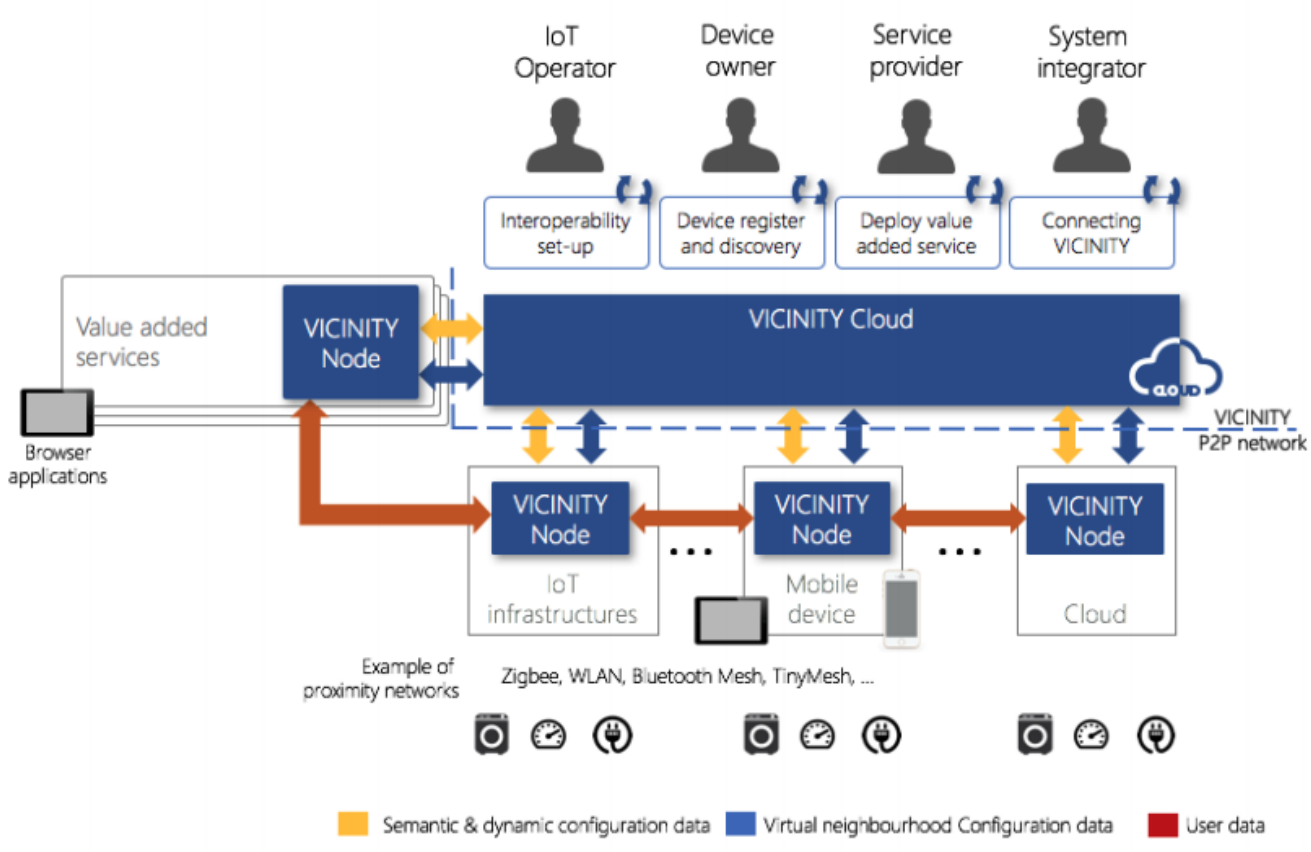


FIGURE 12 - VICINITY'S HIGH LEVEL ARCHITECTURE [8]

VICINITY's approach to system and data security focuses on defining a "secure zone" where core elements are protected via different mechanisms, such as XMPP SASL authentication, IDS/IPS measures in place and active in platform as a service (cloud) provider, firewall rules, hash password storage, certification, creation of logs and audit trails, amongst others.

2.5.1 VICINITY'S APPROACH TO SEMANTIC INTEROPERABILITY

The project's semantic interoperability approach is based on the VICINITY ontology (see Figure 13). It is mainly composed of a core information model that can be extended through different domain-specific and cross-domain modules, based on use case and partners requirements. The project's core model is publicly available at http://iot.linkeddata.es/def/core/index-en.html.

VICINITY's core information model builds on general concepts such as time, space and web things. To improve reusability, VICINITY employs the main concepts and interaction patterns provided by the Semantic Sensor Network Ontology (SSN), developed by W3C [8]. The SSN ontology comprises ten modules covering the main concepts and relationships to describe sensors.

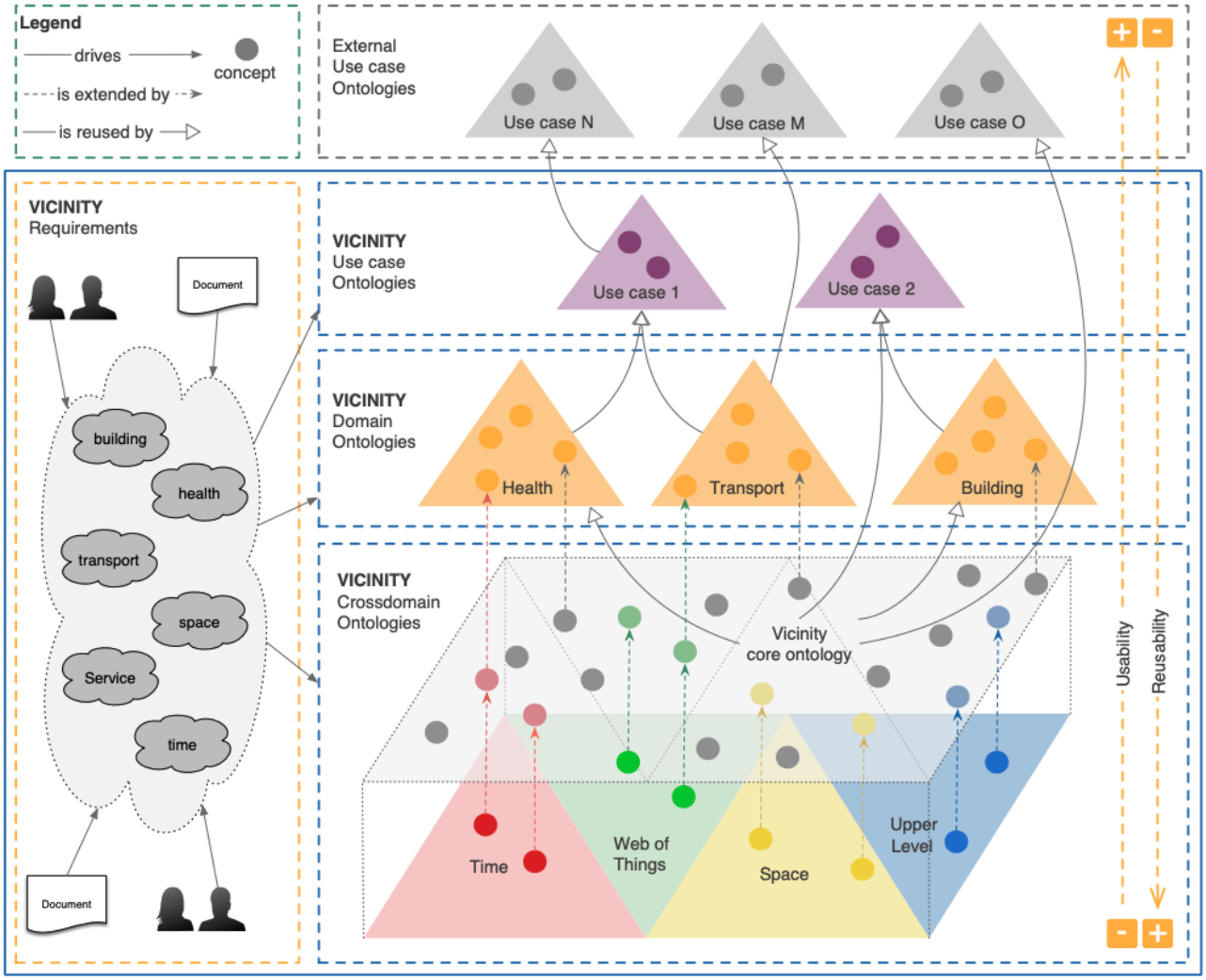


FIGURE 13 - VICINITY'S ONTOLOGY DESIGN [8]

Gateway Adapter APIs, deployed by participating IoT platforms, translate proprietary/internal information models into VICINITY's common abstract information model. Data can then be discovered and queried through SPARQL.

2.6 FIESTA-IOT

The FIESTA-IoT (Federated Interoperable Semantic IoT/cloud Testbeds and Applications) initiative is an EU funded project, developed within the H2020 initiative. The project aimed to produce an experimental blueprint containing tools, techniques, and best practices for large scale deployments for distributed (geographically and administratively) IoT platforms, with pilot sites scattered across Spain, UK, France and Korea.

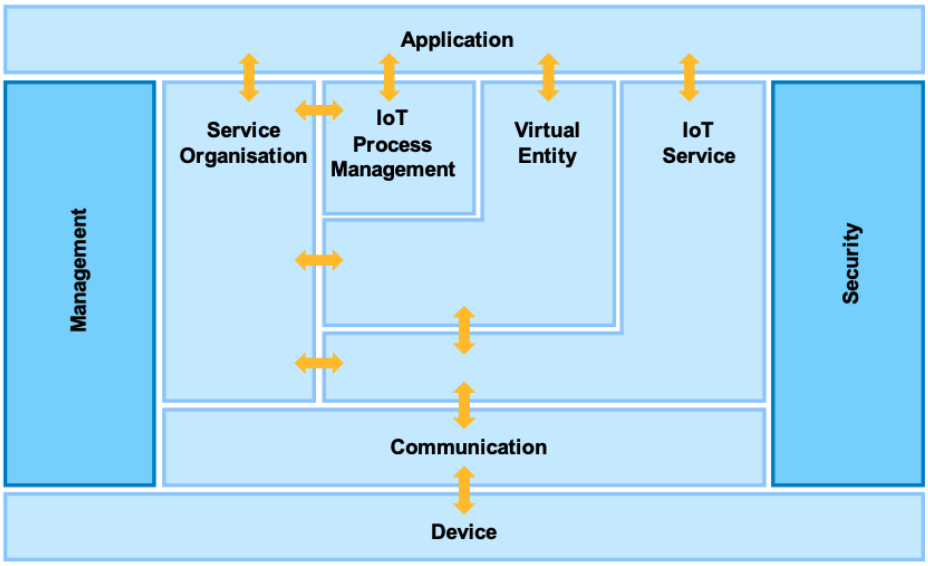


FIGURE 14 - FIESTA-IOT'S FUNCTIONAL MODEL VIEW [9]

FIESTA-IoT uses different viewpoints for describing its IoT Reference Architecture, i.e., the information, deployment and functional views. Figure 14 depicts the latter, consisting of the main following components:

- The **Communication Functional Group (FG)** consists of a message bus (i.e., communication channel) that allows for end-to-end, network or hop-top-hop communication (e.g., publish/subscribe) between devices and FIESTA-IoT's cloud data endpoints.
- The **IoT Service FG** offers two main functions: the IoT Service/Resource Registry and FIESTA-IoT's Meta-Cloud Data Endpoints. The first refers to the project's API for service registry, responsible for centralizing outgoing requests and compile the answers. The Meta-Cloud Data Endpoints are user interfaces for data querying and storage.
- The **Virtual Entity (VE) FG** responsible for creating and maintaining VEs and their association to IoT resources. This FG also offers VE endpoints exposing services to the project's users for interacting with VEs (e.g., get/set properties).
- **The Service Organisation and the IoT Process Management FG** specialize on providing the required tools for modelling, creating and supporting FIESTA-IoT's experiments and available IoT services.
- The **Management FG** handles user registering (i.e., authentication/access) and FIESTA-IoT's WEB Browsing & Configuration graphical interface, offering basic CRUD operations (Create, Read, Update, Delete) for VEs, Resources and Services.

- The **Security FG** covers all of the security-related components introduced by FIESTA-IoT to ensure data privacy, security and trust: authentication, access-control policies, key exchange/management, and Security Certificate generation (Trusted Third Party or TTP).

2.6.1 FIESTA-IOT'S APPROACH TO SEMANTIC INTEROPERABILITY

FIESTA-IoT's approach to semantic interoperability is built around the FIESTA-IoT Ontology. As shown in Figure 15 the project's ontology merges useful concepts from existing ontologies – such as WGS846, W3C SSN, IoT-lite, M3- lite Taxonomy, DUL, Time7 and QU– into a single one [10].

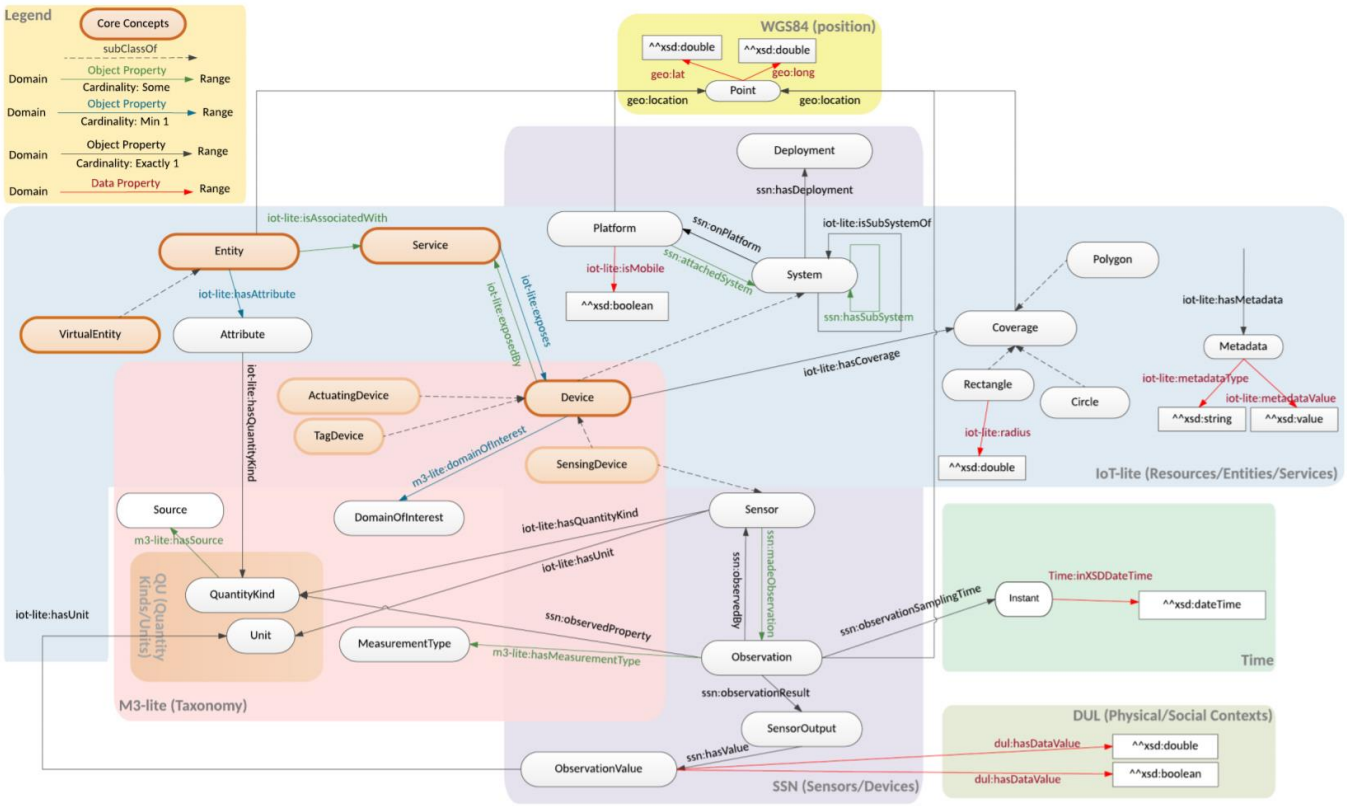


FIGURE 15 - THE FIESTA-IOT ONTOLOGY [10]

The FIESTA-IoT platform then uses Jena Triple store (TDB) for data storage and offers the advantage of supporting spatial queries; a requirement given the project's geographically scattered deployment testbeds. Furthermore, through this mechanisms, new knowledge can be inferred (e.g., mobility of resources) using SPARQL queries.

Lastly, one of the project's specific features is that it integrates specific tools for uploading and converting data to the required RDF form: the LinDA (Linked Data) transformation tool is an open-source data tool where data from multiple sources (e.g., XLS, CSV, and relational database or DB) can be linked and further analysed.

2.7 AGILE IOT

The AGILE (Adaptative Gateways for dIverse muLtiple Environments) initiative was launched in 2016 and is co-founded by the H2020 EU project. Its goal is to provide a flexible hardware and software gateways for building IoT solutions that enable seamless and modular integration of various devices. To extend and support the project's reach, the Commission also launched the Eclipse AGAIL project as a direct output of AGILE, available through the Eclipse Foundation[6].

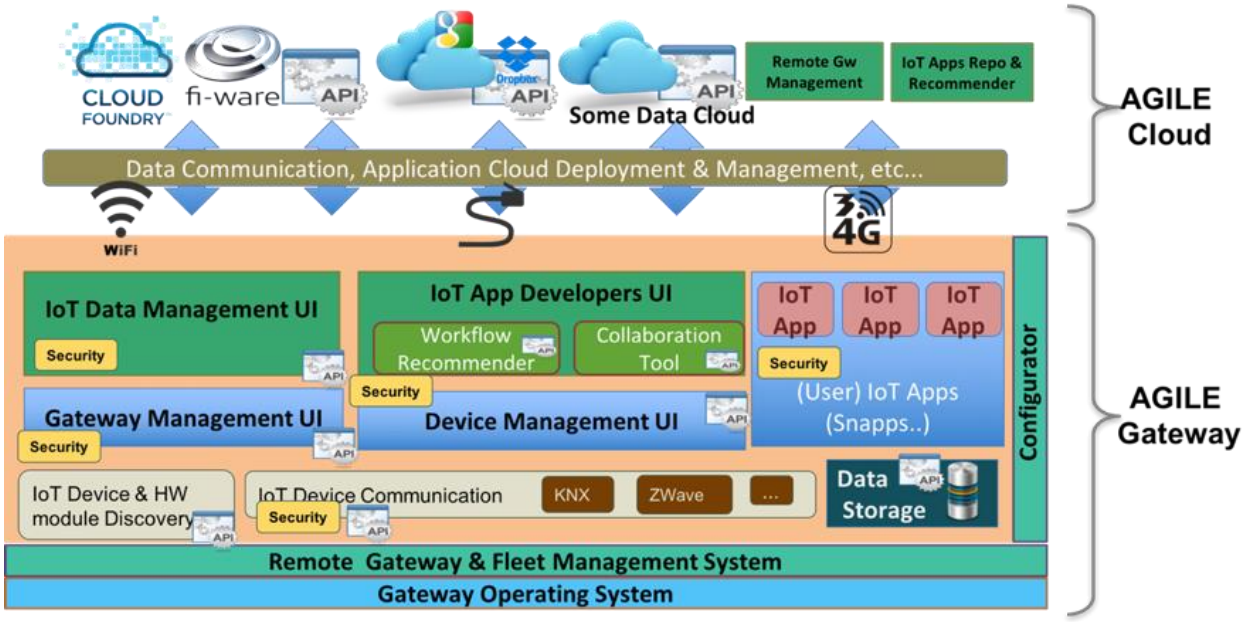


FIGURE 16 - AGILE IOT LOGICAL VIEW [11]

The software stack can be divided into two main bundles, shown in Figure 16. The first is the **AGILE Gateway** bundle, covering the full software stack that runs on edge devices and interfaces with IoT devices hosting IoT applications. The second is the **AGILE Cloud** bundle, which contains different services to extend and support the AGILE Gateway capabilities. Below, a brief description of the main components covered by the project:

- At the lowest level, the **operating system** (OS) runs at the gateway itself. The OS is based on a Linux distribution for embedded devices.
- The **Remote Gateway & Fleet Management System** offers the required capabilities to allow remote access to the gateway and managing a fleet of remote gateways.
- The **Device Discovery, Communication, and Data Storage layer**, consisting of the following modules:
    - The **IoT Device & HW module Discovery** is a micro-service exposed over an API that allows wireless module detection (e.g., Zigbee, LoRa, etc.). Once the module is detected, the module uses the appropriate standard or family of standards (e.g., KNX, oneM2M, etc.) to communicate,

[6] https://www.eclipse.org/org/foundation/

  - The **IoT Device communication** handles the implementation of the actual communication with detected IoT devices. This module is a micro-service exposing the features of existing devices for data polling and device actuation. It supports numerous communication protocols (e.g., KNX, ZWave, Thread, etc.).
  - The **Data Storage** module consists of a local NoSQL database for IoT device data management, exposed via an API.

- The **Gateway and Device Management layer**, consisting of the following modules:
  - The **Gateway Management UI** offers a graphical user interface where users can manage (e.g., see resource status, reboot, etc.) and control devices connected to the gateway.
  - The **Device Management UI** provides a graphical user interface to the Device Discovery and Communication modules to list found devices and real-time data reading/actuation.
  - The **IoT Apps** support the execution of IoT applications offered via AGILE APIs. Such services cover the installation, upgrade, and uninstall of applications located in the AGILE Gateway.
  - The **IoT Data Management UI** offers a graphical user interface for interacting with the Data Storage Layer, covering mainly the querying of data from local storage for real-time view, data visualization, etc.
  - The **IoT App Developers UI** offers graphical interfaces that help developers in creating application logical that will run on the gateway. During specification, this module shall support popular IoT protocols, such as MQTT, WebSockets and CoAP.

- On the **cloud side**, the following modules are integrated to complete and extend the capabilities of the AGILE gateway:
  - The **AGILE Data Cloud Integration** allows to manage data and deploy apps across existing public and private cloud infrastructure,
  - The **Remote GW Management** offers additional services to remotely manage a fleet of Gateways,
  - The **IoT Apps Repository** is a cloud-based repository that hosts AGILE IoT apps and an app recommendations to the project's end-users.

Regarding the hardware architecture, the AGILE Gateway extends the capabilities of the Raspberry Pi platform by developing a "Makers" gateway. Based on Raspberry HAT board specifications[7], the project developed a shield that adds two additional sockets for radio modules and extends the basic connectivity options. The resulting gateway design covers the following objectives [12]:

[7] A Raspberry HAT(Hardware Attached on Top) is an add-on hardware that follows standard specifications, detailed here: https://github.com/raspberrypi/hats.

- small dimensions;
- low power consumption;
- multimodal, multisource modular sensing;
- multiple connectivity options;
- geo-localisation;
- rugged and fine mechanical finishing.

In terms of security, the project follows an attribute-based approach to security. Some of the project's key security features are: **user authentication and registration**; **entity registration** (e.g., for devices such as sensors, OAuth2 clients, etc.); attribute management, allowing for the implementation of various access control mechanisms, such as role-based access control; group management, for defining security policies within a specific group; credential management, which stores credentials for accessing external clouds or systems[8].

Lastly, it is worth noting that the project does not define an approach for semantic interoperability.

2.8 BIOTOPE

bIoTope is an EU funded project, developed within the H2020 initiative. Its goal is to offer the necessary APIs that can help enable horizontal interoperability across cross-domain silos. Following a system-of-systems approach, bIoTope-enabled systems can easily access all available information within the bIoTope ecosystem and create new services and IoT platforms.

[8] http://agile-iot.eu/wp-content/uploads/2018/10/AGILE_D5.3_v1.0_final.pdf

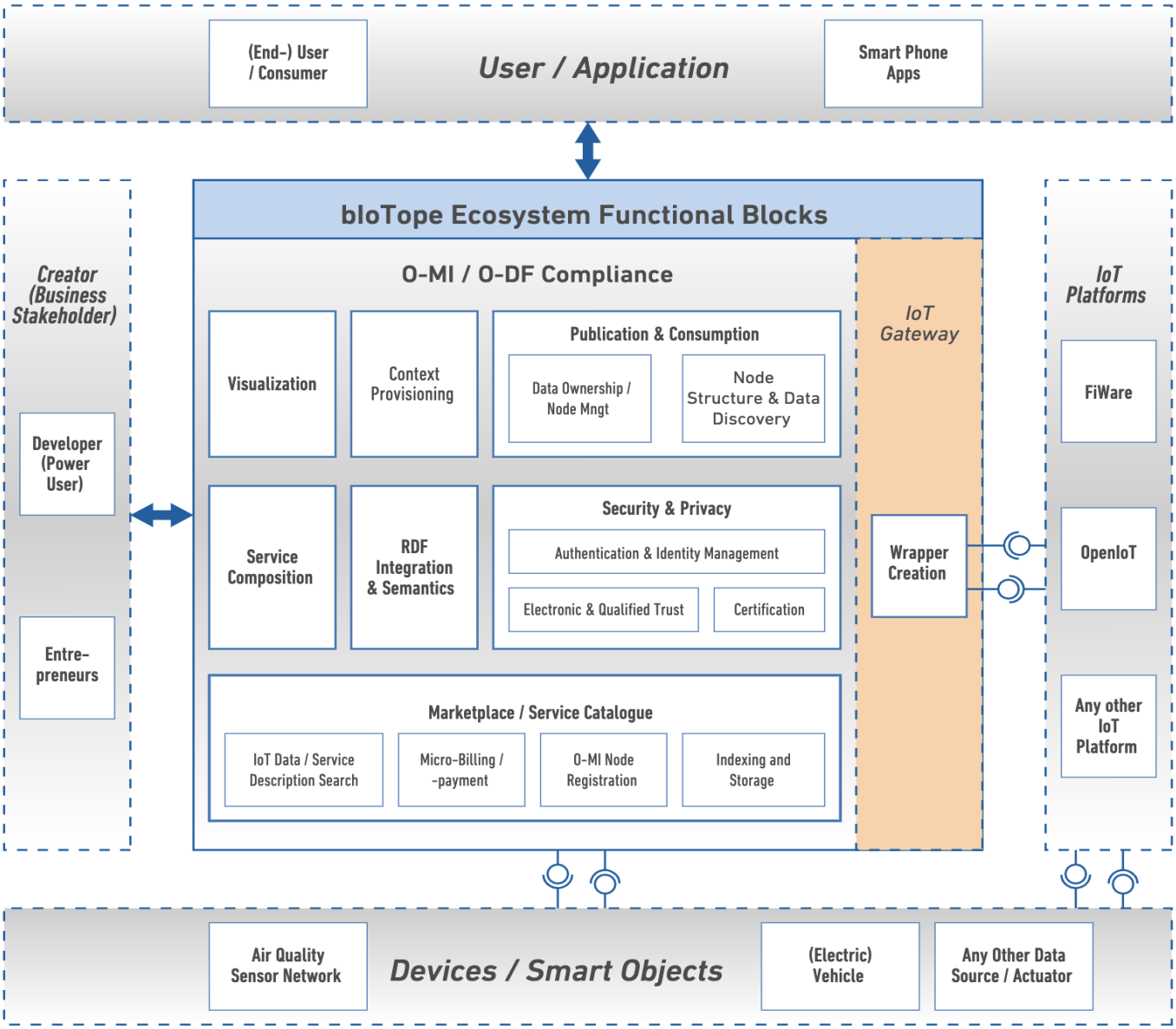


FIGURE 17 - BIOTOPE'S REFERENCE ARCHITECTURE [4]

Figure 17 provides insight into bIoTope's architectural framework, which can be described as a highly flexible and dynamic ecosystem, built around the Micro-Services Architecture (MSA) paradigm [4]. Below, a brief description of bIoTope's key functional blocks:

- **O-MI Nodes** can be viewed as a specific implementation of the Open Messaging Interface (O-MI) standards, defined by The Open Group[9]. The latter provides a framework for real-time, P2P communication between devices (i.e., data publishing and consumption).
- The **Open Data Format (O-DF)** ontology is a standard for representing the payload of IoT applications. It can be defined as a generic object tree representation of information defined by The Open Group, independent of the application or its context. O-DF

9 https://www.opengroup.org/?gclid=CjwKCAjwqML6BRAHEiwAdquMncLVtncwP5flrhl9RlDdZjnJ4iAU9GG3FhAVjKFy76CGJ7ob9ETqFBoCeV4QAvD_BwE

messages can be transported using various messaging protocols or manually, via USB storage drive.

- **Wrappers** are basic software components that translate and expose existing services into the appropriate standards i.e., by using an O-MI node, making the data OD-F compliant. Wrappers can add semantic functionalities to exposed functions, services and data, e.g., through semantic annotation provided by domain-specific ontologies. Each participating IoT platform or device can develop either a specific or a generic wrapper, to improve reusability. Individual connections can be established via the project's IoT Gateway.
- The **Marketplace / Service Catalogue**, and its graphical interface (IoTBnB) allow for service registry and discovery. Additional functionalities, such as billing and payment for accessing available data and services are also offered at this stage.
- The **Service Composition** block enables composition and orchestration of O-MI Nodes as a service, through a NodeRED user interface. Each O-MI Node can the be accessed and queried through the set of available NodeRED functions, once the service workflow has been created.
- The **Publication & Consumption** block enables IoT data publication and consumption trough a Web Service Interface allowing for bidirectional communication based on protocols such as HTTPS. A user interface is also proposed at this stage to enable direct interaction between users and O-MI Nodes.
- The **RDF Integration & Semantics** offers Knowledge as a Service (Kaas) by combining and translating data extracted from O-MI Nodes (i.e., for publication and consumption) and existing Linked Open Datasets[10] into RDF. Once data is expressed in this common format it can be queried using a semantic query language, such as SPARQL.
- The **Visualization** package consists of a user interface offering personalizable dashboards, where data coming from devices can be aggregated and visualized.
- The **Context Provisioning** functional block handles contextual information querying and sharing amongst entities within bIoTope's ecosystem.
- The **Security & Privacy** block provides the required security mechanisms as a service. Security is provided on two levels: the first covers secure authentication and permission methods (i.e., based on OAuth); the second covers secure data transfer and identity management (i.e., MIST).

2.8.1 BIOTOPE'S APPROACH TO SEMANTIC INTEROPERABILITY

bIoTope's semantic interoperability approach is presented in [13]. It can be summarized as supporting an arbitrary information model, extended through domain specific models to cover all use cases specified across pilots.

As presented earlier, the core information model implements The Open Group's O-DF and O-MI standards. Other vocabularies, such as those developed by Schema.org, Semantic

[10] **Linked Open Datasets** can be defined as a collection of datasets released under an open license, made available under a common data vocabulary for semantic data querying. More information on this can be found here: https://www.w3.org/standards/semanticweb/data.

Sensor Network (SSN), and eCl@ss[11] can be used, depending on specific requirements, to cover domain-independent or domain-specific descriptions.

2.9 ANALYSIS AND COMPARAISON

The following section offers a synthetic view of each project's key features and compares it to those that will be offered by the InterConnect project.

In order to provide a synthetic yet comparable view on all of these projects, we've decided to put focus on the following aspects:

- The **Domain** category provides an overview of the key sectors or domains in which the project is involved;
- The **Marketplace** category regroups three sub-categories detailing the main functions offered by each project's marketplace. These functions can be detailed as follows:
    - The **Metadata, annotations** category will be checked if the initiative covered the exchange of interoperable metadata and annotations on a cross-platform or cross-domain setting amongst stakeholders;
    - The **Registry & Discovery** category regroups initiatives offering the possibility to Register and Discover new services via the project's marketplace;
    - The **User Interface** category will regroup projects where a Graphical User Interface (GUI) was developed to facilitate common user interactions with the project's marketplace (e.g., registering a device).
- The **Security** category regroups three incremental sub-categories, each representing an approach to implementing data security & privacy across the project scope. These levels can be defined as follows:
    - **Role-based access-control policy (RBAC)**, where access to certain resources within a network can be restricted to some individual users based on their roles within a group or an enterprise;
    - **Attribute-based access-control policy (ABAC)** allows the definition of a set of attributes (e.g., user attributes, resource attributes, etc.) based on one or more criteria to define each user's access rights;
    - **Ontology-based access-control policy (OBAC)** is an approach to manage access rights where access relies on rules defined within semantic web models and technologies.
- The **Interoperability Framework** category aims to provide an overview of each project's specific approach to interoperability. Three sub-categories are of particular interest:
    - The **interoperability level** based on the IoT World Forum's Reference Model. The goal of this category is to provide a quick overview of the architectural layers covered by each project's reference frameworks. There are seven levels[12]:

[11] eCl@ss is an ISO/IEC-compliant data standard for goods and services, developed and maintained by the eCl@ss e.V. association. More information on this standard can be found here: https://www.semantics3.com/glossary/eclass.

[12] These layers were described at the beginning of this section, in footnote 1. For a more detailed description, visit: http://cdn.iotwf.com/resources/72/IoT_Reference_Model_04_June_2014.pdf.

Physical Devices or "Things", Connectivity, Edge Computing, Data Accumulation, Data Abstraction, Application Layer, and Collaboration and Processes.

- The **Information Model** category describes each project's approach to semantic and syntactic interoperability. Four distinct cases where found: implementation of an existing ontology or standard (E); implementation of a specific ontology, developed and maintain by the project (S); implementation of a modular approach, where extensions to an existing or specific ontology are used to include additional or domain-specific knowledge (X); and no ontology (N/A), in which case the project did not define an approach for semantic/syntactic interoperability amongst stakeholders.
- The **Semantic Reasoner** category regroups projects where semantic reasoning capabilities where included, i.e., new data can be inferred from existing knowledge.

Table 1 identifies and classifies these features.

		Marketplace			Security			Interoperability framework		
	Domain	**Metadata, annotations**	**Registry & Discovery**	**User-Interface**	**Role-based**	**Attribute-based**	**Ontology-based**	**Interopeability level**	**Information model**	**Semantic Reasoner**
symbIoTe	B,M,C		✓	✓	✓	✓		1-7	E+X	
BIG IoT	M, C	✓	✓	✓	✓			6-7	S+X	✓
INTER-IoT	H, E, M	✓	✓		✓			1-6	S+X	
SynchroniCity	C	✓	✓	✓	(✓)[13]	✓		1-7	E+X	
VICINITY	C, M, H, B	✓	✓		✓			3-7	S+X	
Fiesta-IoT	C, B	✓	✓	✓	✓			1-6	S+X	
agile IoT	C, O	✓	✓	✓		✓		1-6	N/A	
bIoTope	C, M, B	✓	✓	✓	✓			1-7	E+X	
InterConnect	E,M	✓	✓	✓			(✓)[14]	1-7	E+X	✓

TABLE 1 – ANALYSIS AND COMPARAISON OF KEY FEATURES ACROSS PROJECTS

[13] Synchronicity offers an attribute-based access-control policy by default but also supports other access-control policies , such as role-based.

[14] At the time of the publication of this deliverable, the InterConnect project aims to provide a Security and Data protection framework that is integrated within the semantic interoperability layer so that defined access control and data/privacy protection rules, required by digital platforms and services, are addressed during semantic discovery and reasoning processes.

Domain		Information model	
E	Energy, Smart Grid	E	Existing ontology or standard
M	Smart mobility	S	Project's specific ontology
C	Smart City	X	Extensions
H	Health, m-health	N/A	Not applicable
I	Cloud, Infrastructure		
S	Smart Homes and Buildings		
O	Others (AgriFood, Environment, etc.)		

3. DIGITAL PLATFORMS CATALOGUE

InterConnect puts together in the same consortium, all relevant players for system operation, providing the basis for interoperability between technologies, but also between service providers (energy or others) and network operators. This section describes the digital platforms available within InterConnect's consortium. This catalogue results from an internal survey that identified twenty-five digital platforms and highlights their general architectures and interoperability indicators.

3.1 ARTEMIS

The platform consists of the Energy data service, a database, a broker, a server (for data acquisition) and the Predictive Analytics service. The Platform analyses and displays the data, offers predictive analytics and sends notifications when the measurements exceed specified thresholds. The current version relies on two algorithms which predict values on an hourly and daily basis. The algorithms provide as output the hourly values that corresponds to the two specified time horizons.

3.1.1 OVERVIEW

Platform name:
ARTEMIS
Partner:
WINGS
Services:
Predictive Analytics
Website:
https://wings-ict-solutions.eu/solutions/utilities
Domain of operation:
<Smart homes>, <IoT>, <Energy domain>
Technology readiness level
<TRL 7>

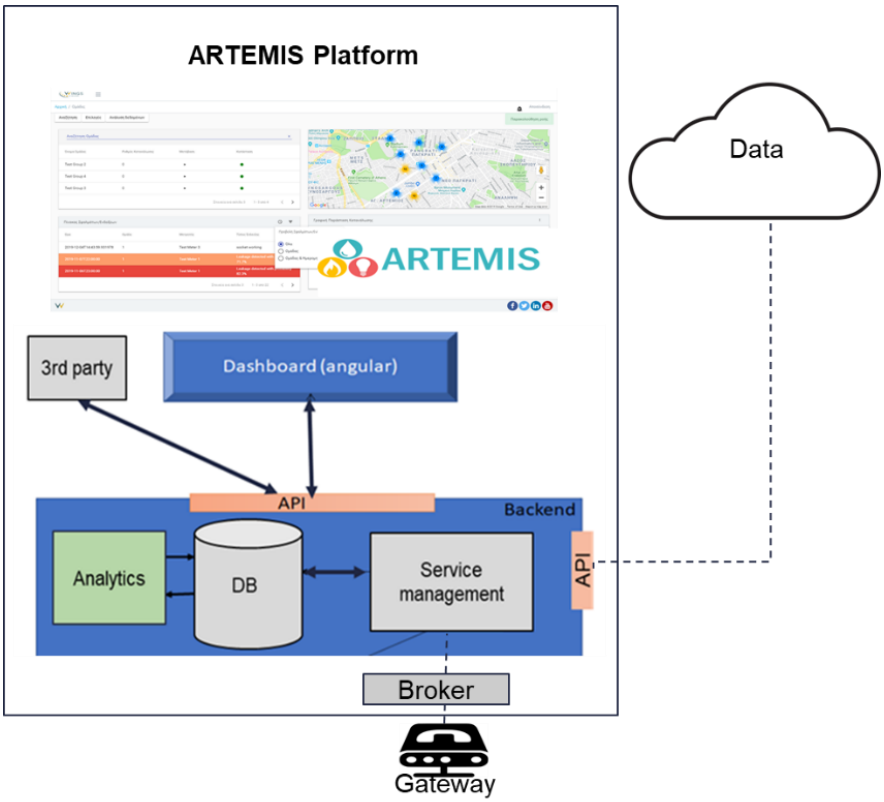


FIGURE 18 - ARTEMIS ARCHITECTURE

3.1.2 INTEROPERABILITY INDICATORS

Data formats
JSON
Data models and ontologies
Custom data model
Protocols for information exchange
REST APIs
Security and data protection
HTTPS, Data encryption, Firewall for database, Authentication of users (passwords), User management
Southbound interfaces:
As described in the architecture there is a southbound interface for connecting to gateways or cloud for acquiring data for analysis and predictions.
Northbound interfaces
As described in the architecture there is a northbound interface for visualizing data on the dashboard and sending recommendations based on predictive analytics to 3rd parties.

3.2 PLANET APP

Planet App monitors the consumptions of end users gathering information from different devices (e.g., smart meters installed in the individual house units, the smart meter owned by the energy provider communicates with our platform (the raw data). In the platform the data is organized, analysed, and processed.

3.2.1 OVERVIEW

Platform name:
Planet App
Partner:
Planet Idea
Services:
Data export for district information and consumption
Website:
https://www.planetsmartcity.com/planet-app/
Domain of operation:
<smart building>, <smart home>, <energy>, <IoT>
Technology readiness level
<TRL 7 >

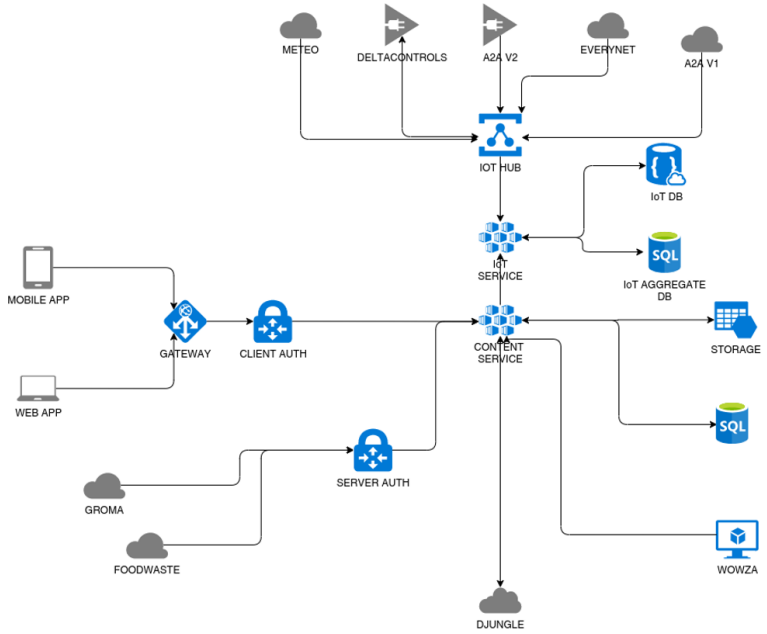


FIGURE 19 - PLANETAPP ARCHITECTURE

3.2.2 INTEROPERABILITY INDICATORS

Data formats
JSON
Data models and ontologies
Proprietary data model.
Protocols for information exchange
MQTT, Web Sockets, HTTP, REST
Security and data protection
GDPR and data segregation
Southbound interfaces:
MQTT, HTTP and web sockets
Northbound interfaces
SOAP, REST and Message queues for third party integration

3.3 CYBERNOC

CyberNOC is a scalable ICT technology that pools flexible resources (e.g. loads, distributed power plants, renewable energy generation, and battery energy storage) into a Virtual Power Plant (VPP) and connects flexibility providers to the various layers of energy markets. VPPs can collect unused or not properly used flexibility and channel it to the electricity system.

3.3.1 OVERVIEW

Platform name:
CyberNOC
Partner:
CyberGrid
Services:
Flexibility facilitator and Virtual Power Plant provider
Website:
Not Addressed
Domain of operation:
<smart home>, <smart building>, <IoT>, <energy>
Technology readiness level
<TRL 8>

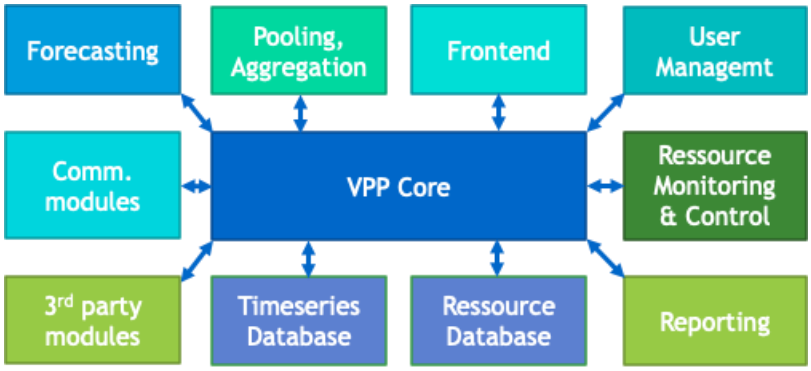


FIGURE 20 - CYBERNOC ARCHITECTURE

3.3.2 INTEROPERABILITY INDICATORS

Data formats
JSON
Data models and ontologies
Custom data model
Protocols for information exchange
MQTT, RabbitMQ, Web sockets, REST
Security and data protection
OAuth, role-based access control
Southbound interfaces:
Modbus, TCP, IEC 60870-5-104
Northbound interfaces
REST

3.4 DYNAMIC COALITION PLATFORM (DCM)

The Dynamic Coalition Manager (DCM) is developed in the FHP project. As a district and building energy management system (DEMS), it will be used in the Belgian Cordium sub-pilot and Belgian ThorPark sub-pilot. The DCM will be adapted or extended to be compliant with the InterConnect interoperability requirements (architecture/interfaces), and to fulfil the required functionality for the Cordium and ThorPark pilots. In the FHP project the DCM was running on VITO's infrastructure (VMs).

3.4.1 OVERVIEW

Platform name:
Dynamic Coalition platform (DCM)
Partner:
Vito
Services:
Building Management
Website:
http://fhp-h2020.eu/
Domain of operation:
<energy>, <smart building>, <smart home>, <IoT>
Technology readiness level
<TRL 5>

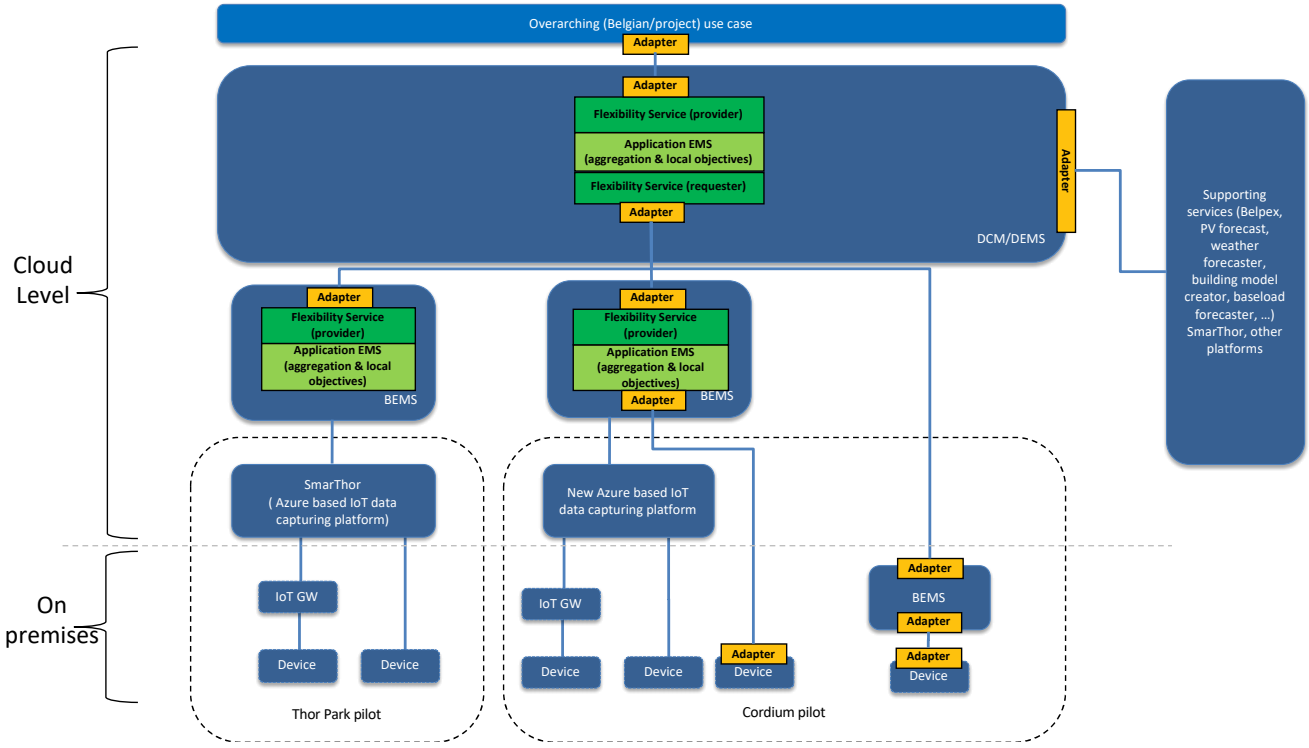


FIGURE 21 - DCM ARCHITECTURE

3.4.2 INTEROPERABILITY INDICATORS

Data formats
JSON, Apache Avro
Data models and ontologies
Not specifically.
Protocols for information exchange
Modbus, KNX, MQTT, AMQP, OMQ, KAFKA, OCPP, REST HTTP.
Security and data protection
Authentication, TLS/SLL encryption, Role-based access control
Southbound interfaces:
The general setup is a hierarchical setup. As such, the DCM does not talk directly to the devices, but always via a GW. However, the DCM concept includes two kinds of GWs: a gateway (BEMS) embedding services like EMS & aggregation, and a pass-through gateway like an IoT gateway. Communication protocols are mostly project-based. In the past (in different projects) ModbusTCP, REST web service (HTTPs), MQTT, AMQP and Kafka interfaces amongst others were used. OCPP is used towards EVSEs.
Northbound interfaces
Services are accessed mostly via web services.

3.5 VITO BEMS

The Building Energy Management System from Vito will be redesigned, taking into account the interoperability guidelines from InterConnect. The platform is based on open components such as TICK stack, Grafana, Home assistant and others. The BEMS concept for InterConnect is based on a cloud application that could be deployed as embedded applications. The embedded application can range from a Raspberry Pi device up to a commercial, industrial grade platform. The architecture for this platform is integrated with platform DCM from Vito in section 3.4. Please refer to Figure 21.

3.5.1 OVERVIEW

Platform name:
BEMS (Building Energy Management System)
Partner:
Vito
Services:
Building Management
Website:
Not addressed.
Domain of operation:
<energy>, <smart building>
Technology readiness level
<TRL 5>

3.5.2 INTEROPERABILITY INDICATORS

Data formats
JSON
Data models and ontologies
CIM, CGMES
Protocols for information exchange
REST, AMQP
Security and data protection
TLS/SSL,
Southbound interfaces:
IEC 60870-5-104
Northbound interfaces
IEC 60870-5-104

3.6 BEEDIP

The extension of software in the energy environment (e.g. SCADA systems) is complex and costly. The expansions often require different data from different sources (e.g. measurements, topology information, master data) and the integration of new modules was up to now mostly reserved to the control system provider. Thanks to beeDIP, it is now easy to add external components to control room software, integrate data and algorithms and test operational control systems without jeopardizing stable operation.

3.6.1 OVERVIEW

Platform name:
beeDIP
Partner:
University Kassel, IEE
Services:
Data integration
Website:
cloud.openmotics.com
Domain of operation:
<energy>
Technology readiness level
<TRL 7>

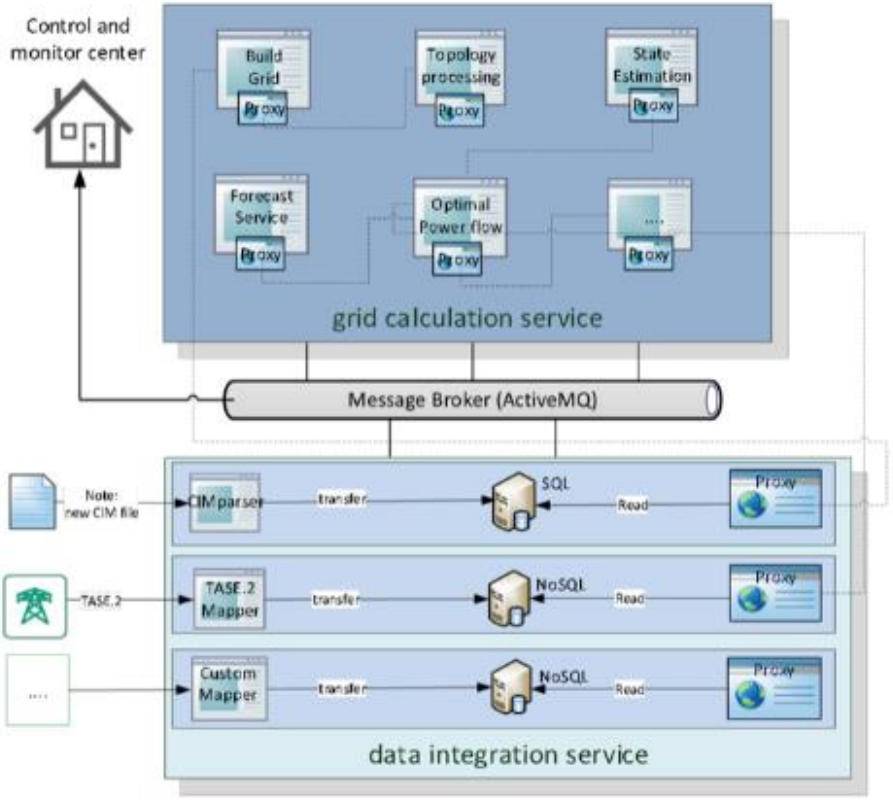


FIGURE 22 - BEEDIP ARCHITECTURE

3.6.2 INTEROPERABILITY INDICATORS

Data formats
JSON
Data models and ontologies
CIM, CGMES, pandapower
Protocols for information exchange
REST, AMQP
Security and data protection
TLS/SSL
Southbound interfaces:
IEC 60870-5-104
Northbound interfaces
IEC 60870-5-104

3.7 SLOR

S-LOR (Sensor-based Linked Open Rules) is a rule-based reasoning engine for sharing and reusing interoperable rules to deduce meaningful knowledge from sensor measurements. S-LOR provides a sensor discovery mechanism to retrieve specific rules classified according to sensor types. S-LOR enables the interaction of users such as web-based application developers with rule-based and semantic reasoning.

3.7.1 OVERVIEW

Platform name:
SLOR – Sensor-based Linked Open Rules
Partner:
Trialog
Services:
Semantic Reasoning and Discovery
Website:
http://linkedopenreasoning.appspot.com/?p=slorv2
Domain of operation:
<smart home>, <smart building>, <IoT>, <energy>
Technology readiness level
<TRL 6>

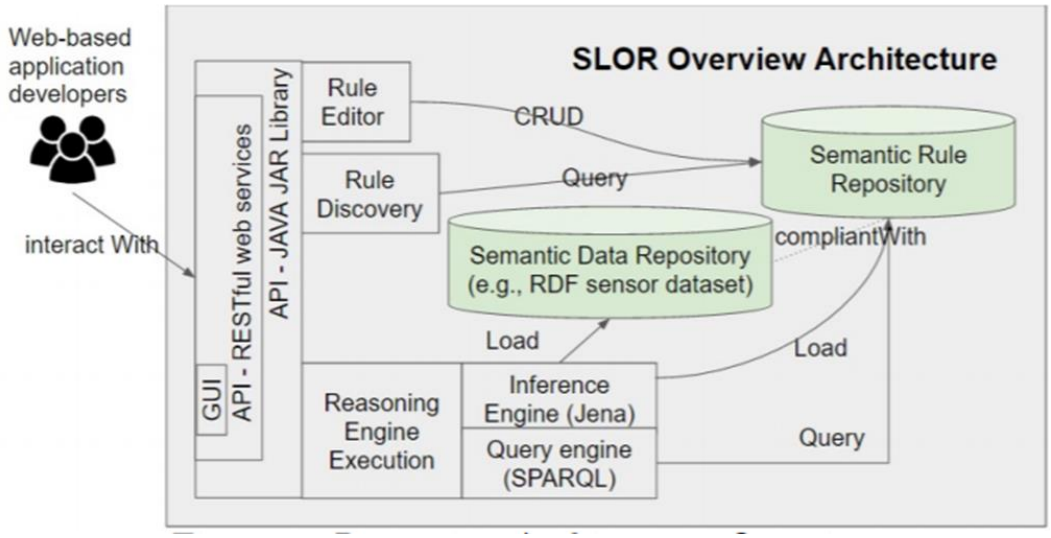


FIGURE 23 - SLOR ARCHITECTURE

3.7.2 INTEROPERABILITY INDICATORS

Data formats
RDF, XML
Data models and ontologies
Ontologies: M3, SAREF, FIESTA-IoT
Protocols for information exchange
SPARQL, REST
Security and data protection
No
Southbound interfaces:
XML, JSON
Northbound interfaces
REST

3.8 REFLEX

ReFlex is a platform for aggregating energy flexibility from multiple sources. It utilizes this aggregated energy flexibility to trade better on wholesale energy markets, provide balancing services and provide congestion management services. ReFlex increases the value of flexibility by using value stacking.

3.8.1 OVERVIEW

Platform name:
ReFlex
Partner:
TNO
Services:
Flexibility Aggregation
Website:
http://reflexenergy.nl/
Domain of operation:
<energy>
Technology readiness level
<TRL 7>

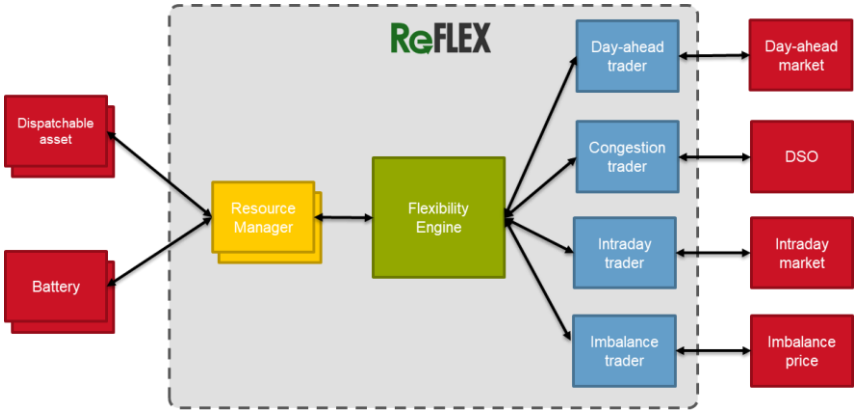


FIGURE 24 - REFLEX ARCHITECTURE

3.8.2 INTEROPERABILITY INDICATORS

Data formats
JSON, XML
Data models and ontologies
Not Addressed
Protocols for information exchange
REST, Web Sockets
Security and data protection
HTTPS, role-based access control
Southbound interfaces:
Energy Flexibility Interface (EFI) (S2/prEN50491-12-2)
Northbound interfaces
Proprietary interfaces (markets, balancing), UFTP (USEF Flexibility trading)

3.9 DEF-PI

DEF-Pi is an open-source platform to run energy-related, microservice-based IoT application. It can run microservices (which we call Apps), which can communicate with each other. Apps can run on both in the cloud and on edge devices (the App doesn't know) and can be moved and reconfigured at run-time. The idea is that specific interfaces for devices (e.g., Modbus, Z-Wave) and optimization systems (e.g., PowerMatcher, OpenADR, tariff-based optimization) can easily be supported by installing an App.

3.9.1 OVERVIEW

Platform name:
dEF-Pi (Distributed Energy Flexibility Platform and Interface)
Partner:
TNO
Services:
Integrator for third-party data services
Website:
https://github.com/flexiblepower/defpi-core
Domain of operation:
<IoT>, <energy>
Technology readiness level
<TRL 7>

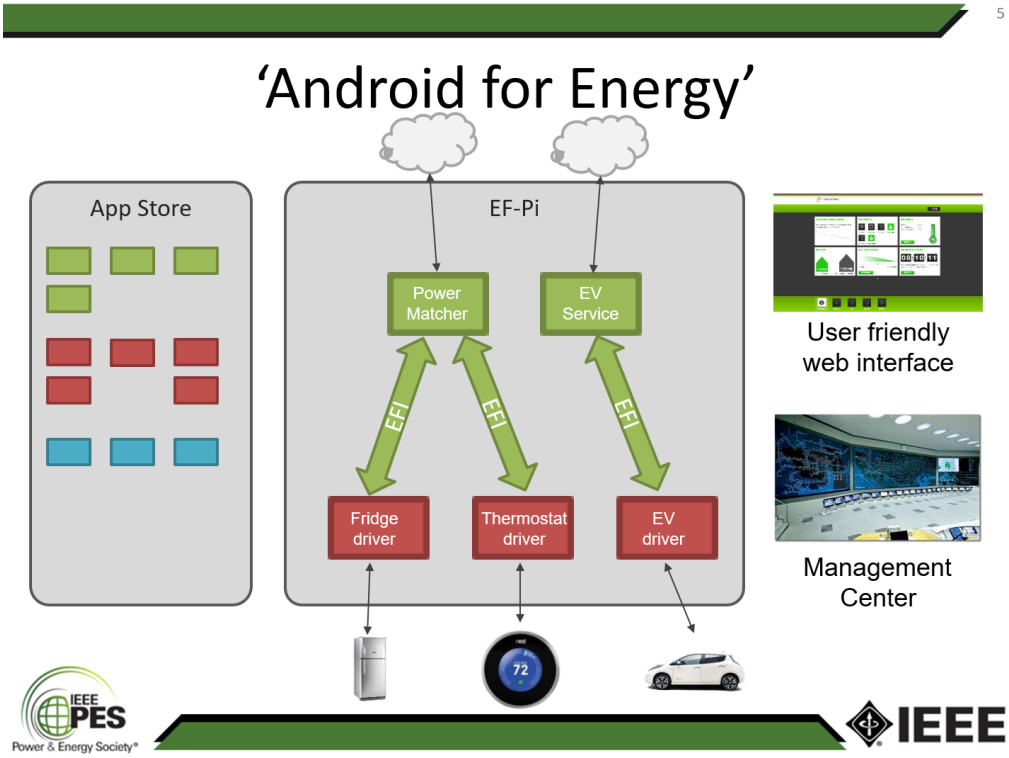


FIGURE 25 - DEF-PI ARCHITECTURE

3.9.2 INTEROPERABILITY INDICATORS

Data formats
XML, Protocol Buffers, REST
Data models and ontologies
Custom data model
Protocols for information exchange
Proprietary
Security and data protection
HTTPS, VPN tunnelling, penetration tests for security validation, data segregation
Southbound interfaces:
Modbus, ZigBee, Z-wave
Northbound interfaces
OpenADR, PowerMatcher, EFI

3.10 THERMOVAULT

The digital platform is responsible for steering electrical thermal appliances. The platform will allow other partners to register their devices to the ThermoVault pool and receive operation commands to leverage the flexibility of their devices and provide multiple energy services.

3.10.1 OVERVIEW

Platform name:
ThermoVault
Services:
Flexibility steering for devices
Website:
No specific website.
Domain of operation:
<energy>
Technology readiness level
<TRL 9>

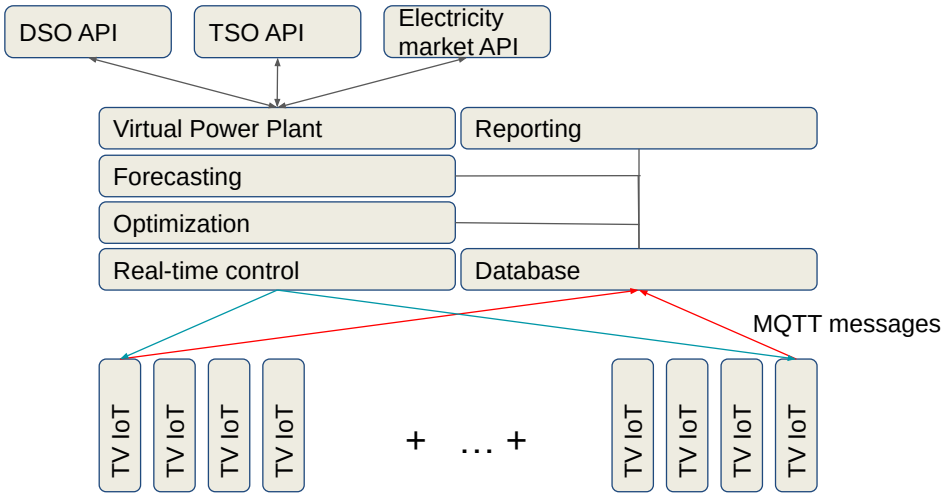


FIGURE 26 - THERMOVAULT ARCHITECTURE

3.10.2 INTEROPERABILITY INDICATORS

Data formats
JSON
Data models and ontologies
No standard data models or ontologies are used.
Protocols for information exchange
MQTT
Security and data protection
MQTT TLS connection, role-based access control
Southbound interfaces:
MQTT
Northbound interfaces
Not Addressed

3.11 SENSINOV

Sensinov is an IoT interoperability cloud-based platform. It allows Building Managers to monitor and control multiple buildings regardless of vendors, offering continuous integration/operation, data exposure via API and centralized building management.

3.11.1 OVERVIEW

Platform name:
Sensinov
Services:
Building Management; Data collection and sharing, control of remote devices, Statistics, Semantic enrichment
Website:
https://sensinov.com
Domain of operation:
<smart building>, <IoT>
Technology readiness level
<TRL 9>

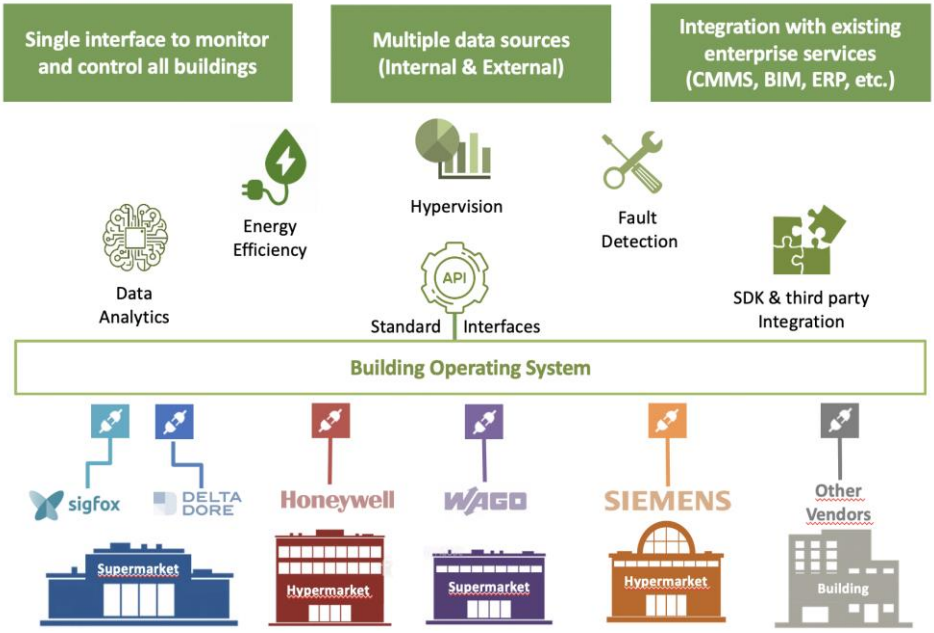


FIGURE 27 - SENSINOV ARCHITECTURE

3.11.2 INTEROPERABILITY INDICATORS

Data formats
JSON
Data models and ontologies
Custom data model based on SAREF, SAREF4ENER, HayStack a ndBrick.
Protocols for information exchange
SPARQL
Security and data protection
TLS/SSL, JWT, authentication, role-based access control. GDPR compliant.
Southbound interfaces:
Connectors (Modbus, Profibus, LoRa, Sigfox, Zigbee, EnOcean, Z-Wave, KNX, etc.)
Northbound interfaces
REST, Web Sockets

3.12 ECOSTRUXURE BUILDING OPERATION

Building Management System Platform. Can be applied to HVAC Control, Lighting Control, Energy Management, Fire Safety, Security & Access Control and Workplace Management Systems. The platform consists in a layer of software (Enterprise Central, Enterprise Server) and hardware (SmartX Controllers). The software layer can be installed locally or hosted in the cloud. Any element of the EBO platform, whether software or hardware, provides the same communication protocols. This means that integration with third-party digital platforms can be done through the software or hardware layer.

3.12.1 OVERVIEW

Platform name:
EcoStruxure Building Operation
Partner:

SE Portugal
Services:
Building management
Website:
https://www.se.com/ww/en/product-range-presentation/62111-ecostruxure%E2%84%A2-building-operation/#tabs-top
Domain of operation:
<smart building>, <IoT>, <energy>
Technology readiness level
<TRL 9>

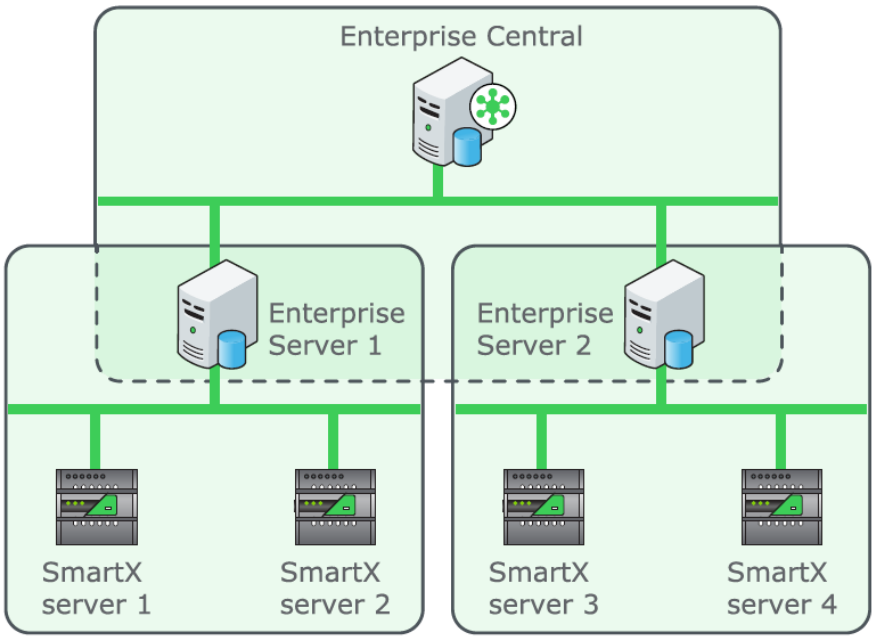


FIGURE 28 - ECOSTRUXURE BUILDING OPERATION ARCHITECTURE

3.12.2 INTEROPERABILITY INDICATORS

Data formats
JSON, XML
Data models and ontologies
Haystack, Brick
Protocols for information exchange
Bacnet, Modbus, KNX, LonWorks, MQTT, REST, SOAP, XML
Security and data protection
IEC62443, CFR21, TLS/SSL, role-based access control
Southbound interfaces:
IO's, Modbus, Bacnet, Lonworks, KNX, MQTT, WebServices (SOAP, REST, XML);
Northbound interfaces
REST, SAOP, SmartConnector

3.13 KONECT

Konect offers software packages for energy-relevant devices and systems to implement smart energy management based on the EEBUS standard. Our EEBUS Solution Sets contain all relevant EEBUS Use Cases – tailored to each important domain for each device and system.

3.13.1 OVERVIEW

Platform name:
Konect – Base of several EEBUS Solution Sets
Partner:
KEO
Services:
Integrator for EEBUS devices
Website:
www.keo-connectivity.de
Domain of operation:
<smart home>, <smart building>, <IoT>, <energy>
Technology readiness level
<TRL 7>

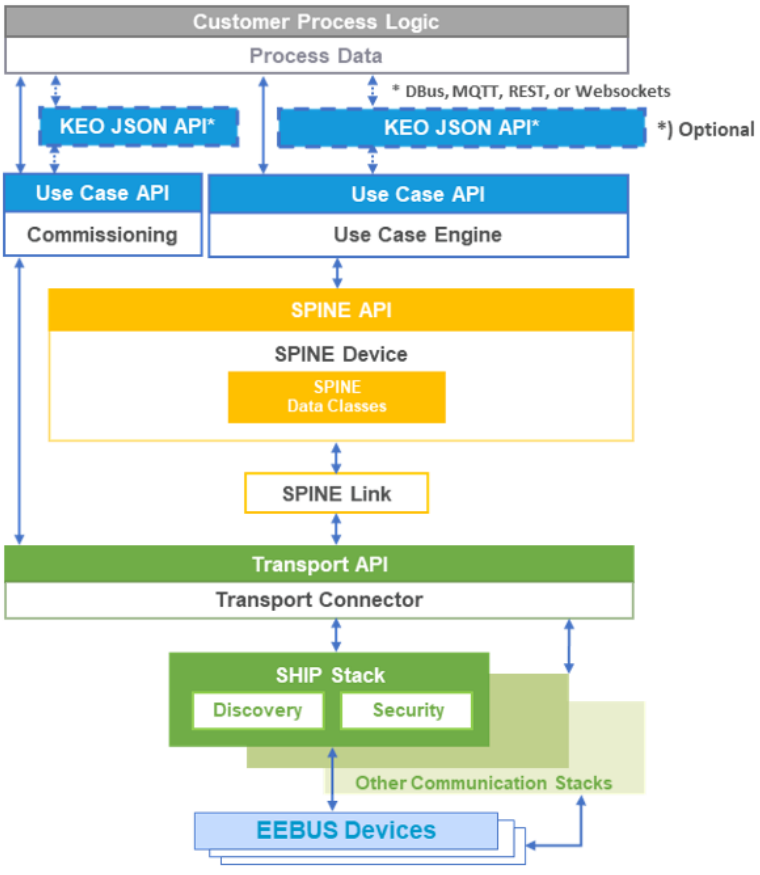


FIGURE 29 - KONECT ARCHITECTURE

3.13.2 INTEROPERABILITY INDICATORS

Data formats
JSON
Data models and ontologies
EEBUS SPINE data model, SAREF4ENER
Protocols for information exchange
SPINE, SHIP, WebSockets, MQTT, REST, dBus, mDNS
Security and data protection
TLS
Southbound interfaces:
EEBUS
Northbound interfaces
MQTT, REST, Web Sockets, dBUS

3.14 GRID AND MARKET HUB

The gm-hub can be defined as a cloud-based solution to support the provision of services in a neutral standardized way between distribution system operators (DSO) (primary actor of this central platform) and stakeholders like retailers, transmission system operators (TSOs), aggregators, group of users and energy services providers (e.g., energy service companies (ESCo), data analytics companies).

3.14.1 OVERVIEW

Platform name:
Grid and Market Hub Platform
Partner:
INESC TEC
Services:
Flexibility for grid operation; Traffic Light System for VPP communication; Front-end consumer infographics: Alarms about high consumption patterns (B2C), Consumption profile for service enhancement (third-party B2B).
Website:
https://gmhub-integrid.eu
Domain of operation:
<energy>
Technology readiness level
<TRL 7 >

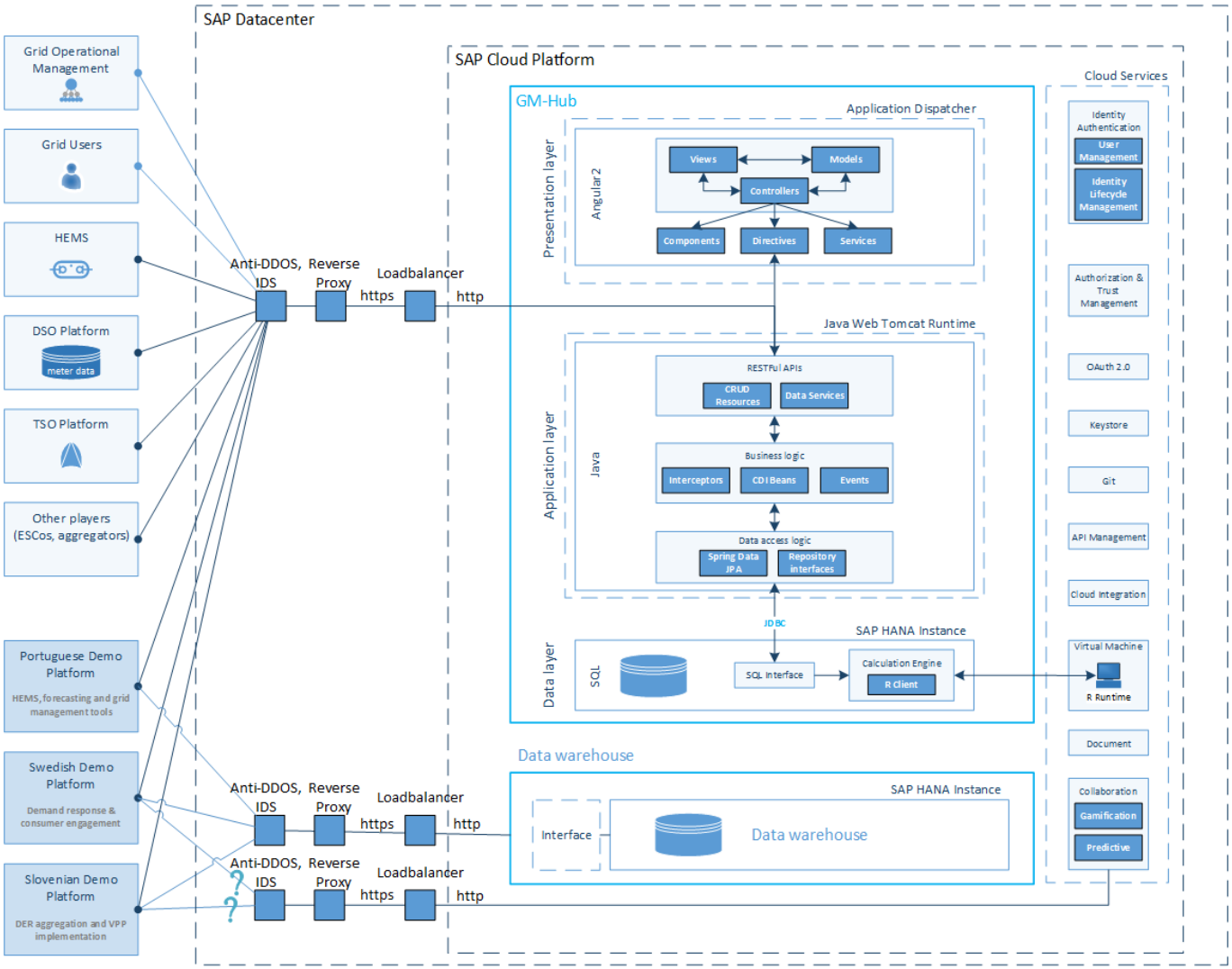


FIGURE 30 - GRID AND MARKET HUB ARCHITECTURE

3.14.2 INTEROPERABILITY INDICATORS

Data formats
JSON
Data models and ontologies
Proprietary APIS, based on CIM.
Protocols for information exchange
JSON-LD
Security and data protection
TLS/SSL, role-based access control, X.509 authentication
Southbound interfaces:
REST
Northbound interfaces
REST

3.15 COGNITIVE LOAD

The Cognitive Load platform provides time series pre-processing and forecasting tools for energy consumption and renewable energy. It holds functions for data cleaning, feature engineering, machine learning and deep learning and uncertainty forecasts.

3.15.1 OVERVIEW

Platform name:
Cognitive Load
Partner:
INESCTEC
Services:
Data cleaning, feature engineering, machine learning and deep learning and uncertainty forecasts.
Website:
Not addressed
Domain of operation:
<energy>
Technology readiness level
<TRL 8 >

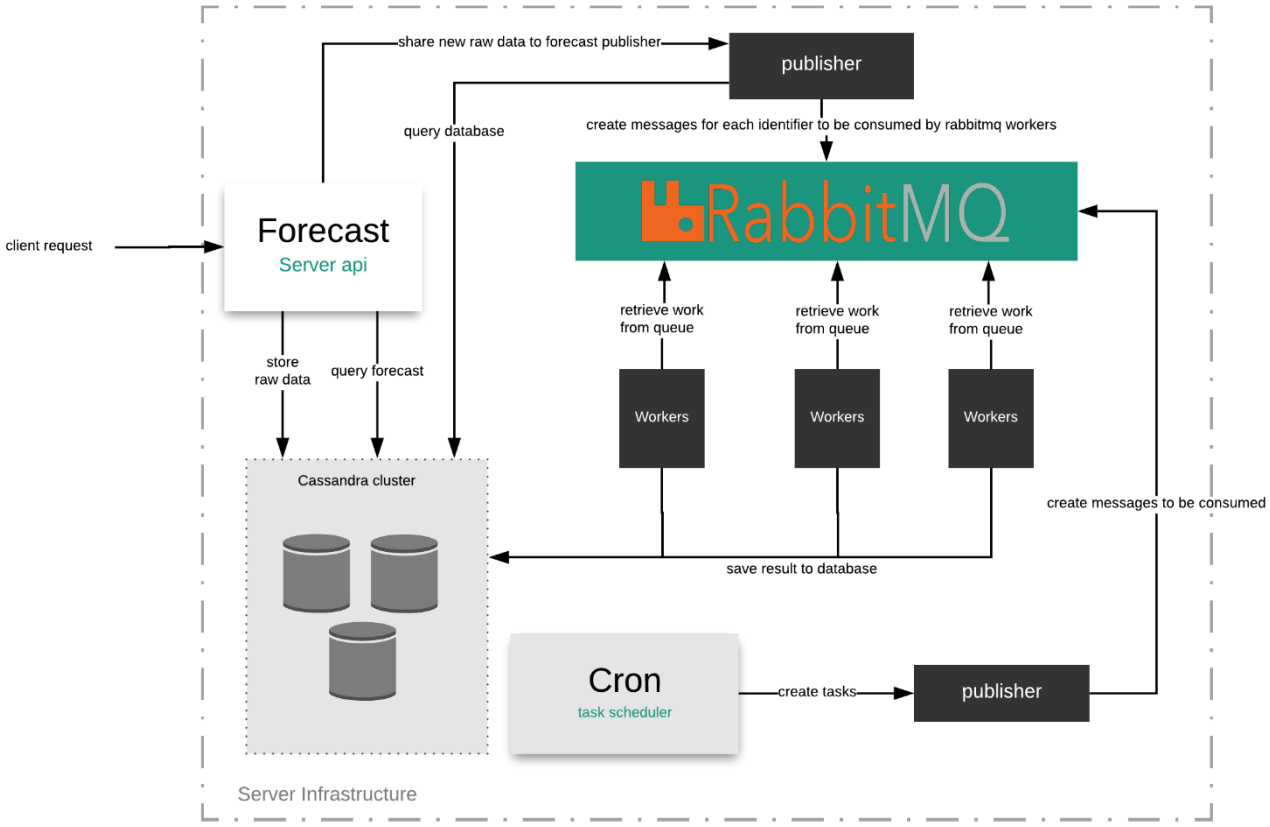


FIGURE 31 - COGNITIVE LOAD ARCHITECTURE

3.15.2 INTEROPERABILITY INDICATORS

Data formats
JSON
Data models and ontologies
Custom
Protocols for information exchange
REST
Security and data protection
No
Southbound interfaces:
Any
Northbound interfaces
REST

3.16 DYAMAND

DYAMAND offers the integration of devices irrespective of the technologies used by the devices. It consists of three components, the DYAMAND client, a software component that is to be installed on a gateway towards the devices to communicate with. This can be a local gateway in case of short-range technologies or in the cloud in case of long-range technologies. Second, the backend provides services to be able to monitor and manage installations (instances of DYAMAND client), discovered devices and applications. Third, the DYAMAND dashboard offers a visualization of all information gathered in the DYAMAND ecosystem. The combination of these components allows DYAMAND to adapt both to an ever-changing technology landscape of connected device technologies, and to adapt to the application(s) that want to use the data gathered from the devices and/or control the discovered devices.

3.16.1 OVERVIEW

Platform name:
DYAMAND (DYnamic, Adaptive Management of Networks and Devices)
Partner:
IMEC
Services:
Device integrator, device control, discovery, data retrieval
Website:
https://www.dyamand.be/
Domain of operation:
<smart building>, <smart Home>
Technology readiness level
<TRL 7>

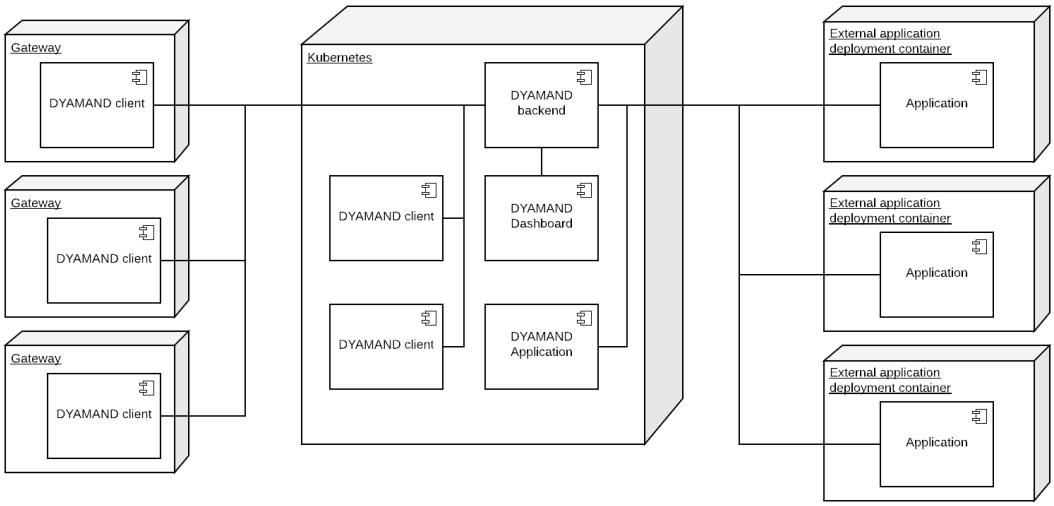


FIGURE 32 - DYAMAND ARCHITECTURE

3.16.2 INTEROPERABILITY INDICATORS

Data formats
JSON
Data models and ontologies
Custom data model
Protocols for information exchange
HTTP
Security and data protection
Authentication, TLS/SSL, role-based access control
Southbound interfaces:
LoRA, ZibBee, others
Northbound interfaces
GraphQL

3.17 ECKO IOT PLATFORM

Hyrde Ekco IoT Platform plays an important role in the overall Hyrde IoT enablement ecosystem. Consisting of a Web portal, Mobile app generator and 3rd party API integrator, Ekco is designed to support Not Addressed Industry through its unique Business Rules and Process platform.

3.17.1 OVERVIEW

Platform name:
Hyrde Ekco IoT Platform
Partner:
Hyrde Volkerwessels iCity
Services:

Data collection and sharing, Command and control of devices, Statistics, Rule-engine, Connector's life-cycle management, Administration, Semantic Enrichment
Website:
https://ekco.co.nl/
Domain of operation:
<Smart building>, <smart home>, <general IoT>, <Fleet telematics>, <Asset tracking>, <smart parking>, <Data science and analytics>, <Business Process automation>, <AI and Image recognition>, <object detection>, <machine learning>
Technology readiness level
<TRL 9>

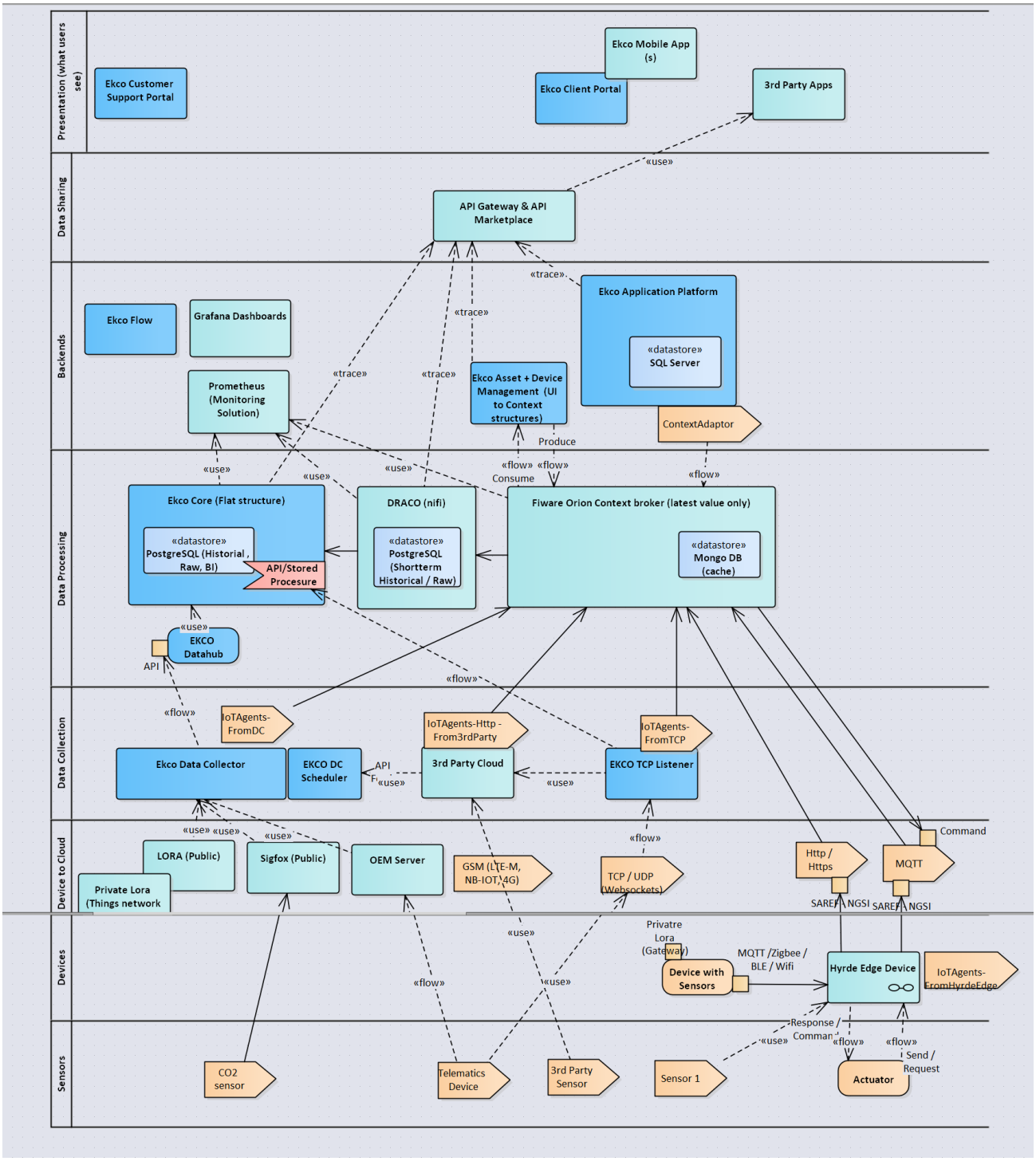


FIGURE 33 - EKCO PLATFORM ARCHITECTURE

3.17.2 INTEROPERABILITY INDICATORS

Southbound interfaces:
Modbus, LoRa, Sigfox, Zigbee, Z-Wave, BLE, SPINE (to be completed), SHIP (to be completed), HTTP Post
Northbound interfaces
RESTFUL APIs, Web sockets, MQTT, webhooks, HTTP Post
Data formats
JSON
Data models and ontologies
Based on an in-house developed Unified data model and common vocabulary
Protocols for information exchange
MQTT, JSON-LD (to be completed), NGSI-v2(to be completed), JSON, Web Sockets
Security and data protection
GDPR compliant, TLS, SSL, JWT and authentication/authorization

3.18 EKCO MARKETPLACE

Hyrde Ekco API Marketplace and IoT micropayment platform allows developers to search and test the APIs, subscribe, and connect to the APIs — all with a single account, single API key and single SDK. Project developers use the Ekco API marketplace to share internal APIs and microservice documentation, and via a search-engine-optimized profile page access features like user management and billing services. Each team can view all of the APIs that are connected to using the dashboard, which monitors things like the number of API requests, latency, and error rates.

3.18.1 OVERVIEW

Platform name:
Hyrde Marketplace
Partner:
Hyrde Volkerwessels iCity
Services:
API Hub, Marketplace and micropayment facilitator
Website:
https://www.hyrde.io/
Domain of operation:
<Smart building>, <smart home>, <IoT>
Technology readiness level
<TRL 9>

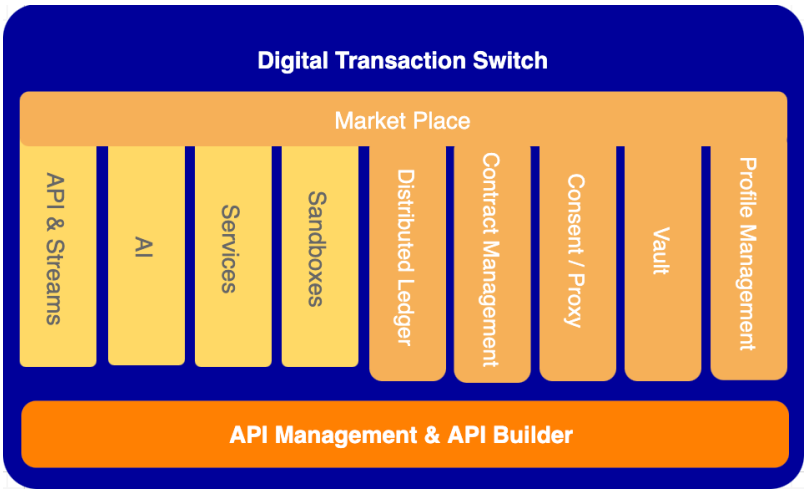


FIGURE 34 - ECKO PLATFORM

3.18.2 INTEROPERABILITY INDICATORS

Data formats
JSON
Data models and ontologies
Based on an in-house developed Unified data model and common vocabulary
Protocols for information exchange
MQTT, JSON-LD (to be completed), NGSI-v2(to be completed), JSON, Web Sockets
Security and data protection
GDPR compliant, TLS, SSL, JWT and authentication/authorization

3.19 HOMEGRID

GridNet platform consists of two entities, the smart home gateway powered by OpenHAB rule engine and a frontend where user can view dashboards with real-time data of their home and historical data. The platform provides demand-side flexibility scenarios for residential setups.

3.19.1 OVERVIEW

Platform name:
HomeGrid
Partner:
Gridnet SA
Short description:
Device control and actuation via gateway, Metering and monitoring, automation scenarios, historical data.
Website:
A custom visualization interface is under development and it will be launched soon.
Domain of operation:
<smart home>, <IoT>, <energy>
Technology readiness level
<TRL 7>

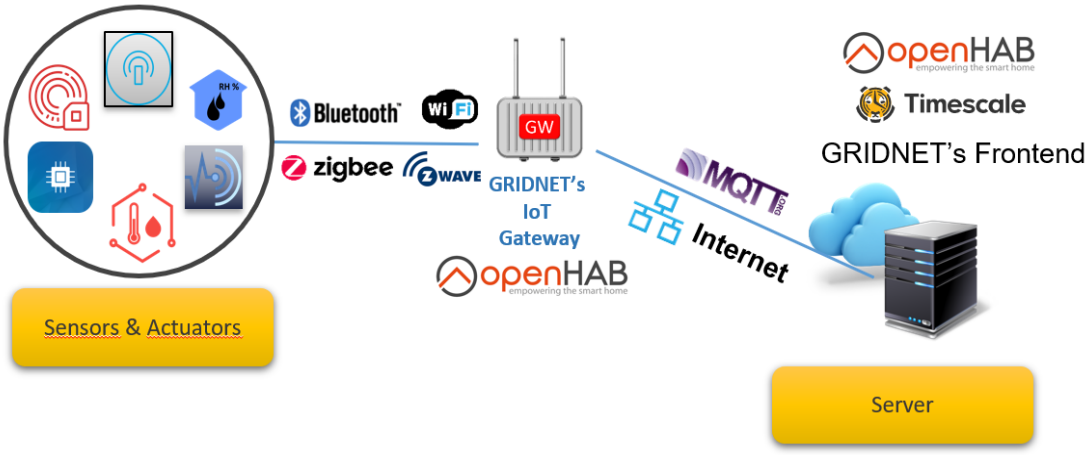


FIGURE 35 - HOMEGRID ARCHITECTURE

3.19.2 INTEROPERABILITY INDICATORS

Data formats
JSON
Data models and ontologies
No standard data models or ontologies are used.
Protocols for information exchange
MQTT, Web Sockets
Security and data protection
SSL/TLS, role-based access control
Southbound interfaces:
MQTT, Bluetooth, ZigBee, ZWave
Northbound interfaces
REST

3.20 GFI SEMANTIC IOT PLATFORM

The Gfi Semantic IoT Platform (SIP) facilitates the smart appliance interoperability ecosystem by automatically finding the needed information, performing the syntax and semantic negotiation and executing within the required context. It federates and provides uniform access information coming from different sources within the complex appliances & energy ecosystem. Effectively, the SIP will increase the situational awareness of business applications by connecting them to features of interests captured by sensory data & IoT such as appliances, meters, homes, buildings, people, etc. in the physical world as well as other data sources like open data can be used. This is done in a secure and reliable manner via a user-friendly interface to engage with the stakeholders in different domains.

3.20.1 OVERVIEW

Platform name:
GFI Semantic IoT Platform
Partner:
GFI
Services:
Data ingestion and exchange between devices, Marketplace for semantic data access from sensors, creation of new data driven services and business models.
Website:
Not Addressed
Domain of operation:
<smart home>,<smart building>
Technology readiness level
<TRL 5>

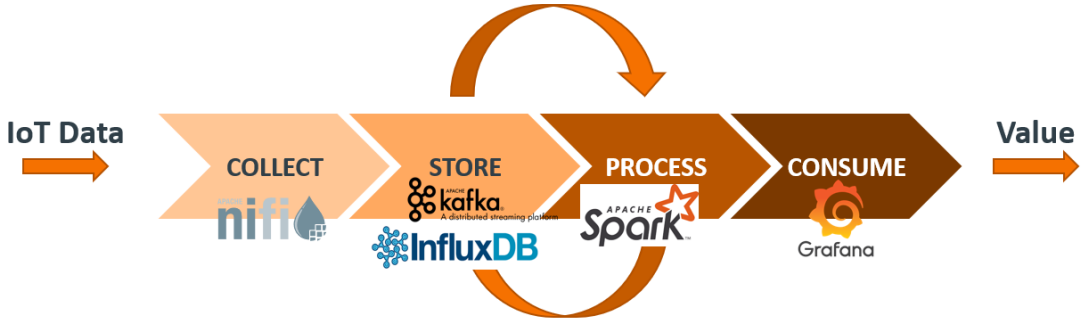


FIGURE 36 - GFI SEMANTIC IOT PLATFORM ARCHITECTURE

3.20.2 INTEROPERABILITY INDICATORS

Data formats
JSON
Data models and ontologies
Custom data model. Any ontology
Protocols for information exchange
HTTP, MQTT, Web Sockets
Security and data protection
OAuth2, TLS/SSL,
Southbound interfaces:
LoRa, SigFox, ZigBee, Z-Wave, NB-IOT, MWTT, FTP, SNMP, OPC-UA
Northbound interfaces
CoAP, WebSockets, REST

3.21 LEONAR&DO

The LeonaR&Do IoT platform is a flexible, scalable, vendor and technology agnostic and secure e2e solution – developed from scratch exclusively by COSMOTE - that can integrate a wide range of (commercial/custom) sensors, any technology, supported by a common backend infrastructure for data storage, processing, visualization and command exchange.

3.21.1 OVERVIEW

Platform name:
LeonaR&Do
Partner:
Cosmote
Services:
Energy-Power measurement and monitoring, Home Comfort, Advanced automation, Security, Real-Time and historical data visualization
Website:
Not Addressed
Domain of operation:
<energy>, <smart building>, <smart home>, <IoT>
Technology readiness level
<TRL 7>

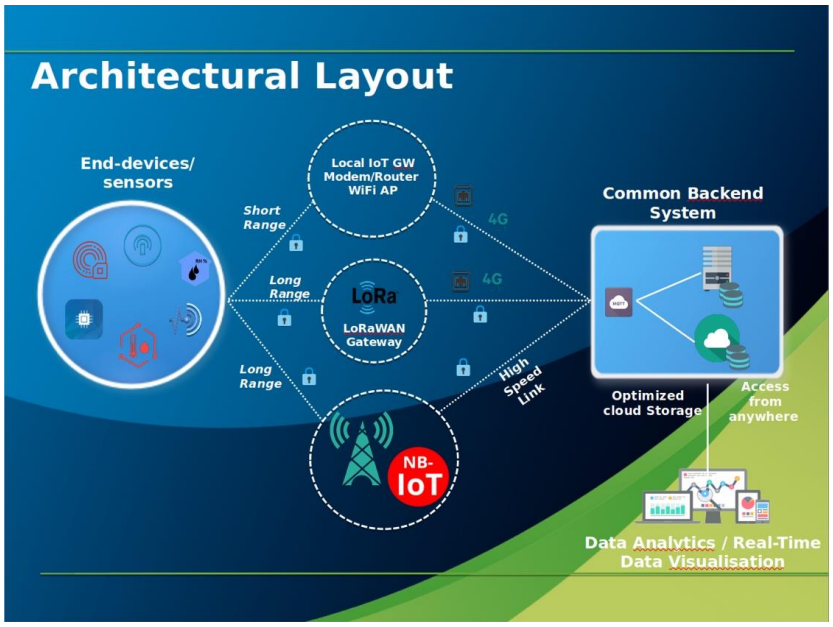


FIGURE 37 – LEONAR&DO ARCHITECTURE

3.21.2 INTEROPERABILITY INDICATORS

Data formats
JSON
Data models and ontologies
Custom data model
Protocols for information exchange
HTTPS, FTP
Security and data protection
TLS/SSL, role-based access control
Southbound interfaces:
MSSQL SCADA, custom interfaces
Northbound interfaces
REST

3.22 OPENMOTICS

The platform is mainly used in the area of Smart Homes and Buildings. It connects Homes with their sensors, devices and appliances to centralized appliances and services. It allows as such to build communities for different types of services. It is a platform for anybody interested in creating (non-)energy services for Smart Homes, Buildings and Communities.

3.22.1 OVERVIEW

Platform name:
OpenMotics Cloud Platform
Partner:
OpenMotics
Services:
Integration between devices and home/building management, Building community services
Website:
cloud.openmotics.com
Domain of operation:
<smart home>,<smart building>
Technology readiness level
<TRL 9>

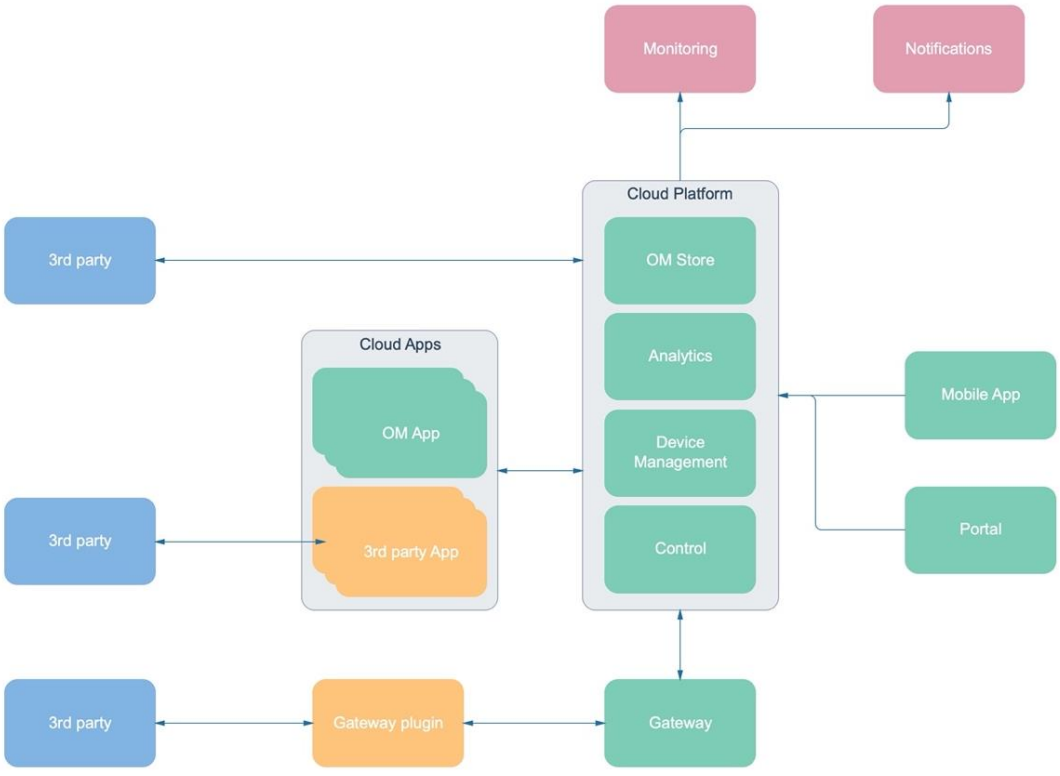


FIGURE 38 - OPENMOTICS CLOUD PLATFORM ARCHITECTURE

3.22.2 INTEROPERABILITY INDICATORS

Data formats
JSON
Data models and ontologies
Custom data model, custom ontology for metric collection
Protocols for information exchange
MQTT, Web sockets, HTTPS, BACnet, modbus
Security and data protection
OAuth2, TLS/SSL, role-based access control
Southbound interfaces:
Ethernet, RS232, RS485, CAN bus
Northbound interfaces
REST

3.23 TIKO

Tiko allows to connect all types of electrical devices, such as heating systems, coolers, PV systems, batteries or e-car charging stations, independently of their brand, and to manage them through apps and web-based applications (temperature control with heaters, consumption visualization). By aggregating those residential small loads, it offers a Virtual Power Plant which provides flexibility down to a 1-second reaction time.

3.23.1 OVERVIEW

Platform name:
Tiko
Partner:
Tiko (via ENGIE)
Services:
Load aggregation, VPP, Integration between devices home/building management.
Website:
https://tiko.energy/
Domain of operation:
<smart home>, <energy>
Technology readiness level
<TRL 9>

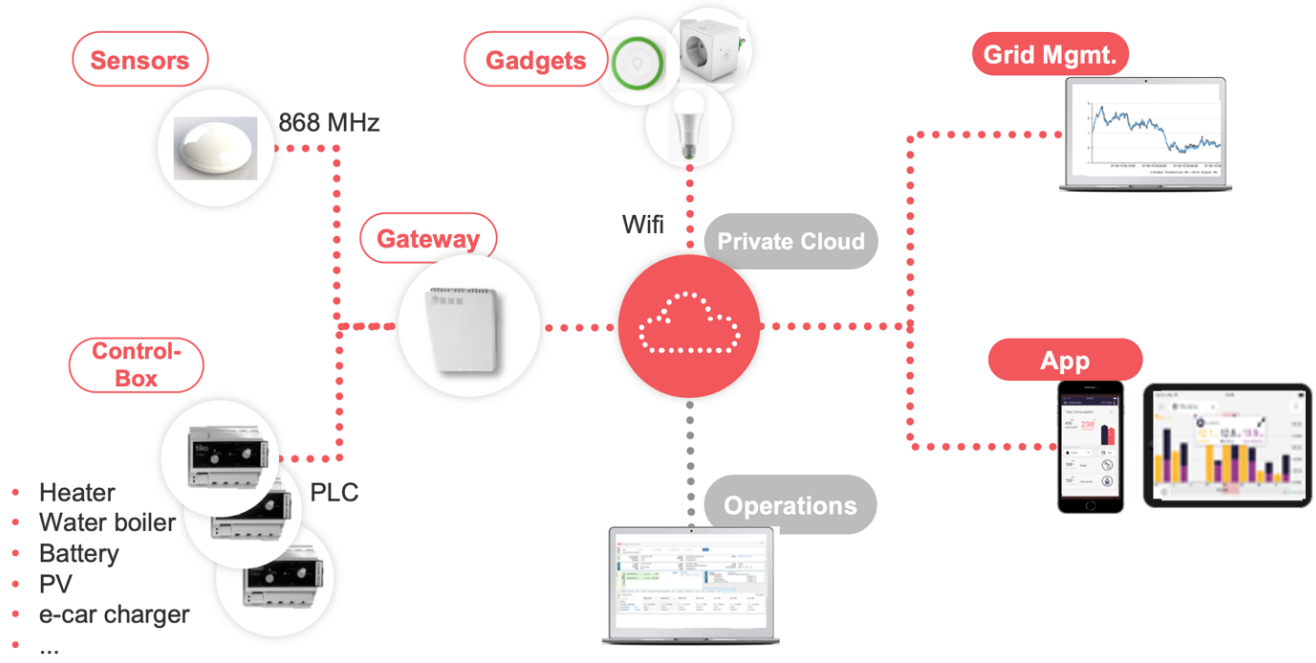


FIGURE 39 - TIKO ARCHITECTURE

3.23.2 INTEROPERABILITY INDICATORS

Data formats
JSON
Data models and ontologies
Proprietary data model
Protocols for information exchange
ModBus, PLC
Security and data protection
TLS/SSL; VPN tunnelling, role-based access control
Southbound interfaces:
Modbus, PLC
Northbound interfaces
REST

3.24 E-FLEX

E-Flex allows flexibility providers to describe their offers, to that the DSO can request their activation and mange that flexibility via the delivery points that are associated. This platform does not perform commercial negotiations.

3.24.1 OVERVIEW

Platform name:
E-Flex
Partner:
ENEDIS
Services:
Flexibility bidding and aggregation, Flexibility activation
Website:
Not Addressed
Domain of operation:
<energy>
Technology readiness level
<TRL 7>

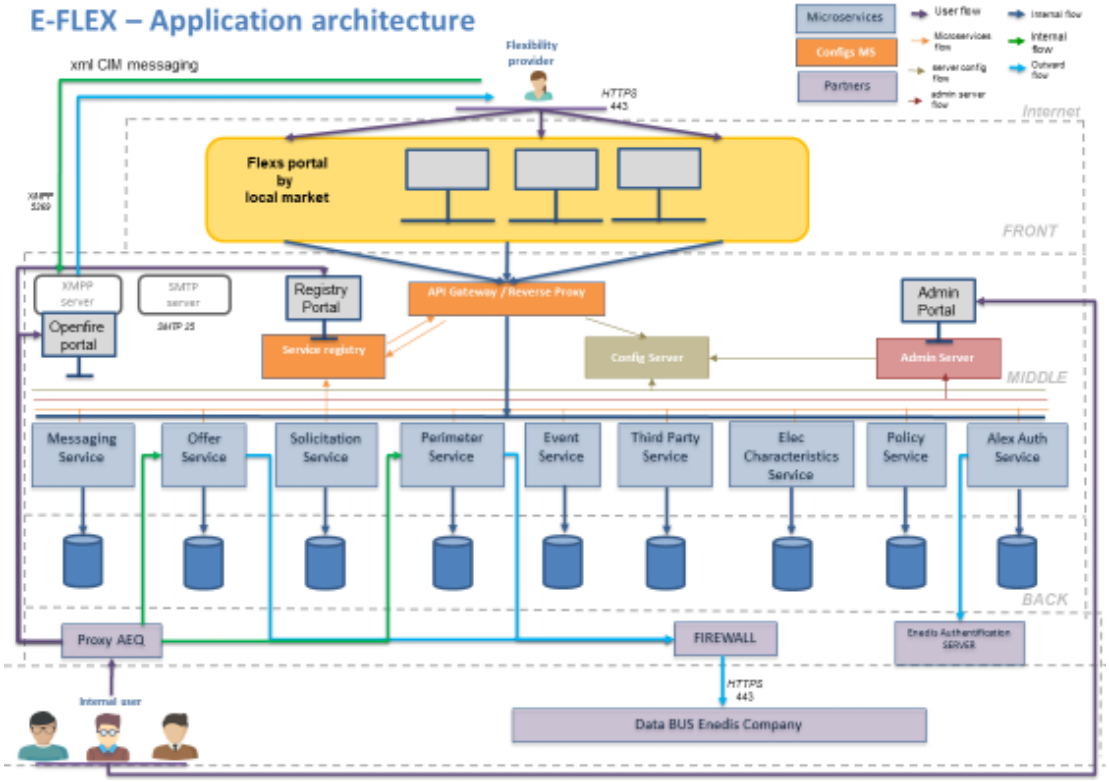


FIGURE 40 - E-FLEX ARCHITECTURE

3.24.2 INTEROPERABILITY INDICATORS

Data formats
XML
Data models and ontologies
IEC CIM
Protocols for information exchange
XMPP, SMTP
Security and data protection
Yes. GDPR compliant
Southbound interfaces:
Proprietary interfaces to send, receive offers. SCADA and flow grid management.
Northbound interfaces
Proprietary interfaces for offer creation, manipulation and flexibility activation.

3.25 SYNAPTIQ POWER

SynaptiQ Power builds on the commercial platform 3E SynaptiQ, which is a commercial platform for asset operations & management in the domain of renewable energy. SynaptiQ currently connects over 6 GW of solar PV plants through more than 1 Mio IoT devices, and is being extended to include the monitoring & control of batteries and EV chargers.

3.25.1 OVERVIEW

Platform name:
SynaptiQ Power
Partner:
3E
Services:
Grid asset management
Website:
https://www.3e.eu/synaptiq/
Domain of operation:
<energy>
Technology readiness level
<TRL 5>

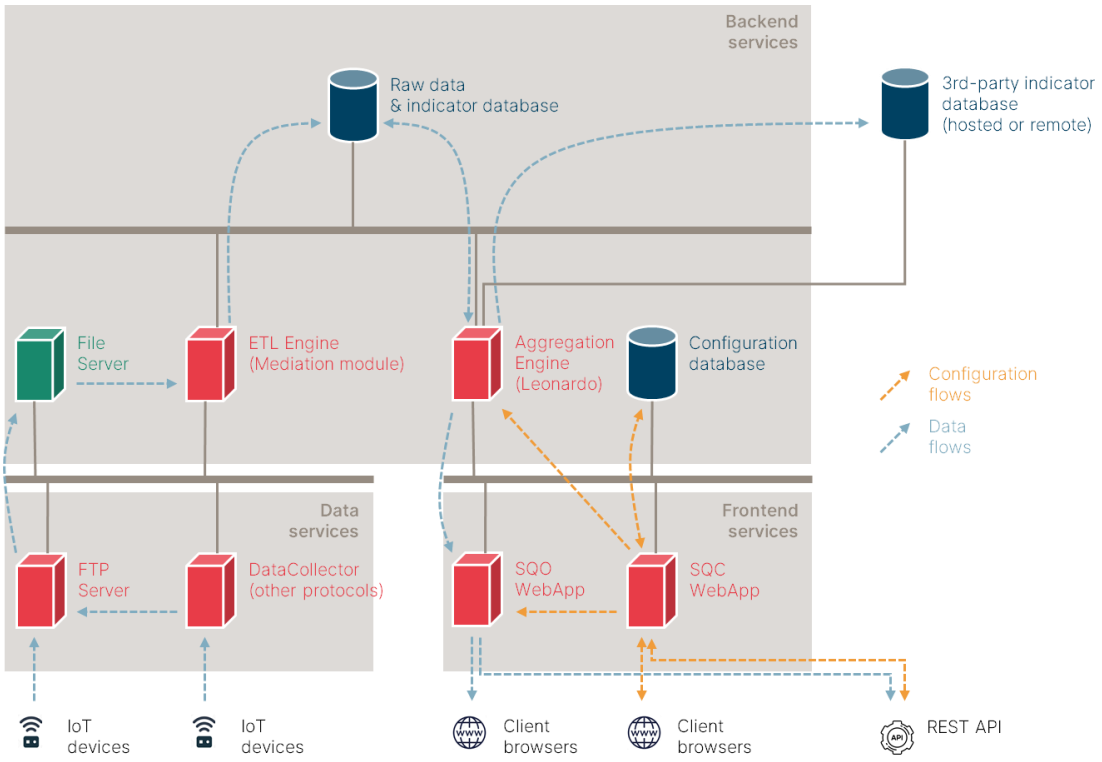


FIGURE 41 - SYNAPTIQ POWER ARCHITECTURE

3.25.2 INTEROPERABILITY INDICATORS

Data formats
JSON
Data models and ontologies
Custom data model
Protocols for information exchange
HTTPS, FTP
Security and data protection
Role-based access control
Southbound interfaces:
MSSQL SCADA, custom interfaces
Northbound interfaces
REST

4. INTEROPERABILITY OF PLATFORMS

Platform and service interoperability strikes as the main milestone and KPI to be achieved on behalf of WP5. Interoperability can be achieved by introducing middleware translation mechanisms that can be delivered to several distinct layers of the reference architecture model. These middleware components are named *adapters* and will provide means for domain and operational data sharing between stakeholders. As overviewed in Section 3, the set of available digital platforms exposes a wide and complex set of services and capabilities, many of them not including the concept of semantic interoperability as they do not adopt any ontology model nor reasoning features that enables them to expose their capabilities and operational data in a semantic and interoperable way.

This section discusses the services, properties and technologies highlighted in Section 3, and together with the reference architecture assembled in WP2, sets the foreground for the architecture description in this deliverable. This section will particularly recapture the overview of digital platforms and look at available services and main functionalities. Moreover, it covers the adoption of ontologies, particularly the ones within the SAREF ecosystem, and the need for external services. Finally, this section discusses interoperability requirements in terms of the supporting ICT technologies, along with the availability of interfaces deployment capabilities for virtual and scalable environments such as the *cloud*.

4.1 DIGITAL PLATFORMS OVERVIEW

The previous section conducted extensive analysis of the partner's digital platforms. This section recaptures those findings as an overview to sponsor the following discussions. Table 2 overviews the digital platforms that were part of the internal survey. Moreover, it also classifies the platforms according to a simple taxonomy, whose purpose is simplifying the discussion. This taxonomy is composed by 10 properties namely: Domain, Type, TRL, Deployment, Interface Logic, External API, Software (SW) Framework, Data Formats, Security and Data Protection and SAREF compliance. Each property is evaluated according to several type levels. The detail for each property follows.

Domain. This property addresses what is the main focus of a given digital platform. The classification is achieved through 4 types, namely: **Smart Homes** to identify platforms and services that address the connectivity to/from/within the domestic environment for efficiency, saving or improved comfort and easy-of-use ; **IoT** to identify platforms and services that act as software gateways to handle devices and feature across specific domains; **Energy** to identify platforms or services that address specific needs for energy, grid management or that induce energy savings; **Smart Buildings** to identify platforms and services that address connectivity to/from/within smart buildings.

Type. This property characterises what is the focus for the majority of functions and services made available by a given digital platform. The classification is made via 4 types, namely: **Analytics** to catalogue platforms or services that ingest data from other sources and extract complex, non-trivial information and generate intelligence; **Aggregator** to highlight services or functions that establish data processing capabilities, often as a representative measure of a

sub-set of samples; **EMS** to identify functions and services that relate to energy management system's features; **Integrator** to identify services or functionalities that represent translation and adoption of new features and services.

TRL. This property represents the Technology Readiness Level, in a scale from 1 to 9. This scale represents how ready a given technology, platform or system is to be adopted by the market.

Deployment. This property characterizes the digital platform in terms of its native deployment setup. The classification is split into 5 types: **Cloud** to identify the capability to use the cloud computing abstraction, despite that a digital platform could be deployed in a private or public provider; **Gateway** to identify the capability that a service or platform has to enable execution at a gateway device; **Edge/device** to identify the capability of a service to be deployed in a device; **Legacy** to identify a platform that is deployed on a proprietary, often closed infrastructure even if it has the capability to expose services via external APIs.

Interface Logic. This property highlights what is the main interface that is considered for a digital platform to relate with other platforms, services or devices. It is split into 3 types: **North-bound** to identify the provision of data and functions to digital platforms classified to be at a superior architectural level (*i.e.,* data consuming services that run at a higher abstraction level or with agglomerated data); **Middleware** to identify digital platforms that offer horizontal functions and services (*i.e.,* translation, adjustment, interoperability with other platforms at a similar architectural level); **South-bound** to identify functions and services that target devices or digital platforms at a lower architectural level.

External API. This property identifies if a digital platform embeds the capability to exchange data with external entities or in an *ad-hoc* fashion via a programmatic interface.

Software Framework. This property surveys the major software frameworks or development ecosystems that are considered to assemble a given digital platform or service.

Data Formats. This property identifies what are the data formats considered for data exchange, namely through the external API channels.

Security and Data Protection. This property identifies if security measures are in place within a given digital platform or service, considering namely user access control and authentication and/or data privacy capabilities. The detail on this property is limited in this deliverable as deliverable D5.3 will address this topic in greater detail.

SAREF compliance. This property characterises if a given digital platform already considers semantic capabilities via the SAREF ontology ecosystem (*i.e.,* SAREF, SAREF4ENER, SAREF4BLDG, etc). It includes two binary types for ***yes*** or ***no*** and a special type **no*** to consider the cases where other ontologies beyond SAREF are considered or some sort of semantic annotation capability.

Name	Partner	Domain	Type	TRL	Deployment	Interface Logic	External API	SW Framework	Data Formats	Security, Data Protection	SAREF
ARTEMIS	Wings	S, I, E	A	7	C, G	↑↓	Y	P, A	JSON	Y	N
Planet App	Planet Idea	E	E	7	C	↑↓	Y	C#, PH	JSON	Y	N
cyberNOC	Cybergrid	E	AG	8	C	⌬↑	N	J, A	JSON	Y	N
DCM	VITO	S, E	AG, E	5	C, L	↑⌬↓	N	P,	JSON	N	N
BEMS	VITO	E,S,I	E	5	C,G	↑↓	Y	P	JSON	Y	N
beeDIP	Uni Kassel	E	I	7	L	↑↓	Y	P, J,	JSON	Y	N*
SLOR	Trialog	I, S, E, B	AG, I, A	5	G, C	⌬↓	Y	S, J	XML	N	Y
ReFlex	TNO	E	AG	6	L, C	↑↓	Y	J	XML, JSON	Y	N
dEF-Pi	TNO	E	I	7		↑⌬↓			XML,	Y	N
Thermovault	Thermovault	E	AG, I	9	C	↓	N	-	JSON	Y	N
Sensinov	Sensinov	S, I, B	I, A, AG	9	L, C	↑⌬↓	Y	N, A	JSON	Y	Y
EBO	Scheiner Electric	B, I	E, I	9	L,ED	↓	Y	C++	XML, JSON	Y	N*
Konect	KEO	E	E, I	7	C,ED	↑↓	N	J, C+	JSON	Y	Y
Gm-Hub	INESCTEC	E	AG, A, I	7	C	↑⌬↓	Y	J, A	JSON	Y	N
CognitiveLoad	INESCTEC	S, E, B	A	8	L	⌬	Y	P	JSON	N	N
Dyamand	IMEC	S, B	A, I	7	C, G, L	↑↓	Y	J	JSON	N	N
Ekco IoT	Hyrde	S, I	A, AG, I	9	C, ED	↑⌬↓	Y	C#, ASP, A, N	JSON	Y	N
Ekco Marketplace	Hyrde	I	A, AG, I	9	C, ED	↑⌬	Y	C#, ASP, A, N	JSON	Y	N
HomeGrid	GRIDNet	S, I, E	I	7	C,ED ,G	↑↓	Y	P, N, C++, J	JSON	Y	N
Semantic-IoT	Gfi FR/RD	I	A	5	C	⌬↓	Y	J	JSON	N	N*

LeonR&Do	Cosmote	S, I, E	I	7	C, G, E, D	⌬↓↑	Y	C++, P	JSON	Y	N
OpenMotics	OpenMotics	S, B, E	I	8	C,ED , G	↑↓	N	P	JSON	Y	N
Tiko	Engie (tiko)	S, E	I, AG, E	8	C, L	↓	N	J, P	JSON	Y	N
Eflex	Enedis	E	I,AG	7	L	↑⌬↓	Y	J	JSON	Y	N
SynaptiQ Power	3E	E	A, I	5	L	↑↓	N	J	JSON	Y	N

TABLE 2 - INTERCONNECT DIGITAL PLATFORM OVERVIEW

Y: Yes N: No N*: No, but supports similar concept

Domain	Type	Deployment	Interface Logic	Software
S: Smart homes	A: Analytics	C: Cloud	↑ : North-bound	P: Python
I: IoT	AG: Aggregator	G: Gateway	↓ : South-bound	A: Angular
E: Energy	E: EMS	ED: Edge/device	⌬ : middleware	C++: C plus plus
B: Smart Buildings	I: Integrator	L: Legacy		C#: C sharp
				PH: PHP
				J: Java
				S: RDF, OWL, SPARQL
				N: Node Js
				ASP: Asp.net

4.2 SERVICES AND FUNCTIONALITIES

The previous overview realises the commonalities between digital platforms, but also what distinguishes them. From the perspective of the services offered to the ecosystem, the set of digital platforms is mainly split into three categories, namely: Aggregators, Integrator and Energy Management Systems. Considering the milestone towards employing a set of interoperable services made available by the interoperability layer, this section will analyse the service capabilities available. The study is made from the domain perspective, but also from the technology perspective.

4.2.1 BASIC SERVICES

Basic services comprehend all functionalities deemed necessary to enable the business logic of a service within the envelope of a digital platform. Usually, a digital platform comprises a

common set of features that enables it to discover capabilities, authenticate users and grant them access to resources. Table 3 identifies and classifies these features.

		Authentication	Data acquisition	Database export	Data translation	Frontend
Platform	**Partner**					
ARTEMIS	Wings	✓	✓	✓		✓
Planet App	Planet Idea	✓	✓	✓		✓
cyberNOC	Cybergrid	✓	✓	✓		
DCM	VITO		✓			
BEMS	VITO		✓		✓	
beeDIP	Uni Kassel	✓	✓	✓	✓	
SLOR	Trialog		✓	✓	✓	✓
ReFlex	TNO	✓	✓			
dEF-Pi	TNO		✓		✓	✓
Thermovault	Thermovault	✓	✓			
Sensinov	Sensinov	✓	✓		✓	✓
EBO	Scheiner Electric	✓	✓		✓	
Konect	KEO	✓	✓	✓	✓	
Gm-Hub	INESCTEC	✓	✓	✓		✓
CognitiveLoad	INESCTEC		✓		✓	
Dyamand	IMEC		✓		✓	
Ekco IoT	Hyrde	✓	✓	✓	✓	✓
Ekco Marketplace	Hyrde	✓	✓		✓	✓
HomeGrid	GRIDNet	✓	✓	✓		✓
Gfi Semantic	Gfi		✓		✓	
LeonR&Do	Cosmote	✓	✓	✓		✓
OpenMotics	OpenMotics	✓	✓	✓	✓	
Tiko	Tiko (ENGIE)	✓	✓	✓	✓	✓
Eflex	Enedis		✓	✓		
SynaptiQ	3E	✓	✓	✓		✓

TABLE 3 - CLASSIFICATION FOR DIGITAL PLATFORM'S BASIC SERVICES

4.2.2 DOMAIN AND ADVANCED SERVICES

Domain and advanced services comprehend the functionalities that are related with the domains identified within Interconnect, namely the Energy and IoT and Smart Homes/Buildings. These domains were chosen as they represent the majority of capabilities made available through the surveyed digital platforms. The Energy domain is subdivided into four subdomains, namely: Flexibility, Grid Stabilization, Monitoring Service and Self-Consumption. The IoT and Smart Homes/Buildings is subdivided into three subdomains, namely: Comfort Series, Other-Services and Interoperability. The subdomains considered are derived from the service ideation process from WP1 [27, p. 105]. Moreover, the Interoperability overarching subdomain/feature is also considered, as some platforms already encompass some of the required capabilities to provide interoperability or that were already going through the process of adopting those capabilities.

		Domains						
		Energy				IoT Smart Homes/Buildings		
		Flexibility	Grid Stabilisation	Monitoring Service	Self-Consumption	Comfort series	Other-services	Interoperability
Platform	**Partner**							
ARTEMIS	Wings		✓	✓				
Planet App	Planet Idea	✓		✓	✓		✓	
cyberNOC	Cybergrid	✓	✓					
DCM	VITO	✓	✓					
BEMS	VITO	✓		✓	✓		✓	
beeDIP	Uni Kassel		✓	✓			✓	✓
SLOR	Trialog						✓	✓
ReFlex	TNO	✓	✓	✓				
dEF-Pi	TNO	✓	✓					
Thermovault	Thermovault	✓	✓		✓			
Sensinov	Sensinov		✓	✓			✓	✓
EBO	Scheiner Electric						✓	
Konect	KEO	✓	✓	✓		✓	✓	
Gm-Hub	INESCTEC	✓	✓		✓		✓	
CognitiveLoad	INESCTEC		✓	✓				

Dyamand	IMEC		✓	✓		✓		
Ekco IoT	Hyrde					✓	✓	✓
Ekco Marketplace	Hyrde			✓			✓	✓
HomeGrid	GRIDNet			✓	✓	✓	✓	
Gfi Semantic	Gfi	✓	✓			✓	✓	✓
LeonR&Do	Cosmote			✓	✓	✓	✓	
OpenMotics	OpenMotics						✓	
Tiko	Tiko (ENGIE)	✓	✓	✓	✓			
Eflex	Enedis	✓	✓					
SynaptiQ	3E		✓	✓				

TABLE 4 - CLASSIFICATION FOR DIGITAL PLATFORM'S DOMAIN AND ADVANCED SERVICES

4.3 INTERFACES AND SUPPORTING TECHNOLOGIES

This section overviews what are the interfaces made available by the set of digital platforms available within InterConnect, together with the supporting technologies and considered data encoding protocols. The digital platforms provided usually have two main interfaces for interaction and data exchange, namely: User Interfaces, for those that have this capability and/or engagement with users (*i.e.,* final consumers, technical staff or administrators) and programmatic interfaces that enable machine-to-machine communication. Table 5 identifies the interfaces that are available at each digital platform. This process is split into two categories, namely: **applicational interfaces**, describing the technology considered for data exchange and request/response triggering, and, **data encoding**, highlighting the data formats considered for message and data exchange encoding.

		Applicational Interfaces										Data Encoding			
		REST	MQTT	Web Sockets	AMQP	Spine	NGSI	SPARQL	ModBus	SPINE	GraphQL	JSON	XML	RDF	Other
Platform	**Partner**														
ARTEMIS	Wings	✓										✓			
Planet App	Planet Idea		✓	✓								✓			
cyberNOC	Cybergrid	✓	✓	✓	✓							✓			
DCM	VITO	✓	✓												✓
BEMS	VITO	✓							✓			✓			
beeDIP	Uni Kassel	✓										✓			
SLOR	Trialog	✓											✓	✓	

ReFlex	TNO	✓		✓								✓	✓		
dEF-Pi		✓							✓				✓		✓
Thermovault	Thermovault		✓									✓			
Sensinov	Sensinov					✓		✓							
EBO	Scheiner Electric	✓	✓						✓			✓	✓		✓
Konect	KEO	✓	✓	✓		✓			✓	✓		✓			
Gm-Hub	INESCTEC	✓										✓			
CognitiveLoad	INESCTEC	✓										✓			
Dyamand	IMEC										✓	✓			✓
Ekco IoT	Hyrde	✓	✓	✓			✓				✓	✓	✓		
Ekco Marketplace	Hyrde	✓	✓	✓			✓					✓			
HomeGrid	GRIDNet		✓	✓								✓			
Gfi Semantic	Gfi	✓	✓	✓								✓			✓
LeonR&Do	Cosmote	✓	✓									✓			
OpenMotics	OpenMotics	✓	✓	✓					✓			✓			✓
Tiko	Tiko (ENGIE)	✓										✓			✓
Eflex	Enedis											✓			✓
SynaptiQ	3E	✓													✓

TABLE 5 - CLASSIFICATION OF AVAILABLE INTERFACES FROM THE DIGITAL PLATFORM CATALOG.

4.4 DISCUSSION

The provided digital platforms offer different services towards the IoT, smart homes and smart buildings and the grid. Most of these platforms provide either services related with grid needs, and digital services related with the final consumers, while bridging the gap between these domains. Each one of these domains implies distinct interaction patterns that are relevant to highlight.

4.4.1 DOMAINS

The IoT and smart home domain include services that directly or indirectly consider the final consumer as a main actor, either as they provide an interface that bridges the gap between IoT gateways and Grid management systems from DSOs and aggregation services; or, they provide means for users to discover, configure and control devices that are usually installed within their households. The platforms that fit within this classification typically expose

programmatic interface capabilities that allow them to extract data, but also usually allow a limited set of interoperability capabilities that are often not semantically driven (*e.g.,* discovery, service enrolment).

The Smart Buildings domain includes services and capabilities that are much related with the smart home domain, allowing devices to be discovered and enrolled. The main difference stems from the fact that the final domestic consumer is not the main actor, but rather a smart building manager or system administrator. The impact translates into the fact that the set of interfaces available is more limited, often closed, and focuses on south-bound and horizontal capabilities for interoperability, and not so much in the capability to export data for high-level platforms or aggregation services.

The Grid domain includes a wide set of platforms and services that very much relate with the management of energy flexibility and grid stabilization services, that together provide quality and continuity of service. These platforms employ a limited, but existing set of interoperability capabilities (*e.g.,* syntactic interoperability) from a horizontal architectural perspective. Data exchange is possible via some of these platforms, precisely to trade grid stabilization and flexibility data between stakeholders around the DSO ecosystem, but it is usually not freely available.

4.4.2 DEPLOYMENT

From the point of view of deployment of these platforms and services, there are clearly two main trends: moving towards cloud services and maintaining proprietary/legacy infrastructures.

Cloud Computing. The cloud computing model allows for transparent scalability and fault-tolerant QoS, both with high impact in the overall service availability, but also in the business model that allows service providers to scale according to demand. This trend is mostly adopted by platforms that offer services towards final consumers, which are focused on providing ubiquitous services, but also middleware and interoperability capabilities (even if limited). However, platforms for stakeholders within the grid domain are also adopting this paradigm, particularly for hosting intermediate aggregation, gateway services and to support the capability for digital twinning of some devices.

Gateway/Edge Devices. Middleware systems that consider data translations, data aggregation, data conversion and protocol translation are usually placed at the level of Gateway systems. These services showed to be often used together with platforms that operate under the cloud computing deployment trend, actually enabling to establish the ICT border in terms of supported systems between platforms and the residential/commercial smart building domain. This type of approach often considers lightweight software that runs on a gateway, acquiring data from devices/sensors and push-it to other platforms for storage and processing. The gateway as a border keeper between domains is often assigned with the capability to relay actuation instructions from controlling platforms or services (usually with holistic decision capabilities) to devices.

Legacy/Proprietary. On the other hand, grid services often rely in full legacy services and proprietary infrastructures for critical services. Moreover, nowadays they also consider a mixed approach between cloud hosted services and legacy systems.

4.5 INTEROPERABILITY REQUIREMENTS

The previous sections identified and characterized the available digital platforms, according to several axis, namely: the overall positioning or technology readiness (Table 2); domain (Table 4) or the supporting technologies and interfaces (Table 5). To support the discussion regarding interoperability requirements, Figure 42 depicts a preliminary view regarding the interoperability layer to be introduced in the next sections of this deliverable. Further details are provided in Section 5. The provision of interoperability is based on the concept of "*Adapters"* that allow the necessary adjustments and become a gate towards the ecosystem of interoperable services. *"Adapters"* will be integrated into digital platforms, gateways, standalone services or devices. They will be based on a generic adapter model, that will then extend a set of common ground functionalities to specific adapters, distinguished on the basis of the underlying native technologies for transport and execution.

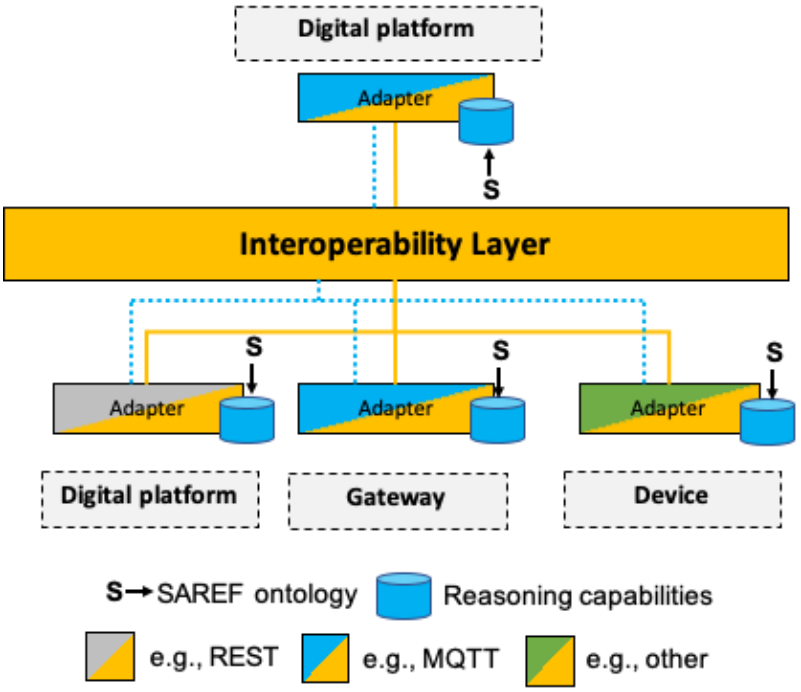


FIGURE 42 - PRELIMINARY ENTITY MAP FOR THE ARCHITECTURE

The provision of interoperability that will enable platforms and services to exchange data into complex business models will be achieved by fulfilling two main classes of requirements, namely: semantic interoperability and reasoning, and interface compliance.

4.5.1 SEMANTIC AND REASONING REQUIREMENTS

Semantic reasoning will be the distinguishing capability for the provision of interoperability within Interconnect. This capability stems as the ability to exchange data between platforms and services, ensuring that there is the capability to dynamically deliver data and "*reason"* (i.e.,

discover) about new capabilities and domains in an interactive and autonomous way. Enabling this capability requires digital platforms to be capable to express their features with the aid of ontologies, which for the case of Interconnect are preferentially the ones belonging to the SAREF family. The conducted survey identified that only seven out of twenty-three digital platforms either adopt already the SAREF ontology or have built-in capabilities to quickly adopt an ontology like SAREF. According to [28], twenty-three digital platforms are currently at a SAREF compliance level 0 (*i.e., no SAREF compliance on data, metadata or reasoning*).

Providing semantic expression capabilities is therefore a key requirement for the integration of a digital platform into Interconnect's ecosystem of pluggable, semantically driven platforms and services. To fulfil this requirement and adopt at least a level 3 compliance [28] (*i.e.,* metadata and/or data use SAREF and reasoning is enabled) digital platforms will require to:

- model their business logic (services) and accommodate the SAREF ontology (WP3);
- expose ICT interfaces for data sharing (if not done already);
- integrate with a WP5 generic adapter that will serve as gateway to reasoning and discovery services.

4.5.2 GENERIC ADAPTERS

Providing technical interoperability requires digital platforms to make use of a common language and a set of data translators. According to the High Level Reference Architecture [28], the adoption of a *"smart adapter"*, a as lightweight software package will bring common data translations in a mesh of smart adapters. From the digital platform survey, Section 4 identifies the ICT protocols and data encodings considered as the basis for the external interfaces that a given digital platform or service offers. WP5 will offer a set of generic adapters that should then be selected by digital platforms. Generic adapters will have all required features for sponsoring the Interconnect interoperability framework and common functionalities already built-in but will require integration with the southbound interfaces (*i.e.,* the interfaces that will provide integration with a digital platform and/or service). Generic adapters will be available for different programmatic languages (*e.g.,* Java, Python, etc.) and with several supporting protocols for data exchange (*e.g.,* REST, MQTT, WebSockets, SPINE, etc.).

From the digital platform catalogue analysis, we highlight the need:

- Accommodate the semantic and reasoning requirements described in section 4.5.1;
- Attach one of the generic smart adapters (to be made available by WP5) that better fits the needs for a specific digital platform or service;
- Consider, if needed, any required adjustment to the service API;
- Consider the use of data encoding formats, namely JSON or XML or adopting required translations;
- Consider the required data translation from the (southbound) digital platforms and services to be fed into InterConnect's interoperability framework.

5. INTERCONNECT INTEROPERABILITY FRAMEWORK ARCHITECTURE

The InterConnect project seeks to achieve semantic interoperability between existing platforms, services, devices and other types of endpoints found in smart buildings and at the edge of smart grid systems. The consortium partners are introducing their high TRL systems for realization of the project use cases in the pilot environments. To enable their semantic interoperability, the project is providing InterConnect interoperability framework. This framework is a set of tools and services which will enable existing digital platforms, operated by the consortium partners, to achieve semantic interoperability without an intermediary platform dedicated to hosting interoperability adapters. This is the main requirement for ensuring future proof design and minimize dependencies on maintaining project level digital platform. Other requirements with impact on specification and development of the InterConnect interoperability framework are given in Table 6.

Requirement #	Requirement description
R1	IC project MUST achieve semantic interoperability without an intermediary digital platform purposefully built for the project to facilitate this interoperability.
R2	IC project SHOULD achieve semantic interoperability based on SAREF ontology and a set of existing, already validated semantic reasoning and orchestration technologies.
R3	IC project MUST specify interoperability toolbox providing enablers and services for realization of interoperable environments required by the project pilots and defined use cases.
R4	IC project SHOULD enable interoperability not just within pilots, but among them in overarching use cases.
R5	IC project MUST support cascade funding partners and integrators to utilize the interoperability toolbox components to make their platforms and services interoperable in the same semantic interoperability framework.
R6	IC project SHOULD implement mechanism for interoperability compliance test and certification.
R7	IC project MUST ensure that achieved interoperability does not impact or limit the privacy protection regulations and mechanisms already implemented by participating entities.

TABLE 6 - HIGH LEVEL REQUIREMENTS FOR IC INTEROPERABILITY FRAMEWORK

Based on these requirements and the status in key work packages of the project, namely:

- WP1 on specification of high-level use cases and project pilots,
- WP2 activities towards specification of IC project reference architecture, data models and interfaces,
- WP3 requirements from service providers working on innovative services.

The high-level specification of the IC interoperability framework is provided in this section. WP5 works on specification and implementation of the IC interoperability framework with focus on enabling semantic interoperability between digital platforms brought to the project by the consortium partners. These platforms will be used for realization of base architectures behind IC project pilots and they will run interoperable energy and non-energy services necessary for realization of the project use cases. Therefore, most of the IC interoperability framework enablers are targeting digital platforms and services hosted on them. The main components of the interoperability framework include (see Figure 43):

- **Semantic interoperability layer** – enables semantic interoperability and reasoning between all endpoints capable of running:
    - **IC interoperability adapter** – provides orchestration and translation of existing interfaces and data models to the unified communication protocol (SPARQL+) and data model based on SAREF ontology.
        - Specification of SPARQL+ and SAREF ontology-based data models is underway within WP2. D2.1 (scheduled for December 2020) [28] will provide detailed overview of the unifying interfacing protocol (SPARQL+) and SAREF based data models.
    - **IC interoperability connector** – provides reasoning for endpoints which already expose interface following unified communication protocol (SPARQL+) and data model based on SAREF ontology.
- **Security and data protection framework** (requirement R7 from Table 6) – integrated with the semantic interoperability layer so that defined access control and data/privacy protection rules, required by digital platforms and services, are addressed during semantic discovery and reasoning processes.
- **Service store** – provides complete catalogue of all interoperable services from energy and non-energy domains. The service store is implemented as a web application providing a frontend interface for onboarding new interoperable services and browsing existing (already onboarded services) by category and other metadata parameters. Service store enables users or local reasoners to find interoperable services of interest and provides them with information on how to access the services running on their hosting digital platforms or available for instantiation through containers and appropriate runtime environments.
- **P2P marketplace enablers** – these enablers can be configured and deployed for specific use cases, on the level of a pilot or on the level of the whole project. The P2P marketplace enablers support implementation of energy transactions as well as other data related transactions typical in community-based scenarios and use cases. The key components:
    - Hyperledger Fabric configurations as a blockchain basis for trusted data access and transaction management;
    - set of smart contract templates representing supported transactions, reports and audits;

- white labelled web application utilizing blockchain network through integrated smart contract interfaces.

- **Interoperability compliance tests and certificates** (requirements R6 from Table 6) – a set of automated tests of achieved minimal interoperability defined for each service and platform category. The interoperability compliance test will be part of the service onboarding process in the IC service store. After successful compliance test, a certification of interoperability compliance will be issued and written in immutable record of all interoperable endpoints based on Hyperledger Fabric blockchain established on the level of the IC project.
- **Supporting services** – a set of supporting services and enablers will be introduced to support production quality instantiation and management of the IC interoperability framework and, through it, the IC reference architecture for smart buildings and energy domains. These supporting services will include:
  - Performance analytics for instantiated IC interoperability framework, with logs and reports;
  - Cloud hosting capabilities for service store, p2p marketplaces and access control mechanisms;
  - Tools and services for 3rd party integrators of the IC interoperability framework – source code repos, test scripts, wiki pages, datasets (addressing R5 from Table 6).

This list of tools addresses the requirement R3 from Table 6. Each of these IC interoperability framework enablers and tools is introduced in greater detail in the following subsections.

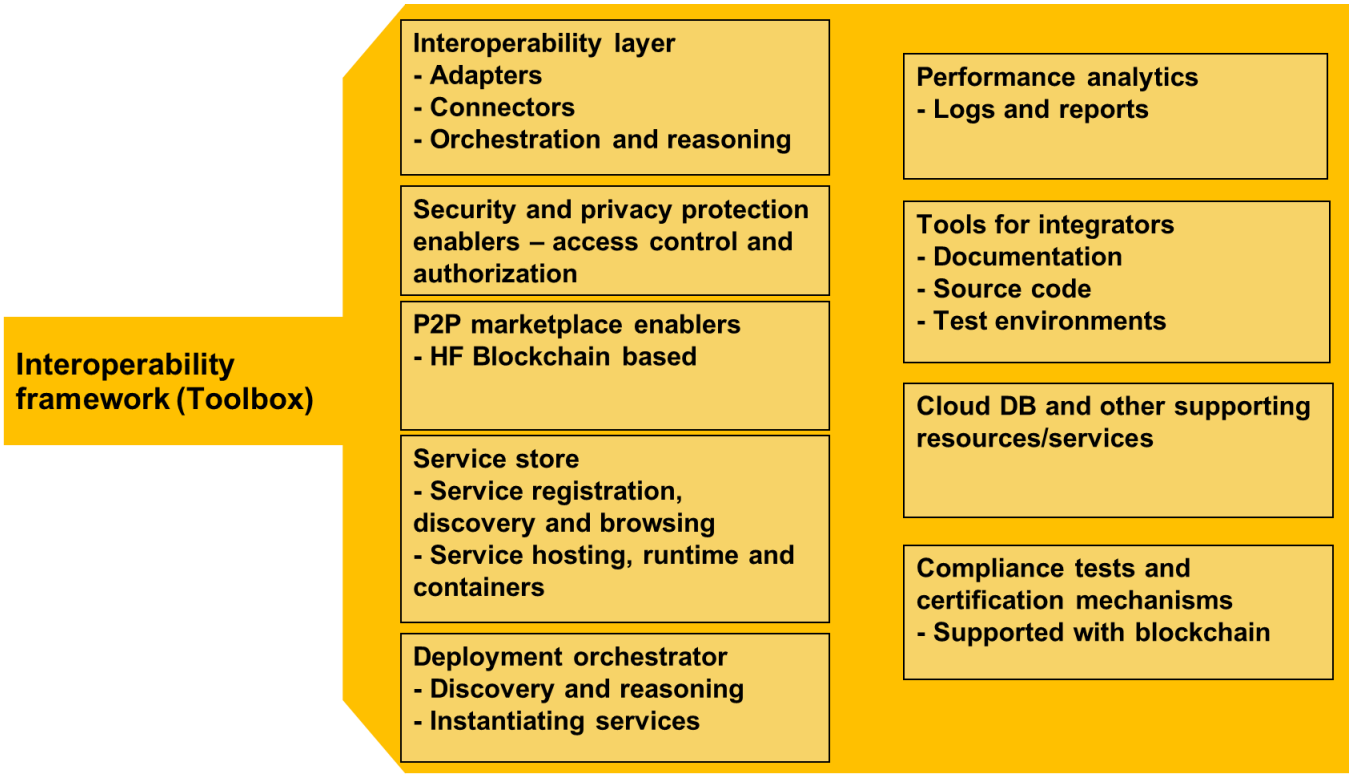


FIGURE 43 - OVERVIEW OF THE IC INTEROPERABILITY FRAMEWORK COMPONENTS

5.1 INTERCONNECT INTEROPERABILITY FRAMEWORK ARCHITECTURE

The WP2 of the InterConnect project is working on specifying interoperable reference architecture for smart buildings and smart grids based on standard reference architectures from IoT and smart grids. Deliverable D2.1 “Secure interoperable IoT smart home/building and smart energy system reference architecture” [28] will provide specification of the InterConnect reference architecture together with specification of all interfaces, data models based on SAREF ontology and semantic interoperability mechanisms. Some functional layers of the reference architecture are already represented in the digital platforms provided by project partners for realization of the pilots and use cases. Especially in platforms which provide vertical solutions for individual or multiple smart buildings. What is missing in most cases is interoperability achieved in a unified way and not per interface/service type. In order to enable instantiation of the reference architecture on digital platforms and other endpoints constituting the project use cases, the InterConnect is introducing the interoperability framework.

Figure 44 shows the simplified high-level reference architecture at its current stage of development within WP2. The reference architecture includes all system layers:

- **Device layer** – including all end devices which are consumers/producers/prosumers of electric energy as well as sensors and actuators;
- **Gateway layer** – including home and building management systems deployed on site;
- **Semantic Interoperability layer** – here is where the InterConnect semantic interoperability layer is established. It is important to note that the semantic interoperability layer is not strictly between networking and application layer, but pervasive network of interoperability adapters and connectors (see section 5.2 for further details) spanning all of the four reference architecture layers.
- **Application layer** – includes all interoperable services (energy, non-energy and grid related) as well as applications built for realization of the project use cases. InterConnect interoperability framework services and enablers are also residing on this layer.

The reference architecture includes interfaces between the main system layers. The InterConnect semantic interoperability layer is more pervasive on all other system layers with its semantic interoperability adapters and connectors deployed on services provided by devices, building management systems and services and applications running on application layer (i.e., on cloud platforms).

WP2 deliverable D2.1 [28] will elaborate on the reference architecture in details.

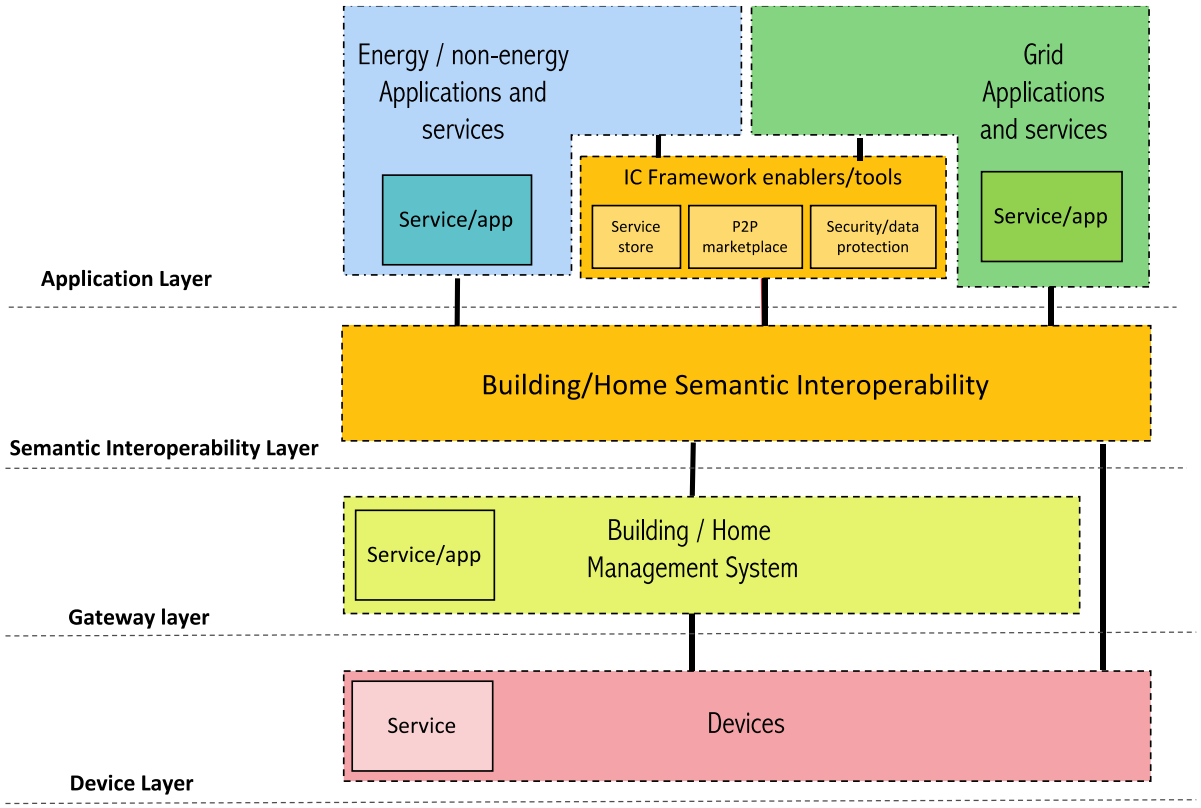


FIGURE 44 - INTERCONNECT SIMPLIFIED SMART BUILDING IOT REFERENCE ARCHITECTURE

The IC interoperability framework enables digital platforms with standard, or custom architecture to interoperate with other platforms and get access to additional services and data streams necessary for building innovative use cases and applications. Apart from the specification for reference architecture, the WP2 will provide the following specifications which are key for proper realization of the IC interoperability framework:

- Specification of unified interoperability interface which is now called SPARQL+ since it will be based on the well-known SPARQL protocol for semantic web. The + means that additional functionalities will be added to the SPARQL protocol to support specific operational patterns and other requirements introduced by the project pilots and use cases;
- Reference data models based on SAREF ontology with possible extensions necessary for addressing requirements derived for the project use cases;
- Semantic reasoning and orchestration mechanisms to be used in realization of the project use cases and innovative applications capable of taking full advantage of the semantic web technologies and knowledge generated and exchanged between endpoints (knowledge bases) participating within the project pilots;
- Security and data/privacy protection framework and best practices for all project pilots and use cases;
- Functional and system requirements for proper instantiation of the specified interoperable reference architecture for IoT and energy domains in line with requirements specified in adopted standard reference architectures.

The overall functional architecture of the IC interoperability framework is shown in Figure 45. The central component is the semantic interoperability layer which interconnects existing digital platforms, and services they offer, among themselves and with the interoperability framework services (service store, P2P marketplaces, compliance certification, data protection and access control and supporting services for production level operation). The semantic interoperability layer comprises configured instances of interoperability adapters and connectors (see Section 5.2.2) hosted on digital platforms (provided by project partners) and supporting services introduced by the interoperability framework. Therefore, the semantic interoperability layer is completely distributed onto existing endpoints, which eliminates the need for centralized platform facilitating interoperability interfaces (addressing R1 from the Table 6). The semantic reasoning and orchestration processes are also provided by this interoperability layer while the interoperable services are adapted to take full advantage of these semantic web mechanisms.

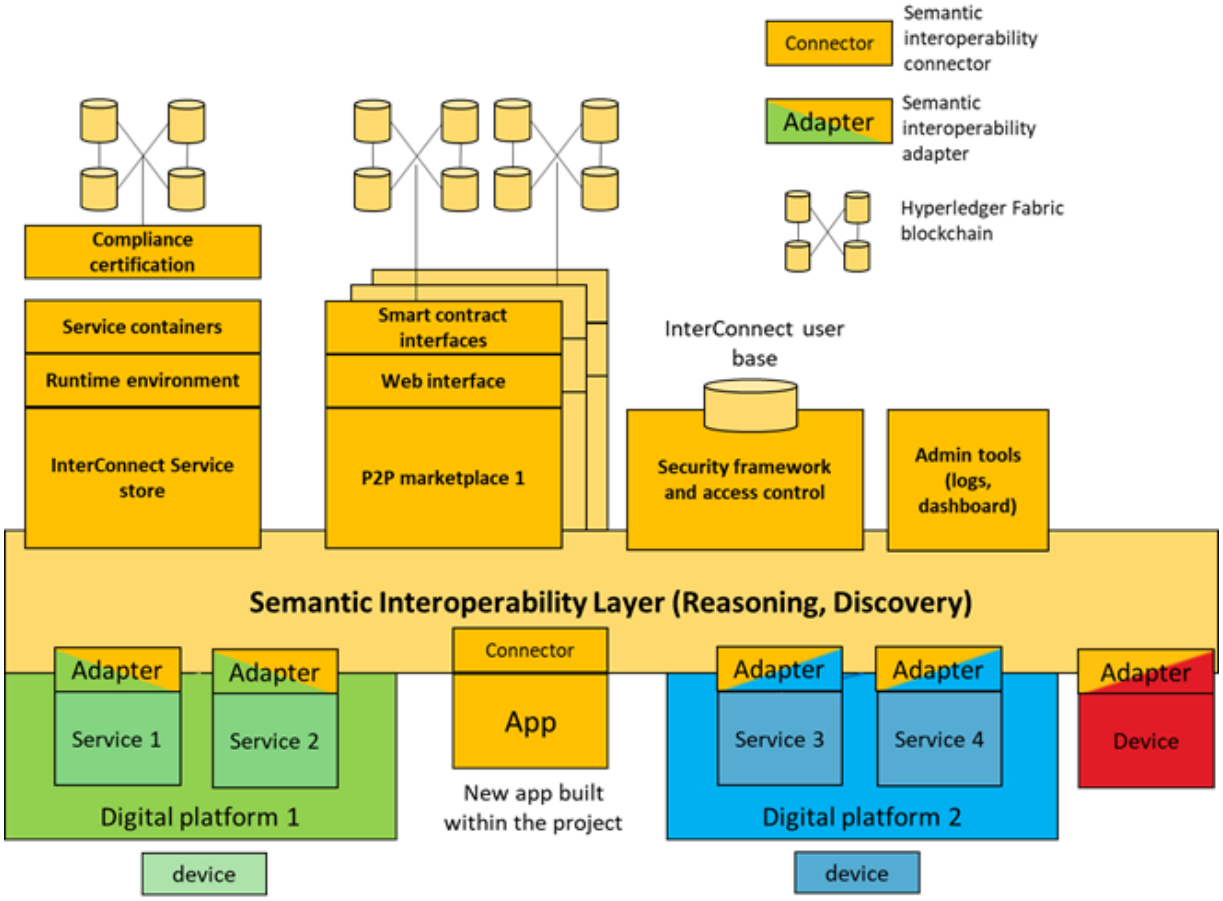


FIGURE 45 - HIGH LEVEL FUNCTIONAL ARCHITECTURE OF THE IC INTEROPERABILITY FRAMEWORK

The goal of the project is to approach instantiation of both, the reference architecture (WP2) and interoperability framework (WP5) from the perspective of the project pilots and on the level of the whole project. Each pilot will instantiate specified reference architecture by employing the IC interoperability framework enablers and tools on top of digital platforms, services and other endpoints comprising the underlying pilot architecture. Use cases are specified based on the available architectural basis within project pilots. However, the goal is to enable realization of all project use cases on all project pilots if all requirements are met. The main set of these requirements related to interoperability are addressed with the same

interoperability enablers being developed for the complete project. Additional requirements might require deployments of new resources and endpoints to support complete use case realization on all pilots (i.e., use case deals with flexibility management in conjunction with electric vehicle charging stations – this means that use case realization might require installation of these EV charging stations at pilot location). How different project pilots and sub-pilots plan to achieve this instantiation of reference architecture with the help of interoperability layer enablers is presented in Section 6 of this deliverable.

The IC project will support overarching use cases as well. These use cases require access to resources and services available across different project pilots. To support them, the IC interoperability framework must be instantiated on the level of the whole project and not just per (sub-)pilot. The IC framework should not differentiate between the same type services that are supported on the different pilots enabling seamless integration on the EU level. Specific approaches for distinguishing IC interoperability framework instances on pilot and project level will be specified within WP5 and T5.2.

5.2 SEMANTIC INTEROPERABILITY LAYER

5.2.1 CONCEPT OF SEMANTIC INTEROPERABILITY (TNO)

According to the GWAC (GridWise Architecture Council) Interoperability framework, also adopted by AIOTI, the following three main levels of interoperability can be identified:

- **Technical Level (Syntax)** covering the aspects of basic connectivity, network interoperability and syntactic interoperability;
- **Informational Level (Semantics)** covering the aspects of semantic understanding and business context;
- **Organizational Level (Pragmatics)** covering the aspects of business procedures, business objectives and regulatory policy.

Each of these levels is divided into sub-levels in order to accurately reference the degree of interoperability. The Figure 46 below gives an overview of this framework called GWAC stack.

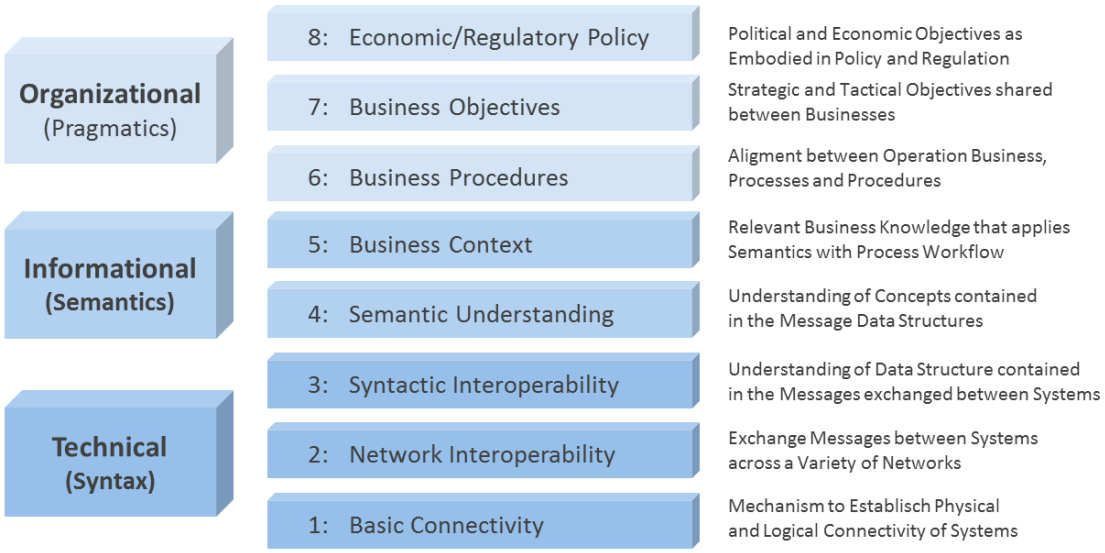


FIGURE 46 - LEVELS OF INTEROEPRABILITY (SOURCE GWAC - GRIDWISE ARCHITECTURE COUNCIL)

In Smart Home systems the sublevels basic connectivity, network interoperability and syntactic interoperability and semantic understanding are relevant. They are discussed in more detail below:

- **Basic connectivity:** Basic Interoperability concerns the digital exchange of data between two systems and the establishment of a reliable communication path. This requires an agreement on the compliant use of specifications that describe the data transmission medium, the associated media-related data encoding and the transmission rules for the media access.
- **Network interoperability:** Network interoperability presupposes an agreement how the information is transported between interacting parties across multiple communication networks. The protocols agreed upon in this category are independent of the information transferred.
- **Syntactic interoperability:** Technical interoperability guarantees the correct transmission of bits. The correct syntax of transferred information is the task of standards such as XML or EDIFACT. Syntactic interoperability refers to the exchange of information between transacting parties based on agreed format and structure for encoding this information. Assuring that transmitted information has a proper meaning is not in the scope of syntactic interoperability.
- **Semantic interoperability:** Beyond the ability of two or more systems to exchange information with correct syntax (i.e. grammatically correct), semantic understanding concerns the (automatic) correct interpretation of the meaning of information. To achieve semantic interoperability, both sides must refer to a common information exchange reference model. This reference model must define the meaning of the exchanged information (the words) in detail. This is the only way to ensure that the communicating systems will correctly interpret the information and commands contained in the transferred data and will correctly act or react. Reference ontologies, such as SAREF, can be used to represent the common reference model. They may also model constraints about the information concepts by specifying assertions and inferences that can be used in reasoning mechanisms (e.g., if this, then that). This

allows resolving interpretation conflicts in situations where two differently named classes in different models mean the same or when a class is a subset or superset of another class.

5.2.2 INTERCONNECT'S APPROACH

InterConnect semantic interoperability layer is envisioned as a distributed network of interoperability adapters and connectors hosted on digital platforms provided by project partners and other solution integrators. The IC interoperability framework services will also feature semantic interoperability adapters and connectors. This will create a semantic/knowledge layer where all interoperable services and endpoints can discover each other and perform reasoning to create new connections and data exchange paths. Note – in the figures in this and subsequent sections a colour coding will be used to depict InterConnect interoperability framework/layer with orange colour. When presenting an interoperability adapter, the orange colour depicts the unified interoperability layer and the other colour represents existing interface implementation.

The IC interoperability framework will provide two types of generic enablers for all services and digital platforms to make their existing communication interfaces interoperable in IC manner (utilize SPARQL+ and SAREF based data models). These enablers are generic IC Interoperability adapter and IC interoperability connector.

Generic IC interoperability adapter (see Figure 47) is to be instantiated per endpoint (software service, digital platform, device) which needs to be made interoperable. The IC interoperability framework will include a set of generic adapters built for a specific interfacing technology. Digital platform operators and service providers will choose a generic adapter best suited for protocol/technology of their existing communication interface (either southbound or northbound).

A set of generic adopters to be implemented within WP5 is defined based on the digital platform catalogue presented in section 3. Most of the digital platforms and services they expose are utilizing one or more of the following communication interfaces: REST, MQTT (i.e., RabbitMQ), Web Sockets, SHIP, SPINE, NGSI, ModBus, Kafka. Generic enablers for other interfaces can be added to the collection during the project and based on requirements of the pilots and use cases. It is important to note that:

- Diversity of digital platforms and services available within the project and project pilots ensures that the IC interoperability framework will provide an extensive set of generic adapters which will attract 3rd party integrators to work with and validate the enablers;
- Once a proper interoperability adapter is selected, the integrator (service provider or platform operator) needs to configure the adapter by (see Figure 48 and Figure 49):
    - Mapping interface functionalities to SPARQL+ and,
    - Mapping internal data model to the SAREF based data model.
- Instructions will be given on how to implement custom interoperability adapters for interfacing technologies for which a generic adapter is not available in the IC

interoperability framework. This way the library of available generic adapters will continue to grow during and after the project.

IC interoperability connector (see Figure 50) will enable application and services purposefully built for the IC project to utilize the semantic reasoning and orchestration functionalities provided by the IC semantic interoperability layer. The assumption is that applications and services developed during the course of the project will utilize SAREF based data models and expose SPARQL+ interface.

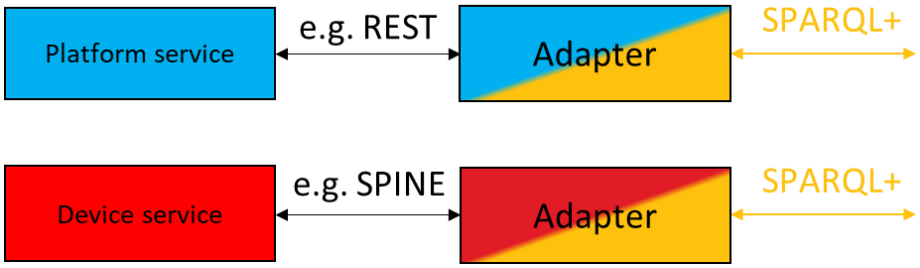


FIGURE 47 - HIGH LEVEL OVERVIEW OF THE IC SEMANTIC INTEROPERABILITY ADAPTER

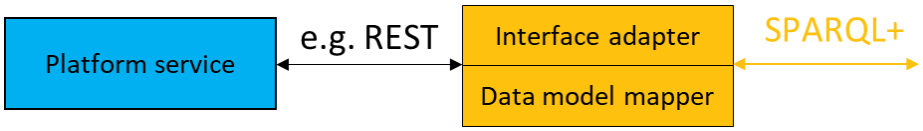


FIGURE 48 - IC SEMANTIC INTEROPERABILITY ADAPTER - TWO MAIN ROLES

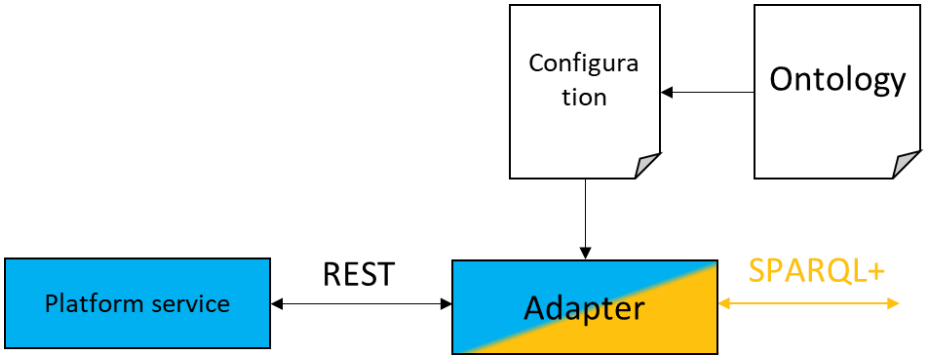


FIGURE 49 - HIGH LEVEL OVERVIEW OF THE IC SEMANTIC INTEROPERABILITY ADAPTER WITH CUSTOM CONFIGURATION

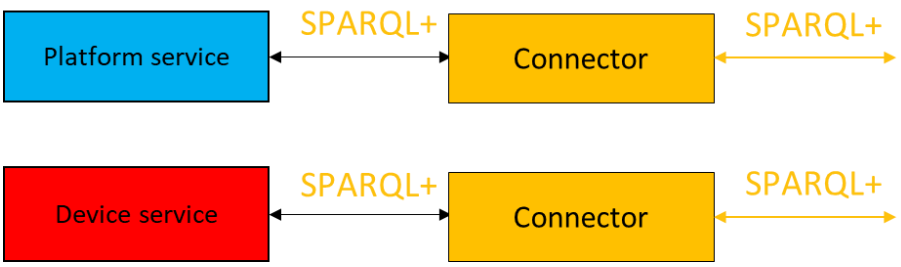


FIGURE 50 - HIGH LEVEL OVERVIEW OF THE IC SEMANTIC INTEROPERABILITY CONNECTOR

Exact implementation of the two interoperability enablers depends on the utilized underlying semantic web technology (two options are presented later in this section). The project WP2 and WP5 are working on specifying the generic interoperability adapters and processes for their instantiation for different categories of services and other endpoints. The Programming framework for adapters will be based on the underlying semantic web technology – i.e., Java for the Knowledge Engine.

With the concept of IC semantic interoperability adapter defined, the IC semantic interoperability layer can be presented in more details. Figure 51 shows a typical pilot ecosystem comprising: two different digital platforms, each with its own set of services (concept of services is presented in the next subsection), managed devices and interfaces; a service running on a platform that might not be part of the InterConnect digital platform catalog; application (i.e. web or mobile) developed for the purpose of a project use case and utilizing the interoperable services (not necessarily providing additional services); IC interoperability framework where specific focus is put onto the IC semantic interoperability layer. Here the IC semantic interoperability layer is showcased as a centralized layer/architecture component responsible for bridging/ interconnecting services, applications and platforms all utilizing different communication interface technologies/protocols/standards.

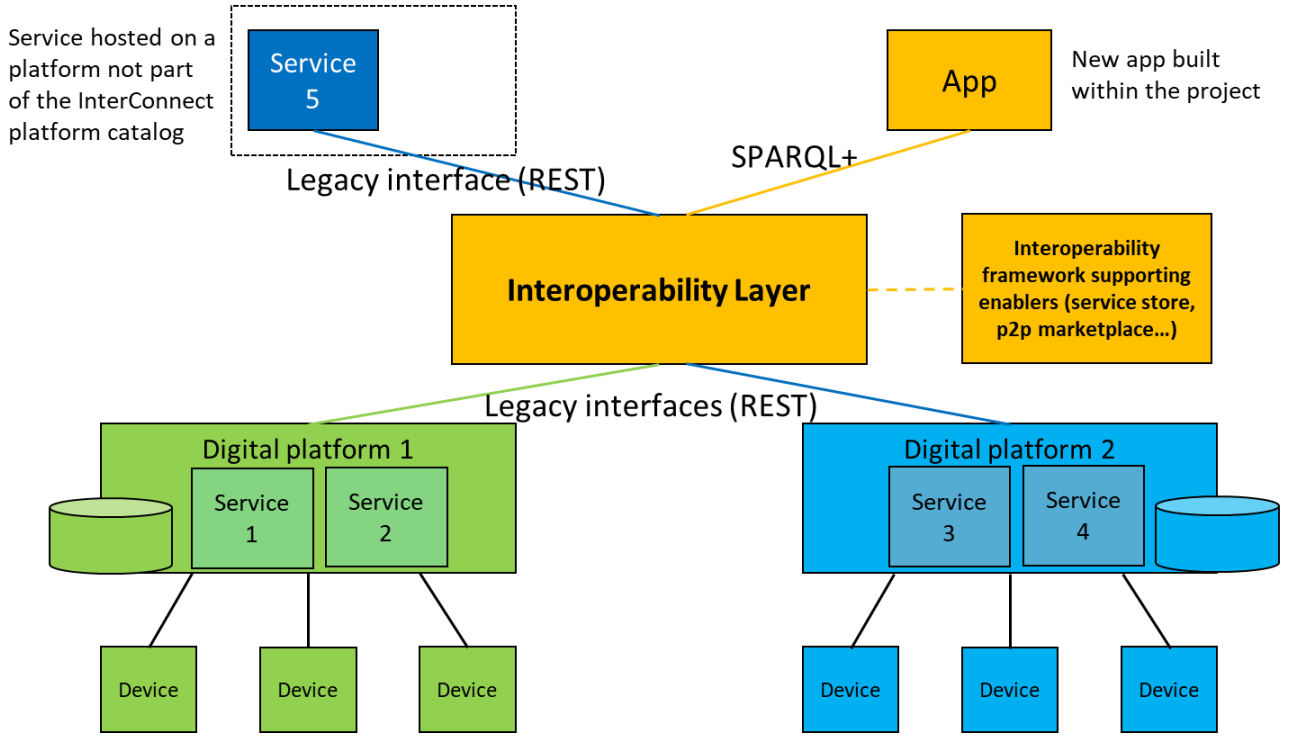


FIGURE 51 - SEMANTIC INTEROPERABILITY LAYER IN CONTEXT OF A TYPICAL PILOT ARCHITECTURE

Figure 52 showcases what comprises the IC semantic interoperability layer – mainly the interoperability adapters and connectors. In this figure the data flows are divided into semantic discovery (metadata communication) and operational data exchanges (actual data and instructions exchanged between participating endpoints). Additionally, the semantic reasoning and orchestration is presented as a separate module just to indicate that it is a specific functionality provided by the semantic interoperability layer.

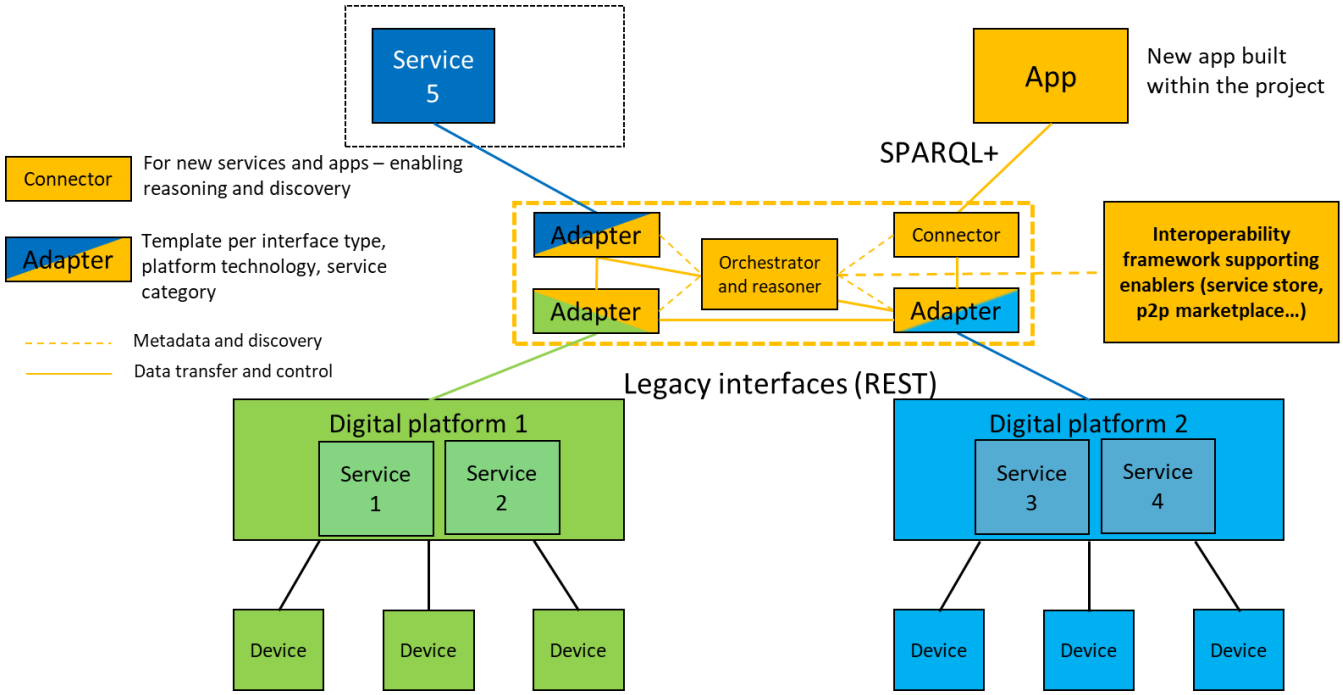


FIGURE 52 - IC SEMANTIC INTEROPERABILITY LAYER COMPRISING IC INTEROPERABILITY ADAPTERS

Figure 53 shows InterConnect approach for deploying the IC interoperability layer. The goal is to distribute the IC interoperability adapters and connectors towards the endpoints which need to interoperate. The adapter instances are hosted on digital platforms providing the interoperable services and/or integrated with services themselves to make them semantically interoperable. The orchestration and reasoning can also be distributed and implemented as part of the interoperability adapters (this approach will be followed in implementation of the IC semantic interoperability layer based on the Knowledge Engine technology). Therefore, the semantic interoperability will be enabled without the centralized facilitator/platform. The IC interoperability adapters can be instantiated on a level of a service (each service with its own adapter), or on a level of the whole digital platform running multiple services. Approach on how to instantiate the adapters will be decided by the platform and service operators.

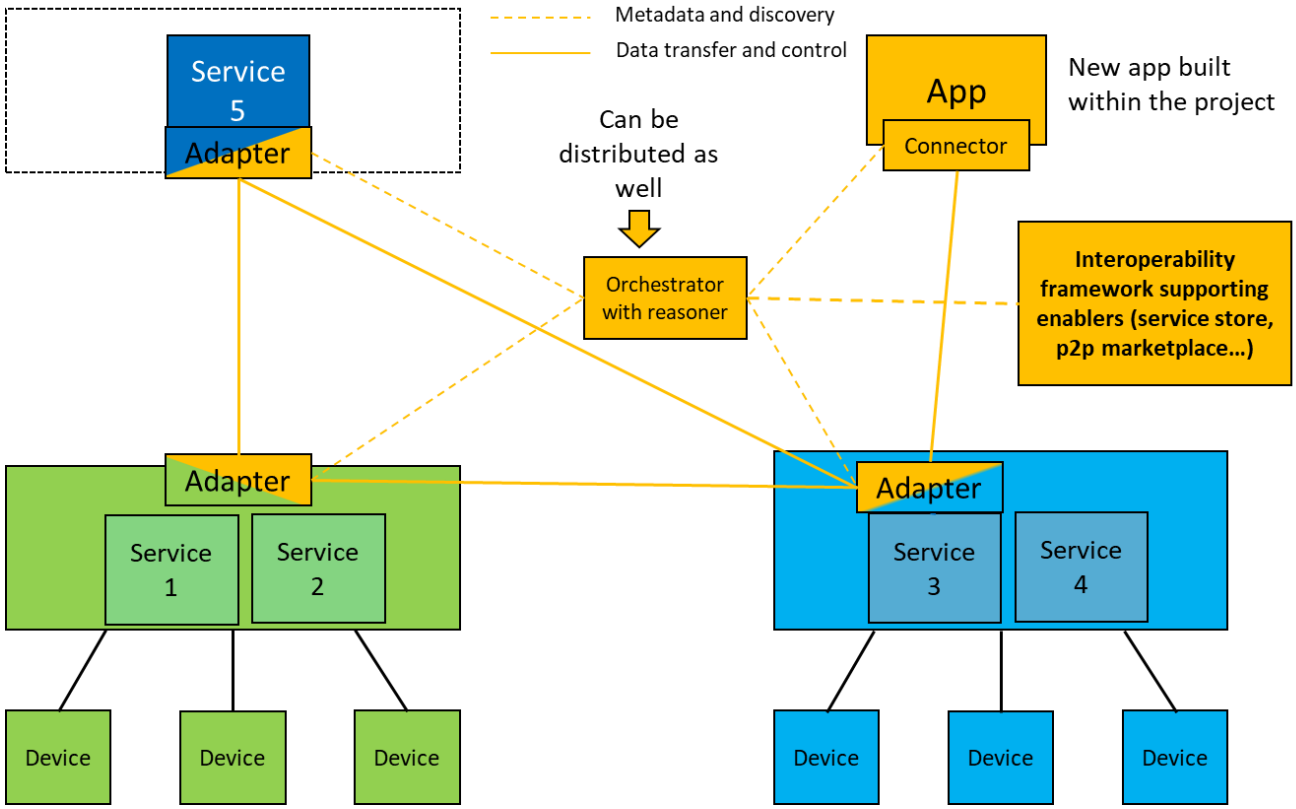


FIGURE 53 - IC SEMANTIC INTEROPERABILITY LAYER DISTRIBUTED ON THE PARTICIPATING DIGITAL PLATFORMS AND SERVICES

Figure 54 shows options for deploying IC interoperability adapters on different system layers of a typical IoT digital platform. The platform providers will decide on how to proceed with instantiating and deploying the IC semantic interoperability adapters. Hosting the adapters closer to the edge/device level will increase the semantic discovery granularity and enable more reasoning options. Hosting adapters on cloud level will allow service/platform operators to maintain full control of the discovery and reasoning with strict access control rules which might be in place. Hybrid deployments are also possible.

More details about the semantic interoperability adapters and their role in enabling semantic interoperability can be found in D5.2 [30].

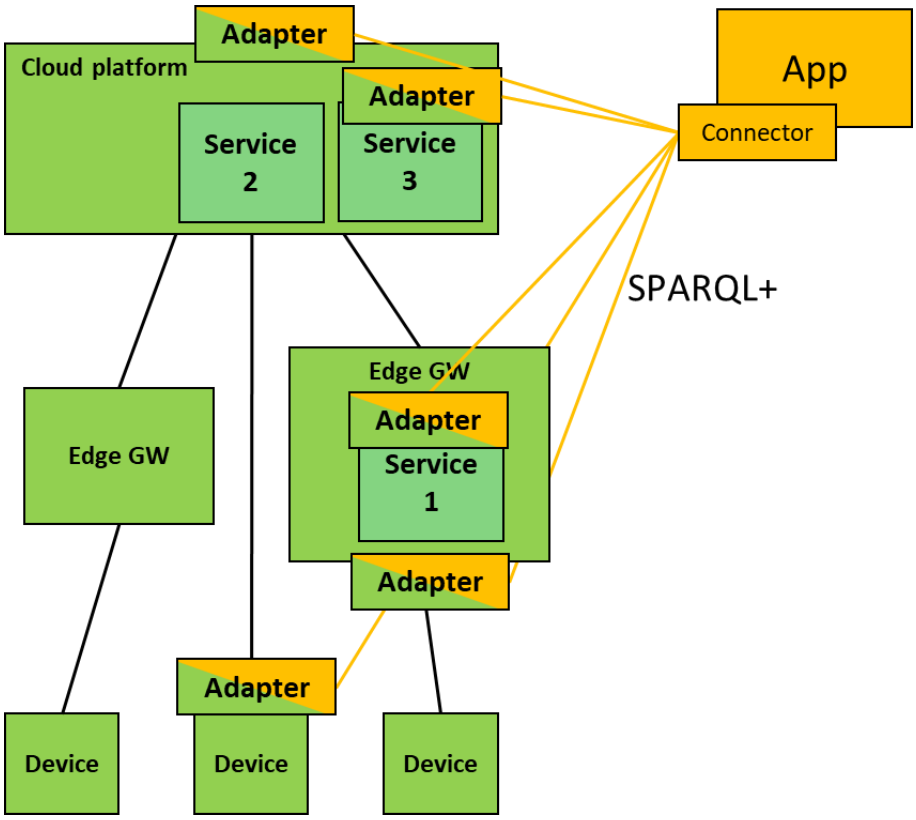


FIGURE 54 - DIFFERENT OPTIONS FOR DEPLOYING IC INTEROPERABILITY ADAPTER INSTANCES

5.2.2.1 ENABLING TECHNOLOGIES FOR INTERCONNECT INTEROPERABILITY LAYER

As the technology basis for implementing the InterConnect semantic interoperability layer, the consortium is considering three technologies:

- **Knowledge Engine** (provided by partner TNO) – as the main enabler for semantic interoperability adapters and reasoning for services running on digital platforms.
- **Web of Things** (W3C standard supported by several project partners with their expertise in implementing and adapting the solution – KEO, Trialog) – as the semantic interoperability complementary to the Knowledge Engine in a sense that it is more suitable for endpoints with limited computational capabilities.
- **Semantic reasoner** (provided by partner Trialog) - retrieves domain knowledge extracted from ontology-based IoT projects relevant to build IoT applications for smart home and smart energy.

All three semantic web technologies are ontology agnostic. This will enable future proof design of the Interconnect interoperability framework in a sense that it could be adapted to utilize other ontologies apart from SAREF.

5.2.2.2 KNOWLEDGE ENGINE

The Knowledge Engine (KE – see Figure 55) is a technology aimed at providing semantic interoperability by means of two features: *translation* and *discovery*. Both these features require a common ontology. The ontology of choice for the Interconnect interoperability framework is SAREF and its extensions. Notice that the Knowledge Engine is ontology agnostic and, in principle, can work with any ontology as long as it is expressed in the RDF/OWL format. From here on we consider SAREF as the common ontology used by the Knowledge Engine in Interconnect.

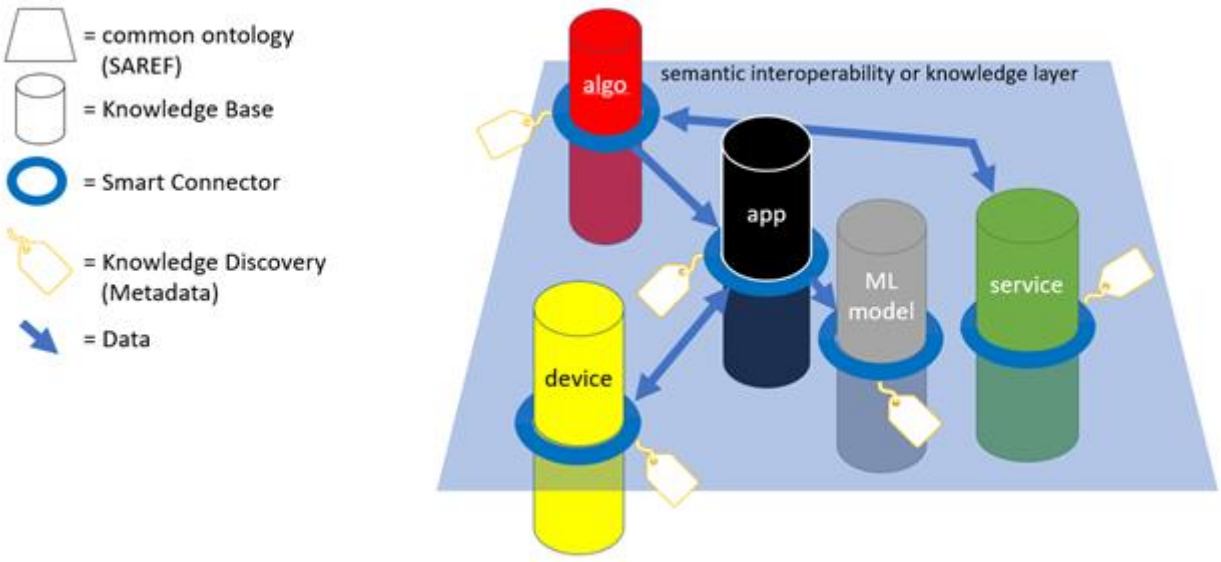


FIGURE 55 - KNOWLEDGE ENGINE CONCEPTUAL APPROACH

The underlying idea is that the KE can interconnect different *Knowledge Bases* (KB), which are depicted in the figure above as cylinders. Knowledge bases can be anything, from devices and services to algorithms, apps, machine learning models or platforms from different vendors. To become semantically interoperable with other KBs, each KB is provided with a specific component, called *Smart Connector* (SC), which realizes the translation mechanism to/from a common ontology (i.e., SAREF).

As a requirement, SCs must know both SAREF and the specific language that needs to be translated to SAREF. Each SC registers itself in a *Knowledge Directory* (KD) (not shown in the figure) with a description of the capabilities that it wants to make available to other SCs. This description is defined as a graph pattern in SPARQL that refers to concepts described in SAREF. These patterns are used for the discovery of knowledge by other SCs. When a SC (and its corresponding KB) is no longer available, or when a new SC becomes available, the Knowledge Directory is dynamically updated. With this up-to-date information, the knowledge exchange among KBs (enabled by the SCs) can take place. This is shown by the arrows in the figure above. The knowledge is exchanged using a combination of SPARQL and RDF messages that refer to SAREF concepts. More details on the KE and its specific component can be found in D2.1 [28].

5.2.2.3 W3C WEB OF THINGS

W3C Web of Things (WoT) Architecture[15] is an abstract architecture designed by industrial partners such as Huawei, Fujitsu, Orical, Panasonic, Hitachi. WoT architectural goals are to improve the interoperability and usability of the IoT. The W3C WoT architecture common principles are (see Figure 56 for high level architecture of the WoT):

- Mutual interworking of different eco-systems using web technology;
- Based on the web architecture using RESTful APIs;
- Using multiple formats which are commonly used in the web;
- Different device architecture supported (e.g., clients, servers);
- Flexibility to map to and cover the heterogeneous physical device configurations for WoT implementations;
- Compatibility between existing IoT solutions, ongoing IoT standardization activities and Web technology based on WoT concepts;
- Scalability to integrate thousands to millions of devices even if they are provided by different manufacturers;
- Interoperability across heterogenous devices and cloud manufacturers.

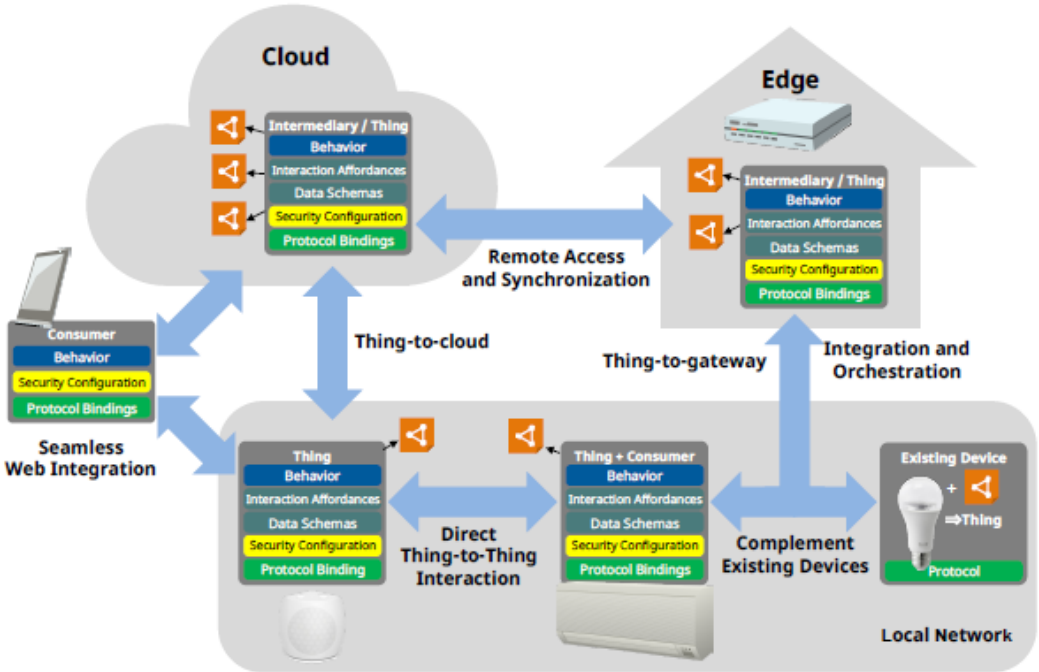


FIGURE 56 - W3C WEB OF THINGS (WOT) ABSTRACT ARCHITECTURE [14]

W3C Things functionalities are (see Figure 57):

- Reading thing's status information;
- Updating thing's status information to support actuation;

[15] https://www.w3.org/TR/wot-architecture/

- Subscribing to, receiving and unsubscribing to notifications of changes of the thing's status information;
- Invoking functions with input and output parameters which would cause certain actuation or calculation;
- Subscribing to, receiving and unsubscribing to event notifications that are more general than just reports of state transitions.

Description mechanism: 1) WoT architecture supports a description mechanism describing things and their functions, 2) descriptions are not only human-readable, but also machine-readable, 3) descriptions allow semantic annotation of its structure and described contents, and 4) descriptions can be exchanged using multiple formats commonly used in the web.

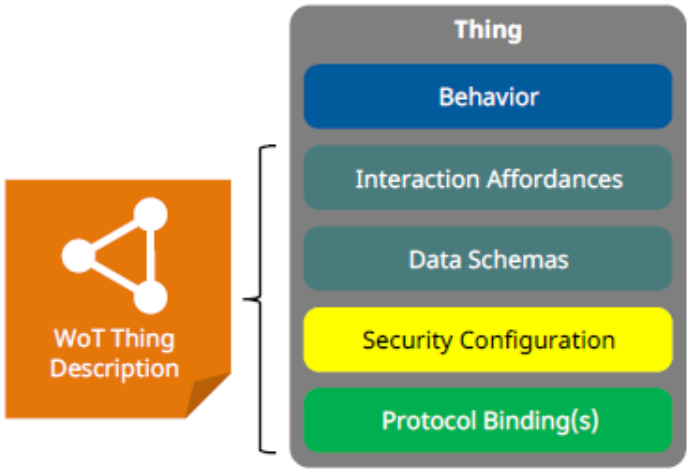


FIGURE 57 - W3C WEB OF THINGS (WOT) ARCHITECTURAL ASPECTS OF A THING [14]

Thing Description (TD) describes metadata about the device, information models representing functions, transport protocol description for operating on information models, and security information. JSON-LD processor is used for processing a TD that enables semantic processing including transformation to RDF triples, semantic inference and accomplishing tasks given based on ontological terms. The WoT Thing Description building block provides interoperability for: 1) machine-to-machine communication, and 2) a uniform format for developers to document and to create applications that can access IoT devices and their data.

A Web Thing has four architectural aspects of interest: 1) behaviour, 2) Interaction Affordances, 3) security configuration, and 4) Protocol Bindings (see Figure hereafter).

Security is considered such as authentication/authorization, secure encryptions i.e. payload encryption, and security mechanisms such as Basic, Digest, Bearer and OAuth2.0. TDs should use integrity protection mechanisms and access control policies, provided only to authorized users. Personally Identifiable Information (PII) in a TD should be limited as much as possible.

5.2.2.4 SAREF-COMPLIANT RULE-BASED REASONER

A semantic reasoner for IoT (Sensor-based Linked Open Rules - S-LOR) is a rule-based reasoner compliant with ontologies (e.g., the M3 ontology that extends the W3 SSN ontology V1). The rule-based reasoner has been also integrated with FIESTA-IoT ontologies that

integrates various IoT ontologies such as M3, IoT-lite, SSN, etc. within the FIESTA-IoT H2020 project. Semantic adaptation will be performed within adapters provided by the InterConnect framework. The Semantic Annotator API (smart connectors in the Knowledge Engine) component explicitly annotates the data (e.g., unit of the measurement, context such as body temperature or outside temperature) and unifies data when needed (e.g., a same temperature sensor provided by various companies can generate different open or proprietary descriptions). The semantic annotation uses ontologies that can be found through ontology catalogues (e.g., LOV4IoT ontology catalogue http://lov4iot.appspot.com/). The ontology chosen must be compliant with a set of rules to infer additional information. The Reasoning Engine API deduces additional knowledge from data (e.g., abnormal temperature) with the usage of inference engine (e.g., rule-based reasoning that comprises IF THEN ELSE rules). Finally, enriched data can be exploited within end-user services available within the Interconnect Service Store. Exact mapping of the SLOR onto the InterConnect interoperability framework and semantic interoperability layer is still early work in progress within WP2.

The reasoning engine for IoT devices to infer meaningful information specification is inspired from [15] - [25]. A rule-based reasoning provides simple IF THEN ELSE logical rules. It will enable deducing meaningful information from semantic sensor data (e.g., IF the room temperature is below 15 Degree Celsius, THEN the temperature in the room is considered as cold). It can be achieved, for instance, with the Apache Jena framework, an open-source Java RDF library which also provides an inference engine (rule-based reasoning) to deduce meaningful knowledge from semantic datasets. AndroJena, a light version of the Jena framework, compatible with Android devices, also provides the query engine and the inference engine for constrained devices if needed. The Jena inference engine is used to infer high-level abstractions by executing a set of "common sense" rules (e.g., following guidelines from experts such as those from the pilots). Ideally, the rule is compliant with: 1) the Jena framework, 2) the W3C Sensor Observation Sampler and Actuator (SOSA)/Semantic Sensor Networks (SSN) ontology and its extension, 3) the Machine-to-Machine-Measurement (M3) [15] and [16] and ontology that classifies sensor type, measurement type, units, etc. to do analytics and reasoning using semantic information, and 4) the SAREF ontology and its extensions for specific domains (e.g., SAREF4ENER, SAREF4BLDG).

Table 7 explains each step of the Figure 58 that illustrates the data workflow.

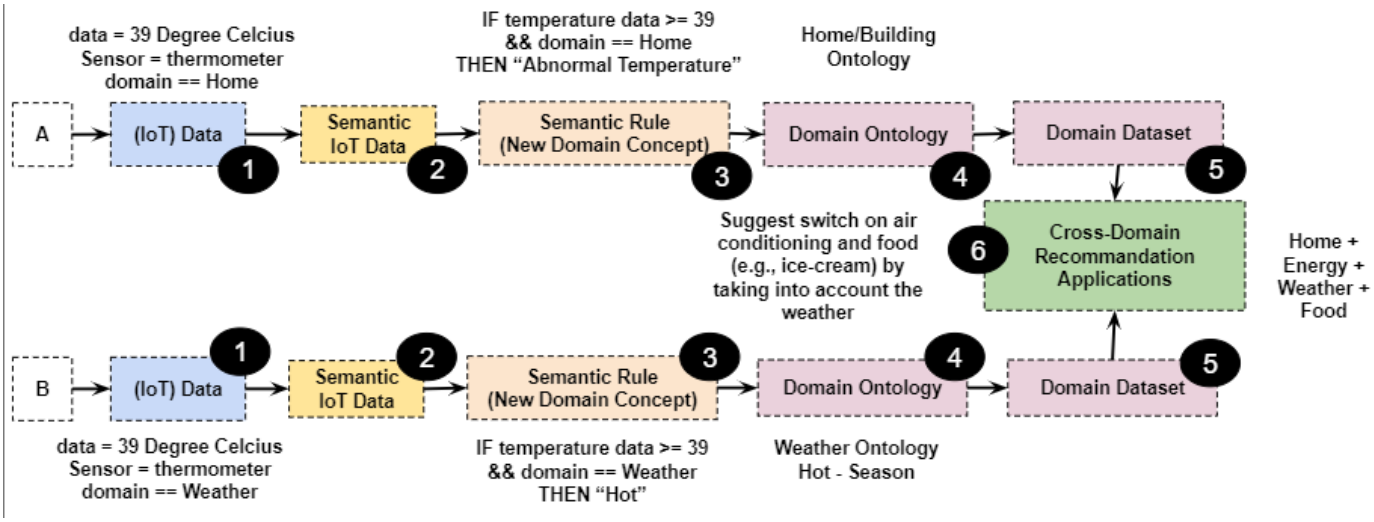


FIGURE 58 - THE IOT KNOWLEDGE-BASED CROSS-DOMAIN RULE-BASED ENGINE AND DATA WORKFLOW

Step 1	The raw measurements generated by the sensors are transformed into metadata with additional attributes: (1) Unit of Measurement, (2) Timestamp, (3) Software Version, (4) Name, (5) Type, and (6) Domain of Operation. Ideally, it could support heterogeneous data formats (e.g., JSON, XML), but requires wrappers to unify sensor metadata descriptions.
Step 2	The framework encodes the metadata using Sensor Markup Language (SenML) to unify sensor metadata before converting into RDF compliant with ontologies (e.g., M3, SAREF ontologies), a key step to later execute the rule-based reasoner.
Step 3	Semantic reasoning drives higher level abstractions as new domain concepts. In the health domain, the reasoning engine explicitly deduces the "flu" concept; in the weather domain, the "hot" concept.
Step 4	The respective domain ontologies are used to classify these new concepts; "flu" as a disease and "hot" as a seasonal condition.
Step 5	The respective domain datasets are used to link data (e.g., food with diseases, menu with season).
Step 6	The concepts, rules, and datasets of the two domains, are combined and cross-domain semantic reasoning takes place. In this example, the cross-domain reasoning produces suggestions for recipes appropriate for a given state of health and the prevailing weather conditions. The recommendations can be acted upon both by end-users and intelligent machines.

TABLE 7 - STEP DESCRIPTIONS OF THE IOT KNOWLEDGE-BASED CROSS-DOMAIN RULE-BASED REASONER

5.3 INTERCONNECT SERVICE STORE

5.3.1 SERVICE CONCEPTS

A service (software) component is a software component offering a service via a (digital) interface. A software component can be regarded as an application or part of an application, and it has or represents some functionality. A service in the real world is realized by performing some of this functionality to accomplish a goal with an impact in the real world. A software component is hosted on a digital platform. A digital platform can host a service component or not. A device is or can incorporate a digital platform. A device hosting some service components (via its digital platform) and offering or using a service via a digital interface is called a smart device. A device with a digital interface is called a connected device. Via one digital interface one or more services can be offered or requested, depending on the implementation.

An InterConnect (IC) service (software) component is a software component offering an IC service via an IC (digital) interface. An IC service stands for the functionality offered via this digital interface by the IC service component. An IC service is compliant with the (or a set of) requirements imposed by the IC Interoperability Framework regarding the functionality provided by the service as well as the features and functioning of the digital interface.

A service offered by a service component can result in some digital data (e.g. result of a forecasting or analysis service) and/or it can have an impact in the real world (a washing program has been started). A service component can be hosted on a digital platform dedicated to hosting software components (e.g. cloud or edge infrastructure) or the digital platform is or is part of a device, of which hosting IC services is not its main goal.

A service by itself is a class or category. For instance, a start delay function can be offered as a start delay service. The start delay service offered by a particular device is a service instance.

An Energy Service is a service of which the main goal is to accomplish an objective in the domain of energy. The scope of an Energy Service can vary for example from improving the energy efficiency at device level, self-consumption at building level (covered in WP3) up to balancing an energy grid or an energy portfolio (covered in WP4). A PV forecasting service is an energy service because it contributes to above mention goals. A start delay service of a device is an Energy Service. Services of which the main goal is not related to the energy domain are referred to as Non-Energy Services. The outcome of a Non-Energy Service may result in some energy consumption as a side effect. In fact, depending on the context an IC service can be regarded as a Energy Service or as a Non-Energy Service, or even as both.

For instance, a washing machine is a device. The washing machine is not regarded as a digital platform, but it usually contains a controller. The controller is a digital platform and can potentially host a service software component[16]. To a user the main service provided by the washing machine is doing the wash. In IC the main service provided by the washing machine is the ability to remotely (and digitally) start or delay the start of a washing machine program.

[16] The IC service software component could also be hosted in the cloud and not on the device itself. In this case the IC service software component communicates via a proprietary or standard interface with the controller. Via the IC interface it is connected to the IC interoperability framework. IC service represents the service offered by the device.

Depending on the context this service can be regarded as a comfort service (non-energy) or/and as an energy service.

Besides Energy and Non-Energy Services, services can be categorized in many ways[17]:

- **IC Regular Services** are the services offered via, not by, the InterConnect interoperability framework. These services comply with the requirements imposed by the interoperability framework. Regular services are listed in the InterConnect service store. An example is a PV forecasting service that is implemented on some digital platforms and can be accessed through interfaces exposed through semantic interoperability controller.
- **IC Framework Services** facilitate the offering and use of Regular Services via an IC platform (e.g. 'discovery service'). IC Framework Services are part of the InterConnect Interoperability Framework.
- Classification **according the run-time dependency**:
    - **Native service:** service running on a vendor's digital platform, making use of specific functions and characteristics of this platform.
    - **IC² service:** IC Regular Service compliant with the IC Service run-time requirements defined for running service containers.
- Classification from the **service user's perspective**:
    - A software component, offering a service, runs 'locally' or 'remotely'. From the perspective of the service user, 'locally' means the service component and the service user component run on the same platform, while 'Remotely' means the service component and the service user component do not run on the same platform.
- Classification according to **how the service is offered as a product in the service store**:
    - **Service subscription model**: the service store facilitates the setup of the interaction with a software component offering a service. The software component itself is not part of the product, only the service it offers.
    - **APP model:** the service is offered as a software component in the service store. The software component is part of the product. It can be downloaded and run on a specific run-time environment.

5.3.2 SERVICE STORE ARCHITECTURE

As one of the main IC interoperability framework tools, the IC service store will provide a single stop for all providers and adopters of interoperable services from energy and non-energy domains. The service store is conceptualized as a web service with its front-end and back-end modules and processes. The main objective is to enable building of the InterConnect

[17] In the course of the WP3 activities additional classification of services may surface, and will be elaborated in the services catalog.

ecosystem of service providers and adopters by allowing them to register new interoperable services and browse existing ones to identify services best suited for the challenge at hand and get all necessary information for accessing and properly utilizing selected services.

The Service Store will also act as the knowledge directory (Knowledge Engine terminology) and provide information about all interoperable services and their capabilities to reasoners running on instantiated InterConnect semantic interoperability adapters. The IC service store will provide a web application with a set of functionalities tailored to fulfil requirements for two main categories of users: 1. Service providers; 2. Service adopters or integrators. As a first step, all users looking to access and utilize the service store will create their InterConnect account and finalize the registration process. After that, they will be able to utilize functionalities provided by the service store.

Service providers, from perspective of the IC service store, are all service operators who adapt their energy and non-energy services to be interoperable by utilizing IC semantic interoperability layer. Once IC interoperable, services can be onboarded onto the service store and made available for usage by 3rd parties. This means that service providers need to instantiate IC interoperability adapter or connector for their service. The complete process for this service interoperability enablement will be defined in the scope of the WP2 and WP3 and will depend on the adopted semantic web technologies (Knowledge Engine and WoT). In the project, adaptation of the existing services and development of new ones necessary for realization of the project use cases, will be executed in the WP3. First, all project partners who are service providers will onboard their services onto the service store and create the first catalogue of interoperable services. During the course of the project, additional services can be onboarded during the cascade funding projects. After the project, all service providers will be able to make their services IC interoperable (following the well-established procedures) and onboard them onto the service store. The goal is to establish the ever-growing catalogue of interoperable services. The main functionalities offered by the IC service store towards service providers are presented in Figure 59.

The first step for each service provider is service onboarding with registration and service offering configuration. Service provider will supply information for onboarded service based on choices and required attributes provided by the service store interface. The onboarding process will act as a wizard guiding service providers through multiple steps towards proper service offering description and inclusion into the overall catalogue. The complete set of parameters and attributes to be requested during the onboarding phase will be defined in future WP3 and WP5 deliverables.

Service providers will choose one or more of predefined service categories and the rest of the onboarding wizard will include steps and configuration parameters specific for the selected category. During the service onboarding, the provider configures access control parameters. This will allow them to maintain access control rules typically applied for their service offerings (i.e. region constraints, service calls per period of time, service call patterns etc.). Access control might also include paid or other types of subscriptions for service usage. The complete set of access control parameters will be specified based on information obtained from WP3. The goal is not to limit the business models and security strategies already in place for provided services.

The following information is provided during the service onboarding phase (list of features to be updated in line with WP3 progress):

- A service identification;
- A short description of the service;
- The service provider (id);
- The version of the service and version history;
- A formal description of the capabilities of the service;
- Product model: Service Subscription or Service APP;
- In case of a service according the Service subscription model:
    - All information necessary to connect to a service instance providing the service.
- In case of a service according the Service APP model:
    - The service software component;
    - Compatibility requirements (the environment needed to run the APP).
- Purchase information:
    - Contract/license agreement, disclaimer;
    - Price.

When onboarded, the service needs to pass IC interoperability compliance test for semantic interoperability and privacy protection. This compliance test will be based on a minimal set of requirements for the specified service category (to be defined in WP2 and WP3). Compliance test will include automated data exchanges and service/interface invocation between the IC service store background test service and the newly registered service running on its hosting platform. Service providers need to follow provided guidelines for making their services interoperable (instantiating corresponding IC interoperability adapter to the service's knowledge base) and after that to proceed with the service onboarding into the IC service store.

After a successful interoperability test, a compliance certificate will be automatically generated and stored in the project level blockchain archive. These certificates will accompany the service store catalogue entries so that service adopters know that a particular service is indeed interoperable as defined by the IC project.

Different service provision options are supported by the IC service store. One option is the provision of interoperable services as containers ready for deployments in adopter's digital platform (IC^2 services). The InterConnect project aims at utilizing Docker and Kubernetes technologies for service containers and corresponding runtime environments. This way service runtime environment can be independent from the underlying operating systems and runtimes available at the adopter's digital platform.

Service containers will have to be created, configured and tested on the service provider end and then uploaded into the service store archive to be available for download and instantiation by service adopters. Smoke tests should be included with each service container so that the

service store runtime environment for containers can test the container configuration during the service onboarding and subsequent instantiations.

After successful service onboarding, successful compliance test and container configuration, service providers will be provided with a set of tools for service maintenance. Service providers will be able to reconfigure and update their service offering through the IC service store interface. Adding new functionalities, updating service container and changing access control are among service maintenance options to be supported. Service providers will also be able to remove their services from the service store catalogue. Service updates will also propagate through established web of reasoners deployed as part of instantiated semantic interoperability adapters.

For successful service maintenance, providers need to monitor service performance. The IC service store will run automated tests of service availability and instantiation outcomes (when adopter instantiates a service container on their digital platform). Service providers will be able to see key performance metrics for their service and get performance reports for a selected period. The performance metrics and reports will be defined within WP3 and WP5 (i.e., service uptime, service response performance, error rates, etc.). Based on the service monitoring reports, service providers may plan for service maintenance. Through the service store ticketing system, the service integrators will provide service providers with feedback or report issues with service usage to the corresponding service providers.

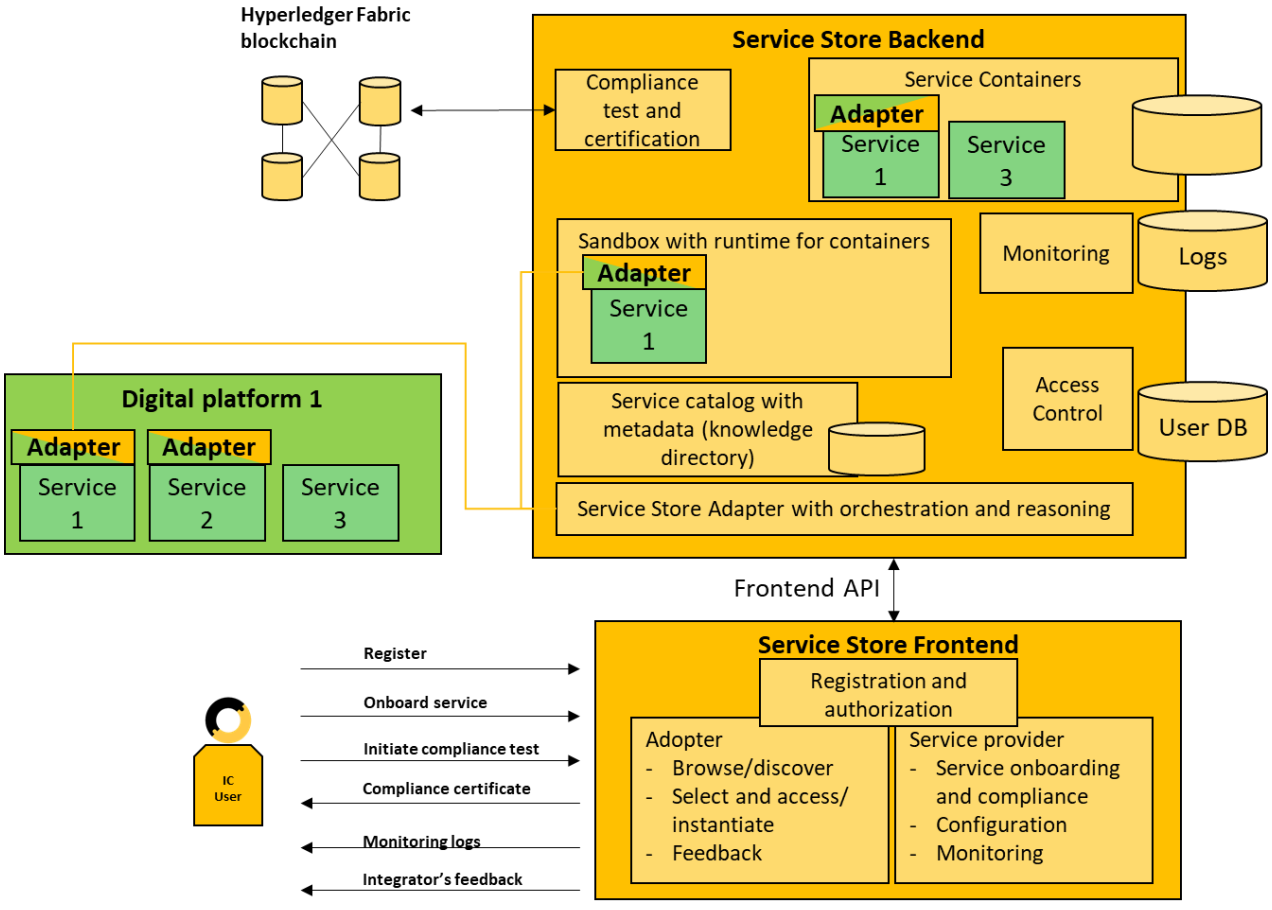


FIGURE 59 - IC SERVICE STORE FUNCTIONAL ARCHITECTURE AND FUNCTIONALITIES PROVIDED FOR SERVICE PROVIDERS

The other IC service store category of users is service adopters/integrators. These adopters are all stakeholders who are service integrators, application developers, platform operators or service providers themselves, looking for specific services to adopt and utilize in their developments. Therefore, service adopters are the main “customers” of the service store. The first adopters of onboarded interoperable services will be IC project partners working on realization of the project pilots and use cases. While working on their use cases, partners will be able to select appropriate services provided by other project partners (not necessarily from the same pilot) and select options for connecting and utilizing those services to achieve goals behind use cases. Further on, the cascade funding partners will act as service adopters and they will be able to browse, select and utilize all onboarded interoperable service for the purpose of realizing their extension projects. Finally, the IC service store will be publicly available for all potential adopters. The main IC service store functionalities provided to the service adopters/integrators are presented in Figure 60.

As a first step, service integrators can browse the complete service catalogue and conduct overview of capabilities and access options for onboarded interoperable services. The browsing will be enabled by service category, provider, pilot, hosting platform, region and IC compliance level. Adopters will also be able to search for services based on keywords. Service interoperability compliance certificate will be displayed for services which successfully passed interoperability compliance tests. It is possible that service adopter cannot access the complete service catalogue if service providers have configured access control rules which limit service listing/browsing. Once a service is selected, the service adopter/integrator can choose how to access a service:

- Adopter is provided with information on how to access the service hosted on service provider’s platform. The instantiated interoperability adapters with properly configures reasoner (and smart connector – Knowledge Engine terminology) will be able to automatically discover services from the Service Store and their capabilities with respect to connectivity and data/functionalities provided.
- Adopter can select service container (if supported by the service provider) and instantiate it within the service store sandbox and perform service testing with included dummy data;
- Adopter can select service container (if supported by the service provider), download it and instantiate it on digital platform. Instructions on how to setup the runtime environment will also be provided.

Some services will require a registration and subscription to be finalized before using it. This will depend on how a service provider configured service access rules for the onboarded service. The service store will not facilitate subscription to services from the catalogue. Adopter will be redirected to the service provider platform to go through the subscription process. Successful service subscription will be signalled to the service store for performance logs and maintenance.

Service integrators will be able to provide to send technical support tickets to the service provider if any issues are encountered while utilizing the selected service. Adopter will receive notifications when a tech. support ticket has been addressed and if the selected service is updated or experiences any difficulties (i.e. the hosting platform or service itself is down for maintenance).

An advance feature for service integrators, which is considered for integration into the IC Service Store, includes sharing access to instantiated service. The goal is to allow adopters to act as service providers for instantiated services (after adopter instantiates service container) and introduce additional service endpoints consequently increasing the overall service provision capacity.

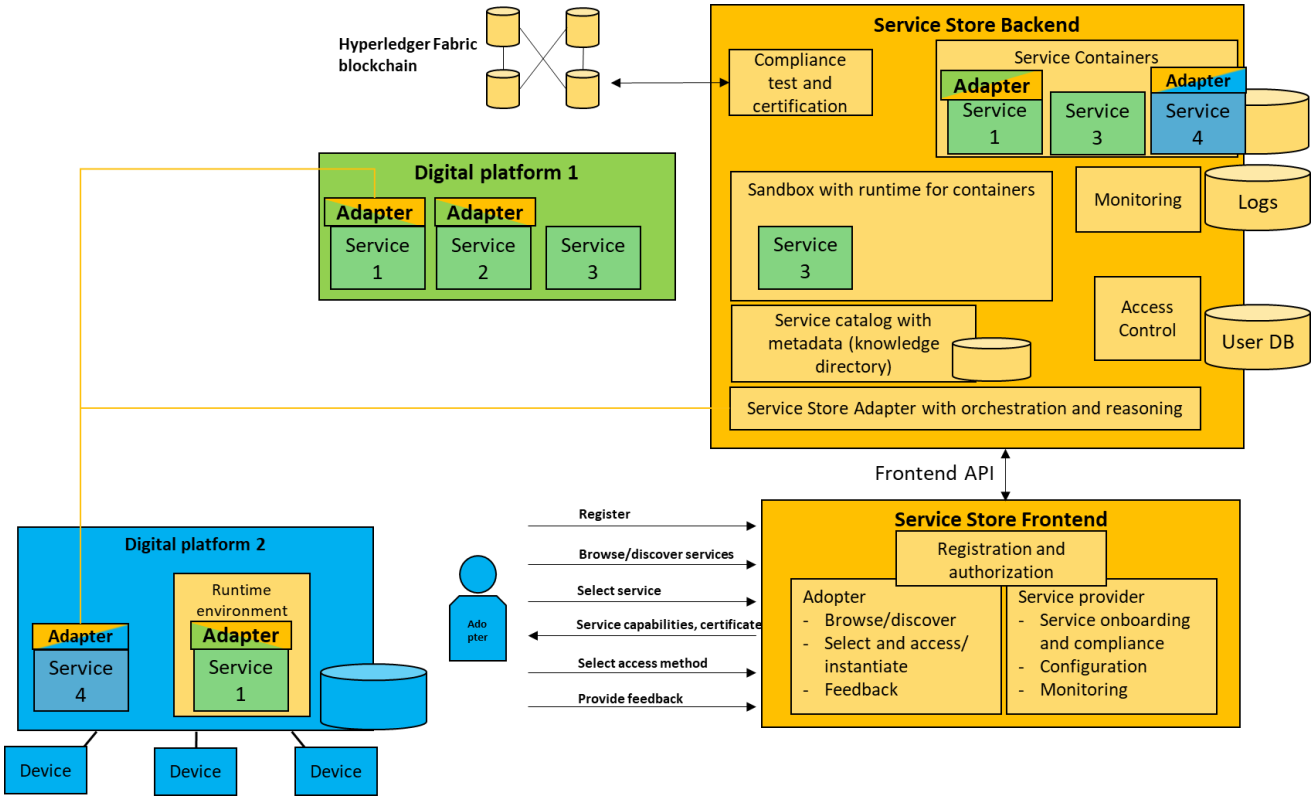


FIGURE 60 - IC SERVICE STORE FUNCTIONAL ARCHITECTURE AND FUNCTIONALITIES PROVIDED FOR SERVICE ADOPTERS

The IC service store will run the IC authentication, authorization and access control management processes. This means that the service store will be the main interface through which IC users will register and get authorization roles. The service store will also include the following background processes necessary for enabling the envisioned functionalities for the service store users:

- **Service runtime environment and sandbox** – enables adopters/service integrators to instantiate service containers and test them before deciding to download them and setup a runtime environment on their digital platforms;
- **Semantic reasoner** – to enable service store participation in the semantic interoperability layer. The semantic reasoner will be able to coordinate with reasoners from onboarded services which will be used for service monitoring and maintenance. The SLOR semantic reasoner (mentioned above) can provide additional knowledge to the knowledge directory (using knowledge from ontology based IoT projects from smart home, building, energy, and grid extracted from the LOV4IoT ontology catalogue[18]).

[18] http://lov4iot.appspot.com/?p=ontologies

- **Knowledge directory** – the Knowledge Engine technology considers knowledge directory as the main record of all registered reasoners and their corresponding knowledge bases. With the knowledge directory all reasoners can discover all registered services and ensure that all updates of the corresponding knowledge bases are always disclosed throughout the semantic interoperability layer. The Service Store will be available for all interoperable services (with properly configured and instantiated semantic interoperability adapters) for discovering services in the catalogue and identifying their functionalities and interfacing options. The semantic reasoning mechanism established around the Service Store will provide automated service discovery and updates.

Services offered through the IC service store can be accessed in three ways (choice of supported service provision options will be an implementation decision made by service provider):

- **Service hosted on originating digital platform**:
  - Access through corresponding interoperability adapter;
  - Discovery through service store reasoner;
  - Operational data forwarding and access control managed by the service provider and hosting digital platform;
  - Services hosted on digital platforms which are not part of the InterConnect interoperability ecosystem and project pilots.
- **Service container instantiated in service store sandbox with runtime environment**:
  - Limited resources to enable service testing;
  - Dummy data sets and test procedures provided by service provider for proper service testing;
  - No operational data forwarding and exchange between service adopter and instantiated service in the service store sandbox;
  - Instantiated service removed from the sandbox after defined period of time.
- **Service container instantiated on adopter's digital platform/endpoint**:
  - Adopter configures runtime environment and instantiates container;
  - Smoke tests specified by service provider are run to ensure proper service container instantiation;
  - Instantiated service is registered with the service store knowledge directory and becomes part of the semantic interoperability layer;
  - Service adopter manages all access control and data/privacy protection procedures.

The IC service store will provide web-based frontend with graphical user interface in support of the provided functionalities to all users. The service store frontend will utilize corresponding

REST API provided by the web framework implemented in the service store backend. Figure 61 shows high level UML usage flow diagram for the IC service store web frontend.

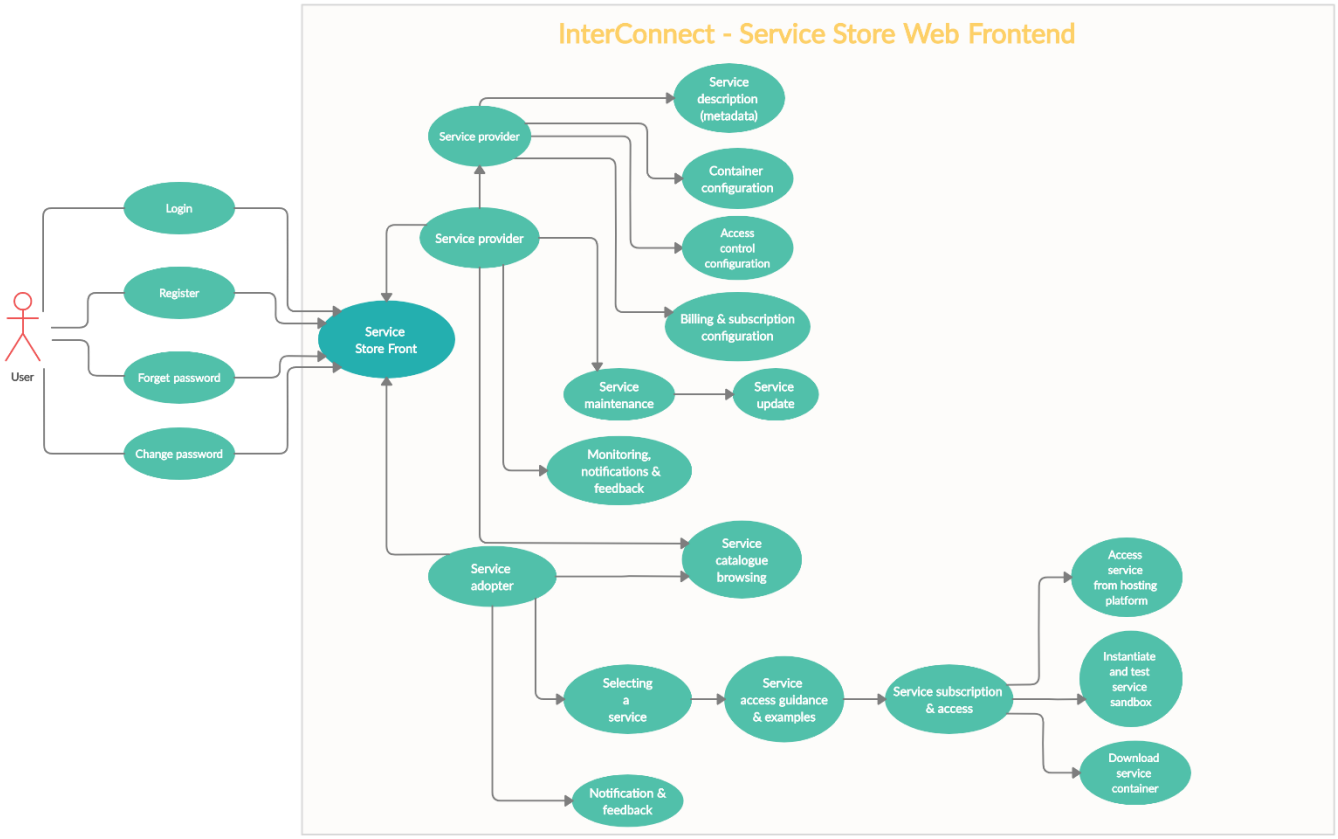


FIGURE 61 - UML USAGE FLOW DIAGRAM FOR THE IC SERVICE STORE WEB FRONTEND

The IC service store will be implemented in Java at the backend and Angular framework for the frontend. During the development and testing phase, the service store will be hosted on servers provided by the project coordinator INESC TEC. It will be possible to instantiate complete IC service store within project pilot as well – this might be necessary for addressing the regulatory constraints and other business-related requirements.

5.3.3 P2P MARKETPLACE ENABLERS

A peer-to-peer or p2p marketplace is created as platforms for connecting those who offer goods and services directly with those who request them. There is no middleman involved in inventory and price management. The middleman is the facilitator of the marketplace. Some examples of p2p marketplaces are AirBnB[19], Uber[20], Etsy[21], OpenBazaar[22], etc.

Proliferation of distributed energy resources (photovoltaic panels, electric vehicles, smart appliances, and battery storage systems) paved the way for p2p energy marketplaces. The

[19] https://www.airbnb.com

[20] https://www.uber.com/

[21] https://www.etsy.com/

[22] https://openbazaar.org/

goal is to enable energy prosumers, consumers and other stakeholders to negotiate and exchange excess energy resources and fulfil their energy needs. In theory, the p2p energy marketplace would allow for lower pricing, reduced monopoly of large energy retailers, flexibility in choosing from whom and what kind of energy is bought or sold.

In the InterConnect project we will pursue distributed ledger technologies, more specifically, consortium and private permissioned blockchain based on Hyperledger Fabric. This technology allows establishing p2p marketplaces where certain level of regulation and organization is required for proper functioning. The Hyperledger Fabric is fast and energy efficient when compared to public permissionless blockchains. This will be our immutable record or ledger of energy and data related transactions in p2p scenarios. Next, we have smart contracts, self executing code accessed through APIs and using trusted information sources for logic validation and execution. Properly configured smart contracts represent relationships between stakeholders and are used for automating processes behind those relationships. Combining smart contracts and blockchain provides basis for many innovative use cases for energy marketplaces like carbon emission trading, loyalty tokens, energy provenance tracking.

Figure 62 provides high level architecture of InterConnect p2p marketplace. The p2p marketplace can be energy marketplace or a marketplace for data transactions required for realization of the community-based use cases. The presented p2p marketplace architecture considers that all EMS and other endpoints in the architecture expose semantic interoperable interfaces as defined in Section 5.2. This can be achieved with supporting data ingestion services which are equipped with semantic interoperability adapters. The marketplace has two main layers. The first layer is a trust management platform based on blockchain and smart contracts. This blockchain records all information from trusted sources, namely EMSs and other relevant sources and can be queried through smart contracts. As an example, information from smart meters about consumption, information about available appliance flexibility and information about energy storage and production will be stored in blockchain. On top of this trusted database, p2p marketplaces for information and energy transaction management can be built. Marketplace would include smart contracts for accessing trusted blockchain and placing orders. It would also provide central interface for facilitating interactions between stakeholders and the exchanged goods as well as transaction management and bidding. The transactions on this marketplace would function as orders for buy, sell or query. Each action is enabled through a smart contract interface provided by the marketplace. Ordering engine matches and executes orders.

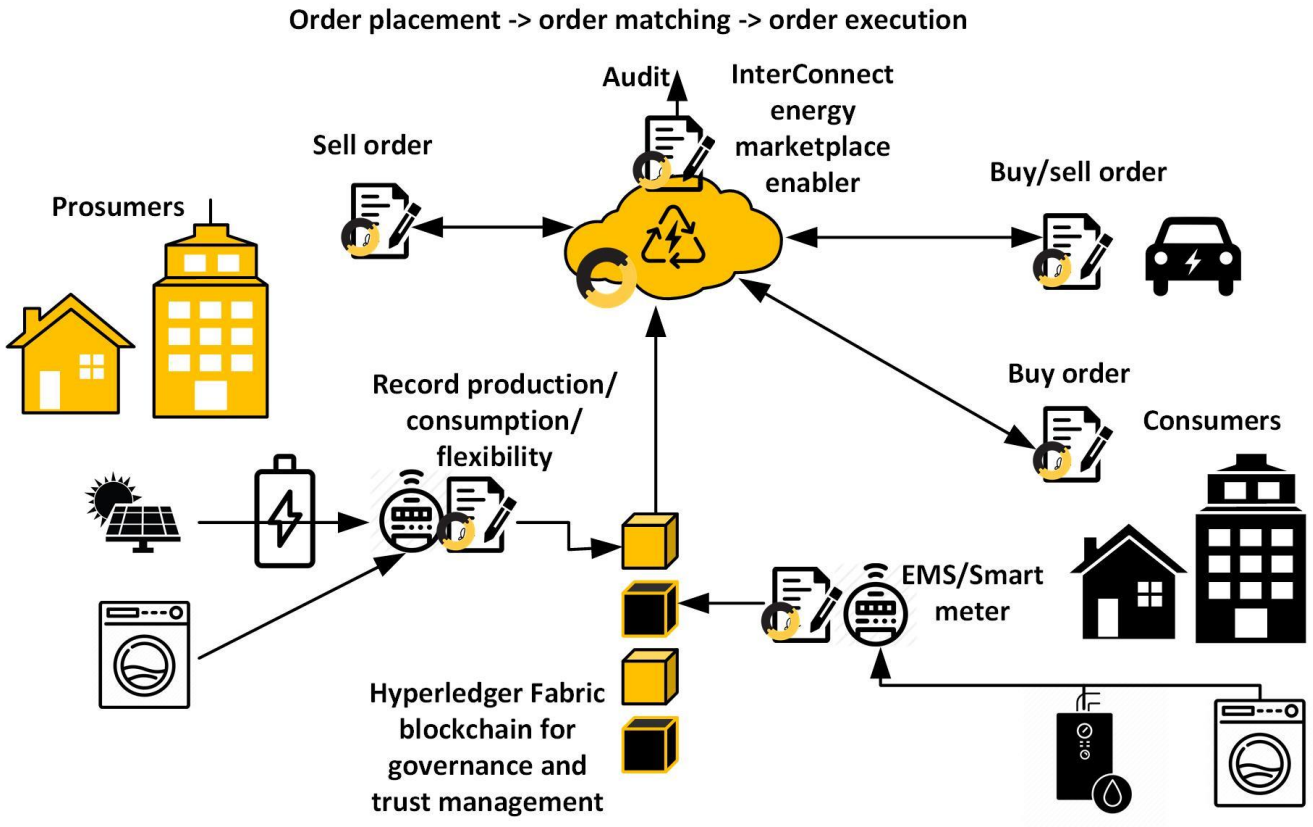


FIGURE 62 - INTERCONNECT P2P MARKETPLACE ENABLERS AND INSTANTIATION EXAMPLE

In the InterConnect project we tackle the p2p marketplace development in the Task 5.4. The goal is to develop enablers which would allow establishment of blockchain ledgers shared between community members and supporting community specific services for data exchange. These enablers include:

- Hyperledger Fabric blockchain configurations for different types of p2p marketplaces (different hierarchies, consortium organizations, etc.);
- Smart contract templates for different types of orders and transactions to be featured in the marketplace. Smart contracts will include APIs for end user GUIs (web application) and APIs for services for automated p2p trading.
- Smart contract templates for generating reports and audits about status of the marketplace and executed transactions - in line with regulatory and business requirements;
- Configurable ordering engine for managing regulatory constraints, transaction priorities and conflict resolutions. The ordering engine also chains the smart contract calls performed by services participating in the p2p marketplace.
- Configurable semantic interoperability adapter for interfacing with the wider InterConnect interoperability framework and interoperable endpoints;
- White-labelled web application for providing interface through which end users place orders. The web application can be instantiated and adapted to specific needs of a community establishing the p2p marketplace.

One or multiple blockchains can be established on the level of the project/pilot while each community use case can have a separate channel with specific read and write rules and smart contracts. Community does not have to be geographically determined but based on joint goals and regulatory frameworks. Figure 63 shows how one Hyperledger Fabric architecture can support different groups of nodes each participating in their own channel with specific rules for data transaction management. The figure shows four groups of nodes: consumer nodes, solar producer nodes, energy storage nodes and utility specific nodes. Each group of nodes can have their own channels with specific smart contracts and rules for data transactions and data writing/reading from the channel/blockchain. Channels interconnecting groups of nodes can be established to facilitate specific types of transactions between these logical groups. The figure also shows ordering engine which is responsible for managing execution of transactions in with predetermined rules.

For the purpose of the InterConnect project, fast prototyping, deployment and validation of the private permissioned and consortium blockchains based on Hyperledger Fabric will be realized with ChainRider[23] blockchain as a service solution provided by the WP5 leader and T5.4 leader VizLore Labs Foundation.

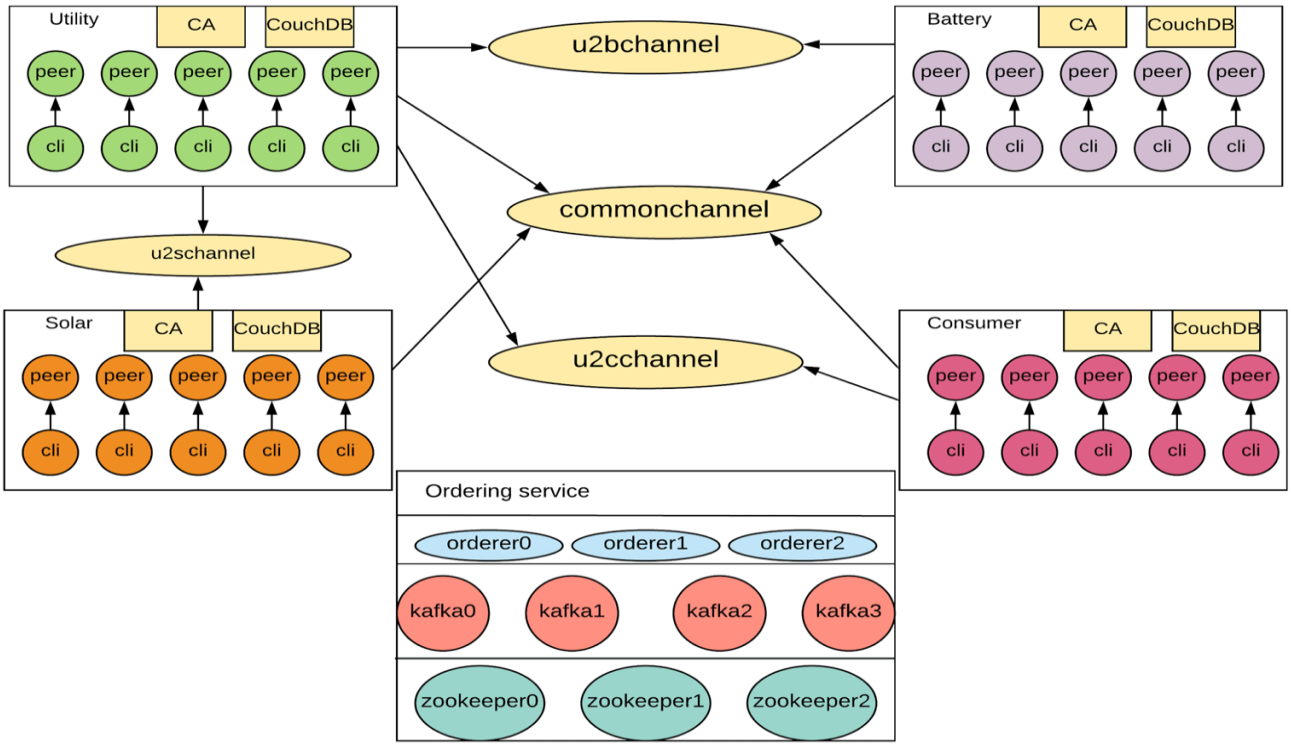


FIGURE 63 - EXAMPLE ORGANIZATION OF HYPERLEDGER FABRIC ARCHITECTURE FOR TRUSTED DATA TRANSACTIONS

Figure 64 shows a p2p community facilitated with Hyperledger Fabric and collection of smart contracts for reading and writing data into the blockchain channels. Interoperability interface for the Hyperledger Fabric based on smart contracts enables the community blockchain system to interacts with the wider InterConnect interoperability framework. Through development of the interoperability adapter for blockchain networks, the project will explore challenges behind interoperability of blockchains. Interoperability and data transactions

[23] https://www.chainrider.io/

between blockchains with different consensus mechanism, data models and transaction rules/smart contract templates should be enabled with one or a set of interoperability adapters. Finally, the interoperability adapters for blockchains will address regulatory constraints when establishing p2p marketplaces for energy. These regulatory constraints and overall integration framework will be specified in cooperation with the WP4.

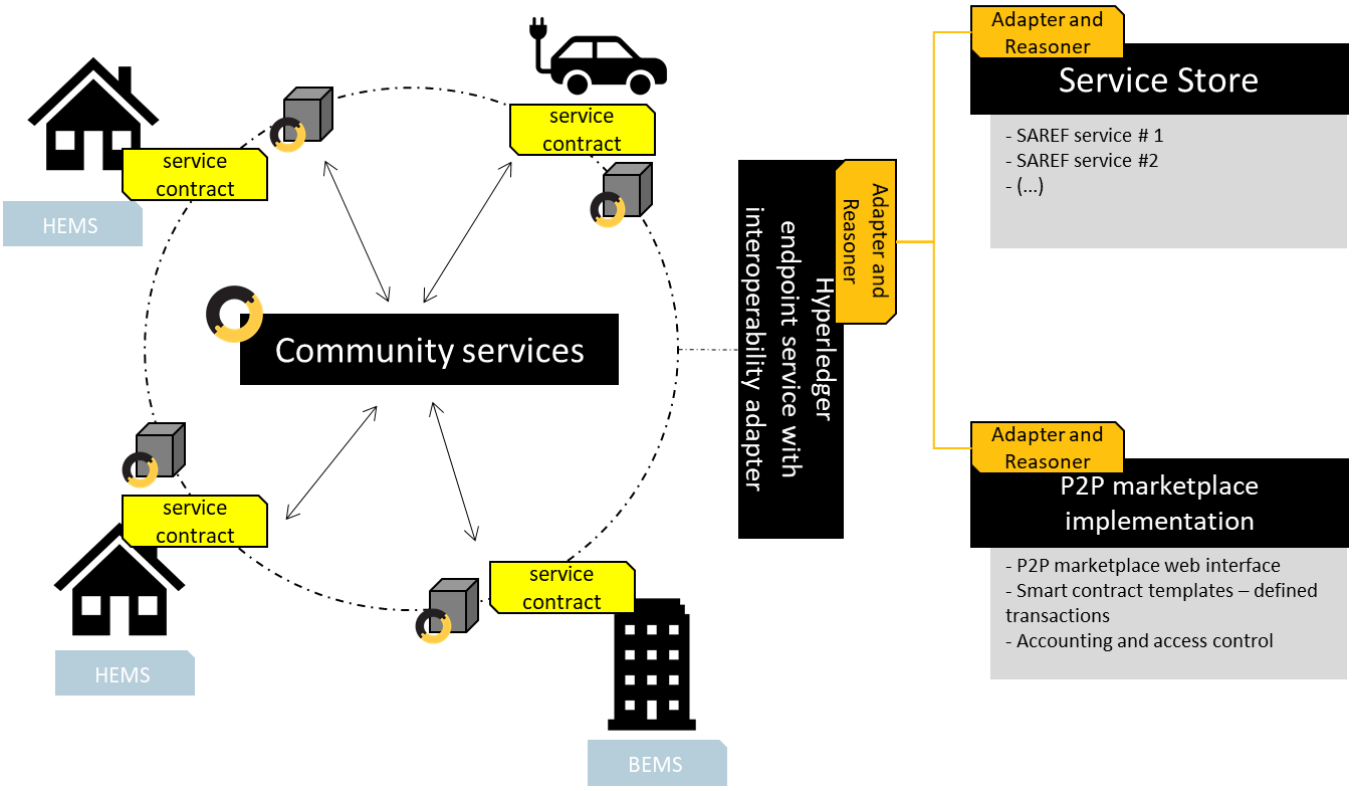


FIGURE 64 - INTEROPERABILITY OF THE INTERCONNECT SEMANTIC INTEROPERABILITY LAYER AND COMMUNITY BASED BLOCKCHAIN NETWORKS

5.4 SECURITY AND DATA PROTECTION FRAMEWORK

The Interconnect interoperability layer does not participate directly in operational data forwarding between services/endpoints equipped with interoperability adapters. This means that the interoperability framework will not relay, parse/process or store any privacy sensitive information exchanged between endpoints participating in realization of project use cases. The privacy protection rules must be followed by stakeholders operating these endpoints (i.e., service provider or digital platform operator), while the IC interoperability framework should support semantic reasoning and discovery following access control rules defined by service providers.

Specific security and privacy protection approach behind each digital platform are included into the WP5 catalog. Section 3 provides overview of these functionalities for each digital platform. The goal of the InterConnect security and privacy protection framework is to ensure that the access control mechanisms and privacy protection rules established by participating endpoints (services and platforms) are followed in the semantic interoperability layer. To this

end, we are defining InterConnect access control enablers which will integrate the access control and privacy protection mechanisms into the semantic interoperability adapters and reasoning procedures. Semantic discovery, reasoning and data translation between legacy and SAREF based data models will include specified access control and privacy protection rules.

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

- InterConnect user registers on the InterConnect Service Store and are recognized as authorized user for accessing InterConnect interoperability framework services. InterConnect user will feature:
    - User ID for authentication, authorization for attribute-based access control;
    - All collected information will be encoded and stored in the InterConnect user database.
- InterConnect endpoint (services, devices) is recognized as an authorized endpoint to participate in the InterConnect semantic interoperability layer and access the framework services.
    - Interoperable endpoints will have authorization ID for attribute-based access control.

Figure 65 shows the first specification of the InterConnect authentication, authorization and access control mechanism as part of the interoperability framework. The goal is to implement access control authority for the complete interoperability framework and integrate it with already existing authentication and access control policies and services residing on interoperable digital platforms and within the InterConnect service store. The aim is to utilize OAuth2 authentication standard (RFC 6749) for delegating user authentication towards their host digital platforms. The OAuth2 It delegates user authentication to the digital platform or service that hosts the user account and authorizes third-party applications/services to access the user account. OAuth2 provides authorization flows for web and desktop applications, mobile devices and smart devices.

The access control policies and identity attributes will be stored on the hosting digital platforms. We also plan to explore implementation options where certain access control policies and identity attributes are stored within the interoperability framework enabler for semantically interoperable authorization and access control as shown in Figure 66. Options for authorizing users with well-known OAuth2 providers like Google and Github will be explored while specifying the overall semantically interoperable access control. One of the main requirements to ensure privacy protection for any identity attributes that are transferred between interoperable authorization entities. Ultimately, the objective is to integrate the authentication and authorization mechanism within InterConnect semantic interoperability adapters and connectors so that the semantic reasoning and discovery follow the established access control rules.

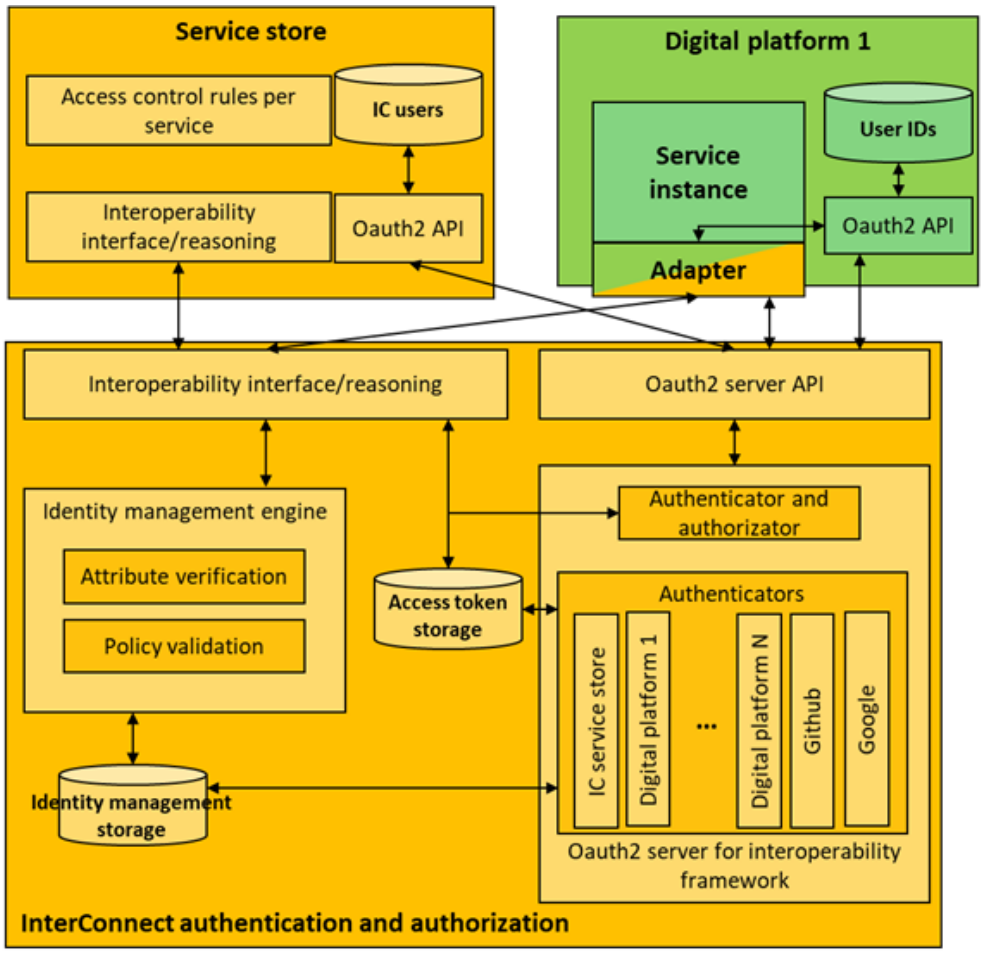


FIGURE 65 - ARCHITECTURE OF THE INTERCONNECT AUTHORIZATION AND ACCESS CONTROL ENABLER - EARLY DRAFT

Access control mechanisms can be specified on the level of the pilot or the whole project. Figure 66 shows a typical pilot architecture with two digital platforms each with its own set of access control rules and data protection frameworks. Semantic interoperability layer interconnects the two platform and their services. User registered on the digital platform 1 can access only the services of the host digital platform. The same stands for a user of the digital platform 2. InterConnect user is authorized to access all interoperable services (if not specifically constrained by interoperable service provider). The InterConnect access control mechanism will enable end users of interoperable platforms to be authorized as InterConnect users. With the user profile from the home digital platform, user can access interoperability framework services and other interoperable services available in the service store.

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

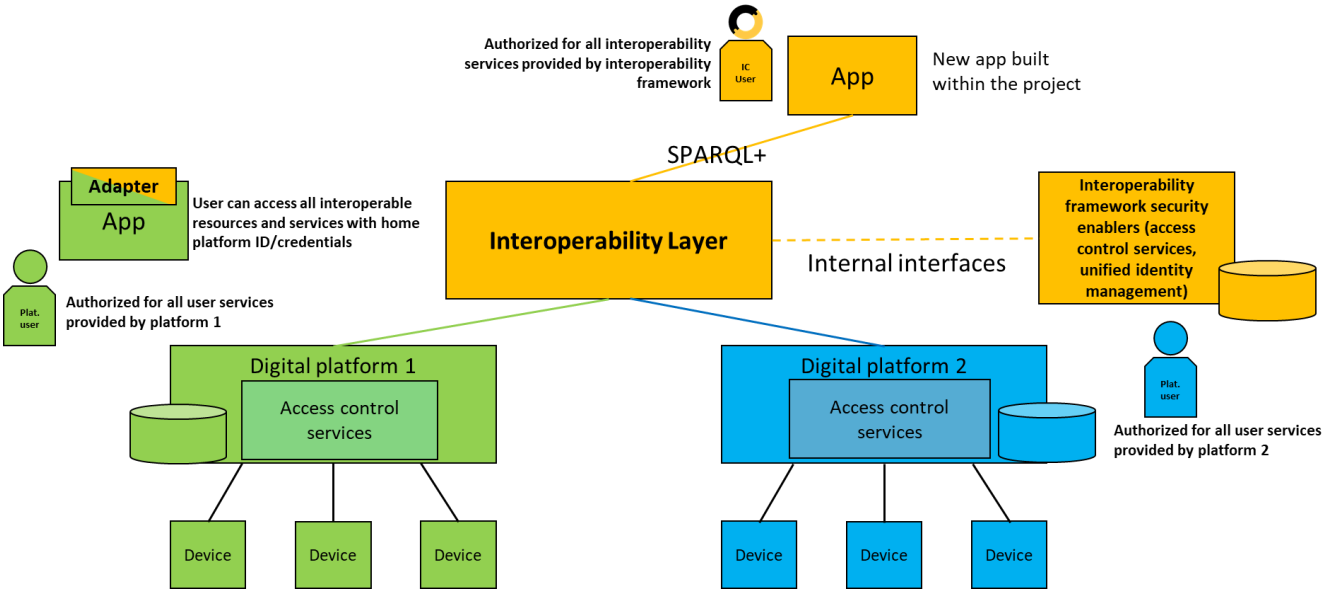


FIGURE 66 - INTERCONNECT ACCESS CONTROL MECHANISM INTEGRATED WITH SEMANTIC INTEROPERABILITY LAYER

The privacy protection mechanism will also be employed as part of the semantic interoperability layer and its adapters/connectors. Within the scope of WP2 the data models will be defined. The goal is to introduce privacy sensitivity categories for data model attributes indicating the level of privacy protection which needs to be followed while transferring, storing and processing data exchanged in the applied data model. This mechanism will be integral part of the semantic interoperability layer and semantic reasoning and discovery processes will have to adhere to established privacy protection policies together with defined access control rules. The complete process will be specified and implemented within dedicated task (T5.3) of the WP5. Data boundaries and message sequence diagrams for authorization are provided in D5.2 [30].

5.4.1 SECURITY AND DATA PROTECTION PLANS FOR PROJECT PILOTS

Dealing with security and data protection is a challenge which need careful preparation when building and deploying IoT systems. This is the case of the seven pilots of Interconnect. The objective of task 2.3 is:

- To assist the pilots in defining a suitable security and data protection plan, while allowing them to develop and experiment IoT innovation for energy;
- To assist the pilots in integrating innovative security and data protection capabilities, such as an unified access control capability;
- To define an innovative practice (called SPOCS, for Security and privacy Plan prOCesS) that can be promoted beyond Interconnect for IoT systems. This practice should combine both security and privacy, in contrast with current practices where security and privacy management are separated, It should also promote continual improvement, e.g., to cope with zero-day attack or unplanned security or privacy incidents;
- To promote the resulting practice and capabilities including at standardisation level.

Cybersecurity threats are continually evolving with the use of connected technologies, thus protecting users and organizations is a constant challenge. Cybersecurity is critical since any security gaps can lead to harm an organization's ability to innovate and to gain and maintain customers. The approach to deal with this challenge, is to define a framework that will help stakeholders integrate security and privacy in their activities. This framework:

- Must address complex IoT systems including hardware, software, information, data, applications, communications, and people;
- Must address systems of system; and
- Must ensure that all stakeholders in the ecosystem apply security-by-design and privacy-by-design.

Today, there is a trend towards adopting a cybersecurity framework that is based in the NIST framework. Two standards are on the verge of being published: ISO/IEC 27100 Cybersecurity concepts and ISO/IEC 27101 Guidelines for cybersecurity frameworks. The latter provides guidance (1) on how to create a framework and (2) how to integrate it into an ecosystem. In parallel, NIST published in 2019 a specific privacy framework. As of today, the NIST privacy framework has not been integrated with its counterpart cybersecurity framework.

Interconnect approach will be to specify a cybersecurity and privacy combined framework for smart grid and IoT compliant with ISO/IEC standards. The framework will help stakeholders create a high-level plan to manage security and privacy concerns in energy (smart grid, smart building and smart home) IoT ecosystems. The creation of the plan is a process which will involve activities such as:

- Identification and analysis of security and privacy threats,
- Identification of possible technical and organisational measures,
- Interaction with system architects building the IoT system to assess the impact of supporting the risk treatments,
- Mapping the resulting measures to stakeholders (organisation measures) and systems (technical measures.

Figure 67 shows the resulting work that will be carried out in task 2.3 to define SPOCS. It comprises in total seven steps: four steps (Task 2.3) with three additional steps (addressed in Task 5.3):

- **Step 1 "State of the art"**: task 2.3 will carry out a state-of-the-art investigation (e.g., ISO standards, NIST frameworks, STRIDE and LINDDUN methodologies), analyze gaps;
- **Step 2 "Identify overall context if pilots"**: task 2.3 will specify a questionnaire to be sent to pilots to get an overview with their experience of security and privacy;
- **Step 3 "Define required method and tools"**: task 2.3 will take the result of the questionnaire to pilots to get an overview with their experience of security and privacy.
- **Step 4 "Define required method"**: task 2.3 will define the resulting methods and tools to be used to define plans.

- **Step 5 "Define workshop methodology and canvas"**; task 2.3 will specify the organization of the workshop to elicit a security and privacy Plan as well as a methodology and resulting canvas;
- **Step 6 "Workshop for project modelization and risk analysis"**: task 5.3 will organize one workshop per pilot and elicit the security and Privacy Plan with each pilot
- **Step 7 "Final Security and privacy plan"**: task 5.3 will finalize each pilot individual security and privacy plan thanks to the feedback received from the workshop organisation with pilots, and background tasks from pilots.

Based on ISO/IEC 27570 (privacy guidelines for smart cities), the resulting security and privacy plan comprises five sub-plans (that will be detailed in D2.2 [29]:

- A governance management plan;
- A data management plan;
- A risk management plan;
- an engineering management plan;
- a citizen engagement plan.

The entire description of SPOCS is detailed in deliverable D2.2 [29].

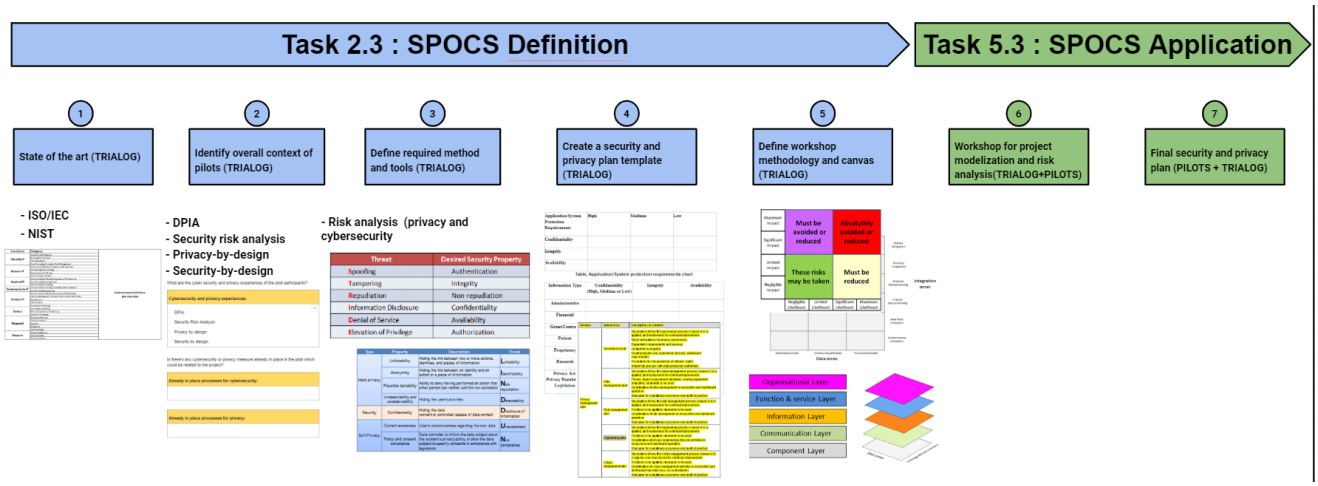


FIGURE 67 - CYBERSECURITY AND PRIVACY FRAMEWORK: SECURITY AND PRIVACY PLAN PROCESS (SPOCS)

5.5 SUPPORTING ENABLERS AND INTEROPERABILITY FRAMEWORK SERVICES

Apart from the main enablers, the InterConnect interoperability framework will include supporting enablers for production grade system operation. Exact list and specification of supporting enablers will be defined within WP5 (scope of the T5.2 and T5.5). In this subsection we provide overview of system performance monitoring, cloud services supporting cloud hosting and tools supporting developers and system integrators.

5.5.1 SYSTEM MONITORING AND PERFORMANCE LOGS

Production grade services and platforms require automated system monitoring and performance reports/alerts based on collected logs from key system elements. For the InterConnect interoperability framework, the monitoring procedures will be applied to:

- Interoperability adapter performance;
- Service store operation;
- Security breaches and threat identification;
- Performance logs for established p2p marketplaces.

Performance logs will be collected on level of different pilots and on the level of the whole project. The generated reports will be used to identify system performance bottlenecks, stability risks and security threats. Based on these reports, development and system update/maintenance tasks will be defined and executed within the T5.5 of WP5. The performance monitoring will take into account the following performance metrics. Metrics are criteria to compare the performances of a system. In general, the metrics are related to speed, accuracy, reliability and availability of services. The following metrics will be considered for the InterConnect interoperability framework performance monitoring processes (list not complete):

- **Service metrics** – service uptime, service response speed/rate, service error responses;
- **Platform metrics** – platform uptime, platform resource usage rates (CPU, storage, memory, networking);
- **Device metrics** – device uptime, device resource usage rates (CPU, storage, memory, networking);
- **User metrics** – user metrics to be specific for different project use cases;
- **Security and privacy protection metrics** – data encryption, data storage (how long data is buffered), interface security, authentication token renewal intervals.

5.5.2 CLOUD BASED SERVICES AND RESOURCES

The InterConnect interoperability framework services will be hosted on cloud/computing platform provided by the project coordinator for development purposes. The services will be organized into containers so that the complete framework can be instantiated per pilot and migrated to other hosting platforms. Reproducibility of the interoperability framework on the level of pilots will be closely managed with proper development and organization of the interoperability framework enablers. Other supporting enablers for cloud-based hosting will be identified and documented during the course of the WP5.

5.5.3 SUPPORT FOR INTEGRATORS

The main goal of the InterConnect interoperability framework is to provide set of tools and enablers for application developers, service providers and platform operators to make their systems interoperable with all other endpoints in the InterConnect ecosystem. The first users of the implemented interoperability enabling toolbox will be project partners working on realization of the pilots and related use cases. The Interoperability toolbox will include the main enablers listed in this section as well as:

- **Source code repos in multiple programming frameworks (to be decided) for all interoperability enablers** with detailed instructions on how to configure/instantiate a software component;
- **Best practices for instantiating interoperability enablers and configuring the semantic interoperability processes** on the integrator side – include automated tests, test datasets and FAQs;
- **Feedback mechanism** – integrators of the enablers will provide feedback through the service store and through dedicated channels (IM system and contact forms) and the core development team of the interoperability framework will work on translating the received information into the development/framework maintenance tasks.

These tools and resources will be available for the cascade funding projects and after that to all 3rd party integrators and developers seeking to make their applications/services/platforms interoperable with the InterConnect framework.

6. PILOT'S INTEROPERABILITY REQUIREMENTS AND IMPLEMENTATION STRATEGY

6.1 GENERAL APPROACH

This section provides an initial analysis of each of the pilots and sub-pilots. The focus is given on their cross-platform interoperability requirements.

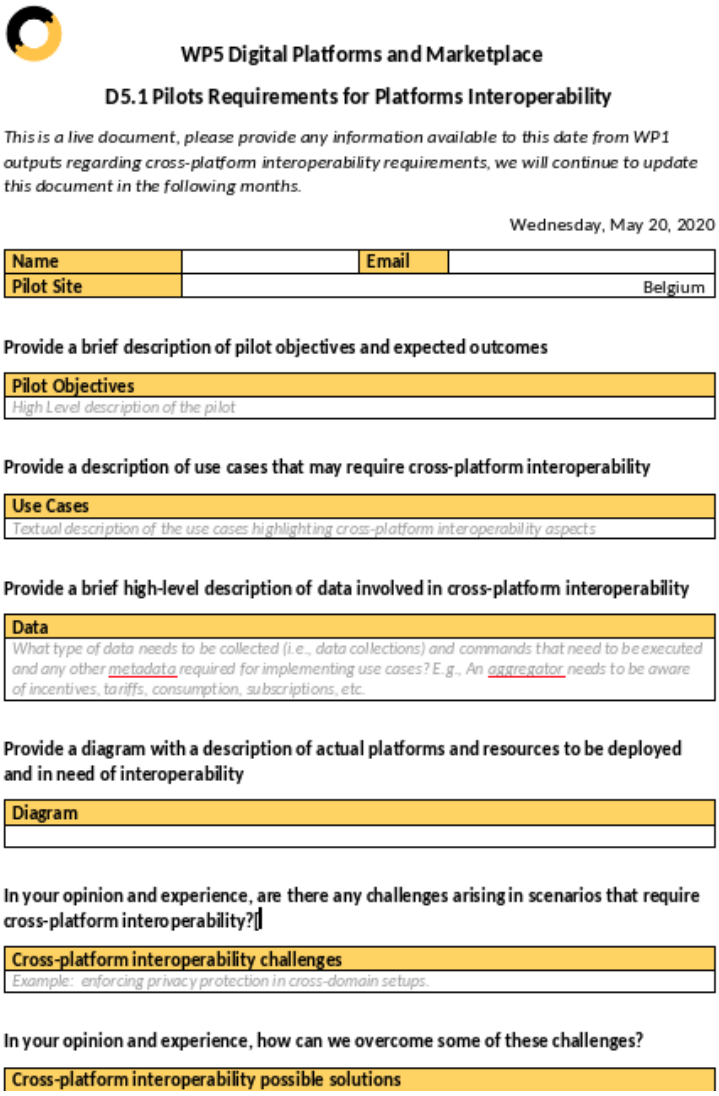
There are seven pilots within the InterConnect project, based in seven countries: Belgium, France, Greece, Germany, Italy, Portugal, and the Netherlands. Some pilots are further divided into sub-pilots, each with their own participating platforms and underlying architecture, producing (sub-)pilot-specific interoperability requirements. Our partner, cyberGRID, is charged with introducing an overarching use case that will interoperate with other pilots.

In the following sub-sections, each (sub-)pilot will be presented by providing:

- An overview table containing information about the (sub-)pilot;
- A brief description of the pilot's objective and expected outcome;
- A description of Use Cases that may require cross-platform interoperability;
- A high-level description of data that needs to be collected and the executable commands needed to implement the pilot's use cases;
- An architecture figure, showcasing each pilot's architectural implementation. The focus is given to providing a first mapping attempt of the interactions between participating digital platforms and adapters in the IC semantic interoperability framework.

The details introduced here were collected during months 7 to 10 of the project (April to July 2020), via a living document shown in Figure 68 to all pilot and sub-pilot leaders. Our objective was to deepen WP1 use cases and focus on defining each pilot's architecture. Also, the document included two questions regarding the main opportunities and challenges arising in cross-platform interoperability scenarios. The results are aggregated and detailed in the last sub-section.

Please note that this is a living document. Therefore, we do not attempt to give an exhaustive list of opportunities and challenges at this early stage, nor do we expect all elements presented henceforth to be static. As not all details are known for most pilots at this stage, our goal was to kickstart critical discussions that will continue to be carried out during the next months, particularly during WP5 activities. All of the pilots' specific requirements, architecture details and technical description of the use cases will be delivered by M24.



WP5 Digital Platforms and Marketplace

D5.1 Pilots Requirements for Platforms Interoperability

This is a live document, please provide any information available to this date from WP1 outputs regarding cross-platform interoperability requirements, we will continue to update this document in the following months.

Wednesday, May 20, 2020

Name		Email	
Pilot Site			Belgium

Provide a brief description of pilot objectives and expected outcomes

Pilot Objectives
High Level description of the pilot

Provide a description of use cases that may require cross-platform interoperability

Use Cases
Textual description of the use cases highlighting cross-platform interoperability aspects

Provide a brief high-level description of data involved in cross-platform interoperability

Data
What type of data needs to be collected (i.e., data collections) and commands that need to be executed and any other metadata required for implementing use cases? E.g., An aggregator needs to be aware of incentives, tariffs, consumption, subscriptions, etc.

Provide a diagram with a description of actual platforms and resources to be deployed and in need of interoperability

Diagram

In your opinion and experience, are there any challenges arising in scenarios that require cross-platform interoperability?

Cross-platform interoperability challenges
Example: enforcing privacy protection in cross-domain setups.

In your opinion and experience, how can we overcome some of these challenges?

Cross-platform interoperability possible solutions

FIGURE 68 - TEMPLATE EXAMPLE FOR COLLECTING CROSS-PLATFORM INTEROPERABILITY REQUIREMENTS

6.2 FRANCE

6.2.1 OVERVIEW

Pilot title	**French Pilot**
Sub-Pilot leader	**Yncréa**
Participating partners	**ENEDIS, ENGIE, GFI (FR), ThermoVault, Trialog, Yncréa,**
Location	**Toulon area, France**

Participating digital platforms from the catalogue	**T-EMS, EMS service provider (Engie, ThermoVault), manufacturer backend, SGE Enedis, metering data platform, flex manager, retailer**
Participating digital platforms not part of the catalogue	**Smart Orchestrator, TIC adapter**

Pilot Objectives

This pilot aims to maximize the use of renewable energy, reduce the environmental impact of energy consumption, and, ultimately, reduce the bill of end-customers. These goals will be attained through:

- Implementation and demonstration of energy ontology for interoperability between smart grids actors (retailers, aggregators, DSO and end-users);
- Validation of IoT architecture and its possible interaction with smart metering infrastructure;
- Business cases demonstrating the economic and social needs of end-users;
- Contribution to Demand-side flexibility (DSF);
- Explore new energy-related multi-domain systems and services (e.g. electricity, heat, water).

Use Cases

Within WP1, two primary Use Cases requiring cross-platform interoperability were defined:

- **[UC1] Dynamic tariff and usage management:** this use case describes how to synchronize the consumption of customer's appliances with the period of best prices from the power supplier to minimize the electricity bill of the consumer. The end-user is informed of the different price periods. The end-user can setup and monitor its appliances (EV, heat pump, water heater, space heater, ...) via an app/web interface. Through the app the end-user can for follow his price schedule with the objective of minimizing his/her electricity bill. The end-user can impose some predefined mode for the dwelling energy consumption (Priority setup). Each service provider can activate the client's appliances it has in charge automatically accordingly to customers settings and preferences. The orchestrator function makes sure that the different service providers active in the house do not foresee to exceed external constraints (max capacity, auto consumption forecast, instantaneous consumption, user preferences, ...). The end-user can override actions of service providers.
- **[UC2] Maximize use of local RES:** this use case describes how to synchronize the consumption of appliances with the period of RES energy production (from PV on the roof of the city hall like Sandro School and the parking close by) . This aim is to maximize the self-consumption of municipal public buildings and potential LEC. The end-user is informed of the period of the RES production. The end-user can setup/monitor its appliances (EV, heat pump, ...) remotely/locally by using different

interfaces. The service provider can activate client's appliances automatically accordingly to customers settings. The end-user can impose some predefined mode for the energy consumption of the apartment/house. The end-user stays the master of the service.

Several external actors are expected to take part during implementation: DSO, flexibility manager, energy supplier, service provider, cloud services providers, appliances manufacturer, HEMS manufacturer, retailers.

Data

The following data is required to implement this pilot's use cases:

MONITORING DIRECTION

- **Energy information,** e.g., tariff information, data generated by the HEMS and service providers; smart meter (data in real time, instantaneous consumption, maximum power subscribed, energy consumed, energy produced), PV production, data generated by EV charging , appliances information.

CONTROL DIRECTION

- For IOT devices/appliances:
  - setup;
  - activate /inactivate;
  - or variable type of signal that the assets should follow (reducing/increasing generation and consumption).

6.2.2 DEPLOYMENT AND ARCHITECTURAL INSTANTIATION

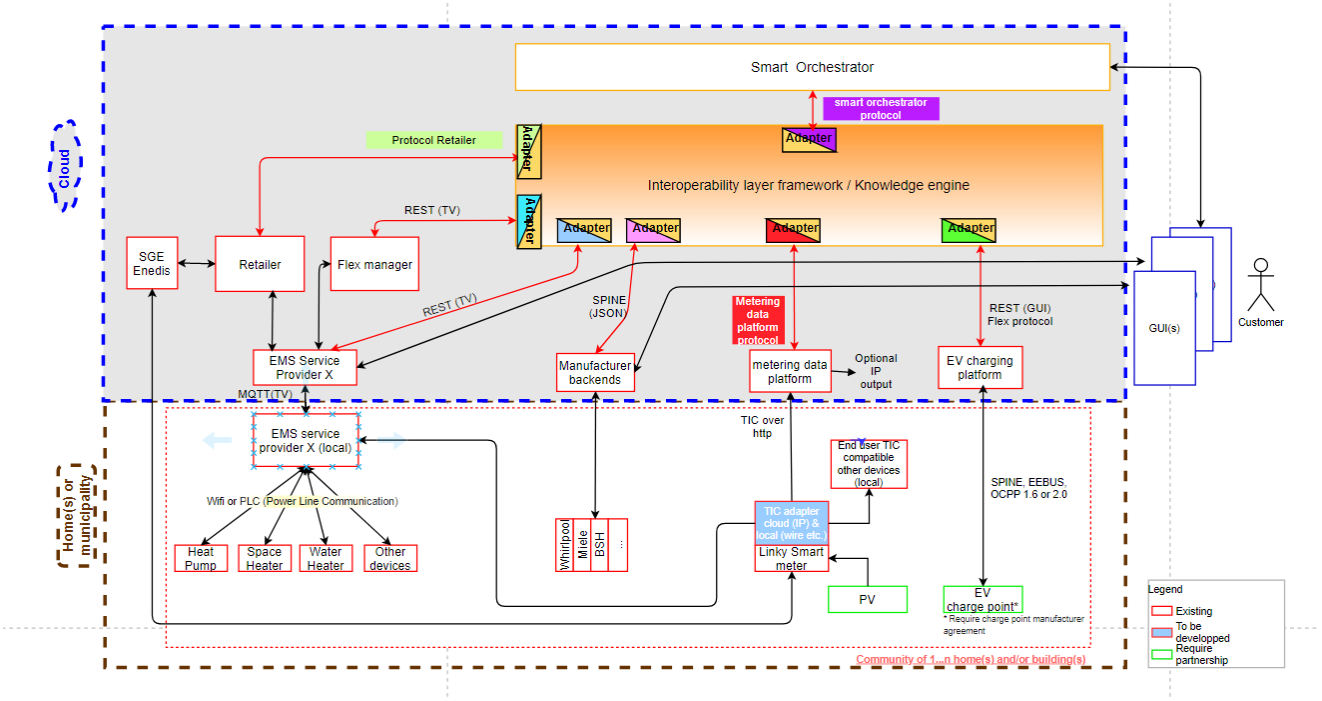


FIGURE 69 - FRENCH PILOT ARCHITECTURE AND INITIAL MAPPING OF INTEROPERABILITY ADAPTERS

6.3 BELGIUM

The Belgian pilot has seven sub-pilots:

- Cordium Hasselt – led by VITO;
- Thor park Genk – led by VITO;
- Student rooms tower Antwerp – led by IMEC;
- Smart District Nieuwe Dokken Gent – led by Ducoop and OpenMotics;
- Zellik Green Energy Park Brussels – led by VUB;
- Nanogrid Leuven – led by Th!nk-E;
- Oud-Heverlee public buildings – led by 3E;
- Mechelen - led by Thermovault.

The following sections provide detailed descriptions of each sub-pilot's objectives, defined use-cases, and architectural implementation.

6.3.1 OVERVIEW SUB-PILOT OUD-HEVERLEE

Sub-Pilot title	**Oud-Heverlee public buildings**
Sub-Pilot leader	**3E**
Participating partners	**3E, Daikin, ABB**
Location	**Oud-Heverlee, Belgium**
Participating digital platforms from the catalogue	**SynaptiQ Power**
Participating digital platforms not part of the catalogue	**DeltaQ**
Sub-Pilot Objectives	
This sub-pilot objective is to steer the HVAC system, EV charger, and battery of a cluster of non-residential buildings (e.g., standard offices, such as city hall, etc.) to limit the impact on the low-voltage grid (220V), minimize the electricity bill of these buildings, and unlock the available flexibility to an aggregator.	
Use Cases	
Within this pilot, two use cases were defined: • **[UC 11] Integrated community energy platform :** Develop an interoperable ecosystem where HVAC installations and EV charging stations, controlled by different IoT platforms or proprietary software, and community demand management platforms can interact to optimize energy consumption. • **[UC 9] Community flexibility:** Demonstrate the available flexibility in thermal systems at the building level to limit the impact on the low-voltage grid.	

Data
The following data is required to implement this sub-pilot's flexibility services: **MONITORING DIRECTION** • **Energy information**, e.g., on-site non-flexible load demand and generation, consumption profiles, desired thermal comfort from end-users, energy contracts of the community members, etc.; • Forecasting data; • Price/Tariff schemes. **CONTROL DIRECTION** • HVAC setpoints; • EV charging power setpoints; • Battery charging / discharging power setpoints.

6.3.2 DEPLOYMENT AND ARCHITECTURAL INSTANTIATION

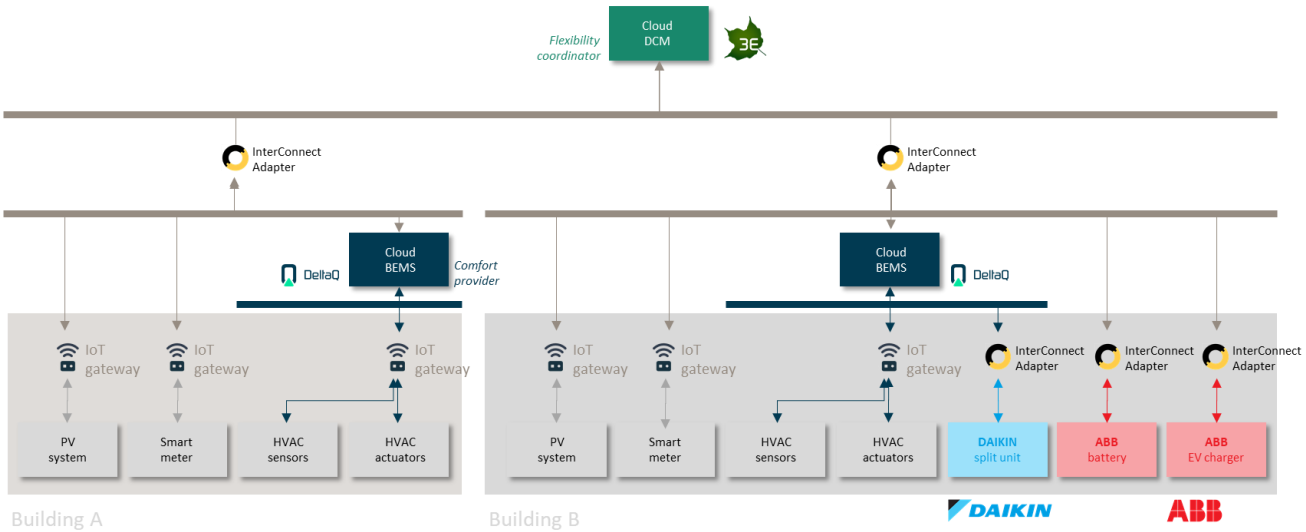


FIGURE 70 - BELGIAN 3E SUB-PILOT ARCHITECTURE AND INITIAL MAPPING OF INTEROPERABILITY ADAPTERS

6.3.3 OVERVIEW SUB-PILOT NANOGRID

Sub-Pilot title	**Nanogrid Leuven**
Sub-Pilot leader	**Th!nk-E**
Participating partners	**From Interconnect:** • Th!nk-E **From outside consortium:**

	• Witteveen+Bos • Kamp C • Ahrend • Reynaerts • Imtech • I.Leco • Rumst Recycling • Knoopwerk • Atelier Ief Spincemaille • Knauf • Sobeltec • ABB • Remeha • Energy Remodeling • KU Leuven • UHAsselt
Location	**Leuven**
Participating digital platforms from the catalogue	**N/A**
Participating digital platforms not part of the catalogue	**I.Leco Software platform**

Sub-Pilot Objectives

This sub-pilot aims to provide a holistic, collaborative approach to advance towards significant changes in the way we look at buildings and neighborhoods.

Use Cases

Expected results will be achieved via the following **technical, business, and environmental** use cases:

- Evaluate inductive power supply principles and their use for air purification and experiment with their integration in walls, ceilings, and furniture;
- Demonstrate effective flexibility management in a neighborhood designed for this purpose;
- Deployment of the Living Lab Smart Innovation Hub;
- Demonstrate the feasibility and experiment with the identified approaches to deliver a facade that generates more energy compared to its cradle to grave usage (i.e., from creation to disposal).
- Research a building design without active heating or cooling and assess the impact on a neighborhood multi-energy operation. Cooperation between building elements, furniture, and tests on comfort perception is critical for evaluating adequate flexibility.

The cooperation of building components and other elements with smart technologies will help promote flexible buildings and neighborhoods (hydrogen cogeneration, smart windows, DC

grid, V2G, interaction with neighborhood battery that is installed on-site). The emphasis will be on the holistic approach, identified as a need for future neighborhoods.

Data

The following data is required to implement this sub-pilot's flexibility services:

MONITORING DIRECTION

- **Energy information,** e.g., active power (generation, consumption), voltage, current, etc.

CONTROL DIRECTION

- Setpoints of devices;
- ON/OFF;
- Discovery.

6.3.4 DEPLOYMENT AND ARCHITECTURAL INSTANTIATION

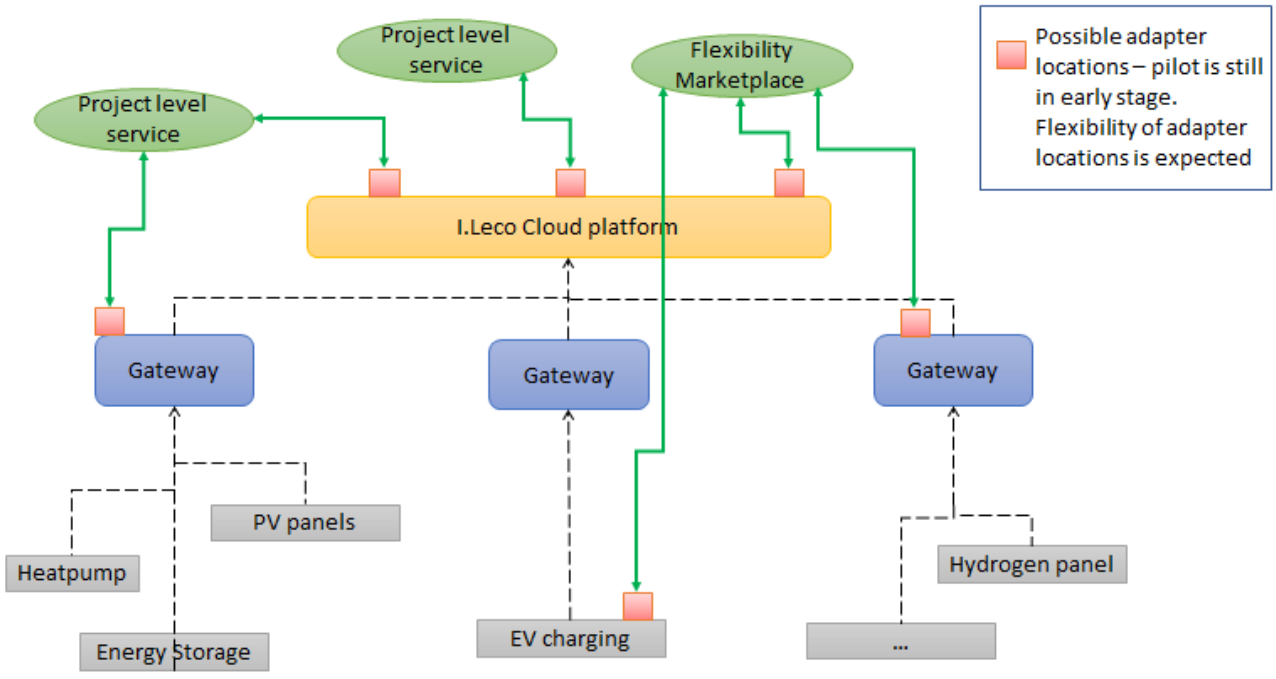


FIGURE 71 - BELGIAN TH!NK-E SUB-PILOT ARCHITECTURE AND INITIAL MAPPING OF INTEROPERABILITY ADAPTERS

6.3.5 OVERVIEW SUB-PILOT CORDIUM HASSELT AND THORPARK

Sub-Pilot title	**Cordium Hasselt and Thor Park Genk**
Sub-Pilot leader	**VITO**
Participating partners	**VITO**
Location	**Hasselt and Genk Belgium**
Participating digital platforms from the catalogue	**Dynamic coalition platform (DCM), Vito BEMS**
Participating digital platforms not part of the catalogue	**SmarThor**

Sub-Pilot Objectives

This pilot aims to reduce energy consumption's environmental impact and reduce overall energy costs for site owners. From VITO's perspective, these sub-pilots will allow exploring new concepts related to interoperability and energy management.

Use Cases

Within these sub-pilots, seven business use cases were defined:

Cordium

- **[UC 12] Community optimization of efficient heat generation:** The main objective is to maintain HDN costs reduced by optimizing the use of local RES generation, thermal storage and controllable loads (e.g., controllable HP). This is mainly achieved by minimizing the instances at which gas is used to produce heat. The service reduces heat generation and distribution costs by, among other approaches, lowering the temperature of the DHN (distribution heat network). Maintaining an optimal temperature range helps to minimize losses and needs for extra heat;
- **[UC 13] Peak shaving via direct control of HP:** Modulate power demand of a controllable heat pump (HP) by applying direct control in a dynamic manner. The heat pump is primarily managed to avoid for the local peak power demand (site level) to go above a certain capacity threshold. By managing the loading of the HP penalties are avoided, especially when the main supplying source of electricity is the distribution grid (e.g., at times of low RES generation or when RES generation may be more profitable elsewhere). The service controls the heat pump load considering the state of other assets for heat and electricity generation and storage (e.g., BTES, Thermal storages, local electricity generation, HPs, P2H). Additionally, the service takes into account the optimization of local RES self-consumption (managed by another service);
- **[UC 14] RES self-consumption:** optimal self-consumption of photovoltaic systems (PV) and wind turbines electricity, at the building level, namely by engaging end-consumers (using virtualization for energy asset sharing and by providing automatic control of heat pumps and smart devices like whitegoods, smart plugs. The service

maximizes consumption of local RES generation at hours of high production to reduce electricity supply costs for heat generation. At times when heat demand is low the electricity generated by local resources may be converted in heat and stored or used to provide non-energy services. The coordinated consumption takes into account the strategies set by the peak-shaving service;

- **[UC 15] Community car sharing:** A community car sharing (mobility) service for Cordium community members. Community members can create an account, book the EV and check their service utilization via an online system.

Thor Park

- **[UC 13] Peak shaving:** Modulate power demand of the building by direct and dynamic management of grid capacity utilization avoiding penalties for brief incursions of power demand above the contracted network capacity. The service controls building loads (heating/cooling system, EV chargers, HP, etc.) in a coordinated manner taking into account optimization of local RES self-consumption;
- **[UC 14] RES self-consumption:** Maximize consumption of local RES generation (e.g., from PV panels) at hours of high production to reduce electricity supply costs. The coordinated consumption takes into account the strategies set by the peak-shaving service;
- **[UC 7] EV charging pricing for flexibility use:** Incentivize smart charging through price signals. The proposed tariff structure signals to the EV charging infrastructure manager the periods at which flexibility (aggregated at parking lot level) may be used for other services. The proposed tariff scheme (defined by the energy service provider) all costs for the provision of flexibility in a dynamic way;

From an interoperability standpoint, the following activities and actions will be covered:

- Connect to services discovered via the service store, running on a cloud platform;
- Have an IC² service run-time platform embedded in the Distributed Energy Management System (DEMS) & Building Energy Management System (BEMS) platforms;
- Download and deploy IC² service (app) from the service store onto the BEMS platform;
- Have several providers for the same service type, thus allowing to switch service providers;
- Ability to provide services to other partners via service store;
- To represent and exchange heterogeneous flexibility information (and allocation) in a uniform way. One data model/interface for flexibility.

Thus, for these sub-pilots the focus is on BEMS-DEMS and DEMS – grid actor interaction. Plug and play devices (and their exposed services) can be easily connected to the BEMS network, via some EEBus compliant devices.

Data

The following data is required to implement this sub-pilot's use cases:

MONITORING DIRECTION

- **Between DEMS-BEMS:** Flexibility plan, consumption plan, dispatching negotiation (dual decomposition, ADMM, …), allocation, status, tracking info;
- **Between DEMS or BEMS platform and 3rd party services:** Service specific API via REST or Message broker (MQTT, AMQP).
- **Between BEMS and devices:** Status information.

CONTROL DIRECTION

- **Between DEMS-BEMS**: Flexibility plan activation, dispatching negotiation (dual decomposition, ADMM, …), allocation;
- **Between DEMS or BEMS platform and 3rd party services:** Service specific API via REST or Message broker (MQTT, AMQP).
- **Between BEMS and devices:** Activation commands like on/off, setpoints, power profiles, etc.

6.3.6 DEPLOYMENT AND ARCHITECTURAL INSTANTIATION

The DCM (Dynamic Coallition Manager) acts as district energy management system (DEMS) or community management system. It is based upon bottom-up aggregation of prosumption and flexibility, provided by the buildings.

The buildings' BEMS provides the following functionality:

- Performing local optimization
- Creating a thermal building model.
- Negotiating with the dispatcher service about adapting its proposed prosumption plan

To accomplish this the BEMS will make use of (building) services, currently implemented as web services. These services can run in the cloud or on BEMS HW on the buildings' premises.

Two types of edge interaction (DCM – building) are foreseen:

- The building has a local intelligent BEMS containing the logic to provide the BEMS functions. The interface towards the DCM will be able to provide the prosumption plans and flexibility graphs, is able to negotiate with the dispatcher service and manage/steer the prosumption according to the agreed plan.
- The building has no local intelligent BEMS. It provides low level information (sensor values, setpoints, …) towards the DCM's 'active GW'. The 'active GW' will perform the above-mentioned functions on behalf of the building. It makes use of the 'building service' web service.

IC Adapters will be integrated at the northbound and southbound interfaces of the BEMS, and at the northbound and southbound interfaces of the DCM. IC adapters towards supporting services will also be added.

The SmarThor platform and a new Azure based IoT platform function as data capturing platforms. On top of that, SmarThor might provide some additional supporting services.

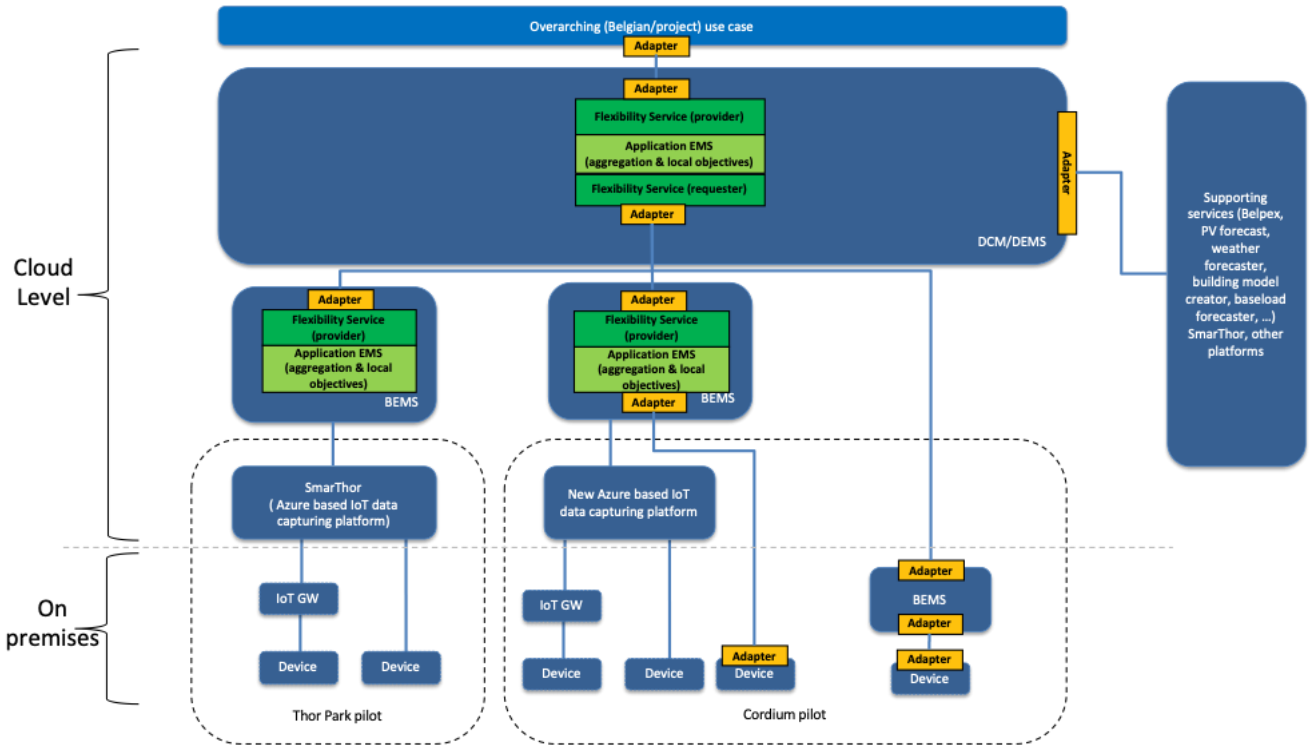


FIGURE 72 - BELGIAN VITO SUB-PILOT ARCHITECTURE AND INITIAL MAPPING OF INTEROPERABILITY ADAPTERS

6.3.7 OVERVIEW SUB-PILOT STUDENT ROOMS TOWER ANTWERP

Sub-Pilot title	**SmartKot – Student housing Antwerp**
Sub-Pilot leader	**IMEC**
Participating partners	**IMEC, Lammp**
Location	**Antwerp, Belgium**
Participating digital platforms from the catalogue	**DYAMAND**
Participating digital platforms not part of the catalogue	**N/A**
Sub-Pilot Objectives	
This pilot's main objective is to test smart grid solutions within a smart student dormitory building context, and ultimately, to evidence the advantages of having such solutions to improve the efficiency of the building energy consumption and the balance of the grid. In order to do this IMEC will perform energy consumption monitoring and will explore the gamification of the use of common appliances	
Use Cases	

This pilot will demonstrate an interoperable platform's applicability by providing a student dormitory with access to a smart grid marketplace. The latter is expected to allow the building to leverage the grid's offer/demand information and dynamically adapt its consumption, reduce electricity costs, and stabilize the grid.

These results will be achieved by equipping the building with several smart appliances (washing machines, dryers, dishwashers, smart meters, etc.) to interact with the grid to adapt as much as possible usage patterns. In order to involve students in the collaborative smart energy usage, they will be encouraged with bonuses and discounts in the student residence.

Some of the possible adaptions are:

- **[UC 19] Student consumption monitoring:** through the use of smart meters IMEC will identify consumption patterns and provide feedback to students to improve their energy consumption profiles
- **[UC 16] Gamification of use of common appliances:** common appliances can be intelligently used, optimizing capacity and scheduling its active time beforehand to try to minimize activity time during grid peak hours.

Data

The following data is required to implement this sub-pilot's use cases:

MONITORING DIRECTION

- **Energy information**, i.e., grid status, active power (generation, consumption) to develop patterns and trends;
- Model **meta-data from local Building Energy management system**.

CONTROL DIRECTION

- Setting for assets and on/off signals;
- Discovery of devices (i.e., plug & play).

6.3.8 DEPLOYMENT AND ARCHITECTURAL INSTANTIATION

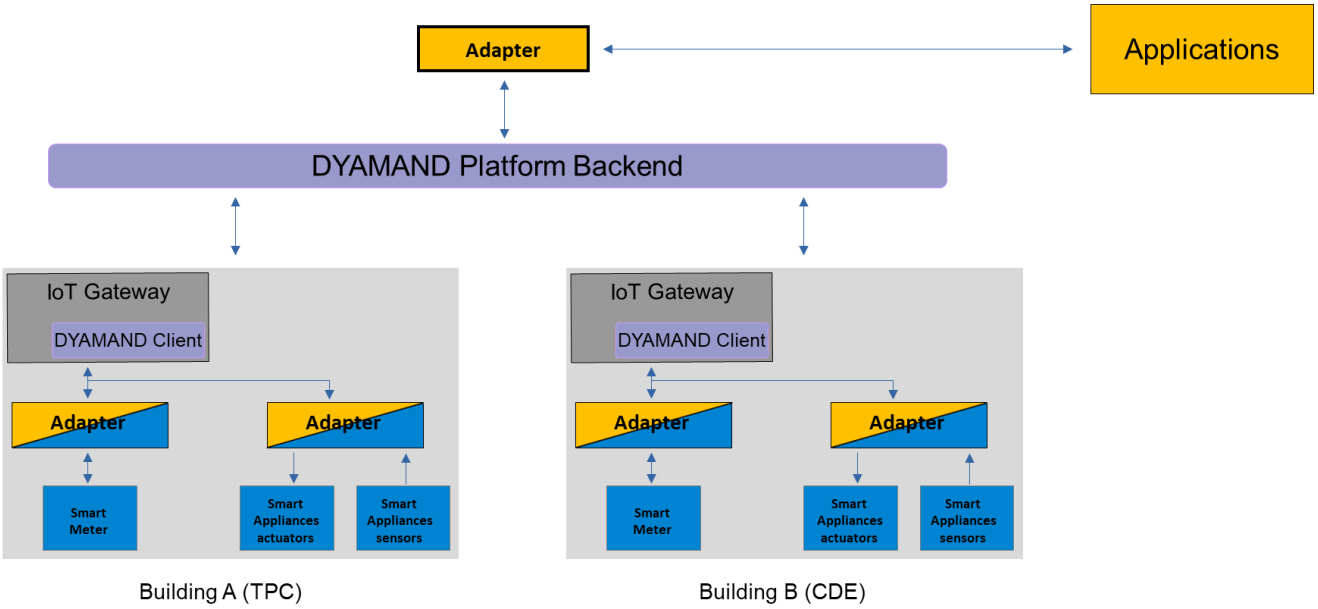


FIGURE 73 - BELGIAN IMEC SUB-PILOT ARCHITECTURE AND INITIAL MAPPING OF INTEROPERABILITY ADAPTERS

6.3.9 OVERVIEW SUB-PILOT NIEUWE DOKKEN

Sub-Pilot title	**Smart District Nieuwe Dokken Gent**
Sub-Pilot leader	**Ducoop**
Participating partners	**Ducoop, OpenMotics**
Location	**Gent**
Participating digital platforms from the catalogue	**OpenMotics**
Participating digital platforms not part of the catalogue	**Belpex**
Sub-Pilot Objectives	
This sub-pilot aims to manage and operate a large residential Local Energy Community in Ghent, bringing smart Energy IoT-appliances into practice in a real-life environment. Furthermore, it wishes to improve the partner's alignment with STORM and Farys Solar, allowing them to ultimately match the energy consumption with the excess wind energy and a local large PV set-up.	
Use Cases	
• **[UC 11] Centralized Energy Management System for Community:** monitor and control collective appliances loads (e.g., District Heating Network, EV-charging	

infrastructure, vacuum sewage system pumps, water treatment plant, etc.) via an EMS system that is managed by the sustainability cooperative DuCoop.

- **[UC 19] Local Energy Community Dashboard:** Interaction between a neighborhood and individual households (smart appliances in houses) via DuCoop's home automation network (in cooperation with OpenMotics) that allows for monitoring of energy, water, etc. consumption and smart appliances in the individual houses. This end-user platform can create interactions between individual energy consumers and the collective EMS, grid balancing agents, potential 3rd party services, etc.

Data

The following data is required to implement the aforementioned use cases:

MONITORING DIRECTION

- **Energy information**, e.g., real-time consumption and production data in the district (industrial/end-user level), local and regional grid balancing data (TSO/DSO);
- **Environmental data,** e.g., weather data, and prediction models for consumption behavior and local RES-production
- Model data **from Battery management and local Energy management system**.

CONTROL DIRECTION

- On/Off signals;
- Power/current/voltage signals or set points;
- Temperature set points;
- Flow set points.

6.3.10 DEPLOYMENT AND ARCHITECTURAL INSTANTIATION

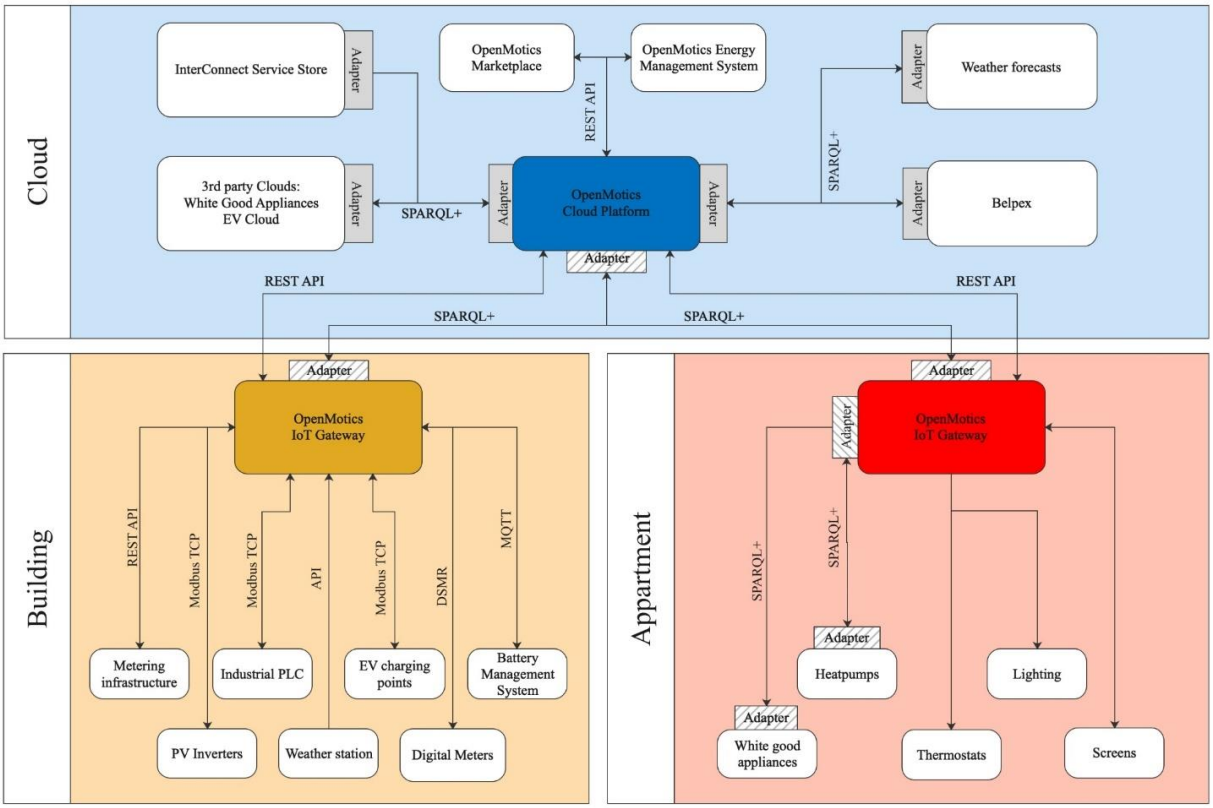


FIGURE 74 - BELGIAN DUCOOP/OPENMOTICS SUB-PILOT ARCHITECTURE AND INITIAL MAPPING OF INTEROPERABILITY ADAPTERS

6.3.11 OVERVIEW SUB-PILOT GREEN ENERGY PARK ZELLIK

Sub-Pilot title	**Zellik Green Energy Park**
Sub-Pilot leader	**VUB**
Participating partners	**VUB**
Location	**Zellik Green Energy Park, Brussels**
Participating digital platforms from the catalogue	**N/A**
Participating digital platforms not part of the catalogue	**N/A**
Sub-Pilot Objectives	
This sub-pilot aims to demonstrate the value of integrating bi-directional charging infrastructure and household appliances inside the micro-grid.	

Use Cases

The main objective is to integrate energy and non-energy services (e.g., mobility) at the Green Energy Park living lab site and evaluate the added value for the stakeholder's integration of SAREF-compliant household appliances and bidirectional charging sites. The pilot aims to tests following scenarios:

- **[UC 11] Centralized Energy Management System for Community:** Energy management systems at building and neighborhood level as well as interacting with the grid;
- **[UC 10] Peer-2-Peer Energy Community:** P2P services and standardized interface with the distribution network. Implement and demonstrate a future business model for P2P trading and V2Gion of the pilot.

This sub-pilot will consist of three clusters of assets in Smart Villag Lab, managed by EMS:

- Charging infrastructure
- Smart houses
- Neighborhood batteries

Adapters between household appliances and building management system will use the following protocols:

- Services trade between and Energy Management system;
- EMS interacts between BMS, Battery manager, Charge point Operator and Grid;
- EMS supports services between stakeholders;
- The Smart meter interacts with digital EAN meter and BMS.

Data

The following data is required to implement this sub-pilot's energy and non-energy services:

MONITORING DIRECTION

- **Energy management information:** real-time consumption and production, environmental data and forecasts, consumption and production forecasts. SoC of static batteries and Vehicles, mobility forecaster, and charging needs

CONTROL DIRECTION

- Settings for power all assets (voltage, current), on -off signals;
- Setpoints temperature (house, vehicles) , time constraints;
- Setpoints SoC batteries (home, neighborhood).

6.3.12 DEPLOYMENT AND ARCHITECTURAL INSTANTIATION

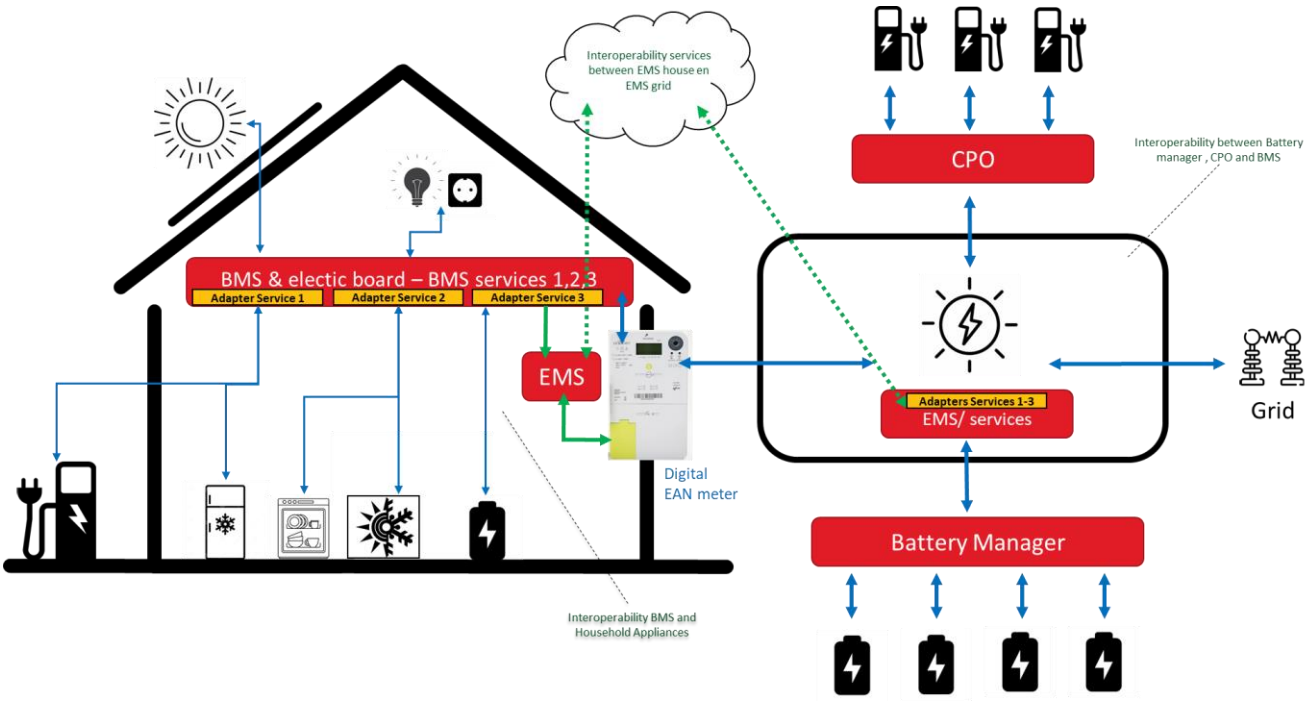


FIGURE 75 - BELGIAN VUB SUB-PILOT ARCHITECTURE AND INITIAL MAPPING OF INTEROPERABILITY ADAPTERS

6.3.13 OVERVIEW SUB-PILOT GENK

Sub-Pilot title	**ThermoVault appartments**
Sub-Pilot leader	**ThermoVault**
Participating partners	**ThermoVault**
Location	**Genk, Belgium** *(Second site to be discussed)*
Participating digital platforms from the catalogue	**Thermovault**
Participating digital platforms not part of the catalogue	**N/A**
Sub-Pilot Objectives	
This sub-pilot aims to prove the potential benefits of community self-consumption and peak shaving energy services by controlling thermal loads and interacting with whitegoods and electric vehicles. Moreover, partners participating in this sub-pilot wish to prove these services' convenience, when combined with existing services like energy efficiency and frequency response.	

Use Cases
• **[UC 9] Smartifying my Local Energy Community:** demonstrate the potential benefits of cross-platform interoperability and energy flexibility. This sub-pilot's primary energy flexibility source is thermal loads, augmented by integrating other energy platforms controlling electric vehicles and whitegoods.
Data
The following data is required to implement this sub-pilot use case: **MONITORING DIRECTION** • **Energy information**, e.g., load demand/generation and forecast, smart meter data; • **Feed-in tariffs** subsidies, e.g., community members tariff, **CONTROL DIRECTION** • On/off; • Temperature setpoints; • EV power setpoints; • Whitegoods specific (unknown at this stage).

6.3.14 DEPLOYMENT AND ARCHITECTURAL INSTANTIATION

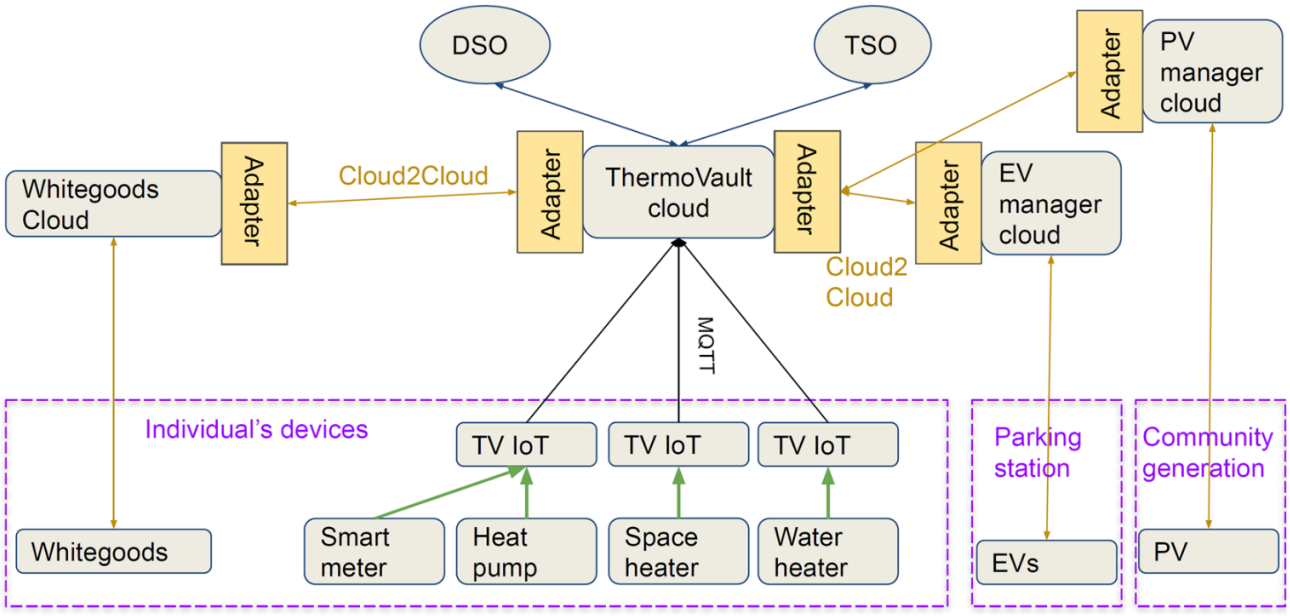


FIGURE 76 - BELGIAN THERMOVAULT SUB-PILOT ARCHITECTURE AND INITIAL MAPPING OF INTEROPERABILITY ADAPTERS

6.4 GREECE

6.4.1 OVERVIEW

Pilot title	**Greek Pilot**
Pilot leader	**GRIDNET**
Participating partners	**GRIDNET, WINGS, COSMOTE, AUEB, GFI, HERON**
Location	**Athens, Volos, Thessaloniki**
Participating digital platforms from the catalogue	**HomeGrid, LeonR&Do, ARTEMIS, Gfi Semantic IOT Platform**
Participating digital platforms not part of the catalogue	**HERON**

Pilot Objectives

The goal of this pilot is to demonstrate the implementation of advanced flexibility scenarios in a residential set-up by fulfilling the following actions:

- Experiment with users interacting with the electricity and wider energy system, under real-life conditions;
- Demonstrate the implementation of SAREF in two open-source IoT ecosystems, which integrate different automation frameworks;
- Showcase the benefits of IoT assisted energy management by involving many different types of appliances (e.g., white-goods, HVAC, metering and control, PV panels, EV charging systems);
- Showcase the resulting data analytics applications and services (optimized flexibility decisions, energy forecasting, predictive analytics, complex event processing, data correlation, data management, optimized EV charging/discharging, etc.);
- Validate user acceptance and understanding of consumer behaviour through mobile apps to engage end-users through incentives (energy cost, social responsibility, etc.);
- Demonstrate viable concepts that ensure privacy, liability, security, and trust in the resulting DR platform by exposing anonymized and aggregated data out of user premises.

Use Cases

Within WP1, the following Use Cases requiring cross-platform interoperability were defined:

- **[HLUC 1] Energy Monitoring & Management:**

Monitoring: Users can monitor power/energy consumption, both total and at phase/plug level for their connected devices

Manual energy management: On top of energy monitoring users can perform manual actuation for connected devices at relay or plug-level, also for lights switches or other devices, e.g., A/C.

Automatic energy management: In addition to manual management users can benefit from automated actuation based on rules/events both set by themselves or allowed/agreed upon to be performed by third parties e.g., in the context of DSF requests

- **[HLUC 2] Home Comfort**

  Monitoring: Taking advantage of non-energy related sensors such as temperature humidity, NH3, CO, dust particles etc., users can have a detailed overview of their homes' environmental parameters.

  Manual management: users can perform actuation actions to their devices based on data acquired from installed sensors, e.g., turn on the dehumidifier if humidity exceeds a certain level.

  Automatic management: Users can define certain rules and create event-based automations, based on installed non energy sensors e.g., turn off A/C if the room temperature goes beyond a certain value etc.

- **[HLUC 3] Flexibility Provision**

  This Use Case describes how end-users can participate explicitly in demand response schemes. Through a web-based dashboard or through their mobile app the users will be able to monitor the current state of their home appliances and decide when they will participate in a demand response scheme and how much of their harnessed flexibility will be released in the system. In order to achieve the aforementioned goal, their consumption data should be collected by various installed smart meters and smart devices, and the collected data should be analysed and visualized by a technology provider, in cooperation with their retailer.

  As a result, the participating users will know at each point of the day the state of their smart appliances, their capability to provide flexibility and an estimation of the collected revenues from their participation in demand response schemes, in order to be able to decide if they want to provide flexibility to the system.

- **[HLUC 4] Data analytics Services**

  Data analytics user behaviour analysis services can be offered both to end-users/consumers and to GRID actors

  Consumers: advanced alerting can be provided to end users regarding energy consumption abnormal patterns based on real time data and historical data analysis. In addition, cost recommendations regarding their energy consumption patterns can be offered as well as cost recommendations regarding specific devices, e.g., reduce energy consumption by shifting washing machine operation to night hours when energy is cheaper, etc. Forecasting via data analytics regarding the monthly energy

consumption plus possible cost savings recommendations could also be provided as well as awards if the guidelines offered are accepted and performed by the end users. Analysed data and predictions based on usage patterns can be used to show potential impact of user's action to his/her overall energy footprint as well as to energy bills.

Grid: Analysed data and predictions based on usage patterns of customers can be used to provide useful insights of demand and schedule supply accordingly. Also, electricity producers/grid operators can provide tailored-made offers based on their customers' needs and give them bonuses/incentives for shifting loads to off-peak hours.

- **[HLUC 5] Security services**

  The user having installed a set of security-related sensors (door/window sensor, activity detector, flood/fire sensor, IP cameras, etc.) at his property will be notified (see push notifications) upon a security breach (see intruder or sensor value exceed a certain predefined threshold). End-users will be able to enable/disable the alarm on demand via the Mobile App from anywhere, anytime. Capability for automated alarm activation (based on rules) could be introduced.

- **[HLUC 6] Increase CO2 savings and become eco-friendly**

  This use case describes how a DSO/Aggregator can provide feedback to consumers regarding the CO2 emissions reduction based on their actions. Through a user interface like a web page or a mobile App, built by a technology provider, the consumers will be able to monitor their consumption provided by a smart meter. The system, based on the output of a DR framework, will ask the consumers through the user interface to shift their loads, in order to optimize GRID operations. The consumers, through the user interface will get feedback related to CO2 savings based on their responses to GRID's requests.

- **[HLUC 8] Unified User Interface Application**

  By means of state-of-the-art technologies and secure interfaces, the end user will able to monitor every (inter)connected device at his house with the touch of a button through the unified user interface built by the technology providers. Either by laptop, PC or a mobile device, if there is an internet connection, then streams from indoors and outdoors cameras, energy and power consumption measurements, environmental measurements etc. will be available 24/7, both real time and historical data. In addition, devices that support control functions/actions such as smart plugs, smart white devices, A/C modules etc. will be controlled through the unified user interface where everything can be integrated, offering a uniform experience. The built-in notification system will allow end user to respond and react to DSO/Aggregator DSF requests (semi-manual DR) without the need of physical presence at the house premises and/or respond to local events, e.g., abnormal consumption patterns, house premises security breaches etc.

- **[HLUC 9] Appliances' energy efficiency**

  Analysed data and predictions based on usage patterns of customers can be used to provide useful insights of how an appliance is used, both in terms of energy consumptions patterns and usage statistics, that is when an appliance is used and in

what way e.g washing machine is used 3 times a week, two of which happen during night hours when it is generally most cost effective. In addition, by analyzing these data, comparison with other similar devices/appliances from other users could be performed and various performance or energy efficiency indices could be extracted, e.g., a washing machine being used in this way is 30% most energy efficient than the 90% of users, or a user's fridge is the least energy efficient of all the users. On top of that, a recommendation system could be implemented by suggesting possible actions to improve appliances' energy efficiency.
Data
The following data is required to implement this pilot's flexibility services: **MONITORING DIRECTION** • **Energy information**, e.g., total energy consumption, power, etc.; • **Environmental data,** i.e., temperature/humidity, precipitation, wind speed, etc.; • **Data telemetry**: e.g.., from motion/contact sensors, etc. **CONTROL DIRECTION** • Setpoint, ON/OFF or variable type of signal that the assets should follow for reducing and/or increasing generation/consumption.

6.4.2 DEPLOYMENT AND ARCHITECTURAL INSTANTIATION

The Greek pilot consists of a residential set-up from 3 different smart home IoT-based providers seen in the "Home Level" of Figure 77. The households that participate in the pilot are all equipped with smart meters and sensors. The collected measurements are made available by each platform provider independently (GRIDNET, COSMOTE, and HERON). Consumers' data is depicted on top of the architectural figure and consists of a Mobile App, a Data-analytics platform, and a Flexibility platform provided by AUEB, WINGS, and GFI. The services mentioned above need to exchange data with the smart home platforms to collect the required measurements for realizing the various use cases that will be implemented in the context of the Greek pilot ecosystem.

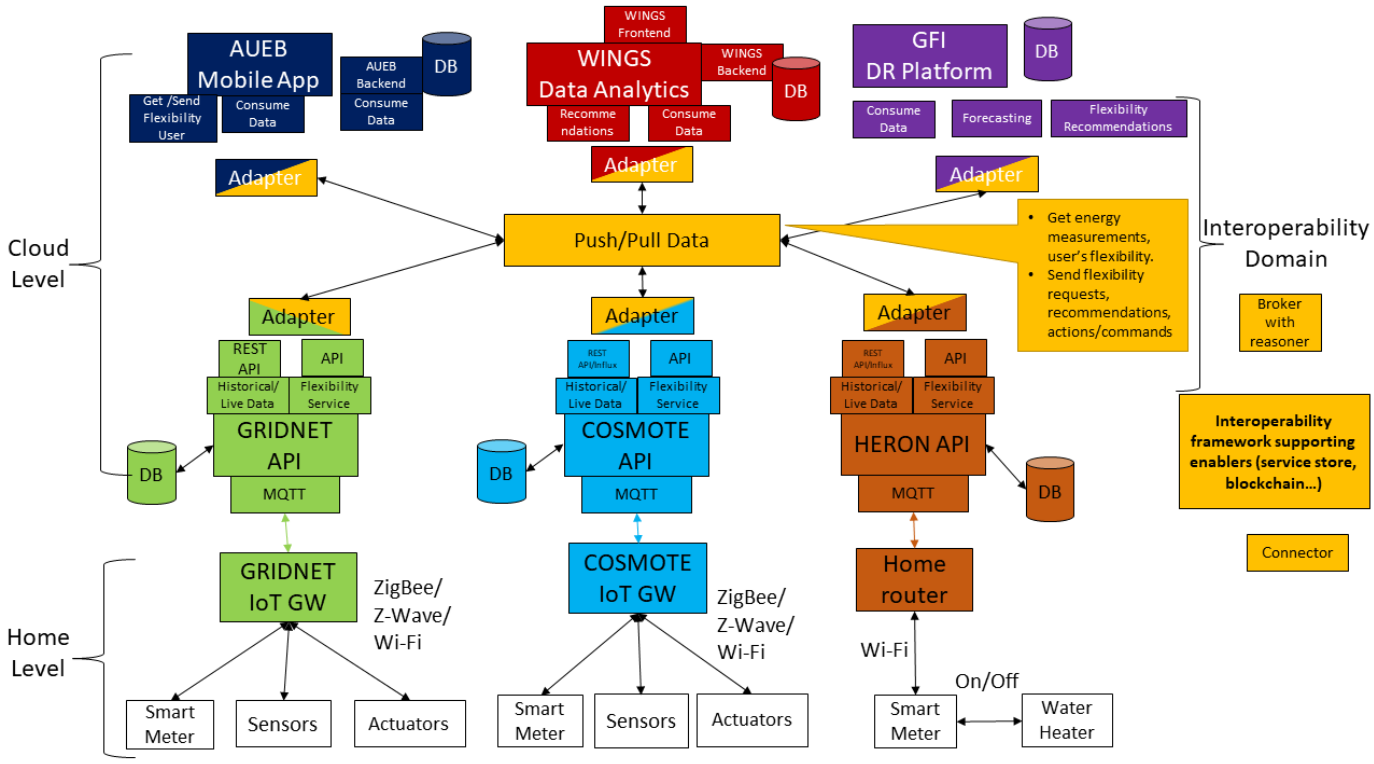


FIGURE 77 - GREEK PILOT ARCHITECTURE AND INITIAL MAPPING OF INTEROPERABILITY ADAPTERS

6.5 PORTUGAL

6.5.1 OVERVIEW

Pilot title	Smart grid infrastructure as an enabler of new business demand to integrate DSF in e-markets – Portugal
Pilot leader	EDPD
Participating partners	EDPD, INESC TEC, SonaeMC, Sensinov, SEP, Elergone, DOMOTICA SGTA, ThermoVault
Location	Multiple Locations: Commercial (12) & Residential (5)
Participating digital platforms from the catalogue	Cognitive Load, Grid and Market Hub Platforms, Sensinov, EcoStruxture Building Operation (EBO), ThermoVault

Participating digital platforms not part of the catalogue	Elergone (TBC), DSO Platform (TBC)

Pilot Objectives

This pilot's objective is to test how a Smart Grid infrastructure can enable new business demand to integrate DSF in e-markets. More precisely, the overall goal can be detailed as follows:

- Exploit different energy services for households, commercial buildings, and energy communities;
- Exploit interoperable digital platforms for energy and non-energy services based on cloud and hybrid connectivity solutions;
- DSF Management at the local level with different business use cases, such as P2P, energy efficiency, e-mobility;
- Integration of DSF for wholesale market bidding strategies with the development of the DSO's flexibility market;
- DSO acts as an enabler of new business models while ensuring safe and reliable grid operation.

The Portuguese pilot has some unique features since it combines both residential and non-residential end-users, DSO, ICT solutions providers, and electricity retailers. This deployment setting will extend SAREF to a new generation of interoperable BEMS system for non-domestic end-users and offer technical conditions to test a standardized DSO interface between smart grid operation and market players.

Use Cases

Within WP1, several Use Cases requiring cross-platform interoperability were defined for the Portuguese pilot:

- **[UC 1] Monitoring Energy Consumption:** This Use Case describes how a user can, throughout technological solutions, such as the Energy Management System (EMS): 1) have convenient access to the data generated from all their appliances, in order to monitor their consumptions of energy; 2) set preferences on AC temperatures (within some activation and limitation conditions); 3) increase energy cost savings (e.g. having best tariffs); 4) offer flexibility (by shift usage in exchange for best tariffs); 5) set preferences about flexibility on the usage of some appliances, offering flexibility by possible shift loading in time of some defined appliances (washing and dish machines, EV charging) ; 6) have notifications (according their preferences) about improvements of their consumption behaviour; 7) have control based on informed decision (scheduled actions/ autopilot mode);
- **[UC 2] Subscription of services for domestic energy management:** This Use Case describes how the end-user can have the ability to select which (sets/modules) services to subscribe (ex. Load optimization for EVs; PV forecasting; Recommendation System)

through technological solutions, such as the Energy Management System (EMS) - concept of the "Energy as a Service".

- **[UC 3] Data sharing via consumer enabled preferences and profiling:** This Use Case describes the possibility to enable consumer data to be shared, while allowing the consumer to choose what data (and metadata) is selected, according to a profile. Data ownership and control should be user centric and reflect user's preferences. An array of data streams emerge from the domestic realm, exposed or abstracted by the EMS. The consumer gains awareness for the data streams at his/her disposal and selects which data streams he/she allows to be shared.
- **[UC 4] Prosumer data ingestion for third-party enhanced data driven services:** This Use Case will create new data driven services requires access to data, but also awareness of its representativeness, geographical dispersion, and origin profiling. Data driven services should be able to filter and give back rewards to create incentive and engage prosumers.
- **[UC 5] DSO Open Data 4 New Energy Services:** This use case describe the Data interfacing mechanism for the exchange of new added-value data for consumers and DSOs, with the creation of a bi-directional data interfacing mechanism between DSO and consumers, enabling the exchange of new added-value data for DSO and consumers
- **[UC 6] Multi-Level integrated Energy Management System (iEMS) for Commercial Buildings:** aims for integrated management of retail shop chains by combining local and centralized-level energy management capabilities. In this case, existing stores/buildings have a heterogeneous set of technologies; interoperability enables more efficient energy management;
- **[UC7] Flexibility Aggregation of Commercial Buildings:** some of the consumption/generation existing in the commercial buildings are flexible, so retailers/aggregators need interoperable tools to interact with end-consumers, estimate/manage/activate/deactivate the existing flexibility;
- **[UC 8] Convenient Smart EV charging at Commercial Buildings:** This use case describes the particular case of EV charging flexibility and subsequent flexibility management regardless of the flexibility purpose (local building management, portfolio imbalance optimization, DSF to DSO). It also regards the integration with iEMS (Intelligent Energy Management Systems) for optimal energy management.
- **[UC 9] Enabling community services via P2P and Blockchain enablers for SAREF services:** communities acting as a platform to collect data, interact with prosumers, and deploy decentralized energy and non-energy services. P2P enablers allow tertiary services with a SAREF interface to reach out to communities and automate and trigger actions. A common approach to deploy community services exempts service providers to become experts in P2P and blockchain while enabling them to leverage on this capability;
- **[UC 10] Regional Flexibility Portfolio - Distributed Flexibility Management:** This use case will describe how the DSO can develop an interfacing mechanism (through DSO Interface) that will enable to perform local and regional congestion management

& voltage control based on the interconnection to both commercial and residential flexibility pools – rules-based or agreement solutions.

- **[UC 11] Electric Vehicle Smart Charging – Flexibility Management Through Impactful Embedded Variable Load:** the EV charging stations installed in some buildings are consumption assets for demand flexibility and EV forecast. They enable innovative mobility services where EV management platforms, building management systems / iEMS, and EV user Apps can interoperate. This use case will describe how a collaborative flexibility management system can be developed between the DSO and the electric mobility charging operators.
- **[UC 12] Retrofitting Solutions for Energy Efficiency & DSF 4 DSO :** This use case will describe the development of a collaborative mechanism between DSO and a technical platform provider, that by deploying retrofitting equipment (water heater, boilers and heaters) at household level, an innovative market for DSF for DSO at local and granular level can be created. This interfacing between DSO and cloud-base solutions at systems level.

Data

The following data is required to this pilot's use case implementation:

MONITORING DIRECTION

- **Energy and non-energy information**, e.g., power, consumption, production (e.g. from PV), voltage level, number of connected devices, temperature, humidity, status, run-time, etc.;
- Communication **monitoring information**, e.g. last communication from a certain device;
- **Forecast,** e.g. energy consumption, production, EV consumption, storage;
- **EV information,** e.g. charge and forecast information (power consumption, charge time, usage time, user ID);
- **Flexibility** information, e.g. grid needs & market/platform offers (day ahead, intraday, smart contracts)
- Assets and Resources **location**;

CONTROL DIRECTION

- Setpoints to manage energy consumption, production and storage;
- ON / OFF commands for managing individual loads or groups of loads;
- Scenario definition (to type and model the levels of flexibility of the installation);
- ON/OFF commands to authorize the use of the EV, by the user;

6.5.2 DEPLOYMENT AND ARCHITECTURAL INSTANTIATION

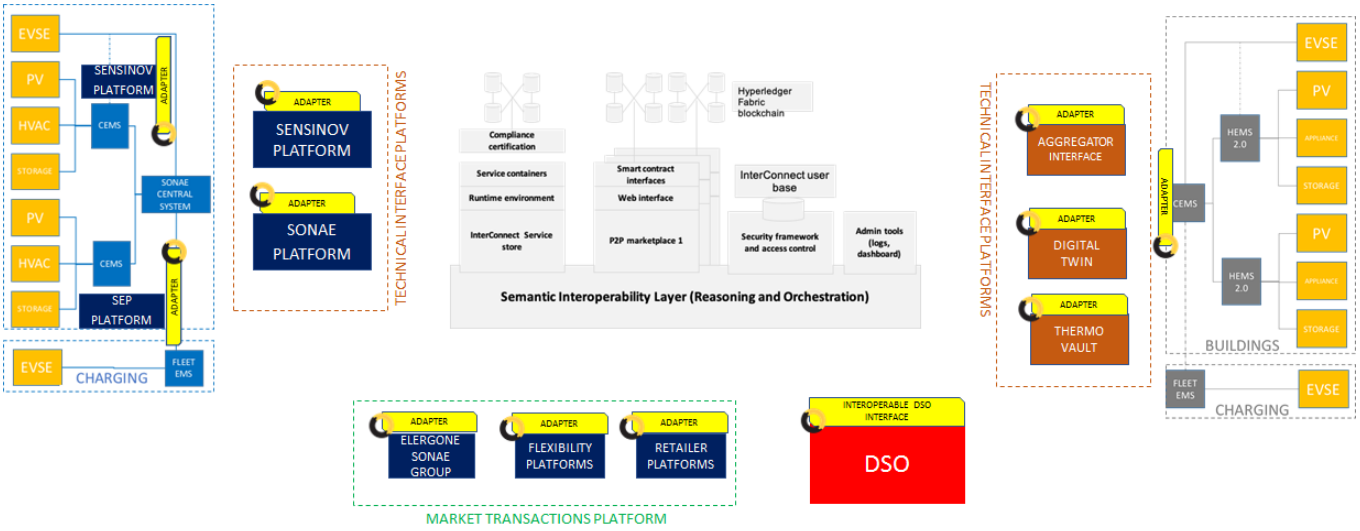


FIGURE 78 - PORTUGUESE PILOT ARCHITECTURE AND INITIAL MAPPING OF INTEROPERABILITY ADAPTERS

6.6 GERMANY

The German pilot has two sub-pilots:

- Hamburg Pilot and Beedip Architectures;
- Residential Pilot at Norderstedt.

The following sections provide detailed descriptions of each sub-pilot's objectives, defined use cases, and architectural implementation.

6.6.1 OVERVIEW SUB-PILOT HAMBURG AND BEEDIP ARCHITECTURES

Sub-Pilot title	**Commercial Pilot Hamburg**
Sub-Pilot leader	**KEO**
Participating partners	**KEO, IEE, Uni Kassel, EEBUS, Wirelane**
Location	**Hamburg**
Participating digital platforms from the catalogue	**beeDIP, Konect**
Participating digital platforms not part of the catalogue	**N/A**
Sub-Pilot Objectives	

This pilot aims to demonstrate how Smart Grid infrastructure can act as an enabler to integrate new demand from the business sector as DSF in e-markets. Moreover, the goal is to:

- Manage maximum power consumption of apartments or residential houses by setting power limitation setpoints which will be implemented by the energy management system with the support of connected, intelligent devices;
- Prevent blackout situations through overload protection logic of the energy management system and interoperable EEBUS communication;
- Enable flexible load adjustment and load shifting thanks to intelligent EEBUS devices;
- Enable cost-optimized operation of devices through flexible tariffs;
- Generate an energy forecast from the aggregated energy requirements of the complete building.

This sub-pilot combines the local DSO and ICT solution providers, offering the technical conditions required to test a standardized DSO interface between smart grid operation, market players, and end-users. Based on the German standardized Smart Meter Gateway infrastructure iMSys for the communication to DSO and marked place, it will allow the extension of SAREF to a new generation of interoperable HEMS systems.

Use Cases

Within WP1, several Use Cases requiring cross-platform interoperability were defined for this commercial pilot:

- **[HLUC 1] Cost optimized operation of devices:** flexible tariffs to balance production/ demand and enable price-optimized operation of devices at the customer site;
- **[HLUC 2] Power monitoring at grid connection point:** enhanced grid monitoring and transparency on building level to identify hot spots;
- **[HLUC 3] Power limitation at grid connection:** enable control of energy consumption in overload scenarios to prevent blackouts;
- **[HLUC 4] Local overload protection**: avoid local fuse breaker activation;
- **[HLUC 5] Indication to start uncontrolled devices when energy is cheap:** manually triggered power consumption in underload scenarios;
- **[[HLUC 7] Coordinated charging of EV:** enables negotiating charging plans for electric vehicles to meet energy requirements and optimization goals, such as cost savings by taking inexpensive PV energy;
- **[HLUC 8] Incentive table-based power consumption management:** enables the energy manager to negotiate the power consumption plan of devices (e.g., heat pump). The energy manager can also use the devices' flexibility through the price of energy (incentive table). Energy managers can negotiate consumption plans without touching the devices' internal process;
- **[HLUC 9] Flexible start of white-goods:** white-goods can offer their flexibility to the DSO by running at a later time, for instance.

Data
The following data is expected to be made available for this pilot's use case implementation: **MONITORING DIRECTION** • **Energy information**, e.g., power consumption, power production, voltage, current, charging plan of EVs, smart meter, etc.; **CONTROL DIRECTION** • power limitation set-point • local consumption power forecast and agreed power plan • Dynamic tariffs; **feed-in tariffs** subsidies.

6.6.2 DEPLOYMENT AND ARCHITECTURAL INSTANTIATION

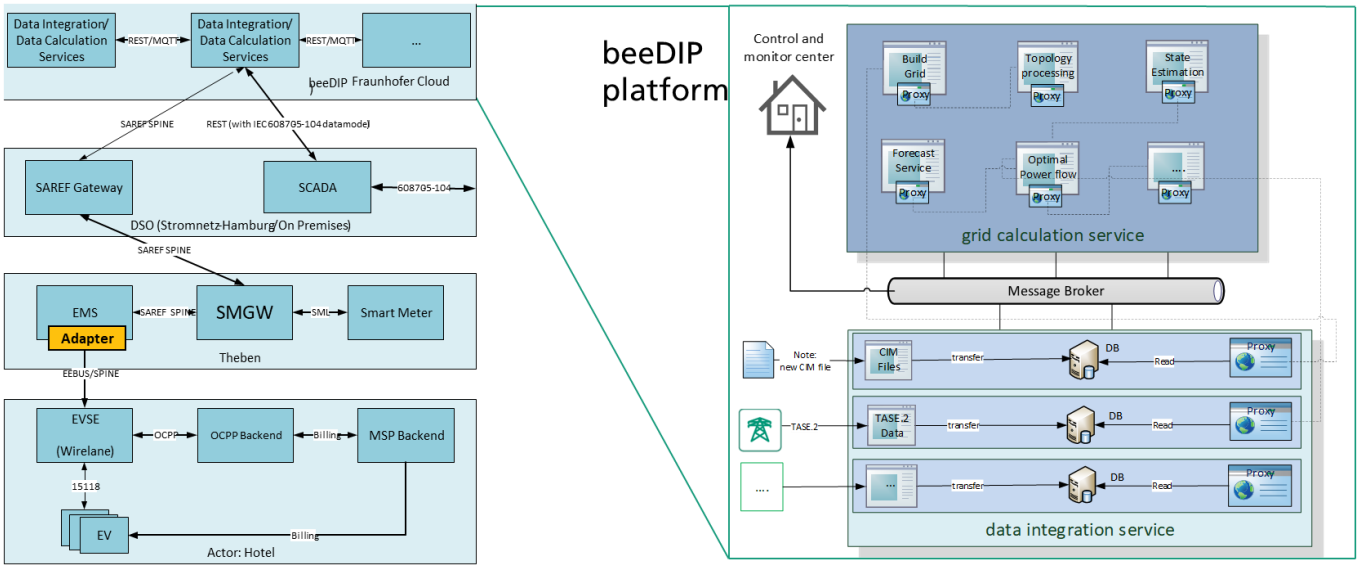


FIGURE 79 - GERMAN IEE SUB-PILOT ARCHITECTURE AND INITIAL MAPPING OF INTEROPERABILITY ADAPTERS

6.6.3 OVERVIEW SUB-PILOT NORDERSTEDT

Sub-Pilot title	**Residential Pilot Norderstedt**
Sub-Pilot leader	**EEBUS**
Participating partners	**EEBUS, KEO, Vaillant, Miele, Daikin, Wirelane, Whirlpool, BSH, BTT**
Location	**Norderstedt, Germany**
Participating digital platforms from the catalogue	**Konect**

Participating digital platforms not part of the catalogue	Stadtwerke Norderstedt

Sub-Pilot Objectives

This pilot aims to demonstrate how Smart Grid infrastructure can act as an enabler to integrate new demand from the business sector as DSF in e-markets. Moreover, the goal is to:

- Manage maximum power consumption of the buildings by setting power limitation setpoints which will be implemented by the energy management system with the support of connected, intelligent devices;
- Prevent blackout situations through overload protection logic of the energy management system and interoperable EEBUS communication;
- Aggregate charging plans of electric vehicles to offer flexibility;
- Enable flexible load adjustment and load shifting thanks to Intelligent EEBUS devices
- Enable cost-optimized operation of devices though flexible tariffs
- An energy forecast is generated from the aggregated energy requirements of the individual vehicles and devices

This sub-pilot combines residential and non-residential end-users, DSO, and ICT solutions providers, offering the technical conditions required to test a standardized DSO interface between smart grid operation, market players, and end-users. Based on the German standardized Smart Meter Gateway infrastructure iMSys for the communication to DSO and marked place, it will allow the extension of SAREF to a new generation of interoperable HEMS/BEMS systems.

Use Cases

Within WP1, several Use Cases requiring cross-platform interoperability were defined for this residential pilot:

- **[HLUC 1] Cost optimized operation of devices:** flexible tariffs to harmonize or production/demand and enable price-optimized operation of devices at the customer site;
- **[HLUC 2] Power monitoring at grid connection point:** enhanced grid monitoring and transparency on building level to identify hot spots;
- **[HLUC 3] Power limitation at grid connection:** enable control of energy consumption in overload scenarios to prevent blackouts;
- **[HLUC 4] Local overload protection**: avoid local fuse breaker activation;
- **[HLUC 6] EV fleet charging:** cost-optimized fleet charging while considering individual demands and grid constraints;

- **[HLUC 7] Coordinated charging of EV:** enables negotiating charging plans for electric vehicles to meet energy requirements and optimization goals, such as cost savings by taking cheap PV energy;

Data

The following data is expected to be made available for this pilot's use case implementation:

MONITORING DIRECTION

- **Energy information**, e.g., power consumption, power production, voltage, current, smart meter, etc.;

CONTROL DIRECTION

- power limitation set-point;
- power forecast and agreed power plan;
- Tariffs (static, with three distinct levels); feed-in tariffs subsidies.

6.6.4 DEPLOYMENT AND ARCHITECTURAL INSTANTIATION

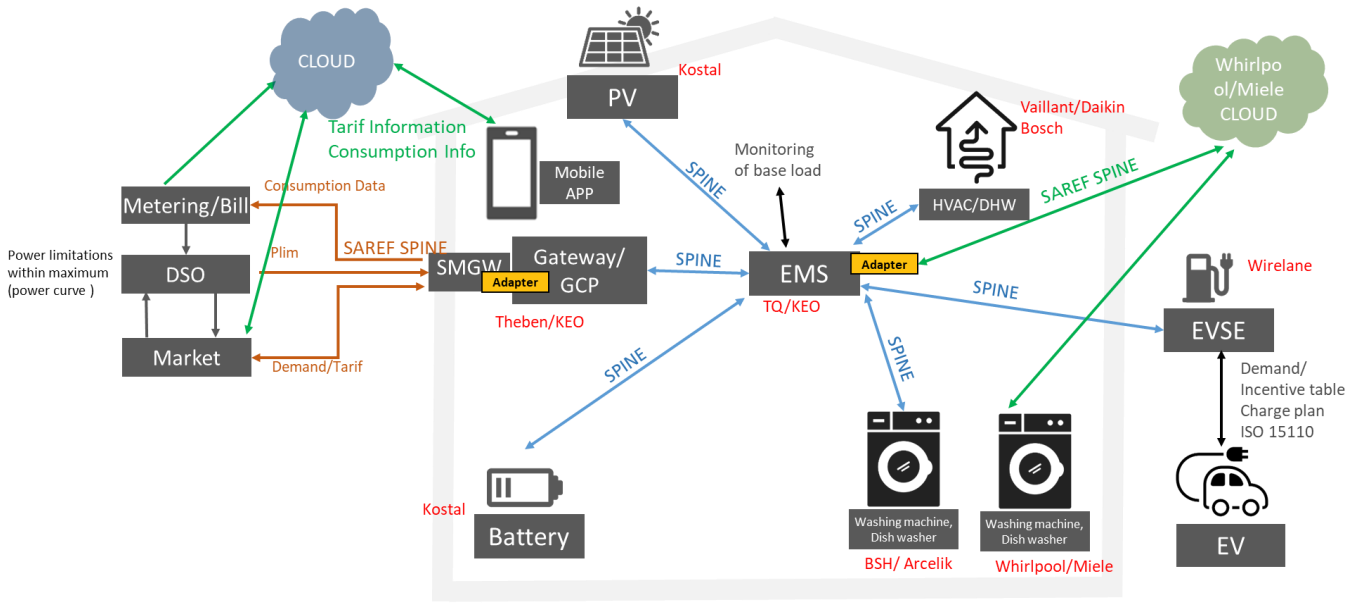


FIGURE 80 - GERMAN EEBUS SUB-PILOT ARCHITECTURE AND INITIAL MAPPING OF INTEROPERABILITY ADAPTERS

6.7 NETHERLANDS

6.7.1 OVERVIEW

Pilot title	**Dutch Pilot**
Pilot leader	**iCity - Hyrde**

Participating partners	**iCity, Hyrde, TNO**
Location	**Stijp-S - Eindhoven, Netherlands**
Participating digital platforms from the catalogue	**Hyrde Ekco IoT Platform, Hyrde Ekco API Marketplace, dEF-Pi, ReFlex**
Participating digital platforms not part of the catalogue	**Energy Monitoring Platform, Samsung SmartThings, Fiware context broker, Draco**

Pilot Objectives

The pilot's objective is to implement a set of devices, appliances, and sensors to increase the level of comfort and convenience while offering extra energy and non-energy services through the platform. Therefore, this pilot will explore and define the possibilities for demand-side flexibility and develop new business models for these services. This pilot will consist of two distinct locations:

- A residential building with rental apartments (the exact number of apartments will be known by M24); and
- A mixed-use building, with 10.000m2 office space and 50 privately owned apartments.

Use Cases

Two main high level use cases were defined for this pilot that require cross-platform interoperability:

- **[HLUC 1] Devices that can be controlled to free up time:** via an easy to use GUI (i.e., App and or (touch) screen display), users can easily set preferences for themselves but also for other persons in the household to automate tasks enabling normal daily life routines and tasks. By knowing who is at home, the system will automate based on set preferences. Devices, such as whitegoods, lighting, motion/presence sensors, thermostats, smart locks, smart switches etc., will be controlled remotely and automatically to improve end-users' comfort and health;
- **[HLUC 2] Devices that can be controlled to save money:** through a building management platform, all data is gathered and analyzed (via machine learning) by detecting trends. Systems will go to standby mode if the off-peak period arises in a building, i.e., during evenings for the elevator. Lights will be turned on only when movement is detected or expected. Monitoring will also be used to compare seasonality in energy consumption and allow for preventive maintenance (i.e., see unusual consumption) to optimize total energy usage.

Data

The following data is expected to be made available for this pilot's use case implementation:

MONITORING DIRECTION

- **Energy information**, e.g., power, power limitation setpoint, consumption, production, voltage, current, charging plan of EVs, smart meter, etc.;
- **Device type metadata,** context data, digital twin config, settings, status, updates;
- **Error codes**;
- Support **metrics**;
- Device data telemetry;
- Device and sensor context information.

CONTROL DIRECTION

- Setpoints for devices;
- Switching On/off;
- Dim value or percentage (value between a range 0 - 10 ; 0 - 100);
- Location / text attribute.

6.7.2 DEPLOYMENT AND ARCHITECTURAL INSTANTIATION

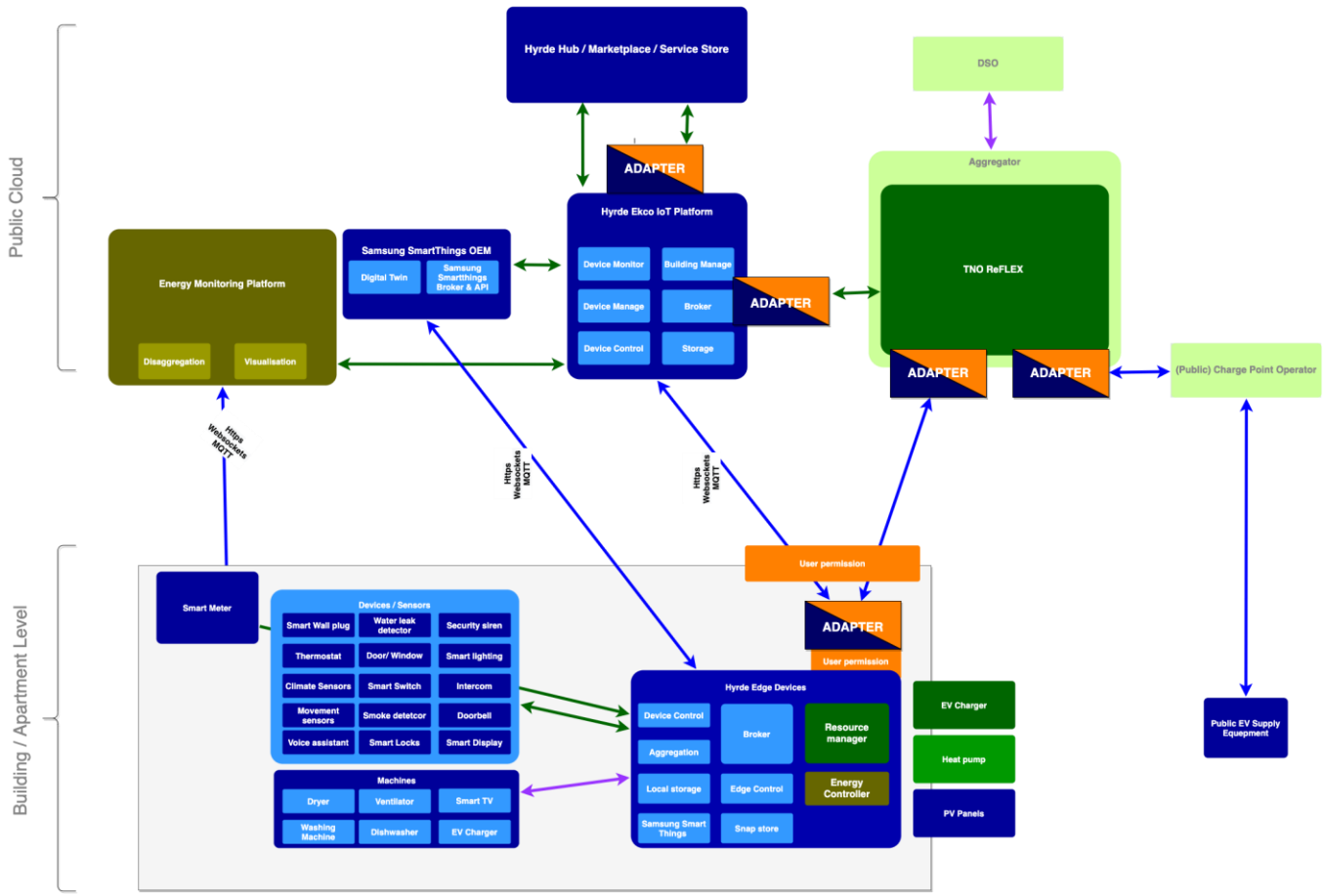


FIGURE 81 - DUTCH PILOT ARCHITECTURE AND INITIAL MAPPING OF INTEROPERABILITY ADAPTERS

6.8 ITALY

6.8.1 OVERVIEW

Pilot title	**Italian Pilot**
Pilot leader	**Planet Idea**
Participating partners	**Planet Idea, RSE, Whirlpool**
Location	**Milan, Italy**
Participating digital platforms from the catalogue	**Planet App**
Participating digital platforms not part of the catalogue	**N/A**

Pilot Objectives

This pilot has three main objectives, which can be detailed as follows:

- Test and demonstrate an interoperable energy management system for residential dwellings, leveraging on different home appliances (type and manufacturer);
- Guarantee a seamless interoperability and data exchange between systems and devices within the Planet App;
- Exploit energy and non-energy services, including flexibility services for grid support.

Use Cases

The work carried in WP1 led to the specification of the following use case for the Italian pilot:

- **[UC 2] Digital Platform for End-User Control and Awareness:** digital platforms collect and combine information from connected domestic appliances (IoT sensors and smart appliances status) and external information from external actors (smart tariff, flexibility service setpoints) to provide optimal flexibility service and cost-effective energy consumption. Users will be able to set their flexibility preferences for each device at a specific time. Information will be visualized through an APPservice, which provides a notification service for optimizing consumption during peak hours.

This pilot's interoperability requirements will allow different systems to integrate various data sources (from connected devices), guaranteeing a seamless communication and control (through APIs). On the other hand, the Digital Platform shall listen to setpoints requests exposed by the aggregator through its system. Devices need to activated/deactivated remotely and automatically through a set of secure APIs.

Data

Below, an overview of the type of data and commands that needs to be collected and executed for implementing this pilot's use cases:

MONITORING DIRECTION

- **Energy information**, e.g., historic/forecasted grid capacity, RES production, voltage level, power consumption, power needs, etc.;
- **Device data telemetry and status**, e.g., registration and status of connected devices; Consumption of connected devices; Power Capacity of connected devices;

CONTROL DIRECTION

- Peak shaving and load control of houses and dwellings. From a dedicated App, users can:
    - Choose what flexibility services he wants to offer and be informed about smart tariffs offered by the service provider;
    - Verify and control the seamless integration of a whole constellation of home devices.

Once access credentials for the digital services are verified and validated, through the Planet app, the consumer accepts data transfer. The living service provider will ask the manufacturer's cloud the list of connected devices (e.g., washer, dishwasher) claimed in the user account. The list of devices will be saved in the user's account.

The user selects in the EM App (part of Planet Idea's App) which devices he allows to be flexible. Once the Appliance is programmed to start, the Appliance (through its cloud) provides the information on Power Profile, Start and End time, which is visualized in the EM App. Users can also input boundary conditions for the shifting of the cycle in the EM App. On the EM cloud, all input from all users is aggregated. Users can disable or enable the flexibility for each device at any time.

6.8.2 DEPLOYMENT AND ARCHITECTURAL INSTANTIATION

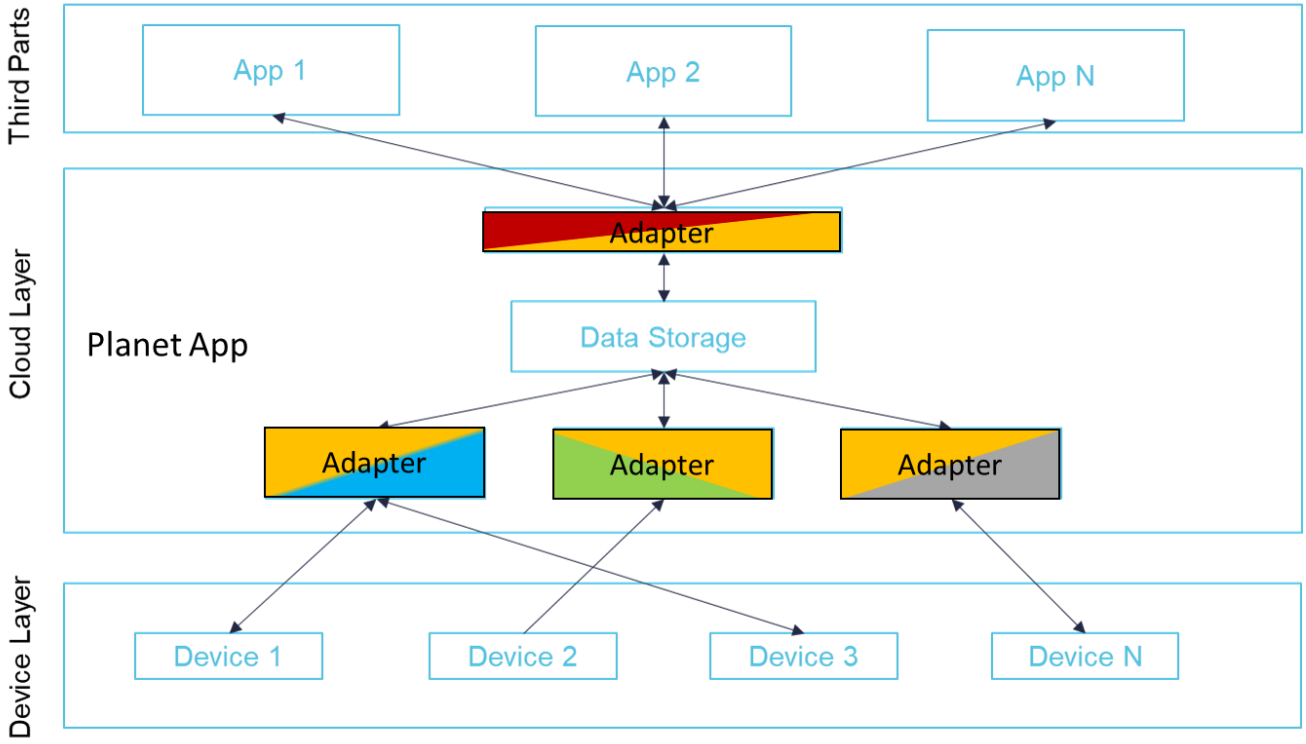


FIGURE 82 - ITALIAN PILOT ARCHITECTURE AND INITIAL MAPPING OF INTEROPERABILITY ADAPTERS

6.9 CROSS-PILOT DEMO FOR ANCILLARY SERVICES

6.9.1 OVERVIEW

Pilot title	**Cross-Pilot Demo of Pan-European Ancillary Services**
Pilot leader	**cyberGRID**
Participating partners	**cyberGRID**
Location	**N/A**
Participating digital platforms from the catalogue	**cyberNOC**
Participating digital platforms not part of the catalogue	**N/A**
Pilot Objectives	
The pilot will demonstrate the interoperability advantages between the digital platforms operating in several of the national pilots by creating an overarching demonstration. The focus	

is on showcasing the functionality that will be done using a service that enables exchanging flexibility information cross-border.

It aims to aggregate different energy assets across various project pilots into the flexibility pool, providing Pan-European cross border balancing services to the TSO.

Use Cases

Aggregation of different types of energy assets from various pilots generates the technical problem from the connectivity point of view. Each energy asset or, the more specifically, a RTU (Remote Terminal Unit), that connects energy assets with the SCADA systems, which has a dedicated standard and protocols to exchange the needed operations.

Because the Clean Energy for All Europeans package allows for even the smallest energy assets to contribute to flexibility, the number of such assets could drastically increase in the near future. This would also increase the overall number of private communication protocols and platforms. Therefore, interoperability will become an increasingly crucial system need since various vendors will require their specific standards to exchange the needed data. This would likely increase costs, security, and reliability problems to the critical infrastructure for the integrator of the balancing services and to the entire power network. Interoperability will be critical for realizing a well-functioning, efficient, and profitable flexibility market. This can be facilitated through the use of a flexibility aggregation platform in addition to addressing other technical specifications of the broader system, such as communication standards. This would also provide additional tools that could help facilitate TSO-TSO coordination efforts after the InterConnect project is over.

Due to the upper mentioned facts, it is essential to develop a secure, standardized, reliable, and reusable communication standard to exchange the required data among different stakeholders.

Data

For the operation of the flexibility management platform and allowing seamless integration between different pilots the generic energy asset needs to be modelled providing the at least the following set of attributes to be able to offer the balancing services to the TSO:

MONITORING DIRECTION

- Active power (generation, consumption);
- Availabilities; whether or not the asset is available to be activated for the balancing purposes;
- Forecasting data, short- or long-term forecasting. This information is important in the specific type of energy assets such as EVs (e.g. to know when certain a car will be connected to the charging station);
- Baseline data, short and/or long-term forecasting.
- (OPTIONAL) Other assets specific data; e.g., for battery: SOC, SOH, Temp, Reactive power, Current, Voltage, etc.;
- Setpoint ACK; acknowledgment of the setpoint that was received by the energy asset.

CONTROL DIRECTION

- Setpoint; ON/OFF or variable type of signal that the assets should follow (reducing increasing generation/consumption).

6.9.2 DEPLOYMENT AND ARCHITECTURAL INSTANTIATION

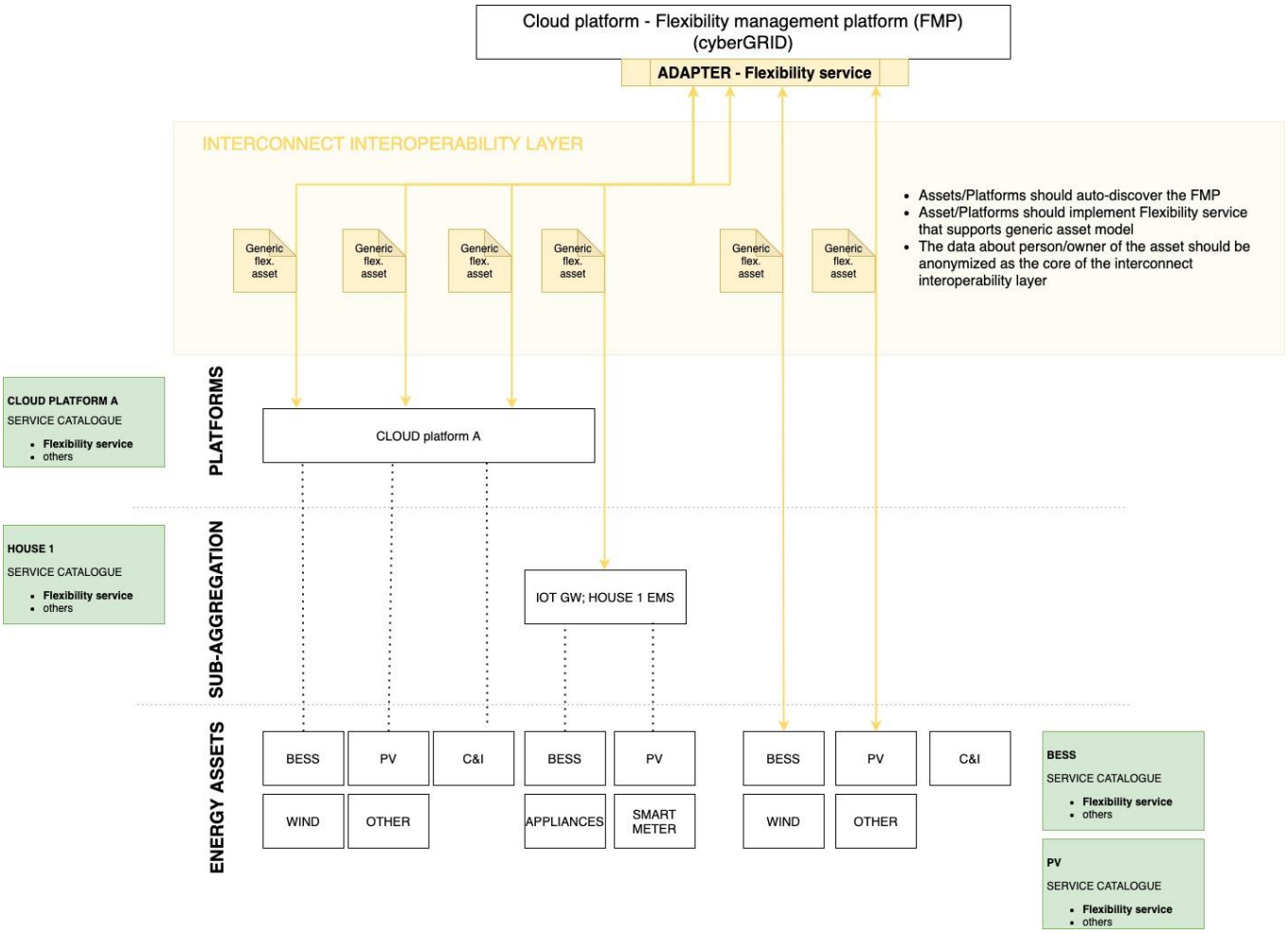


FIGURE 83 - CYBERGRID OVERARCHING USE CASE ARCHITECTURE AND INITIAL MAPPING OF INTEROPERABILITY ADAPTERS

6.10 IC'S CROSS-PLATFORM INTEROPERABILITY: CHALLENGES AND OPPORTUNITIES

This section provides an overview of the key challenges and opportunities arising in scenarios that require cross-platform interoperability.

(Sub-)Pilot leaders were asked to share their take on these two aspects: their answers, although diverse, can be aggregated into several coherent and more straightforward categories. However, aggregating all responses by a single criterion implied a level of genericity that is undesired (e.g., one of the challenges commonly addressed by respondents is "Interoperability"). Thus, Figure 85 and Figure 87 help provide a more in-depth view onto more specific concepts or categories. These figures can be interpreted as follows:

- The **left-hand** axis regroups the main aggregating criterion for each cited opportunity or challenge. Commonly cited categories are “Data”, “Stakeholders”, “System/Architecture”, and “InterConnect”;
- The **right-hand axis** details the repartition of the main criterion into sub-categories (e.g., commonly cited challenges can be classified in the category “Data Interoperability” or “Stakeholders Interoperability”);
- Since there was only a small pool of respondents, we did not consider it fit to produce an exhaustive quantitative analysis of these trends, but rather provide an insight into how commonly participants evoked a concept when responding. The **width of each link** conveys this information.

The next paragraphs will provide further insight into the responses supplied by IC partners.

In terms of **challenges**, the most cited elements are shown in Figure 84 and Figure 85:

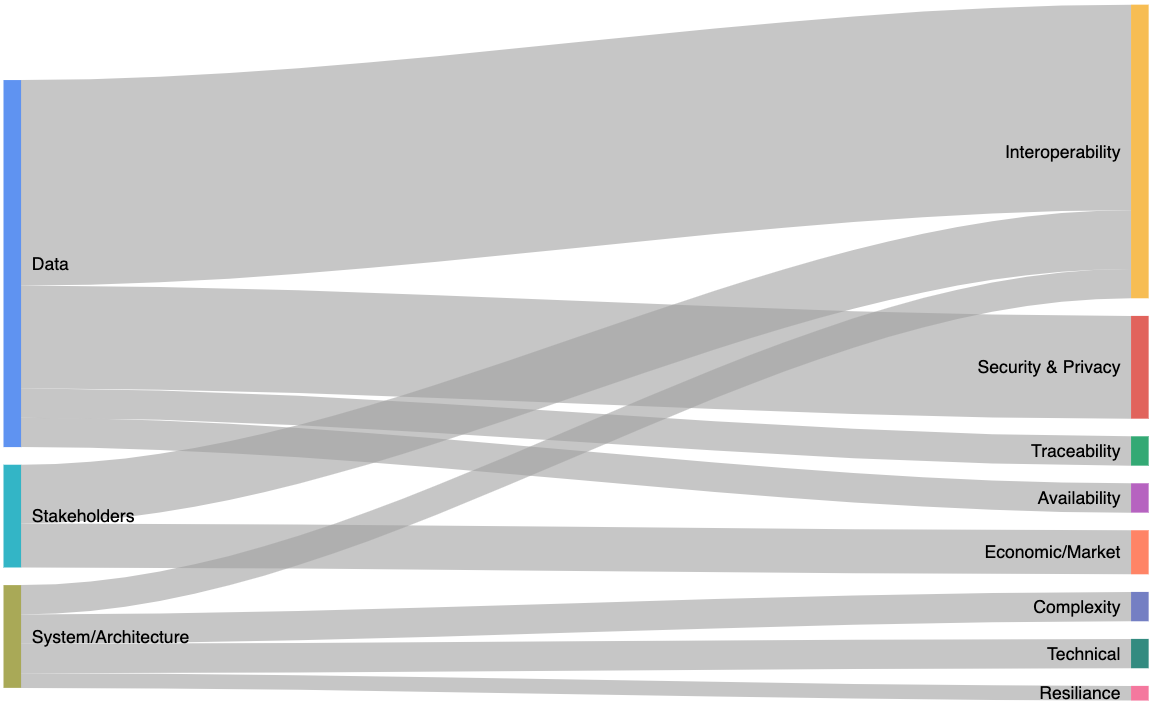


FIGURE 84 - MAIN CHALLENGES ARISING FROM CROSS-PLATFORM INTEROPERABILITY SCENARIOS

- **Data:** the most common challenge for all respondents is data, and it most often refers to ensuring data privacy & control, traceability and availability (from the perspective of the end-user). The technical, syntactic and semantic interoperability of data and metadata is also perceived as one of the major challenges to be addressed, namely when it comes to interfacing with the Grid and ensuring cross-platform interoperability.
- **Stakeholders:** stakeholders and the economic or regulatory environment are perceived as a challenge by some of the respondents. The stability and the foreseeable evolutions of the market (e.g., in terms of scalability) are difficult to predict, creating uncertainty. In terms of interoperability, proprietary ecosystems make it difficult to achieve interoperability amongst stakeholders (e.g., multi-vendor IoT platform).
- **System/Architecture:** refers to the technical (i.e., hardware and software components) and their current capabilities. A common concern is the increased system complexity and its effects

on the system's overall resilience. A lack of open end-points (e.g., APIs) is also noted by some participants, who also mention the lack of technical readiness and affordability in some cases.

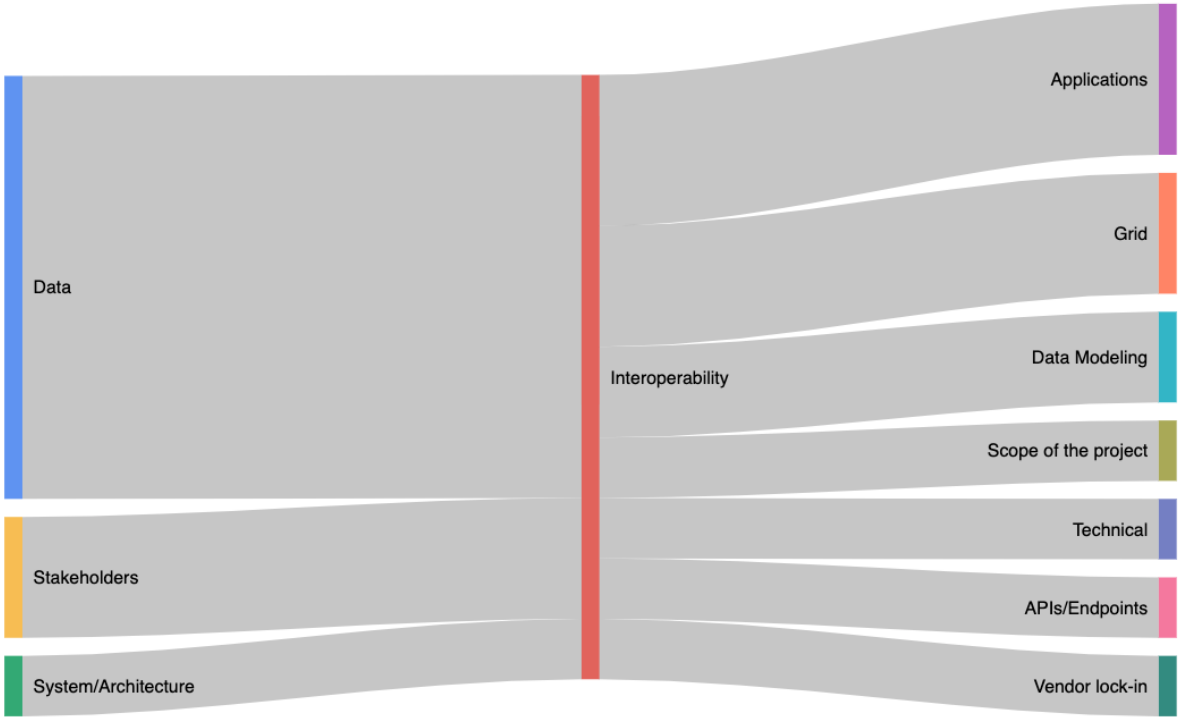


FIGURE 85 - FOCUS ON MAIN INTEROPERABILITY CHALLENGES

In terms of **opportunities**, the most cited elements are shown in Figure 86 and Figure 87, they cover the following topics:

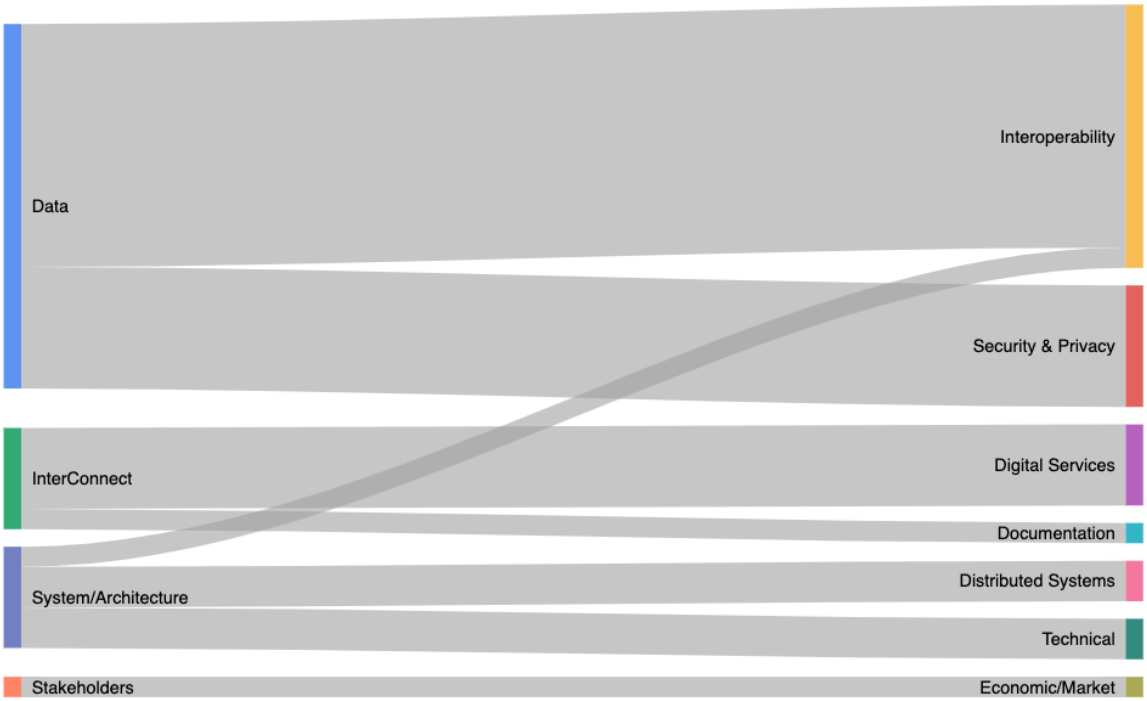


FIGURE 86 - MAIN OPPORTUNITIES ARISING FROM CROSS-PLATFORM INTEROPERABILITY SCENARIOS

- **Data:** most solutions cover aspects relating to data interoperability, e.g., common data models, interfaces, and development of software adapters and translators that can help achieve interoperability on a syntactic and semantic level. Solutions for ensuring data security & privacy via access control policies and by anonymizing and/or aggregating data. Privacy by design is also considered as an efficient solution to ensure system-wide security and end-users' right to privacy.
- **InterConnect:** the project is in itself an opportunity for advancing common cross-platform interoperability issues. In this regard, the IC Interoperability Framework and the set of enablers it will offer (e.g., P2P Marketplace, IC Service Store) will help promote and facilitate interoperability at a wide scale. Documentation also appears as an important aspect, also promoted by the project.
- **System/Architecture:** covers the set of solutions that can help unlock common challenges, e.g., local deployments and integrating the concept of "fallback design", for ensuring that systems are always available. Moreover, the technical complexity previously mentioned can be partially subdue via the development of virtual networks. Lastly, interoperability can be facilitated by offering a set of interoperable APIs and endpoints.
- **Stakeholders:** solutions for common stakeholder concerns offered by some respondents cover the creation of new KPIs and calculation methods that take into account additional measures for added value, e.g., increased sustainability of the grid. Improved user awareness and the creation of a large-scale proof of concept is also considered as an opportunity in this context.

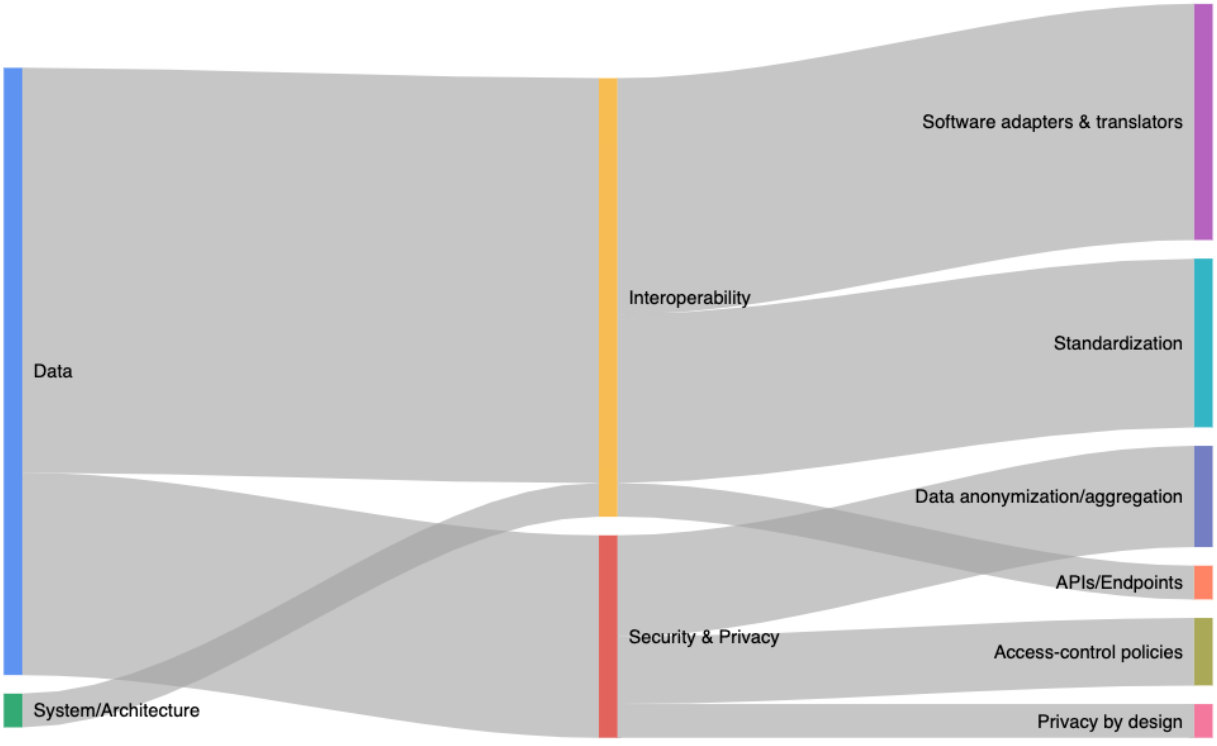


FIGURE 87 - FOCUS ON MAIN INTEROPERABILITY AND SECURITY & PRIVACY CHALLENGES

7. CONCLUDING REMARKS

This document reports the current progress and results of the WP5 (more precisely Task 5.1) activities within the InterConnect project.

This document starts with an analysis of other European IoT Platform Initiative projects from the perspective of achieved interoperability (with focus on semantic interoperability). Going forward, the InterConnect project will base its semantic interoperability framework on best practices documented by these projects.

Moreover, WP5 has the goal of making digital platforms - operated by the consortium partners - interoperable to enable realization of the project pilots and use cases. All digital platform operators from the consortium provided a set of information about their platforms including the main platform capabilities (services and interfaces) and capacities for interoperating with other platforms and services (APIs, data models, security and data protection mechanisms). This information about all participating digital platforms comprises the digital platform catalogue. In this document, overview of the digital platform catalogue is presented and results of the first round of digital platform interoperability analysis are introduced. Based on these results, the Task 5.2 “Implementation of the interoperability toolbox and service store” development and integration activities per digital platform and per IC interoperability framework enabler will be specified.

Next, this deliverable provides high level specification of the IC interoperability framework and its main components:

- Architecture of the IC interoperability framework and its relationship with the WP2’s IoT reference architecture for smart homes/buildings is presented;
- Details about the IC semantic interoperability layer are presented. The concept of IC semantic interoperability adapters and connectors is detailed in Section 5, together with short overview of the selected base technologies (Knowledge Engine, WoT, S-LOR). It is important to note that the key concepts of the interoperability layer (SAREF based data models and SPARQL+ interfaces) are still under development within WP2.
- The IC service store is presented as the main catalogue of all interoperable energy and non-energy services. The service store will be used by end users (service providers and service adopters/integrators) and by the semantic interoperability layer and reasoners participating in it.
- InterConnect project’s approach for enabling implementation of custom P2P marketplaces (for energy and non-energy transaction) is presented with focus on application of distributed ledger technologies. The P2P marketplace enablers will be further specified and developed within Task 5.4.
- The InterConnect security and data protection framework is introduced with the note that it is in early stages of development within Task 2.3 and Task 5.3. The main innovation pursued by the project relates to integration of authorization, access control and privacy protection mechanisms with the semantic interoperability layer.

Finally, interoperability requirements of all project (sub-)pilots are presented. For each project pilot an overview of the interoperability requirements, use cases, participating platforms and

data flows are provided. Each (sub-)pilot is accompanied with architecture figure presenting all participating digital platforms, key services and other endpoints on top of which the InterConnect interoperability framework will be instantiated. The first deployment decisions for hosting IC semantic interoperability adapters and connectors are discussed. It is important to note that each project (sub-)pilot is still being discussed within pilot teams. Therefore, the information presented in Section 6 of this document should be seen as report on the current status of these internal pilot discussions. All specifications and architectural overviews will be further updated and elaborated as the project reaches the kick-start of the pilots and use cases.

REFERENCES

EXTERNAL DOCUMENTS

[1] symbIoTe, "Final Report on System Requirements and Architecture," Pavle Skočir (UniZG-FER), 2017.

[2] symbIoTe, "Revised Semantics for IoT and Cloud resources," Michael Jacoby, 2017.

[3] BIG IoT, "High-level architecture specification," 2017.

[4] IoT European Platforms Initiative, "Advancing IoT Platforms Interoperability," River Publishers, 2018.

[5] INTER-IoT, "System Integration Plan," 2017.

[6] SynchroniCity, "Reference Architecture for IoT Enabled Smart Cities, Update," 2018.

[7] SynchroniCity, "Guidelines for the definition of OASC Shared Data Models," 2018.

[8] VICINITY, "VICINITY Architectural Design," 2017.

[9] FIESTA-IoT, "FIESTA-IoT Meta-Cloud Architecture," Francois Carrez, 2015.

[10] FIESTA-IoT, "Semantic Models for Testbeds Interoperability and Mobility Support and Best Practices V2," Rachit Agarwal/Nikolaos Georgantas/Valerie Issarny, 2016.

[11] "Eclipse AGAIL," 2020. [Online]. Available: https://projects.eclipse.org/proposals/eclipse-agail.

[12] AGILE IoT, "D1.1 AGILE Gateway architecture specifications and initial design," 2016.

[13] bIoTope, "D2.4 bIoTope SoS Reference Platform Specification," 2017.

[14] "Web of Things (WoT) Architecture," 2020. [Online]. Available: https://www.w3.org/TR/wot-architecture/.

[15] A. Gyrard, "Designing cross-domain semantic Web of things applications," Ubiquitous Computing, 2015.

[16] M. Serrano and A. Gyrard, "A Review of Tools for IoT Semantics and Data Streaming Analytics," *The Building Blocks of IoT Analytics - Internet-of-Things Analytics.*

[17] A. Gyrard, "Interpreting IoT Data with Sensor-based Linked Open Rules (S-LOR)," 2016.

[18] A. Gyrard and A. Sheth, "IAMHAPPY: Towards an IoT knowledge-based cross-domain well-being recommendation system for everyday happiness," 2020.

[19] P. Murdock, L. Bassbouss, A. Kraft, M. Bauer, O. Logvinov, M. Alaya, T. Longstreth, R. Bhowmik, P. Martigne, P. Brett, C. Mladin, R. Chakraborty, T. Monteil and M. Dadas, "Semantic Interoperability for the Web of Things," 2016.

[20] A. Gyrard, M. Serrano, S. Kanti Datta, J. Bosco Jares and M. Intizar Ali, "Sensor-based Linked Open Rules (S-LOR): An Automated Rule Discovery Approach for IoT Applications and its use in Smart Cities," Perth, Australia, 2017.

[21] M. Bauer, H. Baqa, S. Bilbao, L. Daniele, I. Esnaola-Gonzalez, M. Girod-Genet, P. Guillemin, A. Gyrard, W. Li, M. Lefrançois, A. Kung and J. Lee, "Semantic IoT Solutions - A Developer Perspective," 2019.

[22] C. Jennings, Cisco, Z. Shelby, Sensinode, J. Arkko and Ericsson, *Media Types for Sensor Markup Language (SENML),* 2012.

[23] A. Gyrard, C. Bonnet and K. Boudaoud, "Helping IoT application developers with sensor-based Linked Open Rules," *7th International Workshop on Semantic Sensor Networks, in conjunction with the 13th International Semantic Web Conference (ISWC),* 2014.

[24] A. Gyrard, C. Bonnet and K. Boudaoud, "Enrich Machine-to-Machine Data with Semantic Web Technologies for Cross-Domain Applications," Seoul, Korea, 2014.

[25] M. Bauer, H. Baqa, S. Bilbao, L. Daniele, I. Esnaola-Gonzalez, M. Girod-Genet, P. Guillemin, A. Gyrard, W. Li, M. Lefrançois, A. Kung and J. Lee, "Towards Semantic Interoperability Standards based on Ontologies," 2019.

INTERCONNECT DOCUMENTS

[26] InterConnect Grant Agreement number 857237.

[27] InterConnect project. “D1.1 Services and use cases for smart buildings and grids”. 2020.

[28] InterConnect project. “D2.1 Secure interoperable IoT smart home/building and smart energy system reference architecture”, unpublished report. 2020.

[29] InterConnect project. “D2.2 Privacy and security design principles and implementation guidelines”, unpublished report. 2020.

[30] InterConnect project. “D5.2 Data Flow Management”. 2020.